

Copy of Meeting Minutes 4 December 2019

Kantara FI-WG Teleconference

[Pending approval](#) | [Date and Time](#) | [Attendees](#) | [Agenda](#) | [Minutes](#) | [Next Meeting](#)

Pending approval

Date and Time

- **Date:** Wednesday, December 4, 2019
- **Time:** 16:30 EDT

Attendees

- Keith Wessel (co-chair) (v)
- Nick Roy (v)
- Alan Buxey (v)
- Andy Morgan (v)
- Judith Bush (v)
- Scott Cantor (v)
- Walter Hoehn (co-chair) (v)

Agenda

1. Roll call (QV [group participation agreement](#))
2. Agenda bash
3. Approval of [10/16 meeting minutes](#)
4. Discussion of handling revision to implementation profile
5. Update from Bella and Colin

Minutes

1. Roll call (QV [group participation agreement](#))
 - a. Quorum achieved
2. Agenda bash
3. Probably need to vote within the group on a committee draft that goes to the board for approval.
4. In the SAML 2.0 implementation profile, IIP-ALG06 states:
The following DigestMethod algorithms SHOULD be supported for both of the above key transport algorithms for backward compatibility.
[*http://www.w3.org/2000/09/xmldsig#sha1](http://www.w3.org/2000/09/xmldsig#sha1)

This requirement should be corrected to read:
The following DigestMethod algorithms MUST be supported for both of the above key transport algorithms for backward compatibility.
[*http://www.w3.org/2000/09/xmldsig#sha1](http://www.w3.org/2000/09/xmldsig#sha1)
5. Options include publish errata, or bump version number to 1.1 or 2.0
6. Colin believes that a version number bump with this edit will not require a non-member re-ballot according to the [operating procedures](#)
7. Should we add links to errata wiki to both documents while we are at it? (Where is the errata wiki link?)
8. Minutes approved
9. Approval of [10/16 meeting minutes](#)
10. Discussion of handling revision to implementation profile
 - a. Al: Scott will update the document and send a local diff to the list. We are keeping SHA2, making SHA1 support a MUST.
 - b. Al: Keith run the diff past Colin to make sure it's OK without a rebalot.
 - a. Definitely not 2.0.
 - b. Group recommends 1.1.
 - a. Don't need a re-review if the change does not break implementations, per Kantara Operating Procedures v3.0
 - b. Technically, you can never change a SHOULD to a MUST in a non-breaking change
 - c. Practically, very few implement SHA2 at this level, and almost everyone implements SHA1. So practically, this is a non-breaking change.
No one has built a SAML stack based on this yet.
 - d. Make it clear to Colin what we're doing, make sure he's sound with it.
 - a. Al: Keith check with Colin on if there is any type of set practice with regard to inclusion of errata link in a document.
11. Update from Bella and Colin
12. Al: Nick post minutes, update previous minutes to approved.

Next Meeting

- **Date:** TBD
- **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.