
SUNET

Identitetshantering vid Sunet

En allmän uppdatering vid

Sunetdagarna hösten 2019

Vetenskapsrådet

SWAMID – Tjänsteundersökningen

- Tjänsteundersökningarna för båda SWAMIDs delar, webbinloggning och eduroam, besvarades av drygt tio personer var
- SWAMID fick som helhet positiva resultat men det fanns några förslag på förbättringar
- Många saknar SWAMIDs workshopar som genomfördes flera gånger per år. Vi återupptar detta från och med idag och det kommer fler redan i början på nästa år.

SWAMID Operations
De som får SWAMID att fungera

- Anders Nilsson, Umeå Universitet
- Björn Mattsson, Blekinge Tekniska Högskola
- Einar Lönn, Sunet
- Eskil Swahn, Lunds Universitet
- Fredrik Domeij, Umeå Universitet
- Jan Johansson, Stockholms universitet
- Johan Peterson, Linköpings universitet
- Paul Scott, Karlstads Universitet
- Pål Axelsson, Sunet (produktägare SWAMID)
- Tommy Larsson, Umeå universitet

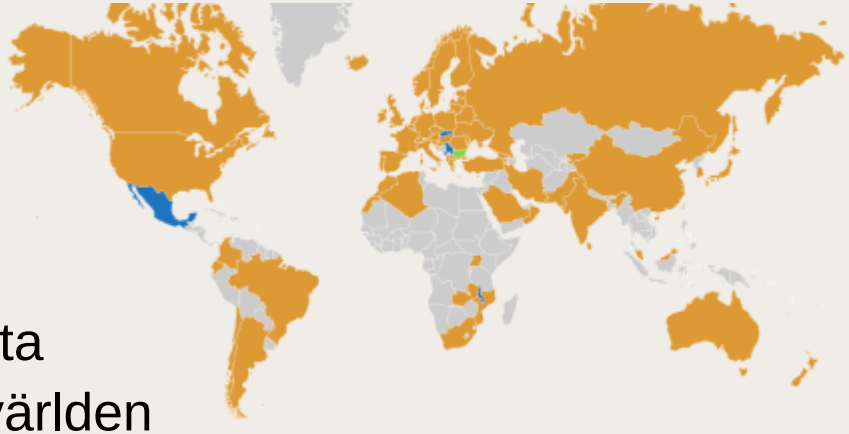
SWAMID Operations behöver utökas med minst en person som kan FreeRadius

SWAMID Board of Trustees
De som formellt bestämmer

- Valter Nordh, Sunet (ordförande)
- Fredrik Nilsson, Karolinska institutet
- Hans Wohlfarth, Kungliga Tekniska högskolan
- Jan Nordin, Högskolan i Gävle
- Magnus Höglund, Högskolan Dalarna
- Mauritz Danielsson, Ladokkonsortiet
- Per Zettervall, Universitets- och högskolerådet
- Per-OlovHammargren, SNIC
- Sverker Holmgren, Nationell delegat i European e-Infrastructure Reflection Group (e-IRG)

SWAMID – Webbinloggning via SAML

- För webbinloggning används idag en speciell dialekt för SAML som heter saml2int som används för multilaterala identitetsfederationer
  - Multilateral betyder att det finns många inloggningstjänster och många webbtjänster anslutna i federationen
  - saml2int reglerar hur metadata distribueras och hanteras
  - saml2int finns nu i ny version som ställer nya krav
- SAML-federationen innehåller runt 6000 entiteter i vårt metadata varav ca 2600 är identitetsutfärdare i 66 länder runt om i hela världen



Uppdatering av SWAMIDs policyramverk

- SWAMIDs nuvarande policy är från 2010 och har därför byggts på med nya delar i flera omgångar, senast under 2018 med nya MFA-profilen
- Policyöversynen består främst av fyra delar:
  1. Harmonisera med övriga akademiska identitetsfederationer
  2. Modernisering av godkända inloggningstekniker i tillitsprofilerna
  3. Översyn av godkända metoder för verifiering av användare
  4. Bygga om inloggningsprofilen för MFA med hög personverfiering till en ny tillitsprofil

Vad innebär policyöversynen för oss som redan idag använder SWAMID?

