SWAMID Blog



Viktigt! Shibboleth IdP v4.3.1 End-of-Life 1 september 2024

Pål Mikael Axelsson posted on Feb 27, 2024

Inom SWAMID är det många organisationer som använder Shibboleth Identity Provider för organisationens SWAMID-kopplade identitetsutfärdare. Nu är det dags att uppgradera till en nyare huvudversion eftersom den tidigare huvudversionen går End-of-Life senare i år. Det är av säkerhetsskäl alltid viktigt att endast använda aktuella och underhållna versioner av programvara och detta är också ett krav i SWAMIDs teknologiprofiler. För er som använder Shibboleth Identity Provider finns det två sätt att hantera att näst senaste huvudversion blir End-of-Life, antingen genom att uppgradera till version 5, att byta till annan programvara än Shibboleth Identity Provider, t.ex. ADFS med ADFS Toolkit, eller att byta till Sunets nya tjänst eduID Connect[1] som lanseras senare i vår. Vilken väg ni än väljer så måste ni bli klara med detta absolut senast under november 2024 och genomför helst arbetet i god tid. Vi uppmanar er därför att aktivt delta på webinar och diskussionsmöten under våren.

Uppgraderingar av huvudversioner innebär alltid mer arbete än uppgradering inom samma huvudversion och det är därför särskilt viktigt att göra ett bra förberedelsearbete. SWAMID Operations kommer att ge er information om hur ni både förbereder och genomför uppgraderingen på ett bra sätt via webinar och öppna diskussionsmöten.

[1] eduID Connect är en avgiftsbelagd tjänst som använder eduID för användarkonton och ett administrativt gränssnitt för att koppla dessa till organisationen.

SWAMID finns som stöd i uppdateringen

För att underlätta arbetet med att uppdatera från äldre versioner kommer SWAMID Operations att genomföra två olika arrangemang, dels ett inledande webinar som beskriver uppdateringsprocessen och därefter öppna mötestillfällen varannan vecka under våren där vi hjälper varandra i uppdateringsprocessen. Detta betyder att vi inte kommer att ha något hackaton där alla gör jobbet på plats. Orsaken till detta är att vi alla har olika förutsättningar och är på olika plats i uppgraderingsprocessen redan nu.

Webinar om uppgradering till Shibboleth IdP v5

Syfte	Shibboleth Identity Provider version 4.3.1 går End-of-Life i början av september i år. För att uppgraderingsprocessen ska gå så smidigt som möjligt bjuder SWAMID Operations in till ett webinar där vi beskriver de olika stegen samt vad man behöver tänka på.
Målgrupp	Detta webinar vänder sig till er som är tekniskt ansvariga för Shibboleth-baserade identitetsutfärdare, eller kommer att genomföra uppgraderingen, vid SWAMIDs medlemsorganisationer.
Datum & tid	10.00 – 11.00 torsdagen den 11 april, Zoom-länk: https://sunet.zoom.us/j/67204746559?pwd=T3VJNlQwOG9xYkRBeFFLQ0lYL1dRQT09
Talare	Paul Scott

Öppna diskussionsmöten om frågor som dyker upp på vägen

Syfte	Som uppföljning till webinariet om uppgradering av Shibboleth Shibboleth Identity Provider version 4.3.1 bjuder SWAMID Operations till ett antal öppna möten där det är möjligt att få hjälp av SWAMID Operations och andra som genomför uppgraderingen.
Målgrupp	Dessa öppna möten vänder sig till er som är tekniskt ansvariga för Shibboleth-baserade identitetsutfärdare, eller kommer att genomföra uppgradering, vid SWAMIDs medlemsorganisationer.
Datum & tid	9.00 – 10.00 torsdagarna den 18 april, 2 maj, 16 maj, 30 maj och 13 juni, Zoom-länk: https://sunet.zoom.us/j/67204746559?pwd=T3VJNlQwOG9xYkRBeFFLQ0lYL1dRQT09

Vad händer om vi inte uppgraderar i tid?

