Identity Assurance Framework
Additional Criteria: US Federal Privacy

Version: **2.0**

Date: 2012-01-18

Editor: David Wasley, Internet 2
Joni Brennan, Kantara Initiative

Contributors:

http://kantarainitiative.org/confluence/x/GQAGAw

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

Abstract:

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

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

http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV.

Filename: Kantara Initiative_IAWG_US FP Report_v2.0.doc

Notice:

1 INTRODUCTION

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

This additional criteria 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. The requirements found in the IAF SAC and this additional criteria apply only to CSPs, not 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.

2 Identity Subject Privacy Requirements

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

2.1 **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.

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

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. However, the attributes required by the RP application to complete the transaction must be pre-arranged by policy agreed to between the CSP and the RP well in advance of the transaction and must comply with section 2.3 below.

2.2 **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.

2.3 **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.

2.4 **Unique Identity --** Federal applications that do not require personally identifiable 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.

2.5 **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.

2.6 **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.

2.7 **Termination** – In the event a 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.

2.8 **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.

2.8 **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 document. The CSP must provide evidence to their Kantara Initiative Accredited Assessor both of the existence of this process and its compliance thereto.

2.9 **Technology Requirements –** CSP's must use one or more of the ICAM-approved identity assertion protocol profiles when engaged in any identity transaction with government applications. (See http://www.idmanagement.gov for the current list of protocol profiles from which to choose.)

Acronyms Used in this Document

CSP	Credential Service Provider
IAF	Identity Assurance Framework
ICAM	Identity, Credentialing, and Access Management
PII	Personally Identifiable Information
SAC	Service Assessment Criteria
US	United States
WG	Working Group