Attribute Release Requirements

This document is an attempt to rewrite the R&S specification for clarity and simplicity without breaking existing R&S deployments.

⚠ The following draft text is for discussion only! For comparison, the official normative text is shown below the horizontal line.

2. Syntax

The following URI is used as the attribute value for the Research & Scholarship (R&S) Entity Category and Entity Category Support attribute:

```
http://refeds.org/category/research-and-scholarship
```

A Service Provider that conforms to R&S exhibits the following entity attribute in its metadata:

An entity attribute for SPs that conform to R&S

```
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <!-- entity attribute for SPs that conform to R&S -->
  <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.org R&S entity attribute value -->
    <saml:AttributeValue>
      http://refeds.org/category/research-and-scholarship
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

An Identity Provider that supports R&S self-asserts the following entity attribute in its metadata:

An entity attribute for IdPs that support R&S

```
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <!-- entity attribute for IdPs that support R&S -->
  <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.org R&S entity attribute value -->
    <saml:AttributeValue>
      http://refeds.org/category/research-and-scholarship
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

5. Attribute Bundle

The *R&S attribute bundle* consists of the following attributes:

- *shared user identifier*
- *person name*
- *email address*

where *shared user identifier* is a persistent, non-reassigned, non-targeted identifier defined to be any one of the following:

1. `eduPersonPrincipalName` (if non-reassigned)
2. `eduPersonPrincipalName` + `eduPersonTargetedID`

and where *person name* is defined to be any one of the following:

1. `displayName`
2. `givenName` + `sn` (surname)

and where *email address* is defined to be the `mail` attribute.

6. Attribute Request

Service Providers SHOULD request a subset of the R&S attribute bundle that represents only those attributes that the Service Provider requires to operate its service.

7. Attribute Release

An Identity Provider supports the Research & Scholarship (R&S) category if, for some subset of the Identity Provider's user population, the Identity Provider is willing and able to release the R&S attribute bundle to **all** conforming R&S Service Providers without administrative involvement, either automatically or subject to user consent.

An Identity Provider MUST release the R&S attribute bundle to any conforming R&S Service Provider upon request, without regard for any R&S attributes requested in Service Provider metadata.

---

2. Syntax

The following URI is used as the attribute value for the Entity Category and Entity Category Support attribute: http://refeds.org/category/research-and-scholarship

5. Attribute Request

Service Providers SHOULD request a subset of R&S Category Attributes that represent only those attributes that the Service Provider requires to operate its service.

6. Attribute Release

Identity Providers are strongly encouraged to release the following bundle of attributes to R&S category Service Providers:

- personal identifiers: email address, person name, eduPersonPrincipalName.
- pseudonymous identifier: eduPersonTargetedID.
- affiliation: eduPersonScopedAffiliation.

Where email address refers to the mail attribute and person name refers to displayName and optionally givenName and sn (i.e., surname).

An Identity Provider supports the R&S Category if, for some subset of the Identity Provider's user population, the Identity Provider releases a minimal subset of the R&S attribute bundle to R&S Service Providers without administrative involvement, either automatically or subject to user consent. The following attributes constitute a minimal subset of the R&S attribute bundle:

- eduPersonPrincipalName
- mail
- displayName OR (givenName AND sn)

For the purposes of access control, a non-reassigned persistent identifier is required. If your deployment of eduPersonPrincipalName is non-reassigned, it will suffice. Otherwise you MUST release eduPersonTargetedID (which is non-reassigned by definition) in addition to eduPersonPrincipalName. In any case, release of both identifiers is RECOMMENDED.

7. Examples

Standard entity attribute for R&S Service Providers:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://service.example.com/sp">
<Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
<mdattr:EntityAttributes xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:Attribute
Name="http://macedir.org/entity-category"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue>http://refeds.org/category/research-and-scholarship>
</saml:Attribute>
</mdattr:EntityAttributes>
</Extensions>
…
</EntityDescriptor>
```

Standard entity attribute for R&S Identity Providers:

```
<EntityDescriptor xmlns=”urn:oasis:names:tc:SAML:2.0:metadata”
entityID=”https://service.example.com/idp”>
<Extensions xmlns:mdattr=”urn:oasis:names:tc:SAML:metadata:attribute”>
<mdattr:EntityAttributes xmlns:saml=”urn:oasis:names:tc:SAML:2.0:assertion”>
<saml:Attribute
Name=”http://macedir.org/entity-category-support”
NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”>
<saml:AttributeValue>http://refeds.org/category/research-and-scholarship> </saml:Attribute>
</mdattr:EntityAttributes>
</Extensions>
…
</EntityDescriptor>
```