UMA telecon 2010-05-13

UMA telecon 2010-05-13

- **Date and Time**
- **Agenda**
- **Attendees**
- **Minutes**
  - New AI summary
  - Roll call
  - Nominations for vice-chair and spec editor are open
  - Approve minutes of 2010-04-22 and 2010-04-29 meetings
  - Action item review
  - Set up UMA chat room?
  - EIC workshop report
  - Review IIW-week plans
  - Any SMART project showstoppers
  - Christian's issues sent to the list
  - Claims 2.0
  - Report from legal subteam on progress and next steps
- **Next Meeting:** UMA telecon 2010-05-27

**Date and Time**

- **Day:** Thursday, 13 May 2010
- **Time:** 9:00am-10:30am PST | 12:00-1:30pm EST | 16:00-17:30 UTC
- **Dial-In:**
  - Skype: +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)

**Agenda**

- Administrative
  - **Roll call**
  - Note: No telecon May 20 due to IIW/OAuth meeting
  - Nominations for vice-chair and spec editor are open
  - Approve minutes of 2010-04-22 and 2010-04-29 meetings
  - Action item review
  - Set up UMA chat room?
- EIC workshop report
  - Slides
  - Christian's Python prototype
  - Christian's comments
- Review IIW-week plans
- Discuss protocol issues
  - Any SMART project showstoppers
  - Christian's issues sent to the list
  - UX and interop for Step 2
  - Claims 2.0
  - Any others
- Report from legal subteam on progress and next steps
- AOB

**Attendees**

As of 13 May 2010 (pre-meeting), quorum is 6 of 10. (Brian Armstrong became non-voting, and Christian became voting, just before the meeting.)

1. Adams, Trent
2. Catalano, Domenico
3. Fletcher, George
4. Machulak, Maciej
5. Maler, Eve
6. Scholz, Christian

Non-voting participants:

- Mark Lizar

Regrets:

- Tom Holodnik
- Thomas Hardjono
- Lukasz Moren
- Paul Bryan

**Minutes**
**New AI summary**

<table>
<thead>
<tr>
<th>Date</th>
<th>Owner</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-05-13-2</td>
<td>Eve</td>
<td>Print the IEEE S&amp;P poster in smaller form for distribution at IIW.</td>
</tr>
<tr>
<td>2010-05-13-3</td>
<td>Christia</td>
<td>Spec out a &quot;requester metadata&quot; flow.</td>
</tr>
</tbody>
</table>

**Roll call**

Quorum achieved.

- Note: No telecon May 20 due to IIW/OAuth meeting

Confirmed. No meeting next week.

**Nominations for vice-chair and spec editor are open**

We’ll leave nominations open until our next telecon (May 27). Please feel free to send nominations to Eve or to the Kantara staff@ alias.

**Approve minutes of 2010-04-22 and 2010-04-29 meetings**

Minutes of 2010-04-22 and 2010-04-29 meetings APPROVED.

**Action item review**

- 2009-12-03-4 Eve Open Add terms-negotiation scenarios to Scenarios document.
- 2010-03-10-2 Maciej Open Do next round of spec editing. We’ll target spec edits to catch up to implementations by the demonstration timeframe. Eve and Maciej will coordinate on this.
- 2010-03-10-6 Joe Open Revise the protected inbox scenario for next week’s call.
- 2010-03-25-1 Paul/TomH Open Send email giving examples of how a resource-oriented scope approach is necessary. Now “overcome by events”.
- 2010-04-08-2 TomH Open Revise the tax scenario for inclusion in the Scenarios document. Let’s consider this closed because he sent email on it.
- 2010-04-29-1 Domenico? Open Revise Claims 2.0 and SAAC specs To be done by May 6. Consider this closed; Domenico will send his proposal to the list.

**Set up UMA chat room?**

Christian has done so! He will send email to the list about this. Trent suggests turning on logging, so that new entrants can get the context.

**EIC workshop report**

- Slides
- Christian's Python prototype
- Christian's comments
- Christian's liveblog

Domenico took some photos and video of the event, which he's preparing for next week (hmm!).

**Review IIW-week plans**

Maciej will be presenting an UMA poster both at IIW and at the IEEE Security and Privacy poster session on the Tuesday night in Oakland. Domenico prepared a (gorgeous) poster in A0 form, which Maciej has printed and will bring with him from the UK. He can display this at IIW too.

Lukasz is attending IIW as well. So are Mark, Eve, TomH, etc. We’ll definitely sign up to host a “discussion session” (in which we should definitely do the SMART demo first, and then see where the discussion goes) of UMA, and we should be prepared to sign up for any demo speed-dating sessions. Should we show the Python prototype at all? We may not want to run it as a demo, but it may be valuable for people who learn best by reading Python.

