UMA telecon 2010-02-04

UMA telecon 2010-02-04

- Date and Time
- Attendees
- Agenda
- Minutes
  - New AI summary
  - Roll call and introductions
  - Approve minutes of UMA telecon 2010-01-28
  - Action item review
  - Webinar recap
  - Implementors’ report
  - Lexicon discussion
  - Spec review
  - Deferred
- Next Meeting: UMA telecon 2010-02-11

Date and Time

- Day: Thursday, 4 Feb 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 22 Jan 2010, quorum is 9 of 17.

1. Akram, Hasan
2. Andrieu, Joe
3. Bryan, Paul
4. Catalano, Domenico
5. Davis, Peter
6. Fletcher, George
7. Holodnik, Tom
8. Lizar, Mark
9. Machulak, Maciej
10. McIntosh, Michael
11. Maler, Eve
12. Smith, Bill

Non-voting:

- Iain Henderson
- Tom Smedinghoff

Guests:

- Joni Brennan (staff)

Regrets:

- Trent Adams
- Mike Hanson

Agenda

- Roll call and introductions
- Approve minutes of UMA telecon 2010-01-28
- Action item review
- Webinar recap
- Implementors’ report
- Lexicon discussion
- Scenario review
  - Custodian (splitting authz-side parties)
  - Health data (trusted dynamic resource discovery)
  - Employer/employee (other mandatory access control)
- AOB

Minutes
New AI summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-01-14-2</td>
<td>Eve</td>
<td>Open</td>
<td>Revise requester and authorizer definitions for review.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AI extended to include authorizer terms on 2010-02-04.</td>
</tr>
<tr>
<td>2010-02-04-1</td>
<td>Iain</td>
<td>Open</td>
<td>Share Mydex screen shots that illustrate how a relationship manager UX can be handled.</td>
</tr>
</tbody>
</table>

Roll call and introductions

Quorum was reached. Tom S. introduced himself; he's a lawyer practicing at a firm in Chicago. He chairs an ABA legal task force focusing on all forms of identity management.

Approve minutes of UMA telecon 2010-01-28

Motion to accept minutes of UMA telecon 2010-01-28 APPROVED.

Action item review

- 2009-10-15-2 Eve Open Write a "Hey, Sailor" scenario to illuminate the needs around Requesters that ask for resource access without the User expecting them: She's going to try real hard to dispense with this soon.
- 2009-12-03-04 Eve Open Add terms-negotiation scenarios to Scenarios document: It has seemed more practical to wait on this until we get our requester concepts straight, since "requester identification" is the lowest hanging fruit among the terms scenarios (and that one is at least drafted already).
- 2009-12-17-4 Eve Open Propose a requirement or design principle about constraining our V1 scope to "full-blown" sites: The issue here was whether the protocol needs to change depending on whether someone who is controlling a requester or host is using some sort of unusual device or rich Internet application. Paul suggests that for requesters, the answer is no. And even if a host is, well, hosted on an iPhone, as long as it presents a web service endpoint on the network, nothing seems to need to change. Joe's company has some use cases (not documented for UMA purposes yet) that involve hosting information on your client device and possibly "pushing" it somewhere (to a requester after a terms negotiation phase). George proposed a way to handle this with only a slight deviation from the normal flow.
- 2010-01-14-2 Eve Open Revise requester definitions for review: OBE.
- 2010-01-14-3 Domenico Open Develop wireframes for approved scenarios: Maybe the next one should show user consent by SMS in real time.
- 2010-01-14-5 Eve, Paul, George Open Construct a draft use-case email for OAuth IETF group consumption: now closed.
- 2010-01-28-2 Joe Open Edit protected inbox scenario in response to telecon and email discussion: Joe will get started on that.
- 2010-01-28-3 Paul Open Propose in email how multiple protections on a resource could work: now closed.

As a side note, we decided that we are UMAnitarian! 😊

Webinar recap

The webinar materials are all now available from the UMA Explained page. Thanks to Joni and Dervla for managing to get the recordings up! The WebEx experience was disappointing. We can leverage what we learned this time in future, but we're inclined to switch services.

Implementors' report

Two implementation efforts are starting up, one at Fraunhofer (C#) and one at Newcastle (Java). Maciej has started an UMA-dev mailing list so that any developer can ask questions easily. Both projects will involve case studies with students.

