UMA telecon 2012-03-08

UMA telecon 2012-03-08

Date and Time

- WG telecon on Thursday, 8 Mar 2012, at 9am PT (time chart)
  - Skype: +99051000006481

Agenda

- Roll call
- Approve minutes of 2012-02-23 meeting
- Tweet chat planning
- Interop planning
- Work through issues
  - Issue 49 (ad hoc meeting report, discussion, resolution, editor instructions)
- Review any additional open action items
- AOB

Minutes

New AI summary

Eve and Thomas: Edit the spec and add swimlane diagrams showing flow options. (Meet on Friday.)

Roll call

Quorum was reached.

Approve minutes of 2012-02-23 meeting

Minutes of 2012-02-23 meeting APPROVED.

Issue 49

See relevant information:

- Notes from yesterday’s ad hoc meeting
- Łukasz’s description of the current spec vs. a proposed solution: email
- Jacek’s description of SMART’s authz code-based solution for the requester side, and George’s proposal for a solution: email thread
- Domenico’s diagram of the human parties: email
- George’s final post-meeting diagram

In George’s initial diagram, the “Access Alice’s calendar with no token” means “with no RPT”. His flow imagines that there is a new separate step where an empty RPT is issued, which would then require the requester to go back a bunch of times to get a RAT, get an RPT, start filling it with permissions, etc. This doesn’t seem right, since the host shouldn’t care whether the requester has a RAT or even an RPT yet when it tells the requester that it needs an UMA permission to get to this resource.

What if MyCalendar gets and conveys a permission ticket in all circumstances where there’s insufficient permission (no token, invalid token, token with insufficient permission)? Then TripFollwr would be sent to the AM to rectify the situation regardless. Is there any danger in the permission ticket getting out into the wild? We can’t see any, just as we couldn’t before. It’s a permission request ticket, not a permission ticket per se. Currently the host doesn’t include anything identifying the requesting side in its permission registration process at the AM anyway (Section 3.4).

Once Roger/TripFollwr is told by MyCalendar that it needs to go to CopMonkey to get an RPT, TripFollwr could independently recognize the fact that it doesn’t have a RAT yet for Roger with CopMonkey, and request it directly. So even though it has a permission ticket, it can’t quite use it until it has a RAT in hand, and then it can go about trying to win the permissions it needs.

It seems very logical to get MyCalendar entirely out of the job of handling or caring about RATs, since it’s not a party to that token (so to speak). So it’s not just syntactic sugar/optimization to embed RAT issuance in the process of permission requests; it’s an appropriate time and place with the appropriate parties at the table. Would it be possible for the permission request process to leverage any claims CopMonkey happened to collect while issuing the RAT, so that Roger isn’t unnecessarily inconvenienced? We think so.

We really like the full separation of authentication and authorization. We have now fully mirrored an OAuth flow on the authorizing and requesting sides.

We edited George’s diagram dynamically on the call; the result is here. We achieved consensus on this new approach, which will require a fair amount of spec work:

- Terminology distinctions between tokens
  - Instead of HAT and RAT, let’s use “protection API token” and “authorization API token”
- Terminology cleanup around permission registration
  - What’s being registered is a pending permission request, not an entitlement/permission per se
• Authorization code (or other "three-legged") flow for the AAT instead of client credentials
• Flow changes in Section 3 to reflect:
  • The issuance of a permission request ticket in all cases where the RPT won't suffice for resource access
  • The embedding of the step where an AAT gets provisioned if it didn't yet exist

Let's close issue 49.

Next Meetings

• WG telecon on Thursday, 15 Mar 2012, at 9am PT (time chart)
• WG telecon on Thursday, 22 Mar 2012, at 9am PT (time chart)
• WG telecon on Thursday, 29 Mar 2012, at 9am PT (time chart)

Attendees

As of 28 Feb 2012, quorum is 6 of 11.

1. Catalano, Domenico
2. D'Agostino, Salvatore
3. Fletcher, George
4. Hardjono, Thomas
5. Machulak, Maciej
6. Maler, Eve
7. Szpot, Jacek

Non-voting participants:

• Cox, Kevin

Regrets:

• Koot, Andre