Kantara Initiative Response to OIF RFI

We are pleased to offer this response to your RFI, dated Nov. 22, 2009 7:05 ET. As noted by Brett McDowell in his response on Nov. 23, our full response was delayed pending discussion of this response by our Board of Directors, who met on Dec. 3 in the evening. We appreciate that this delay is acceptable.

As noted in your RFI materials, some of the details about your OIF program are still evolving. As such, our responses have been developed based on the information provided, but we welcome the opportunity to discuss these further, answer follow-up questions based on more information, etc.

1. **What aspects of your organization or its products, services, expertise, relationships, business model, or other factors do you feel are a particularly good fit with those requested under this RFI?**

To best answer this question, a high level understanding of Kantara Initiative, its various participants, its output and its certification and assurance program is important as any or all of this could be utilized by the OIF at various stages.

The Identity Assurance Framework (IAF) forms the basis of the Kantara Initiative trust framework offerings. The primary features in the IAF are:

- An Overview: http://kantarainitiative.org/confluence/download/attachments/655421/Kantara+IAF-1000-Overview.pdf
- A Glossary: http://kantarainitiative.org/confluence/download/attachments/655421/Kantara+IAF-1100-Glossary.pdf
- A summary of Assurance Levels: http://kantarainitiative.org/confluence/download/attachments/655421/Kantara+IAF-1200-Levels+of+Assurance.pdf
    - NOTE: The three above documents were originally combined in a single document, with the Service Assessment Criteria document; we determined these are better separated, and are thus in the process of voting out the new, self-standing versions of the documents; for historical purposes, you may review the fully published versions as part of v1.1 of the Identity Assurance Framework document available here: http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-assurance-framework-v1.1.pdf
- Description of the Assurance Assessment Scheme – [IAF-AAS] available here: http://bit.ly/kantara-IAF-1300-assurance-assessment-scheme (NOTE: this was also previously published under the Liberty Alliance but is in draft update within Kantara Initiative currently; for historical purposes, the Liberty Alliance URL for this

(c) 2009 Kantara Initiative

document is: http://kantarainitiative.org/confluence/download/attachments/655421/Liberty+IAF-1300+draft+0.8+AAS.pdf)

The first three documents above are applicable to all elements and levels of the IAF and serve as the reference basis for all other documents. [IAF-AAS] describes, both generically and specifically, the nature of and processes relating to each of the Kantara Initiative forms of Grant of Rights to use the Kantara Initiative Assurance Mark, this Mark being the principal form of recognition offered by the IAF processes.

At the secondary level, the [IAF-AAS] itself has two subordinate documents, these being:

- Assessor Qualifications and Requirements – [IAF-AQR] available in the Working Drafts section of our web site here: http://kantarainitiative.org/confluence/display/idassurance/Working+Drafts
- Service Assessment Criteria – [IAF-SAC] available here: http://kantarainitiative.org/confluence/download/attachments/38371432/Kantara+IAF-1400-Service+Assessment+Criteria.pdf. NOTE: This document has been approved by the IAWG and has now entered the Kantara All Member review period.

The group is also exploring program offerings for Service Approval Authority (SAA) and Federation Operator Rules & Guidelines (FORG, pronounced as "forge"). Work on the FORG is underway (draft here: http://bit.ly/kantara-IAF-1500-federation-operator-policy-guidelines), but since it is early stage and the SAA work has yet to begin, it does not form part of our current framework. We mention this to demonstrate that the work at Kantara, continues to evolve with participation from a broad set of participants.

Through our ICAM application process, we recognized the value of creating profiles that are specific to geographies, implementations and/or jurisdictions. These will be published in the form of profiles which can be called upon by Assessors when evaluating against a specific implementation type (in association with the larger accreditation, as defined in the SAC). The first, in development specifically for the US Government Federal Privacy Profile, is available as here: http://kantarainitiative.org/confluence/download/attachments/38371386/IAF-US+Federal+Privacy+Profile+v.1DRAFT.pdf. It is intended to address needs specific to ICAM requirements for those seeking that extra level of certification. We anticipate other profiles will be developed as and when appropriate and encourage open participation in the development process.

Tertiary documents support each of the secondary documents as required, these generally being proforma for the application processes, specification of the application subject, licensing agreements and terms of use, and other products establishing scoping, terms, etc.

