UMA telecon 2010-09-23

Date and Time

- WG telecon on Thursday, 23 Sep 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 2010-09-16 meeting
  - Action item review
  - Updates from the wider UMA world
  - Review progress on dynamic registration
- Paris F2F planning
- Scenarios and use cases
  - Review new scenario template and other changes
  - Discuss any changes needed to location scenario to support spec and implementation work
- Protocol work
  - Discuss "scope flow" in protocol (email) and UX (PDF)
  - Discuss need to further profile existing OAuth profiles
- AOB

Attendees

As of 02 Sept 2010, quorum is 6 of 10.

1. Catalano, Domenico
2. Fletcher, George
3. Hardjono, Thomas
4. Hoffmann, Mario
5. Machulak, Maciej
6. Maler, Eve
7. Moren, Lukasz
8. Scholz, Christian

Non-voting participants:

- Kevin Cox
- Sal D’Agostino
- Mark Lizar
- Anna Ticktin (staff)

Regrets:

- Herve Ganem

Minutes

New AI summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-09-23</td>
<td>Open</td>
<td>Follow up with Phil W. re holding a F2F meeting at IIW XI.</td>
</tr>
<tr>
<td>2010-09-23</td>
<td>Open</td>
<td>Review Domenico's wireframes and our recent emails with &quot;scope&quot; in the subject line, and weigh in with thoughts in email.</td>
</tr>
</tbody>
</table>
Roll call

Quorum was reached.

Sal's company, IDmachines, provides identity services to government and enterprise. He is involved in the US government's initiative around identity verification (such as PIV-I). He was formerly involved in CoreStreet.

Approve minutes of 2010-09-16 meeting

Minutes of 2010-09-16 meeting APPROVED.

Action item review

- 2010-08-26-4 Eve, Domenico Open Write up generic Alice/Bob trust framework scenario. In progress. To be distributed and discussed more thoroughly next week.
- 2010-08-26-6 Eve Open Ping Denise Tayloe of Privo to see if she has interest in taking custodian scenario forward. Pending Scenario doc edits.
- 2010-09-02-1 Thomas Open Categorize all existing scenarios by their distinctive aspects. Well under way.
- 2010-09-16-1 Mark Open Update main trunk of the Legal Considerations document with Legal subteam input.
- 2010-09-16-2 Eve, Thomas, Mario Closed Meet to discuss sharing Scenario document editing duties.
- 2010-09-16-3 Christian Closed Update core spec with Step 3 text.

Updates from the wider UMA world

- Fraunhofer project: Mario reports that they have been discussing the location scenario, and it's much more complex than they thought! They need more clarity from us about how is playing the different roles.
- SMART project: The code publication has had a slight delay, but it's still under way.
- Hold IIW F2F first week of November?: Of the folks on this call, George, Maciej, Lukasz, likely Eve, and possibly Sal will be at IIW 2010b and could plan to attend an UMA F2F on the Monday. Let's plan on that.
- Review progress on dynamic registration: Maciej would like to schedule a phone call for next week, for all interested folks (UMA, OAuth, and other). Christian suggests that Maciej conducts this discussion on the OAuth list instead of in a phone call.

Scenarios and use cases

- Review new scenario template and other changes (doc)
- Discuss any changes needed to location scenario to support spec and implementation work

Thomast has enhanced the Introduction and Instructions section to include a template of “dimensions” and “building-block features” for which each scenario should provide a description. So far we have scope, cardinality, nature of host, dynamism vs. staticness, resource discovery, nature of access to protected resources, and person-to-self.

Eve wonders if the scope and nature of access to host ones can be combined somehow. And perhaps the person-to-self one can be renamed end-to-end or something.

The location scenario has been revised to include answers to the template.

Eve would like to see examples of real or imagined scopes provided in scenarios, and to see as much evidence of real-world scopes as possible (which, in the location case, is certainly possible) to inform our design process. Since she submitted this scenario, she should flesh it out more.

Regarding the cardinality dimension, can this be a discussion-starter instead of a “deterministic” topic? There are many aspects around cardinality that could be relevant.

Let's review the dimension template more over time, before we apply it to all of the scenarios thus far documented. We'll keep experimenting with scenarios 6, 7, and 11.

Discuss "scope flow" in protocol (email) and UX (PDF)

Eve had previously put together a speculative list of where the concept of scope impacts UMA.

- Step 1 (or anytime thereafter?)
  - Host registers scopes with AM.

This seems right.

- Step 2
  - Requester attempts protected resource access at host, allowing host to infer potential suitable scope(s).

In today's OAuth deployments, often the client, which has been statically provisioned with credentials, was told at registration time (out of band of OAuth) about what actions they could perform at that API. Christian comments that in Facebook, the client dynamically passes its desired scope during request time instead. Where scopes are openly documented, does it make sense for UMA – or even OAuth itself – to allow a requester/client to be explicit in telling the resource server/host what scope(s) it wants? For UMA, it would be more logical to do this when the requester approaches the AM (see just below).

- Host redirects requester to AM with info about what scope(s) to ask for (needs to be secured somehow?).
The host has the privilege of saying what scopes are available, but the user has the privilege – through their policies – of saying who gets access under what conditions. So should the host have told the requester all the possible scopes that apply to that resource, so that the requester can choose what scopes to ask for? But this has security and privacy implications, e.g. in the case where the user’s tagging of their photos might be revealed (unless the scope string obscures the actual tag, like "tag_restriction:abc123", but it maps to "pictures-of-waterfalls"). Then again, for simple read vs. read/write access cases, this could be really useful. Perhaps, outside of the purview of UMA, a host can make available some user preference settings for sharing this. This sounds complicated, but we could allow the ecosystem to experiment with such features if UMA says nothing about what to do. We hope to be able to lean on generic OAuth for any processes where tokens are downgraded to handle lower scope and upgraded to handle additional scope (the latter requiring user consent), though.

So maybe the host is authoritative for telling the requester what scope(s) to ask for in order to have the best chance of success in getting an access token for those scopes, but if the host’s API is well enough documented that the requester wants to try for more/bigger scopes, it can approach the AM with a different set. This would mean that the host is not responsible for making the scope information tamper-proof, which simplifies things considerably.

We discovered that we are still not sure that scopes should be a flat list, vs. a flat list of actions (with resources handled as a separate dimension – it was unclear from our discuss whether they would also have to be registered with the AM). We will focus exclusively on this issue next week.

(The rest of the proposed list is below, for the record; we didn’t finish discussing it.)

- Requester conveys desired scope(s) in approaching AM.
- AM uses desired scope info to match applicable policy (hmm, did we account for multiple scopes here?).

Step 3
- Requester attempts access, this time with token, allowing host to infer required suitable scope(s)
- (Host conveys token to AM for validation)
- (Assuming token is valid, AM returns applicable scopes for it)
- Host maps applicable scopes to scope of attempted access

**Next Meetings**

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