UMA telecon 2011-02-10

UMA telecon 2011-02-10

- Date and Time
- Agenda
- Attendees
- Minutes
  - New AI summary
  - Roll call
  - Approve minutes of 2011-02-03 meeting
  - Action item review
  - Upcoming events
  - Ian Glazer blog post
  - Kantara roadmap items
  - Discuss role of digital signatures
  - Step 3 host-AM communication options
- Next Meetings

Date and Time

- WG telecon on Thursday, 10 Feb 2011, at 9-10:30am PT (time chart)
  - Skype line "C": +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214

Agenda

- Roll call
- Administrative &c.
  - Approve minutes of 2011-02-03 meeting
  - Action item review
  - Thoughts on Ian Glazer blog post?
  - PET Symposium call for papers deadline is Feb 28
  - SOUPS call for papers deadline is Mar 11
  - Think about IIW 12 opportunities?
  - Interest in booking meeting time at Berlin Kantara meeting in mid-May?
- Technical
  - Discuss role of digital signatures (see design principle proposal discussion and signed message discussion)
  - Step 3 host-AM communication options (see Christian's 'pad')
  - Claims 2.0 etc. depending on AI completion
  - Spec editing assignments for all
- AOB

Attendees

As of 8 Feb 2011, quorum is 8 of 15.

1. Mohammad, Alam
2. Bryan, Paul
3. Catalano, Domenico
4. D'Agostino, Salvatore
5. Maler, Eve
6. Morrow, Susan
7. Scholz, Christian
8. Wolniak, Maciej

Non-voting:

- John Bradley
- Kevin Cox
- Frank Wray

Others:

- Dervla O'Reilly (staff)

Regrets:

- Maciej Machulak
- Lukasz Moren
- Cordny Nederkoorn

Minutes
New AI summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-02-10</td>
<td>Alam</td>
<td>Open</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Share details of his planned UMA demo with the list.</td>
</tr>
<tr>
<td>2011-02-10</td>
<td>Eve</td>
<td>Open</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Revise the Requirements document to add the new DP 13.</td>
</tr>
</tbody>
</table>

Roll call

Quorum was reached.

Approve minutes of 2011-02-03 meeting

Deferred due to desire to review for a longer period.

Action item review

- 2010-11-18-4 Eve Open Capture new user stories in the wiki.
- 2011-01-06-4 Susan Open Write draft UMA trust model. Drafts sent to list. In process. Slated to be closed after her meeting on Feb 21.
- 2011-01-27-1 Paul Bryan Open Revise the Claims 2.0 spec to reference and profile JWT. In process.
- 2011-01-27-3 Paul Bryan Open Revise the "scoped access" flow list to reflect decisions made in today's meeting. In process. He will do this in Christian's 'pad.'

Upcoming events

- RSA next week
- Book meeting time/demo at Berlin Kantara meeting in mid-May?

We don't seem to have critical mass to hold a formal meeting, but Alam has offered to show an UMA-related demo during the Berlin meeting time. He and Dervla will work on scheduling the demo time, and Alam will share details of his planned demo with our list.

- PET Symposium call for papers deadline is Feb 28
- SOUPS call for papers deadline is Mar 11

If anyone is interested in submitting a paper and wants help, please speak up.

- IIW 12 opportunities

Eve, possibly Susan, and likely Sal will be in attendance. It would be great to be in a position to show some new demos.

Ian Glazer blog post

UMA gets a mention. People may want to check it out and comment on the post or share thoughts on our WG list.

Kantara roadmap items

- 2011Q1:
  - Complete draft of solution for scoped access in UMA protocol
  - Complete draft of UMA trust model
- 2011Q2:
  - Document understanding of trusted claims and relationship to OpenID Connect

Discuss role of digital signatures

- See design principle proposal discussion and signed message discussion
- Editing assignments?

If we can push complexity to the AM by having it verify its own signatures on behalf of a host (though a back-channel call) as necessary, we achieve the benefits of signatures without necessarily burdening the host unduly. The proposal wording was:

"Don’t preclude strong authentication through digital signatures, and leverage and adopt signatures as options if a reasonable measure of interoperability can be achieved."