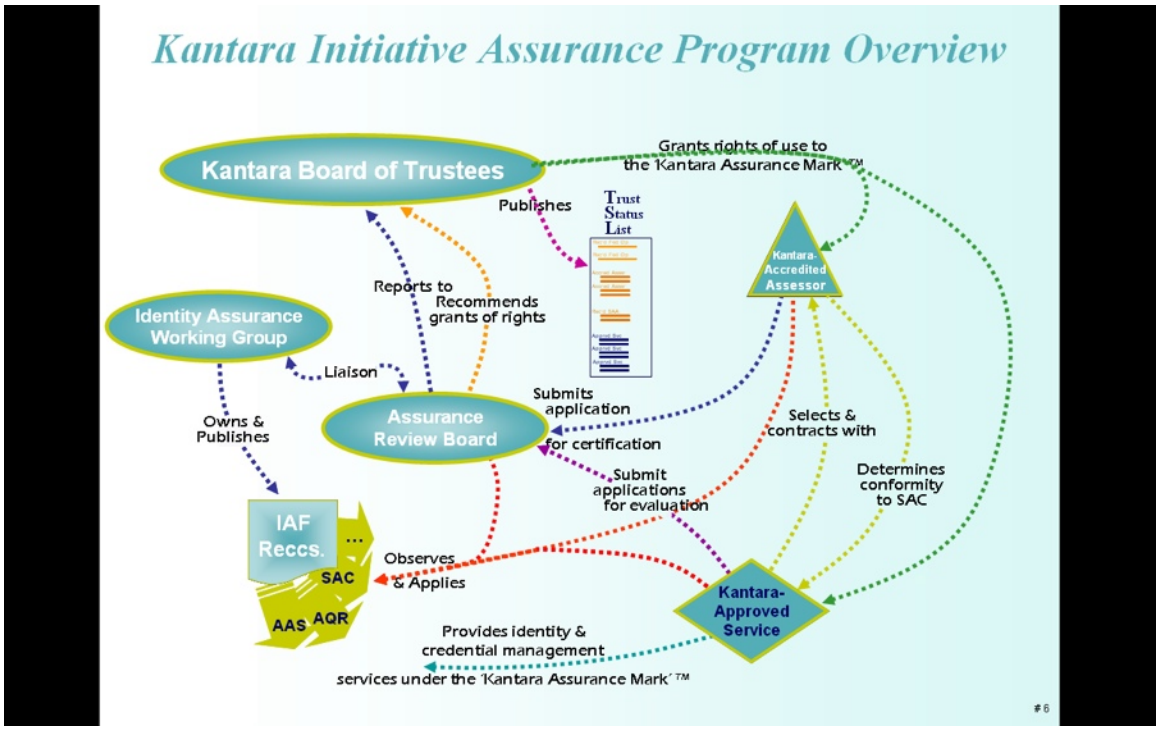
An Assurance Review Board (ARB) effects oversight and processes all applications under the IAF. The ARB is comprised of representatives of the identity marketplace ecosystem, and currently includes representatives from the following communities:

A. Credential Service Provider (CSPs);
B. Relying Party (RP);
C. Assessor/Auditor;
D. Federation Operator; and
E. "Interested Party"—ie. an entity that stands to benefit from such a program, but does not have an offering to put through the program for certification.

(c) 2009 Kantara Initiative

Current ARB appointees include Mark Coderre, Aetna – US; Nigel Tedeschi, BT – Europe; David Temoshok, GSA – US; Nathan Faut, KPMG - US; and Leif Johansson, SUNET/NORDUnet – Europe.

A quick overview of our current program, the reporting functions, and involved processes is summarized in the below diagram:



Any or all elements of this Framework, oversight body, approved assessors, etc., could be leveraged by the OIF in executing your program. This is a reasonably mature process that has received input since July 2007 from many participants from across geographies, verticals and organization sizes, and should represent a solid reference point for the OIF.

Per your request for financial data, our fee structure has been approved by our Board of Trustees and is available here: http://kantarainitiative.org/confluence/display/BoT/Board+of+Trustees+Minutes+2009-11-05. We intend to operate this program on a fully-loaded cost recovery basis with no net impact on our annual budget, operated chiefly to increase overall marketplace adoption of identity-based solutions and encouraging increased numbers of trusted transactions at all levels of assurance. We are amenable to discussing alternate mechanisms, such as self-certification, internal audit certification , etc. with the proviso that such mechanisms would of necessity be designed and operated in a manner acceptable in the marketplace.

