UMA telecon 2020-10-15

UMA telecon 2020-10-15

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 2020-10-08
- Policy Manager draft - review text
  - Ideally put comments in GitHub ahead of time
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

- Approve minutes of UMA telecon 2020-10-08

MOTION: Thomas moves to approve minutes of UMA telecon 2020-10-08: APPROVED.

Vice-chair role

Time to fill this role once again. Eve nominates Alec (and he accepts).

MOTION: Thomas moves and Andi seconds and Michael thirds!: Install Alec as vice-chair for a term of one year. APPROVED by acclamation. Yay!

Policy Manager draft - review text

- Ideally put comments in GitHub ahead of time

Domenico has provided a UX sample of a "personal data wallet". Check out the new section on our User Experience page.

The discussion of last week was: How to fill in the required_claims in the posted policy? Required claims already have a way to be put into JSON in UMA Grant. Only email (in last week's discussion) would come under that definition. Was RAR discussed last week? No, but other options were: JWT or OAuth (could be RAR now). There's SCIM (lots of kinds of claims), RAR, specific claims as in OIDC, VCs... George suggests focusing on the structure and critical aspects vs. the claims themselves. UMA even goes "meta" from claim structure by having "claim tokens" and formats for them since there are already so many. Should we lock down some likely formats? This is akin to a relying party saying "I need a particular kind of claim".

We had discussed in the past a "hashed claims discovery" mechanism that might, in a secure fashion, allow the AS to specify specific claim values it needs through need_info (issue #254). If security concerns override, then the user could always be asked to interact with the AS.

Do we need some better language around all the different "ecosystem topologies", or "deployment patterns"? For example, whether clients are third-party wrt the AS/RS is a "normal OAuth" choice (though many OAuth deployment have first-party clients). Whether RS's are third-party wrt the AS is an UMA-specific "wide ecosystem" choice. There are also choices around "where to put the IdP". Now with the current extension work, "policy manager colocated with AS" means "just UMA" (silently, though the spec doesn't strictly require that), while "policy manager colocated with RS" starts to require more interoperability and thus suggests the need for the extension work. Sal suggests "flat, hierarchical, decentralized". This starts to intersect (hah) with the Venn that Eve, Alec, and Adrian were working on over the last few weeks that tries to describe client trust relationships.

Especially for public clients (e.g. mobile apps), we need to worry about client trust. That's not an UMA-specific problem, but we need to (continue to) be aware of it. Is there a way we could build in a DPOP mechanism in UMA? DPOP didn't exist at the time we published UMA Grant, so we only pointed to what was available at the time. UMA is deployed on other technology and context and it's important to be aware of and strengthen it.

Eve is trying to distinguish "scope" from "purpose". The former has to do with the action the RS has to allow/deny when it gets the token. The latter has to do with what the RqP can do subsequently with the access it eventually got (e.g. use the data for marketing purposes). (See our very old "simple access authorization claims" work for a way to embed this in required claims!)

The required-claims piece seems different from the other pieces in that required claim values need to be drawn from the RqP, while the others need to be drawn from the RO, in order to build a complete policy. Does policy need to be standardized for interoperability, or can it be handled like UMA Grant handles claim tokens and formats now? We think the latter. Alec will put in strawman solutions for both required claims (in claim token/format fashion) and policy overall (in similar fashion) for us to consider.

Sal notes that ISO 29184 provides some nice controls around notice (for things like purpose). There is a draft ISO 25760 around consent receipts.

Attendees

As of October 7, 2020, quorum is 6 of 10. (Michael, Domenico, Mike, Peter, Sal, Gaurav, Thomas, Andi, Maciej, Eve)

1. Michael
2. Domenico
3. Sal
4. Thomas
5. Andi
6. Eve

Non-voting participants:

1. Alec
2. Scott
3. George
4. Anik
5. Kate