UMA telecon 2016-01-14

Date and Time

- Thu Jan 14, 9-10am PT
  - Voice: Skype: +99051000000481 or US +1-805-309-2350 (international dial-in lines), room code 178-2540#
  - Screen sharing: http://join.me/findthomas - NOTE: IGNORE the join.me dial-in line shown here in favor of the dial-in info above (Kantara "line C" and the Skype line)
- UMA calendar: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Approve minutes of UMA telecon 2016-01-07 if quorum
- Quick legal subgroup update
- Update on AIs from last week
- Review roadmap use case/technical issue matrix (Eve AI) and figure out what to dive into/how/when in Q1
  - Good F2F opportunities?
  - Good liaison opportunities?
  - Charter AIs?
- AOB

Minutes

Roll call

Quorum was not reached.

Quick legal subgroup update

The subgroup meetings are going to continue, and consensus was reached on releasing beta model text by the end of Q1.

Update on AIs from last week

Andi now has the data he needs for the blog post. We need to publish the specs first; that should happen tomorrow.

Mike is doing a Kantara blog post about RSA sessions, including those that relate to UMA (and beer!), and can mention others. Eve is doing a privacy talk with Josh Alexander (and they'll be singing again too ☺). A good idea is to send calendar invitations to those you'd really like to come to your talk. Hopefully Kantara will be sponsoring the Non-Profits on the Loose party again at RSA! Keep on the lookout. Even if not, let's all try to get together and hoist an UMArtini (or something – or a BLT...).

Thomas and Maciej and Eve are very close to finishing other AIs.

Review roadmap use case/technical issue matrix (Eve AI) and figure out what to dive into/how/when in Q1

- Good F2F opportunities?
- Good liaison opportunities?
- Charter AIs?

We are looking for "customer need" for these use cases and technical issues. Let's put initials of participants where they can confidently express "customer need" in 2016 or 2017 (or, if you want to remain pseudonymous, get in touch with Eve and she will put XX in for your initials).

<table>
<thead>
<tr>
<th>use case</th>
<th>technical issue</th>
<th>IoT</th>
<th>API security</th>
<th>federated authz</th>
<th>RS authorization discretion (also &quot;legal&quot;?)</th>
<th>RO access limit discretion (also &quot;legal&quot;)</th>
<th>wide ecosystems (is this a meta-use case?)</th>
<th>access federations (&quot;legal&quot;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAT burden</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>permission reg extension</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS client-to-AS-first efficiency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS self-contained token validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPT needs refresh token*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shoebox endpoint*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
An issue that Mike wants UMA to explore is the new NAPPS solution being proposed that uses PKCE. It leverages new system browser capabilities to return control to a native app using a custom scheme that the native app registered. Could this solution be applied to how a client delivers an RPT to a mobile app? Since the client just makes a direct back-channel call to the RPT endpoint at the AS, is this needed? Perhaps not right now, but maybe this could be used where we use a redirect flow (redirecting Bob for claims gathering after getting need_info with redirect_user), or if we start considering an authorization code-type flow for a redesigned client interaction with the AS a la Justin's suggestion (AAT-free).

Mike remarks that a self-contained token is interesting but may be a nice-to-have for him vs. a self-contained token. In the work he's describing here, the client-to-AS-first pattern could be relevant.

Adrian would like an RS to be able, based on jurisdictional requirements, to get hold of verified attributes of the requesting party. This likely goes beyond healthcare, he surmises. What happens if the RS trusts the AS to be the RO's agent but doesn't trust the RO not to make policies that end up putting the RS out of compliance with jurisdictional regulations without further RS-specific authorization procedures (e.g., by assessing verified attributes presented by the RqP)? Currently UMA says that if the RS cares about such attributes, it can gather them locally; it doesn't (by default) get them from the AS. Are we interested to develop a token profile for this to come from the AS? Perhaps there's not enough impetus.

What about a "Shoebox" endpoint? The AS could present this endpoint for more than "consent receipts" – importantly, notifications are a big part of many laws. It would be great to bounce this off our legal subgroup. Is it, in fact, right for the AS to take on such an endpoint?

What "RO access limit discretion" means is that we want to set up a one-way valve. Currently the spec it's a MUST, but technically it's not possible to enforce that the RS not give access when the permissions in the RPT say "no" in a technical fashion. However, it may be possible to set up a conformance suite in such a fashion to catch such cases and force the throwing of an audit log entry. In fact, this could be a case where a "Shoebox endpoint" could be a key part of a technical solution, in that we could mandate notices for certain kinds of access given.

At: Eve: Put starred items in the left column into GitHub issues.

At: Eve: Post matrix in a more prominent wiki place and start to check off relationships among the columns and rows, and advertise the opportunity to state priorities.

Attendees

As of 18 Dec 2015, quorum is 6 of 11. (Evariste, François, Domenico, Sal, Thomas, Andi, Robert, Maciej, Eve, Søren, Mike)

1. Eve
2. François
3. Domenico

Non-voting participants:

- Steve
- Katie
- Adrian
- George