UMA telecon 2010-01-14

Date and Time

- **Day:** Thursday, 14 Jan 2010
- **Time:** 9:00-10:30am PST | 12:00-1:30pm EST | 17:00-18:30 UTC (time chart)
- **Dial-In:**
  - Skype: +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)

Attendees

As of 12 Jan 2010, quorum is 9 of 17.

1. Adams, Trent
2. Akram, Hasan
3. Andrieu, Joe
4. Bryan, Paul
5. Catalano, Domenico
6. Fletcher, George
7. Holodnik, Tom
8. Machulak, Maciej
9. McIntosh, Michael
10. Maler, Eve

Guest:

- Joni Brennan (staff)

Regrets:

- Iain Henderson

Agenda

- Roll call
- Approve minutes of UMA telecon 2009-12-17, UMA telecon 2010-01-07
- Action item review
- Webinar planning
- Lexicon discussion
- Consider UMA logo idea
- Opportunity to provide scenarios as input to the OAuth process
- Review scenario docket
- Custodian
- E-commerce
- Walk through personal loan wireframes
- New action items

Minutes

Roll call
Quorum was reached.

Approve minutes of UMA telecon 2009-12-17, UMA telecon 2010-01-07

Motion to accept minutes APPROVED.

Action item review

- Eve: Add terms-negotiation scenarios to Scenarios document: Some more work has been done on these, particularly the requester identification scenario, but it's still in progress.
- Webinar team: Draft slide deck for group review: Eve is on the hook to produce a first draft by this weekend.
- Eve: Propose a requirement or design principle about constraining our V1 scope to "full-blown" sites: Eve sent a query to the list about this. Pending.
- Webinar team/WG: Publicize the webinar through blogging, tweeting, etc.: It will be time to do this very soon.
- Joe: Submit a protected-inbox scenario: Done.

Webinar planning

Title: "UMA Update: Making the world safe for user-managed access"

Proposed abstract: "When dealing with many websites, the price we're forced to pay to is "hand over the data" – data that's sensitive, valuable, and personal. The new User-Managed Access web protocol promises to help web users share their data more selectively to better effect, and to help websites get access to fresher and better-quality data. This session will review UMA benefits, progress to date, and next steps."

Joe suggests adding something that will help the abstract distinguish UMA from OAuth.

In addition to slides, which Eve will draft this weekend for webinar team review, Paul will prepare the "peekaboo" version of the swimlane diagrams. We think Domenico's recent graphics will be used heavily in the slides. We'll have the ability to take phone and WedEx "raise your hand" question to help us know what to deep-dive into.

We'll have a limit of 25 people who can attend; we'll limit our own attendance to 5.

Lexicon discussion

Eve proposed some definitions (sans terms) in email:

1. An HTTP client (per HTTP) capable of interacting with hosts and AMs to request, and receive access to, protected resources.
2. A web application that manifests a #1.
3. A legal person (for example, an organization or natural person) that has deployed a #2 in order to seek access to a protected resource.
4. A web user acting as a representative of a #3, capable of assisting an AM's process of determining the suitability of that #3 for access.
5. A web user on whose behalf a #3 is acting in seeking access to a protected resource.

Joe suggests that #3's definition needs a change: Who deployed the application isn't quite right given that there might be a "requester delegate" in play (an outsourced cloud-based host). We want to express that #3 is somehow on the hook (liable) for the access that ultimately gets granted; it's on their behalf that the #2 application is deployed, even if they didn't deploy it themselves. Paul gives the example of his Google calendar trying to access Joe's Google calendar. Google is the #3.

Tom makes a connection to the Custodian scenario (to be discussed shortly). Eve cautions that some seemingly custodian-related use cases might, in reality, turn out to be vanilla UMA use cases, without a need to split the "authorizing user" into multiple concepts the way we're splitting "requester" into five concepts here.

The intent behind the option of "natural person" in the definition of #3 is that some people might really run their own mail servers, blogs, and UMA requesters. These people could be said to be in the #5 role as well, in this case, and even in the #4 role.

Is the agreement forged between the authorizing user and #3, or between the authorizing user and #5 (if present)? Or is it a combination of both, depending? For example, Paul might want to make Google not cache the data for too long – but might also want Joe not to expose Paul's calendar availability to other people. If you're allowing the soccer team to see photos, you are granting that access to the soccer team and not to others they might want to pass the photos along to. People in the #5 role aren't in a very good position to "speak for" #3 companies (like Kinko's for printing the photos) in promising anything. This is where standard agreements, and safe harbor statements that say a party isn't liable for certain things others do, can perhaps come in.

