Entitetskategorier

Att göra attributrelease enklare och samtidigt mer integritetsskyddande

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

Definition

Attributrelease

Den information om användaren som skickas från en identitetsutgivare (*IdP*, Identity Provider) till en tjänsteleverantör (*SP*, Service Provider eller Relying Party) i samband med användarens inloggning.

Information som skickas kan vara person-, auktoriserings- och organisationsinformation.

Definition

Entitetkategori

En markering i metadata för tjänsteleverantör (*SP*, Service Provider eller Relying Party) eller identitetsutgivare (*IdP*, Identity Provider) som gör det möjligt för

- en IdP att göra ett automatiserat informerat beslut om attributrelease till SP eller
- en SP att veta om en IdP stödjer en viss kategori.

SWAMID använder endast första varianten idag.

Så varför entitetskategorier?

- Entitetskategorier används för att förenkla och förbättra hanteringen av personuppgifter.
- I SWAMID1 rekommenderades det att alltid släppa en basuppsättning personuppgifter till alla tjänster.
  - Enkelt men kanske lite väl enkelt ur ett integritetsperspetiv.
- I SWAMID2 rekommenderas det att en IdP släpper personuppgifter endast till de som uppfyller SWAMIDs regelverk och som har efterfrågat dem.

Aktuell status 2013-09-26

Identitetsutgivare som idag släpper attribut baserat på entitetskategorier:

- Antagning.se (NyA IdP)
- Högskolan i Jönköping
- Uppsala universitet
- fler?

Tjänsteleverantörer som är markerade med entitetskategorier finns på SWAMIDs Wiki.

- https://wiki.swamid.se/display/SWAMID/Service+Providers

Generell attributrelease

Alla tjänster som finns registrerade i SWAMID eller via interfederationer som SWAMID är medlem rekommenderas från identitets-utgivaren få en tjänsteunik identifierare för igenkänning vid återkommande inloggningar samt en sessionsunik identifierare.

Den tjänsteunika identifieraren används för att användaren ska kunna personalisera tjänsten för sina egna behov och är inte spårbar mellan olika tjänster.

SWAMIDs entitetskategorier
Research & Education

Kategorin används för tjänster vars syfte är att stödja forskning och utbildning vid svenska lärosäten.

En IdP förväntas släppa en basuppsättning med lågriskattribut: namn, epostadress, användarid med domändel, organisationsanknytning med domändel samt viss statisk organisationsinformation.

Attributrelease för denna kategori bör endast ske om tjänsten även är markerad med en personskyddskategori.

SWAMIDs entitetskategorier
Personskyddskategorier

HEI Service

Tjänsten finns vid universitet, högskola eller servicemyndighet för högskolan.

NREN Service

Tjänsten är en tjänst tillhandahållen av SUNET.

EU Adequate Protection

Tjänsten finns inom EU och EES eller i Schweiz eller annat land som har motsvarande personuppgiftslagstiftning som EU.

SWAMIDs entitetskategorier SFS 1993:1153

Kategorin används för tjänster uppfyller syftet i ”studiedokumentationsförordningen”.

Tjänster som kan få denna kategori är tjänster för

- studentkontohantering på lärosäten
- registrering på kurs eller program
- framstegsbaserade tjänster och
- VFU-portaler.

En IdP förväntas släppa personnummer, samordningsnummer eller NyAs interims personnummer.

GÉANT Dataprotection Code of Conduct

Kategorin används för tjänster som uppfyller EU Data Protection Directive.

En IdP förväntas släppa de attribut som krävs för att tjänsten ska fungera. De attribut med låg risk som kan släppas är namn, epostadress, användarid med domändel, organisationsanknytning med domändel samt hemmaorganisationens domännamn.

Kategorin är interfederativ och kräver att tjänsten uppfyller ett antal krav, t.ex. har en integritetspolicy.

Att få entitetskategorimarkering

För att en tjänst ska bli uppmärkt med en eller flera entitetskategorier genomgås följande process:

- Ansvarig för tjänsten ansöker till SWAMID Operations om att bli uppmärkt med en eller flera kategorier enligt de instruktioner som är publicerade.
- SWAMID Operations behandlar och beslutar.
- Vid positivt beslut märks tjänsten med aktuella kategorier.

Teknisk IdP-implementation

Shibboleth

- Använd Shibboleth 2.3.4 eller senare.
- Konfigurera attribute-filter.xml för att hantera entitetskategorier.

Microsoft ADFS2

- Använd kommande uppdaterade skriptet Femma.py med pysaml2, finns endast i test.
- Hör av er till Roland Hedberg för att testa.

Vilka attribut behövs för SWAMIDs entitetskategorier och CoC?

Personuppgifter

- eduPersonTargetedID
- eduPersonPrincipalName
- norEduPersonNIN
- email
- displayName
- givenName
- surname
- eduPersonScopedAffiliation

Organisationsuppgifter

- organizationName
- norEduOrgAcronym
- countryName
- friendlyCountryName
- schacHomeOrganization

transientId måste släppas till alla

Eventuell ny entitetskategori i SWAMID: Library Service

Denna kategori ska om beslut fattas användas för bibliotekstjänster eftersom användning av dessa är enligt lagstiftningen känslig ur ett integritetsperspektiv.

En IdP förväntas släppa en begränsad uppsättning med lågriskattribut: organisationsanknytning samt auktorisationsattribut med särskilt värde.

Attributrelease för denna kategori bör endast ske om tjänsten även är markerad med en personskyddskategori.

Till sist…

- Frågor?
  - Fråga oss nu…
  - Skicka epost till SWAMID Operations eller
  - ring någon i SWAMID Operations och fråga!
- Mer information på SWAMIDs Wiki:
  - Entity Categories
    - https://wiki.swamid.se/display/SWAMID/Entity+Categories
  - Example of a standard attribute filter for Shibboleth IdP
    - https://wiki.swamid.se/display/SWAMID/Example+of+a+standard+attribute+filter+for+Shibboleth+IdP

Nästa SWAMID Webinar

Att köra en identitetsutgivare under Windows Server

31 oktober kl. 10.00-11.00

https://connect.sunet.se/swamidwebinars/