UMA telecon 2016-08-04

UMA telecon 2016-08-04

Date and Time

- Thursdays, 9-10am PT
  - Skype: +9905100000481 / international lines / web calling interface / code 1782540
  - Screen sharing: http://join.me/findthomas - NOTE: do not use the join.me dial-in line
  - UMA calendar: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Approve minutes of UMA telecon 2016-06-30, 2016-07-07, 2016-07-14
- Logistics items
  - Telecon interruptions
  - I-D expirations
- For reference: MPD sequence diagram and generic low-level sequence diagram
- Client awareness of scopes and set math
- How to give resource set ID context to standardized resource set and scope semantics profile idea?
- AOB

Minutes

Roll call

Quorum not reached. Critical mass for rough consensus reached.

Approve minutes

Approve minutes of UMA telecon 2016-06-30, 2016-07-07, 2016-07-14: tbs

Logistics

- Note: No WG calls on August 11 and August 25. (Also no legal subgroup calls on August 12 and August 26.)
- Do we want to refresh our "pointer Internet-Drafts" (core and RSR), wait till we have new finished versions, or never update them again?

If we have no opinion on the IETF I-D question, we'll take no action at least until we publish final versions of our next specs.

Spec text update

Eve shared status on our work against our roadmap. We are substantially through the items, with the devil being in the detail (actual spec text). What's a reasonable timeframe for completion of said roadmap? Stability of specs with chance to implement and test by end of year, with ratification (membership voting) plans after that? Sarah thinks so. No other opinions expressed. Eve's thinking on the balance to be achieved: There's keen interest in wide ecosystem use cases, but pressure to get big changes right.

Client awareness of scopes and set math

See 2016-06-02 and 2016-06-16 notes.

In the latter set of notes, there's a discussion about how clients are free to request more scopes and RS's are free to register fewer than what the client requested. George believes that the reason to allow the client to request scopes at all is to reduce chattiness (in the case that the client is smart enough to know what it wants and can handle). In other words, if the client knows it wants scopes A, B, and C, it can request all of them up front. And so we need to preserve the scope-unawareness flow when the client isn't that smart. Adrian adds that data minimization suggests that the client should ask for as few scopes that it needs to do its job; we should probably be adding some non-normative spec text in the security and privacy considerations about this, inspired by the OAuth specs.

The RS, as an API publisher, will need to account for scopes that are common to the kinds of resource sets that they (the scopes) are on. The kinds/types /classes vs. instances (with rsid's) distinction is reminiscent of the solution we thought we came up with last week for standardizing FHIR/HEART resource set and scope semantics (or any standard/public API that is implemented by multiple API publishers). So, in terms of the list in the 06-02 list for set math purposes, there's a #0 on the list that is the "API documentation", likely in Swagger or Swagger++, which says "here are the scopes for this API and how to use them" and, if there are resource set types, "here are the resource set types with which the scopes are associated". That's the "class" level, whereas RSR is the "instance" (RO context) level. Clients have to implement what the API publisher says is available to implement. Standard APIs are only different from proprietary APIs in that the API documentation is standardized (and, perhaps, will include our "trick" for protection API extensibility profile).

Is it recommended for security to register for the scopes they want? Is it hairy compared to other scopes because some scopes might be specific to only some resource sets? Actually, as long as the scopes are distinguished by URI in a per-resource set way, the friendly name could still be (say) "Read" and they'd be unique per resource set. This is up to the RS to manage. However, the actual registration process may look a bit different from today's OAuth scope registration process.

Let's discuss client registration for scopes more next time.
Spec text instructions (issue 165):

* Now that the client can ask for scopes, add security and privacy considerations as mentioned above
* Say something about how RS's need to include API documentation about scopes (as step 0), and how that ties to step 1

**Client-to-AS-first flow**

Though we have put this aside for now, it's still on our 2016 roadmap docket. There is interest in it, and also a question about implications for HEART.

**Resource set ID context for standardized semantics profile idea**

See these notes.

We dug into this a tiny bit, but only insofar as it pushed the client awareness of scopes topic forward.

**Attendees**

As of 1 Aug 2016, quorum is 6 of 11. (Domenico, Sal, Nagesh, Andi, Robert, Paul, Maciej, Eve, Jeffrey, Mike, Sarah)

1. Domenico
2. Maciej
3. Eve
4. Sarah

Non-voting participants:

* Kathleen
* Ishan
* Robert
* François
* Adrian
* Scott F
* James
* George

Regrets:

* Justin
* Sal
* John W
* Mike
* Jeffrey