UMA telecon 2010-12-22

Date and Time

- WG telecon on Wednesday, 22 Dec 2010, at 9-10:30am PT (time chart)
- Skype line "C": +9900827042954214
- US: +1-201-793-9022 | Room Code: 295-4214

Agenda

- Roll call
- Approve minutes of 2010-12-16 meeting
- Action item review
- Scope in the core spec
  - Discuss results of focus call
  - See pirate pad
- JSON tokens, local validation of tokens, trusted claims
  - Discuss results of focus call
- Conformance clauses in the core spec
- AOB

Attendees

As of 21 Dec 2010, quorum is 8 of 14.

1. Mohammed, Alam
2. Bryan, Paul
3. D'Agostino, Salvatore
4. Fletcher, George
5. Hardjono, Thomas
6. Machulak, Maciej
7. Maler, Eve
8. Morrow, Susan

Regrets:

- Domenico Catalano
- Lukasz Moren
- Christian Scholz

Minutes

New AI summary

<table>
<thead>
<tr>
<th>Event</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Revise reg and scoped-access specs to reflect 2010-12-22 discussion.</td>
</tr>
</tbody>
</table>

Roll call

Quorum was reached.

Approve minutes of 2010-12-16 meeting

Minutes of 2010-12-16 meeting APPROVED.

Action item review
Paul notes that the "proof-of-work" technique is useful in general for mitigating the risk of DOS attacks. He doesn't believe it should be baked into the UMA protocol (though the claims request-response protocol can serve as a way to do this in step 2), and Thomas agrees. We generally think this should be dealt with at the Internet layer, not the UMA application layer. Alam still has a concern about advertising the AM endpoint to requesters who show up without an access token; this is something to keep an eye on over time.

**Scope in the core spec**

A partial draft proposal based on the focus call of 21 Dec 2010 (notes) was mailed to the list.

Eve is guessing that this proposal, or a follow-on proposal that matches the group's wishes, might ultimately be folded into the core spec.

Step 1b in the flow summary: "AM maps authorization constraints to permissions according to the user's instructions (out of band)." Thomas comments: It's a little confusing to say "out of band" here; "independently" or "entirely internal to the AM's operations" would be better. Maybe mention this is entirely up to user interface/experience considerations. Do we need to write any kinds of specs around the user experience of "creating policies", "setting authorization constraints", etc.? Maybe we need a best practices document at the very least! Perhaps this could be akin to the Universal Login Experience (ULX) work, only around user-centric policy setting in UMA vs. IdP discovery in web SSO.

It may be worthwhile to note in the rreg spec that a resource set ID could be a direct URL, though this leaks data. There are use cases for wanting to do this, however.

Step 2b: "Host tells requester the identifier of a resource set that would suffice for access to the resource, and redirects requester to AM (defined in this specification for now)." It is assumed that the requester has out-of-band knowledge of possible actions on the resource to which it had attempted access, through host API documentation." George comments: So the host already knows that the protected resource in question equates to, or is part of, some resource set(s) that it previously registered with the AM, and chooses which resource set identifier to tell the requester to ask for.

Re step 2b, Eve asks: What do we think about the fact that the host can exercise a bit of a judgment call when it chooses what resource set ID to give to the requester? For example, what if a protected photo is in two sets, "photos tagged with #puppies" and "photo album - New Puppy"? We seem okay with this.

Re step 2b, should we stick with the idea that action IDs are well-known and the host shouldn't tell the requester what action to ask for? We think so. George points out that it would be difficult for the host to know the requester's intent, and it's a good idea to push this out to an "out-of-band" process that involves the host documenting its API publicly and the requester deciding what sorts of actions it wants to ask for access to. And the requester could likely try only one action at a time anyway (e.g. reading vs. updating) when it first approaches the protected resource, even if it wants the right to perform multiple actions. So a requester could simply "ping" (GET) a resource, discover it's UMA-protected, and then be required to do its homework to look up its options for actions if it wasn't already familiar with this host's service provider documentation.

(Eve has added an issue to the rreg spec about the future possibility of pointing to standardized action IDs vs. defining them by value.)

Step 2c: "Requester asks AM for an access token, specifying the identifiers of the desired resource set and action(s) (defined in this specification for now)." How does the AM know which user's policies to look up when the requester shows up? Maciej comments: In one of the SMART implementations, it's the whole resource set URL being given to the requester, which identifies the user through the {userid} path component being supplied. If this isn't done, another option is for the host to tell the requester "ask for access to this resource set for this user", and name the user ID. Another is for it to manage its resource set ID namespace such that the IDs are unique across all users, so that the AM can figure out which user's policies to look up. The first two options "leak" correlatable user ID information, even though ideally the ID string has been made pseudonymous, so we'd like to avoid this if possible. The last option puts a burden on the host to manage that namespace and a (small) burden on the AM to figure out the right host, user, and resource set description, working backwards from knowledge of the resource set ID conveyed from the host to the requester. But even if we use the last option, a host can only manage its own namespace (unless we dictate some sort of UUID approach for resource set IDs), so the AM still needs to be told the host! Is it safe to share the host's client ID with the requester for this purpose?

George proposes: An alternative to all this is a limited-time (10 minutes?) transaction identifier (an "authorization event ID") that the host first creates directly at the AM, then gives to the requester, and gets conveyed by the requester to the AM.

We ran out of time for discussion of steps after 2c.

**Next Meetings**

- No meeting on Thursday, 30 Dec 2010
- WG telecon on Thursday, 6 Jan 2011, at 9-10:30am PT (time chart)