UMA telecon 2021-03-25

UMA telecon 2021-03-25

Date and Time

- **Primary-week Thursdays 10:00am 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 2021-03-18
- ONC Annual Meeting, Virtual Booth Update
- Authorization Code Grant
- Pensions Dashboard, any updates
- AOB

Minutes

Roll call

Quorum was NOT reached.

Approve minutes

- Approve minutes of UMA telecon 2021-03-18

Deferred

Pensions Dashboard

All sorted, waiting for final review & confirmation of final licenses

ONC Annual Meeting, Virtual Booth

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

Authorization Code Grant

https://groups.google.com/g/kantara-initiative-uma-wg/c/OHYcZe8l8Vs

Initial Thoughts/questions:

- Seems strange to get emailed a callback url, would the RqP have to open that link in the same browser?
- Mixing the purpose of UMA with authentication?
- Where is the response to request 2? that's a 302 to the AS
- Seems to have some relationship with the OAuth device code flow to perform some out-of-band authorization of a user-agent? Similar to the CIBA discussion, more in scope as CIBA was RO authn, while this is RqP authN
- Does the link need to be RqP specific? No because the token request includes bob's email as a pushed claim

Assume these pre-reqs:

- Alice has shared a link with Bob
- Alice has setup her AS to anyone who can demonstrate control of bob@email.com

Nice feature:

- The AS can authenticate the email without a direct integration to that email provider as an issuer(IDP or for claims pushing)

Suggested Changes:

- RqPClient does RPT less request to RS to get the ticket
- Line 2 is a uma token request with a 'request_submitted' response
- 3, 4, 5 should be 'out of scope'
- 6 is a uma token request that 'work', returns a token

Profiles Discussion, relationship manager draft

???: Can one resource be protected by two Authorization Servers?
???: Can one resource be registered multiple times as the SAME AS? Not prevented by UMA Fedz, are there any use-cases for this? Yes, nothing prevents this
THere is discussion of some of these topic here: https://kantarainitiative.org/confluence/display/uma/UMA+Implementer's+Guide#UMAImplementer'sGuide-perm-request-patternsConsiderationsRegardingResourceServerPermissionRequests

Should we provide additional guidance on this topic?
There is also no restriction for the RS to have only 1 URI for a resource.
THere was some previous discussion around wild-card in resource path, other templating

- How does Alice know the URL of the resource?

```
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)




Possible API 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 (RMT) (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

informative
The use of the `uma_management` scope when requesting a RMT may indicate to the RS's authorization server that establishment of one or more PATs with an available UMA AS is 'useful'

RM -> RS: /authorize?scope=uma_protection
Alice <-> RS: authenticate
RS -> RS: are there any PATs available PATs for Alice?
RS --> Alice: 'do you want to setup an UMA AS?'
Alice -> RS: yes@ uma.as.location
RS --> Alice: 302 uma.as.location/authorize

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 is a resource server defined identifier for a resource.
Before a resource is registered at an AS, there is no handle/reference available (unless the RS provides one)

GET /my-resources/
```
[
{
        "_resource_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/rsrcs/photoalbum",

   // uri/location of the resource?

   protected_at: (optional) [
      {
      // (_id in UMA Fedz)
      // does the RMT need to know this value? yes since this resource can be registered multiple times at an
AS
      "authorization_sever_resource_registration_id" : "_as_issued_id_for_resource_ABC"


      "authorization_server" : "as_identifier",
      "registered_scopes" : [ "view" ],
      "user_access_policy_uri" : url (optional)
      }
   ]
},

]
```



Protected Resources
```
[
{
        "_resource_id" "ABC",
           "authorization_sever_resource_id" : "_as_id"

           "authorization_server" : "as_identifier",
           "registered_scopes" : [ "view" ]
},
{
        "_resource_id" "ABC",
           "authorization_sever_resource_id" : "_as_id_2"
           "authorization_server" : "as_identifier_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

RS_1 holds pension A with identifier a
RS_1 registers pension A


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

GET /my-authorization-servers/
```
[
{
as_url: "http://authserver_id.ca"
has_as_pat: true
},
{
as_url: "http://authserver_id2.com"
has_as_pat: false
}
]

```

POST /my-as/:one/resource
```
{
   _rs_resource_id:
   scopes: []
}
```

~~~~
```

vs

POST /my-resource/:abc/authorization-server
```
{
   _as_id:
   scopes: []
}
```
~~~~

AOB

Attendees

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

Voting:

1. Eve
2. Peter
3. Michael
4. Alec

Non-voting participants:

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

Regrets: