UMA telecon 2012-03-22

UMA telecon 2012-03-22

Date and Time

- WG telecon on Thursday, 22 Mar 2012, at 9am PT (time chart)
  - Skype: +9905100000481

Agenda

- Roll call
- Approve minutes of 2012-03-08 and 2012-03-15 meetings
- Tweet chat AIs and other outstanding AIs
  - April 25th okay for third tweet chat?
- Review latest spec in preparation for new I-D submission
  - Using join.me
- Interop planning
- AOB

Minutes

New AI summary

- Eve and Thomas: Rev spec based on UMA telecon 2012-03-22 results.
- Thomas: Publish rev 04 spec as I-D.
- Eve: Change voting participant status for habitual non-attendees.

Roll call

Quorum was not reached.

Approve minutes of 2012-03-08 and 2012-03-15 meetings

Deferred due to lack of quorum.

Tweet chat AIs and other outstanding AIs

- April 25th okay for third tweet chat?
Deferred.

Review latest spec in preparation for new I-D submission

- Using join.me

Should we explain in Sec 1.3 that the various token types are meant to be extension types, and require both token format definitions and protocol sub-flow definitions/implications? This is somewhat similar to the claim type proposition. Yes.

Fix missing space near "JSON" in Sec 1.5.

Fix missing "for" in Sec 1.3.

Should we issue the RPT separately from the permissions that would go in it? Because the AM is building a set of known claims about Roger independently of a particular host or protected resource, claims should be reusable. Could the claims be hung off the AAT for that reason? We think so. As Roger interacts with TripFollwr, if the AM has enough claims to satisfy the request for the current permission, could TripFollwr ask for it silently? Roger only needs to be redirected over if the AM never got the needed claims before, or they've expired, etc. Ideally the TripFollwr request for permission is back-channel, and only if CopMonkey responds with "I need claims", then TripFollwr needs to do the redirect.

What if we were to change Sec 3.4.4 to be exclusively back-channel? We wouldn't need the redirect URL to be supplied in the request anymore (it would move to Sec 3.5.1 and, implicitly, to 3.5.1.1). We wouldn't need the state property or the callback URL either. Since it's now a server-to-server interaction, we should be able to mandate POST. However, the edge case is a JavaScript requester actually running in a browser. Can we just mandate POST for now, copying the security rationale text that appears in Sec 3.3 for the same reason? Yes. We also need to add an example of the requester's permission request; copy the request in Sec 3.3 for inspiration. We also need to add a "need_claims" response to the list of UMA errors in Sec 3.4.4.

Sec 3.5.1 needs to make clear that any authorization flow profiles that involve humans need to a) redirect the user, and b) provide redirect, callback, state, etc. information as required to get the user back to the requester app safely. Sec 3.5.1.1, in depending on OpenID Connect, for example, has all this baked in by virtue of the OpenID Connect specs themselves.
So, do we need a separate "UMA token" issuance endpoint compared to the permission request endpoint? If we had it, it could act a lot more like vanilla OAuth, maybe handing out a refresh token in addition etc. Since the RPT system already has two levels of expiration (RPT and permission), and since the claims-gathering flow is separate from the RPT per se, a refresh token doesn't seem valuable. Agreed.

We reached rough consensus on all these points. If any participants who couldn't make it to this call have a big problem with any of these directions, speak now.

**Interop planning**

We'll pick this up, along with the KI.org blog entry idea, after the next I-D is published.

**Next Meetings**

- WG telecon on Thursday, 29 Mar 2012, at 9am PT (time chart)

**Attendees**

As of 12 Mar 2012, quorum is 8 of 13.

1. D'Agostino, Salvatore
2. Fletcher, George
3. Machulak, Maciej
4. Maler, Eve
5. Moren, Lukasz
6. Szpot, Jacek

Non-voting participants:
- Cox, Kevin

Regrets:
- Catalano, Domenico