UMA telecon 2009-08-13

UMA telecon 2009-08-13

Date and Time

This is a Focus meeting.

- Day: Thursday, 13 August 2009
- Time: 9-10:30am PDT | 12noon-1:30pm EDT | 16:00-17:30 UTC (time chart)
- Dial-In: +1-218-862-7200
- Code: 987-632 (do not press "#")

Attendees

- Akram Ibne, Hasan
- Hanson, Michael
- Henderson, Iain
- Hodges, Jeff
- Lizar, Mark
- Machulak, Maciej
- Maler, Eve
- Nagelberg, Alan
- Scholz, Christian

Regrets

- Bryan, Paul
- Smith, Bill

Agenda

- Roll call
- Approve UMA telecon 2009-08-13 minutes
- Action item review
- Confirm future meetings’ time slot and length
- Review leadership team nominations and electronic ballot process
- Collect any budget request ideas
- Scenario and use case review
- Collect expressions of implementation interest

Minutes

Roll call

9 of 26 participants attending. Quorum not reached.

Approve UMA telecon 2009-08-13 minutes

Deferred to a "quorate" meeting (or an electronic ballot if they start stacking up).

Action item review

All items from the last meeting were closed.

Confirm future meetings’ time slot and length

We agreed that a 60-minute call length is sufficient. We also decided that we'd have meetings weekly, but that we would alternate "quorate" meetings (everyone tries to attend and we can get any formal business done) and "focus" meetings (we dig deeply into technical work and the leadership team is expected to attend at a minimum).

Today's meeting was a "focus" meeting, so next week is a "quorate" one.

There may not be critical mass for a real September F2F meeting in Las Vegas. We might have more of a BOF there instead.

Review leadership team nominations and electronic ballot process

The formal Editor role may include contributing content, but also includes "riding herd" on other contributors. Everyone who has scenarios and use cases to contribute is encouraged to edit the document directly, but if they don't want to or can't, they can contact the Editor for assistance or send proposals directly to the list.
Collect any budget request ideas

Iain had suggested two ideas in email, which we discussed on the call:

- Funding for prototyping work
  In the past, Liberty had funded some open-source prototyping work up to $15,000. We anticipate getting some private prototyping efforts under way anyway, but maybe this sort of funding could supplement.
- Funding to help contribute to the proposed consumer research
  The VPI, eGov, P3, and Consumer Identity groups have already expressed an interest in this. A proposal is already being worked on, for serious studies that could approach US$150-200K in total for Kantara. Mozilla Labs has launched a Test Pilot group, which collects end users who are willing to test out features. It wouldn't be a formal user behavior study, but such volunteer labor could help with many areas of consumer research.

Scenario and use case review

Christian has added a Distributed Social Networks scenario to the document. The "service catalogue" concept sounds a lot like XRD; are they the same? Not entirely clear if the communities are all fully engaged with each other.

What might be unique about a use case for this scenario is that the "requesting service" might be approaching a "discovery agent" first rather than the SP ("responding service"). Michael asks what relationship the "discovery agent" and the "authorization agent" should have, and, if they're separate, which direction their conversations flow.

The "social" part of this scenario doesn't seem like the unique aspect; it applies to all sites, not just social ones. (Perhaps we'll add a "contact book" service-specific scenario later, which adds the notion of building access control lists out of contact entries.)

This scenario, along with others, will highlight the need to modularize policy expression away from authorization decisions. Today, OAuth has very coarse granularity (binary). The sentiment does indeed seem to be that the "Policies Specific to the Web Resource Type" issue should defer too many application-API-specific or resource-format-type semantics. Can we just do some very generic RESTful profile that covers, say, obvious GET and POST semantics, and then combine it with the SP's ability to RESTfully assign a resource to each filtered version of the content?

We discussed the proposition of having the SP convey to the AM a manifest of managed resources, including human-readable and possibly machine-readable labels.

ProtectServe has chosen, so far, to design a flow whereby the AM has to be pinged reasonably frequently (nearly every access episode). By contrast, something like OpenID CX has more longer-lived tokens. We need to find scenarios and use cases that illustrate our need to either have the AM reach out to the Consumer, vs. the need to avoid frequent AM-in-the-loop decision-making. This also has second-order impacts on how much of an audit log the AM can maintain: requests for access, or actual incidences of access?

Eve reviewed the first two "master" scenarios (calendar and photo set). We're going to need a scenario that highlights the possibility of selling data access. The DataPortability TOS work defines, e.g., terms that cover import and export rights. "Open arms", "ever fresh", and "graceful exit" describe various terms of service they've defined. See their draft proposal. Sites could use the associated logos to advertise their capabilities to users, such that users with particular data-sharing requirements could find sites with particular abilities to accept those terms.

Collect expressions of implementation interest

Iain of Mydex, for one, expressed interest.

Next Meeting: Quorate

- Day: Thursday, 20 August 2009
- Time: 9-10am PDT | 12noon-1pm EDT | 16:00-17:00 UTC (time chart)
- Dial-In: +1-218-862-7200
- Code: 987-632 (do not press #)