2. **What aspects of your organization or its products, services, expertise, relationships, business model, or other factors do you feel may *not* a good fit with those requested under this RFI?**

(c) 2009 Kantara Initiative

The Kantara Initiative offering is a complete, reasonably mature program—this can be perceived as a positive or a negative for the OIF, depending on your objectives with a partner(s). The OIF RFI has stated that the OIDF and ICF intend to author and maintain a suite of documents that would provide identity federation trust and potentially allow for application to and approval from the U.S. General Services Administration as a Federal ICAM Trust Framework Provider. The Kantara Initiative has already done this through an established governance process with both industry and government representatives. The Kantara Initiative IAF, as detailed above, provides for all documents listed in the OIF intended suite of documents except for a "Relying Party Application and Agreement Package" which was not determined necessary or viable at this time for the scale of projects envisioned for the KI IAF Program. We are open to discussing the requirement for these documents and determining how best to proceed. KI has already applied to the U.S. GSA ICAM for TFPAP approval. The entire IAF suite of documents has been reviewed extensively by a large cross-section of members and participants, in addition to an in-depth comparison against NIST 800-63, and KI anticipates GSA ICAM approval shortly as an approved Trust Framework Provider to the U.S. Federal Government. This infrastructure—all or part—is something KI can offer immediately to the OIDF and ICF and its members in at least three ways:

a. The OIDF and ICF could adopt the IAF as an established industry Identity Assurance Trust Framework and determine to accept KI accreditations of Assessors and certifications of Identity Providers under the IAF and TFPAP Program requirements and recognize the KI Identity Provider Assurance Marks; and/or
b. The OIDF and ICF could simply accept KI accreditations of Assessors and certifications of Identity Providers under the IAF and TFPAP Program requirements to issue service marks of their own; and/or
c. The OIDF and ICF could join KI as participants at any time to participate in the KI IAF Program which guides the ongoing maintenance of the KI IAF suite, the development of new trust documents, and the ongoing assurance processes of the KI.

Please note that KI is planning to extend the existing IAF to address requirements for certifying identity federations to perform Identity Provider assessments and to approve Identity Providers that would qualify for the KI Assurance Marks (note: SAA and FORG work-in-progress mentioned earlier). Given the considerable amount of time, effort, and resources to produce the current version of the IAF, we anticipate that it will be some time before KI will be able to produce a companion trust framework to the current IAF to address federation trust. Nevertheless, that is the intention of KI and therefore the OIDF and ICF might consider participating in the development of that next generation trust framework to take advantage of the existing governance and broad-based industry and government representation in KI.

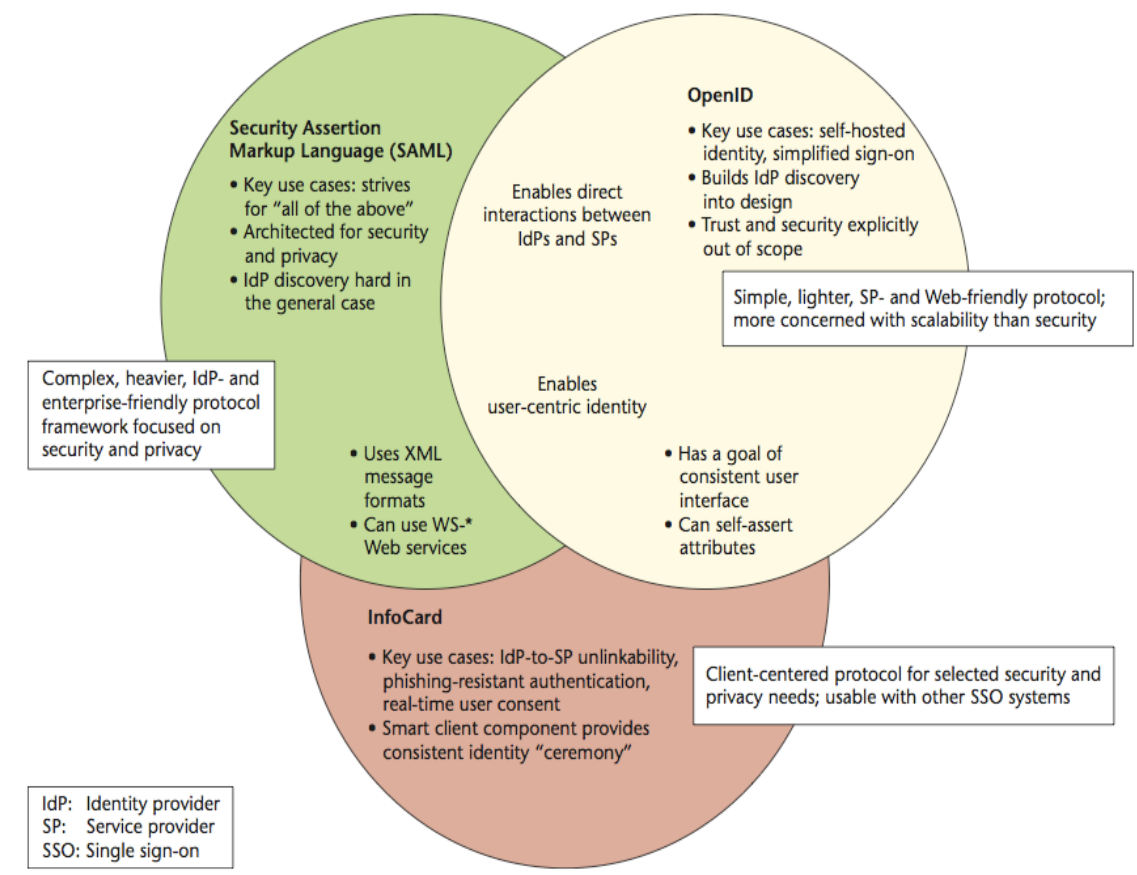
3. What unique partnership benefits do you believe your organization can bring to this outsourcing partnership?

