UMA telecon 2019-03-28

UMA telecon 2019-03-28

Date and Time

- Thursdays 6am PT (during “summertime skew”, till Mar 31: 1pm UK, 2pm CET)
  - 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 of UMA telecon 2019-03-14
- IETF 104 recap and next steps
- Interop planning
- Charter refresh
- Meeting schedule
- AOB

Minutes

Roll call

Quorum was not reached.

Approve minutes

- Approve minutes of UMA telecon 2019-03-14

Deferred.

KNOW Identity recap

KNOW has largely been a "panel conference", which is good for people who don't know a lot yet and want to get broad knowledge fast.

George went to a blockchain panel. He heard the statistic 19, or perhaps 25, methods of registering DIDs. When you resolve it you get a JSON-LD defined schema. Every method can define within that schema its own methods of how that namespace works. IOW, it is a unique namespace. So, a thousand flowers are obviously still blooming. This is over and above Verifiable Credentials.

George was on a panel about standards, with Sarah Squire and others. There was a good breadth of experience there.

He believes this method doesn't solve privacy, but may enable privacy. It's a mindset change. For example, Google doesn't technically need any Verifiable Credentials. It just needs a consistent DID. (But their business model needs more...) Sovrin is adding a layer of private DIDs where you don't resolve them to get the public key and they don't (he thinks) go on the chain. It's all peer-to-peer. He was unclear how key rotation works at this point. There is continuing evolution, innovation, etc. at this point given the use cases they're trying to solve.

Adrian adds that he's been a part of the VC/DID work for some years and is glad to hear George bring this discussion here. He believes federation has reached its limits in terms of privacy. This new work is assigning DIDs to edges – to relationships – by virtue of the pseudonymous identifier. (Eve asks: Is that like pseudonymous identifiers in federation, though?)

IETF 104 recap and next steps

Eve's take, informed by debriefing Pedro who was in the room (we hope he can join us next week to discuss more in person): The audience was a little overwhelmed by both the amount of content and the comprehensiveness of the specs. Ludwig had sort of warned us about the "wall of text" effect. They did seem to be examining the proposition in good faith. Tony suggested simply using the token exchange spec. We understand where he's coming from in terms of the token semantics, but believe there would still have to be quite a lot of specification along the lines of exactly what we've done. FedAuthz would still have to exist to achieve the "wide ecosystem" goal. The UMA Grant spec might be able to accommodate those semantics, but still with a lot of work.

Does it make sense to open up UMA to using token exchange? We mentioned this as a possibility explicitly, but also suggested constraints on changing UMA based on the experience of existing implementers and deployments.

Would they be interested in the wide-ecosystem use cases? There is a little bit of that in the distributed OAuth work, whose future is uncertain. OIDF might be taking that up. Dynamic client registration has some of that. The healthcare world is driving some of this conversation on the client side (looking at the "patient designee" language in some of the regs).

Standardizing elements of the software statement so that Bob's client can be onboarded under Bob's signature dynamically as required is something that would push things forward in a wide ecosystem. This doesn't inherently require DIDs or OIDC. It just requires standardizing the bold part.

Interop planning

AI: Eve: Gather enough implementers to discuss the "state of interop" and put together this session. Who will speak? What is the content?
Charter refresh

The current charter as of 27 Feb 2018 has us producing mostly business model outputs. We still are on the hook for some of those. With the contributions made, there are IETF-directed activities it behooves us to do. Maybe we shouldn’t edit and close a new 2019-era charter until we know the OAuth WG’s plans for certain. Work items for us could include:

- "Operational" interop work
- Business model work
  - Could include harmonizing with DID/VC group efforts – Adrian notes that he writes papers on business model topics in those venues
- Any profile/extension work of interest to a "horizontal" UMA2 community (until such time as UMA2 might possibly get opened up for serious revision in IETF – could take a long while)

Use cases of interest to potentially tackle, whether here or in IETF:

- RS-offline use case, a la the ACE C-to-RS flow
- Incorporating (profiling for?) PoP and other stronger tokens vs. just bearer
- Privacy-enhanced AS represented by a "wallet" (a la the Identos demo/preso)
- Are we ID-agnostic enough? Do we handle “ZKP identities” for Alice sufficiently well?
- Speaking of ZKP, does our claims collection model accommodate Alice specifying a policy saying “Bob has to be ‘over 18’” and enable ZKP for proof?

Meeting schedule

We are meeting Thu Apr 4 but not Thu Apr 11.

Attendees

As of 18 Oct 2018, quorum is 5 of 8. (Domenico, Peter, Sal, Andi, Maciej, Eve, Mike, Cigdem)

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

Non-voting participants:

- Thomas
- Adrian
- George
- Nancy
- Tim

Regrets:

- Lisa