2021-08-19 Minutes

Attendees:

Voting Participants: Ken Dagg, Martin Smith, Mark Hapner, Mark King, Richard Wilsher

Non-voting participants: Roger Quint, Varun Lal, Chris Lee, Jimmy Jung

Staff: Kay Chopard

Agenda:

1. Administration:
    a. Roll Call and quorum determination
    b. Agenda Confirmation
    c. Minute approval (DRAFT minutes of 2021-08-12)
    d. Staff reports and updates
    e. LC reports and updates
    f. Call for Tweet-worthy items to feed (@KantaraNews)
2. **Discussion**
    a. **Finalize proposed criterion language regarding "comparable alternative controls."**
    b. **Finalize proposed text (if any) regarding use of "presentation attack detection" (PAD.)**
    c. **Confirmation of other non-substantive changes to criteria to be included in the package to be submitted.**
3. Any Other Business and Next Meeting Date

Meeting notes:

Administrative items:

IAWG Chair Ken Dagg called the meeting to order at about 1:04PM (US Eastern), and called the roll. It was noted that the meeting was quorate.

Minutes approval: Mark King moved approval of the draft Minutes of the IAWG meeting of Aug 12 . Richard W. seconded. The minutes as distributed were approved unanimously.

Staff reports and updates: ED Kay Chopard–New APM Lynzie Adams, starts next week on Monday. Hope she will be on the next IAWG call. Kay Invites anyone to offer suggestions re: any Kantara issues, strategy, etc. .

LC reports and updates: Ken – The LC met yesterday. There was a discussion of the appropriate scope of activity of Kantara WGs, DGs. Results to be communicated to all when guidance is finalized. Ken says IAWG's activities seem to be well within our appropriate scope.

Ken reminded WG participants that Kantara staff is ready to help them publicize their newsworthy activities via the @KantaraNews Twitter handle. Requests can be sent to Ken D or Kay C.

Discussion*:*

Finalize proposed criterion language regarding "comparable alternative controls (CACs)."

Ken invited Richard W. to comment.

Richard thinks "make available" discussion last week (which he reviewed via the recording of the meeting) was off-target. The term "make available" has been used for a long time in Kantara criteria texts, and has not caused a problem. The principle is to tell assessees what must be done, not how to do it.

Martin S.– In proposing a more pro-active approach, I think we were taking account of NIST's David T's reported view, that use of an alternative control should be an explicit client (i.e., RP) risk decision taken at the executive level. and that Kantara should not appear to be endorsing the service-provider's assertion that an alternative control is "comparable."

Richard W.-- But Kantara can't make the RP do something. We might further insure the RPs attention via things we already do, like requiring a statement of criteria applicability; we might also consider requiring that use of a CAC is at least noted in the publicly publishable part of the SPA, which Kantara will publish.

Martin S.: Assuming we do want to take account of David T's viewpoint, it seems we need to find some way to make sure the RP is specifically alerted to the use of a CAC.

Ken: should we add to the criterion that the RP acknowledge receipt of the CAC information? Jimmy J. - that would not be possible or effective – the RPs won't read it. But if KI provided notice we would have done all we can,

Ken : Given this discussion, is it OK with everyone to go with "no change"

Jimmy J: can we put in the "Notes" column of the criteria spreadsheet that we (KI) are going to publish fact of CAC? If we do something unusual, we need to make sure they (the RP) know about it.

Richard W: Suggest we need to modify the SPA to require that "where CACs are provided that it is at least noted (stated) in the publicly publishable part of the SPA, so that it is a declared capability." We don't have to provide specifics on what the CAC is or how it works, but only that the mere fact that it exists is stated. Kantara will publish that through the CSL.

Ken D: And that puts the client (RP) on notice and if they don't check further the onus is on them.

Ken: with that addition-- is group OK with this resolution?

Mark H: Ok with current language; my concern is that the concept of comparable is so poorly defined in 800-63-3 hard to reason about how an assessor should proceed.

Richard W: We did try in sub-clause a-c to add some specificity.

MH: They (NIST) don't define criteria or what information should be communicated. I am still uncomfortable, but don't see what else we can do.

RW: Without any documentation of the NIST risk assessment for the specified controls, how can assessor establish "comparable."? Difficult situation.

