UMA telecon 2019-12-19

UMA telecon 2019-12-19

Date and Time

- Thursdays 6am PT
  - Screenshare and dial-in: https://global.gotomeeting.com/join/857787301
  - See UMA calendar for additional details: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Approve minutes of UMA telecons 2019-10-03, 2019-11-21, 2019-12-05, 2019-12-12
- Explore idea of UMA extension that reuses some portion of RAR/PAR
- AOB

Minutes

Roll call

Quorum was not reached.

Approve minutes

- Approve minutes of UMA telecons 2019-10-03, 2019-11-21, 2019-12-05, 2019-12-12

Deferred.

Reminder: Identiverse CfP is open till Jan 10

Keep those cards and letters coming!

Explore idea of UMA extension that reuses some portion of RAR/PAR

Some handy links about RAR/PAR:

- Roundup by Aaron Parecki of IETF 106 artifacts, including spec links
- Brief discussion on the UMA WG list of RAR/PAR interest
- Medium article from Torsten L on the specs from Sep

PAR is currently at rev 01. There has been a call to accept it as a work item in the OAuth group, and it’s looking very likely. Justin noted that he has implemented it. The adoption call was a compound one for both PAR and RAR, but now things have gotten more separated out. Torsten has also proposed through FAPI issue #275 to use PAR and RAR in FAPI. So our attempt at experimentation here is timely.

Would this be so invasive that we’d have to reinvent a permission ticket structure to replace the resource ID and hunt around for something in XYZ to replace it (the transaction handle), and then end up accidentally discovering “how XYZ really does UMA”? We have a RqP doing the authorization request, not “the user” (the RO).

The purpose of PAR is to enable the client to push fine-grained details of its need for access on the back channel so it doesn’t need to send them on the front channel, but we’re already doing that anyway. UMA already allows for multiple resources per RS to be requested, and differentiated scopes per resource. The introduction to RAR (which is at rev 03 right now says (emphasis added):

“OAuth 2.0 authorization framework [RFC6749] defines the parameter "scope" that allows OAuth clients to specify the requested scope, i.e., the permission, of an access token. This mechanism is sufficient to implement static scenarios and coarse-grained authorization requests, such as"please give me read access to the resource owner's profile"(586,729),(769,751) but it is not sufficient to specify fine-grained authorization requirements, such as “please let me make a payment with the amount of 45 Euros” or “please give me read access to folder A and write access to file X”.”

Let’s give names to the two use case aspects that RAR's data structure solves. The first could be called transaction grain and the second could be called resource grain. UMA already solves for resource grain.

We have defined how Alice can set conditions of access for an RqP. What about Bob setting the conditions for his own access? Adrian has a diagram that is useful for thinking about this question. “Credentials presentation” maps to Bob having to present claims to Alice’s AS (each circle is some service/software representing the entity shown) so that he can prove he’s suitable against her policy. “Resource scope request” is his client's request for scoped access to some specific resource. “Data use assertion” is the new thing here: It’s what he tells Alice about how/why he intends to use the access he was granted. The RS (“Store” here, meaning data store) has to need to know this information. If the "store" is outsourcing authorization to an AS, then indeed the AS could handle all of that.

Consent receipt work with an UMA flavor seems to be coming from Mark L, so stay tuned for that. Nancy will hopefully share use case for transaction grain that we can consider next. And it’s “on us” to work through some XYZ flows that meet UMA use cases (or show why it doesn’t meet UMA use cases yet).

Happy holidays to everyone and see you in 2020!
Attendees

As of 16 Jul 2019, quorum is 5 of 9. (Domenico, Peter, Sal, Thomas, Andi, Maciej, Eve, Mike, Cigdem)

1. Sal
2. Thomas
3. Eve
4. Cigdem

Non-voting participants:

- Adrian
- George
- Nancy
- Scott
- Colin