UMA telecon 2011-04-21

UMA telecon 2011-04-21

- Date and Time
- Agenda
- Attendees
- Minutes
  - New AI summary
  - Roll call
  - Approve minutes of 2011-04-14 meeting
  - Action item review
  - IIW plans
  - Spec editor elections
  - Scoped access review
  - Dynamic client registration I-D editing
- Next Meetings
  
  Date and Time
  - WG telecon on Thursday, 21 Apr 2011, at 9-10:30am 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 2011-04-14 meeting
  - Administrative
  - Action item review
    - IIW plans; no WG meeting 5 May 2011?
    - Spec editor elections
  - Scoped access review
    - Thomas spec text proposal
    - Frank/Kirk: mappings of use cases onto the flow and collection of UX practices
    - How/when to publish all this?
  - Dynamic client registration I-D editing
    - How/when to publish all this?
  - AOB

  Attendees
  
  As of 21 Apr 2011 (pre-mtg), quorum is 8 of 14.

  1. Mohammad, Alam
  2. Bryan, Paul
  3. D'Agostino, Salvatore
  4. Hardjono, Thomas
  5. Machulak, Maciej
  6. Maler, Eve
  7. Moren, Lukasz
  8. Morrow, Susan
  9. Scholz, Christian
  10. Wray, Frank

  Non-voting participants:

  - Kevin Cox

  Minutes

  New AI summary

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-04-21-1 Eve</td>
<td>Open</td>
<td>Update the scoped access proposal into I-D form for discussion.</td>
</tr>
<tr>
<td>2011-04-21-2 Eve</td>
<td>Open</td>
<td>Revise the dynamic client registration spec again.</td>
</tr>
<tr>
<td>2011-04-21-3 Cordy</td>
<td>Open</td>
<td>Look at scoped access flow for error conditions we've missed.</td>
</tr>
</tbody>
</table>

  Roll call

  Quorum was reached.
Approve minutes of 2011-04-14 meeting

Minutes of 2011-04-14 meeting APPROVED.

Action item review

- 2010-11-18-4 Eve Open Capture new user stories in the wiki.
- 2011-01-27-1 Paul Open Revise the Claims 2.0 spec to reference and profile JWT. Let's drop this for now, until we're ready to go the meaningful token route.
- 2011-03-02-1 Nat Open Put together JWT-compliant examples of Claims 2.0 and Simple Access Authorization Claims. Eve to reach out to him.
- 2011-04-07-2 Frank, Kirk Open Match constellations to scoped access diagrams to see what happens. This is in progress.
- 2011-04-07-3 Thomas Open Turn the results of the ad hoc call on scoped access into core spec text. This is in progress. The core spec needs to refer out better to the "children" specs.
- 2011-04-14-1 Maciej, Alam Open Build list of FAQs (both questions and candidate answers) on the wiki. This is in progress.

IIW plans

The whole SMART team will be there. Maciej had proposed several sessions that they could convene, such as results of the UMA UX study (Maciej W.) and technical details of the implementation and use of the UMA/j framework (Łukasz and Maciej M.). Eve proposes that another good session would be "UMA solutions for OAuth scope upgrades", especially if we can do it as early in the conference as possible. The process of open-sourcing the UMA/j implementation is awaiting various timing considerations, but it's just about stable right now.

NOTE: No WG meeting 5 May 2011, because of IIW. It's been removed from the online calendar.

Spec editor elections

MOTION and second: Install Thomas Hardjono as the UMA WG spec editor. APPROVED.

Thanks to Christian for his last year's worth of service! And thanks to Thomas for his willingness to serve! The Leadership Team page has been updated.

Christian has a script that automatically pulls from his mrtopf GitHub repository, but his repository and Eve's are not being automatically synced/merged, because merge conflicts would need to be manually handled anyway. Thomas has been in the habit of uploading a new version and retaining old ones with distinct names, in the OASIS style. Should we consider this, or a hybrid where we collaboratively edit xml2rfc-encoded content into an etherpad? Thomas will reach out to Christian with any questions.

