UMA telecon 2010-02-18

Date and Time
- **Day:** Thursday, 18 Feb 2010
- **Time:** 9:00-10:30am PST | 12:00-1:30pm EST | 17:00-18:30 UTC (*time chart*)
- **Dial-In:**
  - Skype: +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)

Agenda
- Roll call
- Approve minutes of UMA telecon 2010-02-04 and UMA telecon 2010-02-11
- Action item review
- Review F2F plans
- Spec review: editor’s choice
- Lexicon discussion
- Scenario review
  - Custodian (splitting “authorizing user” and “host service user”)
  - Employer/employee (other mandatory access control in addition to UMA discretionary access control)
  - And the “multiple protections on a resource” thread
  - Health data (trusted dynamic resource discovery)
- AOB

Attendees
As of 14 Feb 2010, quorum is 8 of 15.

1. Adams, Trent
2. Akram, Hasan
3. Andrieu, Joe
4. Bryan, Paul
5. Catalano, Domenico
6. Holodnik, Tom
7. Lizar, Mark
8. Machulak, Maciej
9. Maler, Eve

Regrets:
- Bill Smith

Minutes

**Roll call**

Quorum was reached.

**Approve minutes of UMA telecon 2010-02-04 and UMA telecon 2010-02-11**

Minutes of both meetings APPROVED.

**Action item review**
Discussion of analytics wireframes

Paul comments that it's possible to put too much emphasis on analytics. The right to control data access doesn't extend to controlling the data once it has left the host. We certainly don't want to imply that DRM is involved, for example.

In addition, note that any audit logs available to the AM reflect, at best, a host's request for a policy decision, rather than actual access events (and decisions can be cached, such that many accesses could correlate to a single policy decision request. Many moons ago, the idea of adding an optional /required protocol exchange where hosts can give AMs accurate access logs, is it still interesting to have the coarse granularity of using policy decisions (especially knowing the length of decision caching) as a proxy for windows of access opportunity, since we know a request for access was made, and a contract was entered into, and a policy decision was made and conveyed along with an acceptable cache period? It seems so (and Eve invites anyone who needs more precision to write a scenario proving it). It's certainly possible for AM services to make available to their users a means for setting this validity period; the protocol is silent on this. And if you need to prove a requester actually got certain access at a certain time for legal reasons, you could go to the host to establish that.

Joe suggests that trend analysis would be useful. And Paul wonders if the privacy exposure knob is meant to be "read-only" or "read-write" (so that the user can turn the knob); the signals to the user need to be clear.

Domenico explains the many factors that can be used in calculating a privacy risk exposure. His final slide explains this a little bit.

Paul comments that we should be clear which parts of "UMA-native" and which parts are value-add that an AM offers (e.g. the classifications of personal data).

Eve notes that OAuth-style connections might involve putting data back into a host, so that presents other opportunities for analytics.

Review F2F plans

Let's meet just the Wednesday 9am-noon, instead of also meeting Tuesday afternoon. We're likelier to get quorum this way. We'll still cancel the Thursday call that week.

Lexicon discussion

Joe notes that "user agent" isn't in our lexicon; Eve will add a reference to the source (HTTP spec?) of that term. He also notes that the terms PDP and PEP, being from a particular domain, don't have a place in any "official" diagram explaining the high-level protocol view.

On the contractual diagrams, Joe notes that there are secondary TOSs and EULAs that generally obtain between the user and all the intermediary parties. We could add secondary arrows showing these. Eve wonders if it's truly correct to show a single access authorization agreement document, vs. the back-and-forth negotiation that our protocol currently involves. Paul and Joe concur that the current diagram and lexicon term aren't right; a contract offer could be embedded in the AM's claims-required message, which the requester could fulfill/accept in the response message, but if the AM asks only for proof of age, there isn't an explicit agreement.

(Eve then freaks Paul out by noting that our model doesn't preclude requesters from including claims-required blocks in their response containing claims! But we don't want to get into this amount of complexity.)

How, then, do we talk about the legal level of what we're doing, so that the result is enforceable? If "contractual view" and "terms negotiation" and "access authorization agreement" aren't correct, we need other language. Joe asserts that either contracts are involved, or warrants and representations are involved. E.g., if someone warrants that they're over 18 and they're not, how can we make this actionable? This seems to come down to the "promises vs. statements of fact" dichotomy we have already identified. Joe suggests just separating access authorization requirements and access authorization claims (which are promises and/or statements). And we need to define these extra terms. We will call this the "legal view". And we should ideally show claims-related documents flowing in the protocol view as well.

For the user experience views of the protocol, Joe would like to see an ordering of the arrows. Also, he would take out the words "service" in this diagram given that it only focuses on user interactions that are required for the protocol. Maybe the user experience views of the protocol therefore aren't even needed.
Joe's preference for "host service user" is to say "host user" instead, but we had some worry that this implies that the user is a host. We played with several other options in addition: "user of the host", "hosting user" (wrong), "primary resource user", and "primary resource controller". We didn't settle on an answer, but we started to deep-dive into discussing the custodian scenario.

**Custodian (splitting "authorizing user" and "host service user")**

We discussed, without firm conclusion, whether the UMA protocol can be completely silent on the split in user roles proposed by Eve. The split may not even be necessary, according to his conception. Paul will explain more in email.

**Next Meeting: UMA telecon 2010-02-25**

- **Day:** Thursday, 25 Feb 2010
- **Time:** 9:00-10:30am PST | 12:00-1:30pm EST | 17:00-18:30 UTC (time chart)
- **Dial-In:**
  - Skype: +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214 (other local country numbers available on request)