UMA telecon 2018-05-31

UMA telecon 2018-05-31

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 2018-05-24
- Pass-downs from the LC
- Decoupled flow walkthrough
- Business model device/artifact mapping
- Enterprise use case collection
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

Approve minutes of UMA telecon 2018-05-24: APPROVED by unanimous consent.

Pass-downs from the LC

- ID Pro memberships available; let the staff know if you're interested
- North America member plenary idea: 3 hours or more on Fri Oct 26 after IIW 27 in SF; potential inter-WG efforts?

Early thoughts on the plenary: Mike can't make it.

Decoupled flow walkthrough

Client-initiated backchannel authentication (CIBA) was invented by the MODRNA group. Mike observes that the OAuth password credentials grant, currently being discussed again, is sort of similar. Usage of it is discouraged but it's often a pattern of last resort. Why is it there? To provide a less-completely-horrible way to do what people would do anyway. Really? Harrumph. The grant lets you throw out the password and just deal with the token. And it lets you standardize on OAuth vs. also doing real screen-scraping. The idea in CIBA is that Bob (a call center agent or similar) wants to send a notification to the AS to authenticate Alice out of band. The phishability of both is still a big security consideration.

In George's environment, the challenge is to complete the authentication loop without the call center worker party ("Bob") seeing the code or whatever. "Proof of presence" by the user seeking service ("Alice") is insufficient. A fake person pretending to be Alice shouldn't be able just to hit an Approve button.

Eve has done an analysis attempting to map UMA to the decoupled requirements. We could dictate that `request_submitted` be used (See Grant Sec 3.3.6) and that could trigger a notification flow that requires a specific kind of authentication. Could this be done as a profile? Talking about "sessions" is weird, especially because it may not be about a browser at all, but a mobile authenticator app. What if the Bob side wanted to collect a set of claims? Could the UMA infrastructure for claims collection be leveraged, only in the other direction (by some AS acting on behalf of the RqP)?

We're given to understand that polling is considered harmful by OB. CIBA has both polling and notification. Since UMA is so asynchronous in its outlook, would it want to make use a notification endpoint on the Bob side for the Alice side to use?

Do we think this approach is interesting to keep analyzing? There's interest among Mike, Bjorn, and Maciej so far. It seems to meet the "*potentially* fit for purpose" bar if we think about `request_submitted`.

Business model device/artifact mapping

Eve reviewed the current state.

Enterprise use case collection

Some thoughts variously from Mike and Eve:

UMA and XACML are not necessarily mutually exclusive. However, organizations are struggling to avoid vendor lock-in with XACML and some are looking for new ways to scale better; XACML has challenges with that while the OAuth architecture does better. It can be valuable to do analytics over a standard policy format. David B mentioned OpenPolicyAgent.org at EIC, which is a policy engine framework with a policy expression format. ANSI RBAC is a standard, whereas ABAC is not a standard. Justin says, "Yes, let's kill XACML." 🙂

Mike should be ready to demo the Gluu Gateway next week. Let's continue the enterprise discussion next time.

Attendees

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

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

Non-voting participants:

- Adrian
- George
- Mark
- Bjorn
- Nancy Lush - Lush Group - is on the HEART WG - welcome to the group!
- Justin

Regrets:

- Tim
- Andi