I SWAMID teknologiprofil för SAML2 WebSSO under avsnitt 5.4 finns kraven på den federativa programvaran för identitetsutfärdare beskriven och krav 5.4.11 definierar att medlemsorganisationer ej får använda programvara som inte längre underhålls eller innehåller kända säkerhetsproblem. Detta innebär att alla som idag använder Shibboleth IdP version 4 eller tidigare måste uppdatera innan 1 september 2024. Om inte uppdatering genomförs i god ordning kommer SWAMID Operations att föreslå SWAMID Board of Trustees att fatta beslut om att organisationens identitetsutfärdare avregistreras från SWAMID 2024-12-01. Detta kommer innebära, efter beslut har fattats, att organisationens användare inte kommer att kunna logga in i tjänster anslutna till SWAMID förrän uppgraderingen är gjord. Denna process beskrivs kortfattat i SWAMIDs policy under avsnitt 6.3.

Viktigt om uppdateringsprocessen

Om ni inte redan använder Shibboleth 4.3.1 uppdatera till denna version! Detta för att både få rätt konfiguration och rätt varningsmeddelanden i loggar. Samma metod för uppdatering ska användas som nedan. Observera att varningsmeddelandet om stödet för eduPersonTargetId är felaktigt skrivet och är i avvecklat i version 5.

Shibboleth Consortium beskriver i release-notes för IdP v5, ReleaseNotes - Identity Provider 5, att befintliga konfigurationsfiler bara kan användas om uppgraderingen görs i befintlig installation. Följ anvisningarna och installera inte den nya versionen separat för att därefter försöka använda de gamla konfigurationsfilerna. IdP:n behöver istället uppgraderas "på plats" genom att använda en installationskatalog som innehåller en kopia av en tidigare fungerande konfiguration av V4.3.1.

Vidare skriver de att plugins behöver uppdateras innan själva IdP:n uppgraderas och att plugins också ska uppdateras efteråt. Detta eftersom stora interna förändringar skett mellan v4 och v5. Uppgradera och testa alla plugins innan IdP-uppgraderingen påbörjas, och uppdatera åter alla plugins efter IdP-uppgraderingen slutförts, innan IdP:n startas. Installationsprogrammet varnar om detta och rapporterar vilka plugins som behöver en uppdatering.

SWAMID Operations
Pål Axelsson och Paul Scott


Avveckling av SWAMIDs testfederation
Pål Mikael Axelsson posted on Nov 06, 2023
På Sunetdagarna nu i höst informerade vi om att SWAMIDs gamla testfederation kommer att avvecklas och ersättas av SWAMIDs QA-federation. QA-federationen finns på plats redan idag med samma uppsättnings verktyg som i SWAMIDs produktionsfederation.

SWAMIDs testfederation kommer att stängas av vid halvårsskiftet 2024. Nyregistreringar i SWAMIDs testfederation är inte längre tillåtna!

Adresser till verktyg i SWAMIDs QA-miljö:

- Metadataverktyget: https://metadata.qa.swamid.se/
- Metadata via MDQ (nya modellen): https://mds.swamid.se/qa/
- Metadata via aggregat (gamla modellen): https://mds.swamid.se/qa/md/
- Hänvisningstjänst: https://ds.qa.swamid.se/ds
- Release-check: https://release-check.qa.swamid.se/.

SWAMIDs alla instruktioner för både identitetsutfärdare och tjänster går att använda men ni behöver byta aktuella URLar enligt ovan i konfigurationsfilerna.

Mer och aktuell information publiceras på wikisidan QA for SWAMID SAML WebSSO.

Pål Axelsson


Annual check of metadata for Identity Providers and Service Providers registered in SWAMID
Pål Mikael Axelsson posted on Nov 01, 2023

In SWAMID's SAML WebSSO Technology Profile Section 3 on Compliance and Audit, there is a requirement that all registered Identity Providers and Service Providers must annually validate that the registered entity is still operational, and that the metadata is correct.

