IAWG Meeting Minutes 2013-12-05

Kantara Initiative Identity Assurance WG Teleconference

IAWG Approved Meeting Minutes on 2013-12-12

NOTE: These meeting minutes also contain notes from December 6 2013 - a continuation of this meeting for discussion of the FICAM TFS update material.

Date and Time

- **Date:** Thursday, 5 December 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 2013-11-21
    d. Action Item Review
    e. Staff reports and updates
    f. LC reports and updates
    g. Call for Tweet-worthy items to feed (@KantaraNews or #kantara)
2. Discussion
    a. IAF-1400 draft for 45 day public review - see linked document: Kantara IAF-1400 SAC v3-1.docx
    b. Disposition of 800-63-2 -> SAC Mapping working documents - where/how to store for future reference?
    c. FICAM TFS Program update comments from IAWG members & consolidation
    Link to review documents and comment template here: https://kantarainitiative.org/confluence/x/fYHwAw
    d. **REMINDER**: Ad hoc call to continue FICAM TFS discussion Friday December 6, 2013 10:00 Eastern.
3. AOB
    a.
4. Adjourn

Attendees

Link to IAWG Roster

As of 2013 November 21, quorum is 5 of 8

Meeting achieved quorum

Voting

- Myisha Frazier-McElveen (C)
- Rich Furr (V-C)
- Andrew Hughes (S)
- Scott Shorter
- Matt Thompson
- Richard Wilsher
- Cathy Tilton

Non-Voting

-

Staff

-

Apologies

- None

Notes & Minutes

Administration

Minutes Approval

IAWG Meeting Minutes 2013-11-21

Motion to approve minutes of 2013-11-21: Furr
Seconded: Shorter
Discussion: None
Motion Carried

Action Item Review

See the Action Items Log wiki page

Staff Updates

- Director's Corner Link
- Event Radar 2013 and 2014 Link

LC Updates

- Discussed charters
- eGov planning be working on an updated profile this year
- There was discussion about membership as it relates to WG Chair/Vice-Chair roles

Participant updates

Discussion

IAF-1400 for 45 day Public Review

- The final version of the IAF-1400 SAC for 45 day public review is here: Kantara IAF-1400 SAC v3-1.docx
- Move to release this document to to 45 day public review: Furr
- Seconded: Wilsher
- Discussion: None
- Motion carries

Disposition of 800-63-2 -> IAF mapping documentation

Email from Richard Wilsher 2013-12-05 - The referenced document is attached to this page

---

Colleagues,

I attach a draft Working Group Report for IAWG Members' review, with the purpose of adopting this document within the Kantara IAF document suite.

As explained in the Abstract, this report was produced for Kantara as a product of an undertaking sponsored by two Kantara members, to bring the Service Assessment Criteria (KI-IAF 1400) into full alignment with NIST's SP 800-63-2. It was a specific output of the Statement of Work under which the SAC alignment was performed and is a partial re-structuring of NIST's SP 800-63-2 with mappings into the SAC v4.0 (as the aligned SAC will be identified), performed under certain self-imposed restrictions (which are described in the Apologia, which appears on the second page of the document).

This report serves a number of valuable and distinct purposes:
i) it renders the essential parts of SP 800632 as a much clearer set of requirements than in their original form;
ii) it provides a reference work which underpins and justifies the majority of the revisions made to the SAC v4.0 in order to achieve the alignment (a small number of other identified changes have been opportunistically introduced);
iii) it has enabled clarification of parts of the original NIST document which were ambiguous, unclear or otherwise doubtful, and records those clarifications;
iv) it facilitates service providers wishing to demonstrate their compliance with SP 800-63-2 by providing a set of discretely-referenceable requirements which the original document cannot support;
v) in addition to the above, it provides clear guidance where a US-specific profile for meeting both Kantara SAC requirements and SP 800-63 compliance should be developed (which would serve the same purpose for any other jurisdiction wishing to adopt SP 800-63);
vi) by virtue of the two points above, this WG report facilitates both internal and third-party review and assessment of services which are intended to specifically comply with 800-63-2's provisions;
vii) finally, this report has the potential to act as a future, structurally-improved, revision to SP 800-63, as has been previously discussed with NIST personnel and was an intention of the original tasking. It will therefore be offered to NIST as a potential basis or stimulant for a future revision to 800-63.

This document has been previously circulated and reviewed a number of times by the IAWG during discussions concerning the mapping of the SAC to SP 800-63-2, at those times being identified as EZP-63-2, so its content should be no surprise to you – there's been no material change there.

I am therefore recommending this report for adoption into the IAF doc suite, for which reason it has been given a fitting IAF reference / identity. I hope we can consider this during the meeting of Dec 12th. On its hopeful adoption I will render as a formal doc at v1.0 and submit to the Secretariat in PDF from for publication and Word form for archiving.

Best regards,
Richard.

- Wilsher has floated the idea of publishing it as a report
- Furr - OK with it as a report, not OK with including it within the IAF document
- Wilsher - not actually a working document - it realigns 800-63-2 text and clarifies ambiguous items in 800-63-2. This document is intended to go back to NIST as input to a potential 800-63 update. Indicates where a US Federal Profile could be developed. The document should be made publicly available.
- Frasier-MacElveen - that last reason is a good case to exclude it from the actual IAF - it should be a Report.
- The document only deals with 800-63-2 - when Kantara IAF is assessed against the FICAM TFPAP the 800-63-2 is not actually in scope - the document might cause confusion at that time.
- The document is useful, should be publicly available, we appear to agree that it should be a Report.
- Frasier-MacElveen - The Executive Summary appears to say that Kantara is providing advice/direction to Federal Agencies - we should not do this.
- Wilsher: the Apologia covers how the document was created. The Executive Summary could simply be deleted.
- Group suggests that the Apologia becomes the Executive Summary
- This document is non-normative - assessors should not be using this for assessment. It is only for background information.
- A CSP could choose to reference this document - this is not a Kantara requirement.
- Wilsher to update and forward the document to IAWG for consideration.

