UMA telecon 2012-03-15

UMA telecon 2012-03-15

Date and Time

- WG telecon on Thursday, 15 Mar 2012, at 9am PT (time chart) **beware of summertime skew! check local times carefully!**
  - Skype: +9905100000481

Agenda

- Roll call
- Approve minutes of 2012-03-08 meeting
- Tweet chat review
- IDtrust event review
- Work through spec resolution to issue 49
  - IETF I-D planning
- Review any additional open action items
- Interop planning
- AOB

Minutes

Roll call

Quorum was not reached.

Approve minutes of 2012-03-08 meeting

Deferred due to lack of quorum.

Work through spec resolution to issue 49

We dynamically reviewed the new spec text and edited it inline.

Do we actually need different AM endpoints for PAT and AAT issuance and PAT and AAT user authorization? The client in each case will have a client ID, which the AM could use to distinguish their role – or is that true? Normally, the AM (AS) would store these at least with client ID and, ultimately, with a set of permissions (scopes). Do we have to define UMA API scopes? We could distinguish the protection API and the authorization API by means of normal OAuth scopes. That way, a client that needs to serve as both a host and a requester for the same user (authorizing and requesting, respectively) could just upgrade the scopes they want from that AM. We could conceptually identify them separately in the spec, but we agree that implementations will likely make the endpoints the same.

How do OAuth-protected APIs document their available scopes? Can we just document the relevant scope in the section where the API is defined? It seems so. We could say that it's possible to extend/profile UMA APIs and identify profile-specific scopes, as long as the basic UMA API is not disrupted. This could be helpful in vertical deployment scenarios such as healthcare, for example. We decided to try consolidating these endpoints.

The RPT is now described as being bound to requesting party, requester, host, and AM – but not to authorizing user. Each permission is a little blob "inside" the RPT that is additionally associated with an authorizing user. The RPT now enables the AM to reuse claims from the requesting party across requests for permission for multiple users' online stuff, which should be a great benefit for usability. The AM becomes a deep claim-checking device that can operate for the benefit of all of its authorizing users. It's also becoming a panopticon for requesting parties' claims! This would be true for any RP, but the AM's "multi-tenant" nature wrt requesting parties' claims on behalf of its authorizing users makes it subject to a high standard.

Looking at the new intro to Section 3, is it correct? We think it's correct as far as it goes, but we're fuzzy on the AAT issuance followed by the permission request. What is Roger's experience? If the vanilla OAuth flow for AAT issuance goes properly, wouldn't Roger be bounced back and forth multiple times? Or do we need a server-to-server (back-channel) connection between the requester (client) and the AM (server)? The providing of claims at the AM is between Roger and that AM, so that if the AM has to return an error on the back channel to TripFollwr because it needs claims it doesn't have (providing a URL to redirect the requesting party to), this could require TripFollwr to redirect Roger to CopMonkey only at that point.

TripFollwr, the requester app in this instance, isn't inherently involved. If it happens to be Roger's IdP, then great – the flow would be perfectly optimized even if the protocol keeps them conceptually separate.

From a pure UX perspective, ideally you'd want a single redirect to involve all the CopMonkey/Roger interactions all at once. Because OAuth and OpenID Connect aren't friendly to dynamically passed data (namely the particular requester app, whether TripFollwr to iCal to whatever). So the user may have to answer answers about the same claims multiple times for different requester apps.

Could the requester ask for an RPT without presenting an AAT? That would break OAuth.

Have the SMART folks figured out clever UX optimizations to avoid multiple redirects to the AM for the AAT and for claims-gathering?

Next Meetings

- WG telecon on Thursday, 22 Mar 2012, at 9am PT (time chart)
• WG telecon on Thursday, 29 Mar 2012, at 9am PT (time chart)

Attendees

As of 12 Mar 2012, quorum is 8 of 13.

1. Catalano, Domenico
2. Fletcher, George
3. Hardjono, Thomas
4. Maler, Eve

Regrets:

• Machulak, Maciej
• Morrow, Susan
• Szpot, Jacek