2021-07-15 Minutes

Attendees:

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

Non-voting participants: Jimmy Jung, Roger Quint

Staff:

Agenda:

1. Administration:
    a. Roll Call and quorum determination
    b. Agenda Confirmation
    c. Minute approval (DRAFT minutes of 2021-07-08)
    d. Staff reports and updates
    e. LC reports and updates
    f. Call for Tweet-worthy items to feed (@KantaraNews)
2. **Discussion**
    a. **Continued discussion of SP-800-63 'comparable alternative controls' - Review Richard W. alternative-controls process draft updated based on comments at last IAWG meeting , and discussion of next steps.**
    b. **Decision on undertaking comments on the recent Pan-Canadian Trust Framework (PCTF) document, comments due 7/28.**
    c. **Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. See: https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation**
    d. **Component Service Consumer criteria.**
3. Any Other Business and Next Meeting Date

Meeting notes:

Administrative items:

IAWG Chair Ken Dagg advised he would be late, so Vice Chair Martin Smith called the meeting to order at about 1:15PM (US Eastern), and called the roll. It was noted that the meeting was quorate.

Minutes approval: Martin noted a question on the draft minutes, which was resolved and will be reflected in the final. With these changes the draft Minutes of the IAWG meeting of June 24 were approved unanimously.

Staff reports and updates: No update.

LC reports and updates: No update.

Martin reminded WG participants that Kantara staff is ready to help them publicize their newsworthy activities and via the @KantaraNews Twitter handle. Or send to Ken D or Kay C.

Discussion*:*

In view of the delayed arrival of Ken D. and Richard W., Martin suggested taking up agenda items on PCTF and EU Digital ID framework, and reverting to the "comparable alternative controls" topic when Ken and Richard arrived.

Decision on undertaking comments on the recent Pan-Canadian Trust Framework (PCTF) document, comments due 7/28.

Martin recalled that at the July 8th IAWG meeting Ken had mentioned receiving a new PCTF document, with any comments due July. Ken had reported that in a quick review he doubted it would be of great relevance to the WG, but said we could discuss it at today's meeting and decide whether to develop comments on the document.

Mark K. suggested that we might want to make sure that others developing national ID frameworks were at least aware of the new document, but said he had no other comments on the document. No one spoke up in favor of submitting comments on the document.

Roger Quint said that it would be very useful to implementers of ID systems (CSPs and RPs) to be able to compare the characteristics of different frameworks and the extent to which they were interoperable or compatible. He wondered if Kantara had any plans to provide guidance like this, and also whether Kantara was doing anything to promote interoperability or compatibility between frameworks, including its own IAF.

Mark K. said that some frameworks that are being developed simply made no mention of interoperation with other frameworks or how users other than their own nationals would be able to interact with services using their framework. He said Kantara had submitted comments to that effect.

Martin agreed that a "side-by-side" comparison of multiple frameworks would be very useful. He added, however, that to create and maintain such an artifact would require a substantial effort, beyond the resources of a volunteer WG. Financial sponsorship would be required. Another member said he believed that Colin Wallis may have in fact sought to find a sponsor. Martin said that in submitting comments on various frameworks Kantara has also consistently recommended that they provide for independent assessment and certification of conformance of participating service providers (principally CSPs) with the framework's standards and service-operations rules, i.e., the kind of assessment that Kantara provides against the Kantara IAF.

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

Martin asked Mark K. if he thought it was important for Kantara to weigh in on this proposal. Mark said that he merely wanted to bring this to the WG's attention as it is a formal proposal. He added that if Kantara wanted to provide input, it might be better received if it came from or at least through Kantara Europe, based in EU Member-State Estonia.

Continued consideration of 'comparable alternatives': discuss revised DRAFT Kantara criteria/process (Wilsher), and next steps

Ken Dagg and Richard Wilsher having joined the meeting, the WG resumed last week's discussion on this topic. Richard shared his draft Kantara "comparable alternative controls" with updates made following last week's WG discussion.

Richard suggested that the goal of an alternative control might be described as an appropriate balance between false positives and false negatives, or some way the CSP could express the risk accepted by using the alternative control. He added that he was not yet satisfied with this formulation.

