UMA telecon 2012-05-10

Date and Time

- WG telecon on Thursday, 10 May 2012, at 9am PT (time chart)
  - Skype: +9905100000481

Agenda

- Roll call
- Approve minutes of 2012-04-19 and 2012-04-26 meetings
- Eve regrets for May 17 – Thomas can chair; or Maciej?
- Vice-chair position up for election this month
  - Nominations
  - Vote this time?
- IIW update
  - Feature requests and use cases
- OAuth/IETF update
- Interop update
  - OSIS wiki
- Trust model update
  - Legal ad hoc meeting review
- Action item review
- Spec/issues review
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes of 2012-04-19 and 2012-04-26 meetings

Minutes of 2012-04-19 and 2012-04-26 meetings APPROVED.

Eve regrets for May 17

Maciej is available for both May 17 and May 24. Eve can create agendas for both.

Vice-chair position up for election this month

Maciej is willing to serve again. We’ll collect further nominations until such time as we get a chance to vote while quorate.

MOTION: Approve Maciej as vice-chair for another year. APPROVED by acclamation. Thanks, Maciej!

IIW update

It was a good meeting in terms of seeing high levels of interest in protecting personal information on the Web. There was a lot of VRM stuff this time. UMA is a big leap for many folks. Street Identity/OpenAXN and OpenID Connect are just reaching more people's consciousness. Maciej had some discussions with folks from the hardcore OAuth and OpenID Connect communities, and they are amenable to taking out dynamic client registration. It also seems that people who are more sensitized to the Attribute Provider use case are getting used to the idea of our “radical” separation of AS and RS, which hardcore OAuthers don’t seem to need otherwise. The net is that OpenID Connect is driving a set of use cases that OAuth by itself wouldn’t. In other words, once an Attribute Provider is conceived of as a resource server/host, UMA looks important.

Issues Eve collected that need to be added to GitHub:

- Make OpenID Connect MTI?
- Official Kantara/OIX statements/liaisons?
- Publish handy scope descriptions for common APIs (possibly including location)
- Publish handy standard promissory claims (possibly including CC, StandardLabel)
- Enshrine trust model work in Kantara/OIX trust framework efforts
- Requester-to-AM-first flow for the Street Identity/Attribute Provider use cases – high priority!
- Make it a no-brainer to write community and deployment profiles of UMA: document all the spec toggles (in the spec itself?)

Maciej needs the latter issue for auto-discovery of claims that live in a PDS. If the user has already introduced the PDS to their IdP, the requester should be able to discover what the AM protects. So the question the requester wants to be able to ask: What claims/resources could the AM offer if the requester could satisfy the policy? Project hData also needs this! What if the resource set registration process has the AM automatically create resources in a discovery service whose API is completely standardized? Has OpenID Connect already done this standardization?
Should Domenico's Trust Model User Guide be a Service Operator Criteria doc? Kantara would find that really useful.

Is it viable for us to explicitly position UMA as a Privacy By Design technology because it shifts the burden to requesting parties and because it enables more granular user-controlled protection of resources? We think this is fair.

Three legs good - four legs better! Let’s name our next tweet chat or webinar with this. 😊

**Interop update**

Eve will meet with Pam tomorrow to learn how to work the OSIS wiki.

**Trust model update**

Eve walked through the current state of the Trust Model doc, which is now in IETF-ready I-D spec form. SMART AM is the first deployed AM in the world, so the spec obligates Newcastle to adhere to the contractual terms! NCL will look at the doc closely.

**Action item review**

**Spec/issues review**

The SMART AM implementation’s RPT endpoint just gives out the RPT. It doesn't do the permission request part. In fact, the requester goes to ask for the RPT for a particular host even before it attempts access at the host, so it doesn't have a permission ticket yet. This is compliant with the older version of UMA, where the host doesn't eagerly register a permission and get a ticket! There seem to be exactly two viable technical approaches:

1. "SMART AM today": Two endpoints: RPT endpoint to which the host immediately sends a requester that came without an RPT, without having eagerly registered a permission, plus a permission endpoint to which the host sends a requester that did come with an RPT along with giving them a permission ticket.
2. "Optimized": Single endpoint: Permission endpoint to which the host sends all requesters that came either with or without RPTs, first having eagerly registered a permission in all cases.
3. "Splitting the baby": Host has the option of eagerly registering a permission before responding to a requester that came without an RPT, which is the requester’s signal to approach the permission endpoint, which will give it an RPT. This enables the host to take the "SMART AM today" approach if it wants to, or to take the "splitting the baby" approach simply by registering a permission for requesters without RPTs.

**Attendees**

As of 25 April 2012, quorum is 6 of 10.

1. Catalano, Domenico
2. D’Agostino, Salvatore
3. Hardjono, Thomas
4. Machulak, Maciej
5. Maler, Eve
6. Moren, Lukasz

**Next Meetings**

- WG telecon on Thursday, 17 May 2012, at 9am PT (time chart) – Eve regrets – Thomas will chair, or Maciej if available
- WG telecon on Thursday, 24 May 2012, at 9am PT (time chart)