# UMA telecon 2010-10-28

## UMA telecon 2010-10-28

- Date and Time
- Agenda
- Attendees
- Minutes
    - New AI summary
    - Approve minutes of 2010-10-14 and 2010-10-20 meetings
    - Action item review
    - Review action and discussion items from Paris F2F
    - Resource registration (new draft from Maciej)
    - Agenda-bashing for IIW F2F
- Next Meetings

### Date and Time

- WG telecon on Thursday, 28 Oct 2010, at 9-10:30am PT (time chart)
    - Skype line "C": +9900827042954214
    - US: +1-201-793-9022 | Room Code: 295-4214

### Agenda

- Roll call
- Approve minutes of 2010-10-14 and 2010-10-20 meetings
- Action item review
- Brief updates from the wider UMA world
- Review action and discussion items from Paris F2F
- Resource registration (see new draft from Maciej, coming shortly)
- Agenda-bashing for IIW F2F
- AOB

### Attendees

As of 11 October 2010, quorum is 7 of 12.

1. Catalano, Domenico
2. D'Agostino, Salvatore
3. Fletcher, George
4. Holodnik, Tom
5. Machulak, Maciej
6. Maler, Eve
7. Moren, Lukasz
8. Scholz, Christian

Non-voting participants:

- Mark Lizar
- Cordny Nederkoorn
- Mike Seilnacht
- Anna Ticktin (staff)

Regrets:

- Kevin Cox
- Thomas Hardjono
- Torsten Lodderstedt

### Minutes

#### New AI summary

| | | | |
|---|---|---|---|
| 2010-10-28-1 | Eve | Open | Work with Sal and George to put together a set of flow options/user stories for review at the IIW F2F. |

Quorum was reached.

#### Approve minutes of 2010-10-14 and 2010-10-20 meetings

Minutes of 2010-10-14 and 2010-10-20 meetings APPROVED.

#### Action item review

- 2010-09-30-1 Eve Open Incorporate Fraunhofer's input on the location scenario into the Scenario document. (Mario's document is here.) Eve suggests that we treat Mario's document on a separate track, seeing it as an "advanced" person-to-person/mobile app location scenario vs. Eve's "basic" one. Treat this AI as OBE.

- 2010-10-07-2 Sal, Domenico Open Propose the next version of the trusted claims solution, making appropriate simplifying assumptions. Domenico has sent out a new set of UX wireframes and flows (web sequence diagrams are here), but hopes to continue revising the document with Sal.

## Review action and discussion items from Paris F2F

Maciej comments that people were worried about the protocol's complexity from the perspective of a user. Some suggested that the entire flow should be possible to initiate only when a user wants to share a resource. Eve wonders if we can map out a set of canonical UX flows through the entire protocol, choosing a different entry point each time. George comments that this would flush out the precise requirements and constraints on dynamicism across all the pairwise relationships that need to be set up. Where could conventions and defaults simplify the complexity of a user's experience? From a protocol level we need to support ultimate dynamicism, but there will be many cases where we don't need that flexibility.

The newly updated basic location scenario describes, for starters, a "host-initiated" flow. And Maciej's new resource registration draft selects the host as an initiation point for setting up sharing/protected/policy. The SMART project folks have also seen that people would want to start at the AM to protect/share things, but since the AM would be visited less often, he decided not to cover it in his draft. Eve sees the usefulness of an AM-initiated protection flow if a person is trying to protect/share several things using the same policy (such as a "family" ACL).

So we seem to have the following overall "tasks" that a person would perform, and we can break them down by initiation point:

- Protect/share a resource
- Protect/share multiple resources from the same host
- Protect/share multiple resources from multiple hosts
    - Host-initiated (Maciej's latest draft solves for this)
    - AM-initiated (this has protocol implications, e.g. it needs "pull" registration, so Maciej has left it out for now, for simplicity)
    - (In the person-to-self sharing case, is there a requester-initiated option?)
- Define/change policy (may be embedded in protect/share or may be standalone; could include change of desired scope)
- Host-dictated change of scope (John Bradley question from the Paris F2F?)
- Host-AM introduction (may be embedded in other flows or may be standalone)
    - Host-initiated
    - AM-initiated (what would that look like?)
- Resource discovery/provisioning
- Revoke access

Mark is interested in elucidating the flow of "notice" from the user to the host.

We'll take this further at the IIW F2F.

## Resource registration (new draft from Maciej)

Maciej walked the group through his draft. The flow choice we made is discussed more above (host-initiated selection of a resource for protection). Then the host "pushes" a form-encoded set of information about the resource and scopes. The user gets redirected to the AM to attach policy to it, and ultimately the user gets redirected to the host to continue doing whatever they were doing. This is the way the SMART project currently implements resource registration. They currently assume that the host-AM introduction task was performed previously, but it's possible for this task to be handled dynamically.

The reason JSON is not used (for the host's request message containing the resource info to register) is that the form-encoded format is most natural for the host to "speak". JSON is used in responses from the AM. This draft follows Christian's proposed "push" flow to a first approximation.

The draft involves a resource URI and an optional set of scopes, i.e., actions on the resource. Eve wonders if we could have a two-level resource registration format, where in the case of "API-style" protected resources you'd typically have a trivial single resource URI, and all the interesting bits would be in the list of potential scopes. Christian is potentially okay with the two-level approach but mostly wants to have a single specified answer to experiment with. Does it make sense to provide a place from which scope descriptions could be pulled? Right now, it's only possible to have "display names" in a single language. Eve wonders why the example on page 3 doesn't say "scopes=edit,view". The reason they have proposed it this way, with parameters that implicitly refer to scope, is that it provides a way to supply "display names". But an explicit "scopes" parameter could be provided along a pointer for discovering descriptions the way Christian has suggested.

Also, what about registering resources in batch? In Maciej's work they have not accounted for this case anymore.

If the user chooses to constrain the possible scopes at the host, they can do that, but this would apply to *all* sharing managed through the AM. The protocol being proposed by Maciej allows for the list of scopes to be whatever the host allows, so it's implementation-dependent. Eve believes it may be confusing for Alice to be in the "host-initated protect/share" flow and to choose any scopes on the host side, since she may have "sharing with Bob" in mind and not yet "managing sharing" generically for that resource. Thus, right now she prefers an implementation choice where the host doesn't expose to the user what scopes it's registering. Maciej agrees.

What happens if Alice wants to share a resource with Bob on Monday through this flow, and with Carol on Tuesday through a similar flow? And what happens if the scopes are reduced or otherwise changed through this process? Does the registration info get overwritten on Tuesday? Maciej says the host should re-register the same resource using the same flow, to account for the user having, say, deleted the resource registration on the AM side (is that a new flow/user story?). The approach he is taking for now is that, to minimize resource state management between the host and AM, the host should control all canonical resource registrations.

Regarding scopes, Eve's new location scenario work highlights a question about how the OAuth system of scopes matches with UMA's system of user-dictated scopes. Do we need to have a claim communications cycle that explicitly collects acknowledgment from the requester that a particular set of scopes is all they'll get an access token for, or should we leave scope management entirely to the OAuth layer? We'll ask this question next week.

### Agenda-bashing for IIW F2F

- User stories/tasks/flows
- Resource/scope registration

## Next Meetings

- WG F2F on Monday, 1 Nov 2010, at 11am-5pm PT (time chart) - no dial-in, and no telecon this week
- WG telecon on Thursday, 11 Nov 2010, at 9-10:30am PT (time chart) - Maciej to chair?