UMA telecon 2018-09-20

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, UMA telecon 2018-09-13
- Update on PIPC/captive insurance discussions and next steps over the next couple of months
- Update on interop testing activities
- Update on CIBA/UMA discussions
- Reminder: no meeting on Sep 27
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2018-08-23, UMA telecon 2018-09-13: APPROVED.

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

Eve and David will coordinate at CIW tomorrow on setting up the initial meeting with the insurance contact.

Update on interop testing activities

Keycloak deployed an instance for Gluu to test against. They didn't test claims gathering, but they tested everything else, and after some effort, they got things working. There were some issues around client registration, which is sort of out of UMA's scope. Gluu was using dynamic client registration. The Keycloak engineer is going to do a writeup. The RS/C interaction wasn't working at first.

Mike has also written to Prabath of WSO2 to suggest doing interop testing, and the latter indicated interest. WSO2 has apparently finished their UMA2 development. They're not supporting claims gathering either. Why might this be? Mike sees claims gathering as useful for collecting consent etc. Eve surmises that this is an outgrowth of the two distinct use cases hinted at by the "assertion flow" vs. "authorization code flow" design patterns hidden within the claims collection model expressed in the UMA grant (see Bertrand's post). Cigdem sees claims gathering as optional, and some vendors are just doing what's mandatory at first. Adrian notes that SSI is all about how you encode and present credentials. The VC (verifiable claims/credentials) group is doing this, and HIE of One implements this (Michael Chen confirmed to Eve that the implementation uses uPort at the claims gathering endpoint). HIE of One is also interested in interop testing, and suggests that doing this is important for adoption, e.g. with Medicare, so that it can certify client apps. Eve has begun talking to ForgeRockers about this as well.

Eve discussed the status of all this work with the Leadership Council yesterday, and pointed them to our old UMA1 interop testing wiki area (link goes to the results matrix; see the additional links near the top of the page). The matrix currently assumes that participants don't test "role against role" within their own solutions, but perhaps we should do that, since, e.g., an AS and an RS should indeed work as independent functions/roles.

Update on CIBA/UMA discussions

Mike and Eve had a discussion about extending the notification options for UMA through a simple extension spec. Mike's concern is that since CIBA at base has a foundation on federated identity/authentication, it may not be fully appropriate to solve the set of use cases. Bjorn notes that there was heavy discussion around the philosophical question of authorization and authorization(approval)-by-authentication. But there are multiple ways to do things. So it should be fine to try and solve the use cases in what we see as the most appropriate way. Eve's biggest question is around multi-party delegation of access.

Another extension Mike is keen to explore is scope expressions. The WG just requires some "language to look at" so we can consider the extension properly. Starting an extension doc in xml2rfc format could just copy one of our existing specs and gut whatever isn't needed. The XSLT stylesheet is in the util subdirectory.

Let's just call this "decoupled", not "CIBA/UMA". In our next meeting (Oct 4) we'll look at specific flows.

Adrian also speaks up for working on notification more, for his own purposes. Since in his use cases the RO controls the AS, it's necessary for the AS to act as the agent of the RO in the right fashions.
At: Adrian: Write some user stories to characterize the requirements for RO notifications.

Eve and her folks have been working on a way to send notifications to requesting parties that a resource has been shared with them, where possible. Perhaps this is something we can compare notes on eventually and capture as a best practice, or even standardize.

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:

• Bjorn
• Adrian
• Nancy

Regrets:

• Tim
• Sal
• Andi