IAWG Meeting Minutes 2017-03-09

Kantara Initiative Identity Assurance WG Teleconference

Date and Time | Agenda | Attendees | Minutes Approval | Action Item Review | Staff Updates | Discussion | AOB | Attachments | Next Meeting - topic will be 800-63C and the new charter

Date and Time

- **Date:** Thursday, 2017-03-09
- **Time:** 12:00 PST | 15:00 EST
- Dial-in Details NEW
- Please join the meeting from your computer, tablet or smartphone. https://global.gotomeeting.com/join/380672837 You can also dial in using your phone. United States: +1 (312) 757-3119 (more phone numbers)
- Access Code: 380-672-837
- Test session

Agenda

1. Administration:
    a. Roll Call
    b. Agenda Confirmation
    c. Minutes Approval:
    d. Action Item Review
    e. Organization Updates - Director's Corner
    f. Staff reports and updates
    g. LC reports and updates
    h. Call for Tweet-worthy items to feed (@KantaraNews or #kantara)
2. Discussion
    a. Leadership Elections
    b. Discuss NIST SP 800-63B for 800-63-3 IAWG Comments

Attendees

Link to IAWG Roster

As of 2017-01-12, quorum is 4 of 7

⚠ Use the Info box below to record the meeting quorum status

ⓘ Meeting *(did / did not)* achieve quorum

Voting

- Ken Dagg (C)
- Scott Shorter (S)
- Andrew Hughes (VC)
- Richard Wilsher
- Adam Madlin

Non-Voting

- Marc Aronson
- Ken Crowl
- Denny Prvu

Staff

- Colin Wallis (ED)
- Ruth Puente

Apologies

- None

Voting Members for Cut/Paste

- Ken Dagg (C)
- Andrew Hughes (VC)
- Scott Shorter (S)
- Paul Caskey
- Adam Madlin
- 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 2017-03-02

Motion to approve minutes of 2017-03-02:
Seconded:
Discussion:
Motion Carried | Carried with amendments | Defeated

Action Item Review

-

Staff Updates

Director's Corner Link

- Colin reports on the Digital Signatures workshop with FICAM / SAFE-BioPharma / ETSI, about digital signature interoperability.
- Discussions about the future / difficulty the GSA is encountering in maintaining the federal PKI bridge, the need for directing for more abstract framework. Expectation that the PKI side and the TFS will put profiles of the framework against broader FICAM framework. Differences between the Kantara Initiative Trust Status List versus a PKI approach to that.
- Richard reports that there are issues of alignment between federal government and the EU, but not sure what the issues become. The issues are somewhat secondhand - Lachelle mentioned NIST wanting to align with international standards, but RGW observes that NIST is very insular and does not really conform with international standards
- Colin mentioned one thing coming out of the workshop, the analysis of differences between ETSI and US digital signature requirements, the main thing holding back a trusted federation was issues of lack of policy and regulation on the US side. There was discussion and interest in 800-63-3 and how to comply with the identity proofing requirements, and potential practical solutions. Some concerns with the timeframe for getting this onboard - the standard 12 months that NIST offers is probably not going to be achieved by any of those parties.

LC Updates

- Check the LC blog

Participant updates

-

Discussion

Leadership Elections

Ken Dagg has been nominated for chair, Scott Shorter has been nominated for vice chair, Denny Prvu has been nominated for Secretary. Richard Wilsher moves and Ken Crowl seconds. Without objection the election is carried.\

Charter

Ken is waiting to hear back from Angela Rey on comments on the charter.

800-63-B

Comments from RGW:

1. Numerous references to "digital service" without being clear what they mean.
2. Refer extensively to the "subscriber" whereas other schemes include "subscriber" and a "subject". The "subscriber" may be the organization who wants credentials issued to a number of subjects. Would make easier alignment with other sources.
3. The documents are called "guidance" but it contains requirements. Are the contents mandatory or not?

Andrew is reviewing and finding internal inconsistencies in the way terms are used, it's not clear what the state model is to get from non-authenticated to authenticate state, versus the authenticators and secrets and other things needed to assert the identifier. They do say that the purpose of authentication is to produce an identifier, versus the purpose is to get access to a service.

Scott suggests whether it's possible to use the term identified access to a service.

Andrew notes that they reference "classic kerberos" versus "modern kerberos"

Denny notes that there's a section around usability, but how it looks on the screen and the user interface, is that something that is in the scope now? Andrew Hughes responds that they obtain usability from following the NSTIC guiding principles, which include usability. The idea being that authenticators that are difficult to use are not trusted.

RGW mentions the issue of uniqueness of credentials, and inconsistency in the use of the term "digital service" in the introduction to SP-800-63-B. Section 4 uses the term as if it refers to the Credential Service Provider, whereas the introductory text uses the term as if means the Relying Party.

Section 4 is marked normative, so it should be clear about requirements, use shall statements for that.

Ken agrees with the comment about Subscriber versus Subject. He has gone through cases as a trustee for someone incapacitated, he was the subscriber and they are the subject.

Andrew has a similar observation about the model and state diagrams being inconsistently applied. When you become a subscriber because you have enrolled, the definition of enrollment doesn't include the definition of a service account. Since they are unclear on the enrollment process its not clear what the subscriber is.

RGW suggests maybe this means that 800-63A should include the idea of enrollment and becoming a subscriber/subject. Overall, changing the term from subscriber to subject.

Andrew is wrestling with the question of "are you still a subscriber when you are federating authentication?"

Ken notes that "other attributes that identify the subscriber as a unique subject may be provided".

Part of the model inconsistency is differences in how the verb "authenticate" is applied, does the subscriber authenticate or does the CSP do the authenticating.

On guidance versus technical requirements. Richard observes that on the first page they should be referring to requirements rather than guidance. Calling it guidelines dilutes the force of the requirement.

Andrew can observe that they are putting normative statements in the document but not using normative language.

Andrew observes that a state model would be helpful to show how entities go from non-authenticated to authenticated state, verifiers in pre-authenticated to post-authenticated state. Scott concurs on the state model.

Denny asks about if there's a model for them to reference. Andrew observes that 800-63-3 describes the model of the architecture for the discussion in the documents. There's a role diagram that infers some changes of state, it's indistinct but it illustrates that a claimant becomes a subscriber. Probably not complex, but not documented at this point. Denny wonders about disability acts in various parts of the world.

Additional comments from RGW - section 4.1.2 - cryptographic authenticators at AAL1 shall use approved cryptography. Scott suggests that this is in line with NIST's mission to push approved cryptography for all uses of government cryptography.

Additional comment RGW - 4.1.4, 4.2.4, 4.3.4 there are references to 800-53 "or equivalent standard" but what is the method of judging what an equivalent standard is.

Andrew has a comment on section 4.5 - summary of requirements, they don't have rows for records retention or privacy requirements.

Ken notes that there are currently no normative usability requirements.

AOB

Attachments

Next Meeting - topic will be 800-63C and the new charter

- **Date:** Thursday, 2017-03-16
- **Time:** 12:00 PT | 15:00 ET
- **Time:** 12:00 PDT | 15:00 EDT
- United States Toll +1 (805) 309-2350
- Alternate Toll +1 (714) 551-9842
  Skype: +99051000000481
    - Conference ID: 613-2898
- International Dial-In Numbers