UMA telecon 2019-09-05

UMA telecon 2019-09-05

Date and Time

- **Thursdays 6am 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 of UMA telecon 2019-08-08
- Status on UMA2 IETF I-Ds
- Contributing to XYZ use cases
- Nominations for chair and vice-chair
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

- Approve minutes of UMA telecon 2019-08-08

Deferred.

Status on UMA2 IETF I-Ds

Our I-Ds have expired. Even though we (meaning Eve) didn't minute it very thoroughly, we did conclude (didn't we?) that we wanted to go the independent /individual submission route. We would need to resubmit the drafts and change the tag to Informational. Then we'd have to get in touch with the (edited) Independent Submissions Editor and provide a list of relevant information.

There are two formatting issues created in making the I-Ds – these are totally I-D artifacts:

- The UMAGrant link in the references section of FedAuthz is broken.
- In the UMAGrant spec, the union/intersection set math symbols didn't come out right.

In addition, we may want to consider absorbing a couple of GitHub issues that would make this turn into an UMA 2.0.1 because of our semantic versioning commitment:

- 362 (IANA registration of "UMA" scheme)
    - #362 takes an email and some time for registration (assuming they accept it). Our argument for inventing the scheme was that a client playing in both UMA-grant and other-OAuth-grant ecosystems would need to get the "UMA" scheme signal in order to know how to respond, so it's needed for interoperability. We would like to **register the scheme**.
- 361 if it's a non-normative change to metadata)
    - #361 needs investigation on our part. Are we compatible with the constraints on the .well-known path? We say in UMAGrant Sec 2 that "The discovery document MUST be available at an endpoint formed by concatenating the string /.well-known/uma2-configuration to the issuer metadata value defined in [OAuthMeta]". So if the issuer has a path in it, our language might break. In principle, most people don't use paths unless they deploy a multi-tenant platform, and that's when they run into issues with our now-OBE language. Some options: 1) We could put in non-normative language that warns people that, say, they could run into problems with multi-tenant path use cases or something given that we're not pointing to the final metadata RFC and this could be changed in a future version. Or 2) We could just not do anything for now. The sentiment is to choose **option 2**: Don't do anything for now.
- 360 (typo)
    - #360 is easy to decide. **Fix the typo.**

An UMA 2.0.1 is still "UMA2". It's a patch release that fixes a couple of unimportant bugs. George and Thomas speak in favor. We had looked up whether Kantara has an errata process and it sort of may, but this should be better since most people, especially devs, have a strong expectation of what patch numbering means. We should publish any patch spec versions (on the KI site) in the same place as the original version, such that if you expected to get "UMA 2.0.0" but there is, say, an "UMA 2.0.2" available, you get that in the same location. An "UMA 2.1" would be in a different location because semantically that's significant.

Nancy notes that a use case where the AS is not the IdP is something she's running into now. Eve is finding that this is where deployments might typically choose interactive claims gathering, PCT usage, etc.

Contributing to XYZ use cases

Justin sent this compendium of use cases for XYZ to the OAuth list.

OAuth2 had baked into it the concept of "grants", and that meant a lot of things got squished into grants. Extensibility is in XYZ, but it comes in different ways. Might this mean there won't be an explosion of specs over time, the way OAuth2 was susceptible to? Weirdly, client IDs aren't there, error messages on the front channel... They're not there because you don't need them.

We should be sure to capture, not just use cases that OAuth is struggling with, and use cases that UMA solved because OAuth couldn't do them on its own, and use cases that UMA is struggling with, but also use cases that people have pressed OAuth and UMA into service for "just fine" as far as they are concerned but they're not at all sure how XYZ would solve.

George would like to be able to define and name an extension with a clear set of functionality.

UMA-related use cases Eve would like us to write up:

- Alice-to-Alice sharing (RO-to-self)
- Proactive Alice-to-org sharing (RO-to-client developer, so to speak)
- Bob is assured to a certain level that Alice is who she says she is (strong Alice-to-AS binding or "CIBA-like")
- Transactional and long-term management of sharing of preferences with service providers

She would be grateful for volunteers to help draft some of these for next week.

IETF 106 is in November in Singapore. Justin will be there in person. He's working on hopefully having them hold a BOF on XYZ there. Thomas advocates for a new WG.

Nominations for chair and vice-chair

Voting deferred. We do have a meeting next week.

Attendees

As of 16 Jul 2019, quorum is 5 of 9. (Domenico, Peter, Sal, Thomas, Andi, Maciej, Eve, Mike, Cigdem)

1. Domenico
2. Peter
3. Thomas
4. Maciej
5. Eve
6. Cigdem

Non-voting participants:

- Pete Palmer
- George
- Justin
- Nancy
- Lisa
- Vlad

Regrets:

- Mike
- Sal