- De identitetsutfärdare som idag är godkända för SWAMID AL1, SWAMID AL2 och MFA-profilen ska fortsätta vara det även efter översynen
- De identitetsutfärdare som idag ***inte*** är godkända för någon tillitsprofil måste bli godkända för minst SWAMID AL1 inom av SWAMID Board of Trustees beslutad tidsram
- Alla användare som kan använda SWAMID måste minst uppfylla kraven för SWAMID AL1 enligt samma tidsplan som identitetsutgivarna
- Alla webbtjänster som använder SWAMID måste uppfylla vissa nya baskrav enligt nya saml2int men även beroende på GDPR

Programvaror för SAML-baserade identitetsutgivare

SWAMID Operations stödjer aktivt följande identitetsutgivare

- Shibboleth Identity Provider
  - Version 4 släpps under Q4 eller Q1 nästa år och alla kommer behöva uppdatera under 2020
- ADFS med specialprogramvaran ADFStoolkit
  - ADFS stödjer inte ”out of the box” multilaterala federationer utan behöver ”klister”

Ny best practice för attributrelease vid webbinloggning

- Förändrad användningen av entitetskategorier, mer information efter fikat…

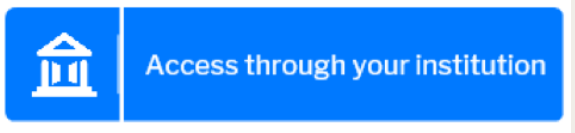
inAcademia – ny tjänst i eduGAIN som ni måste känna till

- inAcademia är ny internationell tjänst som syftar till att en användare på lärosäten ska säkert kunna visa att denna är student för en kommersiell tjänst
- Begränsade personuppgifter överförs från lärosätet till inAcademia för att göra valideringen och eventuellt tillse att en student endast kan ta del av ett erbjudande en gång
- Inga spårbara personuppgifter överförs från inAcademia till den kommersiella tjänsten
- Första organisationen som kommer att använda inAcademia är den svenska tjänste Mecenat för att ge svenska studenter tillgång till studentrabatter

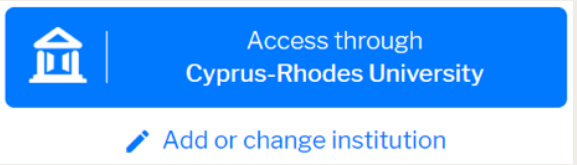
Seamless Access en ny smartare och bättre hänvisningstjänst

- Idag med flera tusen identitetsutfärdare har det blivit väldigt svårt att göra en bra hänvisningstjänst som är lätt förståelig
- De akademiska förlagens intresseorganisationer tillsammans med identitetsfederationerna skapade ett projekt för att hitta ett bättre sätt
- Projektet har nu kommit med rekommendationer som omsätts i praktiken i den nya hänvisningstjänsten SeamlessAccess.org
- För att använda hänvisningstjänsten SeamlessAccess.org lägger webbtjänsten in en särskild komponent på sin webbsida för att visa en smartare inloggningsknapp.
- Valet av identitetsutfärdare sparas i webbläsarens, inte i webbtjänsten eller hos SeamlessAccess.org

