UMA telecon 2013-03-21
UMA telecon 2013-03-21

Date and Time

- Focus meeting on Thursday, Mar 21, at 9am PT (time chart)
  - Skype: +9905100000481

Agenda

- Action item review
- Review/discuss any progress on profiling UMA/OIC for optimized Alice-to-Bob workflows
- Review/discuss Keith's work on NSTIC-flavored case studies and UMA-protected OpenID Connect, as available, and comparison work
- Review/discuss Eve's API authz case study (added here as a forcing function)
- AOB

Minutes

Action item review

Are we at a point to try interop tests again? Cloud Identity Ltd has very little time available, but is theoretically interested in participating. Let's prioritize interop testing and generating implementation-based spec issues higher in our work stream.

Thomas is beginning to prioritize the higher-ed profile work more highly. The other potential MIT Media Lab participant he was thinking about is out of pocket in Europe for a couple of months, so it's just Thomas working on this. Eve will point Thomas to the email thread in which she proposed substantive profiling efforts/contents, which he can use as a kind of checklist. The acid test would be: Could someone pick up his profile and one of the open-source implementations, and rough out a POC solution that can be tested and can drive profile improvements?

Keith may want to take a fresh look at his draft case study on Managing Accessibility Needs and Preferences, to revise as necessary now that he's found the right partner to test it out.

Thomas will look at his spec-editing AI.

Keith is waiting with bated breath to install the Gluu stack to look at the UMA tests (and also to look at its SCIM implementation!).

Review/discuss any progress on profiling UMA/OIC for optimized Alice-to-Bob workflows

Eve tried to set up an ad hoc meeting; Nat is so busy that he's the only one who hasn't responded! Eve will create a meeting without Nat, hoping that John's presence will compensate at least partly.

Review/discuss Keith's work on NSTIC-flavored case studies and UMA-protected OpenID Connect, as available, and comparison work

The "UMA-protected OIC" scenario and particularly its "personal discovery" characteristics were last discussed in February. There's a couple of sub-scenarios for "UMA-protected OIC": One is Alice-to-Alice ("normal" OIC where Alice herself is starting a login session on some client app), and Alice-to-Bob ("extended" OIC or claims-extended UMA, which Domenico has created many wireframes for and which SMARTAM has implemented).

OpenID Connect today specializes in 1) ensuring that Alice's claims are protected and that she gets to consent to their sharing with some app, and 2) enabling Alice (herself, again) to log in to that app as a "client" of the source of the claims. In other words, OpenID Connect is mainly a SSO protocol, which also allows login-time transfer of attribute (claims) for the relying party to function correctly. As an aside, since OpenID Connect is also a species of OAuth, it may enable post-login-session retrieval of attributes (claims) once Alice has logged off.

What we're imagining with "UMA-protected OpenID Connect" could be one of two totally separate things:

1. Alice is still the user who is trying to log in to some relying party, but instead of using "plain vanilla OAuth" for that relying party/client app to access her claims, the claims are protecting by a super-duper version of OAuth which is really UMA. In this case, the way Alice would have protected those claims is not by consenting at run time to their sharing (at least in the normal OAuth fashion), but by setting policies that let the client (and its user = Alice) get all the way through to the claims successfully. Today, if this were put in place without any optimizations, the process would feel to Alice to be similar to how OAuth works, only it would unfortunately have an extra step: the AAT issuance step. We hope to optimize this away in some fashion through the conversations with the OIC experts.

2. Alice has some claim that she's willing to share with Bob, such as a flag indicating whether a certain medical test result was positive or negative. So Bob is the one who uses some client/"relying party" app in trying to access Alice's claim, which is UMA-protected. Today, OIC doesn't really do this at all. This is what Nat was exploring in his blog post, but his imagined workflows are currently neither correct UMA nor today's OIC. And again, if they used today's UMA, they would have to include some extra steps/clicks such as the AAT issuance step, which is a drag. (Eve digressed to describe the PAT/AAT/RPT token ecosystem that underlies UMA; basically, the AAT is client-app-centric and the RPT is requesting party-centric. Thomas's comment on Nat's post fleshes out why this is important.)

Based on this conversation, we went into a philosophical discussion and "performance art" about NSTIC, government funding and its value, the competitive landscape in which UMA plays, and whether enterprise or "user-centric" scenarios will see adoption first. While we're seeing enterprise takeup in the form of Gluu's work, perhaps the time is now for the NSTIC-esque use cases, since the world has been explicitly working on solving what everyone agrees is the same problem space for years. We sense urgency in solving this soon, "our way". See Eve's 2008 slide deck, which predated ProtectServe. 😊
Eve's goal: Do the same kind of optimization exercise that OpenID 2.0 and OAuth 1.0 underwent in the beginning, to reduce inefficient flows, so that UMA is fully ensconced within both SSO flows and entitlements flows.

Review/discuss Eve's API authz case study (added here as a forcing function)

This will be based on the Gluu demo and the scenario notes. Hey, let's call it Entitlements 2.0.

Attendees
- Eve
- Thomas
- Keith
- Domenico
- Andrew
- Adrian
- Maciej
- Sal

Next Meetings
- All-hands meeting on Thursday, Mar 28, at 9am PT (time chart) - look at issues list and prioritize; work up a more formal completion roadmap