UMA telecon 2011-10-27

UMA telecon 2011-10-27

- Date and Time
- Agenda
- Attendees
- Minutes
  - New AI summary
  - Roll call
  - Approve minutes of 2011-10-13 and 2011-10-20 meetings
  - Action item review
  - Upcoming timeline and IETF/OAuth news
  - Status of implementations
  - UMA core spec (new permanent location) issues
- Next Meetings

Date and Time

- WG telecon on Thursday, 27 Oct 2011, at 9am 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 2011-10-13 and 2011-10-20 meetings
- Action item review
  - Upcoming timeline and IETF/OAuth news
  - Considering doing another webinar – got a request for another one, which should cover "privacy, mobile applicability, and incorporation of the cloud"
  - Impact of 2012 budget requests
- Status of implementations
- Trust Model next steps
- UMA core spec (new permanent location) issues
- AOB

Attendees

As of 20 Oct 2011 (post-mtg), quorum is 8 of 14.

1. Mohammad, Alam
2. Bryan, Paul
3. Fletcher, George
4. Maler, Eve
5. Wray, Frank

Regrets:

- Catalano, Domenico

Minutes

New AI summary

- Eve: Send kickoff email proposing a new UMA webinar date, content, and other action items, taking into account expressed desires for topics covering "privacy, mobile applicability, and incorporation of the cloud".
- Thomas: Implement the result of issue #3, now reopened in case there are questions, and other conclusions from 2011-10-27 telecon.
- Eve: Reach out to Frank, Sal, Susan, Kevin, and Domenico to get a trust model best-practices doc started.

Roll call

Quorum was not reached.

Approve minutes of 2011-10-13 and 2011-10-20 meetings

Deferred due to lack of quorum.

Action item review

- 2010-11-18-4 Eve Open Capture new user stories in the wiki.
- 2011-09-22-4 Various Ongoing Build list of FAQs on the wiki. Lukasz owes a SMART project FAQ.
- 2011-09-29-1 Frank, Sal, Dom Open Examine loci of LOA/LOC/LOC implications in the Trust Model doc.
Paul has been busy taking flak on his other JSON-related specs 😞, so he hasn't worked on the CRUD one yet. His ongoing RESTful API design work, including UMA, has informed this whole process. He may put some or all of this on a solely informational RFC track. The idea is to codify common patterns. We discussed CouchDB vs. MongoDB; the former can be deployed on mobile but the latter gets more attention.

### Upcoming timeline and IETF/OAuth news

On the OAuth list, the rechartering discussion has continued. UMA’s mechanism of dealing with scopes and permissions is richer than OAuth's, and there's perhaps some support for adding that type of structure. We still don't know exactly which pieces, if any, of UMA might truly be a candidate for sedimenting.

Regarding dynamic client registration, there has been some movement in recent weeks, and some independent innovation around client instance registration specifically. Travis Spencer's idea uses push notification in a clever fashion as a key component to achieve this. Eve's level of confidence that we can point off to a suitable solution in the near-ish term is rising.

Does it make sense to plan another webinar? We could put the emphasis on showing multiple implementations and OpenID Connect integration. There is high interest in this. Alain thinks he may possibly be able to supply screenshots towards this end, but he can't do a live demo due to a variety of constraints. Frank is interested to be one of the co-speakers, talking about his interest.

### Status of implementations

Eve is collecting more implementation status, so as to update the Implementations wiki page and add some FAQs.

#### UMA core spec (new permanent location) issues

George has a concern about the host's new REQUIREment to let a requester in if the permissions are correct, even if it sniffs something wrong with, say, the requester's IP address. Originally we’d said SHOULD. There are a couple of arguments you could use for making the SHOULD case: For one, the host may be under the constraints of mandatory access controls that would militate against giving access despite the advice from the AM. For another, this takes away the host's ability to do risk-based assessments. Ultimately, hosts need to mitigate their very probable real-world liabilities if something was obviously wrong about the access attempt. The rationale for a MUST is that any MACs (vs. discretionary access controls) are at a layer other than the UMA layer. George points out that REST collapses all layers into one, in a sense. The host could respond in those cases with 403, or 500. If a host elects to deny access according to its own judgment in opposition to the AM's response of a perfectly valid token with perfectly valid and active permissions, or even prior to talking to the AM in the first place, perhaps we should say that the host is free to give any HTTP error that suits the circumstances.

Should we distinguish between transient errors and fatal errors? This would provide a hint to the requester about what else to try, vs. telling the user "Sorry, what you were trying won't work." HTTP's errors do have some semantics around this. Client errors generally mean that the client did something wrong, and they should try again and do it right. 503 (Server Not Available) is another example of an obviously transient (retryable) vs. fatal (non-retryable) error.

We have consensus to move back to a SHOULD basis for this language, ideally providing an explanation about how the host is still at liberty to control its own access control policies as long as they're tighter than the AM's.

This closes issue #15.

We discussed issue #24. George points out that this whole proposition only makes sense with our current opaque-token option, since if the host received a structured token and validated and looked at it fully locally, the AM wouldn't have a chance to know the host's intent. A back-channel call to inform the AM of the host's intent would be antithetical to the reason why you'd want to use structured tokens in the first place: performance. However, the AM would still have an audit trail because it minted and signed the token in that case. And the host will have ecosystem pressures against it if it does provide access inappropriately.

Maybe, given the fact that we still cater to the opaque-token case, we could make it an optional property that the host can supply in asking for token status from the AM. They'd have to supply a scope (sort of a permission template), not an actual permission. What the AM would supply in return is an actual permission.

Let's give this a try in the spec.

### Next Meetings

- WG telecon on Thursday, 3 Nov 2011, at 9am PT (time chart) – NOTE: UK and Europe have changed their clocks so this will appear one hour earlier than usual to participants in those locations
- WG telecon on Thursday, 10 Nov 2011, at 9am PT (time chart) – NOTE: back in sync on most apparent time differences around the world – ALS O NOTE: – Eve regrets; who will serve as chair pro tem?
- WG telecon on Thursday, 17 Nov 2011, at 9am PT (time chart) – NOTE: Likely Eve regrets; who will serve as chair pro tem?
- NO WG telecon on Thursday, 24 Nov 2011 – U.S. Thanksgiving holiday
- WG telecon on Thursday, 1 Dec 2011, at 9am PT (time chart)