In order to facilitate compliance with the annual inspection requirement, SWAMID Operations will send out a reminder to all Identity Providers and Service Providers. If the Identity Providers and Service Providers representative does not access SWAMID's metadata tool within a reasonable time after reminders and annual confirm the entity, the entity in question will be deregistered from SWAMID until this process is completed. We will send out the reminder to administrative and technical contacts in metadata. Check that these contact details for all yours all Identity Providers and Service Providers are correct via https://metadata.swamid.se and if not correct, update as soon as possible.

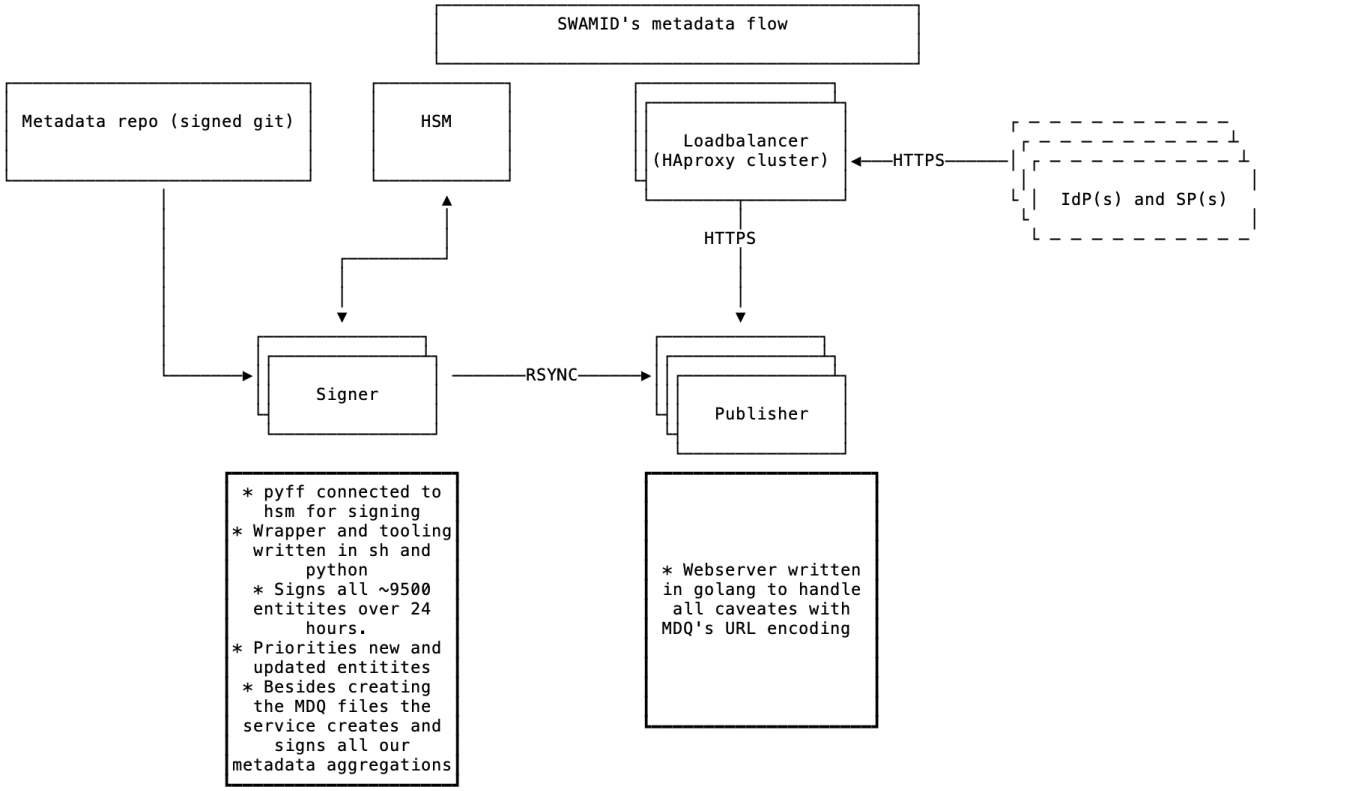
It is possible in advance to enter https://metadata.swamid.se/admin and carry out the annual check for your registered entities by searching for the respective entity, opening the detail view, and click on the "Annual Confirmation" button.