Tom asks about #4. Joe explains it as the "Foto-Mat pornography problem"! Eve had thought that a person who works for #3 and represents them may, in the course of events, be involved in the access-granting process (clicking "I Agree" or solving a captcha on an UMA-mediated screen), which has UX and legal implications, if not protocol ones. But a different #4 person may be involved in actual data/service access, which is indeed the Foto-Mat porn problem and has legal implications at the least.

Consider UMA logo idea

The group generally likes the logo itself and the idea of visually representing UMA in various materials.

Motion to make Domenico the UMA Graphics/UX Editor APPROVED. (Whoo-hoo!)

Domenico has agreed to contribute the logo to Kantara for management.

Opportunity to provide scenarios as input to the OAuth process
The OAuth telecons are scheduled. The current plan is for us to submit information about our approved UMA scenarios in email to convey our key use cases (endpoints, parties, actions, etc.). Does this have to be in I-D form to be effective? It might not be quite as effective if just in a plain email, but there may be IPR questions around the I-D approach. Let's do the email approach for now, and see how it goes.

Review scenario docket

Eve's goal is to get all the awaiting-submission scenarios submitted by next Thursday.

- The Iain/Joe car-buying line item should be struck; we'll incorporate references to it on a case-by-case basis.
- Maciej's higher-ed scenario will show a person who uses many different systems for "lifelong learning", with one university serving as a locus of control.
- In the health data scenario, there's almost a "profile" of UMA in that it uses UMA for two different purposes – the first being a way to protect access to an XRD-based discovery service for both adding entries and reading entries.
- Mike M. may be able to submit a scenario on information card integration; he'll check. George wonders if cards can be employed to any protocol, not just UMA, for provisioning URLs of resources of various types. The bigger question is around how identity "flows" through UMA in general.
- Can we add the ACL/PoCo aspect to the custodian use case? Let's discuss below.

Custodian

Should we add an ACL aspect to this scenario? Yes. George notes that AOL does a lot of both ACLs and parental control already. ACL management is a nightmare today because it can't be shared or factored out from multiple control points.

Eve is a bit worried that we're combining together two things in this scenario:

1. One would involve splitting an "authorizing user" into a "user whose hosting is controlled" (a child) and a "user who administers authorization policies" (their parent(s)). This could potentially be handled by having the user-at-the-host be the child and the user-at-the-AM be the parent, when the host and AM are introduced.
2. The other would involve just vanilla AM, in that the child is the "#5 role" behind the requester. In this case, how can does it work for the #5 role to be attested to?

Don't miss George's and Praveen's blog entries about identity tokens on this subject:

- Protecting "discovery" information
- Open identity token
- Open identity token and personal discovery service

E-commerce

This is getting closer. Hopefully the people who have commented on it in the past, at least, can review it closely and decide if it has a clean bill of health.

Walk through personal loan wireframes

Deferred. Please do this on your own time and send any thoughts to the list.

New action items

New AIs:

<table>
<thead>
<tr>
<th>Date</th>
<th>AIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-01-14-1</td>
<td>Eve: Open Revise webinar abstract with the webinar team's help and get it onto the relevant websites.</td>
</tr>
<tr>
<td>2010-01-14-2</td>
<td>Eve: Open Revise requester definitions for review.</td>
</tr>
<tr>
<td>2010-01-14-3</td>
<td>Domenico: Open Develop wireframes for approved scenarios.</td>
</tr>
<tr>
<td>2010-01-14-4</td>
<td>Domenico: Open Contribute UMA logo to Brett for future Kantara management.</td>
</tr>
<tr>
<td>2010-01-14-5</td>
<td>Eve, Paul, George: Open Construct a draft use-case email for OAuth IETF group consumption.</td>
</tr>
<tr>
<td>2010-01-14-6</td>
<td>Maciej: Open Revise custodian scenario</td>
</tr>
<tr>
<td>2010-01-14-7</td>
<td>Mike M: Open Check on whether he should be writing an information card use case.</td>
</tr>
</tbody>
</table>

Next Meeting: UMA telecon 2010-01-21

- Day: Thursday, 21 Jan 2010
- Time: 9:00-10:30am PST | 12:00-1:30pm EST | 17:00-18:30 UTC (time chart)
- Dial-In:
  - Skype: +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)