KD: This implies that the service provider has to provide its own analysis of the effectiveness of the regular NIST control, in order to have something to which the proposed alternative can be compared.

KD: Moves to approve language for the package: seconded by Mark Hapner.

KD: Approved without objection or abstention.

Finalize proposed text (if any) regarding use of "presentation attack detection" (PAD.)

Ken D. invited Kay C. to provide background on the exchange with Phil Lamm of GSA,

KC: The background is just the one short email question; and Phil has not followed up on it in other discussions since then. The subject of the email from Phil (cc: David T.) was "Kantara's view on facial biometric comparison and PAD as a 63-3A IAL2 requirement." The text says that 63-3A IAL2 does not have a normative requirements for use of PAD for IAL2 remote, but that NIST's Implementation {SIC} Guidance does require it. Does Kantara require use of PAD at IAL2 remote?

RW: I was puzzled that we got the question since the answer (which is "no") can be seen by looking at the criteria spreadsheet.

RW: Previously, I believe we had decided tentatively to remove draft language in 63A referring to use of PAD, since the only NIST normative requirement seems to be buried under a "SHOULD" and we have generally taken the position that we only include normative requirements ("SHALLs") in our criteria. However, it would be possible to express that if a CSP chose to implement PAD, then it SHALL implement it as specified by the NIST SHALL language.

RW: Our current language on B5.2.3 could probably be clarified to make all the sub-paras conditionally required, only if the SP chose to implement PAD. So, in fact our criteria appear to require PAD but we should make a change to clarify that the requirement is conditional on a choice by the SP.

Roger Q: NIST does not require PAD currently. I thought the letter might be asking if KI was doing anything more than NIST is now willing to do.

RW: So that's not what Phil's question was. And the answer to his question about whether Kantara requires use of PAD is "no." Of course an SP could go beyond NIST requirements and could ask an assessor to review those extra mitigations.

KD: Since we do have material changes in this package, so we can consider this change material with no extra process.

RQ: Agree with the conditional approach as described. I think that implements the NIST intent

Ken D. asked for a motion to change the SAC in 63A and B to reflect optional nature of PAD, and if the option is chosen to assess against requirements as discussed. Mark K so moved; Mark H. seconded. The motion was approved unanimously.,

Confirmation of other non-substantive changes to criteria to be included in the package to be submitted.

Ken D noted the time, and said we would defer to the next meeting discussion of the miscellaneous errata to be included in the criteria change package.

Richard W. Noted that all five sets of errata have been reviewed by IAWG at some point and are considered minor, and he confirmed he can pull them together for approval at the next meeting.

Ken D said we will vote next week to complete criteria revisions package for submission.

Other Business:

MK: Any further UK Government response? KC: The UK contacts are still on holiday. However, Allison McDowell did respond from vacation and will connect next week. MK: let's add that report to the agenda for next week please.

KD: How about Australia? KC: did have a 1-on-1 with Jonathan Thorpe, head of the DCA agency, but that was not Colin's contact. He is supportive of Kantara's goals for interoperability, and also thinks Kantara can help them because they are generally using NIST standards. He is hoping companies don't have to go through same assessment process multiple times for different countries. He is looking for KI to provide some leadership in these areas. We also had outreach from Baruku (ph), who wants to talk about their work, but nothing scheduled yet

KD: that's excellent–-nice to hear the Australians are looking to us to coordinate inter-government work. Hope we can use that with other governments–including Canada.

RW: I've drafted modifications to PAD criteria we just discussed–hoping for a quick sanity check of revised language.

Ken D.: Sounds OK to me but let's review it next week.

Jimmy J: I'm OK with it, too but I was hoping we could be a little more daring to somehow credit CSPs who use PAD, since it is so important. But I agree Richard's text tracks what NIST says.

KD: We really can't create criteria that go beyond NIST.

RW: We actually have executed some interpretations that strengthen NIST criteria.

Martin S.: Maybe the thing to do is to make sure we submit a comment advocating making PAD mandatory when NIST issues the 63-4 draft for review. JJ: I like that idea.

Ken D.: Next week (August 26) we will meet to finalize the criteria change package for submission to Kantara review.

Ken thanked participants for their work and adjourned the meeting at about 2:02PM US Eastern.