The consultation process and review by the Schema Editorial Board identified areas in which the language and layout of the entity category proposal could be improved. One major concern is not addressed - the concern that the category in itself creates an anti-pattern (see comments at: https://wiki.refeds.org/display/CON/Entity+Category+Consultation%3A+Authentication+Only). If this was seen to continue to be a concern, it would not be possible to move forward with this category.

Authentication Only Entity Category

Overview

All Identity Providers and Service Providers are invited to use the Authentication Only Entity Category with their members to support completely anonymous, privacy-preserving single sign-on to Service Providers meeting the requirements described below.

The keywords “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]; this specification may be extended to reference other protocol-specific formulations as circumstances warrant.

1. Definition

Candidates for the Authentication Only Entity Category are any Service Providers that grant service access solely based on proof of successful authentication; they wish to provide a completely privacy-preserving experience and do not require any user attributes.

Example Service Providers may include (but are not limited to) services to support access to online content and research data sets that require no specific information about users or their affiliation to work effectively.

The following sections detail the requirements for both Service Providers (SP) and Identity Providers (IdP), 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:

`https://refeds.org/category/authenticationonly`

3. Semantics

By asserting that it is a member of this Entity Category, a Service Provider claims that it will not use attributes for purposes that fall outside of the Service Provider's privacy statement as listed in the privacy statement url in metadata as defined in the SAML V2.0 Metadata Extensions [MDUI]. Identity Providers may indicate support for Service Providers in this category by asserting the Entity Category Support Attribute with the above value; self-assertion is the typical approach used.

By asserting this attribute, Identity Providers are indicating that they will not release any user attributes to Service Providers who assert support for this category.

4. Attribute Handling

When a Service Provider claims membership in the Authentication Only Entity Category, it is signaling to the Identity Provider that it wishes to provide a completely anonymous, privacy-preserving service to the user. It does not wish to receive any user attributes from the Identity Provider.

When an Identity Provider sends an authentication assertion to a Service Provider in the Authentication Only category, it MUST suppress any user attributes from being released to the Service Provider. This includes any attribute that is released by default from the Identity Provider.

5. Service Provider Requirements

Service Providers MUST NOT require any user attributes from an Identity Provider in order to provide service to a user who has successfully authenticated.

ServiceProviders MUST provide at least one mdui:PrivacyStatementURLvalue [MDUI].

A Service Provider that conforms to Authentication Only exhibits the following entity attribute in SAML metadata:

An entity attribute for SPs that conform to Authentication Only:

```
<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="https://macedir.org/entity-category">
    <saml:AttributeValue>
      https://refeds.org/category/authenticationonly
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

6. Identity Provider Requirements

By declaring support for this category, an Identity Provider MUST suppress release of any attributes which might disclose the identity of the user to Service Providers who assert support for this category. .

An entity attribute for IdPs that support Authentication Only:

```
<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="https://macedir.org/entity-category-support">
    <saml:AttributeValue>
      https://refeds.org/category/authenticationonly
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

7. References

[EntityCatTypes] Young, I., Ed., Johansson, L., and S. Cantor, "The Entity Category Security Assertion Markup Language (SAML) Attribute Types", RFC 8409, DOI 10.17487/RFC8409, August 2018, <https://www.rfc-editor.org/info/rfc8409>.

[MDUI] Cantor, Scott et al. “SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0”, March 2005, <https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/os/sstc-saml-metadata-ui-v1.0-os.html>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.