UMA telecon 2010-09-30

UMA telecon 2010-09-30

- Date and Time
- Agenda
- Attendees
- Minutes
- New AI summary
- Approve minutes of 2010-09-23 meeting
- Action item review
- F2F and subteam plans
- Updates from the wider UMA world
- Flat list of scopes vs. scopes-of-action on resources
- Next Meetings

Date and Time

- WG telecon on Thursday, 30 Sep 2010, at 9-10:30am PT (time chart)
  - Skype line "C": +9600827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214

Agenda

- Administrative
  - Roll call
  - Approve minutes of 2010-09-23 meeting
  - Action item review
  - Updates from the wider UMA world
  - F2F and subteam plans
- Flat list of scopes vs. scopes-of-action on resources
  - Revise Domenico's latest UX wireframes
  - If we get to it, discuss "scope flow" in protocol (see last week's minutes for relevant notes)
- AOB

Attendees

As of 30 Sept 2010 (pre-meeting), quorum is 6 of 11.

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

Non-voting participants:

- Kevin Cox
- Herve Ganem
- Mark Lizar
- Frank Wray
- Anna Ticktin (staff)

Regrets:

- Mario Hoffmann
- Tom Holodnik

Minutes

New AI summary

<table>
<thead>
<tr>
<th>ID</th>
<th>Owner</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-09-30-1</td>
<td>Eve</td>
<td>Incorporate Fraunhofer's input on the location scenario into the Scenario document.</td>
</tr>
<tr>
<td>2010-09-30-2</td>
<td>Thomas</td>
<td>Write up a &quot;secure descriptor&quot; proposal and send to the list.</td>
</tr>
</tbody>
</table>

Quorum was reached.

Christian gives regrets for next week's meeting.
F2F and subteam plans

We will hold a F2F at IIW XI from 11am to 5pm on Monday, Nov 1. No room yet.

Updates from the wider UMA world

The SMART project folks have just made an exciting announcement. They have released a new OAuth 2.0 library, called OAuth leeloo, which is currently at V0.1. It supports some UMA extensions that will be supported fully as part of the near-future UMA/j framework. Spring is partially integrated. The blog post with the announcement is here.

Eve wrote a position paper on UMA that was accepted for an upcoming W3C privacy workshop. The paper has been getting some strong reviews, so it will probably be discussed at the workshop even though she's not able to attend to present it.

Mario and his team have fleshed out the location scenario for their implementation purposes.

Flat list of scopes vs. scopes-of-action on resources

Maciej's original proposal involves registering just resource URLs. Eve's proposal involves registering resources and actions (a matrix). Christian's proposal involves registering resources and actions and (a matrix). Christian's proposal (http://groups.google.com/group/kantara-initiative-uma-wg/browse_frm/thread/7d6a37434d4a3e8/e84f5845b3397fccc?lnk=gst&q=scope#84f5845b3397fccc) involves registering a flat list, which could contain resources or actions or both, but they'd have to be squished together.

George: A "scope" could be seen as an action that a requester wants to take, and you could apply constraining "filters" or "qualifiers" that reduce their, um, scope of operation. Gerry Beuchelt has described how the hData goal, for now, is to enable UMA protection for an entire set of data for a patient; doctors want to know everything about you, not just part of the data.

It's important to take into account the kinds of requesting parties to think about the whole scope problem. For example, doctors may want the whole set of information, but maybe researchers need an anonymized/blurred/redacted version, which is akin to the location scenario's need for a "read at the city level" scope. And some parties, such as pharmacists, may deserve to know the patient's full prescription record (what meds they're taking), but nothing else. And insurers are another constituency. Fine-grained access is inherently hard. As Mark Zuckerberg says, "Public is the new normal" – but it's because it's too hard to do otherwise!

George: Simplifying the problem into a flat list may be oversimplifying.

We walked through Domenico's latest UX wireframes.

Calendars are an interesting example, possibly a true exception case, because the iCal standard dictates the difference between free/busy and detailed views, and we're likely to interpret this as different resources vs. different scopes on the same resource. Thus, on slide 7, the host would likely register (at the AM) the user's choice of "all scopes" as two resources with "read" scope on them, rather than registering this as a single resource with two scopes. Of course, the UX could still present this as a "scope checklist" to the user, though this could be extra-confusing if we want to popularize the concepts of the two dimensions.

Christian: Wouldn't the resources, in fact, be the individual calendar entries? Eve: Was thinking of the whole calendar as a resource, a la the iCal data format standards. George: But what about doing a PUT or POST into a calendar? You'd normally be creating a new resource. Who owns the resulting entry, and how could it be UMA-protected??

Eve: Would prefer to see resources as having a single "authorizing user" who may have the right to delegate 100% of the possible access rights to another person! George: There are real-world examples of co-ownership and equal rights to authorize third-party access, but he's willing to go with the simplifying assumption for now. For example, just sticking with calendar entries, the person who has the right to add entries to your calendar tends to have the (sometimes sole) right to delete it as well.

Mark: Notes that his work on "Master Controller" issues is relevant to this question. Thomas: Active Directory and other directory services already have the notion of groups owning resources. Eve: The web doesn't inherently have this concept. We've "bought" the simplicity that the web's RESTful architecture gives us; have we bought too many constraints along with that? We have also bought OAuth's simplicity around a resource owner having to authenticate to an authorization server in order to authorize third-party access; implicitly this resource owner could be a group of people, depending on how they manage "accounts" at the AS.

Herve: There are use cases in the world of needing multi-party decisions, similar to the "relationship cards" solution Eve has described. Eve: Recognizes the real-world complexity that can be introduced, but is sincerely hoping we can solve the simplest possible problem.
Eve: Coming back to the wireframes, notice that CopMonkey can only know how to present Travel Calendar as a "primary axis" of scope and free/busy or details as a "secondary axis" of scope if the host gave it two axes of information. Do we want to allow this in our spec? Herve: Continues to have a concern about how the AM presents the policy-to-scope options to the user. Eve: Is it sufficient to have a scope description along with a scope string in each case? It seems so, though Christian's proposal also included the important element of different language translations of the description. Thomas: This description should be thought of as a "secure descriptor". Herve: This is getting closer and closer to the way file systems are managed, with folders and files and the permissible operations on them.

Eve: Would it be possible to ratchet up interoperability of scopes by registering permissible scopes when registering content types? This would be one place to standardize resources as RESTful APIs.

Maciej: The current SMART work has focused on a single axis, mixing resources and operations freely. Eve: It may be messy to "explode" everything into a single axis, but it has the capacity to express everything that you could have in two axes. Herve: That's not correct; you lose the ability to expose the two levels to the users. Eve: Stands corrected! 😊 Indeed, all of our UX explorations seem to gravitate towards the two axes, which is interesting; if we need them in a single case, perhaps we want to preserve the ability to have them. Herve: In fact, folder hierarchies are quite common, and we might want to preserve that option generically too. Eve: Indeed, and photo albums could take advantage of that. Although we started down that path earlier, with registering "all resources", we were worried about having to maintain so much state dynamically between the host and AM. Herve: It could be simpler than this, because folders implicitly summarize everything within them.

Based on today's conversation, we seem to have gone back to having sympathy for "multiple axes" vs. "one axis", but we still have not made a firm decision. Christian: Let's focus on completing a single scenario in order to learn more, and then proceed to more and more scenarios.

Next Meetings

- WG telecon on Thursday, 7 Oct 2010, at 9-10:30am PT (time chart) on line C