UMA telecon 2021-09-16

UMA telecon 2021-09-16

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 2021-09-09
- Correlated Authorization
- OAuth vs UMA content
- AOB

Minutes

Roll call

Quorum was NOT reached.

Approve minutes

- Approve minutes of UMA telecon 2021-09-09

Deferred

Correlated Authorization

https://github.com/uma-email/poc

Today in UMA can push the token, addition is binding the ticket to the pushed token

There's nothing bad about this claim token profile, not sure what the specific use-case or outcome it tries to create

What is the motivation for needing the correlation? Is there a specific outcome the correlation creates over 'ticket challenge-less' claims pushing?

- not allowing RpQ token reuse. Is this beneficial? is it tied to the first use of that token and require re-issuance if the AS needs_info
- non-interactive RqP id assertion

OAuth vs UMA content

Since this a common information request, could we create some good standard content/position?

EIC Points:

OAuth

- Tokens issued to a Resource Owner at a Client
- Communication between Resource Server and Authorization Server is out of scope
  - this necessarily 'narrows' the ecosystem, since the RS and AS need to agree ahead of time on authorization details
  - usually RS/AS are in the same domain (eg TLD) **Is this something that OAuth *says* or is it what people naturally implement?**

There are OAuth extensions that drive to UMA-like outcomes, such as Token Exchange which allows a Client to get a token representing another party. Or GNAP which takes a bunch of UMA + OAuth features and derives a new authorization protocol.

Typically considered as 1 RS and 1 AS, with many RPs/clients

UMA

- Tokens issued to a Requesting Party at a Client

- Defines API between RS and AS for: resource registration, permission ticket creation and introspection
- There can be "many of everything" not just Clients this is a "hard" concept for people to grasp at times

People ofter struggle with the 'nicknamed tokens', understanding they are access token which specific scopes/purposes. PCT has often been a hard one to understand, not widely implemented today because of this?

UMA Outcomes:

- RO to RqP delegation,
- decouple consent(policy settings, consent as pre-condition for any tokens/grants) from transaction(token issuance), can happen ahead of time or just in time
- AS Discovery and RO selected AS,
- Request and grant for specific fine-grained resources, doesn't look at an entire RS as the resource but allows arbitrarily small resource registration

UMA is very flexible and comprehensive, which creates it's own set of interoperability challenges. Requires interop/ecosystem profiles which immediately undercut the UMA goal of wide-ecosystem.

- Even client registration at the AS is challenging. UMA implies that it's dynamic since 'any client can be used', however this isn't in wide practice today (most clients today are pre-registered)
- culmination of different barriers (technical, common practice, understanding) that make UMA difficult to use in practice

Trust Registry helps with decentralization and creating a more informed AS. More granularity around the purpose, state for authorization and checking for changes (new role for PCT?) Captures, AS endpoint, purpose, scope of permissions. There will be many of them, ideally not too many for each RS. How do they interact? Regional/local collaboration, and then combining regional networks with congruent code of practices to create a wider ecosystem.

Topic for future weeks: outcome of user stories discussion, PDP architecture includes the concept, TOIP/SSI are starting to define this ecosystem function

Topic for future weeks: ANCR records update, Privacy as Expected.

AOB

https://www.ontario.ca/page/consultation-policy-framework-ontarios-digital-identity-program Feel free to submit comments to Ontario about the DI strategy

Alec will be away next week

Attendees

As of October 26, 2020, quorum is 5 of 9. (Michael, Domenico, Peter, Sal, Thomas, Andi, Alec, Eve, Steve)

Voting:

1. Alec
2. Sal

Non-voting participants:

1. Zhen
2. Ian

Regrets:

1. Eve