UMA telecon 2011-04-28

Date and Time

- Roll call
- Approve minutes of 2011-04-21 meeting
- Action item review
- IIW planning
- Next Meetings

Agenda

- Roll call
- Approve minutes of 2011-04-21 meeting
- Action item review
- IIW planning
  - Blogging
  - Sessions and conveners
  - Slides
  - Screenshots
  - Graphics
  - Documents
- Scoped access review
  - Thomas spec text
  - Frank/Kirk swimlanes
  - Cordny input on error flows
- OAuth interim meeting planning
- AOB

Attendees

As of 21 Apr 2011 (pre-mtg), quorum is 8 of 14.

1. Mohammad, Alam
2. Catalan, Domenico
3. D’Agostino, Salvatore
4. Fletcher, George
5. Hardjono, Thomas
6. Machulak, Maciej
7. Maler, Eve
8. Moren, Lukasz
9. Morrow, Susan
10. Wolniak, Maciej
11. Wray, Frank

Non-voting:

- Kirk Brown
- Kevin Cox

Regrets:

- Paul Bryan

Minutes

Roll call

Quorum was reached.

Approve minutes of 2011-04-21 meeting

Minutes of 2011-04-21 meeting APPROVED.
Action item review

2010-11-18-4 Eve Open Capture new user stories in the wiki.
2011-03-02-1 Nat Open Put together JWT-compliant examples of Claims 2.0 and Simple Access Authorization Claims. Pending. Eve will reach out to Nat.
2011-04-07-2 Frank, Kirk Open Match constellations to scoped access diagrams to see what happens. Frank will do more work tonight.
2011-04-07-3 Thomas Open Turn the results of the ad hoc call on scoped access into core spec text. Thomas, Eve, and Maciej met and made some progress.
2011-04-14-1 Maciej, Alam Open Build list of FAQs (both questions and candidate answers) on the wiki. Alam has made some progress.
2011-04-21-1 Eve Open Update the scoped access proposal into I-D form for discussion. This will be in "slide form" first.
2011-04-21-2 Eve Open Revise the dynamic client registration spec again.
2011-04-21-3 Cordny Closed Look at scoped access flow for error conditions we've missed.

IIW planning

Blogging: The SMART team is planning three blog posts. Eve is planning to blog the scoped access ideas to start getting feedback.

Sessions and conveners: Maciej M. and Eve agreed to co-convene a "New Stuff in UMA" session. The SMART team will convene a couple of other sessions, including a demo/technical implementation session (Luksasz) and a UX session (Maciez W. will preview the SMART interface, their research, and the factors that made them change the interface).

"Assignments": The SMART team agrees to be assigned the task to collect FAQ. Maybe we can give an assignment to Cordy. In general, we should be prepared to compare notes during breaks and such. We should all keep our eyes and ears open for use cases and scenarios.

It turns out George will be there and Susan won't.

- Scoped access review

What should the "elevator pitch" be when we try to convey UMA's technical proposition? We seem to like "phases" and agreed to use this wording consistently in all our new materials:

- **Phase 1:** protect a resource.
- **Phase 2:** get authorization.
- **Phase 3:** access a resource.

Cordny made a few comments about error conditions in the 'pad. What is the right thing to do if there's an HTTP-level error? We're assuming that the invoking application just has to deal with things like proxy gateway failures etc. in its own way. George prefers UMA messages about tokens being invalid and such to return HTTP success (200), but OAuth has chosen to use 400 and 401 for such conditions.

Note that our AM has a token validation endpoint that's UMA-specific and not part of OAuth, whereas our host needs to respond to the client/requester about invalid tokens in a way that is OAuth-compliant (ideally). So if we choose to use 200 in an AM's "token-invalid" response, it might look inconsistent next to the message that the host has to turn around and give the requester, but we could choose that direction. There is a sharp difference of thinking among web protocol designers around this. It seems to relate to requiring the requesting side to do more work to dig into the guts of a message when HTTP says something is "OK". Thomas and Eve agree with George in protesting this as a layer violation. However, we're in agreement that, with fully mature RESTful interfaces, an HTTP failure when you're trying to PUT something (like a requested scope) makes sense.

We got consensus on the following TOC:

- x.1 Requester approaches host to attempt access to a protected resource
  - x.1.1 If requester has no token or token is invalid, host responds with token-getting information (*cross-ref to embedded x.2*/x.2.1 interaction if requester presented a token that turns out to be invalid)
  - x.1.2 If requester's token has insufficient scope, host responds with authorization request information (*cross-ref to embedded x.2 and x.3 interactions*)
  - x.1.3 If requester has a token with sufficient scope, host gives access (*cross-ref to embedded x.4 interaction*)
  - x.1.4 If access request is ambiguous with respect to the specific user at the host, host responds with ambiguous-user error
- x.2 Host requests token validation from AM
- x.2.1 AM gives token-invalid response (*these don't strictly need to be sub-sub-sections*)
- x.2.2 AM gives token-valid response
- x.3 Host does requested-scope registration with AM
- x.4 Requester asks AM to grant authorization for scope

Thomas will indicate clearly in the spec where we:

- Pull in OAuth by reference (obvious)
- Copy OAuth patterns (indicate the delta)
- Veer off precipitously

We made some changes and additions to the 'pad on the call.

Eventually, once we're able to profile JWT for our uses, the token can contain enough information to identify a user, which could theoretically solve the problem of the requester approaching the host and attempting to access a resource that is "shared" among several users (such that the access attempt may be ambiguous wrt the specific user at the host). Without that, UMA is making a very large simplifying assumption that the nature of the access attempt can do this disambiguation for now.

Next Meetings

- No WG telecon on Thursday, 5 May 2011, due to IIW 12
- WG telecon on Thursday, 12 May 2011, at 9-10:30am PT (time chart)
- WG telecon on Thursday, 19 May 2011, at 9-10:30am PT (time chart)
• WG telecon on Thursday, 26 May 2011, at 9-10:30am PT (time chart) – Eve regrets; can Maciej do agenda, chair, and do notes-wrangling?