Signalera tillitsprofil genom eduPersonAssurance

I identitetsfederationen SWAMID är tillit till att universitet och högskolor hanterar användare och inloggningar tillräckligt bra grunden för att tjänsteleverantörer ska lita på att det är rätt användare som loggar in. För att definiera vad som är tillräckligt bra i SWAMID finns två tillitsprofiler, SWAMID AL1 och SWAMID AL2. För mer information om tillitsprofilerna se sidan SWAMIDs Assurance Profiles.

Notera att det även är rekommenderat att släppa värden från REFEDS Assurance Framework tillsammans med SWAMIDs tillitsprofiler, se Release of assurance statements in the attribute eduPersonAssurance based on SWAMID Identity Profiles.

Organisationens tillitsprofiler i metadata

En identitetsutgivare får aldrig signalera annan tillitsprofil för en användare än vad både organisationen och användaren är godkända för. Organisationens godkännanden finns inlagt av SWAMID i metadatan för dess identitetsutgivare. Om en organisation är godkänd för SWAMID AL2 finns de unika identifierarna för både SWAMID AL1 och SWAMID AL2 medan om en organisation är godkänd för SWAMID AL1 finns endast den unika identifieraren för SWAMID AL1.

Tillitsprofiler i metadata

```
<saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns="" Name="urn:oasis:names:tc:SAML:
attribute:assurance-certification" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>http://www.swamid.se/policy/assurance/al1</saml:AttributeValue>
    <saml:AttributeValue>http://www.swamid.se/policy/assurance/al2</saml:AttributeValue>
</saml:Attribute>
```

eduPersonAssurance

Det attribut som används för att signalera till en tjänst vilken tillitsprofil är eduPersonAssurance. Alla användare vid en organisation behöver inte uppfylla samma tillitsprofil så länge som inloggningstjänsten via attributrelease kan särskilja vilken tillitsprofil som användaren har.

- Om användaren är godkänd för SWAMID AL2 och organisationen är godkänd för SWAMID AL2 signaleras detta via eduPersonAssurance med värdena http://www.swamid.se/policy/assurance/al1 och http://www.swamid.se/policy/assurance/al2,
- Om användaren är godkänd för SWAMID AL1 och organisationen är godkänd för SWAMID AL1 eller SWAMID AL2 signaleras detta via eduPersonAssurance SWAMID med värdet http://www.swamid.se/policy/assurance/al1,
- Om användaren inte är godkänd för någon tillitsprofil i SWAMID eller organisationen inte är godkänd för någon tillitsprofil i SWAMID får inte SWAMIDs tillitsprofiler signaleras via eduPersonAssurance,

Att både SWAMID AL1 och SWAMID AL2 signaleras för en användare som är godkänd för SWAMID AL2 beror på att tjänsteleverantörerna inte ska behöva veta tillitsprofilernas inbördes ordning.

Exempel Shibboleth: eduPersonAssurance finns i LDAP med endast högsta värdet

Förutsättningar:

- Användare som endast är godkända för SWAMID AL1 har i LDAP eduPersonAssurance med värdet http://www.swamid.se/policy/assurance/al1.
- Användare som är godkända för SWAMID AL2 har i LDAP eduPersonAssurance med värdet http://www.swamid.se/policy/assurance/al2.
- Användare som inte är godkända för varken SWAMID AL1 eller SWAMID AL2 har inte dessa markeringar i LDAP.

```
<resolver:AttributeDefinition xsi:type="Script" xmlns="urn:mace:shibboleth:2.0:resolver:ad" id="
eduPersonAssurance" >
     <resolver:Dependency ref="myLDAP" />
     <resolver:AttributeEncoder xsi:type="SAML1String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder" name="
urn:mace:dir:attribute-def:eduPersonAssurance" />
     <resolver:AttributeEncoder xsi:type="SAML2String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder" name="
urn:oid:1.3.6.1.4.1.5923.1.1.1.11" friendlyName="eduPersonAssurance" />
     <Script>
          <![CDATA[
               if ((eduPersonAssurance) && (eduPersonAssurance.getValues().contains("http://www.swamid.se/policy
/assurance/al2"))) {
                    eduPersonAssurance.getValues().add("http://www.swamid.se/policy/assurance/al1");
               }
          ]]>
     </Script>
</resolver:AttributeDefinition>
```

Exempel Shibboleth: eduPersonAssurance finns i Active Directory som gruppmedlemskap

Förutsättningar:

- Användare som endast är godkända för SWAMID AL1 är medlemmar i gruppen SWAMID-AL1.
- Användare som är godkända för SWAMID AL2 är medlemmar i gruppen SWAMID-AL2.
- Användare som inte är godkända för varken SWAMID AL1 eller SWAMID AL2 är inte medlemmar i någon av dessa bägge grupper.

```
 <resolver:AttributeDefinition xsi:type="Script" id="eduPersonAssurance" >
     <resolver:Dependency ref="myLDAP" />
     <resolver:AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:eduPersonAssurance" />
     <resolver:AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.11" friendlyName="
eduPersonAssurance" />
     <Script>
          <![CDATA[
               if (memberOf) {
                    for (i=0; i < memberOf.getValues().size(); i++) {
                         if (memberOf.getValues().get(i).equals("SWAMID-AL1")) {
                              eduPersonAssurance.getValues().add("http://www.swamid.se/policy/assurance/al1");
                         }
                         else if (memberOf.getValues().get(i).equals("SWAMID-AL2")) {
                              eduPersonAssurance.getValues().add("http://www.swamid.se/policy/assurance/al1");
                              eduPersonAssurance.getValues().add("http://www.swamid.se/policy/assurance/al2");
                         }
                    }
               }
          ]]>
     </Script>
</resolver:AttributeDefinition>
```