SWAMID

Swedish Academic Identity Federation

Vad händer i SWAMID

2022-03-24

SWAMID

Välkomna till SWAMIDs förmiddag på Sunetdagarna våren 2022

9.00—9.45

- Vad händer i SWAMID under 2022
- Att som tjänst få användaruppgifter vid inloggning
  Uppdatera nu eller förlora vilka attribut din tjänst får tillgång till när en användare loggar in!
- SWAMIDs nya metadataverktyg

10.00—10.45

- ADFS Toolkit
  ADFS Toolkit gör ADFS som IdP till en första klass medborgare i SWAMID. ADFS Toolkit växer med nya möjligheter, till exempel multifaktorinloggning.

SWAMID

Vad händer 2022

- SWAMID beslutade i december 2021 en ny teknologiprofil för SAML WebSSO och den införs under 2022
- Alla tjänster måste se över och genomföra förändringar om hur de signalerar till identitetsutgivarna i SWAMID vilka attribut de behöver
- SWAMID fortsätter att utveckla ADFS Toolkit så att identitetsutgivare kan använda välja programvara enklare
- SWAMID kommer att anordna workshops där vi träffas och diskuterar olika frågor under året (om hälsoläget tillåter)

SWAMID

SWAMID Operations finns som ett stöd

- Om din organisation vill bli godkänd för en ny tillitsnivå eller planerar att börja använda multifaktorinloggning i SWAMID, ta kontakt med SWAMID Operations för att få stöd längs vägen
- Om din organisation vill börja använda ADFS som IdP ta kontakt med SWAMID Operations för vägledning, vi installerar inte men vi hjälper till med goda tips och idéer
- Om en tjänst funderar på hur de kan få bästa nytta av SWAMID ta kontakt med SWAMID Operations för vägledning
- SWAMID Operations nås på operations@swamid.se

SWAMID

Att som tjänst få användaruppgifter vid inloggning

SWAMID

SWAMID förändras

- SWAMID skapades för över femton år sedan och det har skett en kontinuerlig förändring som nu måste genomföras för alla
- För drygt tio år sedan var SWAMID först med att införa standardiserad attributrelease, nu har övriga federationer börjat komma i kapp och vi måste använda samma standarder
- SWAMID var från början en liten informell klubb som välkomnade alla men nu måste vi vara mer formella.
- Idag innehåller SWAMID 62 IdP och 713 SP och vi får från interfederationen eduGAIN ca 4700 IdP och ca 3500 SP

SWAMID

Krav för att en tjänst får finnas i SWAMID

Registreringskrav 1:

- att det är en tjänst ägd av en medlemsorganisation,
- att det är en tjänst som har ett avtal med minst en medlemsorganisation,
- att det är en tjänst som en myndighet tillhandahåller till minst en medlemsorganisation,
- att det är en tjänst som åtminstone delvis drivs i syfte att stödja forskning och utbildning, eller
- att det är en tjänst som fått särskilt tillstånd av SWAMID Board of Trustees.

Registreringskrav 2:

- att tjänsten accepterar SWAMID Metadata Terms of Access and Use.

SWAMID

Krav på information till användare

- Tjänsten måste publicera en publik webbsida som beskriver tjänsten inkl. hur användare får hjälp om de får problem
- Tjänsten måste publicera en publik webbsida som beskriver hur tjänsten behandlar personuppgifterna de tar emot från användarens inloggningstjänst (IdP)
  - SWAMID har publicerat en mall för hur en sådan ”privacy policy”: https://wiki.sunet.se/display/SWAMID/Service+Provider+Privacy+Policy+Template
- Länkarna till de bägge webbsidorna måste publiceras i metadata

SWAMID

Övriga krav för att få finnas som tjänst

- Tjänsten måste följa SWAMIDs incidenthanteringsprocess om en säkerhetsincident uppstår som berör användare som loggat in med hjälp av SWAMID
  https://wiki.sunet.se/display/SWAMID/SWAMID+Incident+Management+Procedures
- Tjänsten måste i metadata publicera administrativ och teknisk kontakt och bör publicera kontakter för support och incidenthantering
- Tjänsten måste vara korrekt registrerat i metadata enligt regelverket i SWAMID SAML WebSSO Technology Profile
  - Mer information alldeles strax

