Uppdatering entitetskategorier

Gruppering av tjänsteleverantörer för automatisk attributrelease

Definition

En entitetskategori är en särskild märkning av en tjänsteleverantör (SP) eller en identitetsutgivare (IdP) i metadata för att visa att denna har vissa behov, uppfyller vissa krav eller tillämpar en fördefinierad uppsättning regler och riktlinjer.

Hur fungerar det ***utan*** entitetskategorier?

- **Alternativ 1:** Identitetsutgivaren (IdP) definierar alltid via manuell konfiguration vilka attribut en viss tjänsteleverantör (SP) ska få vilket är tidsödande och skalar inte för flera hundra tjänsteleverantörer.
- **Alternativ 2 (rekommenderades i SWAMID 1):** Identitetsutgivaren skickar ut en standard-uppsättning av attribut till alla tjänsteleverantörer med manuell hantering av vissa extraattribut vilket är mindre bra ur ett integritetsperspektiv.

Hur fungerar det ***med*** entitetskategorier?

- **Alternativ 3 (rekommenderas i SWAMID 2):** Identitetsutgivaren tittar i metadata och skickar ut en uppsättning av attribut baserad på tjänsteleverantörens entitetskategori(er) eventuellt med manuell hantering av vissa extraattribut. Detta är den ”gyllene medelvägen” som gör att en identitetsutgivare kan skalbart skicka definierade attribut utan manuell konfiguration och samtidigt stärka den personliga integriteten.

Exempel på ett problem

- **En forskare från ett svenskt lärosäte ska delta i ett forskningssamarbete utanför det egna lärosätet.**
- För detta samarbete finns det en eller flera nödvändiga webbtjänster som är skyddade med federativ inloggning.
- Dessa webbtjänster är antingen anslutna direkt till SWAMID eller via interfederationen eduGAIN.
- När forskaren loggar in får denne inte tillgång till tjänsten eftersom forskarens identitetsutgivare inte släpper attribut till en för identitetsutfärdaren okänd webbtjänst.
- ***Forskaren kan därför inte delta i samarbetet!***

Entitetskategorier för tjänsteleverantörer (SP)

- Entitetskategorier för tjänsteleverantörer används för att beskriva dess behov av attribut från identitetsutgivare samt under vilket lagrum leverantören agerar.
- Exempel:
  - Grupperad standardrelease till tjänsteleverantörer, dvs. släpp attribut A, B och C till tjänsteleverantörer som tillhör kategori X och A, C och D till tjänsteleverantör Y.
  - Tjänsteleverantörens definierade lagrum.
  - En kombination av ovanstående två exempel.

Entitetskategorier för identitetsutgivare (IdP)

- Entitetskategorier för identitetsutgivare används oftast för att till tjänsteleverantörer signalera att utgivaren gör attributrelease enligt definierad entitetskategori för tjänsteleverantörer.
- Exempel:
  - Identitetsutgivare Z släpper attribut enligt definitionen för kategori X till de tjänsteleverantörer som har denna kategorimärkning i metadata.

Entitetskategori i metadata

- I SAML2 metadata är det möjligt att via en definierad utökning lägga till en eller flera entitetskategorier per leverantör eller utgivare.

```
<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>https://f.example.org/foo</AttributeValue>
      </Attribute>
      ... Fler entitetskategorier ...
    </EntityAttributes>
  </Extensions>
  ...
</EntityDescriptor>
```

REFEDS Research and Schoolarship (nyhet)

https://refeds.org/category/research-and-scholarship/

- Denna nya internationella entitetskategori är avsedd för tjänsteleverantörer som stödjer forskning och utbildning för alla eller en delmängd av federationens medlemmar.
- Rekommenderad attributrelease:
  - Namn, e-postadress, eduPersonPrincipalName, eduPersonTargetID och eduPersonScopedAffiliation.
- Använder entitetskategori för identitetsutgivare för att markera att utgivaren stödjer kategorin.

REFEDS Research and Schoolarship (nyhet), forts.

- Är i stort sett en internationaliserad version av inCommon Research and Schoolarship och SWAMID Research and Education.
- Ersätter på sikt SWAMID Research and Education för de flesta tjänsteleverantörerna.
- Fungerar i interfederationen eduGAIN vilket gör att internationella forsknings- och utbildnings-sammarbeten underlättas.

GÉANT Dataprotection Code of Conduct

http://www.geant.net/uri/dataprotection-code-of-conduct/v1

- Denna internationella entitetskategori är avsedd för tjänsteleverantörer inom EU och EES (eller finns i länder på EUs vita lista) som levererar forskningsresurser eller andra tjänster till universitets- och högskolesfären.
- Rekommenderad attributrelease:
  - Namn, e-postadress, eduPersonPrincipalName, eduPersonTargetID, eduPersonScopedAffiliation och schacHomeOrganisation.

GÉANT Dataprotection Code of Conduct

- Entitetskategorin tar särskild hänsyn till personuppgiftslagen och ställer särskilda krav på tjänsteleverantören.
- Fungerar i interfederationen eduGAIN vilket gör att internationella forsknings- och utbildnings-sammarbeten underlättas.
- Fungerar väl för kommersiella aktörer som levererar tjänster till utbildningssektorn i Sverige.

SWAMID SFS 1993:1153

http://www.swamid.se/category/sfs-1993-1153

- Denna identitetskategori finns endast inom och SWAMID och är avsedda för tjänster som uppfyller intentionen i Förordning (SFS 1993:1153) om redovisning av studier m.m. vid universitet och högskolor.
- Rekommenderad attributrelease:
  - Personnummer och eduPersonTargetID.
- Särskild prövning för att få entitetskategorin.

SWAMID Research and Education

- Denna identitetskategori finns endast inom och SWAMID och är avsedda för tjänster som stödjer utbildning och forskning. Används tillsammans med tre lagrumsentitetskatagorier.
- Ersätts på sikt av REFEDS Research and Schoolarship och GÉANT Dataprotection Code of Conduct.
- Rekommenderad attributrelease:
  - Namn, e-postadress, eduPersonPrincipalName, eduPersonTargetID, eduPersonScopedAffiliation och statisk organisationsinformation.

SWAMID Bas

- Detta är ingen egentlig entitetskategori utan en rekommendation om standardrelease till tjänster som inte har någon entitetskategori.
- Rekommenderad attributrelease:
  - eduPersonTargetID

Eventuellt kommande entitetskategorier

- Förnärvarande diskuteras det om att införa två nya internationella entitetskategorier inom REFEDS.
  - En entitetskategori för bibliotekstjänster som endast skickar över särskild markering om rätt att använda bibliotekstjänst samt eventuellt eduPersonTargetID och eduPersonScopedAffiliation.
  - En internationaliserad Code of Conduct för tjänsterleverantörer som inte finns inom EU, EES eller på EUs vita lista. Denna entitetskategori har högre juridisk risk för oss inom SWAMID.

För mer information

- SWAMID har en wikisida som formaliserat beskriver vilka entitetskategorier som används inom SWAMID.

  http://wiki.swamid.se/display/SWAMID/Entity+Categories