SWAMID Operations
Pål Axelsson


MDQ in SWAMID
Johan Rikard Wassberg posted on Sep 11, 2023
Since 2016 SWAMIDs metadata has been signed with a key in a HSM. This has been fine since we previously only were creating a handful of metadata aggregation files (of different sizes). The problem with the aggregated feeds is that it takes time and memory(!) to load an in SWAMID's case 80 MB XML file in to the Identity Providers and Service Providers. Had a conversation recently with a new SP in our federation. They guessed that `shibd` crashed on start since it appeared to just hang - told them to take a deep breath and relax.

One solution for this memory and size problem isto start using the MDQ Protocol instead of big aggregated files. By using the MDQ protocol the SPs and IdPs don't need to load the whole federation. Instead they loads requested entities on the fly. So if both an IdP and an SP uses MDQ the SP will first fetch the IdPs metadata from the MDQ server and then redirect for login. The IdP will then fetch the SPs metadata from the MDQ server, prompt for authentication and then redirect the user back to the SP. Pretty easy flow but it requires the MDQ server to be fast and always available!

Our software of choice, pyFF, can act as a MDQ server and serve signed metadata files on request. But connecting pyFF to the HSM makes the signing too slow and would in a case of many requests in a short time create a heavy load on our HSM servers, which we would like to avoid. pyFF can be run in batch mode which will sign all entities and output them to disk (e.g for mirroring) but that would still require us to sign around 9500 entities each run which once again would put our HSMs at risk. Another factor why we chose the design we ended up with is that we would like to protect the machines (signers) connected to the HSM from the internet.



So what we came up with is tools and wrappers around pyFF which fetches SWAMIDs and eduGAINs metadata (a total of around 9500 entities), splits them up in parts, and signs all entities over the current day. That's around 400 per hour and we run it 4 times an hour via cron. This creates a reasonable load on the HSMs. We prioritises new, updated or removed entities which are usably published 15 minutes after we detect a change. The tooling is based on a `python` script we call mdqp which have som pre and post scripts written in `sh`.
The basic flow looks like:

- Metadata is fetched from git (a signed commit is verified) and eduGAIN
- pyFF reloads the metadata
- The given amount of entities (new, updated or removed prioritised) are fetched from pyFF via `mdqp`
- Our aggregated feeds are fetched from pyFF
- All signed entities and files are rsynced to the publishers (web servers)

There are two ways of getting an entity through the MDQ protocol:

- Getting them by entitiyId, e.g /entities/https://connect.eduid.se/sunet
- Getting them by the sha1sum of the entityid, e.g entities/{sha1}47918903a357c193bcd985a23c5958a8a43278c0

Both methods should be url encoded which makes things complicated. "Regular" webservers (e.g apache2 or nginx) decodes an incoming encoded url string before processing the request which would make it impossible for us to store the first alternative on disk (contains slashes). We also would like to support both alternative with the same file on disk so for that purpose we ended up writing ourself a very small and simple web server in golang which will serve our very niche set of requirements.

The web servers themselves are *protected* by a geo distributed cluster of HAProxy to even out the load and terminating TLS.

Happy MDQing.

See our wiki for more information about getting started with MDQ in SWAMID.

