UMA telecon 2009-10-01

UMA telecon 2009-10-01

Date and Time | Attendees | Regrets | Agenda | Minutes | Next Meeting: UMA telecon 2009-10-08

Date and Time

- **Day:** Thursday, 1 Oct 2009
- **Time:** 9:10-10:30am PDT | 12:10-1:30pm EDT | 16:10-17:30 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 in attendance:

1. Adams, Trent
2. Akram, Hasan
3. Andrieu, Joe
4. Bryan, Paul
5. Catalano, Domenico
6. Davis, Peter
7. Fletcher, George
8. Hanson, Michael
9. Henderson, Iain
10. Hogberg, Jonas
11. Lizar, Mark
12. Machulak, Maciej
13. Maler, Eve
14. Scholz, Christian
15. Smith, Bill

No non-voting participants in attendance.

Regrets

- None

Agenda

- Roll call
- Approve minutes of UMA telecon 2009-09-10, UMA telecon 2009-09-17
- Discuss planned slight adjustment to group meeting time (x:00-y:30)
- Action item review
- Discuss meeting schedules for the IIW timeframe in early November
- Discuss OAuth reuse vs. "inspiration" in the ProtectServe protocol sketch, to inform spec writing
- Discuss proposed requirements and ways of collecting requirements going forward (see recent email – after 1 Oct 09, use this link to the email instead)
- Discuss any questions about new and revised scenarios and schedule acceptance votes
- AOB

Minutes

Roll call

Quorum (13 of 24) reached.

Approve minutes

All pending meeting minutes (UMA-telecon-2009-09-10 and UMA-telecon-2009-09-17) APPROVED by unanimous consent.

Group meeting time

Confirmed that we'll go back to meeting x:00-y:30 (starting at the top of the hour and maxing out after 90 minutes) in future.

Action item review

- 2009-08-27-4: Hasan: Derive and document proposed requirements from the Calendar scenario. We decided to close this one, as the requirements work done to date on the list meets the need.

- 2009-09-03-2: 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. Still open. Michael will do this by next week.
- 2009-09-17-3: Eve: Revise the Issue in the scenario doc regarding how requesters can meet terms, to incorporate the discussions that have taken place to date. Still open. Eve will do this by next week.

IIW meeting

George may or may not be able to make it because of the OpenID meeting going on that same day. There may also be an XRI/XRD meeting sometime around then. We'll still plan to meet Monday 1-5pm.

AI:

Eve	Open	Confirm IIW-timeframe meeting location.	

OAuth faithfulness in UMA spec

Paul is getting ready to write the specs, and the first technical question he has faced (for some time now) is: How little can we deviate from OAuth? In the ProtectServe work, one area of the protocol sketch had to deviate from OAuth because Hosts (in our view of things) can't be trusted with information that would let them correlate a user's activities at multiple Requesters (Consumers). OAuth requires a consumer key and a (sometimes optional) access token, but ProtectServe needed to enforce that *only* an access token be passed. This is necessary because we bifurcate the Host (policy enforcement point) from the AM (policy decision point); otherwise the Host, when furnished with the consumer key, could impersonate that consumer.

We want be able to reuse existing OAuth libraries if we can. We could profile OAuth to require the access token, but requiring the consumer key *not* to be provided counts as an extension that would hamper reuse. What if we were to publicly document a single standard consumer key? This doesn't entirely help, since Requesters still need to register themselves (each uniquely) with the AM.

It's acknowledged that we're still "deviating" from OAuth in terms of adding functionality. So reusing a library amounts to getting a leg up on implementing the higher-level functionality.

George notes that OAuth is heavily SP-centric. If you throw an "IdP"/"STS" (in our case an UMA AM that issues tokens) in there, things start to break. Eran and Yahoo! seem to be looking at the token-issuing role as being important to take into account. George believes we should take our issues into the IETF.

George wonders if the AM could *issue* consumer tokens and keys. But Paul notes that we still have to prevent the Host from getting visibility into that data.

