

1



2

3

## 4 **Identity Assurance Framework** 5 **Additional Criteria: US Federal Privacy**

6

7

8 **Version:** 2.0

9 **Date:** 2012-01-18

10 **Editor:** David Wasley, Internet 2  
11 Joni Brennan, Kantara Initiative

12 **Contributors:**

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

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

16 **Abstract:**

17 Kantara Initiative Federal Privacy Additional Criteria for CSPs that desire certification  
18 under the IAF for interoperation with US Federal Agency applications under the Open  
19 Government program.

20

21 **Note:** On 12 July 2011, the Kantara Assurance Review Board unanimously voted to  
22 accept the FICAM Privacy Guidance for Trust Framework Assessors and  
23 Auditors Version 1.0 as an assessment guide applicable to the US Government Federal  
24 Profile of the IAF. This document should be reviewed and considered by Assessors and  
25 Auditors when determining whether an Applicant Identity Provider should be approved  
26 against the US Federal Government Privacy Additional Criteria of the Identity Assurance  
27 Framework, and during re-assessment audits required for renewal of a certification. The  
28 full document can be found on the Federal Identity Management home page or by  
29 following this link :

30 [http://www.idmanagement.gov/drilldown.cfm?action=openID\\_openGOV](http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV).

31

32 **Filename:** Kantara Initiative\_IAWG\_US FP Report\_v2.0.doc

33

34

34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56

**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.

## 56 1 INTRODUCTION

---

57 **Kantara Initiative Federal Privacy Additional Criteria for Credential Service**  
58 **Providers (CSPs) that desire certification under the IAF for interoperation with**  
59 **US Federal Agency applications under the Open Government program.**

60  
61 This additional criteria is required for use with US Federal government applications in  
62 conjunction with Kantara Initiative certified CSPs. This supplements the Kantara IAF  
63 level of assurance requirements found in the SAC. [The requirements found in the IAF  
64 SAC and this additional criteria apply only to CSPs, not to Relying Party Applications  
65 (RPs).] The Kantara Initiative Identity Assurance Program, acting in the capacity of a Trust  
66 Framework Provider to the US Federal Government, assumes that all US Agency RP  
67 applications will operate in compliance to all US Federal privacy and identity management  
68 policies, laws and regulations.

## 70 2 Identity Subject Privacy Requirements

---

71 The Credential Service Provider must assert and comply with an Identity Subject  
72 Privacy Policy that provides for at least the following:

73  
74 2.1 **Informed Consent** – At the time the Identity Subject initiates registration, the CSP  
75 must provide the Subject a general description of the service and how it operates  
76 including what information, if any, may be released by default to any Relying Party and,  
77 if the Subject indicates intent to use the service to gain access to Federal government  
78 applications, must make available to the Identity Subject what additional information, if  
79 any, may be released to such applications. The Subject must indicate consent to these  
80 provisions before registration can be completed.

81  
82 CSPs should provide a mechanism for Identity Subjects to deny release of  
83 individual attributes to Federal government applications, as specified and  
84 specifically accommodated for in the ICAM approved Authentication Scheme  
85 being utilized by the CSP. It is recognized, and the Identity Subject should be  
86 cautioned that such denial may result in a denial of service by the application  
87 unless alternate means of access are provided to the Identity Subject by the  
88 application itself.

89  
90 [If Subjects are allowed to establish a continuing approval or denial for release of  
91 certain attributes, for example to avoid being asked anew each time, then there  
92 must be some mechanism by which an Identity Subject can alter or withdraw any  
93 of those established preferences.]

94  
95 [Note: CSPs are not expected to provide such a mechanism for attribute-level  
96 opt- out for Identity Subjects when the Identity Subject is engaging with a

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

- 140 notice must be provided to Identity Subjects. Such notice must include a clear  
141 delineation of what has changed and the purpose of such changes.  
142
- 143 **2.8 Dispute Resolution** – CSP’s must have a dispute resolution process for addressing  
144 any dispute resulting from a complaint filed by an Identity Subject utilizing its  
145 service who notifies the CSP regarding a failure to comply with any terms in the  
146 CSP Service Definition required by the SAC, and/or any additional criteria defined  
147 in this document. The CSP must provide evidence to their Kantara Initiative  
148 Accredited Assessor both of the existence of this process and its compliance thereto.  
149
- 150 **2.9 Technology Requirements** – CSP’s must use one or more of the ICAM-approved  
151 identity assertion protocol profiles when engaged in any identity transaction with  
152 government applications. (See <http://www.idmanagement.gov> for the current list  
153 of protocol profiles from which to choose.)  
154  
155

155 **Acronyms Used in this Document**

156

157 CSP Credential Service Provider

158 IAF Identity Assurance Framework

159 ICAM Identity, Credentialing, and Access Management

160 PII Personally Identifiable Information

161 SAC Service Assessment Criteria

162 US United States

163 WG Working Group |

164