UMA telecon 2013-06-13

UMA telecon 2013-06-13

Date and Time

- **Focus** meeting on Thursday, June 13, at 9am PT (time chart)
- Skype: +9905100000481

Agenda

- (Get on join.me)
- Action item review
- Spec issues review and resolution: #83
- RS=C optimization opportunities
- Review proposed "ox" claim profile
- Discuss testing needs: test harness? other?
- AOB

Minutes

Terry founded a research and advisory firm in the identity area. He feels user-controlled access is immensely important. He has multiple large clients trying to figure things like this out.

Action item review

Done. Next week he'll be able to report on the early-pilot phase that they're entering with the Gluu stack. He's had interest in gathering support to do additional pilots. Keith has no cycles for this, but we can ask around.

Spec issues review and resolution

Issue 83:

One scenario is that Bob views Alice's photo without having "copied" it into his own area where he has full RO rights. Another is that Bob copies the photo, thereby gaining full (potentially inappropriate) RO rights. If Bob offers a claim that means he agrees to constrain his own downstream sharing, then this puts the second solution firmly into the realm of our binding obligations. For example, Eve goes to Flickr and logs in, and finds George's public photo of a flower. Flickr shouldn't enable Eve to set CopMonkey resource protection over George's photo. George cautions against being too prescriptive; there are circumstances where Alice might want to award Bob something like "admin" or "access management" permissions, so that even if Bob was the initial resource owner/authorizing party, he might be a downstream one. Andrew asks: How is "protectable resource" as in Sec 2.3.1 of Binding Obs defined? It's not, yet!

Does this really need to be specified, or is this simply the definition of what a "resource server" is? It's responsible for mapping resources to their rightful owners and controllers. UMA just lets it outsource protection (the mapping of access control rules to access actions). Maciej points to Puma's conceptual diagram that demonstrates the essentiality of what web apps have to do in terms of mapping protectable resources to logged-in owners. But Andrew's point about "protectable resources" not being defined is a good one. OAuth's definition of "resource owner" (which we borrow from, in part) is pretty good, but OAuth doesn't define "protected resource". What we may need is a definition for the resources that are capable of/candidates for being protected by a legitimate resource owner. The PAT that the resource server chooses to make the resource set registration call to the authorization server is exactly the mapping that the RS has chosen to make to a particular resource owner.

What we haven't decided is whether this is so obvious as to not require technical or binding obs wording, or whether we should add wording to clarify.

No decision yet.

RS=C optimization opportunities

Maciej points out that the old Delegating Access Management to Custodians scenario is very similar to this. Could George use this as a basis for experimenting with some optimized swimlanes?

RS=AS optimization opportunities

Mark brings this up as an area of interest. The AS could easily issue itself an RPT and authorization data. He is working in the Netherlands on a project for secondary education (ages 16-18). The Delegating Access Management to Custodians scenario is valuable here as well.

CIS meeting opportunities

Eve and possibly George can join a "working summit" to be held (in circumstances TBD) during Cloud Identity Summit on Tuesday, July 9. If you were on the fence about attending, hope to see you there!

Review proposed "ox" claim profile

Deferred.
Discuss testing needs: test harness? other?
Deferred.

Attendees
- Eve Maler
- Maciej Machulak
- George Fletcher
- Terry Gold
- Andrew Hughes
- Keith Hazelton
- Thomas Hardjono
- Lukasz Moren
- Mark Dobrinic

Next Meetings
- **Focus** meeting on Thursday, June 20, at 9am PT [time chart] - GPII early-phase news
- **All-hands** meeting on Thursday, June 27, at 9am PT [time chart] - George regrets
- (No meeting - vs. potential F2F/summit during CIS - on Thursday, July 11?)