

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27



## Identity Assurance Framework: Overview

**Version:** 2.0

**Date:** 2010-04-24

**Editor:** Colin Soutar, CSC on behalf IAWG  
Joni Brennan, IEEE-ISTO

### Contributors:

The full list of contributors can be referenced here:  
<http://kantarainitiative.org/confluence/display/idassurance/IAF+2.0+Contributors>

### Abstract:

The Kantara Initiative Identity Assurance Work Group (IAWG) was formed to foster adoption of identity trust services. The primary deliverable of the IAWG is the Identity Assurance Framework (IAF), which comprises several documents that detail the levels of assurance, and the certification program that bring the Framework to the marketplace. The IAF comprises primary documents such as this Overview publication, the IAF [Glossary](#), a summary [Assurance Levels](#) document, and an [Assurance Assessment Scheme \(AAS\)](#), which encompasses the associated assessment and certification program, as well as two secondary documents: the [Service Assessment Criteria \(SAC\)](#), which establishes baseline criteria for general organizational conformity, identity proofing services, credential strength, and credential management services against which all CSPs will be evaluated; and the Assessor Qualifications and Requirements which provides an

28 overview of the requirements which applicant assessors must fulfill in order to become  
29 Kantara-Accredited Assessors.

30 This present document provides an overview of the IAF documents and program.

31

32 **Filename:** Kantara IAF-1000-Overview.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 Copyright: The content of this document is copyright of Kantara Initiative. © 2010  
55 Kantara Initiative.

56

57	<b>Contents</b>	
58		
59		
60	<b>1 INTRODUCTION .....</b>	<b>4</b>
61	<b>2 Understanding The Kantara Initiative Identity Assurance Framework .....</b>	<b>7</b>
62		

## 63 1 INTRODUCTION

---

64 This document relates to the Kantara Initiative Identity Assurance Framework [IAF]  
65 which has been developed within the Kantara Initiative Work Group (IAWG) and  
66 corresponding public special interest groups with input from members of the global  
67 financial services, government, healthcare, IT, and telecommunications sectors.

68 This document is intended to enable non-IAWG participants to understand and  
69 familiarize themselves with the IAF and thus be a starting point for industry professionals  
70 who want to learn more and possibly conform to the IAF.

71

### 72 1.1 Intended Audience

73

74 The intended audience for this document encompasses users of electronic identity  
75 credentials, entities that rely upon these electronic credentials, credential service  
76 providers who issue these electronic credentials, and assessors who review the business  
77 processes of credential service providers. This audience typically includes managers and  
78 decision makers responsible for developing strategies for managing access to online  
79 resources based on trustworthy identification of potential users, as well as providers of  
80 trustworthy online identity credentials.

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

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

88

### 89 1.2 Overview

90

91 In order to conduct any sort of business in an online world, entities (which include  
92 people, organizations, applications, machines, etc.) need to be able to identify themselves  
93 remotely and reliably. However, in most cases, it is not sufficient for the typical  
94 electronic credential (usually a basic userID/password pair or a digital certificate) to  
95 simply make the assertion that “I am who I say I am ... believe me.” A relying party  
96 needs to be able to know to some degree that the presented electronic identity credential  
97 truly represents the individual referred to in the credential. In the case of self-issued  
98 credentials, this is generally difficult. However, most electronic identity credentials are  
99 issued by Credential Service Providers (CSPs), often referred to as identity providers  
100 (IdPs): your workplace network administrator, your social networking service or online

101 game administrator, a government entity, or a trusted third party. You may have multiple  
102 credentials from multiple providers ... most people do.

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

- 104 1. Entities who are the subjects of identity credentials issued by a CSP, variously  
105 referred to as “subjects” or “credential holders”;
- 106 2. CSPs who are providers of identity services and issuers of electronic identity  
107 credentials;
- 108 3. Auditors or assessors who review the business processes and operating  
109 procedures that CSPs follow; and
- 110 4. Entities that rely upon the credentials issued by CSPs, referred to as “relying  
111 parties (RPs).”  
112

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

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

137 The [IAF](#) provides a means to enable relying parties to understand the trustworthiness of  
138 electronic identity credentials by other parties at commonly agreed levels of assurance.  
139 The IAF specifies the verification and proofing checks that CSPs carry out on entities, the  
140 way that CSPs run their services, and how the CSPs, themselves, are assessed by

141 accredited assessors to verify they are operating their services in conformance with their  
142 proclaimed level(s) of assurance and the stated terms of service.