Scoped access review

Initial mappings of use cases onto the flow (image source):

This is an attempt to mix the OAuth healthcare use case and the UMA hData scenario, with the simplification that the hData "DAS" (discovery and authorization service) is just doing authorization and not discovery. Our original conception of covering hData use cases was that it could cleverly use UMA to protect the discovery portion of the service, but that's not reflected here. So, as currently conceived, this diagram is a useful generic mix of use cases interesting to both OAuth and hData.

The PCP (primary care physician) is the host in this scenario, and what it's hosting is an hData-compliant API that offers hData-formatted data.

Alice might have a default policy rule that says she needs to be consulted in real time, e.g. by SMS, if a requesting party asks for access.

There's an assumption that, for the healthcare case specifically, likely there are some "trust framework" and compliance/authentication requirements that the parties can test in each other ahead of time or dynamically. This may give a dimension of vertical specificity to what is otherwise just generic UMA. Frank observes that insurance companies would make convenient DAS's -- in fact, discovery of the discovery service endpoint (or specific resources) could be done off of a magstripe on an insurance card! In a lighter-weight non-healthcare scenario, truly dynamic introduction of parties for low-risk/low-value data transfer might be accomplished.

The diagram would be more convenient if it were to remove the labels of PCP and SleepWell as being both a requester and host, since at this stage the PCP is only a host and SleepWell is only a requester. A follow-on diagram can illustrate the low-level protocol details, and another could show how SleepWell, in turn, becomes a host. Even the high-level diagram probably also needs to show a dotted arrow for discovery of the protected resource location and also a claims/authorization flow.

Spec text planning:

Thomas suggests submitting the core spec, with scoped-access stuff in it, as an I-D prior to the next IETF meeting. This means we'd have to submit by roughly late June. July 24 is the next IETF meeting, in Quebec. The OAuth group is going to be rechartered at this meeting, so this would be a perfect juncture for presenting UMA as a potential work item. We'd also very much like to have a spec draft before IIW -- and in fact we may need a "discussion document" (ideally in I-D form!) to ensure full consideration.

Eve has proposed, in private email to Thomas, some terminology we can use in the spec to distinguish between "resource registration" and "scope registration" and "authorization" stages. For example:

- prsID (identifier of a resource set)
- action (action represented by a URI)
- requested scope (what a host registers at an AM)
- granted scope (what an AM associates with a requester's access token)
- granted scope manifest (what a host gets back when it asks for token validation)

Thomas notes that we should account for errors of the sort where the host registers a requested scope that's "broken" in some fashion, that is, it doesn't correspond to any known resources (or the actions don't correspond to) stuff already registered at this AM for this user.
New ideas for scoped access:

An idea came up to enhance the token validation flow, to get it philosophically closer to an XACML-like policy decision point/policy enforcement point (PDP/PEP) model. The host could (optionally?) include, along with its token validation request to the AM, the requested scope that it's going to be looking for in the manifest that comes back. This would give the AM the opportunity to pre-tell the host "yes, that's in the manifest", which is an implicit "yes" to the implicit question "should I let this guy in?". It also seems to have some slight non-repudiation properties, since the host goes on record with the AM about the type of attempted access.

UX best practices:

Kirk has an idea that we should collect UX options, to help implementers know how to start. Frank imagines that practices will differ per industry or use case, so maybe we can't say "best"! But Eve likes the idea of capturing baseline/naive UX ideas, vs. shoot-the-moon ideas.

Dynamic client registration I-D editing

We should do a keep_alive, just adding someone's last name. We can use Thomas's. It's okay to have four authors for now.

Next Meetings

- WG telecon on Thursday, 28 Apr 2011, at 9-10:30am PT (time chart) (Eve may be a bit late - Maciej will initiate call and chair for first 15 min)
- No WG telecon on Thursday, 5 May 2011, due to IIW 12
- WG telecon on Thursday, 12 May 2011, at 9-10:30am PT (time chart)
- WG telecon on Thursday, 19 May 2011, at 9-10:30am PT (time chart)
- WG telecon on Thursday, 26 May 2011, at 9-10:30am PT (time chart) – Eve regrets; can Maciej do agenda, chair, and do notes-wrangling?