Requirements for Federations Operators Assessing R&S

Assessing Service Providers for R&S Compliance

The following requirements are proposed as a minimal expectation for a Federation Operator to be asserting R&S for Service Providers within their federation. It is important when using Legitimate Interests as a reason for processing data that organisations are able to demonstrate that they conducted an assessment, documented this assessment and given transparency and visibility to that assessment (see guidance from Article 29 WP).

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The Federation Operator actively declares support for R&amp;S. Declare support by email to <a href="mailto:contact@refeds.org">contact@refeds.org</a>. This will be re-verified as part of the REFEDS annual audit.</td>
</tr>
<tr>
<td>2.</td>
<td>Maintain a detailed description of the federation's administrative process for tagging a Service Provider with R&amp;S. Host a wiki or web page with information for SPs.</td>
</tr>
<tr>
<td>3.</td>
<td>Have a clear assessment process for Service Providers. Consider using the following checks:</td>
</tr>
<tr>
<td></td>
<td>- Can the SP demonstrate a reasonable need to use the full R&amp;S bundle?</td>
</tr>
<tr>
<td></td>
<td>- Is there a relevant and appropriate relationship between the data subject and the Service Provider?</td>
</tr>
<tr>
<td></td>
<td>- Would there be a reasonable expectation on the part of the data subject that personal data will be released?</td>
</tr>
<tr>
<td></td>
<td>- Does the Service Provider demonstrate appropriate safe-guards / effective behaviour regarding data protection (e.g. do they have a privacy notice? do they use a code of conduct etc?)</td>
</tr>
<tr>
<td></td>
<td>- Does the entity meet the registration criteria in Section 4 of the specification?</td>
</tr>
<tr>
<td>4.</td>
<td>Have a Process for reviewing use of R&amp;S. Have measures in place to review R&amp;S where you are the Registration Authority. This may be in line with the annual REFEDS review of R&amp;S.</td>
</tr>
<tr>
<td>5.</td>
<td>Have a Process for removing R&amp;S from a Service Provider. Have a simple process that allows for the removal of R&amp;S if an entity no longer meets the requirements, cannot demonstrate compliance or no longer wishes to support R&amp;S.</td>
</tr>
</tbody>
</table>

Technical Details

The following technical information may be useful.

The R&S entity attribute for SPs

```xml
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <!-- the RandS entity attribute for SPs -->
  <saml:Attribute
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="http://macedir.org/entity-category">
    <!-- the REFEDS RandS entity attribute value -->
    <saml:AttributeValue>http://refeds.org/category/research-and-scholarship</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```
The R&S "support" entity attribute for IdPs

```xml
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <!-- the RandS entity attribute for IdPs -->
  <saml:Attribute
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="http://macedir.org/entity-category-support">
    <!-- the REFEDS RandS entity attribute value -->
    <saml:AttributeValue>http://refeds.org/category/research-and-scholarship</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

A Shib IdP V3 configuration that releases attributes to ALL R&S SPs

```xml
<afp:AttributeFilterPolicy id="releaseToRandSSPs">
  <afp:PolicyRequirementRule xsi:type="saml:EntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://refeds.org/category/research-and-scholarship/>

  <!-- attribute rules here -->
</afp:AttributeFilterPolicy>
```

For brevity, the `<afp:AttributeRule>` elements have been omitted from the previous configuration element. For details, visit the R&S IdP Config wiki topic.

Resources

1. REFEDS Research & Scholarship Entity Category specification [http://refeds.org/category/research-and-scholarship](http://refeds.org/category/research-and-scholarship)
2. Shibboleth IdP V3
   a. EntityAttributeExactMatch Configuration [https://wiki.shibboleth.net/confluence/x/OAEnAQ](https://wiki.shibboleth.net/confluence/x/OAEnAQ)
   b. RegistrationAuthority Configuration [https://wiki.shibboleth.net/confluence/x/TAEnAQ](https://wiki.shibboleth.net/confluence/x/TAEnAQ)
3. Shibboleth IdP V2
   a. AttributeRequesterEntityAttributeExactMatch Configuration [https://wiki.shibboleth.net/confluence/x/ByVAX](https://wiki.shibboleth.net/confluence/x/ByVAX)