UMA telecon 2016-07-07

UMA telecon 2016-07-07

Date and Time

- Thursdays, 9-10am PT
- Skype: +99051000000481 / US +1-805-309-2350 / international lines / web calling interface / code 1782540
- Screen sharing: http://join.me/findthomas - NOTE: do not use the join.me dial-in line
- UMA calendar: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Approve minutes of UMA telecon 2016-06-30
- Logistics
  - When/how to extend our design time?
  - 8:30-10am PT calls on Thursdays
  - 9-10:30am PT calls on Thursdays
  - Additional calls on other days
  - Multiple options
  - How about going long on today's call?
- Spec editorship duties
  - For reference: MPD sequence diagram and generic low-level sequence diagram
    - MPD writeup on consent
      - Is doing consent later okay?
      - Is doing consent OOB okay?
      - Would an "UMA refresh token" alternative make any sense?
    - The Alice-to-Alice sharing mechanism in light of MPD
    - Trust elevation extension mechanisms and MPD
- Registering multiple resource sets
  - Input from George on existing spec text?
  - Client awareness of scopes
    - Concrete proposals based on multiple-resource-set directions?
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2016-06-30: Deferred.

Logistics

Mike speaks in favor of regular 60-minute calls and additional ad hoc calls among, say, spec editors and interested others. Robert and Justin agree. Okay, we seem to have consensus around that.

Justin has little availability for an editing session next week; Eve will suggest some times for a kickoff session the week of July 18.

MPD writeup

The "claims" endpoint is really the "interaction" endpoint for all purposes.

Justin has introduced a new idea of an "UMA refresh token" (URT) as a static refresh artifact along with the client presenting the ticket at the token endpoint, to signal a cross-session RqP relationship with the AS. This would be used in concert with a one-two punch of gathering consent at the claims endpoint and then pushing claims at the token endpoint. Eve wonders about the name: It represents the RqP's persistent consent or authorization, even if its function at the AS might be to "refresh" something. James suggests: consent context token.

We have a lot of naming issues to sort out, so let's not decide right away.

We have consensus to proceed with spec text for a mechanism that keeps consent "in-band" vs. "out of band", by virtue of a "token-ish" method that the client uses to preserve the AS's memory of the RqP. If the AS doesn't issue an urt-ish thing, then consent must be sought every session.

What about Alice-to-Alice sharing? If she's sent to the claims endpoint, would we anticipate that it would be collapsed into an authorization endpoint as well, and then have it hand out (say) authorization codes in addition? The client wouldn't be expecting that; it's expecting a ticket. Ultimately, Eve had a re-epiphany about the lack of a need for any special treatment of Alice as an RqP; Alice as an RO can simply make policies about "herself as an RqP" (and the AS could, if it wishes, handle various Alice-to-Alice cases specially if it wishes). Justin would, however, like to see some experimentation where there's some confluence of the two endpoints.
We discussed the “Allow ID Tokens as RPT” thread (correction: it was the “Questions about MPD” thread). An AS needs to have an identified and authorized RqP. Strictly speaking, does that mean the user needs to be “logged in”? James defines this as having had an interactive authentication experience, which his implementation doesn’t require; it all depends on what auth modules have been leveraged. Justin’s read of the meaning of “logged in” is broader, just meaning “has an authentication session”.

We didn’t quite get to the topic of trust elevation extension mechanisms, but this will depend on how the spec text shapes up.

Attendees

As of 23 Jun 2016 (post-meeting), quorum is 6 of 11. (Domenico, Kathleen, Sal, Nagesh, Andi, Robert, Agus, Maciej, Eve, Mike, Sarah)

1. Domenico
2. Sal
3. Nagesh
4. Robert
5. Maciej
6. Eve
7. Mike
8. Sarah

Non-voting participants:

- Justin
- Adrian
- Colin
- James