UMA telecon 2016-04-07

UMA telecon 2016-04-07

Date and Time

- Thu Apr 7, 9-10am PT
  - Voice: Skype: +99051000000481 or US +1-805-309-2350 (international dial-in lines), room code 178-2540#
  - Screen sharing: [http://join.me/findthomas](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](http://kantarainitiative.org/confluence/display/uma/Calendar)

Agenda

- Roll call
- Approve minutes of UMA telecons 2016-03-24 and 2016-03-31
- IIW roundup
  - UMA video opportunity
  - Session ideas and plans
- "Why UMA" check-in
- Content and case study progress
- Examining solutions for wide ecosystem challenges ([Eve's challenge analysis doc](http://kantarainitiative.org/confluence/display/uma/Calendar)) – look at:
  - UMA-protected UserInfo? (various)
  - Different patterns of Alice's AS and RS's accepting and providing federated logins? (Adrian)
  - "Multi-party" proposal? (Justin) (engages with #APIsec and #simplify use case buckets too)
  - AS requests claims and client does act_as Bob to send them? (Mike, James)
  - Alice's AS dynamically gets client credentials to Bob's claim sources? (various)
  - Meta-suggestion: Should trust elevation methods be modularized? (James)
  - Others?
- AOB

Minutes

Q2 is conference season – meeting series to get some interruptions

General logistics note: We meet next week, but not April 21 or 28. We'll also miss May 12 for EIC, and some random other Thursdays and Fridays; keep an eye on the online calendar and your inboxes if you subscribe. (Let Eve know if you want invitations.)

Roll call

Quorum was not reached.

Approve minutes

Deferred.

UMA video

Mike is motivated to put together a Doodle poll to see who's interested to throw $100 into a pot to jointly sponsor (as the UMA WG) a 1-minute video.

"Why UMA" check-in

Eve is waiting to hear from Pedro about a Red Hat case study.

Wide ecosystem

We reviewed the paragraph called "The role of the AAT" in the challenge analysis document. George notes that the AAT is supposed to be a tuple of Bob, the client, and the AS, but what is the "Bob" we're talking about here – what identity in particular are we talking about? Is it really true that Bob needs to create an account at the AS? It's not strictly true that an account is needed, in fact. Could it all just be transient? The AAT, at least, needs to live long enough for the client to use it when making RPT endpoint calls etc. Some AS's might have a business model that prefers creating lots of accounts, but others might not. Is "session" a better way to describe the AAT requirement than "account"?

Alice says that "the entity that controls this identifier can do this thing with my resources". The canonical scenario's policy condition given in the document is roughly in identifier-based form (unless the email address in question is shared). Is there an identifier vs. authenticator distinction? How philosophical is this? How would any of Bob's claims get persisted across his sessions at a single AS if he wants access to multiple RS's, potentially for resources controlled by multiple RO's? (Note that regardless of these conditions, the persistence would still be tied to a single client; an AAT would be client-specific, being an OAuth access token.) Having an account at the AS doesn't make his claims any more fresh. If you look at different kinds of clients (mobile, IoT, etc.), Ishan suspects that since different AS's left to their own devices would have made different choices about an AAT, clients would prefer different choices themselves. But isn't an AAT tantamount to a session cookie? Yes, but they're not identical. A thermostat itself doesn't maintain a session itself; its gateway proxy does.
Ishan notes that since data goes stale, the AS may always want to grab the latest data. It could evaluate a freshness metadata field, of course, but it's going to want to mitigate risk by grabbing the latest.

**AI**: Eve: Add a #trust issue about liability for claim staleness.

We agreed that the various solution possibilities for #wideeco may not be mutually exclusive, and also that we shouldn't nail down final choices of solutions till we analyze additional relevant use case buckets in our roadmap. We'll ask champions for the various solutions to present in future weeks.

The challenge document should now be open for everyone to comment (you probably need to reload it).

Here's more information about the IETF ACE group and its documents. See also this older (now-expired) spec about ACE for OAuth and UMA.

**Attendees**

As of 20 Feb 2016, quorum is 7 of 12. (François, Domenico, Kathleen, Sal, Thomas, Andi, Robert, Maciej, Eve, Mike, Sarah, Ran)

1. Kathleen
2. Robert
3. Eve
4. Mike

Non-voting participants:

- Andrew
- Adrian
- George
- Ishan