IAWG Meeting Minutes 2013-04-04

Kantara Initiative Identity Assurance WG Teleconference

Date and Time | Agenda | Attendees | Non-Voting | Staff | Apologies | Notes & Minutes | Next Meeting

Call recorded for purposes of note taking

Minutes approved, IAWG call 2013-04-11

Date and Time

- **Date:** Thursday, 4 April 2013
- **Time:** 07:00 PT | 10:00 ET | 14:00 UTC (time chart)
- United States Toll +1 (805) 309-2350
  Alternate Toll +1 (714) 551-9842
  Skype: +99051000000481
    - Conference ID: 613-2898
- International Dial-In Numbers

Agenda

1. Administration:
    a. Roll Call
    b. Agenda Confirmation
    c. Minutes approval - IAWG Meeting Minutes 2013-03-14
2. Discussion
    a. Agile IAF
    b. Errata
    c. Roadmap review
        i. Healthcare profile?
3. AOB
4. Adjourn

Attendees

- Myisha Frazier-McElveen
- Matt Thompson
- Scott Shorter
- Bill Braithwaite
- Richard Wilsher

As of 14 January 2013, quorum is 4 of 7

Non-Voting

- Nathan Faut
- Rich Furr
- Ken Dagg

Staff

- Andrew Hughes

Apologies

Notes & Minutes

- Bill Braithwaite moves to approve; Scott Shorter seconds; minutes approved with no revisions

Agile IAF

- the idea of Agile IAF is, if we take a look at the underlying trust framework that we are constructing with the IAF and SAC, then as we decompose that in to the services that are offered by the various actors and roles via their relationships and protocols, then we can possibly accredit/certify /approve the Service Providers have a tighter scope and scale
- if this is viable, then there is work to be done on the list of actors and roles; need to have discussions around what kind of things could receive a trust mark from Kantara
    - today, the trust mark is being used as if it means you have FICAM approval (which isn't what it actually means)
    - at the microlevel, would a trust mark mean we have trusted attribute providers? that we have to keep a massive interop table? that we have partial federations or aggregations of different kinds of micro services?

    - the SAC themselves do not need modifications; we need to understand how to apply this to specific approval programs
- suggestion: need to define what we consider to be the service elements of an end-to-end solution; look at tScheme, 800-63 and get a simple, high level view of the components and the relations between them
    - there are probably a set of atomic service roles and relationships that exist within a trusted identity federation or arrangement; if it is possible to come down to that list, then we can start building from there
    - take the model we have been working on and break it down one more level and use tScheme and 800-63-2 and whatever else to effect that breakdown
    - this might help with making cross-mappings between different frameworks, using it as a findings guide if nothing else
- group is in agreement about this method of breaking down the services
- next step is for Andrew to get the thoughts written down and sent to group, and from there advise ARB on what is possible and and what should be considered for approvals; remember we have real-world vendors asking for this kind of change
    - if a service provider wasn't providing all of the functionality covered by the SAC, they should provide a definition of what they are not doing and some guidance regarding what the organization picking up those elements would have to do
    - should also separate the consideration in to: whether or not Kantara wants to move forward with this AND the implications to FICAM approval; there may be a delta between the two when we get in to this
    - is there a place for us to be certifying the identity system that is the accumulation of all the bits and pieces that define a system? that's one of the things that gets the FICAM profile met; is it a service or an integration of services and therefore a federation? for FICAM certification we need end-to-end full service, and so someone has to step up and offer the full service, and that may include the sub services but for FICAM certification someone has to take responsibility for all the pieces; a subservice cannot say they are certified and FICAM approved
    - Kantara needs to intervene at the federation or integration level, if we are being asked to give FICAM-certification, then all the subservices has to be certified as well; someone has to be the prime for the overall certification
    - Kantara itself does not give FICAM approval; FICAM approval involves both FICAM profile acceptance by GSA and Kantara certification
    - maybe we can identify classes of services to help the FICAM people support modular components?
- if you look at all the attribute groups, you look at attribute providers and stand-along service providers; there is a profile/trust mark available to attribute providers; the Kantara trust mark would have value in and of itself, either in a formal federation that recognizes different trust marks
    - with this kind of dynamic use, there needs to be an automate-able way to verify the trust mark (the KTR)
    - it needs to be clearly expressed that we are doing this in several stages and will review at the end of each step how it all ties together

Errata

- Submitted ticket #533469 - **This is considered Errata and accepted**

> *I've got a question about the proper interpretation of AL1_ID_IPV#010 and #020: If read literally these conditions say that a AL1 IdP must provide In-Person Public Verification (base on self-asserted identity).*
>
> *Why is this not an option for an IdP? The way I see it most IdPs operating at AL1 ***only*** would opt _out_ of IPV entirely (I suspect you won't be able to get a google account by showing up in person at G HQ for instance).*
>
> *I propose the following change to the lean-in text of 3.1.2.2:*
>
> *Replace:*
>
> *"An enterprise or specified service must:"*
>
> *With*
>
> *"An enterprise or specified service that provides In-Person Public Identity Verification at AL1 must:"*
> *----------*
>
> *To view/respond to the ticket, please login to the support ticket system.*

