UMA telecon 2010-07-01

UMA telecon 2010-07-01

- Date and Time
- Agenda
- Attendees
- Minutes
  - New AI summary
  - Roll call
  - Approve minutes of 2010-06-17 and 2010-06-24 meetings
  - Next meetings: focus group? WG? Legal subteam?
  - Action item review
  - xml2rfc/I-D/github/bitbucket status and issues
  - Third-party-asserted claims, "identity tokens", trust model
  - RRAPI
  - Next Meetings

Date and Time

- WG telecon on Thursday, 1 Jul 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 2010-06-17 and 2010-06-24 meetings
  - Next meetings: focus group? WG? Legal subteam?
  - Action item review
  - xml2rfc/I-D/github/bitbucket status and issues
  - Third-party-asserted claims, "identity tokens", trust model
  - UMA-protecting the requesting party's claims
  - Dynamic client registration
  - Schedule for submitting I-D
  - RRAPI
  - Push? Pull?
  - AOB

Attendees

As of 3 Jun 2010 (post-meeting), quorum is 6 of 10.

1. Adams, Trent
2. Catalano, Domenico
3. Hardjono, Thomas
4. Holodnik, Tom
5. Machulak, Maciej
6. Maler, Eve
7. Moren, Lukasz
8. Scholz, Christian

Non-voting participants:

- Joe Andrieu
- Nat Sakimura
- Mark Lizar

Regrets:

- Gerry Gebel

Minutes

New AI summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Owner</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-07-01</td>
<td>Christia n</td>
<td>Open</td>
<td>Sketch a new version of push+pull RRAPI, taking into account the 2010-07-01 discussion, the Artifact Binding, and the SMART resource registration writeup.</td>
</tr>
<tr>
<td>2010-07-01</td>
<td>Eve</td>
<td>Open</td>
<td>Link from our wiki to the github area as the official working repository for our specs.</td>
</tr>
<tr>
<td>2010-07-01</td>
<td>Eve</td>
<td>Open</td>
<td>Send Domenico's draft model writeup to the list for comment.</td>
</tr>
</tbody>
</table>
Roll call

Quorum was achieved.

Approve minutes of 2010-06-17 and 2010-06-24 meetings

Minutes of 2010-06-17 and 2010-06-24 meetings APPROVED.

Next meetings: focus group? WG? Legal subteam?

Let's do a focus meeting on Wednesday 7am PT. (See below.) Don't forget about the upcoming Legal subteam meeting; MarkL will get some chatter going on the list in preparation for this.

Action item review

- 2009-12-03-4 Eve Open Add terms-negotiation scenarios to Scenarios document.
- 2010-05-27-3 Eve Pending Find and distribute info on the new proposal for OAuth signing.
- 2010-05-27-4 Eve Pending Ask Dave Crocker for help with Step 1 user stories.
- 2010-06-17-1 Christian, Eve Open Work on the conversion of the core spec and the dynamic registration spec to xml2rfc. In progress.

xml2rfc/I-D/github/bitbucket status and issues

Christian has gotten Kantara approval to use github, with the appropriate Kantara IPR and wiki links. His first priority for the xml2rfc conversion is the stuff we want to submit to IETF. Maciej will forward the SMART protocol documents to the list shortly (now done).

Third-party-assigned claims, "identity tokens", trust model

Domenico’s proposal involves reusing UMA to protect the requesting party’s claims, such that the AM is in a position to request the claims.

The example we used to discuss the idea was:

- Alice is the authorizing user (one type of "subject")
- CopMonkey is her AM (AM1 in the slides)
- She wants to share a calendar with Bob
- Bob is the requesting party (another type of "subject")
- SMARTam is his AM (AM2 in the slides)
- He stores third-party-assigned claims about him in his IdP (say it’s Google), which is a "claims host"

Thomas asks: Is it possible for the model on slide 9 to be extended “horizontally”? If so, transitive trust across AMs and multiple claims hosts should be possible. It appears to be the case. Is trust truly transitive, though? Trust could “leak” over longer chains of IdPs (look at SAML’s control of IdP proxy hops). A super-duper IdP that is certified at a high level in a known trust framework starts with high quality.

In a way, reusing UMA itself makes things more complicated because it’s harder to keep all the actors straight, but it also keeps things as simple as UMA itself is (however simple that is!). In other words, if we go in this direction, we could remove the very simple and specialized (and less functional) claims request/response model, where this removal makes UMA simpler -- but actually doing claims stuff in step 2 will then mean having to “import” all of UMA into that point, requiring every AM to be a requester endpoint too.

Note that the current simple claims protocol doesn’t allow the requester to throttle who gets to see the claims; it assumes that the requester will hand it out to any AM that asks.

Does it make sense to have both, with the base protocol keeping the simple/specialized claims request/response protocol in step 2, and an extension /profile for circumstances where high LOA (Level of Assurance) and LOP (Level of Protection) are both needed in trust frameworks?

No conclusion yet, but now it’s on our docket. We may want to add it to the scenarios document eventually.

RRAPI

- Push? Pull?

Nat notes that the AB model now has both push and pull mode. AB started with push for its use cases, but Google, Yahoo!, and other providers didn’t like this, so they added pull. The problem is that the data being pushed and the user themselves end up on different servers on different continents, and there’s a propagation issue. The timing of server interactions is sensitive specifically during the Step 1 introduction process, when the user is naturally “visiting” the AM.

(In Step 2, where a requester has to wait for a user’s real-time consent and the user is currently offline, we had originally designed a callback/polling system to allow the requester to manage the token-getting process. Nat likes this approach for handling notification.)

Christian is concerned that having both push and pull makes UMA more complicated.

Eve asks: What should happen in the period after the AM meets the host (say, Flixr.com) but before the host has successfully provisioned the AM with its resource and scope details? We believe the AM should reject requests for access tokens for any un-heard-of resource until it has heard from the host. The internal error condition would be something like “unknown resource”.

In the post-introduction case, like the examples Eve sent to the list in email, do we need push or pull or what? Maybe you don’t need either push or pull in a plain host-AM communication:

1. Alice sets up a "vacation 2010" tag-based policy at the AM (let’s assume she has to do this per-host for now).
2. Alice uploads a new photo into Flixr with tag "vacation 2010".
3. Without Alice going to the AM in the interim, the requester approaches Flixr looking for the newest photo that was tagged with "vacation 2010".
4. The host tells the requester what scope information to carry to the AM in order to let the AM make an access decision without having been specifically informed of the newest photo. But would it have to attach all the possible scopes that apply to this resource? This seems wrong (and does it reveal too much to the requester?). OR: The AM gives back an access token that has structured conditional scope information ("If the resource has this tag, let them in").

Conclusion so far: For initial resource registration, we think we need pull (or stated another way, "push with a ping" where the ping stimulates the AM to pull something – or does this have the same latency problem? we can work on this). For subsequent resource registration/changes, we think we'll also have to support push; the need for the host to update the information at the AM will never entirely go away.

**Next Meetings**

- Focus meeting on Wednesday, 7 Jul 2010, at 7-8am PT (time chart)
- WG telecon on Thursday, 8 Jul 2010, at 9-10:30am PT (time chart)
- Legal subteam meeting on Monday, 12 Jul 2010, at 1-2pm PT (time chart)