

1



2

3

4 **Identity Assurance Framework:** 5 **US Federal Privacy Profile**

6

7

8 **Version:** 1.0

9 **Date:** 2010-06-24

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

12 **Contributors:**

13 <http://kantarainitiative.org/confluence/x/7gKDAg>

14

15 **Status:** This document is a **Kantara Initiative Report**, approved by the Identity
16 Assurance WG (see section 3.9 and 4 of the Kantara Initiative Operating Procedures)

17 **Abstract:**

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

21

22 **Filename:** kantara-report-iawg-iaf-us-federal-privacy-profile-1.0

23

24

25

Notice:

26

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.

27

28

29

30

31

32

33

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.

34

35

36

37

38

39

40

41

42

43

44

45

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

46

47 **1 INTRODUCTION**

48 **Kantara Initiative Federal Privacy Profile for CSPs that desire certification under**
49 **the IAF for interoperation with US Federal Agency applications under the Open**
50 **Government program.**

51
52 This profile is required for use with US Federal government applications in conjunction
53 with Kantara Initiative certified CSPs. This supplements the Kantara IAF level of
54 assurance requirements found in the SAC. No requirements found in the IAF SAC or this
55 Profile apply directly to Relying Party Applications (RPs). The Kantara Initiative
56 Identity Assurance Program, acting in the capacity of a Trust Framework Provider to the
57 US Federal Government, assumes that all US Agency RP applications will operate in
58 compliance to all US Federal privacy and identity management policies, laws and
59 regulations.

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

- 62
63 a. **Informed Consent** – At the time the Identity Subject initiates registration, the CSP
64 must provide the Subject a general description of the service and how it operates
65 including what information, if any, may be released by default to any Relying Party
66 and, if the Subject indicates intent to use the service to gain access to Federal
67 government applications, must make available to the Identity Subject what additional
68 information, if any, may be released to such applications. The Subject must indicate
69 consent to these provisions before registration can be completed.

70
71 CSPs should provide a mechanism for Identity Subjects to deny release of
72 individual attributes to Federal government applications, as specified and
73 specifically accommodated for in the ICAM approved Authentication Scheme
74 being utilized by the CSP. It is recognized, and the Identity Subject should be
75 cautioned that such denial may result in a denial of service by the application
76 unless alternate means of access are provided to the Identity Subject by the
77 application itself.

78
79 Note: CSPs are not expected to provide such a mechanism for attribute-level
80 opt- out for Identity Subjects when the Identity Subject is engaging with a
81 government application on behalf of their employer or university and such
82 attributes are required by the RP application to complete the transaction, pre-
83 arranged by policy agreed to between the CSP and the RP well in advance of
84 the transaction.

- 85
86 b. **Optional Participation** – Identity Subjects that are members, for example
87 employees, faculty, or students, of an organization that provides identity services as
88 part of its business processes should be allowed to opt-out of using that

- 89 organization's identity services to gain access to government applications if such
90 access is not required by their organizational responsibilities or there is an alternate
91 means of access to the government application.
92
- 93 c. **Minimalism** – Identity Provider must transmit only those attributes that are explicitly
94 requested by the Federal RP application or required by the Federal identity assertion
95 profile.
96
- 97 d. **Unique Identity** -- Federal applications that do not require personally identifiable
98 identity information (PII) must be given a persistent abstract identifier unique to the
99 individual Identity Subject. When allowed by the technology, the CSP must create a
100 unique identifier for the Identity Subject that is also unique to each Federal
101 application.
102
- 103 e. **No Activity Tracking** – CSPs must not disclose information regarding Identity
104 Subject activities with any Federal application to any other party or use the
105 information for any purpose other than problem resolution to support proper operation
106 of the identity service, or as required by law.
107
- 108 f. **Adequate Notice** – At the time an Identity Subject initiates access to a Federal
109 government application, that application may provide text to be displayed to the
110 Subject before any PII is provided to the application by the CSP. That text may
111 include
- 112 • a general description of the authentication event,
 - 113 • any transaction(s) with the Federal application,
 - 114 • the purpose of the transaction(s),
 - 115 • and a description of any disclosure or transmission of PII that will be requested
116 by the Federal application.
- 117 The Subject should be allowed to cancel the access transaction at this point.
118
- 119 g. **Termination** – In the event an CSP ceases to provide this service, the Provider shall
120 continue to protect any sensitive data including PII and destroy it as soon as its
121 preservation is no longer required by law or regulation.
122
- 123 h. **Changes in the Service** – Should the CSP alter the terms of use of the service, prompt
124 notice must be provided to Identity Subjects. Such notice must include a clear
125 delineation of what has changed and the purpose of such changes.
126
- 127 i. **Dispute Resolution** – CSP's must have a dispute resolution process for addressing
128 any dispute resulting from a complaint filed by an Identity Subject utilizing its
129 service who notifies the CSP regarding a failure to comply with any terms in the
130 CSP Service Definition required by the SAC, and/or any additional criteria defined
131 in this Profile. The CSP must provide evidence to their Kantara Initiative

- 132 Accredited Assessor both of the existence of this process and its compliance thereto.
133
134 j. **Technology Requirements** – CSP’s must be compliant with one or more of the
135 ICAM-approved Authentication Schemes when engaged in any identity transaction
136 with government applications. (See <http://www.idmanagement.gov> for the
137 current list of technology protocols from which to choose.)
138