IAWG Meeting Notes 2015-07-30
Kantara Initiative Identity Assurance WG Teleconference

Date and Time

- **Date:** Thursday, 2015-07-30
- **Time:** 12:00 PST | 15:00 EST | 20:00 UTC (Time chart - US Standard Time)
- **Time:** 12:00 PDT | 15:00 EDT | 19:00 UTC (Time chart - US Daylight Saving Time)
- United States Toll +1 (805) 309-2350
- Alternate Toll +1 (714) 551-9942
- Skype: +99051000000481
  - Conference ID: 613-2898
- International Dial-In Numbers

Agenda

1. Administration:
   - a. Roll Call
   - b. Agenda Confirmation
   - c. Minutes approval: DRAFT IAWG Meeting Minutes 2015-07-16
   - d. Action Item Review
   - e. Staff reports and updates
   - f. Assurance Review Board (ARB) and Leadership Council (LC) reports and updates
   - g. Call for Tweet-worthy items to feed (@KantaraNews or #kantara)
2. Discussion
   - a. Final review of NISTIR 8062
   - b. SAC Update
   - c. Discussion of possible additional documents to review:
     - i. NISTIR 7904, DRAFT Trusted Geolocation in the Cloud Proof of Concept
     - ii. NISTIR 8053, DRAFT Deidentification of Personally Identifiable Information
     - iii. NISTIR 7966, DRAFT Security of Automated Access Management Using Secure Shell (SSH)
     - iv. NCCOE Derived Credentials Building Block
     - v. others?
3. AOB
   - a.
4. Adjourn

Attendees

*Link to IAWG Roster*

As of 2015-01-22, quorum is 6 of 11

Use the Info box below to record the meeting quorum status

Meeting did not achieve quorum

Voting

- Ken Dagg (C)
- Andrew Hughes (VC)
- Scott Shorter (S)
- Richard Wilsher
Non-Voting

- Colin Wallis
- Angela Rey

Staff

- Ruth Puente
- Joni Brennan

Regrets

- None

Voting Members for Cut/Paste

- Ken Dagg (C)
- Andrew Hughes (VC)
- Scott Shorter (S)
- Rich Furr
- Paul Calatayud (VC)
- Devin Kusek
- Adam Madlin
- Kenneth Myers
- Cathy Tilton
- Richard Wilsher
- Lee Aber

Selected Non-Voting members for Cut/Paste

- Bill Braithwaite
- Björn Sjöholm
- Susan Schreiner
- Jeff Stollman

Notes & Minutes

Administration

Minutes Approval

- DRAFT IAWG Meeting Minutes 2015-07-16

Motion to approve minutes of 2015-07-16:
Seconded:
Discussion:
Motion Carried | Carried with amendments | Defeated

Action Item Review

See the Action Items Log wiki page

Staff Updates

Big announcement is that UMA-Dev workgroup has been formed, a number of articles and quotes coming through.

Leadership Council (LC) Updates

- Joni reports:
- LC agenda has been restructured, creating a placeholder for discussing the tools of the organization, formalize what's been happening
- Groups are encouraged to raise tools they've used or would like to use
- Collaboration standing item, opportunities for collaboration between Kantara groups. UMA and MVCR, IAWG and Health Identity Assurance, etc.
- Still working on the issue of sharing IPR between different groups with different rules.
• UMA has spun off a work group for the reason of supporting different IPR regimes. Now we have a leader of two WGs, is that too many seats on the LC? Leadership will consider how to handle this with new procedures.
• Andrew adds: on the tools discussion, one idea that Eve mentioned was how to deal with release schedules now that they have a specification to manage. Considered moving towards a software product release schedule idea - patch releases/errata, update segments instead of the whole thing, rational version number scheme. Agile methodology is when an issue comes up you throw it in the hopper then determine which release it will be fixed in. Discussed possible repositories (git/github). Discuss the possibility of storing SAC in alternate formats, one possibility is to move it to XML and store it in git, use export filters to generate the word document / PDF or whatever.
• RGW: Word works but has limitations. As Ken originally noted, we're looking for a more flexible way of maintaining it and exporting it to different formats. Many in the group agree that the word document is difficult to manage.

Participant updates

Discussion

NISTIR 8062

- Ken has reviewed and will write up comments. Ken and Scott discussed last week and came to similar conclusions. Call for any other reviews or thoughts on the quality or what might be missing.

