# UMA telecon 2021-08-05

## UMA telecon 2021-08-05

### 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, UMA telecon 2021-06-24, UMA telecon 2021-07-01, UMA telecon 2021-07-08, UMA telecon 2021-07-15, UMA telecon 2021-07-22, UMA telecon 2021-07-29
- Relationship Manager - user stories
- AOB

### Minutes

#### Roll call

Quorum was NOT reached.

#### Approve minutes

- Approve minutes of UMA telecon 2021-06-10, UMA telecon 2021-06-17, UMA telecon 2021-06-24, UMA telecon 2021-07-01, UMA telecon 2021-07-08, UMA telecon 2021-07-15, UMA telecon 2021-07-22, UMA telecon 2021-07-29

Deferred

#### UMA in Wikipedia

https://fr.wikipedia.org/wiki/User-Managed_Access

https://en.wikipedia.org/wiki/User-Managed_Access

Anyone familiar to wikipedia to update content?

Can/should the group review and create some more accurate content?

- Alec to create a google doc with the current content for the group to iterate on

#### Relationship Manager - user stories

2. As Alice, I want a way to grant Bob access to my resources without knowing the URLs, in order to a) not deal with URLs b) share more complex resources (ex not a PDF, a health record)

The RS registers a name and description at the AS, which is how Alice can differentiate resources

In the FR impl, the RS after registering a resource, saves the resource id (and other metadata), and *then* generates the URL. The URL is created after registration, which is what Alice is meant to share with Bob. There was also resource discovery at the RS, that would allow the RqP to query based on specific other claims, this feature is turned on by the RO for each resource. Part of the random URL strategy was to improve the privacy of including information in the URL, instead of sharing rs.com/georges_photos you can share rs.com/<uuid> without leaking information.

The URI registration would allow RqP discovery of resources across RSs. If we consider discovery as a layer ontop on UMA, we can separate the mappings from the authorization path. The URL can change over time, the RS can update the URL separate from any discovery needs.

The RS can also define the hierarchy of policy and groups many resources in a single resource registration, ie taking 1000 or URLs and putting registering a single resource.

When does an AS become as RS to expose a list of protected/available resources? Doesn't necessarily need to be the AS, or can be a separate url discovery service. Registration can be 1-n, not 1-1 eg many resources in one registration. If there are public/private photos, then a request for a public photo can include all public photo resource id, a request for a private resource includes only the single resource id. The registered resources could be 'public photos' and 'private photos'.

What is the UX of Alice managing her resources and policy? What is the UX of Bob being granted access to resources? Where does sharing occur, from the RS or AS?

The idea of a privacy wallet, people keep a record of their identity relationships themselves. That ANCR record defines the PII controller and contact info. Creates a privacy rights access point, in addition to the policy. People can broadcast their services for discovery. This is done so that on each new session the user can compare the privacy statement against the previously agreed to one.

How does Bob reach out to Alice's resources in order to determine where to go? Alice sends a receipt with her policy to Bob, including a URI to the calendar (or to her Privacy Wallet?). If the URI is to his calendar, then Bob can start an UMA flow. Bob would end up with receipts for Alice's AS and her calendar service

Privacy aspects are internal to the AS today in UMA, or are implementation specific. Alice shares a purpose, which must be mapped to authorization for Bob. UMA isn't prescriptive about scopes, there can be a scope such as 'do_not_share' that tell Bob's client to not retransmit to 3rd parties. However these scopes are legal by nature and not technically enforced. The RqP/Client can need to push claims declaring their agreements (eg a receipt) that include the PII controller who is taking custodianship of the information granted to Bob.

Just as discovery is capability on top on UMA, the privacy framework can be a profile on top of UMA. It provides implementation specifics where end-user legal privacy controls are required. Could this use UMA resource scopes sufficiently cover this? Or the claims pushing of a new claim_type eg a ANCR receipt/rights claim?

https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html#rfc.section.3.3.1

1. As Bob(RqP), I want to be able to discover resources available/shared with me, in order to not need URLs sent by Alice
2. As a Client, I want to be able to declare types I understand, in order to successfully use complex APIs
3. As an RS, I want to defer permission ticket creation, in order to a) not have to understand the Client b) not make authZ decisions (tell me don’t make me think)
4. As an ASO, I want to pre-register Clients, in order to assess their appropriateness, capability and complete non-technical activities
5. As a Client, I want to pre-register with ASs, in order to a) test my UX and technical integrations b) declare my capabilities

**AOB**

## Attendees

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

Voting:

1. Domenico
2. Alec

Non-voting participants:

1. George
2. Ian
3. Scott

Regrets:

1. Steve