SWAMID

Att få tillgång till attribut

- I SWAMID används en modell som heter entitetskategorier för att informera identitetsutfärdarna (IdP) om vilka attribut en tjänst behöver till
- Med hjälp av entitetskategorierna kan en IdP fatta automatiserade eller manuella informerade beslut om att ge en tjänst tillgång till attribut
  - 5 av 62 IdP gör manuella informerade beslut, övriga automatiserade

SWAMID

Förändring av entitetskategorier

- SWAMID har tills nu haft en egen uppsättning av nationella entitetskategorier men kommer nu gå över till de som används inom eduGAIN
- Denna förändring ska vara slutförd till årsskiftet och det är bara tjänsterna som inte har genomfört övergången
- De två nya entitetskategorierna som används är
  - REFEDS Research and Scholarship
  - Géant Data Protection Code of Conduct
- Ta kontakt med SWAMID Operations för att få hjälp att välja

opserations@swamid.se

SWAMID

Att veta vem det som loggar in

- I SWAMID finns en gemensam trappstege på hur väl tjänsten kan veta att det är rätt användare som loggar in
- Alla medlemsorganisationer och deras IdP är godkända för minst en tillitsnivå: SWAMID AL1, SWAMID AL2 och SWAMID AL3
- Alla medlemsorganisationer kan informera om vilken nivå aktuell användare har och i metadata står det vilka nivåer organisationen är godkänd för
  - Alla organisationer informerar dock inte om detta ännu
- Inom eduGAIN finns motsvarande stege med andra namn som är direkt mappningsbara

SWAMID

Behöver tjänsten förstärkt inloggning

- Behovet av multifaktorinloggning (MFA) har det pratats om länge
- SWAMID har både stöd i policy och teknik för att begära att en inloggning måste ske med multifaktorinloggning
- Än så länge är väldigt få medlemsorganisationer som stödjer MFA via SWAMID och stödet kommer inte att öka förrän tjänster börja kräva det
- Sunets IdP eduID som är öppen för alla i sektorn har stöd för MFA vilket gör att samtliga användare kan genomföra inloggning med MFA men kanske inte från sin organisations IdP

