Meeting Minutes 17 July 2019

Kantara FI-WG Teleconference

Approved on August 7, 2019 call | Date and Time | Attendees | Agenda | Minutes | Next Meeting

Approved on August 7, 2019 call

Date and Time

- **Date:** Wednesday, July 17, 2019
- **Time:** 16:30 EDT

Attendees

- Wessel, Keith (v)
- Roy, Nicholas (v)
- Bush, Judith (v)
- Cantor, Scott (v)
- Morgan, Andrew (v)

Agenda

1. Roll call (QV group participation agreement)
2. Agenda bash
3. Approval of 6/5 meeting minutes: https://kantarainitiative.org/confluence/x/-QDnBg
4. Reserve working group time at 2019 Internet2 Technology Exchange in December?
5. Review of previous AIs:
6. Review of feedback received so far: https://kantarainitiative.org/confluence/x/6IDJBg
7. Is the level/range of feedback we've received as good as it's going to get? Additional thoughts?

Minutes

1. Roll call (QV group participation agreement - 5 of 9)
    a. Quorum achieved
2. Agenda bash
3. Approval of 6/5 meeting minutes: https://kantarainitiative.org/confluence/x/-QDnBg
    a. Nick motioned
    b. Judith seconded
    c. No opposed
    d. Minutes approved
4. Reserve working group time at 2019 Internet2 Technology Exchange in December?
    a. We'll do this as an ACAMP session
5. Review of previous AIs:
    a. Walter: formatting revisions, Nick followed up about this on email, but not sure where it currently stands. **[DONE]** Walter submitted a PR with some questions sent separately to the list.
    b. AI: Nick follow up again on-list **[DONE]**
6. Review of feedback received so far: https://kantarainitiative.org/confluence/x/6IDJBg
    a. Good discussion of issues on email. Let's touch base to see which aren't yet resolved.
    b. AI: Nick update statuses and dispositions in the wiki **[DONE]**
        i. Issue 1: Done
        ii. Issue 2: Scott's wording is probably as good as we are going to get
        iii. Issue 3: Done
        iv. Issue 4: AI: Keith will ask Rainer for clarification on-list
        v. Issue 5: Scott confirmed that the defaults in Shibboleth don't match the recommendation. Can't split the digests into two different digests because of certain hardware implementations that require them to both be the same. Two possibilities:
            1. Specify SHA1 with SHA1 MGF as path of least resistance
                a. We can be conservative and do this. Optionality not worth it.
                b. Is there a security issue with this? Don't know, not a cryptographer. To the best of our knowledge, not aware of a problem. Has to do with the padding that you use when you encrypt certain kinds of data with RSA.
                c. **Decision:** We'll go with SHA1 until/unless someone tells us it's a problem
                d. AI: Scott will look at the current text and propose a change - the original text is confusing.
            2. Use SHA2 for both as more forward looking
               This is a lot less important than the GCM change. Not a lot of evidence/testing to this point. GCM is probably supported a little bit more than this.
        vi. Issue 6: Force AuthN is only confusing for the people that don't like what Force AuthN means.
            1. Do it or don't do it, but if you don't do it, don't tell the RP that you did do it. Don't silently not do it and hope the RP doesn't notice.
            2. Just because you don't like what it means doesn't mean it doesn't mean that.
            3. The original SAML forceAuthn (isPassive is much clearer) text is not very clear. It's entirely within the domain of a deployment profile to be a lot clearer so that no one is confused. Should be the opposite of isPassive (basically "isActive").
            4. Diplomatic way of responding?

        a. Just say consensus of the people who brought the forceAuthn requirement to the profile is not in agreement with the rationale for allowing fulfillment of forceAuthn requests without actively making the user re-authenticate.
        b. We could also say that there is a broader context that you could bring into play (such as known screen lock policies on all client systems) to fulfill the requirement and respond in the affirmative for forceAuthn request. If your compensating controls are good enough that you feel confident in fulfilling this request and adhering to the spirit of the requirement, then that's fine, but that's your call.
        c. AI: Scott volunteers to come up with text to describe the logon screen experience if people feel that's useful. This would be non-normative guidance.

7. Is the level/range of feedback we've received as good as it's going to get? Additional thoughts?
    a. There are some new issues that got added in GitHub, we should review them next time.
    b. Don't need to push harder at least for now.

Next Meeting

- **Date:** Weds, Aug 7, 2019
- **Time:** *16:30 EDT*
- **Code:** https://global.gotomeeting.com/join/110596309
- You can also dial in using your phone.

United States: +1 (669) 224-3318

Access Code: 110-596-309

More phone numbers

Australia: +61 2 8355 1038

Austria: +43 1 2530 22500

Belgium: +32 28 93 7002

Canada: +1 (647) 497-9380

Denmark: +45 32 72 03 69

Finland: +358 923 17 0556

France: +33 170 950 590

Germany: +49 692 5736 7300

Ireland: +353 15 360 756

Italy: +39 0 230 57 81 80

Netherlands: +31 207 941 375

New Zealand: +64 9 282 9510

Norway: +47 21 93 37 37

Spain: +34 932 75 1230

Sweden: +46 853 527 818

Switzerland: +41 225 4599 60

United Kingdom: +44 330 221 0097

NOTE: *Do not follow the code with a "#" symbol as it may cause the code not to be recognized.*