UMA telecon 2014-10-23

UMA telecon 2014-10-23

Date and Time

- Thu Oct 23 9-10am PT
  - Voice: Skype: +9905100000481 or US +1-805-309-2350 (international dial-in lines), room code 178-2540#
  - Screen sharing: http://join.me/findthomas

Agenda

- Roll call
- Minutes approval if quorum
  - Sample motion: Approve the minutes of UMA telecon 2014-10-09 and 2014-10-16.
- Interop testing status
- Meeting schedule review
  - FT-impacting issues on V1.0 docket
    - 92: trust elevation"need_reauthentication": provide "ACR URL" property?
    - 108: make "protection" and "authorization" scopes able to be implicit?
    - 84: UMA endpoint names vs. OAuth endpoint names
    - 105: status parameter in resource reg
    - 94: start_at for permission validity
- AOB

Minutes

Roll call

Quorum was not reached.

Minutes approval if quorum

Deferred.

Interop testing status

On Monday, the credentials issue was discussed again. Roland has been improving his OIDC handling, so he can use federated login in the fashion supported by NuVeAM. Sampo mentioned that he would improve his implementation around credentials. Marcelo needs more time to supply his credentials.

Meeting schedule review

Done! Next meeting is November 13.

92: trust elevation"need_reauthentication": provide "ACR URL" property?

The name of the response in the third-party profile is actually required_acr_uri. OIDC doesn't specify much detail about the value of an acr; it's just whatever URI has been registered to represent a standard semantic for authentication context – LOA or authentication type or whatever. Eve throws out a proposal: Let's add required_acr_uri, and define it roughly according to how OIDC defines the value. Andi speaks in support as long as it's an optional property in the response from the AS. Maciej notes that whatever structure we use for need_claims and need_reauthentication, we should make them the same given that both would have additional hint information supplied. His preference is to have a structure called something like error_details, with an array that includes whatever information is needed, of which required_acr_uri would be perhaps the only one specified in the core spec.

AI: Maciej: Edit the claim profiles spec to fix the fact that need_claims is an error construct, not a success response.

Maciej's proposal goes something like this:
Yuriy speaks in favor because it isolates the error "metadata", though he would like us to think a bit harder about this to make sure we consider the design pattern a little more carefully. George asks: What if you need both claims and reauthentication? Eve thinks you have to give either one error or the other; they're mutually exclusive. But George notes that if we did have to generate both options, the pattern above would be awkward. But could the two conditions be merged together – that is, could you say that the AS needs a claim of strong auth that results in needing a stronger ACR and thus the AAT needs to be revoked? The same OIDC session might have been the source of both the too-weak AAT and the claim that would have been handed over to the AS a bit later in the process! But the AAT represents something in Bob's sphere of online influence that is "wider" than just the current session and access attempt at this RS. Nonetheless, a highly sensitive resource may still demand a really fresh, really high-LOA AAT anyway.

The ideal (in some sense) is that the AS can reuse various claims collected about Bob in a variety of contexts, e.g. at different RS's. That's the value of an AAT – it gives the AS permission to cache and manage claims for the purpose of authorization.

Eve had thought that the previous AAT would get revoked, but apparently that's not the case. The assumption is that the client still hangs on to the previous AAT, and just reauthenticates the RqP as required in this circumstance. This is seen as a step-up. This issue still isn't entirely closed.

AI: Yuriy: Write some clarifying paragraphs to kick off the specification effort around this issue.

108: make "protection" and "authorization" scopes able to be implicit?

84: UMA endpoint names vs. OAuth endpoint names

105: status parameter in resource reg

94: start_at for permission validity

Deferred. We like the idea of extending the next two meeting times to 1.5 (or 2?) hours to try and get through all the remaining issues.

Attendees

As of 2 Oct 2014, quorum is 8 of 14.

1. Eve
2. Andi
3. Yuriy
4. Maciej
5. Domenico
6. Sal
7. Jin

Eve will remove voting participants on the rolls who are not attending regularly.

Non-voting participants:

- George
- Ann

Next Meetings

We will hold all-hands meetings (calling the roll) through the fall and early winter as much as possible; voting participants please attend! You can subscribe to the UMA calendar (and ask the chair to send you an event invitation) to see the times in your local time zone. Keep in mind that when the clocks change, we experience "summertime skew": our home time zone is Pacific so non-US meeting times may shift.

- (Clocks change in Europe on Oct 26)
- No meeting Thu Oct 30 because of IIW – we are holding an open UMA implementors' meeting on Oct 29 at IIW instead
- (Clocks change in US and Canada Nov 2)
- No meeting Nov 6 (Eve regrets)
- Thu Nov 13 9-10am PT
- Thu Nov 20 9-10am PT
- No meeting Thu Nov 27 because of Thanksgiving holiday in the US
• Thu Dec 4 9-10am PT
• Thu Dec 11 9-10am PT
• Thu Dec 18 9-10am PT: possible to approve V1.0 drafts for public review in January on this date?
• No meeting Thu Dec 25 because of Christmas holiday
• No meeting Thu Jan 1 because of New Year's Day holiday