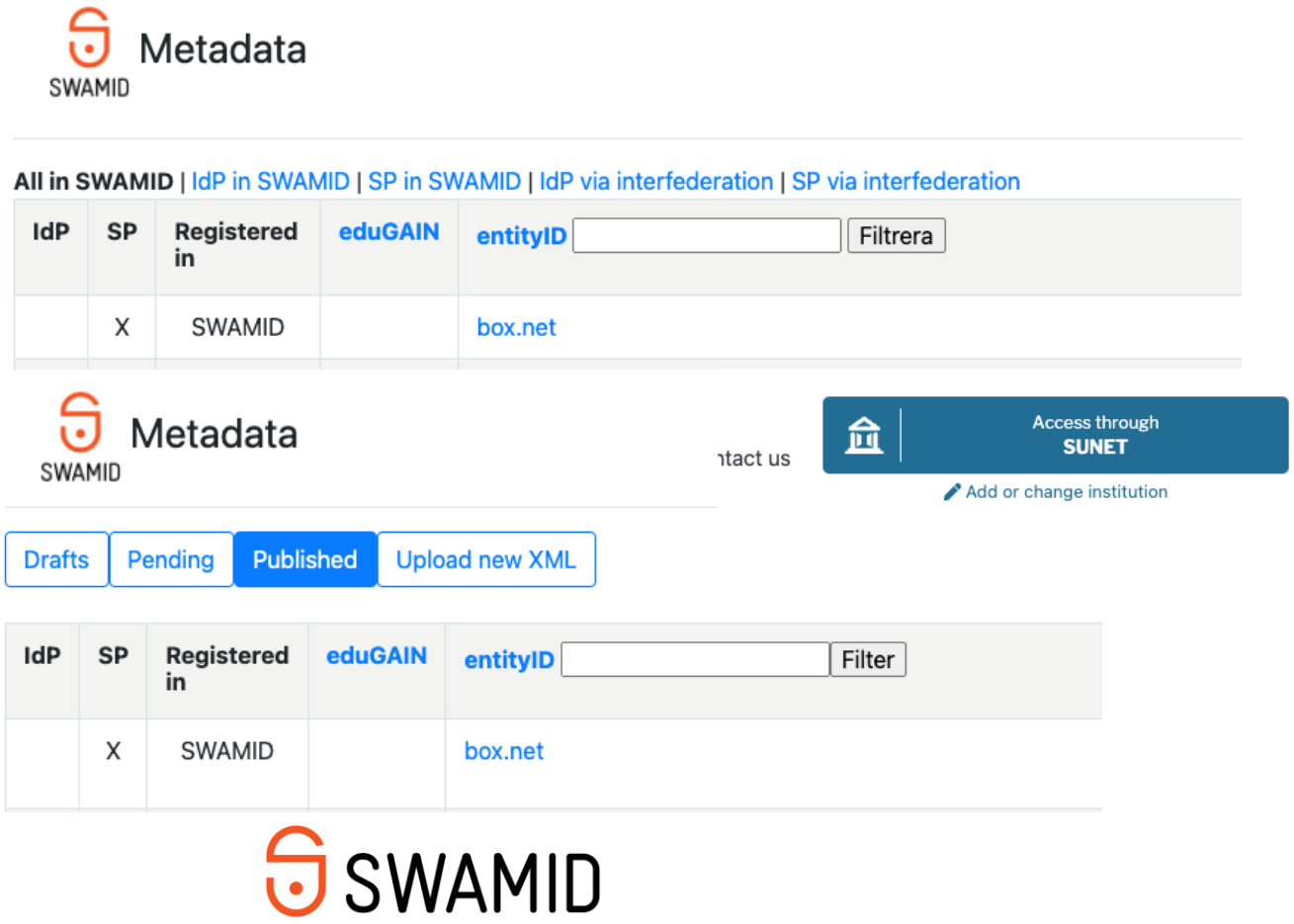
SWAMID

SWAMIDs nya metadataverktyg

SWAMID

View / Admin

- View
  - Alla kan se allt
  - Listar publicerade
  - Visar även eduGAIN
- Admin
  - Kräver inloggning
  - Möjlighet att redigera



SWAMID

Metadata.swamid.se

- Validerar emot
  - SWAMID SAML WebSSO Technology Profile
  - Felaktig SAML-XML
  - GÉANT CoCo (v1)
  - REFEDS R&S
- Övrig info
  - Länkar som är fel
  - Resultat från Release-check (om EntityCategorySupport saknas / felaktig)
  - Cert som är på väg att gå ut
  - Felaktiga FriendlyName

SWAMID

Metadata.swamid.se

- Visar vad som är fel / behöver uppdaterats / läggas till
  - Mindre mail mellan er och Operations
  - Snabbare hantering av era ärenden
  - Flagga upp cert som är på väg att gå ut / gått ut
- Mail (kommer under våren)
  - Cert som går ut / gått ut
  - Länkar som är fel
  - Dags att verifiera en entity

SWAMID

Metadata.swamid.se

- Enbart konton med affiliation employee kan logga in.
  - Fler krav har diskuterats men inte implementerats ännu.
- 3 nivåer
  - Warning – bra om ni fixar till
  - NonBreakning Error – Hindrar inte aktuell uppdateraing. Åtgärda snarast!
  - Error – MÅSTE åtgärdas innan vi accepterar uppdateringen

SWAMID

2022 är ett övergångsår!

- Entiteter med fel (Error) i metadata kommer efter årsskiftet 22/23 att avregistreras ur SWAMID
- Avregistrering sker en bit in i januari 2023 efter försök till en sista kontakt

SWAMID

Vad tyckte du om passet?
Svara på frågorna i pollen!

Obs. Har du en äldre version av din Zoom-klient kan du inte svara på pollen i Zoom.
Skriv i chatten om du vill dela med dig av dina tankar!

SWAMID

Tack för att ni kom och lyssnade!

Nu är det är det frågestund...