UMA telecon 2009-10-08

UMA telecon 2009-10-08

Date and Time | Attendees | Regrets | Agenda | Minutes | Next Meeting: UMA telecon 2009-10-15

Date and Time

- **Day:** Thursday, 8 Oct 2009
- **Time:** 9:00-10:30am PDT | 12:00-1:30pm EDT | 16:00-17:30 UTC (time chart)
- **Dial-In:**
  - Skype: ++9900827042954214
  - US: +1-201-793-9022 | Room Code: 2954214 (other local country numbers available on request)

Attendees

Voting participants:

1. Akram, Hasan
2. Bryan, Paul
3. Catalano, Domenico
4. Davis, Peter
5. Hanson, Michael
6. Lizar, Mark
7. Machulak, Maciej
8. Maler, Eve
9. Scholz, Christian
10. Smith, Bill
11. Stollman, Jeff

Guests:

- Joni Brennan (staff)

Regrets

- Trent Adams
- Iain Henderson

Agenda

- Roll call
- Approve minutes of UMA telecon 2009-10-01
- Discuss upcoming meetings:
  - Add variation to group meeting time to make it easier for Japan-based participants?
  - IIW planning
- Action item review
  - Michael: Create a scenario, or a use case off the Calendar scenario, that explores the need for entity #4 to approach the other entities in the context of some unique entity #5.
  - Eve: Confirm IIW-timeframe meeting location.
  - Revise the wording of the "Resource-specific policy limitations" requirement.
- Discuss spec progress (Paul)
- Review proposed requirements
- Discuss new and revised scenarios and schedule acceptance votes
- AOB

Minutes

Roll call

Quorum not reached.

AI:

Eve	Open	Do a non-voting participant declaration round. Make this a standing action item whenever a meeting has not reached quorum.)	

Approve minutes of UMA telecon 2009-10-01

Deferred due to lack of quorum.

Discuss upcoming meetings

- Add variation to group meeting time to make it easier for Japan-based participants?

Eve had suggested to Nat Sakimura that we could schedule an occasional meeting time that's better for Asia participants, and he expressed interest. We think we could make every fourth meeting be at 1-2:30pm Pacific on Thursdays instead of 9-10:30am Pacific. It's clear on the Kantara calendar.

AI:

Eve	Open	Check with Nat to see if we can start an every-fourth-week meeting time change on Oct 15.	

- IIW planning

We have a meeting room confirmed in the Computer History Museum in Mountain View. We'll work up an agenda eventually. We might be able to "cleverly Skype" the event.

Action item review

- Michael: Create a scenario, or a use case off the Calendar scenario, that explores the need for entity #4 to approach the other entities in the context of some unique entity #5. This is CLOSED, based on his email that Eve forwarded to the list this morning.
- Eve: Confirm IIW-timeframe meeting location. CLOSED.
- Paul: Revise the wording of the "Resource-specific policy limitations" requirement. Still OPEN.

Discuss spec progress (Paul)

The spec writing has just begun. He has created some boilerplate content.

Review proposed requirements

Review the new Consumer Delegate scenario

We discussed Mike's new scenario, forwarded to the list with comment.

Mike's goal was to avoid creating an "omnipotent token" that allows a requester app to use the token for access on the behalf of other parties. Mike based his scenario on concerns arising from recent OAuth discussions.

Eve suggests that a "base" scenario here is that there's a single human being as both the authorizing user and the requesting user, and that there's a single company that hosts its own Requester application. Mike's scenario is a variant where the company outsources its Requester application-hosting to another party (BizTools).

Do we think we can really solve this? Today, app-hosting relationships like this are common, and involve an sharing of private keys (covered by service-level agreements), and concomitant "impersonation" of the company by the outsourced service. We're inclined to say that distinguishing between the two parties is *not* in our scope. This would be our first "rejected" scenario/use case if so, which is a good thing for exploring exactly where our boundaries are.

AI:

Eve	Open	Shove Mike's scenario/use case into the Scenarios document.	

Discussion of requirement P4

Christian made a comment on proposed requirement P4. Eve was trying out a requirement here, but seems to have gotten it wrong. Paul states the requirement as follows:

"Correlation of Authorizing User by multiple Hosts: For resources at Host X and resources at Host Y, X and Y must not find out, through their relationship with the AM, that the same Authorizing User uses the other Host." For example, a user might use the same AM to protect resources at LinkedIn along with their personal interests and hobbies.

We have tentatively agreed to this requirement, but we want to sleep on it (and don't have quorum to vote on it anyway).

A consequence of this requirement would be that the protection of the Authorizing User's privacy extends to trying to protect their connections to each Requester. However, because of the consistency of the IP address that might be used by the Requester app, we can't offer a blanket guarantee. Thus, we're inclined not to state this as a requirement.

New emerging design principle: Our goal is to protect the privacy of the Authorizing User as best we can, but when the AU is the same person as the Requesting User, they are not protected *as* a Requesting User.

AI:

Eve	Open	Capture the two emerging design principles we have identified to date in the Requirement document.	

Google's handling of desktop apps in OAuth

Mike notes that Google's recent OAuth deployment documentation suggests that they are somewhat outside the mainstream in their handling of desktop app flows – it redirects through a browser and through google.com. Security protection uses an "anonymous/anonymous" consumer key in their desktop case, which makes it weaker than the web app case. His recent email has more details.

Distributed services scenario

Even though Christian had dropped off, we briefly discussed this. Let's put this on the docket for next week. Also please look at the Project hData scenario, which looks similar. (The main Project hData site is here.)

AI:

Eve	Open	Invite Project hData's Gerry Beuchelt to next week's meeting.	

Next Meeting: UMA telecon 2009-10-15

In next week's call, we'll focus on:

- Review spec text
- Distribute services scenario and its several use cases

- **Day:** Thursday, 15 Oct 2009
- **Time:** TIME MAY CHANGE: STAY TUNED:9:00-10:30am PDT | 12:00-1:30pm EDT | 16:00-17:30 UTC (time chart) ????
- **Dial-In:**
  - Skype: ++9900827042954214
  - US: +1-201-793-9022 | Room Code: 2954214 (other local country numbers available on request)