TCS Personal Certs

Hinweise und Konfigurationsdetails eines Shibboleth IDPs für das **GÉANT "Trusted Certificates Service**".

entityID

Der global eindeutige Name des SAML Services Providers von Sectigo (dem TCS-Anbieter ab Mitte 2020) lautet: `https://cert-manager.com/shibboleth`

Das Service wurde von der InCommon-Federation registriert und wird von dort über eduGAIN weiterpubliziert. D.h. nur jene ACOnet-Teilnehmerinstitutionen, die sowohl an eduID.at als auch an eduGAIN/Interfederation teilnehmen, können sich über ihre eigene Institution bei diesem Service anmelden, sei es für Admin-Zugriffe oder zum Beantragen persönlicher Zertifikate für Endbenutzer*innen.

Attribute

Admin-Zugriff SCM Portal

Für die TCS-Administrator*innen einer Institution ist die Anmeldung am Sectigo Certificate Manager (SCM)-Portal über SAML möglich. Dazu müssen die Attribute:

- eduPersonPrincipalName
- mail

vom IDP übermittelt werden (und zuvor vom ACOnet-Team im SCM provisioniert worden sein).

Persönliche Zertifikate

Für das Beantragen persönlicher Zertifikate (etwa zum Signieren von E-Mails) braucht das Service die folgenden Attribute:

- mail (institutionelle E-Mail-Adresse)
- displayName (voller Name)
- eduPersonPrincipalName (siehe unten)
- schacHomeOrganization (siehe unten)
- eduPersonEntitlement (siehe unten)

Der Service-URL des SAML Self-Service Portals lautet: https://cert-manager.com/customer/ACOnet/idp/clientgeant – siehe TCS FAQ.

eduPersonPrincipalName

TCS verengt für seine eigenen Zwecke die Definition von eduPersonPrincipalName (ePPN) und verbietet prinzipiell das Neuvergeben eines bestehenden ePPN an eine andere Person bei Nutzung des TCS Personal Certificate Services. Ein solches Wiederverwenden ist zwar ohnehin fast immer *bad practice*, wird aber in der für dieses Attribut autoritativen eduPerson-Spezifikation *nicht* ausgeschlossen. Darüber hinaus wird der ePPN oft aus der lokalen UserID (die zum Login zu Services wie IMAP oder SSH benutzt wird) gebildet, und die Nicht-Wiederverwendung von lokalen UserIDs steht in der Regel nicht zur Debatte, weil lokalen, jeweils unterschiedlichen, institutionellen Entscheidungen und Prozessen unterliegend.

Wenn also die Weitergabe bzw. Übernahme einer UserID von einer Person zu einer anderen (auch nach Jahren der "Stilllegung") an einer Institution *nicht ausgeschlossen* ist, sollte dort die UserID *nicht* zur Erzeugung des `eduPersonPrincicalName`-Attributs genutzt werden. *On-the-wire* übermittelt muß dennoch des Attribut "eduPersonPrincicalName" werden, aber dieses muß dann (zumindest *für dieses Service*) vom IDP *aus anderen Daten gespeist* werden.

Offensichlich ist es keine gute Idee, die Semantik von standardisierten und weltweit eingesetzten Attributen (wie jenen aus eduPerson) für eigene Zwecke abweichend festzulegen, wie das hier bei TCS geschehen ist. Aus Gründen der Kompatibiltät mit eingeführten Services wird dieses Attribut aber (bis auf Weiteres) beibehalten.

eduPersonEntitlement

Zur Beantragung persönlicher Zertifikate muß das eduPersonEntitlement-Attribut den folgenden Werte haben:

- `urn:mace:terena.org:tcs:personal-user`

Etwaige früher verwendete "`-admin`" Entitlement-Werte sind obsolet und können ggfs. lokal entfernt werden: Die Berechtigung für Administrator*innen erfolgt direkt (und nur) in SCM.

N.B.: Diese Entitlements dürfen *nur* unter bestimmten Bedingungen und *nur* an berechtigte Personen vergeben werden, siehe die jeweils gültigen TCS-Vereinbarungen (TODO).

schacHomeOrganization

Die Dokumentation zum Erzeugen/Nachschlagen von Attributen für den Shibboleth IDPv3 enthält eine fertige Vorlage zum Erzeugen von "schacHomeOrganization".

Attribute weitergeben

Die Weitergabe oben definierter Attribute wird wie üblich in `/opt/shibboleth-idp/conf/attribute-filter.xml` eingerichtet:

```
<AttributeFilterPolicy id="TCSportal">
  <PolicyRequirementRule xsi:type="Requester" value="https://cert-manager.com/shibboleth" />
  <AttributeRule attributeID="eduPersonPrincipalName" permitAny="true" />
  <AttributeRule attributeID="displayName" permitAny="true" />
  <AttributeRule attributeID="givenName" permitAny="true" />
  <AttributeRule attributeID="surname" permitAny="true" />
  <AttributeRule attributeID="mail" permitAny="true" />
  <AttributeRule attributeID="schacHomeOrganization" permitAny="true" />
  <AttributeRule attributeID="eduPersonEntitlement">
    <PermitValueRule xsi:type="Value" value="urn:mace:terena.org:tcs:personal-user" />
  </AttributeRule>
</AttributeFilterPolicy>
```