UMA telecon 2011-08-11

UMA telecon 2011-08-11

- Date and Time
- Agenda
- Attendees
- Minutes
  - New AI summary
  - Roll call
  - Approve minutes of 2011-07-07, 2011-07-21, and 2011-07-28 meetings
  - Action item review
  - Review next steps for August
  - Review UMA/hData explorations
  - Discuss core protocol issues
  - Implementation best practices
- Next Meetings

Date and Time

- WG telecon on Thursday, 11 Aug 2011, at 9-10:30am PT (time chart)
  - Skype line "C": +9900827042954214
  - US: +1-201-793-9022 (other int'l numbers) | Room Code: 295-4214

Agenda

- Roll call
- Approve minutes of 2011-07-07, 2011-07-21, and 2011-07-28 meetings
- Action item review
- Review next steps for August
  - Review meeting schedule to allow for better OpenID Connect representation and alignment?
- Review UMA/hData explorations
- Discuss core protocol issues:
  - ...arising from implementation experience
  - ...arising from OpenID Connect synergy efforts
  - ...outstanding from July
- Implementation best practices
  - Doc interest?
  - Time to reawaken the uma-dev list?
- AOB

Attendees

As of 30 July 2011, quorum is 7 of 12.

1. D'Agostino, Salvatore
2. Fletcher, George
3. Hardjono, Thomas
4. Machulak, Maciej
5. Maler, Eve
6. Moren, Lukasz
7. Szpot, Jacek
8. Wray, Frank

Regrets:

- Catalano, Domenico
- Brown, Kirk

Minutes

New AI summary

<table>
<thead>
<tr>
<th>2011-08-11</th>
<th>Ev</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>e</td>
</tr>
</tbody>
</table>

Change the call lengths on the wiki and in the online calendar.

Roll call

Quorum was reached.

Approve minutes of 2011-07-07, 2011-07-21, and 2011-07-28 meetings

**Action item review**

- 2011-04-07-2 Frank, Kirk **Closed** Match constellations to scoped access diagrams to see what happens.
- 2011-04-14-1 Maciej, Alam Open Build list of FAQs (both questions and candidate answers) on the wiki. **Eve will write a few new answers. The SMART team will write a special SMARTAM Q&A.**
- 2011-07-07-2 Thomas Open Capture all current issues, resolutions, and statuses on the UMA wiki. **Now meant to go to github. Thomas has an account now and Eve has enabled issues in the UMA-Specifications repository.**

**Review next steps for August**

- Revise meeting schedule to allow for better OpenID Connect representation and alignment?

Proposal: Change the Thursday meetings to an hour, and try to schedule an OpenID Connect+UMA considerations call every other week at an alternate hour that we mutually work out with John, Nat, et al. Let's officially change the length of the "quorate" calls to 60 minutes.

**Review UMA/hData explorations**

Frank has made some assumptions about hData that are specific to the use case he's selected. We need to check these with the Project hData folks.

In hData, you have to discover the EHR service providers. If a specialist needs information held by your primary-care physician, the specialist may not know the endpoint of the PCP’s service yet. You need to discover the endpoint, and the patient/authorizing user also has to authorize that discovery somehow. We assume that the specialist can learn the location of the discovery service somehow, to "bootstrap" all this. This could be solved by OpenID Connect’s discovery model, we think, as long as that discovery model is protectable/authorizable (through OAuth itself or through UMA?).

A couple of weeks ago we talked about "requester-initiated" vs. "discovery-service-initiated" flows. But the use cases actually break down further:

- **Requester-to-host for one resource set/scope** (has been provisioned the resource location somehow, presumably knows the API for accessing it, doesn’t know what’s required to get access of all the types of permissions it seeks) – we have, so far, solved only for this flow.

- **Requester-to-host for one/multiple resource sets with multiple scopes** (has been provisioned the resource location somehow, presumably knows the API for accessing it, doesn’t know what’s required to get access of all the types of permissions it seeks, but wants to efficiently get multiple permissions added to its token at once)
  - This has been requested by Maciej M. We’d need to drill down farther on the one vs. multiple resource sets question. Implementation choices will change depending on how frequently each pattern is needed.
  - It’s easier to solve for a single resource set with multiple scopes vs. multiple resource sets when the requester approaches the host first, since it would presumably approach with a concrete request against a particular resource.
  - But the host is authoritative for the protected resource sets there, so it could serve as a kind of distributed resource-set discovery service.
  - Or, since the AM has been told all this information by the host, the host could just refer the requester to the AM to find out possible resource sets.
  - But the requester is, so far, completely untrusted, so it should only learn/discover what’s appropriate for it at this point. So maybe sending it to the AM for initial authorization to discover things is needed. This is what we think OpenID Connect wants to do.

- **Requester-to-AM (with discovery functionality) first**
  - We keep going in the direction of seeing the AM as needing discovery functionality!
  - Simple Web Discovery seems to depend on OAuth protection, but our original idea (reflected in the etherpad) was that you’d UMA-protect the discovery service, as a "host of discovery data". Would this actually simplify the OpenID Connect view of discovery services? Currently they seem to be treated specially.

The Project hData folks have experimented with both magnetic stripe cards and QR codes for allowing a patient to provision their discovery service's URL to a medical provider to bootstrap the process.

**Discuss core protocol issues**

- ...arising from implementation experience
- ...arising from OpenID Connect synergy efforts
- ...outstanding from July

We’ll defer until the issues get into GitHub.

**Implementation best practices**

- Doc interest?
- Time to reawaken the uma-dev list?

We have a number of implementers now, but we don’t yet feel we know enough yet to collect best practices.

Eve wonders about best practices on OAuth token timeouts etc. George recalls a great post by Brian Eaton on the OAuth list that touched on token practices.

**Next Meetings**

*Note:* Meetings will move to a 60-minute length in future.

- WG telecon on Thursday, 18 Aug 2011, at 9-10am PT (time chart)
• WG telecon on Thursday, 25 Aug 2011, at 9-10am PT (time chart)
  • Skype line "C": +9900827042954214
  • US: +1-201-793-9022 (other int'l numbers) | Room Code: 295-4214