UMA telecon 2020-11-05

UMA telecon 2020-11-05

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 2020-10-15, 2020-10-22, 2020-10-29
- Policy Manager draft text
- IIW recap
- AOB

Minutes

Roll call

Quorum was not reached.

Approve minutes

- Approve minutes of UMA telecon 2020-10-15, 2020-10-22

Deferred.

Policy Manager Draft

Continuing the discussion from last week left at the hypothesis: there will be many groups of trusting RS/AS/C that serve some known user population (RO /RQP) over some set of resource/API types. Users would be identified either by an AS or RS

The goal of these extensions is to provide Alice a single place to many resources and policy across certifying domains.

As a RS, I need to expose available resource to Alice, in order for her to choose how to put those resources under protection

As a AS, I need to expose the policy conditions I can enforce, in order for Alice to select how her resources will be protected

We've identified 3 'degrees of freedom' to the size of an ecosystem

1. Data Model/API interoperability. How the client understands the response from the RS
2. Authz Protocol interoperability. How is authorization acquired by the client and conveyed to to the RS
3. Trust Model. Why does anyone trust anyone

.. Identity/Authn? IMO this is a specific use of 1-3
ssi note: how does this align with the TOIP stack?

1. Data Model/API interoperability "resource definitions + RS-first"

This can be further split into
1. client downloads a file
2. client interprets a Content-Type (eg an jpeg)
3. client understands some API semantics (custom vs standard)(path can uniquely identify resource/ro?)

2. Protocol interoperability
This is main focus of UMA?

1. OAuth
2. OIDC
3. UMA
4. GNAP/SSI (in dev)

3. Trust Model "directory/trust list/CA"

https://kantarainitiative.org/confluence/display/uma/UMA+Trust+Model+User+guide existing UMA work that needs to be incorporated

* not part of specification, creates requirements around what to specify? *

Often this also defines parts parts 1 and 2. Is this was creates the 'size' of the ecosystem?

Often the trust model is organization-centric? ie the org is setting rules that benefit/protect itself. <- this statement is pretty subjective?

- Google/FB static client registration (Gov.UK? BC Services Card?)
- FAPI, software statement from 3rd party
- UDAP, x509 certification from 3rd party
- Federated/brokered, yes.com, securekey verified.me, signin.org
- Sovin network
- Open/Dynamic registration, maybe facilitated by the user

Can a user-directed ecosystem only exist where the rules are set by organizations? Michael believes this is consistent with UMA and Alec thinks it is for SSI also. SSI has an additional benefit that the verifier/requesting party can live completely outside the 'trust model'
User-directed implies that the user can establish their own trust model, and that organizational actors will accept this user direction. This breaks down when ecosystem needs to be regulated.

Identity/standards groups focus on identity/authentication/authorization but not 'what a resource is'. UMA get's closer since the RS<>AS need some way to "talk about" the resources/scope. However this is still organization centric, since each RS defines the resources it holds (resource.type is optional)

Thomas asks if we can distinguish the provenance of a claim from the trusted third party? Yes, this is what FAPI does, there are many OIDC providers who can provide claims, and one or more TTP who attests to that issuers capability. The user still operates within a TTP defined boundary

Can the AS provide this resource type directory?

One option would be for the AS to have an open resource api (not related to a specific RS). A client could use an 'open' permission api to request a ticket over those 'general' resource. This is very similar to RAR/PAR

Alec believes this supports the hypothesis that there will be many independent AS/RS/C spaces that a single RO would have to operate between (eg health apis vs financial apis). Possible that aspect 1 (API/Data model interop) is a better starting point for the extension work, although the policy manager /resource manager have longer term alignment with an ssi view of user-directed access

Attendees

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

1. Michael
2. Dominico
3. Alec
4. Thomas

Non-voting participants:

1. Kate
2. Bjorn

Regrets:

1. Sal
2. Eve
3. Andi