

UMA telecon 2021-03-18

UMA telecon 2021-03-18

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 2021-02-04](#), [UMA telecon 2021-02-11](#), [UMA telecon 2021-02-18](#), [UMA telecon 2021-02-25](#), [UMA telecon 2021-03-04](#), [UMA telecon 2021-03-11](#)
- ONC Annual Meeting, Virtual Booth Update
- Profiles Discussion, relationship manager draft
- Pensions Dashboard, any updates
- AOB

Minutes

Roll call

Quorum was reached.

Approve minutes

- Approve minutes of [UMA telecon 2021-02-04](#), [UMA telecon 2021-02-11](#), [UMA telecon 2021-02-18](#), [UMA telecon 2021-02-25](#), [UMA telecon 2021-03-04](#), [UMA telecon 2021-03-11](#)

Eve Moves to approve, Andi seconds. Motion Passes!

ONC Annual Meeting, UMA Content For a Virtual Booth

<https://www.healthit.gov/news/events/2021-onc-annual-meeting> March 29-30

Deadline for content submitted is Mar 24

Pensions Dashboard, any updates

Have an agreed path and licenses

Profiles Discussion, relationship manager draft

UMA Resource Server Management

This document extends [UMA Fedz] in order to specify the interface provided by the RS to the RO for resource management. This is achieved by introducing a Resource Management API which is used by a Resource Manager Client to view available resources and direct the AS to use for protection.

** This API could also allows the RO to

- view access history
- set direct policy (ie Adrian clause)
- establish credentials required in AS, (smarthealth.card)

Reqs:

- The RO must authenticate to the RS, in order to authorize access to this API
 - (this capability of the RS is implied by UMA)
- The RO can see a list of resources available at this RS (either protected or not)

- The RO can modify the protection of resources (ie which AS to protect)
- The RO can see AS's available for protection
 - can the RO direct the RS to get a PAT from a new AS? This is tricky depending on how PAT's are issued (ie may require end-user redirection)

Names:

- resource management
- resource declaration
- available resources
- resource access management (RAM)

This document introduces the following new concepts:

- Resource Management API The API presented by the RS to the Resource Manager. This API is OAuth protected
- Resource Management Token (what scope should this Access Token capture?) "uma_management"

1.3 HTTP Usage, API Security, and Identity Context

- add link between RM API and RM Token

The `Resource Management API` allows the Resource Owner to:

- View the available resources hosted at this RS, and their current protection
- View the UMA Authorization Servers available to be used to protect
- Manage the UMA protection of available resources

Starting Conditions:

- The RS hosts resources for the RO
- The RS supports resource protection from an UMA AS
- The RS has a UMA PAT at one or more UMA ASs (try to bring this into the profile, not as a starting condition)

Step 0

The Resource Manager obtains an OAuth Access Token valid for use at the Resource API. The Access Token must allow the RS to determine the RO's resources.

- is there a purpose for NOT the RO to use this interface? Is this 'delegation' too early in

Step 1 (Get Info)

The RM obtains a list of UMA AS's available for resource protection, and a list of available resources

Step 2 (Update Protection)

The RM directs the RS to modify the resource protection either

- putting an unprotected resource under protection at a specific AS, possibly only registering specific scopes
- removing the protection of a resource at an AS. The RS will no longer honor RPTs for this resource from that AS
- modify the protection of a resource, such as to add or remove scopes

Available Resources Endpoint

The API available at the available resources endpoint enables the resource manager to have knowledge of the resources hosted by the resource server for the resource owner.

```
....
[
{
  "_rs_id" "ABC",

  "resource_scopes":[
    "view",
    "http://photoz.example.com/dev/scopes/print"
  ],
  "description":"Collection of digital photographs",
  "icon_uri":"http://www.example.com/icons/flower.png",
  "name":"Photo Album",
  "type":"http://www.example.com/rsrscs/photoalbum",
},
]
....
```

Protected Resources

```
....
[
{
  "_rs_id" "ABC",
  "authorization_sever_resource_id" : "_as_id"
  "authorization_server" : "as_identiflier",
  "registered_scopes" : [ "view" ]
},
{
  "_rs_id" "ABC",
  "authorization_sever_resource_id" : "_as_id_2"
  "authorization_server" : "as_identiflier_2",
  "registered_scopes" : [ "view", "http://photoz.example.com/dev/scopes/print" ]
}
]
....
```

/authorization-servers/:id/resources

```
....
[
{
  "_rs_id" "ABC",
  "authorization_sever_resource_id" : "_as_id"
  "registered_scopes" : [ "view" ]
},
{
  "_rs_id" "ABC",
  "authorization_sever_resource_id" : "_as_id_2"
  "registered_scopes" : [ "view", "http://photoz.example.com/dev/scopes/print" ]
}
]
....
```

In dashboard world, rs_id = PeI (pension identifier)

- to confirm, is the PeI the same as the as_id? ie is it created by the RS or the AS

single person, single resource, single rs: can have multiple resource registration, eg with different scopes

Resource = Patient

Registered Resource 1: Just the Patient Object
Registered Resource 2: The Patient + Sub Objects

Available Resource Description

A registered resource is a JSON document that extends the resource description from [UMA Fedz 3.1 Resource Description](1) with the following parameters:

authorization_server OPTIONAL A string identifying the authorization server that protects this resource
** could also be the AS policy uri from resource registration?

(1 <https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-federated-authz-2.0.html#resource-set-desc>)

List Available Resource Descriptions

Update Available Resources Description

Authorization Server Endpoint

The API available at the authorization server endpoint enables the resource manager to view and manage the authorization servers available for resource protection. The resource owner may allow resource protection only through the set of available authorization servers.

note: a challenge here is that it's quite difficult for this interface to create a relationship between an AS/RS because how the PAT is issued (ie could be interactive)

Currently this is a 'dynamic' API since it conveys information to Alice about whether a specific AS is available for use in other protection APIs (ie is there an active/historical PAT for this AS). If this is static, Alice won't know if she can use that AS for protection

The list of AS's may also be specific to the RO. Bob may have registered AS1, while Alice uses AS2

Authorization Server Description

List Authorization Server Description

...

```
[
{
as_url: "http://authserver_id.ca"
has_as_pat: true
},
{
as_url: "http://authserver_id2.com"
has_as_pat: false
}
]
```

...

Attendees

As of October 26, 2020, [quorum](#) is 5 of 8. (Michael, Domenico, Peter, Sal, Thomas, Andi, Alec, Eve)

Voting:

1. Andi
2. Alec
3. Domenico
4. Eve
5. Thomas
6. Sal

Non-voting participants:

1. Nancy
2. Colin
3. Ian
4. Ken
5. Tim

Regrets: