

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 Privacy Profile

Version: .1

Date: 2009-11-23

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 AAS, and the
28 underworkings of the IAF, is the [Service Assessment Criteria \(SAC\)](#), which establishes
29 baseline criteria for general organizational conformity, identity proofing services,
30 credential strength, and credential management services against which all CSPs will be
31 evaluated. The present document, the US Federal Privacy Policy, is intended to be
32 utilized by assessors who are accrediting Credential Service Providers who intend to meet
33 the Privacy requirements put forth by the US Federal Government through the GSA
34 ICAM Program, and as such functions as a companion piece to the SAC for this specific
35 application. CSPs should review this document to confirm that their service meets these
36 requirements and assessors will utilize it when performing accreditations for this level of
37 certification.

38

39 **Filename:** *Identity Assurance Framework- US Federal Privacy Profile v.IDRAFT*

40

41

42 **Copyright Notice:**

43

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

50

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

62

63 The content of this document is copyright of Kantara Initiative. © 2009 Kantara
64 Initiative.

65

1 INTRODUCTION

Proposed Kantara Initiative Privacy Profile for CSPs that desire certification for interoperation with the US Federal Agencies under the GSA ICAM program.

FOR DISCUSSION & FURTHER REVIEW

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

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

- a. **Informed Consent** – CSP must inform the Identity Subject what information, if any, may be released by default to any Relying Party and must make available to the Identity Subject what additional information, if any, may be released to Federal government applications before any Identity Subject information is transmitted to any government applications.
Identity Provider should provide a mechanism for Identity Subjects to deny release of individual attributes for specific or any government applications unless required by their job duties. Such denial may result in a denial of service unless alternate means of access are provided by the application.
- b. **Optional Participation** – Identity Subjects that are members of an organization that provides identity services as part of its business processes should be allowed to Opt Out of using that organization’s identity services to gain access to government applications if such access is not required by their job duties or there is alternate means of access to the government application.
- c. **Minimalism** – Identity Provider must transmit only those attributes that are explicitly requested by the Federal RP application or required by the Federal identity assertion profile.
- d. **Unique Identity** -- Federal applications that do not require personally identifiable identity information (PII) must be given a persistent abstract identifier unique to the individual Identity Subject. When allowed by the technology, the CSP must create a unique identifier for the Identity Subject that is also unique to each Federal application.
- e. **No Activity Tracking** – CSPs must not disclose information regarding Identity Subject activities with any Federal application to any party or use the information for any purpose other than to support proper operation of the identity service, except as required by law.

- 105 f. **Adequate Notice** – Identity Provider must provide Identity Subjects with
106 adequate notice regarding their identity services and federated authentication.
107 Adequate Notice includes a general description of the service and how it operates.
108 In addition, unless specifically forbidden by law or regulation, Identity Subjects
109 should be able to obtain easily a record of their use of the service within the most
110 recent 6 months for access to Federal government applications including
111 authentication events, any identity transaction(s) with government applications,
112 and a description of any disclosure or transmission of PII to any government
113 application.
- 114 g. **Termination** – In the event an Identity Provider ceases to provide this service, the
115 Provider shall continue to protect any sensitive data including PII and destroy it as
116 soon as its preservation is no longer required by law or regulation.
- 117 h. **Changes in the Service** – Should the CSP alter the terms of use of the service,
118 prompt notice must be provided to Identity Subjects. Such notice must include a
119 clear delineation of what has changed and the purpose of such changes.
120