R&S Clarification Proposal

This document is an attempt to clarify the R&S specification to address issues that have arisen in its initial deployment by federations, particularly confusion over its relationship to other, unrelated mechanisms and regimes for attribute release facilitation. It also attempts to clarify what an SP and IdP are obligated or assumed to be doing, and moves some "implicit" guidance into formally suggested behavior.

> ⚠ While it represents a perception of some mild consensus on the REFEDS list and reflects wider discussion on one phone conference, it currently should be viewed as the author's opinion, pending further review.

Summary of Changes

Minor wording clarifications and larger explicit clarifications addressing points of apparent differing practice are included in green.

Suggested deletions of requirements that have led to confusion and differing practice are ~~struck through~~.

The author believes the changes made would not cause any existing SP claiming the category to become unable to do so. It is a given based on discussion on the list that some IdPs claiming the category would become unable to do so.

Overview

Research and Education Federations are invited to use the REFEDS Research and Scholarship Entity Category with their members to support the release of attributes to Service Providers meeting the requirements described below.

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 [RFC2119]. This definition is written in compliance with the Entity Category SAML Entity Metadata Attribute Types specification [EntityCatTypes].

An FAQ for the Entity Category has been made available to help deployments [R&SFAQ].

1. Definition

Candidates for the Research and Scholarship (R&S) Category are Service Providers that are operated for the purpose of supporting research and scholarship interaction, collaboration or management, at least in part.

Example Service Providers may include (but are not limited to) collaborative tools and services such as wikis, blogs, project and grant management tools that require some personal information about users to work effectively. This Entity Category should not be used for access to licensed content such as e-journals.

Identity Providers may indicate support for Service Providers in this category (typically through self-assertion, though this is not required) to facilitate discovery and improve the user experience at Service Providers.

The following sections detail the requirements for both Service Providers and Identity Providers, in category membership and support respectively.

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
```

3. Semantics

By asserting a Service Provider to be a member of an Entity Category, a registrar claims that:

- 3.1 The Service Provider has applied for membership in the Category and complies with the R&S registration criteria.
- 3.2 The Service Provider’s application for R&S has been reviewed and approved by the registrar.

In possessing the Entity Category Attribute with the above value, a Service Provider claims that it will not use attributes for purposes that fall outside of the service definition.

In possessing the Entity Category Support Attribute with the above value, an Identity Provider claims that it will release attributes to R&S Service Providers as outlined in the “Identity Provider Attribute Release” section below.

4. Registration Criteria

When a Service Provider’s registrar (normally the Service Provider’s home federation) registers the Service Provider in the Entity Category, the registrar MUST perform at least the following checks:

- 4.1 The service enhances the research and scholarship activities of some subset of the registrar’s user community.
- 4.2 Service metadata has been submitted to the registrar ~~and published in the registrar’s public metadata aggregate~~ for publication.
- 4.3 The service meets the following technical requirements:
    - 4.3.1 The Service Provider is a production SAML deployment that supports SAML V2.0 HTTP-POST binding.

- 4.3.2 The Service Provider claims to refresh federation metadata at least daily.
- 4.3.3 The Service Provider provides an mdui:DisplayName and mdui:InformationURL in metadata.
- 4.3.4 The Service Provider provides one or more technical contacts in metadata.
- ~~4.3.5 The Service Provider provides requested attributes in metadata.~~

R&S Service Providers MUST resolve issues of non-compliance within a reasonable period of time from when they become aware of the issue. Failure to do so MUST result in revocation of the entity's membership in the R&S category.

5. Attribute Bundle

The mechanism by which this entity category provides for consistent attribute release is through the definition of a set of commonly supported and consumed attributes typically required for effective use of R&S services. The attributes chosen represent a privacy baseline such that further minimization achieves no particular benefit. Thus, the minimal disclosure principle is already designed into the category.

The use of the `<md:RequestedAttribute>` mechanism supported by SAML metadata is outside the scope of this category, and may co-exist with it in deployments as desired, subject to this specification's requirements being met.

The *R&S attribute bundle* consists (abstractly) of the following required data elements:

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

and one optional data element:

- *affiliation*

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

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

and where *person name* is defined to be either (or both) of the following:

1. `displayName`
2. `givenName` + `sn`

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

and where *affiliation* is defined to be the `eduPersonScopedAffiliation` attribute.

All of the above attributes are defined or referenced in the [eduPerson] specification. The specific naming and format of these attributes is guided by the protocol in use. In the case of SAML 2.0 the [SAMLAttr] profile MUST be used. This specification may be extended to reference other protocol-specific formulations as circumstances warrant.

6. Service Provider Requirements

~~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.~~

Service Providers SHOULD limit their data requirements to the bundle of attributes defined in Section 5, but MAY negotiate for additional data as required via mechanisms that are outside the scope of this specification.

Service Providers are strongly encouraged to support all of the specified alternatives for the *shared user identifier* and *person name* attributes described in Section 5 to maximize interoperability. Failure to do so will result in problems even when working exclusively with Identity Providers that claim support for the category. In the case of the `eduPersonTargetedID` attribute, this recommendation includes the ability to support SAML 2.0's "persistent" Name Identifier format, which is the recommended modern expression of the `eduPersonTargetedID` attribute in SAML 2.0.

In accordance with the requirements in Section 7, if an Identity Provider exhibits the R&S entity attribute in its metadata and no accompanying `eduPersonTargetedID` attribute is recieved, then Service Providers can rely on the non-reassignment of `eduPersonPrincipalName` values it receives from that Identity Provider.

Alternatively, Service Providers can obtain a non-reassigned *shared user identifier* by combining (e.g., concatenating) the `eduPersonPrincipalName` and `eduPersonTargetedID` values. If a given combination of the two values ever changes, Service Providers can assume that the `eduPersonPrincipalName` has been reassigned and now represents a different subject.

A Service Provider that conforms to R&S would exhibit the following entity attribute in SAML metadata:

An entity attribute for SPs that conform to R&S

