UMA telecon 2017-07-20

UMA telecon 2017-07-20

Date and Time

- Thursdays, 9-10am PT
- Screenshare and dial-in: http://join.me/findthomas
- UMA calendar: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Approve minutes of UMA telecon 2017-06-29 and UMA telecon 2017-07-13
- UMA 2.0 work:
  - Discuss proposed items from #337 (forthcoming)
  - Discuss any proposed wording from #332 (forthcoming)
  - Review in-progress Disposition of Comments document (forthcoming)
- Finalizing the specs
  - When will we be ready to vote on progressing specs to the LC and then to All-Member Ballot?
- UMA2 logo ideas
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2017-06-29 and UMA telecon 2017-07-13: APPROVED by unanimous consent.

UMA 2.0 work

Is the right distinction in the Disposition of Comments document "Would the change potentially cause anyone to raise a new IPR issue or not?", rather than "Is it 'editorial' or 'technical'?" So if something goes from, say, MUST to something weaker (SHOULD or MAY), that would (could?) raise IPR issues. But just clarifying something that was unclear in the Draft Recommendation would presumably be editorial. Andrew asks: If no one makes a necessary claim, does it matter? "The tree has already fallen in the forest." The WG will make its case in the comment log where anything seems marginal.

Finalizing the specs

Sample motion when the time comes: "Approve UMA 2.0 Grant and FedAuthz revs 06 as amended by the instructions of UMA telecon 2017-xx-xx as Draft Recommendations and forward them to the Kantara Leadership Council to request certification for an All-Member Ballot as Recommendations."

#332: If the AS is "basically" expiring a previous PCT when it goes to a new authorization process, should we say it MUST? It's more like any previous PCT from a previous assessment has be superseded/overcome by events (namely, "one process/one ticket lifecycle"). How explicit do we need to be about this, for implementers to understand this clearly? We're inclined not to add more refresh token-like text, despite the suggestion, because it's a little too prescriptive, and we agree with the commenter's interpretation that "I would say, that according to the current version, the AS can really choose whether to expire PCT when issuing a fresh one and the client is not forced to discard the old one." Using this behavior, the AS and client would each simply have old PCTs from previous authorization processes and could issue/use them for any future authorization processes they want. The wording throughout Grant doesn't prevent this; we checked. Do we now need to consider clarifying that this "multiplicity" of uses is okay? Is it ambiguous the way things stand? That is, Eve's reading, in the issue, of "basically" expiring is not required. Justin, James, and Mike (Yuriy) all interpret the current text to be okay with more than one-time use. Optimization of future experience is basically the rationale for PCTs, so this makes sense.

Andi brings up the security and privacy considerations; we do cover these, and revocation is also covered, so we're good there. And the AS can always expire at will.

No change in the wording.

#337:

- exp/iat/nbf: There was an original reason for the "split" logic of talking about what happens when exp is absent vs the others. "If the parameter is absent, the permission does not expire." We tried to mean that the permission could live on past the token lifetime, but this is nonsense. 😞 What if we delete this sentence, keep the three other sentences allowing the token-level value(s) to take precedence (or refactor that sentence out to the token level), and live with the fact that we don't say anything about the absence of the OPTIONAL values? What is our intent about implementers' behavior? The RS's behavior is about cache control. The AS is likely not to hand back something already expired. Everything beyond active=true is a hint. So the RS could just try again if it didn't get what it wanted.
- Did a quick tour through the other items. Most should be easy for disposition.

UMA logo ideas
At: Eve: Email out Domenico's first logo idea. Let's send thoughts his way.

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

1. Domenico
2. Sal
3. Andi
4. Maciej
5. Eve
6. Mike

Non-voting participants:

- James
- Justin
- Andrew