--
jocar

SWAMID Operations

- techblog



Tack för 2022 och välkomna till 2023

Pål Mikael Axelsson posted on Feb 01, 2023

2022 har varit ett mycket arbetsintensivt år för oss som jobbar med policy och infrastruktur runt SWAMID men även för er alla som har identitetsutfärdare och tjänster registrerade i SWAMID. Med blogginlägg vill jag tacka er alla för året som gått och allt det arbete ni har lagt ner under både under 2022 och de 15 år som SWAMID funnits.

Under perioden 2019 till 2021 genomförde SWAMID en omfattande uppdatering och förtydligande av SWAMIDs policyramverk vilket gör att vi står på en stabil bas inför framtiden. Den sista delen av policyramverket som uppdaterades under 2021 var SWAMID SAMLS WebSSO Technology Profile och under 2022 har den nya versionen införts. Införandet har inneburit mycket jobb för oss alla men nu är metadata i SWAMID mycket mer korrekt och komplett. För att allt detta arbete skulle vara möjligt tog SWAMID Operations fram ett helt nytt metadataverktyg (https://metadata.swamid.se) som driftsattes i januari och har förbättrats under året. Detta verktyg kommer att fortsättas att utvecklas och vi är alltid intresserad av både buggrapporter och förslag på förbättringar. I mitten av januari 2023 avslutades metadataöversynen och de 45 registrerade tjänster som då ännu inte har åtgärdat kvarvarande brister avregistrerades från SWAMID.

För inloggning i tjänster ska fungera måste identitetsutfärdarna skicka person- och organisationsuppgifter till tjänsterna i samband med inloggning. Inom SWAMID kallar vi detta attributöverföring och för att underlätta denna på ett GDPR-vänligare sätt används något som kallas entitetskategorier. Entitetskategorier är en markering i metadata med kringliggande regelverk som dels definierar vilka tjänster som har rätt under definierade villkor att använda den specifika entitetskategorin och dels vilka attribut som ska överföras. Under 2022 avvecklades SWAMID:s tio år gamla entitetskategorier till fördel för en uppsättning internationellt överenskomna entitetskategorier. Jag vill särskilt tacka alla administratörer av identitetsutfärdare som har jobbat med att under de senast tre månaderna införa stöd för fyra nya entitetskategorier som har som mål att inte leverera mer person- och organisationsuppgifter till tjänsten än vad den behöver för att användaren ska kunna använda den, dvs. dataminimaliserande och integritetsbevarande attributöverföring. Samtidigt har vi höjt tilltron till federativ inloggning eftersom Ladok men även forskartjänster har börjat kräva att tillitsnivå, dvs. hur väl man vet att det är rätt användare, signaleras till tjänsten vid inloggning. Alla identitetsutfärdare har ännu inte genomfört dessa förändringar runt attributöverföring men vi hoppas att så många som möjligt gör det så snart som möjligt så att alla anställda och studenter kan logga in i de tjänster de behöver för att genomföra sitt arbete resp. studier. För att testa och verifiera attributöverföringen med hjälp av entitetskategorier har SWAMID verktyget SWAMID Best Practice Attribute Release check (https://release-check.swamid.se/).

Detta om 2022, vad kommer att hända under 2023? Under 2023 kommer SWAMID inte att införa några nya krav eller regler utan att fortsätta stödja införandet av de nya entitetskategorierna och jobba med inte tvingande förändringar för att förbättra användningen av SWAMID. Vi vet att vissa forskartjänster kommer under året införa krav på multifaktorinloggning och därför kommer vi under våren att anordna traditionella fysiska workshops eller hackatons runt installation och konfiguration av multifaktorinloggning i identitetsutfärdare. Avsikten med dessa workshops är att hjälpa alla organisationer som vill kunna erbjuda multifaktorinloggning med hur man konfigurerar sin identitetsutfärdare. Vidare kommer vi att fortsätta att modernisera SWAMIDs infrastruktur genom att bland annat erbjuda nya förbättrade modeller för att hämta metadata. Nuvarande modell för att hämta metadata kommer att finnas kvar så att denna förändring inte är tvingande utan bara förbättrande.

