UMA telecon 2009-10-15

UMA telecon 2009-10-15

Date and Time | Attendees | Regrets | Agenda | Minutes | Next Meeting: UMA telecon 2009-10-22

Date and Time

NOTE: This month has a lot of summer<->winter time changes in it. Please take careful note of your local hour.

- **Day:** Thursday, 15 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: 295-4214 (other local country numbers available on request)

Attendees

Voting participants:

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

Regrets

- Joe Andrieu

Agenda

- Roll call
- Approve minutes of UMA telecon 2009-10-01 and UMA telecon 2009-10-08
- Action item review
  - "Resource-specific policy limitations" requirement
  - Every-fourth-week meeting time change
  - Mike's scenario into document
  - Capture emerging design principles
  - Rope in Gerry Beuchelt
- Spec progress (Paul)
- Review proposed requirements
- Review distributed services scenario, particularly if Gerry is in attendance
  - See also Project hData use cases
- AOB

Minutes

Roll call

Quorum was reached (15 of 21).

Gerry introduced himself. He's with MITRE. He has a number of projects, a relevant one of which is hData. They are building a federated medical identity record system. UMA is of interest for patient authorization of access to records.

Approve minutes of UMA telecon 2009-10-01 and UMA telecon 2009-10-08

Motion to approve both meetings APPROVED.

Action item review

- 2009-10-01-3 Paul Open Revise the wording of the "Resource-specific policy limitations" requirement. (Discussed today.)
- 2009-10-08-2 Eve Open Check with Nat to see if we can start an every-fourth-week meeting time change on Oct 15. (Haven't heard back.)

- 2009-10-08-3 Eve Open Shove Mike's scenario/use case into the Scenarios document. (Closed.)
- 2009-10-08-4 Eve Closed Capture the two emerging design principles we have identified to date in the Requirement document. (We reviewed the current state of this document.)
- 2009-10-08-5 Eve Open Invite Gerry Beuchelt to next week's meeting. (Closed.)

Spec progress (Paul)

Paul has started the spec writing, but it's not in reviewable form yet. He's now working on some of the detail around metadata that needs to be transferred. He'll get a draft into the wiki by early next week.

Review proposed requirements

P9

Current wording: "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."

Paul wonders if we can be more precise, since this is a bit passive.

"For two resources on different Hosts owned by the same Authorizing User and managed by the same AM, the AM must not allow one Host to be able to discover the User's relationship with the other Host."

Motion to accept this new version of P9 APPROVED.

P1

This is the one about resource-specific policy limitation. Paul has an AI to revise this one, but let's discuss now.

Do we have to discuss the various use cases around the "location scenario" and maybe other scenarios before we can decide on this one? E.g., if the Host (also an OAuth SP) does location services, and it makes available three levels of resource filtering such as address, city, and continent, what if it could tell the AM three URLs that represent these filtering types such that a user can manage such filtering settings at the AM rather than each Host? Could these be conveyed by something like matrix parameters (part of the URL path, not part of the query)?

George wonders if we can start small and layer more sophisticated functionality on top. (One way to do location filtering is "10-meter accuracy", "100-meter accuracy", etc.) Could we be satisfied with people still managing such settings at the Hosts, but maybe with the AM *displaying* the filtering chosen? The fact that a Host can always make different resources for each filtering level/type gives us a big "out" here.

How about this for P1: "Representation-agnostic AM: The AM is not required to understand the representations of resources it is charged with protecting." Examples: location, calendars, photos, etc.

Motion to accept this version of P1 APPROVED.

Motion to **reject** P4 APPROVED.

AI:

Eve	Open	Revise Requirements document to account for UMA telecon 2009-10-15 decisions.	

Review distributed services scenario, particularly if Gerry is in attendance

- See also Project hData use cases

Eve noticed that the "distributed services" scenario is something of a design pattern, which Gerry's hData project also invokes.

Gerry walked us through the slides. The basic motivation behind hData is that there's a lot of overhead in existing health record standards. The old MUMPS system is still being used today. HL7 is frequently used today but it's extremely hard to develop to. The current systems use a single huge record, which is cumbersome. The hData Record Format or HRF has a manifest/root document and sections that are lower in the path. Section URLs resolve to Atom feeds. You should be able to serialize and ship around documents as zip files as necessary.

UMA comes into the hData picture where fine granularity and interoperability between systems are needed. The "hData discovery system" could be a HealthVault or similar.

Question from Paul: Can the policy decision about letting a party get access to a health data feed be made in real time, or does it have to be statically set at the hData discovery system?

Christian comments that the hData scenario is indeed pretty similar to the distributed services example (which references social networking). Paul notes that the basic assumption of UMA is that the AM makes policy decisions in real time, so that enforcement of policy does involve going and asking for policy decisions. Tokens can be cached for a period of time, however.

What's the relationship between a discovery system, or service catalog or discovery service or similar, and an AM? (Both Gerry and Christian are assuming that something like XRD would be used.) Christian's scenario involves doing "mass authorizations". We can describe this as "pre-authorizing a Requester to access resources at known Hosts" before the Requester actually hits each Host.

Is the Requester coming to the AM/discovery service (let's assume they're colocated for the moment – it shouldn't be required but it's very handy) totally out of the blue? In this case, we have the problem of sufficiently identifying the Requester so that the User has a chance of understanding what policies to set. But that wasn't Christian's intent. However, some features of the ProtectServe sketch were already added in anticipation of the more extreme forms of needing to authenticate/identify/feel comfortable with a wide range of Requesters.

One question is whether we want to allow the User to "pre-approve" certain Requesters, and types of access, and resources for them to access. If the User were to publish their patient healthcare record URL on their blog (the "hey, sailor" pattern of provisioning the resource URL to potential Requesters), it should be possible for qualified professionals to "break the glass" and get to the record even if the patient is unconscious, by means of presenting a claim that says they're qualified to do so.

AI:

Eve	Open	Write a "Hey, Sailor" scenario to illuminate the needs around Requesters that ask for resource access without the User expecting them.	

How would health data be filtered for different providers? User interaction would be necessary. This will hopefully be amenable to value-add in the market.

So do we have a requirement to pre-authorize access before the Requester ever hits a Host? Or is it a requirement to pre-**authenticate** particular Requesters (like the service called "New Service" in Christian's wireframe diagram)? Gerry believes that mass authorization is *not* needed in his scenario, and in fact may be illegal in some regimes (e.g. maybe HIPAA wouldn't allow it?). Each case needs a custom pattern of access to various resources (various portions of the entire record).

We need to dig into this further with Christian, perhaps next time.

Gerry	Open	Write an hData scenario for the Scenario document.	

Today, in the U.S., doctors make you sign a blanket HIPAA waiver. But the original intent was to allow patients to grant selective access. This is a lesson to us that we shouldn't expect people/systems to use really really fine-granular access options.

Next Meeting: UMA telecon 2009-10-22

- **Day:** Thursday, 22 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)