Requirements for Federations Operators Assessing Access-Related Entity Categories

Assessing Service Providers for Compliance with Anonymous, Pseudonymous, and Personalized Access Entity Categories

The following requirements are proposed as a minimal expectation for a Federation Operator to be asserting either Pseudonymous Access or Personalized Access 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). They can also be used inversely to ensure that an Anonymous tag is correctly applied.

	Requirement	Implementation
1.	Maintain a detailed description of the federation's administrative process for tagging a Service Provider with Anonymous, Pseudonymous, and/or Personalized Access Entity Categories	Host a wiki or web page with information for SPs.
2.	Have a clear assessment process for Service Providers	Consider using the following checks: ☐ Can the SP demonstrate a reasonable need to use the full attribute bundle for either entity category? ☐ Is there a relevant and appropriate relationship between the data subject and the Service Provider? ☐ Would there be a reasonable expectation on the part of the data subject that personal data will be released? ☐ Does the Service Provider demonstrate appropriate safeguards / effective behavior regarding data protection (e.g., do they have a privacy notice? do they use a code of conduct, etc?) ☐ Does the entity meet the registration criteria in Section 4 of each specification?
3.	Have a process for reviewing the use of these Entity Categories	Have measures in place to periodically review the registration criteria for the Service Providers where you are the Federation Registration Authority.
4.	Have a Process for removing either Entity Category tag from a Service Provider	Have a simple process that allows for the removal of either Entity Category tag if an entity no longer meets the requirements, cannot demonstrate compliance, or no longer wishes to support these Entity Categories.

Technical Details

The following technical information may be useful.

The Anonymous Access entity attribute for SPs

```
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <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">
    <saml:AttributeValue>https://refeds.org/category/anonymous</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

The Anonymous Access "support" entity attribute for IdPs

```
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <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">
    <saml:AttributeValue>http://refeds.org/category/anonymous</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

The Pseudonymous Access entity attribute for SPs

```
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <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">
    <saml:AttributeValue>https://refeds.org/category/pseudonymous</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

The Pseudonymous Access "support" entity attribute for IdPs

```
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <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">
  <saml:AttributeValue>https://refeds.org/category/pseudonymous</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

The Personalized Access entity attribute for SPs

```
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <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">
    <saml:AttributeValue>https://refeds.org/category/personalized</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

The Personalized Access "support" entity attribute for IdPs

```
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <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">
    <saml:AttributeValue>https://refeds.org/category/personalized</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

Resources

1. REFEDS Anonymous Access Entity Category specification https://refeds.org/category/anonymous
2. REFEDS Pseudonymous Access Entity Category specification https://refeds.org/category/pseudonymous
3. REFEDS Personalized Access Entity Category specification https://refeds.org/category/personalized
4. Anonymous Authorization, Pseudonymous Authorization, and Personalized Access FAQ