# UMA telecon 2018-01-04

## UMA telecon 2018-01-04

### Date and Time

- **Thursdays 9am PT**
  - Screenshare and dial-in: https://global.gotomeeting.com/join/857787301
  - See UMA calendar for additional details: http://kantarainitiative.org/confluence/display/uma/Calendar

### Agenda

- Roll call
- Identiverse
  - Interest in an UMA2 workshop
  - The Identiverse CfP is still open until **Jan 12**!
- Approve minutes of UMA telecon 2017-12-21
- Discuss latest on security attack/trust attack analysis
  - Possible to confirm and close specs for Recommendations publication?
- Schedule Consent Receipt analysis
  - With Andrew, Andi, Robert, Tim...
- 2018 charter and roadmap
  - Joint consent receipt work?
  - Working on issues with the "extension" label?
  - Legal?
  - What else?
- UMA2 logo
- AOB

### Minutes

#### Roll call

Quorum was reached.

#### Identiverse

- Interest in an UMA2 workshop
- The Identiverse CfP is still open until **Jan 12**!

Identiverse is June in Boston. Who's interested in participating in an UMA2 workshop? Justin (discussed how MPD is a small delta off final UMA2), tentatively Eve (showing demos is good), Mike (could show Gluu gateway, to be released).

**AI:** Eve: Chat with Thomas about MITREid Connect.

#### Approve minutes

Approve minutes of UMA telecon 2017-12-21: Andi moves to approve: APPROVED.

#### Discuss latest on security attack/trust attack analysis

- Possible to confirm and close specs for Recommendations publication?

Eve asked Justin in email, and asserted:

*"Is the claims_redirect_uri parameter still a vector for the attack in the case where the client sends this value when redirecting the RqP? It's sending the RqP to a known-good AS claims interaction endpoint no matter what (or a known-bad AS entirely, but that's sort of a different "trust attack" that started with the discovery document, as we've been saying -- you can't fix this with OAuth-style mitigations). If I'm stating this accurately, there's simply nothing to fix and no mitigations to mention regarding claims_redirect_uri. The group is of the opinion that we've said enough in the specs about mitigating "trust attack" thingies. (We could say/muse more in a separate doc eventually.)"*

"OAuth-style mitigations" means the mix-up attack mitigations. The problem with the assertion is that the attacker can sit on the front channel. If we had mandated the state parameter (as Justin had preferred!), then it might have provided a mitigation (or nearly full mitigation?) – George thinks that if the state carried the right content, it might work. A nonce wouldn't be enough. Justin notes that Microsoft's OAuth implementation puts a lot of content into the state value (so that it becomes stateless – rimshot). Carrying a lot of application state enables matching it up with a callback.

Justin suggests a non-normative security consideration suggesting that the claims_redirect_uri parameter being susceptible to the same mitigations as the redirect_uri parameter, as in this doc/section. Would adding this to the spec require any new review processes? Andrew's take is that it wouldn't have to, as long as it has no impact on conformity assessment and interop testing (in other words, if it's not connected to testable assertions in the specs). If we don't state it as "MUST", then it's not a MUST – tautologically! Nat's comment was based on wanting it to be a MUST. OAuth's security topics draft doesn't have it as a MUST, but that is an add-on document.

All three of the OAuth-style mitigations are not great. The first two bullets have syntactic implications (the implication is that they would apply to the AS's response in Grant Sec 3.3.3) and yet any attacker sitting in the middle of the front channel could do worse damage to the information included. The third bullet asks the client to take not only the actions specified but a number of other coordinating and tracking actions.

Andi suggests that, since the security topics document is an IETF WG document that is not at last call, it's not a good idea for us to base serious changes on it. Justin likes it. George too. A man in the browser can manipulate and compromise pretty much everything, so AS-specific redirects doesn't sound like it solves much of anything. And UMA is already much less susceptible to discovery attacks because the OAuth situation is based on a user to enter data. In our case, the RS tells the client where to go next. Assume no mal-intent, the next steps are clean. Justin even recommends we could say that *not* putting the claims interaction endpoint in the discovery document is more secure because then the client discovers it directly from the token endpoint.

We could put a line in the UIG about all this instead of the spec. Justin notes that 6749 doesn't even mention 6819. We don't have to mention the security topics doc in the spec at this time.

Consensus: We all agree that this is simply **best practice** at the current time and thus needs to go in the UIG and not the spec.

Updated mix-up attack analysis swimlane (non-normative) based on the group conversation – comments welcome.

### Schedule Consent Receipt analysis

- With Andrew, Andi, Robert, Tim...

**AI:** Eve: Do Consent Receipt analysis scheduling offline.

### 2018 charter and roadmap

- Joint consent receipt work?
- Working on issues with the "extension" label?
- Legal?
- What else?

Deferred.

### UMA2 logo

Eve briefly showed the current logo options being considered, and also the JSON logo, which Justin had observed looks somewhat similar due to the ring shading. She's working with Colin, will reach out to Maciej, and is gathering opinions and whether they have changed since the first couple of conversations, but is not doing a strict group vote.

## Attendees

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

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

Non-voting participants:

- Justin
- George
- Bjorn