Den tekniska miljön runt federativ inloggning håller på att förändras och SWAMID Operations bevakar detta aktivt. Dels har det kommit nya federativa tekniker såsom OpenID Connect Federation och digitala identitetsplånböcker, dels håller leverantörerna av webbläsare på att göra dem mer integritetsbevarande. Bägge dessa förändringar kommer att ge effekter på sikt och vi jobbar aktivt med att se var vi är på väg och vad vi behöver göra för att federativ inloggning kommer att fortsätta att fungera. Vi återkommer med mer information under årets gång.

Med vänliga hälsningar
SWAMID Operations genom
Pål Axelsson



Nya entitetskategorier och signalera tillitsnivåer till tjänster

Pål Mikael Axelsson posted on Nov 13, 2022

För knappt en månad sedan den 20 oktober presenterade SWAMID på Sunetdagarna att vi inför fyra nya GDPR-vänliga entitetskategorier. En av dessa nya entitetskategorier ersätter SWAMIDs gamla entitetskategori SWAMID Research and Education för alla tjänster som idag har den. Eftersom de gamla entitetskategorin kommer att fullständigt avvecklas vid årsskiftet rekommenderar vi alla identitetsutfärdare att införa stöd så fort som möjligt för de nya entitetskategorierna.

Följande är de nya entitetskategorierna:

- **REFEDS Anonymous Access Entity Category** - Kategorin avser tjänster som erbjuder en servicenivå baserad endast på bevis på framgångsrik autentisering samt vissa organisationsattribut, möjliggör ingen personifiering baserat på en användaridentifierare.
- **REFEDS Pseudonymous Access Entity Category** - Kategorin avser tjänster som erbjuder en servicenivå baserad på bevis på framgångsrik autentisering samt möjliggör personifiering baserat på en pseudonym användaridentifierare.
- **REFEDS Personalized Access Entity Category** - Kategorin avser tjänster som erbjuder en servicenivå baserad på bevis på framgångsrik autentisering samt möjliggör personifiering baserat på en organisationsunik användaridentifierare, namn och e-postadress, ersätter SWAMID Research and Education.
- **REFEDS Data Protection Code of Conduct Entity Category (CoCov2)** - Kategorin avser tjänster som antingen inte uppfyller kraven för övriga kategorier eller har behov andra attribut, t.ex. personnummer, än de som erbjuds i övriga kategorier, ersätter på lång sikt CoCov1 men bägge behöver stödjas parallellt.

Följande är de gamla entitetskategorierna som behålls:

- **REFEDS Research and Scholarship Entity Category (R&S)** - Kategorin avser tjänster som direkt stödjer forskning och utbildning baserad på bevis på framgångsrik autentisering samt möjliggör personifiering baserat på en organisationsunik användaridentifierare, namn och e-postadress.
- **Géant Data Protection Code of Conduct Entity Category (CoCov1)** - Kategorin avser tjänster som antingen inte uppfyller kraven för övriga kategorier eller har behov andra attribut, t.ex. personnummer, än de som erbjuds i övriga kategorier, ersätts på lång sikt CoCov2 så bägge behöver stödjas parallellt.

- **European Student Identifier Entity Category (ESI)** – Kategorin avser tjänster som har behov av European Student Identifier, t.ex. tjänster runt Erasmus+.

Följande är de gamla entitetskategorierna som slutligen avvecklas:

- **SWAMID Research and Education** - Ersätts av både Personalized Access och R&S beroende på vilken typ av tjänst det är. Även CoCov2 och CoCov1 används som ersättare i vissa fall.
- **SWAMID SFS 1993:1153** - Ersätts av CoCov2 och CoCov1.

