UMA telecon 2012-12-06

UMA telecon 2012-12-06

Date and Time

- **Focus** meeting on Thursday, 6 Dec 2012, at 9am PT (time chart) – technical, interop, podcast
  - Skype: +9905100000481
  - SEE BELOW for info on the podcast dial-in, which we’ll open up partway into the hour

Agenda

- **Action item** review (including discussion of results of reviewing UMA test frameworks)
- Discussion of discovery metadata registration proposal (forthcoming)

Minutes

**Action item review**

Sal offers to help Mike/Gluu with the enterprise UMA case study. Keith offers to write a case study on UMA for accessibility information. Eve finished the personal cloud case study. Thomas will open the spec on Friday to finish the three small open issues. The SMART team hasn’t yet been able to create its discovery metadata registration proposal.

New technical issues

**Terminology:** Could the UMA spec use the standard OAuth terminology, as in host goes to RS, AM goes to AS, and requester goes to client? We have consensus: Let’s try it. We could try to use “role” terminology to paper over awkward spots, e.g., where the RS is a protection API client to the AS.

**Modularization:** Could UMA phase 1 be separated out somehow? There seem to be use cases for using each half vs. the other: OpenID Connect and AXN seem interested in phase 1 (introduction), and Gluu/OX seems interested in phase 2/3 for scope management.

There are three kinds of discovery. IdP **discovery** (literally parsing out the domain of a user-entered URI) is one kind; tools like .well-known could be used. Another kind/level is AP/IdP or host/AM **introduction**; tools like Account Chooser could help with that. Then there’s a **personal discovery service** a la Liberty ID-WSF’s Disco service. For the discovery service, UMA’s naive way of “solving” claim/resource discovery has been that the requester could construct a “known” location URI of an intermediate resource hosted at the AM, so that the requesting party could qualify in to get access to the pointer stored there, and thereafter get access to the ultimate resource. This conflates discovery and registry functions, and the request for access is also implicitly a request for knowing whether the resource exists. This is why the resource registration function of UMA is so key; enough information about the semantics of the resource has to be “registerable” in a machine-readable way to enable a requester to seek and get access to what they want.

If we were to separate out “phase 1”, that’s not necessarily the right line to draw to make a Disco API spec reusable for both UMA and non-UMA purposes. The key piece is the resource registration CRUD API. We think we should separate this out, and perhaps finally use the http-json-resource spec as well. Should we account for the old XRD provisioning spec as well? Let’s think about leveraging these two. Note that UMA-protecting a discovery resource enables the AM to obscure any PII that might be ensconced in the URI of the ultimate resource, since the requester has to “test in” to get authorization even to know whether it exists.

**Introduction:** Would it be a good idea to mention Account Chooser as a non-normative suggestion in the spec for introduction? Also, should we explicitly acknowledge the possibility of “AM-initiated” introduction vs. our current assumption of “host-initiated introduction”? OpenID Connect doesn’t really solve for IdP-initiated SSO; there are some security issues with getting it to work perfectly. So they’re leaning towards a naive solution where the IdP makes it easy for the user to get redirected to the RP so that they can “start” from the right place. We can use that as well, for now. Whenever the security problems with true IdP-initiated SSO flows get worked out to everyone’s satisfaction, we can pick up on it for AM-initiated host introduction.

**Host metadata pull:** For any metadata about the host/RS that are independent of the specific resources to be protected, Nat has proposed a “pull” model in a blog post. Does this make sense to consider as part of our process of resource registration? It’s possible that hosts need to “push” relevant changes to protected resources regardless.

Attendees

- Eve
- Keith
- Domenico
- Lukasz
- George
- Cordny
- Sal
- Alam
- Thomas
- Maciej

Next Meetings
• **Focus** meeting on Thursday, 13 Dec 2012, at 9am PT (time chart) – educational
• **All-hands** meeting on Thursday, 20 Dec 2012, at 9am PT (time chart) – legal, all topics
• **NO MEETINGS** for the rest of 2012 – happy new year/end-of-the-world!