UMA telecon 2011-01-06

UMA telecon 2011-01-06

- Date and Time
- Agenda
- Attendees
- Minutes
  - New AI summary
  - Roll call
  - Approve minutes of 2010-12-22 meeting
  - Action item review
  - JSON token usage
  - Trusted claims
  - Conformance precision
  - Review rreg and scoped access
- Next Meetings

Date and Time

- WG telecon on Thursday, 6 Jan 2011, at 9-10:30am PT (time chart)
  - Skype line "C": +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214

Agenda

- Roll call
- Approve minutes of 2010-12-22 meeting
- Action item review
  - Decide how to push forward on JSON token usage, `tclaims`, and “conformance precision”
  - New action items?
- Review Jan 4 reg discussion results
- Continue reviewing scoped access in light of latest reg discussion
- AOB

Attendees

As of 6 Jan 2011 (pre-meeting), quorum is 8 of 15.

1. Adams, Trent
2. Mohammed, Alam
3. Battersby, Paul
4. Bryan, Paul
5. Catalano, Domenico
6. D’Agostino, Salvatore
7. Machulak, Maciej
8. Maler, Eve
9. Moren, Lukasz
10. Morrow, Susan
11. Scholz, Christian
12. Wolniak, Maciej

Non-voting:

- Kevin Cox
- Mark Lizar
- Cordny Nederkoorn
- Frank Wray

Minutes

New AI summary

<table>
<thead>
<tr>
<th>Date</th>
<th>AI</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-01-06-1</td>
<td>Paul Bryan, Sal</td>
<td>Open</td>
</tr>
<tr>
<td>2011-01-06-2</td>
<td>Eve</td>
<td>Open</td>
</tr>
<tr>
<td>2011-01-06-3</td>
<td>Eve</td>
<td>Open</td>
</tr>
<tr>
<td>2011-01-06-4</td>
<td>Susan</td>
<td>Open</td>
</tr>
</tbody>
</table>
Roll call

Quorum reached.

Paul Battersby is with Avoco Secure, which has recently entered the identity and information cards arena.

Maciej Wolniak has recently joined NCL. He has previously experience with corporate identity websites.

Eve is joining a new company on Jan 14; she plans to continue in her role as "chief UMAnitarian", but continues to welcome active participation and contributions by others, and her time may be more limited while she figures out the new parameters.

The original charter for this group anticipated a 18-24 month life cycle for incubating end-to-end complete draft specs, and February will be the early part of that range. We seem to be on track.

Approve minutes of 2010-12-22 meeting

Minutes of 2010-12-22 meeting APPROVED.

Action item review

- 2010-11-18-4 Eve Open Capture new user stories in the wiki.
- 2010-12-16-3 Maciej Open Recommend a course of action on the resource registration "list all" functions. Now OBE.
- 2010-12-22-1 Eve Closed Revise rreg and scoped-access specs to reflect 2010-12-22 discussion.

JSON token usage

In the 2010-12-16 meeting, we outlined three ways a JSON web token (JWT, pronounced "jot") could be used. The first way is to allow local token validation in step 3. Paul Bryan is dubious that the token could routinely contain enough information that could avoid the need for a host-AM back-channel conversation at run time. Perhaps we shouldn't try and solve for local token validation in the short term, since the simplest possible mechanism is to have the host naively ask for the whole job to be done by the AM. But we still want to leverage token-signing so that we can more gracefully solve the requester authentication/correlation problem ("Is the party who supplied the token the same party that was originally given the token?")

Trusted claims

Domenico is working on a new scenario for tclaims, which is "enterprise-class". It involves a financial institution registering a user and providing access control restrictions to its consumer-level services based on receiving trusted claims from the user. This could potentially use JWT in the third sense. Let's plan on spending the final half-hour of the next call on this topic.

Conformance precision

A subteam consisting of Eve, Cordny, and Frank will meet ad hoc and do an etherpad conformance language exercise.

Review rreg and scoped access

The first new idea is that instead of registering actions, the host would publish action descriptions and simply point to them in its resource set descriptions. The AM would then have a responsibility to retrieve the action information before displaying policy options to the user. Our assumption is that actions are:

- Global to the host (or maybe even global on a wider scale)
- Relatively small in number
- Relatively stable over time

Could we say that the AM has to re-retrieve any actions whenever the resource set description is changed and respect the cache expiration constraints placed on the action description web resource by the host? If the host changes the description of an action, caching would dictate when the change propagates. If the host adds a new action, it would be responsible for updating any relevant resource set descriptions anyway.

Do we want to consider aggregating all the action descriptions into a single file? For now, let's not. Each action description should have a unique URI reference in some fashion.

The second new idea is that we think we have a way to solve the problem of conveying to the AM, through the requester, which user's resource set is being asked for. This relates to the scoped access solution.

The authorizing user has an account on the host; call it 12345@host. The same user has an account on the AM; call it ABCDE@AM. When the user introduces the host to the AM, the host's resulting access token represents a link between the two accounts. Thus, when the host registers a resource set description and ID at an AM, the AM is capable of inferring which user the resource set belongs to. It's a good idea, though not strictly required, for the host to make resource set IDs unique across its entire user base. We should make this "RECOMMENDED" (though not "STRONGLY", since there's no major risk involved). We think this is not only nice and clean, but also privacy-preserving, since there is no exposure even of a pseudonym for the particular user involved.
We need to evaluate the security risks of exposing the host's OAuth client ID and the user's resource set ID to the requester prior to the requester having won an access token. (This distinction of “before/after the requester access token is issued” is significant for figuring out our security model and trust model; Susan, take note!) An OAuth client ID is not typically flaunted, so it feels unacceptable to require that this piece of information be shared at any stage.

Should we indeed go back to the idea of having the host register a temporary referral at the AM every time it's in the position of refusing a requester until it gets the right kind of token? And how do we handle the situation where the same requester wants access to different resource sets at the same host? Do they simply collect multiple tokens over time, and then keep a mapping of token-to-resource set internally?

**Next Meetings**

- WG telecon on Thursday, 13 Jan 2011, at 9-10:30am PT (time chart)
- WG telecon on Thursday, 20 Jan 2011, at 9-10:30am PT (time chart) – regrets from Eve; can Maciej chair?
- WG telecon on Thursday, 27 Jan 2011, at 9-10:30am PT (time chart)