
SWAMID
Swedish Academic Identity Federation

SWAMID

Ny best practice för attributrelease

SUNET

SWAMID

Bakgrund

- SWAMID var tidiga med villkorsstyrd automatiserad attributrelease genom entitetskategorier
- Vi behöver modernisera vår användning av entitetskategorier baserat på erfarenheter, onödig komplexitet och införande av internationella entitetskategoriramverk i eduGAIN
- Vi behöver göra en översyn med avseende på ny lagstiftning, dvs. GDPR med tillhörande svensk personuppgiftslagstiftning

SWAMID

Attributrelease och GDPR

- Entitetskategorier är en bra balansbräda eftersom de minimerar vilka attribut som överförs från identitetsutgivare och webbtjänst samtidigt som det går att göra automatiskt
- Webbtjänster måste i framtiden tillhanda en ”Privacy Policy” till användarna som beskriver vilka attribut de tar emot och använder och hur de på ett lättläst sätt uppfyller kraven i gällande personuppgiftslagstiftning

SWAMID

Vad är förändringen i SWAMID best practice?

- Entitetkategorin SWAMID Research and Education avvecklas tillsammans med sina tre hjälpkategorier
- Entitetskategorin SFS 1193:1153 avvecklas
- Entitetskategorin REFEDS Research and Scholarship uppdateras med ytterligare några få attribut
- Entitetskategorin Géant Code of Conduct uppdateras med ytterligare attribut som idag hanteras av de entitetskategorier som avvecklas

SWAMID

Attribut som överförs med REFEDS R&S

- eduPersonPrincipalName
- eduPersonUniqueID
  - Sätts till sammavärde som eduPersonPrincipalName endast om ePPN är unik och aldrig återtilldelas till annan användare
- eduPersonTargetedID
  - Endast om eduPersonPrincipalName ***inte*** är unikt och aldrig återanvänds till annan person
- displayName, givenName, sn (surname)
- mail
- eduPersonAssurance
- eduPersonScopedAffiliation

Attribut som kan överföras med Géant CoCo

- eduPersonTargetedID
- eduPersonPrincipalName
- eduPersonUniqueID
  - Samma begränsning som i R&S
- eduPersonOrcid
- norEduPersonNIN
  - Endast för tjänster i SWAMID
- personalIdentityNumber
  - Endast för tjänster i SWAMID
- schacDateOfBirth
- mail
- displayName, givenName, sn
- cn (commonName)
  - Måste innehålla för- och efternamn
- eduPersonAssurance
- eduPersonScopedAffiliation
- eduPersonAffiliation
- De statiska attributen o, norEduOrgAcronym, c, co, schacHomeOrganization och schacHomeOrganizationType

Med CoCo får endast attribut som begärs av webbtjänsten genom metadata överföras

SWAMID

SUNET

SWAMID

Personnummer, varför två attribut?

- norEduPersonNIN används som idag, dvs personnummer, samordningsnummer och studenters interimspersonnummer men begränsas till endast studierelaterade tjänster
- personalIdentityNumber får endast innehålla personnummer och samordningsnummer. Kan användas för alla tjänster såsom personalsystem och forskningsfinansiering

- Observera att SWAMID har i den nya best practice begränsat den rekommenderade användningen av personnummer till endast tjänster som är registrerade i SWAMID, inte i eduGAIN
- https://wiki.sunet.se/display/SWAMID/Svenska+personnummer%3A+norEduPersonNIN%2C+personalIdentityNumber+och+schacDateOfBirth

SUNET

SWAMID

Tidplan för införande av ny best practice

- Från och med nu får nya tjänster både de gamla och de nya entitetskategorierna
- Från och med 2020-05-01 får inga tjänster längre SWAMID R&E och SFS1993:1153 inlagda i metadata
- Från och med 2020-10-31 kommer metadata vara rensat från de avvecklade entitetskategorierna

SUNET

SWAMID

Praktisk information

Nu över till mer handfast och praktisk information

- Attributeresolver och attributfilter för Shibboleth
- Ny version av ADFStoolkit
- Nytt testverktyg för entitetskategorier

SUNET

Tack, frågor?

SWAMID

SWAMID

Swedish Academic Identity Federation

SWAMID Operations, operations@swamid.se
Pål Axelsson, pax@sunet.se – 070-4080175

SUNET