```
<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>http://refeds.org/category/research-and-scholarship</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

7. Identity Provider Requirements

An Identity Provider indicates support for the R&S Category by exhibiting the R&S entity attribute in its metadata. Such an Identity Provider MUST, for a significant subset of its user population, release all required attributes in the bundle defined in Section 5 to all R&S Service Providers without administrative involvement by any party, either automatically or subject to user consent.

An Identity Provider that does not release all of the required elements of the R&S attribute bundle (*shared user identifier*, *person name*, *email address*), for any reason, SHALL NOT exhibit the R&S entity attribute in its metadata. Exceptions, limiting the release of attributes to specific R&S Service Providers, may be permitted in the event of a security incident or other isolated circumstances.

~~For the purposes of effective access control,~~ A persistent, non-reassigned, non-targeted identifier is REQUIRED. If the Identity Provider's deployment of `eduPersonPrincipalName` is non-reassigned, and the organization believes in good faith that it will remain so, it will suffice. Otherwise the Identity Provider MUST release `eduPersonTargetedID` (which is non-reassigned by definition) in addition to `eduPersonPrincipalName`. In any case, release of both identifiers is RECOMMENDED. Likewise the release of all three *person name* attributes (`displayName`, `givenName`, `sn`) is also RECOMMENDED.

Identity Providers are strongly encouraged to release the entire attribute bundle (both required and optional attributes) defined in Section 5 to R&S category Service Providers, both to maximize interoperability and the scope of supported services. The only optional data element is *affiliation*, which while different in nature to the rest of the bundle, is important to many R&S services and is a particular differentiator for academic organizations.

An Identity Provider that supports R&S would exhibit the following entity attribute in SAML metadata:

An entity attribute for IdPs that support R&S

```
<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/research-and-scholarship</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

References

[EntityCatTypes] Young, I, Johansson, L, and Cantor, S Ed., “The Entity Category SAML Attribute Types”, July 2014.

[R&SFAQ] Harris, N., “Research and Scholarship FAQ”, November 2014.

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997.

[eduPerson] Internet2 MACE Directory Working Group, "eduPerson Object Class Specification (201602)", February 2016.

[SAMLAttr] Internet2 MACE Directory Working Group, "MACE-Dir SAML Attribute Profiles", April 2008.