UMA telecon 2021-06-24

UMA telecon 2021-06-24

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 2021-06-10, UMA telecon 2021-06-17
- Relationship Manager - user stories
- UMA Interop Testing
- AOB

Minutes

Roll call

Quorum was NOT reached.

Approve minutes

- Approve minutes of UMA telecon 2021-06-10, UMA telecon 2021-06-17

Deferred

Relationship Manager - user stories

From: https://kantarainitiative.org/confluence/display/uma/UMA+telecon+2020-11-19

As RqP Bob, I want to be able to request access to a set of Alice's resources directly from Alice's AS without knowledge of their location, because I don't have to bother getting or caring about all the locations from Alice first.

- this one was more related to resource definitions - not resource manager
- Alice can give discovery handle (uri to resource), or since Alice's stuff may be in many places, Bob can discover all of the location's by Alice only sharing the AS (as the discover function)
- SAML 1.0 only have IDP initiated SSO, then expanded to other use-cases eg SP initiated SSO. UMA so far has deferred discovery, however this brings it back into the scope
- it's not hard to be told which RS, eg registered the resource_location with the resource
  - there are potential security/privacy concerns with this approach
- Is the client request bounded to a specific RO from the offset.
  - Client says to AS, "im looking for these types of resources (types/definitions/indicators) with these scopes" ie by using a UMA Fedz Permission endpoint exposed to the Client
  - AS returns a UMA ticket and can continue through UMA grant (pushed/interactive claims)
  - What granularity is the Client/RqP making this initial request for resources? Over resource descriptions: resource type + scopes
- **There are major implications for the token response to the Client: token_type, multiple access tokens, including the resource_location + type**
  - Previously only one Resource Server is ever granted (maybe over many specific resources), however this requires only 1 token
  - want to maintain the resource server constrained access tokens
  - another option is we token response in maintained, and the client makes multiple token requests (eg with the PCT) and the specific resource type/indicator
    - PCT fits within current UMA model since the PCT allows the client to get new access tokens for other RSs without having to go through claims gathering again
- This may also enable the RS to register as a resource type provider, is there a way that no specific resources need to be registered at the AS, and that Alice's "ID" is what's conveys back to the RS
  - fits when paths/uris at the RS are not specific (eg /me/profile vs /alice/profile)
  - gets back into the relationship manager profile, where Alice pushes RS known sub to the AS which can be returned to the RS through introspection (or the RPT)

```
{
   "access_token":"sbjsbhs(/SSJHBSUSSJHVhjsgvhsgvshgsv",
   "token_type":"Bearer",
        "resource_type" : "http://resourcetyperegistry.com/a/resource/type" <- this is the contract with the
client over what the response from the RS will be
        "resource_location" : "http://thisspecificrs.com/path/to/resource"
}

// this is a non-conforming to oauth2 as the access_token isn't a string
{
   "access_tokens":[
               {bearer access token with resource location}
]
   "token_type":"Multi"
}
```

As client C used by RqP Bob, want to be able to request access to a set of Alice's resources directly from Alice's AS on Bob's behalf without knowledge of their location, because I(client) don't have to retrieve the locations first.

- the client doesn't have to collect a resource location from Bob before starting the flow, can have a direct relationship with the AS

—
From: https://groups.google.com/g/kantara-initiative-uma-wg/c/f0g98sr22Rw/m/M5jK9z1nAgAJ

As a RO, I want to manage my resources independently of each individual RS (UMA core prop)

- Alice has resources at many resource servers
- In an ideal UMA world, Alice is able to choose her authorization server, and all clients are able to dynamically interact with it. Another case is that the Authorization Server is run for Alice and registers a specific set of clients. Therefore, Alice/Bob may need to interact with multiple authorization servers in order to use the clients they want to.
- could we look at the business persons vs user personas
    - eg the RS operators doesn't trust certain
    - in the bowtie, the RS has 'no-trust' with the client, however this means it needs trust in some TTP
        - this is still an excellent goal, however it requires the RS to have direct vetting/relationships with all clients. The RS may have accumulated the resources during some other business purpose and never intended to become an Authorization Server also.
    - As the custodian, the RS has the most liability in disclosing the resource

As an AS(RS) operator, I need statically registered clients (clients + RSs), in order to meet my federation assurance requirements

As an RS operator, I don't want to trust any RO chosen AS, because I need strong federation assurance (I can't trust a individual person)

As an RS operator, I want to register resources with specific trusted AS, in order to meet my federation assurance

As an RS operator, I want to delegate RP registration and authorization, as I never intended to take on this responsibility/cost

federation issuance is short-hand for trust framework, legal/regulatory/compliance requirements (I can't trust anyone)

These necessarily narrow the ecosystem, UMA+these drafts aim to widens the ecosystem again and remove the need to 1-1 agreements between all parties.

- AS holds the agreements with the Client and RS, no Client<>RS agreements is required ('no-trust')
- Where does the RO fit into this agreement system? We want to allow the RO to experience agency as they participate in this ecosystem
- Can we describe the resulting trust model in GDPR terms.
    - How does this fit the ANCR receipt, consent token/grant type seems forced?
    - Is a consent receipt from the client a required claims for presentation?
    - The client is the one that Alice's information is disclosed to, seems like it(the client) needs to be the one providing Alice a receipt of this (with the contact information etc)

Alec will attempt to organize these use cases into a document for solicitation. We need to get less technical and more business/legal feedback on these goals

As an AS, I want to decouple the consent management UX from the authorization services,

- less required, but motivates the relationship manager client

As a RO, I need a personally controlled user-agent (UMA Wallet) to manage my key material, in order to maintain personal-agency in ecosystems

As a RO, I want to authorize a "UMA Wallet" to manage RS resources, so that I have a single view into my available RS's and Resources

As a RS, I need Alice to authenticate in order to determine which resources she can manage, in order to ensure appropriate management access

As a RS, I need Alice to establish credentials (pub key), so that I can trust externally asserted policy was issued with Alice

AS a RS, I need to trust delegations signed by Alice's key, so that Alice can allow Bob (other keys...) or <<claims gathering condition>> to access her resources

As a RS, I may delegate resource management user experience, so that I can focus of my core service to the RO

As an RS, I need to know which AS(s) Alice wants to use, in order to delegate access control (uma core)

As an AS, I want to delegate RqP identification to a UMA Wallet, so that
- a RqP can choose their private key and consent management provider
- I can avoid directly holding or seeing a users personal details

New term "**BOLTS**"

- Business
- operational
- legal
- technical
- social

UMA Interop Testing

AOB

Attendees

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

Voting:

1. Eve
2. Steve
3. Alec

Non-voting participants:

1. Nancy
2. Tim

Regrets:

1. Domenico