**PRIVACY FRAMEWORK**

**General Description**

**Draft 15 April 2011**

**Kantara Initiative Mission**: Foster identity community harmonization, interoperability, innovation, and broad adoption through the development of open identity specifications, operational frameworks, education programs, deployment and usage best practices for privacy-respecting, secure access to online services.

The privacy environment for identity federations is multi-layered and complex. All participants in an identity federation must comply with applicable statutes, regulations, and in some industries, ethical standards. Beyond that, identity federations can set organizational standards and policies to which they bind their members through contracts or operating rules. Within those standards and policies, identity federations can determine architectures for consumer choice with respect to the personal identity information used for issuance, use and management of identity credentials.

The Kantara Privacy Framework is a set of principles and high-level requirements for collection, use, exchange and retention of personal information associated with Kantara-certified identity federations. The Framework contains the principles that have been developed over the past several decades and serve as a basis for law and regulation around the world. These principles are translated into specific requirements within Privacy Profiles, which apply to federations operating in specific industry verticals or regions. Privacy Profiles will interpret the Framework principles and requirements in light of their specific legal, regulatory, cultural, and contractual constraints and will be tied to a set of service assessment criteria against which a Kantara certification will be issued.

At this time, the Kantara Privacy Framework is a work in progress. The table below illustrates the relationship between the Framework, the Privacy Profiles, and the service assessment criteria. It is shown for illustrative purposes only.

|  |  |  |  |
| --- | --- | --- | --- |
| **Principle** | **Privacy Framework** | **Privacy Profile: US ICAM** | **Service Assessment Criteria:**  **IAF-1400 v. 0.9.1** |
| Notice | Participants in Kantara-certified Identity Federations must provide notice to individuals regarding privacy policies and practices of federation participants. | 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. | **3.5.1.2 Notices and User information**AL1\_CO\_NUI#010 General Service DefinitionAL1\_CO\_NUI#020 Service Definition inclusionsEtc. |
| Disclosure Limitation | Participants in a Kantara-certified Identity Federation may release identity information, including transfer, provision of access to, or divulging in any other manner, only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately. | Identity Provider must transmit only those attributes that are explicitly requested by the Federal RP application or required by the Federal identity assertion profile. | **TBD** |