FICAM TFS Program update comments from IAWG members - December 5 2013 meeting notes

- RF: the ATOS seems to be making the CSPs into Attribute Providers - the current requirement is to only maintain core attributes - there seems to be an extension into a new set of attributes - this would increase costs, might knock smaller CSPs out of the running because they may not have the resources to deal with the extra attributes.
- RF: Anil John referenced ANSI/NASPO Section 6
- MF: Read it as an optional requirement - if they are available then provide the attributes, if not then no issue.
- RF: Verbal indications that the attribute provision is leaning towards mandatory provision (because the Federal Agencies might ask for them)
- SS: There is a section in the RP Guidance on disambiguation of identities - it recommends that the agency goes to an attribute provider without any reference to LOAs.
- CT: Anil mentioned that this set of attributes is needed for the RPs to perform account/identity disambiguation and linking to the right agency account
- MF: most RPs don't identify their clients from these attributes - they know them by other information
- RF: do the SAML assertions have to include the extra attribute data? If yes, then the CSP will have to capture and maintain the extra attributes.
- SS: don't these attributes have to be collected and kept as proof of the ID Proofing process?
- RF: yes. but they do an encrypted hash of the values
- MF: But there are many attributes that are not currently collected
- RF: The registration authority does not store the information - the Certificate Authority keeps it if they want to or need to.
- SS: It appears that Verizon would meet the Bundle 1 requirements.
    - Section 7.2.2.3 discusses how to resolve problems linking CSP-provided identities to accounts. Recommended methods to resolve include:
        - Trusted third party. This method redirects a user to a third-party site (e.g., Experian) where he/she is prompted with several questions to verify his/her identity.
        - Help desk/call center. This method requires the user to call the help desk to resolve linking issues. The help desk can ask a series of questions to verify his/her identity.

        - Now should those "several questions" or "series of questions" correspond to the LOA of the identities in question?

- SS: If they are looking for verified attributes, then it has to be better defined.
- MF: It is unclear if the attributes SHALL be sent if the CSP has them or if they are optional.
- RW: Are we making the assumption that the RP will be dictating the attributes that the CSP will have to gather in the ID Proofing process?
    - (RF: Yes)
    - So, is this assumption correct?
    - (RF: Vz reading is that if the RP asks for it, then the CSP pretty much has to provide it)
    - This needs clarification
- RW: The requirements are stated in terms of what the RP must do. The implication that is not clearly stated is that the imposition on the RP becomes an implication on the CSP. This is essentially a profile imposed on 800-63-2 -> "these are the things needed to sufficiently define an 'identity'"
- MF: consolidate Scott's item with Rich's item
- RW: There's also an issue with the footnote saying 'in order of preference' -> this implies that beyond the core attributes, it is not clear what weighting the additional attributes have (the core gets 96% certainty, so what do the others provide?)
- RF: Danger is in who is interpreting this - CSP will see it one way, Federal RP will interpret differently.
- RF: If adding Attribute Providers into the CSP process, it's possible that the price of the CSP services will rise which might become an inhibitor to RP uptake.
- ALL: review comments that have been circulated so far for tomorrow's call

---

FICAM TFS Program update comments from IAWG members - December 6 2013 meeting notes

Myisha Frasier-MacElveen (Chair), Rich Furr (Vice-Chair), Andrew Hughes (Secretary), Peter McDonald (Symantec), Nathan Faut (KPMG), Cathy (Daon), Scott Shorter (Electrosoft), Bill Braithwaite

- SS: gave overview for 1st eSoft comment
- PM: Submitted a question around what 'Verified' means - Verified is probably distinct from Assurance Level
- SS: For these Verified Attributes - is there any difference between
- PM: Scenario: At LOA2 and LOA3 if a person gives a fingerprint and zip code -> this uniquely identifies an individual. So is the zip code a Verified Attribute or not?
    - There's not enough clarity on how this is intended
- SS: Identity Proofing only establishes that the identity is a real person - it does not actually say anything about the person being the person claiming the identity
    - Need to either include gradations of 'proof' so that this is not an absolute
    - Need to work out how post-registration identity changes should be used to maintain the integrity of the initial proofed identity
- RF: CSPs do a pretty thorough process to establish that the identity information relates to the actual person - either by in person or using antecedent information
    - Never 100% perfect but it is well-understood process
- SS: maybe the RPs would be served better by having ID Proofing process metadata -> that gives hints about provenance -> so the RP can assess risks properly
- BB: the 'real person' establishment has been subsumed into the process of 'identity resolution'/ 'identification of an individual'
- SS: general comments on use of more standardized requirements language e.g. 'shall', 'should', etc
- MF: ATOS document p4 discussion - the reference to Financial Institutions exemption. The identity vetting processes depends on the type of account - so hard to deal with LOA equivalence
- PM: Definition of verification - e.g. Name - what is needed for name variants? For some attributes variants might need to be allowable.
- PM: Concern that if CSPs need to become full-blown attribute providers will require significant resources and investment
- PM: discussed Symantec's comment re verified attribute sources
- PM: if a CSP has to go to additional sources to verify attributes then the CSP's financial model changes

Logistics:

- Andrew to consolidate
- Scott to update his comments
- Myisha to send comments to Andrew
- Andrew to send consolidated sheet to Joni for integration into the ARB document

AOB

Carry-forward Items

Attachments

Next Meeting

- **Date:** Thursday, 2013-December-12

- **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