Ken D, suggested that "a defined risk profile" might work, which both avoids implying that the types of risks that a control might create are limited to its performance on false positives and negatives. Others agreed that an open-ended look at possible risks is appropriate and that Kantara should not imply that assessors would perform quantitative analysis of a controls' effectiveness. Richard W. observed that as far as he could determine, NIST was supposed to have done such a quantitative analysis in developing the 800-63 standards, but that he believed that it had not been published.

Roger Q. expressed concern that most customers (RPs) will not know how to judge the CPS's metrics on performance of their controls. Martin suggested that the RP would rely on the Kantara assessor's evaluation. One member asked if these alternative controls would be assessible. Another said the RP use-cases would be varied, possibly making assessment more complex. Another said that use-case variations should not keep a CSP from documenting and estimating a control's performance, and that the KI assessor's role would be limited to evaluating the CSP's evidence and justifications. Another expressed the view that this was not too much different from what is done now in IAF assessments.

Ken D. noted that the scheduled meeting time had expired and suggested a summing-up of the WP's conclusions at this point.

Richard W offered the view that the CSP should review all the mitigated and residual risks of an alternative control, including any new risks created by the control. This analysis is documented. The CSP's top management is aware of the use of a comparable alternative control; and the CSP does in fact deploy the control. The CSP is required to make any RP client aware of the used of the alternative control and advised of any extra procedures or configuration adjustments needed because of new control. He added that we don't want to specify hard numbers for performance of a control in our criteria.

A member asked if the specification of the control and related documentation would be available for re-use by other CSPs. Several members agreed that the architecture of the alternative control and the associated assessment documentation should be considered proprietary to the CSP that developed it, but that re-use might be achieved by licensing or other agreement with the developer, or perhaps even by the developing CSP offering the control as service component on a SaaS basis. One member wondered if it might hurt the Kantara "brand" if it became known that a service had somehow been certified without meeting the 800-63 requirements. However, another member observed that existing Kantara requirements for publication of information about successful certifications would let other CSPs or interested RPs know that a "comparable alternative control" had been included in the certified CSP service offering, as permitted by NIST.

As for next steps, Ken D. said that once we get Richard's draft finalized, it would go through the standard Kantara process for making "material" changes to the IAF criteria. This process takes about 70-90 days in total.

Richard W. added that we have a number of minor (probably all "non-material") changes to the criteria that should be bundled with this one so as to avoid burdening reviewers with multiple rounds of review.

Richard also noted that he would be unavailable for IAWG work for three weeks starting next week, and suggested that another member take over as IAWG Editor to keep the process moving forward. Ken D. agreed to fill in for Richard as Editor.

4. **Component Service Consumer criteria**

Not discussed.

Other Business:

Next Meeting:

Ken D. proposed that given an otherwise light agenda we should skip next week's IAWG meeting and meet next on July 29th, and then plan to meet two weeks after that (August 12th.) Ken closed the meeting at 3:18PM

Martin's raw notes

RW: don't want to include hard number in criteria.

KD: is this stuff assessible?

MH: don't think so, too many RP use-case variations.

KD: Not impact CSP's ability to document and estimate control's performance. KI assessor would evaluate CSP's justifications.

JJ; I do think this type of assessment is that much different from the existing KI IAF assessments.

MH: Question is: what is the CSP doing to mitigate

KD: Over time at 2:03.

RW: recap: CSP reviews risks of alternative controls, including maybe new risks, documented. CSP's top management is aware of use of comparable alternatives and does deploy them. For each, make RP client aware of the alt control and extra things needed because of new control.

RW: don't want to include hard number in criteria.

MS: re-usable?

RW: don't think so: confidential. KD: agree. not KI job.

JJ: RQ: need to protect KI if we approve a non-std control. Otherwise we look like a black box, and credibility might suffer.

JJ: Or brand says we assess the criteria. If we don't, what will they think.

RW: we ask CSPs to publish their "applicable controls" publicly. SO that's a clue for others that there must be an alternative control in use.

MH: also , added info for agencies about their clients.

KD: need to focus on getting Richard's draft to the point KI can use it.

KD: finalize draft, and then go through material criteria change process. About 70-90 days total.

RW: have a pile of non-material change we should bundle in the package for review. I will be out for next 2-3 meetings. Can I dump Editor on someone? KD.

KD: not meet next week, then again two wwks after

29th of July.

2:18