Iain is still interested in building Mydex implementations with an UMA UX. And Peter is still interested in doing mobile development.

Lexicon discussion

George is, to date, most fuzzy on the legal implications of what we're doing, and his recent email attempted to explore the same level of sophistication on the authorizing side as we've started to achieve on the requesting side.

A question he didn't pose was: In the custodian example, if you have multiple authorizing entities, if Alice and Bob are both executives and they delegate authorization powers to their shared assistant, how does that work? And if some requesting person has to prove who they are to the authorizing side, what role are they in when they do that?

Joe asserts that any authentication process that the requesting person goes through should be opaque to the authorizing side; rather, all that matters is what claim was produced to satisfy a request for claims.

Tom S. explains that in legal terminology, "person" means anything that can enter into a contract, with the two possibilities being "entity" (legal person) and "natural person". But this will confuse technical folks. Would "party" do? And in that case, do we need something like a "requesting intermediary" to describe Google when it's acting on behalf of requester Bob?

Paul makes the case that only the authorizing user and the ultimate requesting user (party?) can forge a contract, and Tom S. agrees. Tom says that if Google acting as an agent for Bob does something wrong, Alice (who has a contractual relationship with Bob, not Google) may be considered a "third-party beneficiary" who could bring a legal claim against Google, though normally Bob would sue Google if they did something wrong. In reality, Google will limit its liability so much in its TOS with Bob (which is "invisible" to any UMA-mediated agreement) that it may limit Bob's ability to have much say over Google's behavior.

Eve wonders if "requesting agent" could be used to refer to the Google case when Bob as requester is involved. Since "agent" is too overloaded in both the technical and legal worlds, people thought "intermediary" was better. There may be arbitrary numbers of intermediaries (mashups, the "requester delegate" situation, etc.), and we can dispense with them all with this one term.

George points out that we're successfully obfuscating the requesting party's identity from the host, since the authorization decision flows through the AM alone.
Eve suspects that when the requesting party is a company/organization, the authorizing user is likelier to affect the requesting party's privacy practices, data retention lengths, etc. than when the requesting party is a person. This is because Bob probably can't force Google-as-requester do anything different! Let's call these two cases **person-to-person sharing** and **person-to-service sharing**. We're definitely interested in the former, but agree that it doesn't have the same kind of goals around redressing the power balance that the latter does.

Eve gets very rough consensus on these terms, so that she can work on formal definition proposals:

- requester (short for requesting endpoint)
- requesting application (software running wherever, on any combination of client/server sides, that engages host and AM endpoints in the requester endpoint role)
- requesting intermediary(ies) (a legal term, meant to help us discuss liability and limitations thereof, referring to a "person" to whom/which legal concepts can be applied)
- requesting party (a legal term for sometimes a legal person/entity, sometimes natural person/human)

We have protocol terms, system terms, and legal terms. Tom argues that we should find terms that suffice in all contexts. You can't sue an application! And an application can't sign a contract! "Intermediary" and "application" do sort of overlap, in that Google is a company and the Google Calendar software is an application, but Eve suspects we can define the terms without mentioning this, and it will be clear which to use in each circumstance.

**Spec review**

Paul's next steps, assuming people are satisfied with the flow we have, are to create real spec prose for it. The other big area to work on is XRD and LRDD; we depend on them heavily. We also need to continue to work with the OAuth V2.0 community to ensure that any UMA requests related to it are considered fully.

The "claims 2.0" area is so large that Paul is inclined to spin up a separate effort to get this done properly. He feels there's no inherent process bottleneck here, other than in implementations. He's thinking we can quickly develop a set of claim types to address documented UMA scenarios. He would prefer that UMA not dictate specific claims solutions.

George notes that if different AMs have a multiplicity of claims they request, this will impede Internet-scale adoption. Ideally, requesters need to be able to hand over some basic kinds of claims according to our baseline use cases, and not have to do anything special. Eve agrees.

ICF has a claims catalog as a public service; maybe we'll end up doing something similar for convenience.

**Deferred**

- Custodian (splitting authz-side parties)
- Health data (trusted dynamic resource discovery)
- Employer/employee (other mandatory access control)
- And the "multiple protections on a resource" thread

**Next Meeting: UMA telecon 2010-02-11**

- **Day:** Thursday, 11 Feb 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)