
SWAMID
Swedish Academic Identity Federation

SWAMID

Information om viktig förändring av SWAMIDs entitetskategorier

SWAMID Webinar 2 2020

SUNET

SWAMID

Bakgrund

- 2013 var SWAMID 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

Vad är attributrelease?

- I korthet överföring av personuppgifter i form av attribut från en identitetsutgivare (IdP) till en tjänsteleverantör (SP) i samband med att användaren loggar in i tjänsten med hjälp av identitetsutgivaren
- Personuppgifterna kan vara direkta såsom unika attribut för aktuell person (enskilt eller i kombination)
- Personuppgifter kan även vara indirekta såsom auktoriserings- och organisationsinformation (identifierar inte användaren)

SWAMID

Attributrelease och GDPR

- Entitetskategorier är en bra balansbräda eftersom de minimerar vilka attribut som överförs från identitetsutgivare till webbtjänst samtidigt som det går att göra ett skalbart automatiserat beslut
- 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 en entitetskategori?

- En markering i metadata för tjänsteleverantör (SP) som gör det möjligt för en identitetsutfärdare (IdP) att göra ett skalbart automatiserat informerat beslut om attributrelease till en tjänst
- Grunden för entitetskategorier är att minimera överföringen av attribut
- För varje entitetskategori finns ett beslutat regelverk som
  - avgör vilka tjänster som använda kategorin,
  - vilka attribut som ingår i entitetskategorin med ev. tilläggsregler och
  - ev. har ytterligare regler att ta hänsyn till

SWAMID

Vad är en entitetssupportkategori?

- En markering i metadata för identitetsutgivare (IdP) som informerar en tjänst (SP) att denna identitetsutfärdare har stöd för entitetskategorin
- En tjänst kan ev. filtrera sin hänvisningstjänst baserat på denna markering

Vad är förändringen i SWAMID?

- 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
  - Om formkraven uppfylls kan samma värde som eduPersonPrincipalName användas om ePPN är unik och aldrig kan ges till en annan användare
- eduPersonTargetedID
  - Endast om eduPersonPrincipalName ***inte*** är unikt och kan eventuellt återanvändas till en 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

OBS! Med CoCo får endast attribut som begärs av webbtjänsten i metadata överföras!

SWAMID

Personnummer, varför två attribut?

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

- Observera att SWAMID har förändringen begränsat den rekommenderade användningen av personnummer till endast tjänster som är registrerade direkt i SWAMID

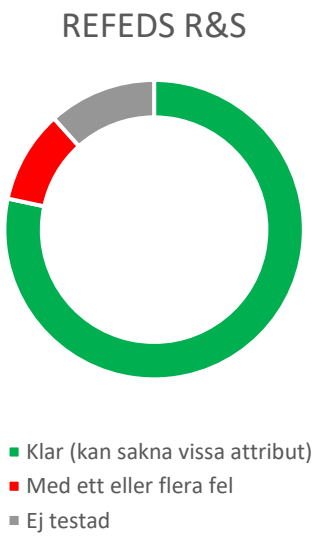
SWAMID

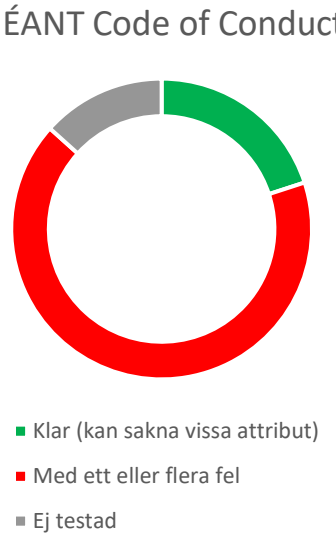
Tidplan för införande av förändringen

- Från och med 2019-10-23 får nya tjänster både de gamla och de nya entitetskategorierna
- Från och med 2020-09-01 ~~(var 2020-05-01)~~ får inga tjänster längre SWAMID R&E och SFS1993:1153 inlagda i metadata
  - Innebär att användare från och med nu gradvis kommer att få problem med att logga in i tjänster som de tidigare kunnat logga in i om identitetsutfärdaren inte ändrar sina attributfilter
- Från och med 2021-03-31 ~~(var 2020-10-31)~~ kommer metadata vara rensat från de avvecklade entitetskategorierna

SUNET

Status för identitetsutgivare 2020-09-16





REFEDS R&S

- eduPersonAssurance saknas ofta för de som är godkända för minst en tillitsprofil
- De som har ett eller flera fel saknar oftast de flesta attributen

GÉANT Code of Conduct

- eduPersonAssurance saknas ofta för de som är godkända för minst en tillitsprofil
- Många som har ett eller flera fel följer ännu den gamla modellen
- Personnummerattributen saknas ofta för de med fel

Shiiboleth Identity Provider

- SWAMIDs exempelfiler för resolver och filter för IdP 3.4.0 och nyare är uppdaterade med den förändrade modellen
  - https://wiki.sunet.se/display/SWAMID/Example+of+a+standard+attribute+resolver+for+Shibboleth+IdP+v3.4.0+and+above
  - https://wiki.sunet.se/display/SWAMID/Example+of+a+standard+attribute+filter+for+Shibboleth+IdP+v3.4.0+and+above
  - Attributresolvern behöver anpassas efter era datakällor
  - Attributresolver hanterar automatisk översättning från norEduPersonNin till personalIdentityNumber och schacDateOfBirth
- SWAMIDs exempelfiler för 3.3.x och tidigare är inte uppdaterade och ska därför inte användas

ADFS Toolkit

- Version 2.0 av ADFS Toolkit är ännu inte officiellt släppt med ADFS Toolkit 2.0 RC5 fungerar fullt ut på ett korrekt sätt
  - Orsaken till att version 2.0 ännu inte är släppt är att SWAMIDs motsvarighet i Kanada inte hunnit att genomföra sina anpassningar och tester fullt ut
- Att uppgradera från tidigare versioner av ADFS Toolkit kräver en del arbete men är väl värt arbetet eftersom i princip allt är genomgånget och ofta förändrat
- Presentationen från vårens webinar om ADFS Toolkit innehåller allt ni behöver veta om installation och uppgradering
  - https://wiki.sunet.se/display/SWAMID/SWAMID+Webinar+1+2020+-+ADFS+Toolkit+2.0

SWAMIDs testverktyg för entitetskategorier

- SWAMID har ett testverktyg för identitetsutfärdare där det är möjligt att kontrollera om man släpper attribut på rätt sätt
- Verktyget finns på adressen https://release-check.swamid.se/
- Totalt genomförs 6 deltester i sekvens och varje deltest visar detaljerat testresultat
  - Deltestrapporterna innehåller alla attribut som överfördes inkl. värden, attribut som förväntades men inte överfördes samt markerar attribut som inte skulle ha skickats
- Testet avslutas med en resultatsida som visar det sammanlagda resultatet av testerna utan att några attributvärden visas

Tack, frågor?

SWAMID

SWAMID

Swedish Academic Identity Federation

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

SUNET