UMA telecon 2020-10-08

UMA telecon 2020-10-08

Date and Time

- **Alternate-week Thursdays 10am 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 2020-10-01
- Policy Manager draft - review text
  - Ideally put comments in GitHub ahead of time
- AOB

Minutes

Roll call

Quorum was not reached.

Approve minutes

- Approve minutes of UMA telecon 2020-10-01

Deferred.

Policy Manager draft - review text

- Ideally put comments in GitHub ahead of time

How can policy/required claims language be conveyed from PM to AS? Couple options

- leave it unspecified in this draft
  - pro: open for extension. It's complicated, define instead a minimum conformance profile
  - con: requires implementation profile. Can't be tested for interop except in context of a profile
- follow oidc claims language
- rely on xacml

Policy can also extend beyond which claim are required from the rqp. Could also define terms for how that access 'work', ie if it should only be valid for n minutes. required_claims doesn't cover this concept

What is the minimum conformance profile?

We can namespace profiles for interoperability. Ie an xacml profile that defines what goes into the required_claims field. The profile would need to present in the AS metadata, and likely have an IANA registration for well known ones. This approach is a good balance between testable interop while leaving room for extension/innovation. There would be well defined profiles for policy (xacml, some kinds of VC, "oidc"-like claims/jwts), but it's still open for custom profiles/implementation

There was previous discussion around xml/xacml that was rejected by the group. The policy language needs to be understood by both the AS and Policy Manager, such that the PM can present UX to the RO. Peter notes xacml recently had a JSON profile defined.

Should we 'try it out' and define at least one of these profile, ie to prove the concept. What minimal profile would cover 80% of cases.

AI: Alec can try to put together a JWT/OIDC like policy profile

What "things" should be present in policy? Should the draft have discussion of leave completely open?

There was the idea there are 3 elements to policy: purpose, who can access (rqp claim), what can they access (resource_type/PI category). This intersects with the Personal Data User/consent receipt specification. This response of creating policy could include a receipt_uri, or the entire receipt contents

required_claims

- email: bob@email.com
- purpose: Read would this be defined values or open of RO definition? (accepting purpose/terms would required interactive claims gathering? Probably not, since required claims can be returned through needs_info)

The required_claims json object could also inherit/build on the one defined in UMA Grant Section 3.3.6 . This helps to further reduce the 'new concepts' in this draft, both resources and policy json definitions build on existing UMA json document types

SPDL Language Brief Introduction is another options for a policy language profile. It could cover more than RqP claims, and allows RO to define expiration of the access...

One question in the draft around including the RO subject, for example for a resource that doesn't identifier the RO, how does the RS get this identity/ro context? This is related to the resource definitions draft and AS-first flows.

Can the RO put information into the policy that is sent to the RS? For example if the RO isn't obvious from the resource uri, could the AS give the RS this subject/specificity. One challenge implementing UMA is that with AS/RS coordination, every resource at the RS may need to be registered. In some ways the entire rs db is represented at the AS in some way. For example, does an RS have to register a resource for each user account (ie for a userinfo or Patient resource). Or even with a non-identifiable URI, register a resource for each user PAT

Attendees

As of September 3, 2020 (pre-meeting), quorum is 5 of 9. (Michael, Domenico, Peter, Sal, Gaurav, Thomas, Andi, Maciej, Eve)

1. Dominico
2. Micheal
3. Peter

Non-voting participants:

1. Alec
2. Anik

Regrets

1. Eve
2. Thomas