UMA telecon 2017-03-09

UMA telecon 2017-03-09

Date and Time

- Thursdays, final special meeting time: 8:30-10am PT
- Screenshare AND dial-in: http://join.me/findthomas
- UMA calendar: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Approve minutes of UMA telecon 2017-03-02
- Logistics:
  - This is our last 90-minute meeting
  - We plan to vote on our specs as WG drafts (simple majority required) and let them percolate for four weeks as "last call" drafts while we invite people to join the group to finalize them with us and implement them
- UMA V2.0 work:
  - 2016 roadmap / GitHub issues for V2.0 (all issues to be kept here for the duration!) / dynamic swimlane
  - Core is up to 19 (updated) and RReg is up to 06 (updated)
  - #286 is open and worth discussing (OpenAPI)
  - #252 is open and worth discussing briefly regarding how to handle editorially and succession-wise (pointing to the V1 security extension spec – ticket rotation)
  - #289 (potentially moving a UIG XSRF security warning to Core if necessary)
  - #270 (URIs as arrays/wildcards) is open but hasn’t gotten a lot of support – needs some really good explanation or it will die
  - Shall we simply close #277? (not doing CRUD reg in bulk)
  - I proposed in email that we close #31 with no action – it sort of wants an “extension” tag, but really it is just open for anyone to make extensions if they need them
  - #273 is open (did the shallow s/user/resource owner/ fix)
  - Other issues are tagged with “process” or “editorial” and can or must be done later

- WG draft vote if we’re ready
- Discuss review period logistics
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2017-03-02: Andi moves to approve the minutes. APPROVED.

Logistics

- This is our last 90-minute meeting
- We plan to vote on our specs as WG drafts (simple majority required) and let them percolate for four weeks as "last call" drafts while we invite people to join the group to finalize them with us and implement them

UMA V2.0 work

- #286 is open and worth discussing (OpenAPI)

The aim of Mike’s proposal is to enable those documenting an API to capture, at the same time as they’re thinking about describing the API for the audience of client devs, to capture related information. It consolidates what would have been two tasks into one. On the other hand, this rationale only applies if you’re using OAI, and it also requires the AS to fetch a bunch of information that’s not relevant to it, and deal with a lot of error conditions ditto.

And what if it’s not a REST API, but a file/folder paradigm with static resources or whatever?

Alternatively, what if the RS just used the OAI format as a common format somehow? Look at how long it took us to decide to add the “description” field last week. But then why not SCIM?? (Said in bitter jest...)

Positive registration is probably the bigger burden than the actual format being registered. We’ve now made it a little more implicit how a tightly coupled AS-RS relationship would be done (by doing away with the huge “extensibility profiles” infrastructure), but it’s still possible to make more efficient through profiling a “different protocol than HTTP” for doing resource registration.

Swagger/OAI is used a lot for API documentation now, and there are a lot of tools for it, but we also have a rationale for all the pieces of the resource description document and scope description document now. It would perhaps be more attractive to extend OAI descriptors property to add scopes to them – but even then, the "customer" of that information is the client, not the AS.

Close this issue with no action but put on the extension label for future experimentation.
• #252 is open and worth discussing briefly regarding how to handle editorially and succession-wise (pointing to the V1 security extension spec – ticket rotation)

V2.0 is not susceptible to the attack mitigated by the extension. Eve recommends adding a sentence to Core sec consid. OK.

• #289 (potentially moving a UIG XSRF security warning to Core if necessary)

Let's delete the UIG section and add nothing to Core.

• #270 (URIs as arrays/wildcards) is open but hasn't gotten a lot of support – needs some really good explanation or it will die

Now that we separated out issue #277 from this one:

A wildcard character is just another character, so if a singleton URI contains wildcards that are known to have special properties only to the RS, great; we're not crazy about giving the AS special wildcard-processing capabilities, though. (This is sub-issue no. 2.) How much are we getting into the game of allowing the AS to use this to be "something else", such as a discovery service? Eve's idea was that the RS could put in both the URL for – say "rev 19" of Core and also the soft link URL for the latest rev of Core. The concern is that it could be abused by the RS. Justin makes the argument that "uri" being meant for more than just display (e.g., true resource discovery), and reaching outside the UMA entity ecosystem, it has greater security and privacy consequences than any of the human-displayable stuff. We have consensus on removing the uri field and marking this issue with the extension label.

• Regarding having removed claim_token_profiles_supported:

In RReg Sec 2.4, remove "_uri" from all the URI examples. Also, have two examples: One without uma_profiles_supported, and one with (using ...IDToken).

• Shall we simply close #277? (not doing CRUD rreg in bulk)

It's closed, with no action; it's only individual RReg for now. We'll see what happens in the next four weeks.

• I proposed in email that we close #31 with no action – it sort of wants an "extension" tag, but really it is just open for anyone to make extensions if they need them

Eve proposes Option 1 from her email (close with no action). James groks. Let's close, put the extension label on it, and put the email proposal into the issue.

• #273 is open (did the shallow s/user/resource owner/ fix)

Eve did the minor editorial change. Now we just need to go out there and see how possible it is to apply RReg to OAuth and OIDC.

Let's add a section to the UIG about this (should have been done a while ago).

WG draft vote if we're ready

A good motion on this would be something like:

“Approve revisions of the UMA V2.0 Core and Resource Registration specification drafts as Work Group Draft Specifications for publication and review, as amended by the specification revision notes in UMA telecon 2017-03-09 and any non-normative copyedits proposed by Sunday, March 12.”

MOTION: Andi moves and Mike seconds. APPROVED by unanimous consent.

These will be Core rev 20 and RReg rev 07.

Discuss review period logistics

We have a couple of open issues that have a new “process” label. Eve plans to work on the Release Notes proper, which have a paradigm of explaining things “per software entity” and in terms of “what changed since the last release”. But we also have an opportunity to do lots of other stuff, like describing how an OAuth client dev can understand what an UMA-friendly client’s needs are.

AI: Mike: Write up a draft of what it looks like to develop an UMA-friendly client from an OAuth client dev’s perspective, and then get Justin's feedback.

AI: All: Please review the new section on set math in the UIG.

Attendees

As of 7 Mar 2017, quorum is 4 of 7. (Domenico, Sal, Andi, Maciej, Eve, Mike, Cigdem)

1. Domenico
2. Andi
3. Eve
4. Mike
5. Cigdem

Non-voting participants:

• Justin
• James
• John W
• Jin

Regrets:
• Sarah
• George