UMA telecon 2018-09-13

UMA telecon 2018-09-13

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 of UMA telecon 2018-08-23
- Update on PIPC/captive insurance discussions and next steps over the next couple of months
- Updates on the UMA world and other relevant worlds (OAuth, OB...) – any appetite for extensions this year?
- Heads up – no meeting in two weeks, on Sep 27
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2018-08-23: Deferred.

General discussion

Tim is working with an EC-funded identity project and has become aware of a project in Azerbaijan related to digital identity, a bit similar to efforts in Estonia. Others on the call have not. Interesting.

Heads up – no meeting in two weeks, on Sep 27

The calendar invitation has been removed. Eve is traveling.

Updates on the UMA world and other relevant worlds (OAuth, OB...) – any appetite for extensions this year?

Bertrand Carlier's blog post is here. As previously discussed, his insight about the OAuth grant flows available within the UMA2 grant flow is a good one. And as Justin has observed, it would be valuable for OAuth to have a formal model for grant flows the way UMA and other specs do, with a permission ticket pattern and all. Mike asks: What's the action item? Is there something worth "factoring out" that could be absorbed by the wider community? Putting a pin in that question for a second...

When we first looked at the decoupled use cases and how CIBA and UMA might variously satisfy them, we observed that neither seemed truly complete and maybe piece-parts could be combined. Mike suggested "UMA-protecting" the /bc-authorize endpoint. The CIBA spec is now going through a modularization process, into a core and at least one profile. (Let's assume Alice is the RO and bank customer, and Bob is the RqP and agent.) There is a need for asynchronous approval by Alice. To what degree is Alice's identity/ her claims required to be proved (authenticated) to Bob and some service representing him (say, an IdP)? The decoupled use cases do expect this, and that's the premise behind using OIDC as the basis behind CIBA.

The core would have the notification modes. We understand that there will be three different notification modes: poll mode, ping mode (you get back a reference ID), and push mode (you get back a token directly). We understand that polling is considered most secure but insufficient for some use cases. Quoting here:

- **Poll Mode** - When configured in Poll mode, the Client will poll the token endpoint to get a response with the tokens.
- **Ping Mode** - When configured in Ping mode, the OP will send a request to a callback uri previously registered by the Client with the unique identifier returned from the Backchannel Authentication Endpoint. Upon receipt of the notification, the Client makes a request to the token endpoint to obtain the tokens.
- **Push Mode** - When configured in Push mode, the OP will send a request with the tokens to a callback uri previously registered by the Client.

Would we need to create an extension (beyond "poll mode", which we already have)?

Eve: Right now only Bob's client is inside the protocol's scope. The user agents that Alice uses to interact with the AS and the RS are "internal" and aren't part of the protocol. Mike: There are multiple APIs, so yes, it's a challenge that UMA is not entirely "reciprocal". The "manage (out of scope)" notation at the RS and "control (out of scope)" notation at the AS in the FedAuthz diagram are the oddities. Nancy: In her company's work (healthcare), they have noticed that Alice's and Bob's roles could be switched. Eve: If we have to expose proof of Alice's authentication to Bob's service, can we do it with some workaround by leveraging the fact that the PAT requires use of the AS's OAuth authorization endpoint and – ideally – production of an OIDC ID token as well? (We do advise in FedAuthz that if identity is needed in addition to access, a PAT should also use OIDC.) Mike: Really don't think that's necessary.

CIBA Core is expected to have a first Implementer's Draft by mid-October, so let's take a look then. Mike is strongly encouraged to play around with an UMA-decoupled swimlane soon, so we can get our heads around this more firmly.
We’re just a bit concerned that some big challenges of party-to-party delegation will be missed if an "authentication-only" approach is taken to the decoupled use cases. If we can do our analysis during the same period that the CIBA Core spec is being worked on and also reach out to key CIBA driving forces (Dave Tonge, Brian Campbell, Don T, Nat) with the ideas and results, maybe we can find a way to work together.

Eve: Work with Bjorn on reaching out to Dave, Brian, Don, Nat on CIBA and UMA.

**Interop activities**

Mike/Gluu has been making progress on interop with RedHat Keycloak.

**Update on PIPC/captive insurance discussions and next steps over the next couple of months**

Deferred until David can join us.

**Attendees**

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

1. Domenico
2. Eve
3. Mike
4. Cigdem

Non-voting participants:

- Scott
- Tim
- Bjorn
- Nancy

Regrets:

- Andi
- Maciej
- Sal