UMA telecon 2016-06-16

UMA telecon 2016-06-16

Date and Time

- Thu Jun 16, 9-10am PT
- Voice: Skype: +9905100000481 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

- (Eve needs to leave a bit early)
- Roll call
- Approve minutes of UMA telecon 2016-06-02
- MPD: Still working through the sequence diagram
  - Client awareness of scopes: replay/conclude discussion at CIS breakfast BOF and on the list; any negative impacts in the dev/business owner relationship?
  - Get-a-token loops
  - Next steps on spec text
- AOB

Minutes

Roll call

Quorum was not reached.

Ishan will take notes after Eve drops.

Approve minutes

Approve minutes of UMA telecon 2016-06-02: Deferred.

MPD

We're looking at the set of scopes involved in step #4 from last meeting.

Note that a "client-to-AS-first" flow is not part of the MPD change proposals, so let's not discuss any of that now.

Take the scenario that the client attempts access with API call "foo", which could represent usage of scopes A, B, C, D, and E. Think of the example of OIDC, where accessing an email address potentially corresponds to the specific claim, "openid", "email", "address", and "profile". (Imagine that OIDC is UMA-protected in this instance.) Another example could be a photo service that allows viewing, printing, drawing a mustache, etc.

Do we want to mandate that the RS register a permission that is totally deterministic in terms of how many scopes it registers for the relevant resource set? Justin prefers that the spec give guidance to the RS to register the set of scopes that appear to correspond to the actual client access attempt.

Suggested wording: "It is RECOMMENDED that the RS register a set of scopes with the permission ticket that would allow the client's request to succeed." This is close to our current wording, except that it's not a MUST, and would allow less scope than would suffice.

What would the various rationales be for the RS registering more, less, or exactly the same as what the client attempted? We can't prescribe scope design, nor the relationship between the RS and client. Since we're planning to make it possible for the client to request more scopes, it should be possible for the RS to register fewer scopes.

Eve posed a couple of questions before having to drop:

Are we injecting into UMA something that's been seen as a detriment in plain OAuth? It's been seen as a business benefit that UMA up-levels to the business owner the semantics of scopes. Do our permission registration and RSR processes help with this?

Also, we have an open issue around registering multiple resource sets. How might we accommodate that? Can we just take it up later?

Ishan's notes (thank you!):

Regarding client unawareness of scopes: In Siteminder, clients were not aware of scopes, enterprise use cases...and continue that pattern. UMA’s proposed change does not preclude clients from being unaware of scopes Mike is interested down the road in how this will allow the development of smarter clients and authorization servers. We are adding back OAuth-like flows around scope that make it easier for development of resource servers /APIs. For enterprise use cases, an UMA gateway may be easier to retrofit on top of existing APIs minimizing development.

Regarding the open issue on registering multiple resource sets: What is the combination of scopes/format for each resource set to determine the scope math? We need to specify a way for allow multiple JSON objects at registration, to allow for backwards compatibility.

A request for discussing the MPD proposal for the next meeting:
• How does the client get the token? (RPT endpoint -> token endpoint)
• Client can specify the set of scopes, and determine scope set math
• Splitting the claims presentation options, non interactive; need to involve the RQP that tells the client to send them to an endpoint at the AS
• Ticket rotation - handle to the next part of the transaction; one time use
• Minor proposed syntax changes

In the next meeting, walk through the MPD sequence diagram to compare/contrast the current UMA flow with the proposed one to eliminate future confusion. (Justin will not be available next week, and will join the call the following week)

Attendees

As of 12 Jun 2016, quorum is 7 of 13. (François, Domenico, Kathleen, Sal, Nagesh, Thomas, Andi, Robert, Agus, Maciej, Eve, Mike, Sarah)

1. Domenico
2. Kathleen
3. Sal
4. Eve
5. Mike
6. Sarah

Non-voting participants:

• Justin
• Ishan
• George
• Adrian
• James