



Personliga certifikat i Sunet TCS

 Mål: Teknisk dokumentation hur ett lärosäte gör för att öppna möjligheten till personliga certifikat via TCS Personal. För frågor kring dokumentationen nedan kontakta operations snabel-a SWAMID.SE

 För mer information om personliga certifikat i Sunet TCS samt dess möjligheter och krav, se [Personal certificates requirements in Sunet TCS](#) i wikin för Sunet TCS.


Förutsättningar

- Lärosätet är godkänt för tillitsprofilen SWAMID AL2 samt användare som uppfyller SWAMID AL2 är uppmärkta med korrekt värde för **eduPersonAssurance!**
- Lärosätet har en Identity Provider uppsatt som är medlem i SWAMID (Om frågor - kontakta operations snabel-a SWAMID.SE).
- Lärosätet har blivit godkänd och konfigurerad som abonnent av TCS Personal.
- Attribut skickas till Service Providers i SWAMID enligt avsnittet attribute-filter.xml på wikisidan "[Example of a standard attribute filter for Shibboleth IdP](#)".

Rekommenderad arbetsgång

1. Modifiera attribute-resolvern för din Identity Provider så att den inkluderar rättighet att använda TCS enligt nedan beskrivet format (`eduPersonEntitlement (EPE)`).
2. Modifiera attribute-release policy för din Identity Provider enligt kod nedan. Syftet är att tillåta ivägskickande av uppgift om rättighet för certifikat baserat på eduPersonAssurance **SAMT** för test på sp.swamid.se.
3. Kontrollera att person med rätt rättighet kan logga in i TCS Personal och TCS Personal eScience med möjlighet att skapa certifikat.

Konfiguration för Shibboleth

 Konfigurationerna under detta avsnitt fungerar endast för Shibboleth 2 eller senare. För simpleSAMLphp och ADFS2 kan konfigurationsexemplen endast användas som inspiration.

Modifiera filen attribute-resolver.xml enligt:

Förutsättning: Attributet eduPersonAssurance är definierat tidigare i attribute-resolver.xml.

```

<resolver:AttributeDefinition xsi:type="Script" xmlns="urn:mace:shibboleth:2.0:resolver:ad" id="
tcsPersonalEntitlement" >
  <resolver:Dependency ref="eduPersonAssurance" />
  <resolver:AttributeEncoder xsi:type="SAML1String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder" name="
urn:mace:dir:attribute-def:eduPersonEntitlement" />
  <resolver:AttributeEncoder xsi:type="SAML2String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder" name="
urn:oid:1.3.6.1.4.1.5923.1.1.1.7" friendlyName="eduPersonEntitlement" />
  <Script>
    <![CDATA[
      if ((eduPersonAssurance) && (eduPersonAssurance.getValues().contains("http://www.swamid.se/policy
/assurance/al2")))) {
        tcsPersonalEntitlement.getValues().add("urn:mace:terena.org:tcs:personal-user");
      }
    ]]>
  </Script>
</resolver:AttributeDefinition>

<resolver:AttributeDefinition xsi:type="Script" xmlns="urn:mace:shibboleth:2.0:resolver:ad" id="
tcsPersonaleScienceEntitlement" >
  <resolver:Dependency ref="eduPersonAssurance" />
  <resolver:AttributeEncoder xsi:type="SAML1String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder" name="
urn:mace:dir:attribute-def:eduPersonEntitlement" />
  <resolver:AttributeEncoder xsi:type="SAML2String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder" name="
urn:oid:1.3.6.1.4.1.5923.1.1.1.7" friendlyName="eduPersonEntitlement" />
  <Script>
    <![CDATA[
      if ((eduPersonAssurance) && (eduPersonAssurance.getValues().contains("http://www.swamid.se/policy
/assurance/al2")))) {
        tcsPersonaleScienceEntitlement.getValues().add("urn:mace:terena.org:tcs:escience-user");
      }
    ]]>
  </Script>
</resolver:AttributeDefinition>

```

Modifera filen attribute-filter.xml

I [Example of a standard attribute filter for Shibboleth IdP](#) finns TCS Personal definierad men bortkommenterad.