UMA telecon 2017-02-09

Date and Time

- Thursdays, special meeting times through Feb 9: 8:30-10am PT
  - Screenshare AND dial-in: [http://join.me/findthomas](http://join.me/findthomas) (NEW)
  - UMA calendar: [http://kantarainitiative.org/confluence/display/uma/Calendar](http://kantarainitiative.org/confluence/display/uma/Calendar)

Agenda

- Roll call
- Approve minutes of UMA telecon 2017-01-26 and 2017-02-02
- Logistics:
  - No meeting Feb 16 because of RSAC
  - This week is our last scheduled 90-minute meeting; plans for Feb 23, Mar 2? Interest in ad hoc work Feb 21/22?
  - At RSAC, Kantara member/IDESG cocktail party on Thursday? No-host drinks somewhere?
- UMA V2.0 work
  - [2016 roadmap / GitHub issues for V2.0](https://github.com/UMA/v20/issues) (all issues to be kept here for the duration!) / dynamic swimlane
  - Core is up to 14 (updated) and RReg is up to 05 (no change)
  - 266: Set math / resource and scope ecosystem AND RReg issues (269, 270, 271, 272, 273, 276, 277):
    - Please see recent ad hoc meeting's notes thread and hopefully forthcoming email from George
  - 260: Cascading authorization servers
    - Discuss Mohammed's input
    - Decide next steps
- Claim token profiling: 263: Claim token profiling / 119: Create an IANA registry for URIs that stand for claim token formats
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2017-01-26 and 2017-02-02: APPROVED.

Logistics

- No meeting Feb 16 because of RSAC
- This week is our last scheduled 90-minute meeting; plans for Feb 23, Mar 2? Interest in ad hoc work Feb 21/22?
- At RSAC, Kantara member/IDESG cocktail party on Thursday? No-host drinks somewhere?

AI: Eve: Schedule 90-minute meetings out through Mar 2, and propose an ad hoc on Tuesday Feb 21, hopefully at the same bat time.

UMAnitarian no-host drinks get-together at Salt House, 545 Mission St, Thursday evening, 6pm+! Drop Eve a line if you think you can make it, or dm or email her that day/evening.

UMA V2.0 work

Example doc for permission requests: We worked through this doc and had lots of conclusions. See that doc for spec instructions.

Previous RPT:

- Is this a super token? All rsid:scope tuples are continually added (and expired)
- Is this a single token per RqP at the client? Does it also need to be bound to the RS?
- Are super-token’s a good idea? Do we want to promote them?
- Motivation?
  - reduce coding complexity for the client?
  - reduce user experience complexity for the user?
  - i.e. the user doesn’t have to keep providing the same claims over and over
- Can we get the same behavior (improved user experience) for the user by using the PCT?
- If we do want to keep the ability to add a previous RPT to a request, what is the effect on authorization assessment?
- Does this effect change in the presence of a PCT on the request?

James has weighed in in favor of a single RPT because of the burden, otherwise, on multi-user clients to manage potentially tens of millions of tokens without knowing which one works for which resource. A client can’t provide multiple tokens to a resource to see which one works.
If you want stateless tokens, you need to keep state in the token. It could be made efficient in various ways, but does it provide an incentive to go stateful instead? Even if the client provides a previous RPT, the AS still has the choice to hand the client a very session-specific token in response. There are various TTL strategies possible. What are the right strategies to simplify client developer logic? We keep dancing around informing the client more precisely what's in the token or what went on between the AS and RS. So far we haven't added anything to the UMA flow to do it. Another way to do it, potentially, is say: Client, if you have a way to introspect the token, go ahead. Is that tenable?

(Justin's rant on OIDC's ID "tokens" not being tokens but rather assertions is somewhere in [here](#).)

Revealing raw permission ticket contents doesn't seem smart because the client has no context to understand requested permissions if they go outside the access attempt. Could informing the client about actually granted scopes be a middle ground? If you pass in a previous RPT and the token was upgraded, you get an extra Boolean property in the response saying "yes, you were upgraded". If the property is empty, then the client knows it got a new one.

In UMA1, the previous RPT had a role that sort of covered both client coding complexity (managing fewer tokens) and RqP experience complexity. In UMA2, now that clients can request scopes and AATs have been supplanted by PCTs, the previous RPT is meant for the former purpose and the PCT is meant for the latter.

So how should authorization assessment be affected by both? **Spec instructions:**

1. The PCT, if present, is part of the claims and other information in evidence, as appropriate, in #2 (noting the temporal nature of this information and the opportunity to update it through claims collection). We already have language for this but **we probably need to add a warning about the possibility of out-of-date info getting updated.**
2. After the assessment, if the result is to issue an RPT, and a previous RPT was on the request, and the AS decides to upgrade it, then add/merge the previous RPT with the `CandidateGrantedScopes`.

Add guidance around the process of the AS deciding to issue upgraded tokens vs. not (the AS should pick one model vs. another), and the client having expectations of which one.

### Attendees

As of 19 Jan 2017 (post-meeting), quorum is 5 of 8. (Domenico, Sal, Andi, Maciej, Eve, Mike, Cigdem, Sarah)

1. Domenico
2. Sal
3. Maciej
4. Eve
5. Mike
6. Cigdem
7. Sarah

Non-voting participants:

- George
- Justin
- Thomas
- Mohammad

Regrets:

- James