UMA telecon 2010-12-16

UMA telecon 2010-12-16

Date and Time

- WG telecon on Thursday, 16 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 2010-12-09 meeting
  - Upcoming meetings: special UMA WG telecon on Wednesday rather than Thursday; no meeting Dec 30; first meeting of 2011 is Jan 6
- Action item review
- UMA validation bounty program: award decision time
- JSON token status (George) and implications for trusted claims
  - Refer to etherpad and trusted claims proposal 08b
- Resource reg spec revisions
  - Review TODO/issues list
- Review conformance testing questions
- AOB

Attendees

As of 16 Nov 2010 (pre-meeting), quorum is 8 of 15.

1. Adams, Trent
2. Alam, Mohammed
3. Catalano, Domenico
4. D'Agostino, Salvatore
5. Fletcher, George
6. Hardjono, Thomas
7. Machulak, Maciej
8. Maler, Eve
9. Moren, Lukasz
10. Morrow, Susan

Non-voting participants:

- Kevin Cox
- Cordny Nederkoorn (latter half)
- Anna (staff)

Minutes

New AI summary

2010-12-16-1	Eve	Open	follow up on the bounty award next steps.
2010-12-16-2	Eve	Open	Check with Paul on preferences for HTTP error responses for unsupported methods in requests.
2010-12-16-3	Maciej	Open	Recommend a course of action on the resource registration "list all" functions.
2010-12-16-4	Eve, Thomas, Sal, Susan, Maciej, Christian	Open	Work in the uma-scope etherpad to propose a scope solution for the core spec.
2010-12-16-5	Eve	Open	Forward prior discussions about DOS and proof-of-work with the list.

Roll call

Quorum was reached.

Approve minutes of 2010-12-09 meeting

Minutes of 2010-12-09 meeting APPROVED.

Note: Upcoming meetings: special UMA WG telecon on Wednesday rather than Thursday; no meeting Dec 30; first meeting of 2011 is Jan 6.

UMA validation bounty program: award decision time

Sal, Susan, Maciej, and Eve had an offline discussion. Sal believes the hData use case is more directly useful than having a conformance test suite, but they could also be used in concert. Eve believes they're both valuable in different and complementary ways. Cordny's original indication of submission interest estimated the work at 40-50 hours.

MOTION: Sal moves, and Thomas seconds: The bounty award should be split $2500/$1500 to Cordny and hData, and in the event that hData can't accept the award, the WG requests of Kantara that $1500 be allocated towards developing a validator in 2011. Carried by unanimous consent.

JSON token status (George) and implications for trusted claims

The latest draft is here; a new one is expected soon. The expectation is that a token will have an envelope, a claims segment (a "body"), and a signature. The body doesn't actually have to be a JSON object; at the IIW meeting, it was agreed that a JSON form would be standardized but other forms could be used. The signature is over both the envelope and the body, because the envelope is extensible. Nat has done some work around accommodating multiple signatures, and that will be supported, though it's not currently documented. There's a proposal for how to add encryption to the token. Breno from Google demonstrated how the sign-first and encrypt-first patterns could solve different problems.

Thomas feels that the IIW discussion just replayed the old S/MIME discussion in a way, and he's concerned that the lessons previously learned may not be absorbed if there isn't enough overlap in the people having a discussion. This is something to keep an eye on.

How can UMA use all this stuff? Several places:

1. A JSON token could allow a host to validate a requester access token locally and not outsource that job to the AM in real time.

1. A JSON token could be used as a claim inside a claims document as we define it in the Claims 2.0 spec. If UMA defines a privileged set of claims, then it could namespace those claims.

1. A JSON token could be an UMA-protected resource, which plays into the trusted claims scenario.

For starters, let's look at the Claims 2.0 spec and see how it matches up. Sal, Eve, and George will think about this, and Eve will ping Paul on it as well.

Resource reg spec revisions

We reviewed the TODO section at the end.

- NEW issue: How should a RESTful API indicate that a particular method is unsupported? Do you get a particular error code?

Maybe 401 is appropriate. Eve will check with Paul about his preferences.

- Consider the question of i18n of resource set and action "name" strings in addition to the newly proposed extension-parameter mechanism.

We looked at the extension mechanism and it looks fine. We can wait on the i18n question until someone really needs it.

- Would implementers expect the "list all" methods to return just a list of IDs, or the whole set of structures? If so, do this through a query parameter? E.g., "?mode={short|verbose}"

The motivation to "list all" is mostly to help the host diagnose and remediate problems if the host suspects that it has gotten out of sync with the AM. The host could, of course, get all the IDs and then do a GET on all the suspicious ones. Maciej notes that actions will tend to be a small set, so it would seem more efficient to have the AM reply with the full descriptions by value. But would the same be true of resource sets? And what should the by-value returned object look like? He'll make a recommendation here.

- In the core spec, we have to say how a {resourceid} plus one or more {actionid}s gets used and flows around as normal OAuth scope information. Base64-encode a JSON representation? Extend to allow a resource parameter? Something else? (See the Requirements Analysis above for guiding requirements.)

We'll get together on the UMA scope etherpad and work on this.

• Should resource set descriptions list action identifiers, as currently specified, or full action description URLs?

Should we rename the parameter name of resource set descriptions to "resource_set"? Yes. We don't want people to equate it with an actual concrete resource.

We clearly need to add an Example section that walks through the matching-up of descriptions, IDs, PUTs, GETs, etc.

What if different hosts register similar "reading"-type actions called different things, or what if they're different but called the same thing? This is treated in a totally host-specific manner so far. Domenico's wireframes show how this could work. Eve brings up the example of FireEagle, which has several quite distinct "reading" actions/scopes.

What if we were to encourage the standardization of APIs and their actions by allowing descriptions to be provided by reference instead of by value? Of course, there's a lot of value add in proprietary APIs and that's okay. Let's make this a NEW issue.

- Flesh out the UMA-level error response section.

Sal notes that this is a specific example of a general category of "invalid request" error. This might be a better error message, possibly with some detail supplied about the host ID being wrong. Maciej notes that at the HTTP level, the right error is a 401: Unauthorized. Is this what we should use? We could add an UMA-specific header indicating the problem. Susan notes that the AM is probably going to want to audit events like this.

Separately, Alam wonders about the possibility of DOS attacks and other security issues when the host tells the requester in Step 2 which AM to go to. Maciej notes that the requester/client has to do some work to indicate that it is trying to interact on an OAuth/UMA basis in its request message, and only then does it learn the AM location. We've discussed this general issue before.

- Should the host hint at an appropriate action description to the requester, or since actions are supposed to be well-known should we leave it out?

Let's save this for the core spec portion of the discussion.

- Note that there are new security and privacy considerations sections.

Susan is our new "privacy czar" 🙂, and will be reviewing this material to see what improvements can be made.

Next Meetings

- WG telecon on **Wednesday**, **22** Dec 2010, at 9-10:30am PT (time chart)
- **No meeting** on Thursday, 30 Dec 2010
- WG telecon on Thursday, 6 Jan 2011, at 9-10:30am PT (time chart)