UMA telecon 2020-07-09

UMA telecon 2020-07-09

Date and Time

- **Primary-week Thursdays 6:30am PT**
  - Screenshare and dial-in: https://global.gotomeeting.com/join/485071053
  - United States: +1 (224) 501-3316, Access Code: 485-071-053
  - See UMA calendar for additional details: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Approve minutes of UMA telecon 2020-06-11, 2020-06-25, 2020-07-02
- New profiles
  - Resource definition profile
  - Wallet profile
- Chairing coverage for next week
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

- Approve minutes of UMA telecon 2020-06-11, 2020-06-25, 2020-07-02

MOTION: Andi moves: Approve minutes of UMA telecon 2020-06-11, 2020-06-25, 2020-07-02. APPROVED by acclamation.

New profiles

- Resource definition profile status
- Wallet profile

Continuing with the flows and diagrams in Alec's recent email and spec text in his other recent email and his user stories in his other recent email...

User stories:

"Decoupling the consent management UX from the authorization services" is the user story intending to support the wallet.

Adrian suggests not using RS, RO, etc. because they are jargon that the rest of the world won't understand. He prefers PDP, PEP, etc. because these have been formally defined in RFCs. What about PAP for consent management/wallet functions? In the past, we have discussed how the XACML-type senses of PDP and PEP don't correspond exactly to AS and RS in the UMA sense because they don't fit neatly into the P*P categories.

(It would be a good idea to number the user stories!)

In their current implementation, there is a kind of pass-through of signed policies of Alice's in the token, so that the RS can ensure that they are the RO's even if the AS can't see them. In VC-talk, the AS is passing through VCs without verifying them and the RS is the verifier. If what is conveyed to the RS is a true policy, e.g. "Bob can access this resource with these scopes", then this is a privacy violation because it can do traffic analysis of information about Bob over time.

We briefly discussed the clause in Sec 1.4 of UMA FedAuthz nicknamed the "Adrian clause": "However, the resource server MAY apply additional authorization controls beyond those imposed by the authorization server. For example, even if an RPT provides sufficient permissions for a particular case, the resource server can choose to bar access based on its own criteria."

Eve notes: There is a kind of ambiguity in the use of "RO" in the user stories in that it is (mostly?) about the use case of UMA-protected resources used for the purpose of satisfying the policy of some other RO. So the RO in this case is also someone else's RqP. This is akin to our original "UMA Trusted Claims" concept, illustrated here. Maybe RqP-as-RO? Also, watch out for the use of the word "consent".

Patrick asks: Are we talking about a self-minted access grant, or a self-minted claim? If I grant access to you with no constraints, should the answer ever be no, or could the AS ever say no?

The spec text includes a diagram with "delegation" in it, between RO and RqP. This extension is mostly RO-focused.

Michael asks: What's in your wallet? 🙂 Alec answers... It's a private-key management for Alice. It's credentials established by the AS to control an AS account, for PAT-type stuff. It's also an independent place where she can maintain a parallel record of the policy she's written. The functions are: Putting resources under management; write policy over those resources; and (?). In a way, a wallet is pretty much like an AS, but just closer to Alice. This is akin to the cascading AS concept. It can be a client type, or it can be an "cloud AS" with all the AS capabilities: a service endpoint that is always on.

Nancy notes: It's an important time for healthcare. Please get engaged. She'll send info to the list.

Eve and Maciej can't make next week's call. Alec is kindly willing to run it.

Chairing coverage for next week

tbs

Attendees

As of July 8, 2020, quorum is 6 of 10. (Michael, Domenico, Peter, Sal, Gaurav, Thomas, Andi, Maciej, Eve, Mike)

1. Michael Amanfi (product architect of EmpowerID – workflow engine development)
2. Domenico
3. Sal
4. Andi
5. Maciej
6. Eve
7. Mike

Non-voting participants:

- Alec
- Adrian
- Patrick Parker (CEO of EmpowerID – works a lot on product design – big on authz! – his Identiverse talk is coming next Thursday)
- Colin
- Nancy