Both the SMART and Python implementations use a “core” flow, without yet showing (e.g.) dynamic host/AM introduction or claims. So what's different from OAuth? Mainly that the user can craft policies that impact whether the requester can get a token – including requiring the requesting party to send (self-asserted for now) claims! So this can be a major leap forward in user-driven policy, even without some of the fancier features.

The major differences between OAuth2 and UMA are:

- Terminology: Resource Owner => Authorizing User
- Terminology: Resource server => Host
- Terminology: Authorization server => Authorization Manager
- Terminology: Client => Requester
- Protocol/trust: The auth and resource servers meet out of band => Host and AM can meet dynamically (using OAuth or UMA!)
- Protocol/trust: The resource server and client meet out of band => Host and Requester can meet dynamically
- Protocol: Authz is binary: you get a token or you don’t => Authz can depend on requester “claims”
- Conceptual: Authz server issues tokens simply if the user delegated authz => User policy dictates token-issuing
- Protocol: Token validation process is unspecified => Host can ask AM to validate token at runtime
We should avoid putting any UMA sessions on Tuesday mid-late afternoon; we should finish them by Tuesday 2pm. We should avoid signing up for the room that has the terrible acoustics.

**Any SMART project showstoppers**

Maciej feels they don't have any showstoppers right now, because they made some simplifying assumptions. They did find places where they had to invent a solution, and he will let us know what those areas were.

**Christian’s issues sent to the list**

We want to change things up in the spec so that:

- The AM has distinct ways its hostmeta of indicating host- vs. requester-related endpoints
- The host looks up its own endpoints for step 1 in the AM’s hostmeta
- The host tells the requester merely what AM protects this resource
- The requester then looks up its own endpoints for step 2 in the AM’s hostmeta

In the OAuth meeting next week, Christian suggests that we should bring up the question of how the OAuth resource server informs the client how to find the relevant authorization server endpoints. Currently, it conveys the user delegation endpoint in a WWW-Authenticate header, so we’d be diverging from OAuth if we use the solution outlined above. But the OAuth spec has precious little information about this process so far, so maybe it would benefit from a hostmeta-based discovery flow anyway.

George believes that in the general (that is, UMA) case, it’s not always appropriate for the AM to hand the requester a user authorization URL quite yet, since in person-to-person sharing scenarios that endpoint wouldn’t be used. OAuth doesn’t get into such sharing scenarios, so they’re thinking about how to solve things simply. UMA “goes there” and makes things more challenging by “crossing identity providers.”

OAuth in its original three-legged form always has Alice on both ends. OAuth in its slightly newer two-legged form has a client service being issued meaningful credentials ahead of time. In completely dynamic Alice-to-Bob sharing, the actual requester service being used has no meaningful credentials yet.

Christian has proposed that there are certain bedrock facts that need to be known about the requester service in all cases, e.g. for logging. If the requester initially presents to the AM an endpoint at which metadata XRD can be looked up, is this easier than claims for this purpose? and/or is it a good adjunct to claims that are used (optionally) for other more sophisticated purposes?

Another comment we might want to make to OAuth is to recommend an "automated self-registration” flow for autonomous clients, such that the client can be dynamic but its credentials are uniquely identifying (vs. looking up static allocation of credentials as originally proposed by the old OAuth Discovery spec). (This is why, in the old UMA flow based on OAuth V1.0, things were so complicated! We had the host uniquely and persistently meeting the AM outside of any user context, and the requester uniquely and persistently meeting the AM outside out of any host/authz user context.)

So the fact that OAuth V2.0 has no flow that allows there to be no client_id on first approach is something we’re having to work around in UMA. Hey, it should it be called the "anonymous client" flow!

**Claims 2.0**

Domenico will mail out his proposal. The essential/hardest "identity token" thing we have to try and solve is something like this: If GMail signed a claim saying the requesting party is bob@gmail.com, we’re likely to believe that they really authenticated him. But what’s harder is to ensure that the bearer of this claim didn’t mess with/steal it, and it’s really still Bob on the other end. (This is what made SAML assertions so hard for SSO. 😓) Let’s discuss the proposal in email.

**Report from legal subteam on progress and next steps**

There’s another meeting of this subteam on May 31 (note: which is a U.S. holiday). We discussed what practical sorts of things might go wrong in an UMA interaction, such that Alice did something wrong, CopMonkey did something wrong, etc., and someone wants to sue someone else. International (country-crossing) use cases get a lot harder, so we may want to simplify our analysis by assuming a single country within which interactions take place for the moment.

**Next Meeting: UMA telecon 2010-05-27**

- **Day:** Thursday, 27 May 2010
- **Time:** 9:00am-10:30am PST | 12:00-1:30pm EST | 16:00-17:30 UTC (time chart)
- **Dial-In:**
  - Skype: +9900827042954214
  - US: +1-201-783-9022 | Room Code: 295-4214 (other local country numbers available on request)