UMA telecon 2011-09-22

UMA telecon 2011-09-22

- **Date and Time**
- **Agenda**
- **Attendees**
- **Minutes**
  - New AI summary
  - Roll call
  - Approve minutes of 2011-09-15 meeting
  - Action item review
  - Leadership elections
  - 2012 Kantara budget proposal status
  - Core protocol issues in GitHub
- **Next Meetings**

**Date and Time**
- WG telecon on Thursday, 22 Sep 2011, at 9-10am PT (time chart)
- Skype line "C": +9900827042954214
- US: +1-201-793-9022 (other int'l numbers) | Room Code: 295-4214

**Agenda**
- Roll call
- Approve minutes of 2011-09-15 meeting
- Action item review
- Leadership elections
  - Chair role is up for election (past due)
- 2012 Kantara budget proposal status
- Core protocol issues in GitHub
  - Work through trusted claims proposal
  - Work through the street identity example (etherpad)
  - Discuss issue #2 in this light
  - Try to close #18
  - Prioritize next issues
- AOB

**Attendees**

As of 22 Aug 2011, quorum is 6 of 10.

1. Catalano, Domenico
2. Fletcher, George
3. Hardjono, Thomas
4. Machulak, Maciej
5. Maler, Eve
6. Moren, Lukasz
7. Morrow, Susan
8. Szpot, Jacek
9. Wray, Frank

Non-voting participants:
- Kevin Cox

**Minutes**

**New AI summary**

<table>
<thead>
<tr>
<th>2011-09-22-1</th>
<th>Eve</th>
<th>Open</th>
<th>Check with John and Nat on Domenico’s proposal as something that can flesh out our Section 3.5.1 as a trusted-claims solution.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-09-22-2</td>
<td>Eve</td>
<td>Open</td>
<td>Schedule ad hoc session to work on OpenID Connect integration and Kantara URL decision-making.</td>
</tr>
<tr>
<td>2011-09-22-3</td>
<td>Susan, Eve</td>
<td>Open</td>
<td>Refresh the trust model document to reflect the new OpenID Connect configuration ideas.</td>
</tr>
<tr>
<td>2011-09-22-4</td>
<td>Various</td>
<td>Open</td>
<td>Build list of FAQs on the wiki. Lukasz owes a SMART project FAQ. Susan owes a FAQ on how UMA is related to OpenID.</td>
</tr>
</tbody>
</table>

**Roll call**

Quorum was reached.
Approve minutes of 2011-09-15 meeting

Minutes of 2011-09-15 meeting APPROVED.

Action item review

- 2010-11-18-4 Eve Open Capture new user stories in the wiki.
- 2011-04-14-1 Maciej, Alam, Eve Open Build list of FAQs (both questions and candidate answers) on the wiki. Eve has written a few new answers. Sal may take on a few too. The SMART team still has to write a special SMARTAM Q&A.

Leadership elections

- Chair role is up for election (past due)

Eve Maler re-elected to the chair role by acclamation.

2012 Kantara budget proposal status

The LC has recommended our requests to the BoT.

Core protocol issues in GitHub

- Work through trusted claims proposal

A new web sequence diagram from Domenico is available, matching the latest OpenID Connect specs.

The interaction shown is a sub-sequence for when a requester is asking for access to some protected resource.

The interaction between the UMA AM and the OpenID Connect AS is entirely governed by OpenID Connect. Can we just say in our spec, simply, that the UMA AM would be required to be an OpenID Connect client and the requester would be required to have an OpenID Connect-enabled IdP? Or should it be an option? The requester itself isn't doing any of this work; it's only the AM doing the work. The requesting party (assuming a human, using a browser) would get redirected over to the AM; an alternative could be creating a new account or leveraging an existing account at that AM.

This solves George's problem of picture-sharing with his sister! This has been one of our major motivating factors for UMA's design. Unfortunately, the way the web works today, there's going to be a reliance on email addresses in policies. However, this isn't a barrier to using IdPs that don't issue email address (like GMail); IdPs like Facebook offer verified email addresses as attributes, and as a fallback, the AM could offer to register an account for George's sister, and even do an email address verification loop when she registers.

The OpenID spec list folks are currently discussing the question of what claims should be standardized. They're likely to rely on URIs to identify extended claim types. There is a "verified" Boolean value on claims, which is generically valuable. We could perhaps point to OpenID Connect's standard claims as being mandatory to support if OpenID Connect claims are being used. The AS side would have to at least be able to recognize the claim types being asked for, even if it's not willing to hand out that data (like birthdate).

We have a choice about whether to make zero, one, or multiple claim formats mandatory to implement for interoperability. We also have a choice about whether to make it possible for third parties to extend to new claim formats. We have consensus that we want to enable UMA to be extensible in this respect (e.g., to allow SAML claims etc. for government and enterprise use cases), and we have consensus that we want to list OpenID Connect as one optional claim format – not mandatory for now.

We think that we now have a solution that works all the way through for human requesting parties operating requester apps that are web-hosted (browser-based), even if some flows would be a bit clunky (e.g. asking Georgina to create a new account at the AM) and we need to look at security considerations with the redirects. SMARTAM already does this redirect, so we have some experience here. You can also bind the trusted identity/claims of the requesting party to any self-asserted claims that the AM asks the user for at the point (e.g. promises), to make them more strongly contractually binding.

We would still need to solve the "requester web services" flows and "requesting humans operating native requester apps" flows.

- Similarities and synergies between OpenID Connect's token introspection/session management feature and UMA's token status feature
- Discuss issue #2 in this light

OpenID Connect really does mean to apply this only to authenticated login sessions, not to looking for active permissions (the way UMA uses this mechanism). Should their mechanism be a bit more flexible and generic? And if so, should they look at the UMA approach? Both use a kind of "artifact" approach, in that an opaque code is being dereferenced. But the token's functionality is pretty different. Should the syntaxes align more? That would probably be ideal.

- Work through the street identity example (etherpad)

Deferred. We'll compare it to our nascent OpenID Connect integration spec text.

- Try to close #18

We'll discuss this in the ad hoc.

Next Meetings

- WG telecon on Thursday, 29 Sep 2011, at 9-10am PT (time chart)
- WG telecon on Thursday, 6 Oct 2011, at 9-10am PT (time chart)
- WG telecon on Thursday, 13 Oct 2011, at 9-10am PT (time chart)
• WG F2F on Thursday, 20 Oct 2011, at 1-5pm PT (time chart) in Redwood City, CA, USA
• WG telecon on Thursday, 27 Oct 2011, at 1-5pm PT (time chart)
• **NOTE:** Daylight saving ends Oct 30 in UK and Nov 6 in US; beware of "summertime skew"