UMA Resource Registration – Draft 01

**Introduction**
This draft defines the resource registration allowing UMA hosts to communicate which resources should be policy protected at authorization managers. For each registered resource, the host expects that the authorization manager will be able to evaluate requests issued by requesters against applicable policies. Resource registration requires that there is a pre-established trust relationship between a host and AM (e.g. a host has been provisioned with an OAuth 2 access token for using the AM).

**Terminology**

**resource registration endpoint**
The authorization manager’s HTTP endpoint capable of receiving information identifying resource at the host.

**Discovery of resource registration endpoint**
The host uses the [sitemeta] and [hostmeta] discovery mechanisms to learn about the URI of the resource registration endpoint at the authorization server at which the host wants to register a user’s resources. The authorization server MUST provide a host-meta document containing:

- Link element with the following rel value of [http://kantarainitiative.org/uma/am/resource_registration](http://kantarainitiative.org/uma/am/resource_registration)
  (REQUIRED)

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<XRD xmlns="http://docs.oasis-open.org/ns/xri/xrd-1.0">
  <Subject>http://am.example.com</Subject>
  <Link rel="http://kantarainitiative.org/uma/am/resource_registration"
    href="https://am.example.com/uma/resource_reg">Resource Registration Endpoint</Link>
</XRD>
```

**Resource Registration Flow**
The Resource Registration flow is suitable when the Authorizing User is at the Host side and wants to register resources managed at this Host with their preferred Authorization Manager. It assumes that...
there is a pre-established trust relationship between a host and AM (e.g. a host has been provisioned with an OAuth 2 access token for using the AM). Establishing such a trust relationship, however, is not a part of this draft.

The flow works as following:

1. The user, when logged in at the Host, selects a resource which should be protected by a user’s preferred AM, e.g. by clicking on a “Share” button visible on the Web site displayed by the Host.
2. The Host makes an authorized request (i.e. with included OAuth token) to the AM’s resource registration endpoint informing the AM about the resource which should be policy protected.
3. Based on the provided information in the request, the AM adds the resource to the pool of protected resources of a user. For example, a resource can be automatically associated with a default policy or may require further managing by the user at the AM. The AM then confirms to the Host with that a resource has been added successfully and provides a URI where a user can be directed to further manage the resource at the AM side.
4. The Host redirects the user to the URI provided by the Authorization Manager and attaches the information about the URI on the host where the user should be redirected back.
5. The User manages a resource at the AM side – e.g. associates a resource with an existing policy or creates a new policy for this resource. The AM then redirects the user back to the URI provided by the host.
Resource Registration

1 - Resource Registration Request
The Host makes an OAuth–authorized HTTP POST request to the resource registration endpoint at the AM and includes the following parameters in the request:

- `uma_resource_uri` (REQUIRED)
- `uma_resource_name` (REQUIRED)
- `scopes` (OPTIONAL)

The host MAY include additional information in the request and the authorization manager MAY ignore this information.

For example, the client sends:

```plaintext
POST /uma/resource_reg HTTP/1.1
Host: am.example.com
Content-Type: application/x-www-form-urlencoded
Authorization: OAuth EQ1GAWxWcKUU
uma_resource_uri=http://host.example.com/photo/123&uma_resource_name=Family%20Photo&view=View%20Photo&edit=Edit%20Photo
```

The parameters are included in the entity body of the HTTP request using the "application/x-www-form-urlencoded" media type as defined by [W3C.REC-html401-19991224].

2 - Resource Registration Response
The Authorization Manager registers the resource information provided by the Host and responds with a confirmation response which defines the location where further processing of such a resource can be done by the user. This location is sent in the entity body of the HTTP response with a 200 status code (OK):

- `uma_resource_uri` (REQUIRED)
- `uma_resource_confirmation_uri` (REQUIRED)

The parameters are included in the entity body of the HTTP response using the "application/json" media type as defined by [RFC4627]. The parameters are serialized into a JSON structure by adding each parameter at the highest structure level. Parameter names and string values are included as JSON strings.
For example:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "uma_resource_uri":"http://host.example.com/photo/123"
    "uma_resource_confirmation_uri":"https://am.example.com/resources/55"
}
```

**Error Message**

If the request for registration is invalid or unauthorized, the authorization server constructs the response by adding the following parameters to the entity body of the HTTP response with a 400 status code (Bad Request) using the “application/json” media type:

- error (REQUIRED)
- description (OPTIONAL)
- error_uri (OPTIONAL)

*TBS: We need standardized error codes.*

**Resource Confirmation**

**3 – Resource Confirmation Request**

The Host redirects the user to the confirmation URI provided by the Authorization Manager in the Resource Registration response and includes the following parameters in the request:

- uma_resource_redirect_uri (REQUIRED)
- state (OPTIONAL)

The host MAY include additional information in the request and the authorization manager MAY ignore this information.

For example, the host sends:

```
HTTP/1.1 302 Found
Location: https://am.example.com/resources/55?uma_resource_redirect_uri=https%3a%2f%2fhost.example.com%2fuma%2fredirect&state=q5543
```

The parameters are added to the URI query component using the "application/x-www-form-urlencoded" format as defined by [W3C.REC-html401-19991224].

The Resource Confirmation request is optional and the host may choose not to redirect the User to the URI provided by the Authorization Manager in the Resource Registration Response.
4 - Resource Confirmation Response

The AM redirects the User to the URI provided by the host in the Resource Confirmation Request. If the state parameter was set in the Resource Confirmation Request then this parameter MUST be included in the response by the Authorization Manager.

The Authorization Manager MAY include additional information in the response and the host MAY ignore this information.

For example, the authorization manager sends:

```
HTTP/1.1 302 Found
Location: https%3a%2f%2fhost.example.com%2fuma%2fredirect%3fstate%3dq5543
```

The parameters are added to the URI query component using the "application/x-www-form-urlencoded" format as defined by [W3C.REC-html401-19991224].

References

[sitemeta] Defining Well-Known Uniform Resource Identifiers (URIs) (RFC5785)

[hostmeta] Web Host Metadata

[W3C.REC-html401-19991224]