UMA telecon 2010-04-29

UMA telecon 2010-04-29

- Date and Time
- Agenda
- Attendees
- Minutes
  - New AI summary
  - Roll call
  - Approve minutes of 2010-04-22 meeting
  - Action item review
  - Recap of situation with Concordia authz workshop (draft abstract) at Burton Catalyst in July
  - Review EIC workshop plans
  - Claims 2.0 draft
  - Implementation concerns
- Next Meeting: UMA telecon 2010-05-13

Date and Time

- Day: Thursday, 29 Apr 2010
- Time: 9:00am-10:30am PST | 12:00-1:30pm EST | 16:00-17:30 UTC (time chart)
- Dial-In:
  - Skype: +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)

Agenda

- Roll call
  - Note: No telecons next week due to workshop; next telecon is May 13 and next focus call is May 12; those are last meetings before IIW
- Approve minutes of 2010-04-22 meeting
- Action item review
  - New protocol issue for “baskets” based on last week’s discussion
  - Next steps on legal subteam: work through a use case? edit the technical report?
  - Claims 2.0 draft
- Recap of situation with Concordia authz workshop (draft abstract) at Burton Catalyst in July
- Review EIC workshop plans
- Protocol spec review, focus team report, implementation status
- AOB

Attendees

As of 7 Apr 2010, quorum is 6 of 11.

1. Bryan, Paul
2. Catalano, Domenico
3. Machulak, Maciej
4. Maler, Eve
5. Moren, Lukasz

Non-voting participants:

- Gerry Gebel
- Jeff Stollman
- Mark Lizar

Regrets:

- George Fletcher
- Trent Adams
- Tom Holodnik

Minutes

New AI summary

<table>
<thead>
<tr>
<th>2010-04-29</th>
<th></th>
<th></th>
<th>Revise Claims 2.0 and SAAC specs</th>
<th>To be done by May 6.</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Pau l</td>
<td>Ope n</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Roll call

Quorum was not reached.
- Note: No telecons next week due to workshop; next telecon is May 13 and next focus call is May 12; those are last meetings before IIW

**Approve minutes of 2010-04-22 meeting**

Deferred due to lack of quorum.

**Action item review**

- 2010-04-08-1 Eve Closed Turn Paul's "claims 2.0" proposal into a draft spec. Done.
- 2010-04-08-2 TomH Open Revise the tax scenario for inclusion in the Scenarios document.
- 2010-04-15-1 Eve Closed Reach out to legal eagles to get review of new technical report.
- 2010-04-22-1 Eve Closed Eve to follow up on Catalyst workshop interest and find out participation fees.

Other ideas for AIs and activities going on:

- Eve added a new protocol issue for "baskets" based on last week's discussion.
- Next steps on legal subteam: Mark agrees that extending the time slots on Louis's Doodle poll is a good idea. Eve wonders if the "starter scenarios" in the Legal Implications doc could be a good set of use cases to start from.

**Recap of situation with Concordia authz workshop (draft abstract) at Burton Catalyst in July**

Gerry is getting involved in the Authorization workshop for XACML reasons, and potentially offers some assistance in getting UMA some exposure there. We'll treat the end of next week as our deadline for figuring this all out.

**Review EIC workshop plans**

Eve, Maciej, Lukasz, Gerry, and Domenico will be at next Tuesday's workshop. We think roughly 20 people will be signed up. Gerry suggests finding out the interests and use cases of the people who attend; Eve will build this into the agenda.

**Claims 2.0 draft**

We now have a defined core structure for claims, which has basic structure for things like issuer (but not subject, which is a flaw). And Eve has published a very early draft of Simple Access Authorization Claims, which needs a lot of work.

The really tricky part is how to match the subject to the claim, and this is currently unsolved in the drafts. Getting subject identification right in the case where the policy demands that only a specific (list of) unique identifier(s) can get access is the tough part.

Paul intends to change the spec in the following fashion:

There's always an issuer, and there's always a subject. A claim-requested could demand subject of "" (any), or could demand a specific subject string (or list of them), such as "bob@gmail.com". If it's a concrete value, then the part of the UMA protocol in which the AM requests claims of the requester may (in a naive situation) have n steps in it, where the AM, having gotten a claim with the right string back, may issue a challenge and ask for it to be signed. Or the AM can in the first/only request-wave include a nonce (which functions as an AM-issued identifier for this subject).

Eve observes that with the advent of webfinger, hostmeta, and the growing LRDD ecosystem, we can start solving problems of "deep authentication" in the right way, vs. whitelisting tricks of old. Thus, Paul points out, solving problems like Gerry's example of Earthlink.com now owning Mindspring.com could be solved with some kind of (presumably brittle) whitelist, or it could be solved by Earthlink.com standing up some dynamically discoverable hostmeta at Mindspring.com.

Maciej and Lukasz are likely to start with the really simple case of claims, such as the Requesting Party Policy claim that's been proposed. This one doesn't require as many unique identifier tricks.

Currently, the Claims 2.0 spec proposes using the signing method proposed by the CouchDB folks. It doesn't have a public key discovery method, but we've added it. The primary alternate candidate is the Magic Signature approach, which was defined in the course of specifying Salmon. Magic Signature base64-encodes everything to get around normalization issues, but it makes the payload look opaque to the casual observer.

In email, George had expressed a preference for Magic Signature. The CouchDB method could be made normalizable, but it turns out it would have to forbid the use of certain JSON corner cases. In the WRAP and OAuth world, Eve observes that the Magic Signature approach has generally been "well tolerated", though a few comments came in about how it could be improved along the lines of SAML's SimpleSign spec. (The CouchDB approach was not mooted there.) We agree in principle to try the Magic Signature approach.

**Implementation concerns**

The big top-of-mind concern right now, other than claims, is the dynamic provisioning of client credentials to new hosts. We had decided that the hostmeta file could indicate a non-client-specific set of credentials that new hosts could use in approaching the AM in order to be introduced to it. Eve had earlier suggested to Maciej that since in OAuth 2.0 the client secret is optional, if the credentials are dynamically provisioned then perhaps only the client ID is needed. (He may provision both anyway.) There are also lots of cases where, in fact, the host and AM might have a static relationship and the AM previously sent the host all the credentials it needed without need of the hostmeta trick.

**Next Meeting: UMA telecon 2010-05-13**

- **Day:** Thursday, 13 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: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)