Kantara Initiative, at its very inception and explicit in its core values, exemplifies the benefit of this sort of relationship to the industry at large. ICF's own Drummond Reed articulates it well on behalf of the community at large, and in particular the ICF Community, in this testimonial: http://www.youtube.com/watch?v=ChVzb6lkDZM&feature=player_embedded, explaining the Venn of Identity and the intersection points of various technology protocols.

(c) 2009 Kantara Initiative

The Identity Assurance Framework is technology agnostic—no specific requirements for technology protocol use are made of applicants. That said, appropriate security measures will be closely evaluated against each Level of Assurance to evaluate compliance with the Level of Assurance Grant sought. The security measures evaluated, and how they map to each Level of Assurance, are detailed in the SAC. Of particularly interest to the OIF effort, perhaps, is that on top of these documents, Liberty Alliance also completed an extensive mapping exercise last year against the NIST 800-63 requirements in this area, providing further assurance that those who complete this certification process will be in compliance with US Federal Government requirements.

We will be certifying services created utilizing a wide variety of open/standard identity technology. In addition to PKI, we see three primary technologies in play here (noting that depending on the protocol used, different privacy and security considerations will apply) and how the service implements the protocol will be evaluated in the certification process:



(c) 2009 Kantara Initiative

It is both the depth of contributions made to-date and this technology agnostic approach that has gained the IAF interest from the international standards community and other industry consortia including: ISO/IEC, ITU-T, INCITS CS1, eAuthentication Partnership (EAP), ICTSB, FSTC, SmartCard Alliance, ANSI IDSP, and others. The driving goal behind this work is to have a program and trust framework that is internationally applicable and recognizable in order to help accelerate marketplace acceptance of and trust in properly deployed identity services compliant to the four levels of assurance. We believe technology is an enabling piece of how this is carried forth, but the underpinnings of the program must be technology neutral, with the technology interoperability requirements defined in an associated interoperability assessment program. To that end, or Board of Trustees have chartered the Kantara Interoperability Program under the guidance of the Interoperability Review Board (IRB).

Our diverse membership is another benefit to the OIF. Our open participation model has encouraged a wide variety of participants at several different levels of engagement. The membership roster can be viewed here: http://kantarainitiative.org/confluence/display/GI/Current+Members. This diverse membership includes representatives from several different governments, among them the US Government, which has been very actively involved in the efforts around the IAF since inception. Members of the US Government have also actively overseen our certification program, both within the program we inherited from Liberty Alliance and now within Kantara Initiative, providing insight, expertise and neutral opinion that has been instrumental in building our programs.

4. What conflicts do you currently have, or might you have in the future, with entering into this outsourcing partnership?

The RFI at hand is admittedly rather ambiguous, so we'd need to better understand proposed relationships in order to fully answer this question. However, as detailed already in this response, you'll see we have a neutral program with many different touch points. For example, the assessors who are accredited operate 100% independently of KI. We see this as a positive in our program; it could be construed as a conflict depending on your program and other relationships you have in place and how they interact. Should this, or other things be perceived as a conflict, we are amenable to working together to develop a mutually agreeable accommodation.

