UMA telecon 2018-12-13

UMA telecon 2018-12-13

Date and Time

- **Thursdays 9am PT**
  - Screenshare and dial-in: https://global.gotomeeting.com/join/857787301
  - See UMA calendar for additional details: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Meeting logistics
  - Reminder: Doodle poll is still open for new meeting time in the new year; respond by Tuesday of next week
  - Meeting at the *usual time* (Thursday 9am Pacific) on Dec 20; *not meeting* on Dec 27
- Approve minutes of UMA telecon 2018-12-06
- Reminder: Identiverse call for presentations is open
- FYI, the Implementations page has been updated

- 180 degrees / decoupled / CIBA use cases
  - Use case doc from Nancy
  - Latest CIBA specs: MODRNA status page, FAPI profile
  - What are *practical* methods, leveraging the existing UMA flows, for a requesting party to know the RO is the RO?
  - How does the RS know the RO is the RO?
  - Previous discussion: May 31, Jun 7, Sep 13, Oct 18, Dec 6 – please refresh your memory
- AOB

Minutes

Roll call

Quorum was not reached.

Meeting logistics

- Reminder: Doodle poll is still open for new meeting time in the new year; respond by Tuesday of next week
- Meeting at the *usual time* (Thursday 9am Pacific) on Dec 20; *not meeting* on Dec 27

Approve minutes

- Approve minutes of UMA telecon 2018-12-06

Deferred.

Reminder: Identiverse call for presentations is open

Deadline is 11 Jan 2019.

180 degrees / decoupled / CIBA use cases

- Use case doc from Nancy
- Latest CIBA specs: MODRNA status page, FAPI profile
- What are *practical* methods, leveraging the existing UMA flows, for a requesting party to know the RO is the RO?
- How does the RS know the RO is the RO?
- Previous discussion: May 31, Jun 7, Sep 13, Oct 18, Dec 6 – please refresh your memory

The MODRNA status page is here. The last issues have just been closed. The plan is to have a CIBA Core spec (current draft here – thanks, Bjorn!), which will move to the Connect working group after IPR issues are resolved, and a MODRNA profile, which will stay in the MODRNA group, along with the FAPI profile. The specs were split just yesterday, and tomorrow the specs will be sent out for public review before the Implementer's Draft vote. Beyond the notification modes we discussed, the substantive changes are around greater implementability and focusing strongly on the mobile use case, and how to treat the return values, and adding security and privacy considerations. Brian C and Dave T did a lot of work on it.

We discussed Mike's analysis from Jun 7. Bjorn wonders if his concerns from that time aren't as applicable to the Core spec as to the MODRNA profile.

It would be a good idea for us to review the Core spec at this juncture. We can analyze if, in fact, the "UMA business model" approach is accounted for, with multiple parties and delegation between them. The Oct 18 notes go into detail on why this is important.

The PAT is the only in-band UMA artifact that suggests a communications channel we could use to prove how Alice could prove who she is to the RqP's satisfaction. Peter suggests that they are doing something like this: They are leveraging a "modified use of scopes" to determine access to things. Alice's IdP has a tightly coupled relationship with the AS (effectively colocated) but they have a protocol-level separation. The scope is placed into the access token that is presented to the RS, but the scope is signed by the AS, which proves that it was Alice that authorized the access to the resource. This sounds like the ecosystem circumstance described in the last paragraph of UMA Grant Sec 5.7. Adrian notes that a Verifiable Credentials approach would give a level of flexibility of how you would achieve that trust. (They're actually using a very long list of resource-type-bound scopes to achieve this now.) Family members and non-family members need to be treated differently. In Peter's case, they have done in-person proofing.

How can we prove that the "Alice" of the managing-resources (at the RS) and the "Alice" of the controlling-access (at the AS) is the same at all times? Is there a good IAL (identity assurance level) across all interactions? In Peter's implementation of sharing, they have keys that are under management and there is a strong binding when Alice first starts registering proofing documents (passports, etc.) and strong lifecycle management throughout, along with consent receipts as part of the RPT(-equivalent). Very interesting.

It seems that we are on the right track for potential profiling (or something), by asking the right questions in specific enough form. More next week.

Attendees

As of 18 Oct 2018, quorum is 5 of 8. (Domenico, Peter, Sal, Andi, Maciej, Eve, Mike, Cigdem)

1. Domenico
2. Peter
3. Sal
4. Eve

Non-voting participants:

- Scott
- Thomas
- Nancy
- Adrian
- Bjorn
- Colin

Regrets:

- Andi
- Cigdem