UMA telecon 2014-01-02

Date and Time

- Focus meeting Thu Jan 2 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

- Discuss Mark’s proposal for AS=C spec text
- Discuss "complex resources and scopes" idea (from convo with Hideki)
- Discuss healthcare use case next steps
  - Dedicated group/subgroup in some other venue?
- Plan demo video, interop, and webinar calendar in Q1
  - PCloud video
  - PHealthCloud video
  - UMA for Enterprise webinar idea
  - Virtual interop activities
- AOB

Minutes

UMA-dev list issues

Mark has a challenge with the existing dev list because it requires a Google account. Yahoo would require the same. What about GitHub? It would require an account but perhaps would be more in the developer spirit. Eve also offers to host a mailing list on her home server, which wouldn’t require any accounts. Mark will propose options on the WG list.

Discuss Mark’s proposal for AS=C spec text

Does Mark’s recommendation around not needing the AAT in Section 3.4.1 make sense? We think that AAT issuance is still important (perhaps once again issued without having to go out to the wire, similarly to the RPT issuance spec text proposal), but using it to make a protected call to the authorization API to get the RPT no longer makes sense when AS=C.

Is Mark’s assumption correct, that when AS=C, RO=RqP? We believe so. In other words, this is effectively an Alice-to-Alice sharing scenario (one out of potentially many). Would AAT issuance actually involve an OAuth-style user flow? We’re not sure it’s needed. It could be buried in the terms of service that the AS has with the RO, which wouldn’t give the RO conscious choice. Could the initial RO interaction with the AS enable a preauthorization of this permission that could generate the AAT silently anytime? Yes.

Does it make sense to have a MUST with exceptions in the spec text? Alternatively, George asks, should we have an “AS=C profile” of the spec that turns the MUST into a MAY? This may be a cleaner way to handle the spec text flow. Mark notes that the proposed text changes are fairly few, so in practice, maybe that sort of infrastructure isn’t valuable enough. But then what about other optimizations we might add?

Eve asks if these are truly profiles or something else (operational modes)? George is agnostic as to the name, but would like to document these options in a simple and clean fashion, e.g. “You don’t have to physically generate the AAT but must track xyz...”. This is useful for auditing of UMA entity behavior, and therefore also useful for attaching Binding Obligations to artifacts.

All of Mark’s proposed text changes could then be sequestered in a single AS=C subsection of the new Optimization Considerations section he proposes to go after Section 7. We may still want to put a blanket statement in Section 3.1 that covers the possibility of undoing the MUSTs around on-the-wire interactions in the specific case of entityX=entityY situations. Eve is wary of enabling any and all MUSTs in the spec to be undone by the simple expedient of a magical profile that negates all interoperability, and wants to protect against this.

Mark will generate a second draft of his proposal. This will enable us to handle whatever optimization opportunities we think are high-priority. AS=C, AS=RS, and even possibly RS=C could be of interest.

Discuss "complex resources and scopes" idea (from convo with Hideki)

Examples of complex scopes might be that a Read scope and a Write scope might be part of a complex ReadAndWrite scope. Examples of complex resource sets might be that a PersonRecord resource set might encompass an Email claim (a smaller resource set) and a FirstName claim.

```plaintext
resource set = something
scopes = URI1, URI2, URI3
resource subsets = [some reference to another resource set - or do they get defined inline with an assumption that these same scopes apply to them]
```

```plaintext
scope = something
subscopes = URI1, URI2, URI3
```

George asks: What about the semantics of which scopes apply to which resource sets? We don't want to get into arbitrary complexity.
What would Roland's example look like in this paradigm? Does he want to separate the Read and Share capabilities of the UMA client/SAML IdP? Right now, these are conflated as far as we can tell, but they could be separated. The reason the IdP even wants the attribute is so that it can share it on with the SP. In UMA's concept of Binding Obligations, the permitted scope matters. Dazza proposed "terms of authorization", wherein the scope definition would contain machine-readable terms of some sort. For example:

scope = something
terms_of_authz = [some machine-readable stuff that says you can get this info but not share it with other parties, e.g.]

If we did subscopes, then we'd have to worry about whether the machine-readable portions are consistent with each other – or only define subscopes "in place" rather than referring to them, so they would directly inherit the parent scope.

George is also concerned about nesting resource sets super-deep. Would you want to use dot-notation to represent resources "above"? Is there the potential for privacy leakage for the client to know about all the possible field values? Eve notes that unlike in OAuth, UMA clients don't have to know anything at all about the possible scopes because this is opaque to them, but they still have to know the RS's API and what's possible there, so if there are ten attributes and the option to both get and set them, it will have to know this.

Mark is working on an attribute release policy for Kennisnet that's similar to Roland's challenge.

Eve notes that Roland could have defined resource sets that implicitly included each other, but were "flat" with respect to AS knowledge of the policy options.

We'll defer sketching solutions a little longer so we can sleep on this.

Discuss healthcare RLS use case next steps

We haven't scheduled any further ad hoc UMA WG meetings to work on this, but had thought about potentially supporting the creation of a group elsewhere to work on this. Mark may have an opportunity for us to present to a Dutch UMA healthcare group soon. The IDESG use case has been presented informally to the NSTIC Privacy committee that Adrian is on; he anticipates hearing back from them eventually. He'd like to be able to point to the work we've done so far in a more formal fashion. Should we prepare a white paper of sorts? Eve is willing to do this, hopefully by the time of the NSTIC plenary Jan 14-16.

AI: Eve: Prepare a healthcare RLS use case white paper for wider consumption.

Plan demo video, interop, and webinar calendar in Q1

The sample apps have been moved to new servers, and have also been upgraded. The flows will remain the same, but they'll gain some new interesting features. Skinning the apps for the PHealthCloud purpose isn't hard, but would take a half-hour or so of dedicated work to identify what's needed.

Keith and Mark are interested in helping with an UMA for Enterprise webinar, and Maciej agrees that doing this is a good idea. Mark and Mike are in talks around the former's open-source Asimba project. Mike's customer would be the case study that the webinar centers on. We're thinking mid-February makes a nice time to consider doing this.

Virtual interop activities: Are we ready to publish our endpoints? Mark isn't quite yet; Maciej is.

Attendees

- Eve
- George
- Mark
- Adrian
- Keith
- Domenico
- Sal
- Maciej

Next Meetings

- [Focus meeting Thu Jan 9 8:30-10am PT](time chart)
- [Focus meeting Thu Jan 16 8:30-10am PT](time chart)
- [Focus meeting Thu Jan 23 8:30-10am PT](time chart)
- [All-hands meeting Thu Jan 30 8:30-10am PT](time chart)