Kantara Initiative Identity Assurance Work Group Interim Report

IDENTITY ASSURANCE FRAMEWORK: US Federal Profile

Version: **1.0 -- 8th draft (v1d8)**

Date: 2010-04-03

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 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 Credential Service Providers (CSPs) – often referred to as Identity Providers (IDP's) – will be evaluated. The present document, the US Federal Profile, is intended to be utilized by assessors who are accrediting Credential Service Providers (CSPs) who intend to meet the privacy and technology requirements put forth by the US Federal Government through the General Services Administration (GSA) administered Open Government Program with oversight from the Identity Credentialing and Access Management (ICAM) Subcommittee of the US Federal CIO Council and, as such, functions as a companion piece to the SAC for this specific application. Such CSPs should review this document to confirm that their service meets these requirements and assessors will utilize it when performing assessments that include this specific certification.

Filename: *IAF-US Federal Profile v1-d6.doc*

Copyright Notice:

1 INTRODUCTION

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

FOR DISCUSSION & FURTHER REVIEW

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

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

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

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

   Note: CSPs are not expected to provide such a mechanism for attribute-level opt-out for Identity Subjects when the Identity Subject is engaging with a government application on behalf of their employer or university and such attributes are

required by the RP application to complete the transaction, pre-arranged by policy agreed to between the CSP and the RP well in advance of the transaction.

b. **Optional Participation –** Identity Subjects that are members, for example employees, faculty, or students, 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 organizational responsibilities or there is an 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 other party or use the information for any purpose other than problem resolution to support proper operation of the identity service, or as required by law.

f. **Adequate Notice** – At the time an Identity Subject initiates access to a Federal government application, that application may provide text to be displayed to the Subject before any PII is provided to the application by the CSP. That text may include
   - a general description of the authentication event,
   - any transaction(s) with the Federal application,
   - the purpose of the transaction(s),
   - and a description of any disclosure or transmission of PII that will be requested by the Federal application.

   The Subject should be allowed to cancel the access transaction at this point.

g. **Termination** – In the event an CSP 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.

i. **Dispute Resolution** – CSP's must have a dispute resolution process for addressing any dispute resulting from a complaint filed by an Identity Subject utilizing its service who notifies the CSP regarding a failure to comply with any

terms in the CSP Service Definition required by the SAC, and/or any additional criteria defined in this Profile. The CSP must provide evidence to their Kantara Initiative Accredited Assessor both of the existence of this process and its compliance thereto.

j. **Technology Requirements –** CSP's must be compliant with one or more of the ICAM-approved Authentication Schemes when engaged in any identity transaction with government applications. (See http://www.idmanagement.gov for the current list of technology protocols from which to choose.)