

SAML Subject-ID Attribuutit

Service Provider

Uuden profiilin käyttöönoton myötä SP:n on nyt mahdollista pyytää SAML Subject-ID:tä tai Pairwise-ID:tä. Tämän käyttöönotto tehdään [resurssirekisterissä](#) SP:lle "SP Basic information" välilehdellä. Tämä lisää metadataan [entiteetti attribuutti määrityksen](#) laajennusta käyttäen (Esimerkki alla, jossa palvelu pyytää pairwise-id:tä)

rr.funet.fi ja metadata

```
<EntityDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://rr.funet.fi/attribute-test">
  <Extensions>
    <mdattr:EntityAttributes>
      <saml:Attribute Name="urn:oasis:names:tc:SAML:profiles:subject-id:req" NameFormat="urn:oasis:names:tc:
SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>pairwise-id</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions> ...
```

Mahdollisia vaihtoehtoja ovat:

- not in use (laajennus ei ole käytössä)
- subject-id (SP pyytää subject-id:n)
- pairwise-id (SP pyytää pairwise-id:)
- none (SP ei pyydä kumpaakaan Subject-ID:tä)
- any (palvelulle kelpaa joko subject-id tai pairwise-id)

Shibboleth-SP:n attribute-map

attribute-map.xml

```
<Attribute name="urn:oasis:names:tc:SAML:attribute:subject-id" id="subject-id">
  <AttributeDecoder xsi:type="ScopedAttributeDecoder" caseSensitive="false"/>
</Attribute>

<Attribute name="urn:oasis:names:tc:SAML:attribute:pairwise-id" id="pairwise-id">
  <AttributeDecoder xsi:type="ScopedAttributeDecoder" caseSensitive="false"/>
</Attribute>
```

Identity Provider

Shibboleth-IdP:n mukana toimitetussa attribuutti filterissä on myös valmiina säännöt näiden subject-id attribuuttien välittämiselle. Filteri laskee pairwise-id:n läpi jos subject-id:nä pyydetään pairwise-id:tä tai any tyyppiä, subject-id välitetään vain siinä tapauksessa jos sitä pyydetään eksplisiittisesti.

attribute-filter.xml

```
<!--
Example rule for honoring Subject ID requirement tag in metadata.
The example supplies pairwise-id if subject-id isn't explicitly required.
-->
<AttributeFilterPolicy id="subject-identifiers">
  <PolicyRequirementRule xsi:type="ANY" />

  <AttributeRule attributeID="samlPairwiseID">
    <PermitValueRule xsi:type="OR">
      <Rule xsi:type="EntityAttributeExactMatch"
        attributeName="urn:oasis:names:tc:SAML:profiles:subject-id:req"
        attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        attributeValue="pairwise-id" />
      <Rule xsi:type="EntityAttributeExactMatch"
        attributeName="urn:oasis:names:tc:SAML:profiles:subject-id:req"
        attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        attributeValue="any" />
    </PermitValueRule>
  </AttributeRule>

  <AttributeRule attributeID="samlSubjectID">
    <PermitValueRule xsi:type="EntityAttributeExactMatch"
      attributeName="urn:oasis:names:tc:SAML:profiles:subject-id:req"
      attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      attributeValue="subject-id" />
    </AttributeRule>
</AttributeFilterPolicy>
```

Esimerkki resolverista kun käytetään pairwise-id:nä computedId:tä ja subject-id:nä eduPersonPrincipalNamea

attribute-resolver.xml

```
<AttributeDefinition id="samlSubjectID" xsi:type="Scoped" scope="{idp.scope}">
  <InputAttributeDefinition ref="eduPersonPrincipalName" />
</AttributeDefinition>

<AttributeDefinition id="samlPairwiseID" xsi:type="Scoped" scope="{idp.scope}">
  <InputDataConnector ref="computedSubjectId" attributeNames="computedId"/>
</AttributeDefinition>
```

On hyvä huomioida että Shibboleth-IdP:ssä oletuksena käytetään BASE64 enkoodausta, mutta suositus on käyttää BASE32 tyyppiä jolloin pienet kirjaimet rajautuvat pois. Kaikki tuotteet eivät suoriudu hyvin merkistöistä joissa isojen ja pienten kirjainten erolla on merkitystä.

- <https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html>
- <https://shibboleth.atlassian.net/wiki/x/TQFwSw>