Authentication Only Resource Access Entity Category

Overview

All Identity Providers and Service Providers are invited to use the Authentication Only Resource Access Entity Category (RAEC) 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 RAEC 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. For the purposes of this document, a *user attribute* is an attribute that reveals or may reveal a person’s identity, personal characteristics, contact information, or affiliation/role/access authorization.

Example Service Providers may include (but are not limited to) services to support access to online content and research data sets that require no 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.

N.B. This specification relates only to personal data passed between the IdP and the SP and does not relate to personal data requested directly from the end-user or their browser, potentially via a consent flow.

N.B. This specification details the default configuration and does not restrict additional entity categories or attributes from being requested or exchanged as a result of bilateral arrangements.

2. Syntax

The following URI is used as the attribute value for the Entity Category and Entity Category Support attribute:

```
https://example.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 definition as defined in the agreement, presented to its users, and referred to in metadata.

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 unless bilateral arrangements are in place.

4. Attribute Handling

When a Service Provider claims membership in the Authentication Only RAEC, 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 unless bilateral arrangements are in place. 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 unless bilateral arrangements are in place.

Service Providers MUST commit to following the principles of the GÉANT Data Protection Code of Conduct, and when supported by their federation assert this in metadata [DPCoCo].

The service provider MUST publish a statement of this practice that is accessible to end-users. This may be included in the service provider's privacy statement.

If the Identity Provider does send user attributes during the authentication flow, the service provider MUST discard them unless bilateral arrangements are in place.

The service provider MUST NOT assert the Anonymous Authorization RAEC, Pseudonymous Authorization RAEC, or Research and Scholarship attribute release bundle entity categories if it asserts this entity category, and the SP MUST NOT request any of the attributes described in those entity categories from the IdP through other mechanisms unless bilateral arrangements are in place [AnonRAEC] [PseudRAEC][R&S].

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://example.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 unless bilateral arrangements are in place.

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://example.org/category/authenticationonly
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

7. References

[AnonRAEC] “Anonymous Authorization Entity Category” - citation TBD

[PseudRAEC] “Pseudonymous Authorization Entity Category” - citation TBD

[R&SRAEC] “Research and Scholarship Entity Category,” REFEDS, https://refeds.org/category/research-and-scholarship.

[eduPerson] “eduPerson,” REFEDS, https://refeds.org/eduperson.

[DPCoCo] “Data Protection Code of Conduct Home,” GEANT, https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home.

[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>.

[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>.

[SAML2Int] “SAML V2.0 Deployment Profile for Federation Interoperability,” Kantara Initiative, 9 December 2019, https://kantarainitiative.github.io/SAMLprofiles/saml2int.html.

[SAML2SubjId] “SAML V2.0 Subject Identifier Attributes Profile Version 1.0,” OASIS, 19 January 2019, https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/cs01/saml-subject-id-attr-v1.0-cs01.html.

[SCHAC] “Schema for ACademia,” REFEDS, https://wiki.refeds.org/display/STAN/SCHAC.

Annex 1 - Implementation Guidance

Relationship to other Resource Access Entity Categories

For Service Providers

By asserting participation in a Resource Access Entity Category, a service provider (SP) is signaling to identity providers its minimally acceptable (required?) user attribute bundle to successfully grant the user access. Particularly when publishing the SP's SAML metadata in a federation, each unique SP SAML entity SHOULD assert at most one Resource Access Entity Category. For example, an SP entity asserting Authentication Only category SHOULD NOT simultaneously assert the Pseudonymous Authorization category. Doing so sends conflicting messages.

If a service needs to accommodate different resource access schemes due to contractual differences, the configuration SHOULD be handled in one of the following ways:

a. Express the difference in a separate entity metadata with a different entity ID;
b. Negotiate and configure the attribute release agreement bi-laterally, outside the scope of the Resource Access Entity Categories.

For Identity Providers

An Identity Provider (IdP) SHOULD simultaneously support all Resource Access entity categories.

Identity Provider Configuration

To properly support the Authentication Only Resource Access category, an Identity Provider (IdP) MUST NOT release any user attributes to an SP asserting the Authentication Only category unless bilateral arrangements are in place.

A *user attribute* is an attribute that reveals or may reveal a person's identity, personal characteristics, contact information, or affiliation/role/access authorization.

If your IdP does not by default release any user attribute, your IdP already meets the requirements of the Authentication Only category. There is no additional work required.

If your IdP by default releases user attributes, you will need to configure an attribute release rule to explicitly block the release of any user attribute to qualifying SPs. This rule must override any default attribute release behavior that conflicts with this rule.

For example, to configure a Shibboleth Identity Provider to block attribute release to support the Authentication Only category, include the following attribute filter policy in the Attribute Filter configuration (attribute-filter.xml):

```
<AttributeFilterPolicy id="refedsAuthenticationOnlyCategory">
  <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
      attributeName="http://macedir.org/entity-category"
      attributeValue="https://example.org/category/authenticationonly"/>

  <!-- In this example, the IdP by default release ePPN and ePTID.
       This configuration overrides those defaults and blocks
       their release. -->
  <AttributeRule attributeID="eduPersonPrincipalName">
    <DenyValueRule xsi:type="ANY"/>
  </AttributeRule>
  <AttributeRule attributeID="eduPersonTargetedID">
    <DenyValueRule xsi:type="ANY"/>
  </AttributeRule>
</AttributeFilterPolicy>
```