Additionally, our approach to Intellectual Property Rights issues could be seen as a positive or a negative, again depending on your perspective and your program goals. We went to considerable effort to set up different IPR Policy options for the various Work Groups to choose from, allowing them to govern their groups under the specific policies that best allow them to meet their goals. This sort of approach, maintained in an open, transparent environment, is reflective of the thorough approach Kantara Initiative has instituted to address, and police, this potentially sticky issue. The OIF RFI does not detail how you intend to deal with IPR related issues, so we are not sure if this approach that we utilize will, as such, be a conflict

In addition to handling IPR is the question of handling confidential information. Though KI does not have any form of confidentiality as it relates to the operations of it's Work Groups (where our Recommendations are developed, e.g. the IAF) all certification programs allow for confidentiality as a means of protecting the interests of the applicants and therefore members of IRB and ARB will be required to comply with specific Non-Disclosure Agreements in order to access critical application materials.

(c) 2009 Kantara Initiative

5. **Based on your experience, what advice do you have for the OIDF/ICF Joint Steering Committee on how it should procede in its decision making?**

Based on our interactions with the Federal ICAM team, we believe the U.S. Government is not looking for a single Trust Framework Provider (TFP) but envisions that there could be multiple TFPs approved for the use and trust of the U.S. Government, other governments, and industry. However, for several reasons, the OIDF and ICF should consider how to leverage Kantara's existing infrastructure as you proceed. There are several factors to consider:

- The development and governance of broad-based Trust Frameworks as envisioned by ICAM and OIDF/ICF represent considerable investment in time, effort, and resources for the development of necessary documents, vetting and review, legal review, and ongoing maintenance. KI (and the Liberty Alliance previously) leveraged work that had initially been done by the Electronic Authentication Partnership to develop the IAF. This made sense due to the considerable efforts and broad-based participation already invested in developing those works, but also to support the KI goals of openness and broad-based representation. KI has made considerable investment in the current infrastructure for the IAF and has broad-based industry and government support. OIDF and ICF should consider ways to leverage that infrastructure for efficiencies, timely delivery, and ongoing maintenance resource requirements. In particular, the OIDF and ICF should consider the service offerings described in the response to question 2 when considering how to leverage existing infrastructure for OIF-related decision-making going forward.
- Assessors accredited for Trust Frameworks must be evaluated and qualified based on the assessment qualifications and assessment procedures required. Obviously there is expense associated with such evaluation and accreditation initially and on an ongoing basis. KI consulted with multiple prospective assessors of different business size and market focus to develop the assessor application and evaluation procedures that best fit industry models. OIDF and ICF should consider such consultation with potential audit firms and assessor groups for feedback on how their participation might be facilitated with initiatives like this, particularly how the existing KI evaluation and accreditation processes can best be leveraged by OIDF and ICF.
- Identity Providers must also be assessed to meet assurance standards and requirements in order to receive any federation assurance mark. Different assessment criteria and approval requirements will certainly represent a financial and administrative burden for potential IDPs. OIDF and ICF should consider such consultation with potential IDPs for feedback on how their participation might be facilitated with initiatives like this, particularly how the existing KI evaluation and certification processes can best be leveraged by OIDF and ICF.
- KI encourages open work groups and open participation in all work group activities, but especially for the development of critical public documents like the IAF suite. Because of the sensitive nature of identity management and trust, KI has made a particular effort to gain the participation of privacy groups and experts in the development and ongoing maintenance and administration of the IAF, including the hiring of a Director of Privacy and Public Policy. This is another reason that OIDF and ICF should consider ways to leverage existing KI infrastructure, particularly work groups focused on privacy, eGovernment/Open Government and development of the IAF and next generation trust frameworks. The OIDF and ICF should also consider how to leverage the existing KI

(c) 2009 Kantara Initiative

processes for addressing privacy and PII protections in advancing Trust Framework schemes. All feedback has shown that privacy issues and concerns are extremely important to the U.S. Federal Government and ICAM and the other governments participating in KI work group and governance processes.

Overall, we believe that in order for trust networks to mature beyond point to point direct auditing, a standard seal for an entities' level of assurance as an identity provider and guidance for commensurate risk must be standardized and brought to market under the direct governance of volunteer stakeholders representing a balanced cross-section of perspectives in the ecosystem. Having 3rd party validation balances out the inherent conflict that can arise between relying parties and identity providers. This is what our program aims to achieve, and we believe should be a chief driver for all participants in this space.

(c) 2009 Kantara Initiative