SAML-konfiguration 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 Historical: 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.
3. Testa om attributreleasen är korrekt enligt instruktionerna på adressen SUNET TCS 2020- Information for administrators#Informationforadministrators-TestthatyourIdPiscorrectlyconfigured.
4. 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.

```
<AttributeDefinition xsi:type="ScriptedAttribute" id="tcsPersonalEntitlement">
     <InputAttributeDefinition ref="eduPersonAssurance"/>
     <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>
     <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:eduPersonEntitlement"
encodeType="false" />
     <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" friendlyName="
eduPersonEntitlement" encodeType="false" />
</AttributeDefinition>
```

I Example of a standard attribute filter for Shibboleth IdP och Example of a standard attribute filter for Shibboleth IdP v3.4.0 and above finns TCS Personal inlagd men bortkommenterad. Modifiera filen attribute-filter.xml.

Konfiguration för ADFS

På wikisidan Manual attribute releases with ADFS Toolkit finns information om hur du hanterar TCS Personal men du måste göra anpassningar efter era egna förutsättningar.