**Date: 4-12-2012**

**PAC Drafting Conference Call**

**Attendees:**

Ann Geyer
Collin Soutar
Nathan Faut
Tom Smedinghoff
Mark Lizar

1. **Drafting Discussion --General**
	* Discussed general scope and intent of document.
	* Clarified that the initial versus of the PAC will provide guidance to Kantara approved assessors about how to audit the privacy requirements applicable to CSPs issuing credentials under the US Federal Identity Profile. Guidance for assessing other national (jurisdictional) requirements can be incorporated into the PAC in the future.
	* Discussed the distinction between an IdP (proofing) and CSP (credential issuing). Clarified that the PAC will refer to the CSP function.
	* Discussed the need to understand and then describe for the assessor how the PAC fits into the Kantara Assurance Framework—perhaps a document map would be useful for this purpose.
	* Discussed the confusion about whether the US Federal Profile is a FICAM or Kantara document. Clarified that FICAM has a Profile and the “Additional Requirements” document is how Kantara incorporated the FICAM profile into its document suite.
	* Discussed whether the PAC should introduce via guidance, additional privacy requirements. Decided that guidance should address requirements already approved by Kantara. If additional privacy requirements are warranted, this question and related work items should be framed and managed at the P3WG level, not the PAC drafting level. Note—strong support exists among several P3WG members that more privacy protection is warranted.
	* Discussed how best to organize the PAC drafting effort. Decided to take each numbered requirement of the Profile in order. After we have completed a couple requirement paragraphs, we can reassess the question of what guidance may be needed of a general nature.
2. **Drafting Discussion – Informed Consent #2.1**
	* Discussed how to interpret the requirement that the registration process be “clearly separate.” Consensus that this means that the process of collecting registration information be distinct from other processes and recognizably distinct to the individual registering. We could not reach a decision on whether the separation statement also meant to include the physical location at which the registration information is collected, processed, and maintained. This issue is put on the parking lot for further discussion.
	* Clarified the guidance should include what “evidence” is recommended to verify that a requirement is met.
	* Clarified that we should use, where appropriate, the terms—OBSERVE, INQUIRE, INSPECT—to organize the recommended actions of the auditor and to organize the manner in which evidence is obtained. These terms are standard terminology to auditors.
	* OBSERVE—the process of registering an individual is distinct from all other CSP functions.
	* INSPECT—the CSP has clearly described the services offered in language understandable by the targeted population. The service description should align closely with the Kantara SAC. Guidance may point to the AICPA SOC webtrust for CA.
	* EVIDENCE of the informed consent
	At a minimum, evidence of the individual’s name, signature, date and time of signature
	OBSERVE this evidence is created during the registration process
	INSPECT that this evidence is maintain over the credential lifecycle
	* The CSP may use the industry standard web privacy policy to provide notice and scope for the informed consent. The policy should include at a minimum, what information about the individual is collected, how it is used over the lifecycle of the information, what is the expected lifecycle.
3. **Parking Lot Items**
	* Does the phrase “registration must be clearly separate” extend to the physical environment?

1. **Tasks Assigned**
* Ask the Kantara ARB for a description of its role and its expectations of assessors to include in the PAC introductory sections. Nathan Laut
1. **Items Referred to Full P3WG**
	* Clarify the scope of the PAC—are new or augmented privacy requirements appropriate for the PAC? Tom and Colin will work on a charter document to sort this issue out.

1. **Attachments:** none