UMA telecon 2010-08-26

UMA telecon 2010-08-26

- Date and Time
- Agenda
- Attendees
- Minutes
  - New AI summary
  - Roll call
  - Approve minutes of 2010-08-12 and 2010-08-19 meetings
  - Action item review
  - Status reports from Legal subteam and the wider UMA world
  - Step 3 presentation of token/credentials
  - The prevalence of options in the spec
  - Resource/scope registration discussion

Next Meetings

Date and Time

- WG telecon on Thursday, 26 Aug 2010, at 9-10:30am PT (time chart)
  - Skype line "C": +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214

Agenda

- Administrative
  - Roll call
  - Approve minutes of 2010-08-12 and 2010-08-19 meetings
  - Action item review
  - Status reports from Legal subteam and the wider UMA world
- Resource/scope registration discussion
  - Identify requirements
  - Begin drawing spec conclusions
  - Assign spec writing tasks
- AOB

Attendees

As of 11 Aug 2010, quorum is 6 of 11.

1. Catalano, Domenico
2. Fletcher, George
3. Hardjono, Thomas
4. Maler, Eve
5. Moren, Lukasz
6. Scholz, Christian

Non-voting participants:

- Kevin Cox
- Mohammad Alam
- Anna Ticktin (staff)
- Herve Ganem
- Mark Lizar

Regrets:

- Maciej Machulak

Minutes

New AI summary

<table>
<thead>
<tr>
<th>Date</th>
<th>AI ID</th>
<th>Owner</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-08-26-1</td>
<td>Mark</td>
<td>Open</td>
<td>Write up CCTV scenario.</td>
</tr>
<tr>
<td>2010-08-26-2</td>
<td>Mark</td>
<td>Open</td>
<td>Set up the next Legal subteam call.</td>
</tr>
<tr>
<td>2010-08-26-3</td>
<td>Herve</td>
<td>Open</td>
<td>Write up real-time scenario(s).</td>
</tr>
<tr>
<td>2010-08-26-4</td>
<td>Eve, Domenico</td>
<td>Open</td>
<td>Write up generic Alice/Bob trust framework scenario.</td>
</tr>
</tbody>
</table>
Roll call

Quorum was reached.

Approve minutes of 2010-08-12 and 2010-08-19 meetings

Minutes of 2010-08-12 and 2010-08-19 meetings APPROVED.

Action item review

- 2010-08-12-3 Maciej, Christian, Eve Closed Write up answers to the philosophical questions posed on 2010-08-12 related to resource/scope registration, for the SMART implementation, resource registration spec, and scope registration spec proposal respectively.

Status reports from Legal subteam and the wider UMA world

Maciej conveys through Eve: UX study results from the SMART project are nearly ready for distribution.

Lukasz notes that he is focusing on implementing OAuth communication flows.

Eve reports that her ad hoc UMA talk at PiT Labs last week garnered a fair amount of interest from various parties at Microsoft involved in CardSpace and U-Prove (who asked questions about unlinkability), and also involved in various consumer identity technologies.

Thorsten Hoellrigl of Karlsruhe University has also been doing some CardSpace-related research that may have synergies with UMA. We’re not sure where all this might go, given that UMA has such a strong server-side focus around managing and evaluating policies.

Step 3 presentation of token/credentials

Christian has raised an issue regarding the requester’s OAuth client credentials (and possibly also its signing of messages) when it interacts with a host-as-resource-server. If the requester presents its AM-issued client credentials, how can the host possibly validate the token locally? Also, it’s a security issue because now the host can impersonate that requester at that AM (keeping in mind that we’re trying to solve for the host, requester, and AM being loosely coupled from entirely different administrative domains).

We struggled with this mightily when UMA was on an OAuth V1.0 basis, and now we need to figure out a more efficient solution than we had before. The complexity of local validation of tokens in this type of environment is so difficult that it makes Eve want to support only outsourced token validation. 😞

George points to Nat’s new OAuth signature specification as providing important input for us around this.

The prevalence of options in the spec

Christian would like to winnow down the number of options in the spec by focusing on fewer use cases. For example, would it make sense to focus on healthcare use cases with Gerry Beuchelt? Or personal data store use cases with Iain Henderson? Eve suggests possibly working with the folks at W3C who are working on a Contacts API. We should also consider having core features that must be implemented, with options on top of that. Christian prefers heavier modularity in the spec.

Eve suggests that the PDS scenario would perhaps be a simple yet powerful choice. It has the following distinctive aspects:

- Authorizing user gets to choose the host(s) of their self-asserted personal data
- Authorizing user gets to choose their AM
- The (multiple) requesting parties are companies that run online services at which the user has a login account

Eventually, a PDS should be usable for “trusted claims” purposes to let people engage in person-to-person sharing from the receiving side, but it doesn’t have to do that right away.

Herve suggests a “presence” use case or similar, in which real-time location/presence data generated by a machine of some sort is UMA-protected. This sounds somewhat related to the CCTV use case we discussed in the Legal subteam call yesterday. Mark is currently working on a proposal to use UMA with video surveillance in the UK, supporting compliance with data protection laws.

Resource/scope registration discussion

- Identify requirements
- Begin drawing spec conclusions
- Assign spec writing tasks

Christian speaks in favor of going with simple scope strings a la OAuth. The discussion last week focused on many issues of synchronization, for example, if the user deletes a resource on the host. How loosely coupled can we get the whole system? Eve would love to avoid requiring the AM to ask the host which scopes it should apply in its policy decision-making process at the time that a requester approaches, seeking an access token. But this would mean that the host has to tell the requester what scopes apply, so that the requester can carry that over to the AM.
Herve observes that "scope" is a higher-order conceptual construct that may complicate things because of the problem of memory (cached data). Is it really a problem if the AM issues an access token for some (implicit) resource that's part of a scope it knows about, and in the meantime the user deletes that specific resource on the host, such that the requester tries and fails to get the resource – not because the token was bad but because the resource doesn't exist? Wouldn't this just be a “different level of error” that could happen at anytime anyway, due to transient web problems etc.?

Thomas points out that p. 26 of the OAuth spec defines the authorization server as "defining" scopes. So perhaps it's entirely appropriate for us, in our effort to couple OAuth entities more loosely, to ensure that the AM "defines" (comes to know about) scopes under the direction of each of the hosts they work with. We think Maciej's objection to scopes is more around avoiding the semantics of actions/methods than around avoiding scopes per se.

Herve poses the problem that different hosts might use the same name for a scope but mean different things by them. So we'll have to account for something like host-namespaced scopes for starters.

**Next Meetings**

- WG telecon on Thursday, 2 Sep 2010, at 9-10:30am PT (time chart) on line C