UMA telecon 2012-01-12

UMA telecon 2012-01-12

Date and Time

- WG telecon on Thursday, 12 Jan 2011, at 9am PT (time chart)
  - Skype: +99051000000481

Agenda

- Roll call
- Approve minutes of 2012-01-05 meeting
- Interop activity
  - Tweet chat idea
- Brief review of non-spec action items
- Work through A/B-priority issues
  - Confirm status of 43, 41, 39, 10, 40 with current state of spec draft; work on 33, 30, 24/14, 12.
- AOB

Attendees

As of 11 Jan 2012, quorum is 8 of 15.

1. Catalano, Domenico
2. D'Agostino, Salvatore
3. Fletcher, George
4. Hardjono, Thomas
5. Klaus, Michael
6. Machulak, Maciej
7. Maler, Eve
8. Miles, Arnie
9. Moren, Lukasz
10. Morrow, Susan

Non-voting participants:

- Cox, Kevin
- Nederkoorn, Cordny

Minutes

New AI summary

<table>
<thead>
<tr>
<th>Time</th>
<th>Approver</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-01-12-1</td>
<td>Eve</td>
<td>Advertise the tweet chat.</td>
</tr>
<tr>
<td>2012-01-12-2</td>
<td>Eve</td>
<td>Migrate remaining &quot;conceptual&quot; issues on the wiki into GitHub.</td>
</tr>
</tbody>
</table>

Roll call

Quorum was reached.

Arnie is joining us for the first time. He is a middleware architect at Georgetown University working with InCommon and the (former "AdmitMe") Common Identity and Trust Collaborative (CommIT) effort. This involves a use case that has high school students moving on to college, and they need to solve for trusted third-party-asserted credentials. Today they concentrate mostly on authentication, but they want to go on to solve for controlling the sharing of credentials.

One participant in CommIT, CommonApp, represents 500 universities. CommIT is part of a strategic partnership between InCommon and the Postsecondary Electronic Standards Council (PESC). Their goal is to simply college applications. A student could use the CommIT app to authorize sharing of data – e.g., log in, authorize, then log out. But perhaps they could also log in to authorize sharing of data that hasn't been created yet ("when I take this test, it's okay to share the results with x, y, and z").

Michael is working in a small company that is working to give control of personal data to that data's owners. They are working on a smartphone app to manage the sharing of contact data. This sounds a little similar to the Fraunhofer AISEC use case.

Approve minutes of 2012-01-05 meeting

Minutes of 2012-01-05 meeting APPROVED.

Interop activity
Cordny reviewed the test cases developed last year, and they need serious updating. He's going to work on that.

We don't necessarily have Kantara budget available for test suite coding, but we might be able to get that once we get our act together better. Maciej will update us on the test-readiness of his code base.

Should we try and do a tweet chat/tweet jam? What about Wed Feb 8 at 9am PT? Yes. Let's pick #umachat.

**Brief review of non-spec action items**

2011-09-22-4 Various Ongoing Build list of FAQs on the wiki. Paul to write a FAQ on "access granularity". Susan to draft a FAQ on "government PDS use cases".
2011-09-29-1 Frank, Sai, Dom, Sus, Kevin et al. Open Prepare Trust Model "user guide". In progress.
2011-10-20-2 Paul Open Define a set of "RESTful CRUD" scopes that can be reusable. In progress.
2012-01-05-1 Cordny Open Examine interop testing needs and materials, and report back by end of January on needed next steps.
2012-01-05-2 Eve Open Look into UMA WG's accepted budget proposals and get suitable AIs on our docket. **Now closed.**
2012-01-05-3 Paul Open Sketch an example of a POST token status request for Thomas to put in the spec.
2012-01-05-4 Thomas Open Add token status request example and POST rationale (from Paul) to Section 3.4 (#39), and remove the mention of OAuth bearer in Section 3.1.3.1 (#40). **In progress.**
2012-01-05-5 Rich Open Reach out to George to examine taking on issue #10. **Now closed.** They are interested to look into this, but won't have time to study issue #10 till a few weeks from now.
2012-01-05-6 Eve Closed Reach out to Lukasz regarding his to-be-assigned action (#41).

**Work through A/B-priority issues**

- Confirm status of 43, 41, 39, 10, 40 with current state of spec draft; work on 33, 30, 24/14, 12.

Discussion on issue #33: The requester access token is indeed only applicable to the current host, as a structural matter. We should instruct Thomas to edit Section 3.3 to make reference to Section 1.4 in explaining this. Let's close this issue.

Discussion on issue #30: Our current protocol builds in a required way for the host to dereference "artifact"-style (opaque) tokens at the token status endpoint at the AM. If we were to build in an option for structured tokens, it has different tradeoffs. For example, there is a higher chance of "authorization latency" for tokens that the host could verify in disconnected fashion. George also surmises that the requester would have to go and get lots more tokens in the signed-token situation. But if the requester was having to get one token per user/host/AM anyway, why are there more tokens? We're not sure there are any needed. Certainly the AM could use a different time-to-live strategy around token and permission lifetimes when it issues opaque vs. structured tokens, and this could require more frequent actions of other types by the other entities.

The reason to prefer structured tokens and local interpretation would have to do with performance and geo-distribution of servers. Some prefer one path, some prefer the other. Our current MTI path is certainly functional.

Could we use a "bearer JWT" that contains signed portions? If we accommodate "structured tokens", it certainly doesn't mean that we have to require those tokens to be signed. However, it's scary privacy-wise and security-wise to allow structured tokens that are both unsigned and unencrypted. Can we just push the creation of other token profiles off to whatever third parties feel like writing these profiles? Yes, as long as Section 3.3 doesn't preclude those opportunities to interpret the token status locally vs. engaging in the token status request dance. We should close this issue with an instruction to Thomas to add wording to Section 3.3 that puts the current first paragraph in the context of mandatorily supporting the MTI "artifact" token_types value (as defined in Section 1.5).

**Next Meetings**

- WG telecon on Thursday, 19 Jan 2011, at 9am PT (time chart) – Eve regrets; Maciej or Thomas will chair
- WG telecon on Thursday, 26 Jan 2011, at 9am PT (time chart)