Första gången

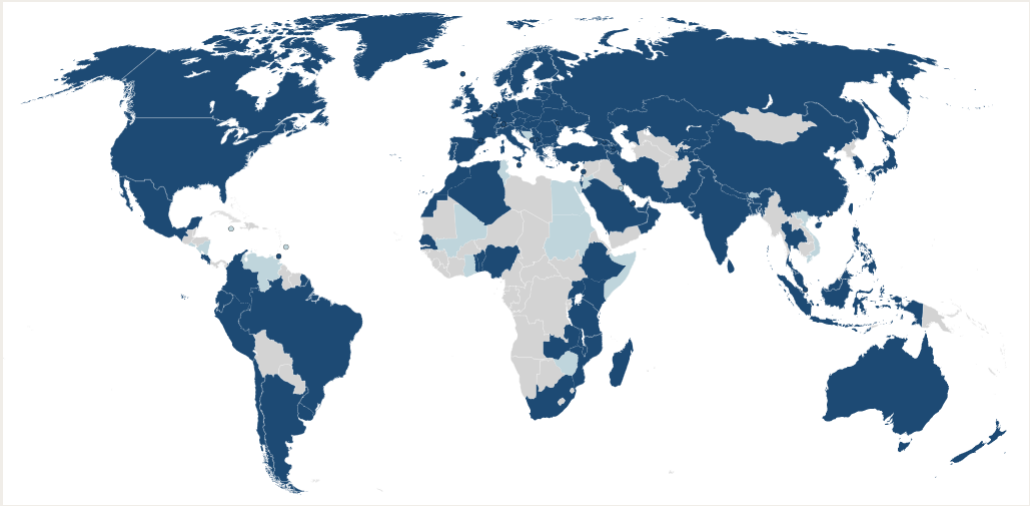


Därefter



SWAMID – Nätaccess via eduroam

- eduroam består av två delar
  - Det trådlösa nätverket med nätverksnamnet eduroam
  - Inloggning i det trådlösa nätverket eduroam
- eduroam finns idag i 101 länder runt om i världen



geteduroam

- geteduroam är ett projekt som syftar till att ge användare inom den akademiska sektorn tillgång till eduroam utan att lärosätet har en egen lokal inloggningsserver
- Användare loggar in på geteduroam med hjälp av sitt lärosäteskonto via SWAMIDs webbinloggning och ansöker om ett eduroam-konto
- Kan inte hantera lokala specialare såsom olika VLAN för besökare, anställda och studenter
- Klartecken från NORDUnets styrelse under NTW2019 i Köpenhamn.
- Läs mer på: https://events.nordu.net/plugins/servlet/conference-attachment/talks/689/1052

eduroam på järnvägsstationer och flygplatser

- Efter att Jernhusen sade upp avtalet med TheCloud tappade vi alla Jernhusen stationer (noteras kan att många järnvägsstationer inte länge ägs av jernhusen) då de sade upp sitt avtal med TheCloud och bytte till Telia.
- Vi har dock diskussioner med Jernhusen och det är inte helt omöjligt att vi kommer tillbaka dit.
- Parallellt pågår även diskussioner med Swedavia om framtiden där målet är att vi via ett direktavtal kan få till avtal med fasta kostnader.

Telia Passpoint

- Fortsatta samtal med Telia om Passpoint
- Fortsatt expansion av eduroam kräver dels att Sunet inte får fler kostnader samt att vi hittar metoder/mekanismer för att enklare nyttja befintliga nät där det inte finns plats för fler samtidiga SSID:n (trådlösa nät)

eduID

- Det nya grafiska gränssnittet som demonstrerades på förra Sunetdagarna har blivit försenat men arbete pågår

SWAMID IdP as a Service
En IdP för små organisationer

- SWAMID täcker idag 38 av 48 lärosäten som har rätt att utfärda examen enligt Högskolelagen
- De flesta av de små lärosätena är anslutna till Sunet och vill använda samma tjänster som övriga lärosäten
- Alla de små lärosätena har mindre än 250 studenter enligt Universitetskanslerämbetet
- De har inte resurserna att sätta upp och sköta sin egen identitetsutgivare
- Motsvarande gäller för väldigt små forskningsorganisationer

SWAMID IdP as a Service
En IdP för små organisationer

- Sunet har tagit fram en ny tjänst för dessa små organisationer som möjliggör åtkomst till webbinloggning via SWAMID
- Basen i tjänsten är eduID och dess användarkonton
- Ovanpå eduID finns en påbyggnad där den mindre organisationen kopplar sina studenters och anställdas eduID till organisationen
- I hänvisningstjänster väljer användare från dessa mindre organisationer sin egen organisation på samma sätt som alla andra
- IdP as a Service kommer att gå i pilotdrift med ett par organisationer senare i höst