
SWAMID
Swedish Academic Identity Federation

SWAMID

Effekterna i SWAMID av Dataskyddsförordningen

SWAMID Operations
Pål Axelsson, Sunet
Eskil Swahn, Lunds universitet

SUNET

SWAMID

Nuläge för personuppgifter i SWAMID

- SWAMID infrastruktur, dvs. metadata för identitetsutgivare och tjänster, innehåller endast personuppgifter i kontaktuppgifterna
- Federativ inloggning via SWAMID är baserad minimalitetsprincipen
  - Personuppgifter överförs endast när en användare loggar in i en tjänst och då endast direkt mellan identitetsutgivare och tjänst
  - Entitetskategorier gör så att en tjänst får tillgång till tillräcklig men inte för mycket information om användaren

Vilka områden är berörda?

- SWAMIDs metadata
- SWAMIDs tillitsprofiler
- Attributrelease från IdP till SP
  - Entitetskategorier och fristående attributrelease
- Rätten att bli glömd
- Loggning
- Incidenthantering

Dataskyddsförordningen (DSF) = GDPR

SWAMID

SWAMIDs metadata

- SWAMIDs metadata innehåller kontaktuppgifter till alla identitetsutgivare och tjänster som är registrerade i SWAMID
  - Administrativa, teknisk, support och säkerhet
- SWAMID rekommenderar starkt att det inte är personliga kontaktuppgifter som ligger i metadata utan funktionskontakter
  - Inte bara för personuppgiftshantering utan även för att säkerställa kontaktväg om personen är ledig, sjuk eller har slutat

SWAMIDs tillitsprofiler 1(2)

- SWAMIDs tillitsprofiler innehåller i sig inga personuppgifter
- SWAMID AL2 är garanten för tjänsteleverantörer att identitets-utgivarens organisation (lärosätet) gör saker på ett bra sätt
- Det är viktigt att identitetsutfärdaren har en integritetspolicy med information om hur denna hanterar personuppgifter inkl. attributrelease, användarens rättigheter och personuppgiftskontakt
  - Skriv inte integritetspolicy och användarregler i samma dokument eftersom ni kan bara upplysa användarna om integritetspolicyn men användarreglerna ska godkännas

SWAMIDs tillitsprofiler 2(2)

- För tjänster där det är viktigt att veta vem som loggar in i tjänsten är best practice att de endast tillåter användare med tillitsnivå SWAMID AL2, ev. i kombination med personverifierad multifaktor
  - Exempel på sådana tjänster är
    - där identifieringen av användaren sker direkt eller indirekt med hjälp av personnummer eller annan långsiktigt unik identifierare
    - i system med känsliga personuppgifter
    - i system med känslig forskningsdata
    - i system där det är viktigt att veta att rätt individ är inloggad

Entitetskategorier i SWAMID

- SWAMID kommer att begära att en tjänst ska påvisa med vilken laglig grund de hanterar personuppgifter som de får via entitetskategoribaserad attributrelease
- SWAMID inför ny best practice för automatiserad attributrelease
  - Entitetskategorierna SWAMID R&E och SWAMID SFS 1995:1153 avvecklas under ordnade former och ersättas med REFEDS R&S och GÉANT CoCo v2
  - GÉANT CoCo v2 är ännu ej klar utan nuvarande version med tillägg av incidenthanteringsprocessen SIRTFI används till den nya är klar
  - SWAMID Operations uppdaterar best practice för attribut filter

SWAMID

REFEDS Research & Schoolarship (R&S)

- Kan endast ges till tjänster som har till uppgift att stödja forskning och utbildning på universitets- och högskolenivå
- Minimal standarduppsättning attribut som ska släppas till en tjänst som bär entitetskategorin
  - Namn, unik identifierare, e-post och affiliering till organisationen
- Identitetsutfärdare måste visa i metadata att de stödjer entitetskategorin
  - Tjänster kan filtrera sin lista över aktuella identitetsutgivare på markeringen

SWAMID

GÉANT Code of Conduct (CoCo)

- Ny version anpassad till DSF utarbetas just nu inom eduGAIN tillsammans med jurister specialiserade på DSF
- Tjänsteleverantören måste uppfylla vissa krav
  - att visa genom en publik integritetspolicy med URL publicerad att de uppfyller DSF
  - att endast begära genom metadata de attribut som är nödvändiga för att tjänsten ska fungera
  - att hantera eventuella personuppgiftsincidenter genom incidenthanteringsrutinen SIRTFI (nytt i kommande CoCo v2)
- Identitetsutgivare måste visa stöd i metadata

SWAMID

Manuell attributrelease

- SWAMID kommer i best practice endast ha med exempel på manuell attributrelease till tjänster som många lärosäten använder där det finns särskilda behov av attributrelease som inte lätt hanteras av entitetskategorierna
  - Exempel: Sektorsgemensamma tjänster och Sunets tilläggstjänster

SUNET

SWAMID

Rätten att bli raderad *(eller rätten att bli glömd)*

- Tjänster ska inte spara personuppgifter om användare som inte längre använder tjänsten än vad som är nödvändigt
- En användare har alltid rätt att så långt som det är möjligt att manuellt bli borttagen ur en tjänst om inte särskilda skäl föreligger enligt DFS eller komplementlagstiftning

Observera: Glöm inte användarnas övriga rättigheter enligt DFS!

Loggning

SWAMID

- Logga inte mer än ni behöver för fel- och incidenthantering
- Spara inte loggarna längre än nödvändigt
  - Det finns ingen formell tidsgräns i lagstiftningen!
  - Rådgör med er personuppgiftsansvarig om lämplig tidsgräns
- SWAMIDs tillitsprofiler ställer krav på viss loggning som behöver finnas under hela användarkontots livstid
  - T.ex. information om hur och när personen är verifierad, byte av tillitsprofiler och när lösenord/multifaktor byttes eller spärrades

Incidenthantering

SWAMID

- I DSF finns krav runt hantering av personuppgiftsincidenter men detta är en utmaning i en identitetsfederativ värld
- I SWAMID används incidentshanteringsmodellen REFEDS SIRTFI för att möjliggöra kommunikation mellan tjänst och identitetsleverantör
- Både identitetsutgivare och tjänster indikerar att de arbetar enligt SIRTFI med en markering i metadata
  - Tjänster kan filtrera sin lista över aktuella identitetsutgivare på markeringen

Hur gör vi för att bli godkända för SIRTFI?

- Ni läser igenom och kontrollerar att ni uppfyller kraven för SIRTFI (https://refeds.org/sirtfi)
- Om ni anser att ni uppfyller kraven för SIRTFI informarerar ni SWAMID Operations
  - Inkl. organisationens IT-säkerhetsfunktions namn och e-postadress
- SWAMID Operations testar att e-postadressen fungerar

OBS! SWAMID Operations kommer inte att granska om ni uppfyller kraven eller inte, det är helt ert eget ansvar!

SWAMID

Swedish Academic Identity Federation

SWAMID