**UMA telecon 2016-05-26**

**UMA telecon 2016-05-26**

**Date and Time**
- Thu May 26, 9-10am PT
  - Voice: Skype: +99051000000481 or US +1-805-309-2350 *(international dial-in lines)*, room code 178-2540#
  - Screen sharing: [http://join.me/findthomas](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](http://kantarainitiative.org/confluence/display/uma/Calendar)

**Agenda**
- Roll call
- Approve minutes of UMA telecons 2016-04-14 and 2016-05-19
- MPD
  - Review new sequence diagram
  - Discuss affordances and implications
- News from Digital Contracts event
- AOB

**Minutes**

**Roll call**

Quorum was reached.

**Approve minutes**

Approve minutes of UMA telecons 2016-04-14 and 2016-05-19: So approved.

**Review of MPD**

We're looking at the swimlane.

The first batch of changes in MPD is around discovery. These are backwards-incompatible, but not particularly invasive. Justin and Sarah note that the discovery document *(currently known as AS configuration data)* is relevant to both the RS and the client, and thus it isn't specific to what UMA calls Phase 1. The alignment done here is to OIDC; OAuth is undergoing its own alignment to OIDC as well. Do we want to align with the other specs in terms of terminology: discovery document vs. configuration data? We have consensus to do this.

Justin suggests an editorial comment in the spec commenting that it's a good idea to use an interactive grant flow when, as is typically the case, an individual end-user is a resource owner. This gives the developer the clearest guidance as to which grant to choose. This would be paired with stronger normative text that identifies the RS as an OAuth client. The editorial comment could then also briefly mention the converse case of an organization *("legal person")* using the client credentials grant *(and point off to the UIG if warranted)*.

If there's a discovery document at .well-known, is it ever a good idea to rely on discovery some other way? Should we make discovery by that means optional? We're covered on this by saying "as needed" already.

The UMA client now needs client credentials, not because it needs an AAT *(one of the reasons before)*, but because it would need it for the exact role that an OAuth client would normally need it – and now, Bob the RqP would be the end-user who is using that client at the AS *(specifically, the token endpoint* that the AS already has, and has had all this time, along with a newly conceived claims endpoint).

The loop in the swimlane involves trading a ticket for a token – repeatedly, until success. This is very analogous to an authorization code flow. Per OAuth, OIDC, and our recent security work, tickets are now one-time-use only.

Note that the "claims" process treats what was previously a separate flow – step-up authentication – as subsumed into the same flow.

It's possible for the client to send claims directly to the token endpoint directly. One question to discuss on the next call: Is there an in-band mechanism by which the RqP can authorize that flow?

The claims endpoint can be treated as a "dispatch" endpoint.

**Swimlane tasks:**
- We should take out the Phase 1 label from the swimlane.

**Spec tasks:**
- Align the terminology and syntax of the discovery document format.
- Insert the editorial comment about which grants are appropriate and normative text about the RS being an OAuth client. *(Also consider a figure about the protection API being protected by OAuth.)*
- Implement the change for issue #155.
- Where the protocol flow currently casually uses declarative text, switch to using normative RFC 2119 text.
Attendees
As of 15 Apr 2016, quorum is 7 of 12. (François, Domenico, Kathleen, Sal, Nagesh, Thomas, Andi, Robert, Maciej, Eve, Mike, Sarah)

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

Non-voting participants:

- Justin
- Adrian
- Colin
- Jin
- John
- James

Regrets:

- Maciej
- Sal?