UMA telecon 2018-02-01

UMA telecon 2018-02-01

Date and Time

- Thursdays 9am PT
  - Screenshare and dial-in: https://global.gotomeeting.com/join/857787301
  - See UMA calendar for additional details: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Roll call
- Approve minutes
  - Approve minutes of UMA telecon 2018-01-18
- Note: Joint consent receipt ad hoc call happening in the next hour (see calendar)
- Legal update
- 2018 charter and roadmap discussion
  - Joint consent receipt work
  - Legal/business/trust (related to the above) (see relevant issues)
  - Extension opportunities (see relevant issues)
  - What else?
  - Updates on auxiliary material editing if any
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2018-01-18: APPROVED.

Note: Joint consent receipt ad hoc call happening in the next hour

Note! (see calendar)

Legal update

The Draft Report will be up shortly. Tim introduced Eve to an attorney who is interested in this work.

2018 charter and roadmap discussion

- Joint consent receipt work
- Legal/business/trust (related to the above) (see relevant issues)
- Extension opportunities (see relevant issues)
- What else?

Mike has mentioned an extension idea around JSON Logic, which describes a simple way to get AND/OR logic and has a lot of libraries. See this use of it; the idea is that the RS could express that the user could have (or the resource is associated with?) scope X OR scope Y (or something like that). Mohammad Jafari has recently release a new UMA server called Pauldron that implements some extension ideas. Eve and James have been discussing UMA requirements with some customers that may result in some extension proposals. We have saved off a variety of issues that might be interesting to look at once again. Justin notes that protected discovery may need some work.

Profiles are also interesting. Many probably want to remain third-party, but it would be nice to point off to them. Financial use cases are interesting. The Pensions Dashboard use case starts with a phase that's "mostly plain OAuth" with a bit of stuff where UMA is helpful, but then proceeds to a classic Alice-to-Bob sharing flow.

AI: Eve: Reach out to find what happened to the Pensions Dashboard profile doc and see if the WG should be pointing to it.

So what's our list of anticipated activities?

- Joint work with consent receipts
- Legal/business/trust (consider changing subgroup name?)
- Extension opportunities – decide which become work items as required
- Promote adoption – could offer guidance on profiling and extension creation by third parties in various sectors (gov, fintech, healthcare...)
- Promote interop? – known that it's challenging

Our familiar discussion about interop: Cross-matrix testing is not that great an experience or productive. A test framework is better. UMA, like OAuth itself, is more challenging to test than something like OIDC (it can protect any API, and more, it has more moving parts that have to interoperate). Assumption: Only AS conformance testing would be on the table first, as only OP conformance testing was done for the first long while.
Justinv is involved in the OB testing effort. A lot of community members would be interested to throw in on a broader conformance testing effort.

**AI:** Eve: Produce charter draft for review.

**Updates on auxiliary material editing if any**

No updates.

**(after end of call) Joint consent receipt/UMA ad hoc notes**

Attending: Andrew, Eve, Andi, Domenico, James, Justin, Sal, Tim, Colin

Our previous notes are here.

Andrew: A consent receipt fits in as an interoperable security audit log entry. It has richness of detail so that it can be processed as something that goes beyond security use cases. The goal is to fulfill the individual's objectives. Andi: If a company gets a subject access request, what happens next? If the audit trail includes a consent receipt, isn't it still very valuable to them? Okay, so maybe "security" isn't the best word.

The current design of Consent Receipts focuses on traditional opt-in consent. UMA is sort of more policy-driven.

Regarding dictating flows and formats: Interacting claims gathering is outside the view/scope of UMA; a profile could dictate a particular thing happening. There are several "consent receipt"-ish formats extant.

The Security Events WG formed a couple of years ago. We've identified more than just consents as artifacts deserving of "receipts". Would a security event token be appropriate, given this? Justin isn't sure that the SET is a good match at this point, actually.

Eve: Muses about the scope of the UMA WG regarding "receipt workflow" sorts of work. Should we be thinking bigger regarding things like the shoebox endpoint (while keeping it appropriately modularized)?

The regs that are dictating that a purpose statement be included (and have specific requirements) would seem to give problems to a RO-specified purpose (user-submitted terms). But why can't our license-based model carry a purpose?

What if we were to propose a POC that develops an end-to-end technical artifact/legal device connection? Tim: Go for the gold and make it GDPR-ready! What would such a POC entail? Does it depend on a running UMA instance, and/or CommonAccord, and/or template clauses, and/or what exactly? It would need to demonstrate:

- Some of the key mappings
- A realistic and evocative business use case – EU jurisdiction and (which?) sector
- A step-by-step end-user walkthrough with "receipts" that Alice (and Bob?) and Larry and Linda the Lawyers (for different parties – how many do we need?) find useful

Eve has an UMA health+IoT+IRM demo that we could perhaps "port" to smart home for this purpose. Let's figure out next steps in the Friday calls, e.g. timeline and answering all the questions posed above.

We decided that this served as our UMA Legal call for the week, 😔 and we'll cancel for tomorrow.

**Attendees**

As of 7 Mar 2017, quorum is 4 of 7. (Domenico, Sal, Maciej, Eve, Mike, Cigdem)

1. Domenico
2. Sal
3. Maciej
4. Eve
5. Mike

Non-voting participants:

- James
- Justin
- Mark