UMA telecon 2018-02-15

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 2018-02-01 and UMA telecon 2018-02-08
- Charter updating
  - See draft
- Consider Tim Reiniger as WG Legal Adviser
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2018-02-01 and UMA telecon 2018-02-08: APPROVED.

Discussion of the new Mozilla IoT gateway project

Here is the TechCrunch article. It is using JSON-LD. Eve mused on Twitter that it could integrate with an UMA AS to be a personal AS. Mike likes JSON-LD and noted that OTTO is using it in preference to Fast-Fed, which is using SCIM.

IoT use cases discussed in chat:

- Thomas: Can my home panel control all my smart-appliances and manage their respective access relationships
- Thomas: Alice-to-Alice
- Thomas: My washing machine be a "resource" to my Control Panel on the wall
- Sal: door controllers...
- Maciej: Thomas, I think the control panel would nevertheless be the client with the AS sitting somewhere else (potentially within the panel as well but not necessarily)
- Maciej: I’d prefer to connect my panel to my existing AS and then use it purely as the client, potentially requesting some new permissions as I add new resources (i.e. new locks and what not)
- Maciej: what do you think
- Sal: actually it needs to be able to run offline, so it end up being AS and RS and the reader is client
- Thomas: Agree. The OIC/OCF model is that there is a "Domain Controller" (not Microsoft AD). The DC will be our AS. The Panel will be the Client. Homeowner is the RqP
- Thomas: The thing is that some vendors are placing the DC board as part of the wall-panel.
- Thomas: The DC board could be (should be) part of the Gateway box.
- But our UMA model fits perfectly.
- Maciej: it does, yes
- Sal: yes, most of these things have pretty archaic architectures, UMA absolutely handles this better..
- Thomas: A bigger problem might be the multi-dwelling (non-Enterprise) use case. Example is an Apartment building where all the apartment units are leased.
- Thomas: The Building Owner is the legal owner, and owner of all AC/HVAC units inside each apartment.
- Thomas: It must allow service personnel access to each apartment.
- Thomas: So we potentially have a hierarchical UMA model.
- Thomas: Each apartment has its own AS. Then building owner has its "Super-AS".
- Maciej: with the 'slave AS' being clients relying on policies in the super AS
- Thomas: Yes. There will be local policies, and then building-wide policies.
- Sal: Yeah, the trick is not to have one offs and have it explode for every control point, 1000+ policies (I have seen this) may enable the disconnected use case but can croak the backend..
- Thomas: Agree.

Needing to push multiple tokens
Mike and Eve had been discussing offline that UMA1 allowed the pushing of multiple claim tokens, but we (deliberately) removed that capability in UMA2 at some point because we couldn't think of a use case. Mike actually has a use case at this point, which is to send, not multiple ID tokens per se, but "badges" such as professional certifications (so, third-party-asserted attributes). Since any claim token format can be defined by anyone, a "compound" claim token format could be defined to carry multiple tokens as necessary. Each badge would typically come from a different authority. There are various authorities: Badgr.io, cred.ly, trailhead.salesforce.com. A badge is just a simple JSON-encoded assertion. It's very similar to an ID token, only the recipient part is weak. The offline version of a badge ("baked") is signed. The hosted version is just a URL that you have to resolve (an "artifact" pattern!). There's an MIT project called BlockCert around verifiable claims about badges. (See our Requirements document for proposed requirement P11 for "verifiable claims" from 2009.)

Okay, so how does such a "verifiable claim" work securely and with privacy with an audience parameter? The issuer of a badge does specify an audience, after a fashion, by specifying an email address. Sovrin would say: Issue a unique DID per badge, then require that the recipient prove that they're the owner of the DID. Mike is working on use cases where simple possession can count for something too.

We went into a discussion of where, on a sliding scale of lightweight to deep security and privacy, we should aim our efforts, and an observation that specs often decide that the perfect is the enemy of the good. More best-practices development is usually welcome and beneficial.

**Charter updating**

- See draft

Discussion point: Given that the UMA architecture succeeded early on in ensuring that the "human as resource owner" use case, do the functional requirements, which focus heavily on this use case, need to be expanded to mention other kinds of resource owners? Eve has edited to say "a person (human or legal person)".

Also, what about devices as/managed by resource servers? Saying "managing data-sharing and service- and device-access relationships" gets us partly there, but what about the disconnection use cases? We only did part of that work in UMA2. We didn't get to a full set of work on locally validated self-contained RPTs. This might be seriously interesting extension work.

Let's think on the right way to add more indications of IoT to the charter.

We didn't vote on it today but we think we're close.

**Consider Tim Reiniger as WG Legal Adviser**

We discussed this. There is considerable support for having him in such a role! Is this the right name for the role? Can't think of suitable alternatives. No time for a vote at the end of the call, but we'll pick this up again next time.

**Attendees**

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

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

Non-voting participants:

- George
- Thomas
- Bjorn