IAWG Meeting Minutes 2015-03-12

Kantara Initiative Identity Assurance WG Teleconference

Date and Time | Agenda | Attendees | Minutes Approval (no minutes to review) | Staff Updates | Tweet Worthy Events | Discussion | AOB

Date and Time

- **Date:** Thursday, 2015-03-12
- **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) 551-9842
  Skype: +99051000000481
    - Conference ID: 613-2898
- International Dial-In Numbers

Agenda

1. Administration:
    a. Roll Call
    b. Agenda Confirmation
    c. Minutes approval: (meeting minutes from 2015-02-26 are having technical difficulties and not available)
    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. FIPS 140-2 versus Common Criteria equivalents
    b. NIST SP 800-63 update
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 achieved quorum

Voting

- Scott Shorter (S)
- Andrew Hughes (VC)
- Devin Kusek
- Lee Aber
- Cathy Tilton
- Rich Furr
- Richard Wilsher
- Adam Madlin

Non-Voting

- Björn Sjöholm
- Pete Palmer
- Angela Rey

Staff

-

Notes & Minutes

Administration

Minutes Approval (no minutes to review)

Staff Updates

- Check out KantaraInitiative.org events page - Joni at SXSW,
- Rumor of a F2F meeting at RSA 4/20 but we're not certain of that

Leadership Council (LC) Updates

- Put aside the all member ballot on social media policy, should be going forward as an e-ballot

Participant updates

Tweet Worthy Events

None suggested. Cathy Tilton mentioned the member success story that the Daon product implementation for USAA. CUNA credit union gave a best in show award to Daon for this.

Discussion

FIPS 140-2 language concerns

FIPS 140-2 vs CC topic. On the ARB call this week, discussioons with assessors in Europe noted that Kantara SAC reflects FIPS 140-2 for cryptographic requirements, and national body approved equivalents, which resulted in a perception of a US centric document. Suggested adding relevant common criteria standards for this. ARB has asked IAWG to consider a rewording of those sections that refer directly to the FIPS to reverse the order - make the core reference the ISO standard, or national equivalents.

Cathy agrees but doesn't think this addresses the problem of crypto on mobile devices, where SP 800-63 requires FIPS 140-2 level 1 certified software modules. Major OS on devices do have FIPS 140-2 certification, but that is specific to the handset, chipset, version of OS, etc.

Bjorn - is this an issue for software validation versus hardware validation.

Richard - as a consequence of this - there is an effect that Kantara or FICAM approval could be technically invalidated by the inability of a service to conform to the particular criteria.

Bjorn agrees with the intent of the change.

Richard suggests not mentioning Common Criteria because it is not a conformance standard, suggests ISO/IEC 19790 which is a FIPS 140-2 clone in ISO format. Suggestion is to state ISO/IEC 19790 or national equivalent. This would reduce the US-centric text.

Bjorn points out there would be no validated software or hardware using the ISO/IEC 19790 program.

Richard reviewed the SAC - where the phrase "FIPS 140-2 or recognized US national equivalent" is used, replace that with a reference to ISO/IEC 19790. Lee Aber was concerned with lack of reference to FIPS 140-2 would confuse government procurement folks who expect that term. Richard Wilsher is concerned that listing local standards is not solving the problem.

Action Item for Richard Wilsher to provide proposed change that reflects the ISO/IEC 19790 approach.

Richard mentions that now would be a good time for an editorial change.

NIST SP 800-63 update

Andrew Hughes reports that Paul Grassi asked for our opinion about whether the RFI vehicle is suitable for gathering information from industry. Is the RFI process appropriate.

Angela Rey responds that RFIs are typically a pre-solicitation information gathering for an agency to collect information to boost the solicitation process. We don't expect that 800-63 will go through procurement process.

Cathy's thoughts are that an RFI doesnt' have to be used as a precursor to a procurement. Alternatively they could do an open request for comments on the existing one. They seem to be looking for a bigger change than just comments on the basic.

RFI can be a time consuming process.

Andrew asks if Kantara has the appetite to reply to an RFI, is there a different way of doing it that would be quicker.

Cathy suggests a workshop would be a good approach. Adam Madlin supports that approach also.

Angela Rey suggest writing an amicus letter to head of NIST and head of DOC. List areas that needs to be addressed and invite them to have a workshop and have a workshop.

Andrew asks, in advance of the possibility of the letter and suggesting a workshop, is it worth developing the list of where 800-63 could be approved?

Cathy mentions that we should lay out the areas of concern that we have.

Andrew suggests we schedule the next meeting to gather concerns with 800-63.

Andrew will respond to Paul that RFI followed by a workshop is a good idea. Didn't hear vocal support of starting the work in advance of starting the scope, after some discussion suggests gathering thoughts to inform what the issues may be. Andrew suggests we work on it at the next available meeting time.

AOB

None

- **Motion to adjourn - Richard Wilsher, seconded Adam Madlin**