- Submitted ticket #57095 - **This is considered a major change, not errata and will need to be addressed in the newer version.**

> *we need to agree whether P3WG is providing input for the notices already required or providing additional/separate notices and whether the Privacy Assessment Criteria are directing assessors to evaluate the content of the required notices for privacy content or something else.*
>
> *There are also requirements for information collected for identity verification/proofing, for credential issuance and management, and for records retention in Part B. I did not see any provisions that deal with the re-use of data derived from proofing or from logs of credential use (i.e., something that corresponds to the "no tracking" requirement under FICAM). I do not know of any review by the P3WG of the requirements or the language of IAF—and building in privacy protections here would seem to be fundamentally important. Should we not be integrating PAC into the existing framework in some way?*
>
> *451 4.2.2 Notices and User Information/Agreements*
>
> *452 These criteria apply to the publication of information describing the service and the*

manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL2_CO_NUI#010 General Service Definition

Make available to the intended user community a Service Definition that includes all applicable Terms, Conditions, and Fees, including any limitations of its usage, and definitions of any terms having specific intention or interpretation. Specific provisions are stated in further criteria in this section.

and actual Subscribers,

Subjects, and relying parties.

AL2_CO_NUI#020 Service Definition inclusions

Make available a Service Definition for the specified service containing clauses that provide the following information:

a) Privacy, Identity Proofing & Verification, and Revocation and Termination Policies;

b) the country in or legal jurisdiction under which the service is operated;

c) if different from the above, the legal jurisdiction under which Subscriber and any relying party agreements are entered into;

d) applicable legislation with which the service complies;

e) obligations incumbent upon the CSP;

f) obligations incumbent upon the Subscriber/Subject;

g) notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose to rely upon the service;

h) statement of warranties;

i) statement of liabilities toward Subscribers, Subjects and Relying Parties;

j) procedures for notification of changes to terms and conditions;

k) steps the CSP will take in the event that it chooses or is obliged to terminate the service;

l) availability of the specified service per se and of its help desk facility.

AL2_CO_NUI#030 Due notification

Have in place and follow appropriate policy and procedures to ensure that it notifies Subscribers and Subjects in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the specified service, and provide a clear means by which Subscribers and Subjects must indicate that they wish to accept the new terms or terminate their subscription.

AL2_CO_NUI#040 User Acceptance

Require Subscribers and Subjects to:

a) indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;

b) at periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance, renewal) and otherwise at least once every five years, re494 affirm their understanding and observance of the terms of service;

```
495 c) always provide full and correct responses to requests for information.
496 of User Acceptance
497 Obtain a record (hard-copy or electronic) of the Subscriber's and Subject’s acceptance of
498 the terms and conditions of service, prior to initiating the service and thereafter at
499 periodic intervals, determined by significant service provision events (e.g. re-issuance,
500 renewal) and otherwise at least once every five years.
501 AL2_CO_NUI#060 Withdrawn
502 Withdrawn.
503 AL2_CO_NUI#070 Change of Subscriber Information
504 Require and provide the mechanisms for Subscribers and Subjects to provide in a
505 timely manner full and correct amendments should any of their recorded
506 information change, as required under the terms of their use of the service, and only
507 after the Subscriber's and/or Subject’s identity has been authenticated.
```

- Submitted ticket #150290 - **This is considered a major change, not errata and will need to be addressed in the newer version.**

```
1. Potentially move the retention requirement to more reasonable in SAC core - but ensure that
it's covered aligned to NIST requirement in US Federal Additional Criteria.
(Part of which set of changes?)

(See http://kantarainitiative.org/pipermail/wg-idassurance/2012-August/001326.html for thread of
email discussion)
```

Roadmap discussion

Healthcare profile

- At the last LC meeting, Pete Palmer gave an overview with Kantara's new relationship with DirectTrust. This is similar to a cross-certification model - they will leverage the Kantara approval process based on the IAF and SACs.
- There may be, as they dig in to the SACs a requirement for a health care profile. Not sure how immediate and effective the cross-over use of the SAC will be. There will definitely be some useful overlap with the assessors, but we have a lot of work to do before a new profile can be created

General Roadmap overview

- focus on Q2 and Q3; changes incorporated in to the Roadmap

AOB

Next Meeting

- **Date:** Thursday, 11 April 2013
- **Time:** 07:00 PT | 10:00 ET | 15:00 UTC (time chart)
- United States Toll +1 (805) 309-2350
  Alternate Toll +1 (714) 551-9842
  Skype: +99051000000481
    - Conference ID: 613-2898
- International Dial-In Numbers