143

144 The IAF is designed to be generic and thereby commensurate with a wide array of  
145 programs spanning the adopted four Assurance Levels, ranging from: open government  
146 programs operating at lower or medium assurance levels; to medium to high assurance  
147 applications such as access to patient electronic health records; to very-high assurance  
148 programs for defence, such as the Transglobal Secure Collaboration Program, where  
149 additional specificity may be provided by the Program, depending on particular business  
150 rules and process.

151

152

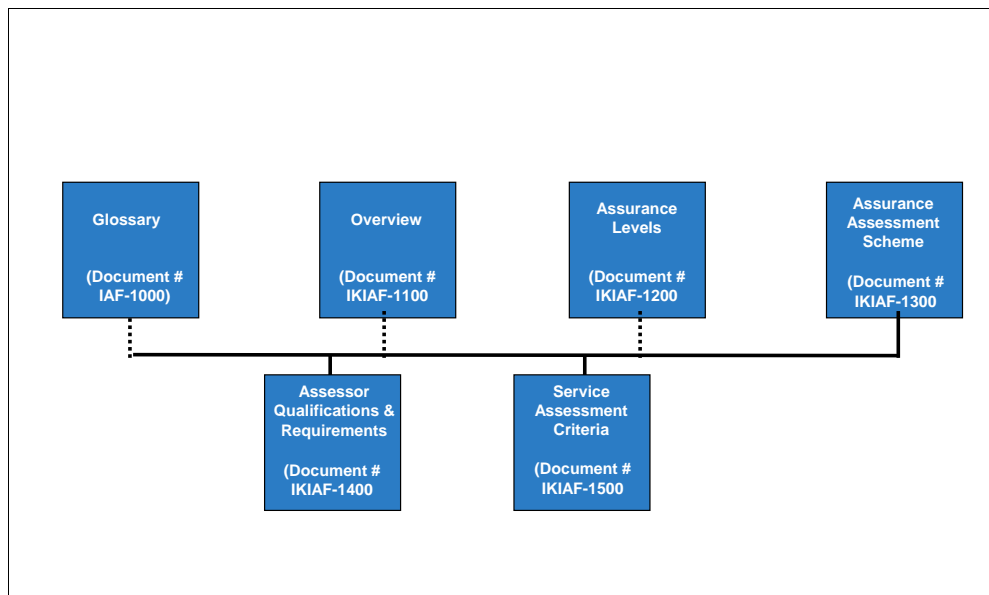
153 **2 UNDERSTANDING THE KANTARA INITIATIVE**  
154 **IDENTITY ASSURANCE FRAMEWORK**

---

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

- 158 1. Assurance Levels;
- 159 2. Glossary;
- 160 3. Assurance Assessment Scheme (AAS);
- 161 4. Service Assessment Criteria, and;
- 162 5. Assessor Qualifications and Requirements.
- 163 6. Associated Profiles

164  
165



166  
167

168 **2.1 Assurance Level Criteria**

169

170 Assurance levels are the levels of trust associated with a credential as measured by the  
171 associated technology, processes, and policy and practice statements. The IAF defers to the  
172 guidance provided by the U.S. National Institute of Standards and Technology (NIST)  
173 Special Publication 800-63 version 1.0.2 [NIST800-63] which outlines four levels of  
174 assurance, ranging in confidence level from low to very high. The level of assurance  
175 provided is measured by the strength and rigor of the identity verification and proofing

176 process, the credential's strength, and the management processes the CSP applies to it. The  
177 IAF then goes on to describe the service assessment criteria at each assurance level.

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

184 A summary of the IAF's approach to assurance levels is provided in the [Assurance Level](#)  
185 document.

186

## 187 **2.2 Glossary**

188 The [Glossary](#) document of the IAF provides a brief summary of commonly used terms that  
189 are used across IAF documents. It presents readers with a baseline understanding of how  
190 terms are used to enable better understanding of the programs and processes being discussed.  
191 As terms and usage can vary from industry to industry, it is recommended reading for anyone  
192 wanting a strong baseline understanding of the Identity Assurance Framework.

193

## 194 **2.3 Assurance Assessment Scheme**

195

196 The [Assurance Assessment Scheme](#) (AAS) portion of the IAF defines the phased approach  
197 used to establish criteria for certification and accreditation, initially focusing on CSPs and the  
198 accreditation of the assessors who will certify and evaluate them. The goal of this phased  
199 approach is to provide, initially, federations and Federation Operators with the means to  
200 certify their members for the benefit of inter-federation and to streamline the certification  
201 process for the industry. It is anticipated that follow-on phases will target the development of  
202 criteria for certification of federations, themselves, as well as best practices guidelines for  
203 relying parties.

