UMA telecon 2016-06-02

UMA telecon 2016-06-02

Date and Time

- Thu Jun 2, 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 - 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

Agenda

- Roll call
- Approve minutes of UMA telecon 2016-05-26
- MPD
  - Review sequence diagram and focus on the last bit, going more slowly through the flows this time
- Any last-minute CIS plans/news
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2016-05-26: APPROVED.

MPD

Discussion about the arrow "request token with permission ticket" and asking for scopes: The RS would/might still have registered a permission with scopes that it judged to be necessary, so the RS and the client would both have an "opinion" about what the extent of access should be. There are two inputs here into what the ultimate granted access should be. Justin suggests it should be completely deterministic how the five relevant sets are combined:

1. The universe of scopes the RS has registered for the resource set
2. The scopes the client has registered for at the AS (if it has done this at all)
3. What the RO has attached to the policy for the resource set
4. What the RS requests for at the permission endpoint (in order to get a ticket)
5. The scopes the client requests at the token endpoint

OAuth's ability for a client to ask for multiple scopes up front makes it less chatty than something that uses a strict least-privilege approach. His early trials with UMA showed that people generally gave out more privileges than that anyway. If TTL strategies and RO (and RS) preferences would prefer to see bundles of scopes handed out anyway, and if some clients can only handle some types of scopes, then does it especially make sense to have the client indicate what scopes it can handle? Justin's ultimate rationale for having clients request the scopes they want is that they are software programmed to use an API, and so they are the proper entity to request what they want.

Can we do away with the permission ticket and simply use the bearer token response? Apparently not, because a permission ticket still is needed to preserve UMA loose coupling and RO context in the doing. However, giving the RS a decision/judgment call to make about the client's extent of access is actually a hard problem, and seemingly not worth it. Given that the design of an API, and particularly the resource set vs. scopes dividing line, is up to the discretion of a designer (that is, it's not a clean object vs. verb philosophical line), letting the client ask for what it wants could be philosophically cleanest. An asynchronous grant flow has interesting benefits to the RO in terms of letting them be free to "edit/uncheck scopes free from the collusion of the RS and client, vs. synchronous grant flows, so there's less concern over a client just "getting its way".

Justin's set math implementation can be viewed here. (The license is Apache2.)

We think the notion of scopes as "registerable" by clients in the OAuth world is directly usable in our new concept of UMA set math. We just need to work out a flow chart of how a client's registered scopes interact, in a specific case, with policies. This is our next step, and then to turn it into spec text.

So step #4 could be entirely uninteresting and deterministic, say, identifying the resource set ID (or possibly multiple resource set IDs? that would be a judgment call).

"Scope design" as a discipline becomes a new thing now, as the RO has a new interactive experience with it, and as RS's convey their semantic intent to an AS at a separate organization (through RSR) for display. OAuth previously has not had this. Even standardized APIs with standardized OAuth scopes haven't had this.

Swimlane edits needed:

- The "request token with permission ticket" arrow should mention the issue number regarding "client should be able to request scopes" (165)

Attendees
As of 15 Apr 2016, quorum is 7 of 12. (François, Domenico, Kathleen, Sal, Nagesh, Thomas, Andi, Robert, Maciej, Eve, Mike, Sarah)

1. Domenico
2. Kathleen
3. Sal
4. Maciej
5. Eve
6. Robert
7. Mike
8. Sarah

Non-voting participants:

- Justin
- Colin
- Adrian
- James
- John W
- Arlene
- Ishan
- Jin
- George