The motivation for requiring the consumer key was to allow the Host (SP) to blacklist certain Requesters (Consumers/Clients). Do we want to preclude this possibility in UMA? We also want to preserve the ability for any user to choose any AM for a managed resource, even if the same Host serves multiple users who have different choices of AM. George asks if we could add a *new* piece of information to solve the problem.

Paul pushes back on seeing the AM as an "IdP", since it's not responsible for assigning an identifier that has larger meaning.

Eve observes that maybe we're having this difficulty because the "Requesting User" behind the Requester is potentially a different person from the Authorizing User (whose accounts on the AM and the Host both represent the "same person").

Michael notes that the current discussions around the OAuth/OpenID hybrid may be resulting in work that we don't want to preclude with our decisions.

We do want to avoid excessive episodes of user authentication, whether we're talking about Authorizing Users or Requesting Users. So when you as an AU want to set up Flickr (a Host) to listen to your AM, you first tell it who your AM is (in pure OAuth fashion). And then if you are also the RU, you provision Piknik (a Requester) with your Flickr resource URLs; this is what's currently not using pure OAuth in our scheme. The next question is: How do you, as the RU, *give permission* to let Piknik get in? The intention was to make this configurable and largely out of band of the protocol proper (e.g. by configuring the policies to say "whenever any Requester approaches a resource for the first time (or every time), ask me by SMS or XMPP or whatever for approval". This is because the user might not be logged into the AM at the time the Requester approach happens.

AI:

Eve	Open	Send out the draft authentication model document to the list.	

So how should we handle this OAuth-faithfulness issue? We agreed to:

- Write and publicize an UMA spec, as an IETF I-D, that deviates from OAuth for our own security/privacy reasons
- Write up the details of the OAuth changes needed, to stimulate consideration of our change request in the IETF (as a "real OAuth spec"?)
- Consider the implications of the OAuth-OpenID hybrid work as best we can (given that this conversation has been happening privately)

Christian will continue to pursue his "proxy"-based approach in parallel, and we can compare as we go.

We'll assume that OAuth 1.0a is our target for discussion, since that is what has been implemented and widely deployed. (It contains the verifier attributes for mitigating the session fixation attack.) What they're doing next is to modularize, and continue to modify, the specs. For example, the redirect loop will be modularized to become merely one way of getting an access token.

Requirements discussion

We discussed the following proposed requirements:

- "Host/AM separation: It must be possible to provide Host and AM functions in separate Web domains."

APPROVED by unanimous consent.

- "Resource orientation: User data access and service access must be enabled through accessing Web resources that have URLs."

APPROVED by unanimous consent.

- "Resource-specific policy limitation: The deployer of an AM must not be required to do any special configuration to enable the AM to present to the User, or to make decisions regarding Requester access to, any resource-specific policies that apply to the resources available at a Host (such as photos of different resolutions, or calendars covering different time periods or levels of detail, or locations at address vs. city level)."

We deferred this one. We like the idea, but agreed the wording sucks. 🙂

AI:

Paul	Open	Revise the wording of the "Resource-specific policy limitations" requirement.	

- "Terms persistence: A set of terms for accessing a resource must be accessible as a Web resource with a persistent URL."

We don't want to get into the problem of persistently storing terms from ten years ago, nor can we prove that two representations of a resource will be "the same" over time.

We discussed the differences between policies and terms. Policies can be unilaterally executed by the AM ("access this resource a maximum of six times"), but terms require agreement on the part of the Requester. In a way, they can fall on a continuum, since we could decide that Requesters have a right to be told some or all of the policies, and since we could also "soften" the way terms work for some scenarios, where the AM merely "asks" the Requester to adhere to the conditions rather than making them promise to adhere to them.

AI:

Eve	Open	Create a wiki page to discuss/explain policies and terms.	

We'll defer this requirement, but as a new starting point, let's remove the "persistence" goal:

- "Terms as resources: A set of terms for accessing a resource must be accessible as a Web resource with a URL."

(Note that the discussion above about not allowing Host correlation of Requesters should be a new pending requirement.)

AI:

Eve	Open	Create a new Requirements document containing all the currently proposed and approved requirements.	

Next Meeting: UMA telecon 2009-10-08

- **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)