Ken's opinions - a wordy document that needs an extensive edit. The process identified seems to be complete, but time and use will tell how good it is. The guidance about what to do in response to risks is not identified, not clear that the document should go forward without including that information. The terminology used is not aligned with what is currently used in the privacy industry.

RGW: this is an internal report (IR). As it stands, its not usable for deriving standards or practices from.

Colin: on the responses from privacy by design engineers and the privacy reference model group. The key issue is the lack of controls when that's obviously needed. The other overriding thing is the lack of cohesiveness with other documents, particularly 800-63 or the work of the P3WG.

Scott had a comment that the definition of the security objectives is not clear.

Colin notes that the objectives cannot be created from scratch (noted by OASIS P3WG).

Ken notes that a letter should be sufficient, the document is not in condition where the comment matrix would be needed.

SAC Update

Ken has not seen email traffic on the SAC.

RGW is mapping criteria to ISO 29115, finding opportunities for Kantara to fill the gap. Aiming to be done around the end of tomorrow, there will be a number of additional criteria across assurance levels. The document at that point would be worthy of consideration by the IAWG. Worth waiting for this.

Ken says so this means an updated set of criteria may be available sometime next week. RGW will aim for two weeks turnaround for the SAC.

Requirements sent out about the tool - we discussed that previously. Andrew gave an update on the process Kantara might use if there was such a tool. Andrew sent out requirements on the 16th - if there are no further comments we should figure out what to do with them.

Joni responds there are two sides to the answer. First, review the requirements to figure out if there's a tool. Eve brought a discussion and had a recommendation for a tool. Either requirements could go to the LC as is, or we could send the requirements and a recommended tool. We could approach the LC for a proposal for funding for a project, or for obtaining tools.

Andrew: what we're talking about is markup tools, a rich editor for marking up documents and being able to generate it in other formats. With the SAC stored in data, we could output based on filters such as LOA, component, etc.

Andrew suggests we ask Eve what they are using and how. Colin mentioned they are tracking over a hundred bugs via spreadsheet.

Core Criteria of the SAC

RGW: The AAS and the RAA have been revised at the ARB. They spoke about getting the docs before the IAWG. RGW asks if they can push the point for IAWG to provide feedback? Joni defers to Ruth. Ruth will help with document management. Joni approve sending the documents to IAWG.

RGW continues - the core criteria should be in the SAC. The SAC says what the criteria are and when they apply, and whether they are mandatory or not and whether they are core criteria covered in the annual review should all be defined in the IAWG. The AAS and RAA are procedural documents and that's what they do best. Removed the conditions for ACRs from AAS, that's all in RAA. In this approach, “core” would be an attribute of a criterion.

Ken has similar thoughts and different end result. SAC identifies the criteria that a CSP must comply with when granted and to maintain the trust mark. CSPs should notify Katnara when a change occurs which would bring them out of conformity, but in reality this is unlikely. Ken would see the ARB stipulating which criteria are assessed during the off-years. Since all the criteria are applied, and if you want to apply some criteria in some circumstances that may belong in the RAA.

Joni - is this about whether criteria are necessary or not, or to inform the process for verifying them? Are there any criteria that must be verified every single year?

RGW confirms that this is a discussion about which criteria must be assessed during every assessment that happens. RAA has been modified to state how criteria are selected for the ACR. If core, it's in. If the CSP or assessor believes there's a risk, assess that. If, between assessments, any newly applicable criteria have to be included. In reality, something like 60-65% of the criteria will be assessed each time. This is captured in the RAA.
Ken mentions that since there’ve been no comment on the topic, it seems that IAWG has no disagreement. The main disagreement is where the criteria should be identified. RGW disagreed and believe that the criteria themselves should be identified first.

We will need to have the remainder of this discussion next week.

Ken will be out from 8/12-8/25.

AOB

**Carry-forward Items**

**Attachments**

**Next Meeting**

- **Date:** Thursday, 2015-08-06
- **Time:** 12:00 PT | 15:00 ET | 20:00 UTC (Time chart - US Standard Time)
- **Time:** 12:00 PDT | 15:00 EDT | 19:00 UTC (Time chart - US Daylight Saving Time)
- United States Toll +1 (805) 309-2350
- Alternate Toll +1 (714) 551-9842
  - **Skype:** +9905100000481
  - Conference ID: 613-2898
- **International Dial-In Numbers**