Att gruppera tjänsteleverantörer

Hur gör SWAMID det enklare för identitetsutgivarna att leverera rätt attribut till tjänsteleverantörerna

Entitetskategori, vad är det?

- Entitetskategorier används för att beskriva hur en identitetsutgivare (IdP) förväntas agera mot en tjänsteleverantör (SP).
- Identitetsfederationen markerar på varje tjänsteleverantör vilken eller vilka entitetskategorier som denna har.
- Entitetskategorier används idag av federationerna SWAMID, inCommon och Renater samt av interfederationen eduGAIN.

Entitetskategori, vad är det?

- I SAML2 metadata för tjänsteleverantörer (SP) är det möjligt att via en definierad utökning i metadata gruppera SP efter olika kategorier.

```
<EntityDescriptor entityID="https://foo.example.com">
  <Extensions>
    <EntityAttributes>
      <Attribute
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
         Name="http://macedir.org/entity-category">
        <AttributeValue>urn:oid:4.7.1.1</AttributeValue>
        <AttributeValue>http://www.swamid.se/category/hei-service</AttributeValue>
      </Attribute>
      ... Fler entitetskategorier ...
    </EntityAttributes>
  </Extensions>
  ...
</EntityDescriptor>
```

Exempel på entitetskategorityper

- Tjänsteleverantörens definierade lagrum.
- Grupperad standardrelease till tjänsteleverantör:
  - Släpp attribut A, B och C till tjänsteleverantörer som tillhör kategori X och
  - Släpp attribut A, C och D till tjänsteleverantörer som tillhör kategori Y.
- Grupperade attributdefinitioner *(ej SWAMID)*:
  - För alla tjänsteleverantörer som har kategori U gäller att namn ska alltid ska levereras i attribut A, B och C.
  - För alla tjänsteleverantörer som har kategori V gäller att namn ska alltid ska levereras i attribut A, B och E.

Entitetskategorier i SWAMID

1. SWAMID Data Protection Entity Categories *(SWAMID DPEC)* – Gruppering med avseende på lagrum för hantering av personuppgifter.
   - HEI Service – Tjänst hos universitet, högskola eller universitetets- och högskolegemensam tjänst – PUL + Särskild lagstiftning
   - NREN Service – Tjänst hos universitetens och högskolornas gemensamma organisation och infrastruktur för nationell och internationell datakommunikation – PUL + Särskilt avtal
   - EU Adequate Protection – Extern tjänst som uppfyller kraven för PUL eller motsvarande, inkl. tredje land.

Entitetskategorier i SWAMID

2. SWAMID Service Provider Attribute Release Entity Categories *(SWAMID SPAREC)* – Gruppering med avseende vilka attribut som bör skickas till tjänsteleverantören.
   - Research & Education – Tjänsteleverantören förväntar sig få och alla eller några av följande attribut; namn, epost, eduPersonPrincipalName, eduPersonTargetedID, scoped affiliation och organisationella attribut.
     - Finns endast I kombination med SWAMID DPEC.
   - SFS 1993:1153 – Tjänsteleverantören uppfyller förordningen och förväntar sig få personnummer.

Entitetskategorier i SWAMID

3. GÉANT Dataprotection Code of Conduct (GEANT CoC) – Gruppering för att på europerisk nivå med uppfyllande av EU data protection directive, dvs. PUL, definiera en minimalistisk release av ofarliga attribut.
   - Fristående från SWAMIDs övriga entitetskategorier med eget regelverk.
   - Attributen är av samma nivå som de som ingår i ett epost, dvs. namn, epost, eduPersonPrincipalName, scoped affiliation och organisationella attribut.
   - *Endast begärda attribut ska skickas över!*

Standardrelease utan entitetskategori

- En tjänsteleverantör som inte har någon entitetskategori ska i normalfallet utan särskild konfiguration för just denna tjänst endast få eduPersonTargetedID.

Tänkta exempel för tjänsteleverantörer

- Antagning.se – Universitetens och högskolornas gemensamma antagningssystem
  - Research & Education tillsammans med HEI Service
  - SFS 1993:1153
- SUNET Connect – SUNETs e-mötesplattform
  - Research & Education tillsammans med NREN Service
- Uppsala universitets Medarbetarportal – Samarbetsverktyg för verksamma vid UU samt inbjudna externa parter (inbjudan via personlig länk)
  - Research & Education tillsammans med HEI Service
  - GEANT CoC