UMA telecon 2010-06-17

Date and Time
- Thursday, 17 Jun 2010 at 9:00am-10:30am PT (time chart)
  - Skype line "C": +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214

Agenda
- Administrative
  - Roll call
  - Approve minutes of 2010-06-10 meeting
  - Action item review
  - Review telecon times: hold some focus group meetings at 7am PT to help participants residing in Japan?
  - UMA guest blog post
  - Authz workshop plans at Catalyst July 26-30?
  - Anyone attending IETF meeting in Maastricht July 26-30?
  - Anyone attending PII in Seattle in August?
  - Any interest in holding UMA F2F at Kantara plenary in Paris Oct 19-21?
- RRAPI and other UMA-specific parts of Step 1
- OAuth-generic dynamic client registration proposals
- Plan for making progress on Steps 2 and 3
- OpenID/AB review? (if AB reps are on the call)
- AOB

Attendees
1. Adams, Trent
2. Fletcher, George
3. Hardjono, Thomas
4. Holodnik, Tom
5. Machulak, Maciej
6. Maler, Eve
7. Moren, Lukasz
8. Scholz, Christian

Non-voting participants:
- Joe Andrieu
- Nat Sakimura

Guests:
- Anna Ticktin (staff)

Regrets:
- Catalano, Domenico

Minutes

New AI summary
• Christian, Eve: Work on the conversion of the core spec and the dynamic registration spec to xml2rfc.

Roll call
Quorum was reached.

Approve minutes of 2010-06-10 meeting
Motion to approve minutes of 2010-06-10 meeting APPROVED.

Action item review
• 2010-03-10-6 Joe Open Revise the protected inbox scenario for next week’s call. Joe has enhanced the scenario. This is now closed.
• 2010-05-13-3 Christian Open Spec out a "requester metadata" flow. Let's assume this will get done in the fullness of time.

Review telecon times
Eve suggests an occasional or regular focus meeting at 7am PT. Nat thinks that could work on Wednesdays, and Christian agrees this could work as long as it's not too regular.

Let's meet next Wednesday, June 23rd, at 7am PT, and then schedule them ad hoc from there. We can use Line C.

UMA guest blog post
Eve has an opportunity to write a guest blog post for Eran's site. George has interest in reviewing such a post. Eve will likely draft it next week, and may use the "doorman" metaphor she'd proposed earlier:

"User-Managed Access builds on OAuth to take Web data sharing and service access to the next level. If OAuth lets you hand out valet keys to your Web resources, UMA aims to give you a resource doorman – on duty 24/7, handling requests according to your strict instructions, and able to give you a full report whenever you wander through the lobby."

Joe notes that the metaphor breaks down in that the doorman protects multiple buildings! But he likes it.

Catalyst July 26-30
We still have no one able to attend and speak on UMA at the authorization workshop. Paul Madsen will likely touch on the subject in his talk.

IETF meeting in Maastricht July 26-30
No one is currently planning to attend.

PII 2010 conference in Seattle in August
Eve is scheduled to appear there and speak on UMA-related topics. Perhaps we can try to do a F2F there? Trent is likely to be attending as well.

Kantara conference in Paris Oct 19-21
We should be mostly done with our work by then, perhaps even having submitted I-Ds to the IETF! So we're not sure we need to reserve an UMA WG meeting time there.

Trent will be in attendance at the conference; Christian may be; Eve doesn't know. Joe may be there for InfoSharing, and George has a slight chance of attending.

OpenID/AB review
AB is essentially an OpenID layer on OAuth2. Nat has just submitted an I-D to the OAuth WG covering the basic "artifact" proposition, which has the OpenID RP receiving an artifact (which is a URL) that it can then dereference to get a JSON file representing the OpenID parameters of interest to it. There is also a request artifact, to allow the OP to use an artifact to get RP information.

