UMA telecon 2016-10-06

Date and Time

- Thursdays, 9-10am PT
- Skype: +9905100000481 / US +1-805-309-2350 / international lines / web calling interface / code 1782540
- Screen sharing: [http://join.me/findthomas](http://join.me/findthomas) - NOTE: do not use the join.me dial-in line
- UMA calendar: [http://kantarainitiative.org/confluence/display/uma/Calendar](http://kantarainitiative.org/confluence/display/uma/Calendar)

Agenda

- Roll call
- Approve minutes of UMA telecon 2016-09-22
- IIW
  - UMA 101 session leader
  - Video premier(s)
- Work on UMA.next issues
  - Core is up to 03
  - RSR is up to 00
  - See email for list and description of the latest changes and discussion agenda
- Review Domenico's diagrams
- FB page care and feeding ideas
- AOB

Minutes

Roll call

Quorum was reached.

Logistics

The call for the week after next will be held Fri Oct 21 instead of Thu Oct 20, just after the Legal subgroup call.

Next week we'll have an 04 within which we should have a permission ticket flow for the RS wherein which there will be a framework for the client to theoretically be able to ask for scopes for multiple resource sets by the time it gets to the AS.

Approve minutes

Approve minutes of UMA telecon 2016-09-22: APPROVED by acclamation.

IIW

The UMA video is up! Is it better to consolidate all links to one channel, or put the video on multiple channels? Inconclusive. Do we want to start a Vimeo channel as well? Let’s not.

Phil has given us an opportunity to do a pre-planned UMA 101 session at IIW. George is giving the session. Others here can provide feedback.

NOTE: Please give an “IP policy benediction” at the start of any UMA content-related sessions. Here's the [IPR policy](http://kantarainitiative.org/confluence/display/uma/Joining+Form) joining form; you could print them out or distribute the links for people's convenience.

Work on UMA.next issues

We need to look at the security considerations of the PCT. It's a bit like a refresh token, in that it's got extra power over an access token and so must be wielded carefully. Could hijacking and replaying a PCT be bad? It's bound to the client credentials like a refresh token would be, but the point is to go get an access token without having to present (or have the RqP get pumped through interactions for) a whole bunch of claims all over again.

In the terminology definition, do we want to go into more detail about the intended usage, or is the existing (fairly large already) detail about the “claim components” of the PCT okay? Sec 1.3.2 has more about the intended usage, similar to the previous AAT description.

Regarding the “[ISSUE: what about at the same or a different resource server?]”, the answer is that it’s immaterial wrt the resource server, just as it was for the AAT.

Regarding issue #251, the telecon notes were not accurate. Unguessable and unforgeable by an attacker is the only requirement; securely random would be one way to meet the requirement. Mike suggests pointing to OAuth Sec 10.10 – or maybe we could leverage its wording – to get the right effect. The specific wording we like is “The authorization server MUST prevent attackers from guessing access tokens, authorization codes, refresh tokens, resource owner passwords, and client credentials.” Say this in the security considerations, or for each token/ticket/thingie? See below.

Spec instructions:

- Add some security considerations around PCTs, including why the client has to make a "best effort"
• Remove the [ISSUE] above and fill in the language
• Regarding "same requesting party as previously", change to "same as the previous requesting party".
• Say "unguessable" as the definition for each token/ticket and then require the one-paragraph version of unguessability once in the security considerations.

Next time, we’ll look at Domenico's diagrams for UMA grant flows.

Next time, for set math discussions:

What does the RS have to do at permission ticket registration time? What is the RS’s motivation for registering anything at all? Its only context is what access the client attempted.

Can the client request scopes from the RS (in addition to just attempting access)? No.

How does the client request scopes from the AS, and what can it ask for (e.g., what interaction does it have if it wants multiple resource sets)?

The question we need to ask at each messaging stage to get the semantics for each actor correct, and crystal-clear, is: What is the context, and "what’s my motivation?" 😊

Attendees

As of 3 Oct 2016, quorum is 6 of 11. (Domenico, Sal, Nagesh, Andi, Robert, Maciej, Eve, Jeffrey, Mike, Cigdem, Sarah)

1. Domenico
2. Andi
3. Robert
4. Maciej
5. Eve
6. Mike
7. Sarah

Non-voting participants:
• Andrew
• François
• Kathleen
• James
• Justin
• Scott F
• Jin
• John W
• Adrian
• George