UMA telecon 2017-03-23

UMA telecon 2017-03-23

Date and Time

- Thursdays, 9-10am PT (back to regular time slot, still in "summertime skew" this week)
- Screenshare AND dial-in: [http://join.me/findthomas](http://join.me/findthomas)
- UMA calendar: [http://kantarainitiative.org/confluence/display/uma/Calendar](http://kantarainitiative.org/confluence/display/uma/Calendar)

Agenda

- Roll call
- Approve minutes of UMA telecon 2017-03-09
- Logistics
- UMA V2.0 work:
  - 2016 roadmap / GitHub issues for V2.0 (all issues to be kept here for the duration!) / dynamic swimlane
  - Core is up to 20 and RReg is up to 06 (WG drafts)
  - See new issues
- AOB

Minutes

Roll call

Quorum was not reached.

Approve minutes

Approve minutes of UMA telecon 2017-03-02: Deferred.

Logistics

Can we move to a Wednesday time next week? Let's try.

AI: Eve: Cancel next Tuesday's meeting (Mar 30) and propose a Wednesday (Mar 29) meeting time if possible.

UMA V2.0 work

Issue #292: Eve was concerned about potential scope collisions. But George points out that collisions would be bad in the context of a whole set of resources that a client would be dealing with, and Justin notes that in UMA, scopes are per resource anyway, and scopes can actually differ per resource.

Consensus: No need to add a new "type" field for scope description documents.

AI: Domenico: Create UMA2 version of the more detailed "UMA oval".

Issue #294: This would be of interest to some folks. Prabath has mentioned RFC 7800 to Eve. Justin notes that it solves only a small part of the puzzle, and that the OAuth PoP architecture draft et al. aren't finalized yet and the WG seems to have no appetite to finish them and that token binding solves All The Problems. George agrees token binding is useful, but it's not very deployable; it just provides correlatability of the same SSL session. Mutual TLS with token binding approaches being equivalent. When you go beyond a two-party system, which OAuth and especially UMA are, then it gets wildly complicated.

Justin recommends his book, chapter 15 especially, specifically page 296. 😊 He points to Hans Z.'s recent [Token Binding writeup](http://example.com).

Right now, in UMA2, we have excised every mention of `Bearer` from Core. So in fact it might be possible for RPTs to make automatic use of PoP tokens. Can we find out? Could token binding be used with refresh tokens (presumably this still applies) and even PCTs? How can we find out? Is it worth stating the result of our investigations in the spec or in the UIG?

PoP is done by the RS. Justin has implemented a way for the AS to hand the RS the JWK it needs to validate the JWT, but there's no official spec (among the plethora of PoP specs) for handing over this particular piece of metadata. So as far as people have gotten is to say, basically, "Use whatever means you have available to get this info – local or introspect etc."

Not being a "P*P" architecture, the RS still "reserves the right to refuse service". The client is the one proving possession. (This is not SAML HoK, where it would be Bob proving possession.) Justin recommends his diagram on pages 385-386!)
AI: Issue on rescinding access positively/downscoping: Eve to add. DONE.

Attendees

As of 7 Mar 2017, quorum is 4 of 7. (Domenico, Sal, Andi, Maciej, Eve, Mike, Cigdem)

1. Domenico
2. Mike
3. Eve

Non-voting participants:

- Justin
- Dean
- George
- Crina
- Scott F
- Jin

Regrets:

- John W
- Sal