

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



Kantara Initiative Identity Assurance Work Group Interim Report

IDENTITY ASSURANCE FRAMEWORK: US Federal Profile

Version: 1.0 -- 8th draft (v1d8)

Date: 2010-04-03

Editor: David Wasley
Internet2

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 is comprised of many different documents that detail the Levels of Assurance and the assurance and certification program that brings the Framework to the marketplace. The IAF is comprised of a set of documents which includes an [Overview](#) publication, the IAF [Glossary](#), a summary [Assurance Levels](#) document, and an [Assurance Assessment Scheme](#) (AAS) document, which encompasses

27 the associated assessment and certification program. Central to the IAF, is the [Service](#)
28 [Assessment Criteria \(SAC\)](#), which establishes baseline criteria for general organizational
29 conformity, identity proofing services, credential strength, and credential management
30 services against which all Credential Service Providers (CSPs) – often referred to as
31 Identity Providers (IDP's) – will be evaluated. The present document, the US Federal
32 Profile, is intended to be utilized by assessors who are accrediting Credential Service
33 Providers (CSPs) who intend to meet the privacy and technology requirements put forth
34 by the US Federal Government through the General Services Administration (GSA)
35 administered Open Government Program with oversight from the Identity Credentialing
36 and Access Management (ICAM) Subcommittee of the US Federal CIO Council and, as
37 such, functions as a companion piece to the SAC for this specific application. Such CSPs
38 should review this document to confirm that their service meets these requirements and
39 assessors will utilize it when performing assessments that include this specific
40 certification.

41

42 **Filename:** *IAF-US Federal Profile v1-d6.doc*

43

44 **Copyright Notice:**

45

46 This document has been prepared by Participants of Kantara Initiative. Permission is
47 hereby granted to use the document solely for the purpose of implementing the
48 Specification. No rights are granted to prepare derivative works of this Specification.
49 Entities seeking permission to reproduce portions of this document for other uses must
50 contact Kantara Initiative to determine whether an appropriate license for such use is
51 available.

52

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

64

65 The content of this document is copyright of Kantara Initiative.

66 © 2010 Kantara Initiative.

67

68 1 INTRODUCTION

69
70 **Kantara Initiative Federal Profile for CSPs that desire certification under the IAF**
71 **for interoperation with US Federal Agency applications under the Open**
72 **Government program.**

73 74 **FOR DISCUSSION & FURTHER REVIEW**

75
76 *[Ed note: Context and background to be added; linkage with Kantara IAF to be*
77 *described; etc.]*

78
79 This profile is required for use with US Federal government applications in conjunction
80 with Kantara Initiative certified CSPs. This supplements the Kantara IAF level of
81 assurance requirements found in the SAC. No requirements found in the IAF SAC or this
82 Profile apply directly to Relying Party Applications (RPs). The Kantara Initiative
83 Identity Assurance Program, acting in the capacity of a Trust Framework Provider to the
84 US Federal Government, assumes that all US Agency RP applications will operate in
85 compliance to all US Federal privacy and identity management policies, laws and
86 regulations.

87
88 The Credential Service Provider (CSP) must assert and comply with an Identity Subject
89 Privacy Policy that provides for at least the following:

90 a. **Informed Consent** – At the time the Identity Subject initiates registration, the
91 CSP must provide the Subject a general description of the service and how it
92 operates including what information, if any, may be released by default to any
93 Relying Party and, if the Subject indicates intent to use the service to gain access
94 to Federal government applications, must make available to the Identity Subject
95 what additional information, if any, may be released to such applications. The
96 Subject must indicate consent to these provisions before registration can be
97 completed.

98 CSPs should provide a mechanism for Identity Subjects to deny release of
99 individual attributes to Federal government applications, as specified and
100 specifically accommodated for in the ICAM approved Authentication Scheme
101 being utilized by the CSP. It is recognized, and the Identity Subject should be
102 cautioned that such denial may result in a denial of service by the application
103 unless alternate means of access are provided to the Identity Subject by the
104 application itself.

105 Note: CSPs are not expected to provide such a mechanism for attribute-level opt-
106 out for Identity Subjects when the Identity Subject is engaging with a government
107 application on behalf of their employer or university and such attributes are

- 108 required by the RP application to complete the transaction, pre-arranged by policy
109 agreed to between the CSP and the RP well in advance of the transaction.
- 110 b. **Optional Participation** – Identity Subjects that are members, for example
111 employees, faculty, or students, of an organization that provides identity services
112 as part of its business processes should be allowed to opt-out of using that
113 organization’s identity services to gain access to government applications if such
114 access is not required by their organizational responsibilities or there is an
115 alternate means of access to the government application.
- 116 c. **Minimalism** – Identity Provider must transmit only those attributes that are
117 explicitly requested by the Federal RP application or required by the Federal
118 identity assertion profile.
- 119 d. **Unique Identity** -- Federal applications that do not require personally identifiable
120 identity information (PII) must be given a persistent abstract identifier unique to
121 the individual Identity Subject. When allowed by the technology, the CSP must
122 create a unique identifier for the Identity Subject that is also unique to each
123 Federal application.
- 124 e. **No Activity Tracking** – CSPs must not disclose information regarding Identity
125 Subject activities with any Federal application to any other party or use the
126 information for any purpose other than problem resolution to support proper
127 operation of the identity service, or as required by law.
- 128 f. **Adequate Notice** – At the time an Identity Subject initiates access to a Federal
129 government application, that application may provide text to be displayed to the
130 Subject before any PII is provided to the application by the CSP. That text may
131 include
- 132 • a general description of the authentication event,
 - 133 • any transaction(s) with the Federal application,
 - 134 • the purpose of the transaction(s),
 - 135 • and a description of any disclosure or transmission of PII that will be requested
136 by the Federal application.
- 137 The Subject should be allowed to cancel the access transaction at this point.
- 138 g. **Termination** – In the event an CSP ceases to provide this service, the Provider
139 shall continue to protect any sensitive data including PII and destroy it as soon as
140 its preservation is no longer required by law or regulation.
- 141 h. **Changes in the Service** – Should the CSP alter the terms of use of the service,
142 prompt notice must be provided to Identity Subjects. Such notice must include a
143 clear delineation of what has changed and the purpose of such changes.
- 144 i. **Dispute Resolution** – CSP’s must have a dispute resolution process for
145 addressing any dispute resulting from a complaint filed by an Identity Subject
146 utilizing its service who notifies the CSP regarding a failure to comply with any

147 terms in the CSP Service Definition required by the SAC, and/or any additional
148 criteria defined in this Profile. The CSP must provide evidence to their Kantara
149 Initiative Accredited Assessor both of the existence of this process and its
150 compliance thereto.

151 j. **Technology Requirements** – CSP’s must be compliant with one or more of the
152 ICAM-approved Authentication Schemes when engaged in any identity
153 transaction with government applications. (See <http://www.idmanagement.gov>
154 for the current list of technology protocols from which to choose.)