UMA telecon 2011-04-07

UMA telecon 2011-04-07

- Date and Time
- Agenda
- Attendees
- Minutes
  - New AI summary
  - Roll call
  - Approve minutes of 2011-03-10 and 2011-03-31 meetings
  - Discuss IETF outcomes and capture actions
  - Drive scoped access solution
- Next Meetings

Date and Time

- WG telecon on Thursday, 7 Apr 2011, at 9-10:30am PT (time chart)
  - Skype line "C": +9900827042954214
  - US: +1-201-793-9022 (other int'l numbers) | Room Code: 295-4214

Agenda

- Roll call
- Approve minutes of 2011-03-10 and 2011-03-31 meetings
- Action item review
- Discuss IETF outcomes and capture actions
  - Update dynamic client reg I-D and draft scoped-access I-D?
  - Discuss latest trust model work
  - New draft material to share, hopefully
  - Drive scoped access solution
  - New diagrams and messaging flows to share, hopefully
- AOB

Attendees

As of 24 Feb 2011 (post-mtg), quorum is 7 of 13.

1. Catalano, Domenico
2. Hardjono, Thomas
3. Maler, Eve
4. Morrow, Susan
5. Scholz, Christian
6. Wolniak, Maciej

Non-voting:

- John Bradley
- Kirk Brown
- Frank Wray

Regrets:

- Paul Bryan
- Sal D'Agostino
- Maciej Machulak
- Lukasz Moren
- Cordny Nederkoorn

Minutes

New AI summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-04-07-1</td>
<td>Eve</td>
<td>Open</td>
<td>Figure out how to do a keep-alive revision of the dynamic client reg spec.</td>
</tr>
<tr>
<td>2011-04-07-2</td>
<td>Frank</td>
<td>Open</td>
<td>Match constellations to scoped access diagrams to see what happens.</td>
</tr>
<tr>
<td>2011-04-07-3</td>
<td>Thomas</td>
<td>Open</td>
<td>Turn the results of the ad hoc call on scoped access into core spec text.</td>
</tr>
</tbody>
</table>

Roll call

Quorum not reached.
Approve minutes of 2011-03-10 and 2011-03-31 meetings

Deferred due to lack of quorum.

Discuss IETF outcomes and capture actions

Thomas reports: It was unfortunate that Eran couldn’t attend the OAuth meeting; this added process friction during the meeting. The big news is that the OAuth WG has been moved under the Security Area at the IETF. One of the long-time Security Area Directors is retiring; the "new guy" is Stephen Farrell, who has long experience in PKIX and IETF and is now at Trinity College in Dublin. Likely more people on the security side will pay attention to OAuth now.

One of the big bones of contention was Eran’s unilateral removal of the client assertion profile, on which the SAML assertion work depends. Thomas leaped into the breach to ensure that the re-added text is written correctly. He also signed up to review the OAuth use cases document; he recommends that we submit use case text and will make recommendations about how to do this as his review proceeds.

We should do a "keep-alive" revision of the dynamic client reg spec as soon as possible to ensure that the topic gets the attention it needs, even if we don’t change it substantively very much. The OAuth tracking page is what gets watched, so an "UMA presence" there is key.

In the next few weeks, we’ll try to update the scoped access proposal according to our discussions, then submit it (or the core spec) for IETF consideration.

- Discuss latest trust model work

Domenico has published a new document called Measuring Elements of Trust.

When the subject (authorizing user) first meets the AM and, separately, the host, these are the first element of bootstrapping trust. And then when the user introduces the host to the AM, this is the second element of bootstrapping trust. This is the key stage at which the user forms mental states about trust and trustworthiness.

After that, we get into regular episodes of data sharing, which is what the trust model constellations are all about. Domenico uses basic geometry to quantitatively measure how much trustworthiness each constellation has. The reason why person-to-self sharing ultimately has a short line is because it involves (real-time) consent, which is powerful for instilling a mental state of trustworthiness (short X-axis distance). What the short line means is that risk is "collapsed" by virtue of this kind of interaction (risk being a kind of inverse of trust). This is a way of assigning quantitative risk to frequently-qualitative factors.

We all agree that the paper is brilliant and Domenico should get a PhD. for it. We will publicize this work into the various Kantara and external threads of conversation on trust models, trust frameworks, and privacy frameworks.

Drive scoped access solution

Eve sent diagrams to the list for consideration (since updated in the same thread).

We discussed the "Host POV", discovering that it’s missing a final box on the left-hand branch where the host gives the requester the ticket.

John comments: A good optimization would be for the AM to also give the host a list of initial claims that will be needed, so that the host can inform the requester of this in case it wants to unilaterally supply claims when it initially approaches the AM asking for authorization. This is similar to some work he’s doing on access authorization by presenting signed JWT tokens.

The ticket should probably be time-limited (just as the token should be time-limited). If the user actually does change policy in between token upgrading and token usage, the requester will simply be punted again.

In the "AM POV", therefore, the requester might be able to show up with claims in hand, which means that its initial approach at the AM could involve a request message that’s identical in every important way to the response to a claims request. A good example of the kind of claim that might want to be passed along "eagerly" vs. " lazily" is the basic identity claim, whether the user’s policy demands that it’s "Alice again" or that it’s "Bob".

Frank suggests mapping user stories/scenarios/constellations.

Let’s schedule an ad hoc call for Wed Apr 13 at noon PT. We think Eve, John, and possibly Domenico can join, and maybe others.

Next Meetings

- WG telecon on Thursday, 14 Apr 2011, at 9-10:30am PT (time chart)
- WG telecon on Thursday, 21 Apr 2011, at 9-10:30am PT (time chart)
- WG telecon on Thursday, 28 Apr 2011, at 9-10:30am PT (time chart) (Eve may be a bit late - Maciej will initiate call and chair for first 15 min)