

1



2

3 Identity Assurance Framework

4

5 Additional Requirements for Credential 6 Service Providers: US Federal Privacy 7 Criteria

8

9

10 **Version:** 2.0

11 **Date:** 2012-02-15

12 **Editor:** David Wasley, Internet 2
13 Joni Brennan, Kantara Initiative

14 **Contributors:**

15 <http://kantarainitiative.org/confluence/x/GQAGAw>

16 **Status:** This document is a **Kantara Initiative Report**, approved by the Identity
17 Assurance WG (see section 3.8 of the Kantara Initiative Operating Procedures)

18 **Abstract:**

19 This Kantara Initiative Additional Requirements for Credential Service Providers
20 (CSPs) describes criteria that must be met by CSPs that are certified under the
21 Kantara Identity Assurance Framework (IAF) and desire additional certification for
22 interoperation with US Federal Agency applications under the Open Government
23 program.

24

25 **Note:** On 12 July 2011, the Kantara Assurance Review Board unanimously voted to
26 accept the FICAM Privacy Guidance for Trust Framework Assessors and
27 Auditors Version 1.0 as an assessment guide applicable to these US Federal Privacy

28 Criteria. That document should be reviewed and considered by Assessors and Auditors
29 when determining whether an Applicant CSP should be approved against the criteria
30 described in this document, and during re-assessment audits required for renewal of a
31 certification. The full FICAM Privacy Guidance document can be found on the Federal
32 Identity Management home page or by following this link :
33 http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV
34

35 **Filename:** Kantara Initiative_IAWG_US FPC Report_v2.0doc

36

37

37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59

Notice:

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

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

The content of this document is copyright of Kantara Initiative. © 2012 Kantara Initiative.

59 1 INTRODUCTION

60 **Kantara Initiative Additional Requirements for Credential Service Providers**
61 **(CSPs) describes criteria that must be met by CSPs that are certified under the**
62 **Identity Assurance Framework (IAF) and desire additional certification for**
63 **interoperation with US Federal Agency applications under the Open Government**
64 **program.**

65
66 These additional criteria supplement the Kantara IAF level of assurance requirements found
67 in the Service Assessment Criteria (SAC). The requirements found in the IAF SAC and
68 these additional criteria apply only to CSPs, not to Relying Parties (RPs). The Kantara
69 Initiative Identity Assurance Program, acting in the capacity of a Trust Framework
70 Provider to the US Federal Government, assumes that all US Agency RP applications will
71 operate in compliance with all US Federal privacy and identity management policies, laws
72 and regulations which include privacy protections for citizen personally identifiable information
73 (PII).

74 75 2 Identity Subject Privacy Requirements

76 The Credential Service Provider must assert and comply with an Identity Subject (Subject)
77 privacy policy that provides for at least the following:

78
79 2.1 **Informed Consent** – At the time the Subject initiates registration, the CSP must
80 provide the Subject a general description of the service and how it operates including
81 what information, if any, may be released by default to any Relying Party. If the
82 Subject indicates intent to use the service to gain access to Federal government
83 applications, the CSP must make available to the Subject a description of what
84 additional information, if any, may be released to such applications. The Subject must
85 indicate consent to these provisions before registration can be completed.

86
87 CSPs should provide a mechanism for Subjects to deny release of individual
88 attributes to Federal government applications, as specified and specifically
89 accommodated for in the ICAM approved Authentication Scheme being utilized
90 by the CSP. It is recognized, and the Subject should be cautioned that such denial
91 may result in a denial of service by the application unless alternate means of
92 access are provided to the Subject by the application itself.

93
94 If Subjects are allowed to establish a continuing approval or denial for release of
95 certain attributes, for example to avoid being asked anew each time, then there
96 must be some mechanism by which an Subject can alter or withdraw any of those
97 established preferences.

98
99 Note: CSPs are not expected to provide such a mechanism for attribute-level

- 100 opt- out for Subjects when the Identity Subject is engaging with a government
101 application on behalf of their employer or university. However, the attributes
102 required by the RP application to complete the transaction must be pre-
103 arranged by policy agreed to between the CSP and the RP well in advance of
104 the transaction and must comply with section 2.3 below.
105
- 106 **2.2 Optional Participation** – Subjects that are members, for example employees,
107 faculty, or students, of an organization that provides identity services as part of its
108 business processes should be allowed to opt-out of using that organization’s identity
109 services to gain access to government applications if such access is not required by
110 their organizational responsibilities or there is an alternate means of access to the
111 government application.
112
- 113 **2.3 Minimalism** – CSP must transmit only those attributes that are explicitly requested
114 by the Federal RP application or required by the Federal identity assertion profile.
115
- 116 **2.4 Unique Identity** -- Federal applications that do not require PII must be given a
117 persistent abstract identifier unique to the individual Subject. When allowed by the
118 technology, the CSP must create a unique identifier for the Subject that is also unique
119 to each Federal application.
120
- 121 **2.5 No Activity Tracking** – CSPs must not disclose information regarding Subject
122 activities with any Federal application to any other party or use the information for
123 any purpose other than problem resolution to support proper operation of the identity
124 service, or as required by law.
125
- 126 **2.6 Adequate Notice** – At the time an Subject initiates access to a Federal government
127 application, that application may provide text to be displayed to the Subject before
128 any PII is provided to the application by the CSP. That text may include
129 • a general description of the authentication event,
130 • any transaction(s) with the Federal application,
131 • the purpose of the transaction(s),
132 • and a description of any disclosure or transmission of PII that will be requested by
133 the Federal application.
134 The Subject should be allowed to cancel the access transaction at this point.
135
- 136 **2.7 Termination** – In the event a CSP ceases to provide credential services, the CSP must
137 ensure that any sensitive data including PII continues to be protected and destroyed as
138 soon as its preservation is no longer required by law or regulation.
139
- 140 **2.8 Changes in the Service** – If the CSP alters the terms of use of the service, prompt
141 notice must be provided to all Subjects. Such notice must include a clear delineation of
142 what has changed and the purpose of such changes.

143

144 2.9 **Dispute Resolution** – CSP’s must have a dispute resolution process for addressing
145 any dispute resulting from a complaint filed by a Subject utilizing its service who
146 notifies the CSP regarding a failure to comply with any terms in the CSP Service
147 Definition required by the SAC, and/or any additional criteria defined in this
148 document. The CSP must provide evidence to their Kantara Initiative Accredited
149 Assessor both of the existence of this process and its compliance thereto.

150

151 2.10 **Technology Requirements** – CSP’s must use one or more of the ICAM-
152 approved identity assertion protocol profiles when engaged in any identity transaction
153 with government applications. (See <http://www.idmanagement.gov> for the
154 current list of protocol profiles from which to choose.)

155

156

156 **Acronyms Used in this Document**

157

158 CSP Credential Service Provider

159 IAF Identity Assurance Framework

160 ICAM Identity, Credentialing, and Access Management

161 PII Personally Identifiable Information

162 RP Relying Party

163 SAC Service Assessment Criteria

164 US United States

165 WG Working Group

166