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

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

Filename: *Identity Assurance Framework- US Federal Privacy Profile v.1DRAFT*

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 <u>should</u> 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 <u>should</u> 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.

f. **Adequate Notice** – Identity Provider must provide Identity Subjects with adequate notice regarding their identity services and federated authentication. Adequate Notice includes a general description of the service and how it operates.

In addition, unless specifically forbidden by law or regulation, Identity Subjects should be able to obtain easily a record of their use of the service within the most recent 6 months for access to Federal government applications including authentication events, any identity transaction(s) with government applications, and a description of any disclosure or transmission of PII to any government application.

g. **Termination** – In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII and destroy it as soon as its preservation is no longer required by law or regulation.

h. **Changes in the Service** – Should the CSP alter the terms of use of the service, prompt notice must be provided to Identity Subjects. Such notice must include a clear delineation of what has changed and the purpose of such changes.