The RP's "request file" (a metadata file) can be signed for an extra level of authentication of the RP/client. If HTTPS is used to retrieve the metadata, you already have a level of authentication.

The "artifact" pattern of pulling metadata is something we can use for host-AM and requester-AM interactions.

Eve wonders if the struggles we've been having with person-to-person sharing ("bob@gmail.com can read this resource") could be addressed by some of the AB work, particularly the OpenID-flavored attributes asserted about the requesting party (and particularly if they're signed). We think there's three user interaction patterns that are likely:

• Due to some kind of existing session that would satisfy the AM's request for a particular identity claim, requester app can generate a suitable claim for the requesting party as bob@gmail.com
• Requester app can do an OpenID-like process to send the requesting party off to authenticate "live" and get an assertion it can pass along as a claim to the AM
• Requester app can redirect the requesting party along to the AM to get rerouted again to the correct OpenID Provider to get authenticated "live" to the AM's satisfaction
Nat believes AB could be used for all three. He will put together some diagrams showing how. Nat points out that identity tokens of this sort are also going to be needed for many kinds of contract, since you need to uniquely identify a party in a known namespace. Signed assertions that (as Thomas observes) came with proof of possession are going to be an important part of many of the UMA solutions. Eve pleads for retaining lower-security and lower-liability use cases by not requiring signing in all cases; we've learned from our legal subteam discussions that although clicking "I Agree" buttons isn't the ultimate in liability assignment, it's also not entirely without power. Tom agrees that signatures have a role in high-value use cases (launching a rocket!) but crypto is also expensive to make people do.

AB also has a solution that Nat believes could be applied to the hData scenario; let's discuss that in the focus group meeting next Wednesday.

Nat points out that the RP/client/requester's metadata could be statically signed, which eases the key management burden. And Eve suspects that higher-value use cases will find it easy to live up to such requirements. Although private key management has never gotten any easier, public key distribution seems to be getting easier through tricks like XRD/JRD, webfinger, and so on.

Tom asks: Can we document the use cases where we think the signature solution is going to be required and acceptable? Nat notes that the OpenID Contract Exchange spec has a notion of a subject and a signatory that is acting as an agent for the subject (e.g. a requesting user).

**RRAPI and other UMA-specific parts of Step 1**

- **Christian's experimental version**

Anna started looking into bitbucket, and will be doing further research with Joni on it today. Christian suggests github too. He plans to work directly in the xml2rfc format to prepare us for submitting our specs to IETF, and one of these two solutions is needed for that vs. the Confluence system. (They also allow for easier collaborative editing and branching.) Eve's main constraint is that we'll only allow people who have signed the KI participation agreement to edit docs. Joe also wants to be sure that we can track who edited what; this will be recorded in the list of spec authors as we go.

We discussed the material under the "host registers resources with the authorization manager" header.

He's currently using JRD, since indeed we're "describing resources". George likes the use of titles, since this can really help from a UI perspective.

Christian wonders if the RRAPI should really be a "scope registration API". Eve agrees that this would be a good idea; let's plunge into defining scopes somehow. This will, of course, impact steps 2 and 3 in various ways. But how will this format work in the case of "not-very-RESTful" scopes? George points to AOL's scopes as an example.

For scope and policies, there are going to be some things the AM could offer an authorizing user "generically", like length of access granted to a requester, "let this group of family members get access to this" (ACLs), etc. But if the host can convey to the AM some specialized info about domain-specific scopes, such as printing vs. viewing photos (these are photo-specific rather than generic to any resource), then the AM can naively pass these along as policy options to the user. And then the resulting access token could stand for the authorized scope whatever it is.

Christian has experimented with assigning unique URL endpoints at the AM for each of the resources (scopes?) registered by the host. This could be useful later; we will see.

**Next Meetings**

- Focus group meeting on Wednesday, 23 Jun 2010, at 7-8am PT (time chart)
- WG telecon on Thursday, 24 Jun 2010, at 9-10:30am PT (time chart)