UMA Claim Profiles

Introduction
In UMA ecosystem, the Authorization Manager provides the access control to the distributed personal data, based on a fine-grained claims-based authorization decision, and it can mediate the online Authorizing User's consent.

UMA Claims profile specifies a set of Claims or attributes necessary for the authorization decision in a specific context.

UMA Claim Profiles
The following diagram shows a first level of claim profiles based on a data sharing taxonomy.

The profiles include:
• Life
• Social
• Participatory
• Enterprise

Claims Life Profile
Personal information sharing is an emerging trend for online daily life activities (Financial credit, Insurance, Home, Healthcare, etc).
A typical Life profile is when an Authorizing User (subject), in order to obtain a specific online service from a Service Provider (SP), should give a consent to share personal information with the SP.

In general, for this profile, there are the following interactions:

I. Authorizing User -> SP (Human interaction for requesting service)
II. SP -> AM (Machine-to-Machine interaction for authorization)
III. Authorizing User -> AM (Human interaction for consent)

The following table defines a set of predefined Claims for this specific profile and the applicable AM's Access policy.

<table>
<thead>
<tr>
<th>Type</th>
<th>Attributes</th>
<th>Description</th>
<th>AM Access Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Requested Data</td>
<td></td>
<td>AM can identify the Claims profile based on requested data</td>
</tr>
<tr>
<td></td>
<td>Resource URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requester</td>
<td>Organization</td>
<td></td>
<td>AM can deny access to Service Providers that are in a black list</td>
</tr>
<tr>
<td></td>
<td>Website</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Responsabile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Management</td>
<td>Purpose</td>
<td></td>
<td>AM can verify if they meet a legal framework, or deny access to SP from specific country.</td>
</tr>
<tr>
<td></td>
<td>Data Retention</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Country/Legal framework</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authority</td>
<td>Authority System</td>
<td></td>
<td>AM can deny access to Service providers that are not authorized by an Authority.</td>
</tr>
<tr>
<td></td>
<td>Authorization Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Attributes</td>
<td>Description</td>
<td>AM Access Policy</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authority</td>
<td>Website</td>
<td>AM can deny access to Service providers that are not authorized by an Authority.</td>
<td></td>
</tr>
<tr>
<td>Authenticity</td>
<td>Signature</td>
<td>AM can verify the Signature for further authenticity and integrity check</td>
<td></td>
</tr>
</tbody>
</table>

**Online Personal Loan Request Scenario**

The following picture shows the online Personal Loan Request scenario where an Authorizing User applies for a online personal loan request, which could represent a Claim Life Profile example.
Claims Request object
{
   "Requested data": "Risk Score",
   "Identifier": "12345",
   "Claims": "life"
}

Claims Response
{
   "Requested data": "Risk Score",
   "Identifier": "12345",
   "Claims": "life"
}
{
    "organization": "Financial Service",
    "website": "https://www.finacialService.com"
}

"responsable":
{
    "name": "Bob Smith",
    "email": "bob@financialservice.com"
}

"authority":
{
    "authority system": "Financial Credit Organization",
    "authorization number": "0987",
    "website": "https://fco.com/"
}

"data management"
{
    "purpose": "Loan request evaluation",
    "retention": "legal framework",
    "country": "US"
}

"signature":
{
    "algorithm":
    "signed data":
}