UMA telecon 2010-08-05

UMA telecon 2010-08-05

- Date and Time
- Agenda
- Attendees
- Minutes
  - New AI summary
  - Roll call
  - Approve minutes of 2010-07-29 meeting
  - Action item review
  - Upcoming focus/legal meetings?
  - Scheduling elections of two members of leadership team due to WG anniversary
  - Status reports from the wider UMA world
  - Dynamic client registration I-D (latest draft, focus meeting notes)
  - Resource Registration spec (latest draft, focus meeting notes)
- Next Meetings

Date and Time

- WG telecon on Thursday, 5 Aug 2010, at 9-10:30am PT (time chart)
  - Skype line "C": +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214

Agenda

- Administrative
  - IRC channel reminder: #umawg on irc.freenode.net (web interface)
  - Roll call
  - Approve minutes of 2010-07-29 meeting
  - Action item review
  - Upcoming focus/legal meetings?
  - Scheduling elections of two members of leadership team due to WG anniversary
  - Status reports from the wider UMA world
- Dynamic client registration I-D (latest draft, focus meeting notes)
  - Hopefully approve final draft for contribution to IETF
- Resource Registration spec (latest draft, focus meeting notes)
  - Report on and discuss focus meeting results
- AOB

Attendees

As of 28 July 2010, quorum is 5 of 9.

1. Fletcher, George
2. Hardjono, Thomas
3. Holodnik, Tom
4. Machulak, Maciej
5. Maler, Eve
6. Scholz, Christian

Non-voting participants:

- Kevin Cox
- Gerry Gebel
- Mark Lizar
- Anna Ticktin (staff)

Regrets:

- Lukasz Moren
- Domenico Catalano
- Nat Sakimura
- Trent Adams

Minutes

New AI summary

<table>
<thead>
<tr>
<th>2010-08-05</th>
<th>Eve</th>
<th>Open</th>
<th>Edit draft 00 of dynamic client registration draft and submit to IETF.</th>
</tr>
</thead>
</table>
Roll call

Quorum was reached.

Approve minutes of **2010-07-29** meeting

Minutes of **2010-07-29** meeting APPROVED.

**Action item review**

- 2009-12-03-4 Eve Open Add terms-negotiation scenarios to Scenarios document.
- 2010-06-17-1 Christian, Eve Open Work on the conversion of the core spec to xml2rfc. Now closed.
- 2010-07-08-2 Christian Open Automate the process of generating viewable HTML and TXT from the xml2rfc files and put them in a consistent place. In progress.

**Upcoming focus/legal meetings?**

Mark Lizar is working with Anna to try and schedule a semi-regular series of legal subteam meetings. Stay tuned.

Eve will hold a focus call tomorrow, Friday, 7-9am PT/3-5pm UK, on line C. The main purpose is for her and Maciej to sync up, but all are welcome to join.

**Scheduling elections of two members of leadership team due to WG anniversary**

The chair and use cases editor positions (currently held by Eve and Hasan) will be up for re-election by Aug 18. Eve nominate herself for chair again, and we anticipate that Mario Hoffmann from Fraunhofer will nominate himself for use cases editor. He will be getting active in the group shortly.

**Status reports from the wider UMA world**

Maciej reports:

Maciej, Lukasz, and Prof. Aad van Moorsel are submitting a paper to the *Middleware for Service-Oriented Computing workshop* associated with the upcoming Middleware conference. The paper is about their UMA/j implementation framework. Also, the SMART UX study will publish some results and new mockups soon.

Eve reports:

She, Maciej, and Trent met last week to discuss how to bring the matching funding request from Newcastle forward. Expect to hear more by next week.

Tom asks:

What's the PII conference going to be like? Something like the Tech Policy Summits in the Bay area. Eve recommends it, though it's a new event.

**Dynamic client registration I-D** ([latest draft](#), [focus meeting notes](#))

The issued_at and expires_in parameters will be left in the I-D, on the assumption that they're optional anyway and it's just food for thought for the OAuth folks. They can always toss one or both if they want.

The question of the native app flow gives us three possibilities: Indicate the need but don't provide a solution, or indicate the need and provide a few draft solutions and implications and considerations, or indicate the need and provide a single fully fleshed-out solution. Eve believes she now has a good enough understanding some of the options to go the middle route.

And do we need both push and pull options? Since pushed metadata could be signed, and the domain of the client could be used to get ("pull")! a public key with which to verify such a signature, is that sufficient security compared to what you could get through metadata pull? Push is a minimum bar we need to cover for the behind-the-firewall cases. But in push, there's no way to verify the actual content of the metadata being pushed; it has to be accepted as self-asserted. And the key management picture has more vulnerabilities and difficulties for metadata push. Since same-domain comparisons are more brittle in complex deployments with proxies and such, just relying on comparing a client's domain and any provided metadata URL may not be sufficient, so signing and verifying a signature (of either pushed metadata or of a pushed URL that points to metadata) is needed in the worst case. Eve can include this discussion of considerations in the draft as well.

Regarding the question of issuing client credentials to instances of applications vs. categories of applications, this should be discussed as part of the requirements. There are interesting implications around what you subsequently show users to confirm that the "right app" is getting an access token, particularly in the context of needing to ensure that the metadata being gotten for the app is "true". This discussion could be added as part of requirement 2.4.

Finally, Nat had suggested to point to the OAuth signature draft and "inherit" its solutions, security considerations, and vulnerabilities. Eve can do that.

The group plans to vote on each draft of this I-D that gets contributed to the IETF going forward.

MOTION: Thomas moves that draft 00, edited by Eve according to the instructions received in UMA telecon 2010-805, be contributed to the IETF on behalf of the UMA WG. APPROVED.

**Resource Registration spec** ([latest draft](#), [focus meeting notes](#))

Let's take a step back and discuss the use cases we want to solve for users' desires. Eve's original conception was that an AM would protect "everything" rooted in a host's domain, by default. But it quickly became clear that a user might have a policy that applies to "all photos at host X", such that when the user uploads photos at host X, they should be automatically covered if there is a policy that says "protect all photos at host X in this way", which implies a push of resource information from host to AM.
Maciej and others on the SMART project have had some learnings from the UX study that suggest users want to be in control of saying which specific resources are protected, both while they are visiting the host and while they are visiting the AM. Each of these circumstances has different protocol implications.

Let's start a thread on the list to hone a set of use cases, and once we get agreement, how to solve them using protocol flows will probably "pop out", at least at a high level. And once we have that approved set, we can include them directly in the spec.

We have a design principle that dictates that the AM shouldn't have to have any resource-specific knowledge in order to help the user craft policies. Somewhat similarly, Maciej is unhappy with the scopes/actions portion of Eve's latest draft, and would prefer that the AM only learn about resource locations.

We'll focus exclusively on resource registration use cases over the next week.

**Next Meetings**

- Subteam meetings Friday, 13 Aug 2010, at 7-9am PT (time chart) on our usual line C
- WG telecon on Thursday, 12 Aug 2010, at 9-10:30am PT (time chart) on line C