204 The AAS establishes the requirements that assessors must have in order to perform  
205 assessments or audits, thus earning the associated Kantara Initiative Mark. It also defines the  
206 rules and requirements they will use when performing the actual assessments on CSPs vying  
207 to earn the associated Kantara Initiative Mark(s) for Kantara Initiative accreditation.

208

## 209 **2.4 Service Assessment Criteria**

210

211 The [Service Assessment Criteria](#) (SAC) document establishes baseline criteria for  
212 organizational conformity, identity-proofing services, credential strength, and credential  
213 management services against which all CSPs will be evaluated. The IAF also establishes a



214 protocol for publishing updates, as needed, to account for technological advances and  
215 preferred practice and policy updates.

216 These criteria set out the requirements that identity services and their CSPs must meet at each  
217 assurance level within the IAF in order to receive Kantara Initiative accreditation.

218 CSPs can determine the assurance levels at which their services might qualify by  
219 evaluating their overall business processes and technical mechanisms against the Service  
220 Assessment Criteria. The Service Assessment Criteria within each assurance level are the  
221 basis for assessing and approving electronic trust services.

222

223 Note that the Service Assessment Criteria defines Common Organization Criteria (CO-  
224 SAC) that must be conformed to by a CSP, as well as Credential Management (CM-  
225 SAC) and ID Proofing Criteria (ID-SAC). A CSP must demonstrate conformity to the  
226 CO-SAC and at least one of the CM-SAC and ID-SAC to attain the Kantara recognition  
227 mark.

228

## 229 **2.5 Assessor Qualifications and Requirements**

230

231 The Assessor Qualifications and Requirements document outlines the requirements  
232 which applicant assessors must fulfill in order to become Kantara-Accredited Assessors.  
233 These requirements will be used to validate applicants' suitability by the Assessment  
234 Review Board (ARB), according to the processes described in the [Assurance Assessment  
235 Scheme](#).

236

## 237 **2.6 Associated Profiles**

238

239 In addition to the generic IAF documents described above, particular implementation of  
240 the IAF may require ancillary specifications, relating to, for example, jurisdictional  
241 privacy principles or operational conditions. These ancillary specifications will be  
242 defined in IAF Profiles, and will be associated with the IAF certification process for that  
243 particular implementation.

244

245 **3 REFERENCES**

---

246 **3.1 Informative**

247

248 [CABForum] See the CA/Browser Forum website at <http://www.cabforum.org/>

249 [CAF] Louden, Chris; Spencer, Judy; Burr, Bill; Hawkins, Kevin; Temoshok, David;  
250 Cornell, John; Wilsher, Richard G.; Timchak, Steve; Sill, Stephen; Silver, Dave;  
251 Harrison, Von; eds., "E-Authentication Credential Assessment Framework (CAF)," E-  
252 Authentication Initiative, Version 2.0.0 (March 16, 2005).

253 <http://www.cio.gov/eauthentication/documents/CAF.pdf>

254 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework"  
255 Electronic Authentication Partnership, Version 1.0. (January 6, 2005)

256 [http://eap.projectliberty.org/docs/Trust\\_Framework\\_010605\\_final.pdf](http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf)

257 [IAF] Cutler, Russ, eds. "Liberty Identity Assurance Framework," Version 1.1, Liberty  
258 Alliance Project (21 June, 2008).

259 [http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-  
260 assurance-framework-v1.1.pdf](http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-<br/>260 assurance-framework-v1.1.pdf)

261 [NIST800-63] Burr, William E., Dodson, Donna F., Polk, W. Timothy, eds., "Electronic  
262 Authentication Guideline: Recommendations of the National Institute of Standards and  
263 Technology," Version 1.0.2, National Institute of Standards and Technology, (April,  
264 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)

265

266

## **Revision History**

267

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

268

a. Released by Liberty Alliance

269

b. Revision and scoping of Initial Draft release

270

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

271

a. Released by Liberty Alliance

272

b. Inclusion of comments to Final Draft

273

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

274

a. Documents contributed to Kantara Initiative by Liberty Alliance

275

4. XAPRIL2010 – Identity Assurance Framework Version 2.0

276

a. Released by Kantara Initiative

277

b. Significant scope build

278

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

279

280

i. Kantara IAF-1000-Overview

281

ii. Kantara IAF-1100-Glossary

282

iii. Kantara IAF-1200-Levels of Assurance

283

iv. Kantara IAF-1300-Assurance Assessment Scheme

284

v. Kantara IAF-1400-Service Assessment Criteria

285

vi. Kantara IAF-1600-Assessor Qualifications and Requirements

286