UMA telecon 2016-05-19

Date and Time

- Thu May 19, 9-10am PT
- Voice: Skype: +9905100000481 or US +1-805-309-2350 (international dial-in lines), room code 178-2540#
- Screen sharing: http://join.me/findthomas. NOTE: IGNORE the join.me dial-in line shown here in favor of the dial-in info above (Kantara "line C" and the Skype line)
- UMA calendar: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Meeting schedule
  - Still spotty: when can we manage to keep meetings on the calendar?
- Approve minutes of UMA telecon 2016-04-14
- Past and upcoming events
  - News from IIW and EIC
  - Preparing for CIS
  - Other goings-on
- Justin’s “multi-party delegation” change proposals
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes
tbs

CIS prep

Don't forget about Cloud Identity Summit. It's not too late to register (contact Andi Hindle for assistance, wink wink). There's a Kantara Summit, an UMA talk, an UMA MasterClass, a HEART talk, and a privacy track, all relevant to what we do here. (And: BLOCKCHAIN!!!!)

Eve, Colin, Andi, George, Maciej, Sarah, Justin, and Ishan are all attending – and speaking. Nagesh may attend.

Meeting schedule

Let’s put next week’s meeting back on the calendar. Huzzah. We’ll have a good long stretch of meetings through June and July.

Any huge absences? Please let Eve know.

IIW and EIC recaps

At IIW, beyond the "MPD" discussion:

- Adrian convened a session where we discussed blockchain/smart contract implications for UMA. Think "escrow" where payment for access to a resource could be worked out, or proving certain elements of identity in a wide ecosystem.
- Eve created a diagram describing different kinds of delegation: RO-to-AS (as an "agent" for executing to Alice's wishes), RO-to-RqP (delegating access to resources), and Resource Subject-to-Grantor (offline wrt the protocol, but an important business/legal relationship).
- Adrian brought up ten kinds of "self-sovereign technology", different from self-sovereign identity*. Think about a "personal" type of UMA authorization service. Contact Adrian for more information.

At EIC:

- Eve gave a keynote that centered on UMA (and a HEART use case). Lots of discussion.
- Ian gave a keynote where he called for an identity p
- rofessional association; Kantara put up a pledge signup site!

Justin's change proposals

For reference: The wide ecosystem challenge analysis document. The challenges came from two sources: the identity protocols used to convey identity /claims require pre-established trust, and UMA itself requires a pre-established AAT. Justin’s proposals eliminate the AAT (much as a very old version of UMA had only two tokens) and do a bunch of other cleanup, which tackles not only #wideeco but also #simplify.

We walked through the bullets in Justin's original email.
Changes include:

- Removal of the RPT endpoint, in favor of using the token endpoint and a new grant type (#153)
- Removal of the AAT (#154)
- Removal of extraneous bits of the resource set registration URL pattern (#155)
- Alignment of the discovery document with OIDC discovery (#157)
- Removal of “version” field in discovery document, instead document is published under new .well-known URL pattern (#159)
- Change use of “scopes” name in responses to something more explicit (#158)
- Ability of client to specify scopes in token request (#165)
- Addition of the claims-gathering URL to the need_info response, removal of “redirect_user” as redundant in this case (#167)
- Simplification of the “need_info” response structure, removal of extraneous object layers (#237)
- Rotation of ticket values on all requests to token endpoint or claims endpoint to mitigate session fixation and related attacks (#239, #205)

Discussion about “Ability of client to specify scopes in token request”: In UMA V1.x, the flow is client-to-RS-first. The client is entirely "dumb" with respect to what scopes are available, and can only attempt access using one scope at a time, and the RS is entirely in control about how many scopes to register: one (stingy), or more than one (generous). Sarah suggests that Justin's motivation is privacy preservation. The client could essentially do a downscoping by requesting fewer scopes than the RS would have requested. But is this the motivation? Are both motivations relevant (downscoping and upscoping)? Also, does Justin's change enable an additional client-to-AS-first flow or is it still client-to-RS-first alone? If the client approaches the AS, how does the client indicate the specific RO and resource needed – does it need to know the rsid? On balance, might there be privacy-destructive aspects if Alice ends up sharing more access? Eve had pointed out at I IW that the asynchronous nature of the RO's control means that the client shouldn't really get to say what scopes it requests anyway. George thinks it's more of a negotiation. And maybe negotiation among RS, C, and RO isn't entirely bad? To be discussed on the legal subgroup call.

It will be key to have accurate swimlanes and hopefully some spec text to stare at during next week's call.

Attendees

As of 15 Apr 2016, quorum is 7 of 12. (François, Domenico, Kathleen, Sal, Nagesh, Thomas, Andi, Robert, Maciej, Eve, Mike, Sarah)

1. Domenico
2. Kathleen
3. Nagesh - Accenture and JPMorgan Chase experience in IAM - now at Optiv and working at home with schedule flexibility!
4. Andi
5. Robert
6. Eve
7. Sarah

Non-voting participants:

- Adrian
- John W
- Jin
- Ishan
- George
- Colin
- Scott

Regrets:

- Sal
- Mike