Should it include something about standard signature solutions? E.g.:

"Don’t preclude strong authentication through digital signatures, and leverage widely supported signature solutions as options if a reasonable measure of interoperability can be achieved."

The goal here is to promote developers not to roll their own implementations, but rather use existing libraries or other open-source/platform solutions.

Motion: Approve design principle 13 with the title "Digital Signatures" and the text "Don’t preclude strong authentication through digital signatures, and leverage widely supported signature solutions as options if a reasonable measure of interoperability can be achieved." Passed by unanimous consent.
Step 3 host-AM communication options

- See Christian’s pad
- Spec editing assignments?

Paul’s conception is that the host will treat the requester’s access token only as authenticating the requester, and that it will always ask for authorization directly from the AM. An authorization decision that the AM gives the host can be cached by the host as an optimization strategy. But let’s say that the requester had previously (in step 2) given claims to the AM, which gave it authorization rights at the time – but that the claims are very time-sensitive. If the requester finally gets around to asking for access at the host but its authorization (which only the AM knows) has expired, then the host will find out from the AM that the requester is not authorized and will have to send it back to the AM.

There are three choices for what the step 3 host-AM token validation communication looks like:

- **PDP option:** Host supplies the attempted scope and asks for a yes/no authorization decision.
  - **Pro:**
    * AM takes on the burden of validating the token.
    * AM has the ability to take into account very time-sensitive user policies for authorizing requesters.
    * Host avoids needing sophisticated PKI (the “dumb host” option).
  - **Con:**
    * Requires AM to be stateful (though this can be worked around).
    * Involves a potentially expensive back-channel host-AM interaction in real time.

- **Hybrid option:** Host asks the AM what scopes this token is supposed to be authorized to access, the AM tells it (along with time-to-live metadata), and the host internally maps what it learned from this exchange to the scope being attempted. (We think this is Christian’s “independent flow” in the ‘pad.)
  - **Pro:**
    * AM takes on the burden of validating the token.
    * Host can avoid some back-channel interactions with the AM in many cases because it can cache more information for longer.
    * AM still has the ability to take into account very time-sensitive user policies for authorizing requesters by minting very short-lived tokens.
    * AM can outsource token validation itself, e.g. if the token contains an encrypted payload intended for a separate party (the "stateless advantage").
    * Host avoids needing sophisticated PKI (the “dumb host” option). Allows graceful extension into the meaningful token option.
  - **Con:**
    * Involves a potentially expensive back-channel host-AM interaction in real time (though likely fewer of them than in the PDP option).

- **Meaningful token option:** Host doesn’t need to ask the AM anything because the requester brought it a “meaningful” (to the host) access token that contains a manifest of the scopes it’s good for.
  - **Pro:**
    * Host can avoid a real-time back-channel interaction with the AM.
  - **Con:**
    * For some use cases, the "scope universe" might be so large that it impacts token size (though maybe these use cases can fall back to an "artifact mode" that amounts to the hybrid mode).
    * The host has to be "smart" to be able to unpack the token content (though this too can be mitigated by allowing the AM to fall back to an "artifact mode").

The current OAuth deployments have very small "scope universes". Some UMA use cases do have small universes too, but other use cases (a professional photographer protecting thousands of photos in a fine-grained manner) may involve many scopes that might have to be transmitted in a single token.

We gained consensus that the hybrid solution is a good place to start and allows us to grow as the underlying technologies mature. Thus, Paul’s existing action item merges with Christian’s completed one, and Paul will sketch the solution directly in the ‘pad.

**Next Meetings**

- WG telecon on Thursday, 17 Feb 2011, at 9-10:30am PT (time chart) (during RSA conference)
- WG telecon on Thursday, 24 Feb 2011, at 9-10:30am PT (time chart)
- WG telecon on Thursday, 3 Mar 2011, at 9-10:30am PT (time chart)