UMA telecon 2014-01-23

Date and Time

- Focus meeting Thu Jan 23 8:30-10am PT (time chart)
- Voice: Skype: +9905100000481 or US +1-805-309-2350 (international dial-in lines), room code 178-2540#
- Screen sharing: http://join.me/findthomas

Agenda

- Review Feb meeting schedule
- UManitarian gathering opportunities
- New Core draft 09b (now uploaded) for consideration as stable “implementor's target” draft
  - Any other issues worth discussing: on GitHub? claims-gathering redirect requirement?
- Other interop planning and uma-dev news
  - Upcoming calls
  - IDESG healthcare RLS use case slides: next steps?
  - Wikipedia corrections
  - Discuss next stage of authz/binding obs work
  - Webinar planning
  - Twitter team planning
- AOB

Minutes

Core 09b

We looked at the new draft. In email, Mark noticed a typo in Security Considerations: "attribute".

We think the profile titles need some work. “Alternate” isn’t really true because nothing is being substitute in (yet – a further third-party profile might do that). These are merely exceptions to the standard protection (or whatever) API. What if we called it, e.g., a Protection API Opt-Out Profile? There’s also the concept of swapping in an alternate communications channel, which is what someone would have to build on this set of opportunities.

What about Extensibility Points? The Protection API Extensibility Profile? Then any third-party profiles that come along to swap in something specific could be called a Protection API Extension Profile for (some purpose).

Maciej remains concerned about readability of the spec as a whole, but we think we’re generally agreed that it wouldn’t help to put a cross-reference to the new profiles everywhere that an API-based interaction is mentioned in Sections 2 and 3.

What about the idea of softening the MUST in Section 3.5.1 about requiring the client to redirect the human user to the AS? George notes that leveraging an “ID token” (or its moral equivalent) is something he proposed a long time ago, and we’ve seen clients using these types of tokens in initial UMA use, without redirecting the requesting party. But the challenge is the chain of trust – is there a shared session that lets this bearer token suffice? Essentially, you have to trust the client sufficiently to convey these claims. OpenID Connect tried to build this into the token but couldn’t get very far in practice. The strongest method would be something a signed or encrypted JWT that only the recipient could unpack/verify and that was directed to that specific audience.

What if we backed off of the MUST, but require claim profiles to state the basis for trusting any client to provide claims itself vs. redirecting the requesting party? Any claim profile that does redirects would need the listed capabilities (redirect URI, callback URI, and state), but a claim profile that doesn’t do redirects wouldn’t need this.

We have examples both in the enterprise world (Gluu) and the user-centric world (Cloud Identity) where the client may already be in possession of claims in the form of some kind of ID token.

Mike elucidates three use cases he’s noticed:

1. UMA AS is OpenID Connect RP (the claim profile we’re already defined – which was defined as the most “naive” and webdev-friendly way to gather claims)
2. UMA C is trusted and was an RP of some other federated interaction (could be SAML or OpenID Connect or whatever)
3. UMA AS is a SAML SP/RP

Gluu is currently doing #2, with OpenID Connect. There’s even a profile written for it. It’s only interested in #3 in a tactical sense, if their customers request it.

Should we consider a name change for the OpenID Connect claim profile and its config data keyword? The real differentiator in each case of a profile seems to be a) what role is the claim gatherer and b) what method does it use to gather the claims and what format it uses to express them. George notes that if the person at the client happens to already have a relationship with the AS, then the AS might have already independently gathered claims previously and could reuse them. (The currently defined OpenID Connect claim profile sort of does this, in that the AS can cache claims. We should move that discussion in the spec to this claim profile.) Note that the definition of an AAT encompasses the presumed right of the AS to be a claims-gatherer, but whatever claim profiles are being used in any one deployment might not exercise that right.

Our reasons for having written the Core spec claim profile we did include:
Demonstrating a good way UMA and OpenID Connect could be used together
Ensuring that clients could remain as "dumb" as possible, putting the onus on the AS to gather claims
Providing a concrete-enough answer for claims gathering in the spec to enable experimentation by implementors
Having a sample claim profile in the Core spec, as an example

Do we want to add a "Trusted Client Claim Profile" to the Core spec? Does saying "trusted" go too far? The generic description would be something like "Client Gathers Claims", with the particular technology choice in Gluu's case for #2 being OpenID Connect. If we did add it, the current claim profile's name and keyword are awkwardly too-broad. Would it be a popular profile? It probably depends on the trust environment around ID tokens, but it would really improve the user experience. So "trust" does seem to apply as a descriptor here. Maybe a "Client Conveys Claims (with technology)" naming pattern? "Authorization Server Gathers Claims (with technology)"?

Changes agreed to:
- Soften MUST around redirects, and just say that if a redirect is used, it MUST have the redirect integrity elements provided.
- Suggest that client-dependent profiles need to state their basis for trust
- Propose new claim profile and keyword for trusted client
- Propose new name and keyword for existing claim profile

AI: Thomas and Eve: Implement claim profiling changes agreed to on telecon 2014-01-23 in Core 09c.

Wikipedia
AI: Eve: Edit the text for the English entry.
AI: Rainer: Edit the German entry based on the English revisions.
AI: Sal: Find a person to write a Japanese entry based on the English revisions.
AI: Domenico: Edit the Italian entry based on the English revisions.

Webinar planning
Let's target mid-March, after SXSW. There will be an UMA dinner at SXSW, on the Monday night! It will be across from the Sheraton, and Gluu is providing dinner. This will be invitation-only, to cut down on spam.

February WG meetings
Please note that we won't meet on Feb 6. See below and the UMA online calendar for details.

Attendees
- Eve
- Łukasz
- Domenico
- Sal
- Maciej
- George
- Mike
- Jin

Regrets:
- Thomas
- Mark
- Andrew
- Adrian
- Roland

Next Meetings
- All-hands meeting Thu Jan 30 8:30-10am PT (time chart)
- No meeting Thu Feb 6 (Eve regrets)
- Focus meeting Thu Feb 13 8:30-10am PT (time chart)