Som ni ser så hör REFEDS tre nya entitetskategorier Anonymous Access, Pseudonymous Access och Personalized Access ihop i en hierarki. De tjänster som endast behöver veta att en användare tillhör en viss organisation använder Anonymous Access, de tjänster som vill kunna ge användaren en mer personifierad åtkomst men utan behov av namn och e-postuppgifter använder Pseudonymous Access och till sist de tjänster som behöver full personalisering använder Personalized Access. Denna hierarki gör att tjänster inte behöver begära mer information än de behöver för att leverera tjänsten till användarna, s.k. dataminimalisering runt personuppgifter. SWAMIDs standardmallar för både Shibboleth och ADFS tar hänsyn till minimeringen på så sätt att om en tjänst begär mer än en av dessa tre får tjänsten attribut baserat på den som är mest dataminimerande, dvs. begärs både Anonymous Access och Pseudonymous Access används den förstnämnda.

För er som använder ADFS Toolkit finns nu en ny version 2.2.0 som har stöd för både de nya entitetskategorierna samt de nya identitetsattributen som krävs. Ni hämtar senaste versionen på adressen https://www.powershellgallery.com/packages/ADFSToolkit/. Praktisk information finns i sunetdagarpresentationen 11-11.45 den 20 oktober.

För er som använder Shibboleth IdP finns detaljer om hur ni kommer i gång med de nya entitetskategorierna även de i sunetdagarpresentationen 11-11.45 den 20 oktober. Självklart innehåller även standardmallarna för Shibboleth på SWAMIDs wikisidor denna konfiguration.

Att signalera tillit

Som alla lärosäten vet börjar Ladok kräva att de personer som har tillgång till modulen nationell översikt uppfyller kraven för SWAMID AL2 från och med kommande årsskifte. Förutom att alla aktuella användarnas måste valideras för SWAMDI AL2 enligt de metoder som ni är godkända för måste identitetsutfärdaren även signalera godkända tillitsnivåer till Ladok och andra tjänster. Ladok kommer att från och med sommaren kräva SWAMID AL2 för alla anställda som loggar in i Ladok från och med halvårsskiftet 2023. Om ni inte är godkända för SWAMID AL2 eller om ni inte signalerar SWAMID AL2 för de användare som uppfyller kraven kommer de inte kunna logga in i Ladok. Aktuell status för vilka som är godkända för SWAMID AL2 finns i medlemslistan på SWAMIDs wiki, https://wiki.sunet.se/display/SWAMID/SWAMID+Members. De lärosäten som ännu inte är godkända för SWAMID AL2 arbetar för fullt med att bli det.

Från och med i januari kommer även EuroHPC-datorn Lumi via identitetsinfrastrukturerna MyAccessId och Puhuri börja kräva tillitssignalering via REFEDS Assurance Framework (RAF). SWAMID tillitsramverk uppfyller kraven i RAF och det är enkelt att signalera RAF baserat användarens tillitsprofiler. Även detta finns stöd för i standardmallarna för både Shibboleth och ADFS. Tänk på att de flesta lärosätena och andra forskningsorganisationer i Sverige har minst en användare eller forskningsgrupp som är beroende av att kunna använda Lumi inom ramen för sin forskning.

För att få veta mer om förändringarna runt entitetskategorier och att signalera tillitsnivåer kan ni ta del av presentationerna från den 20 oktober på Sunetdagarnas wikisida https://wiki.sunet.se/x/yJyvBg. Om ni som identitetsutfärdare behöver mer information eller lite hjälp hör av till SWAMID Operations, operations@swamid.se.

Så i korthet behöver ni göra följande före julledigheterna:

- **Aktivera stöd för de nya entitetskategorierna i era identitetsutfärdare**
- **Konfigurera så att ni kan släppa både SWAMIDs tillitsprofiler och REFEDS Assurance Framework till de tjänster som behöver det**
- **Testa attributreleasen i SWAMIDs testverktyg https://release-check.swamid.se**
- **När ni får grönt på attributreleasen gå in på https://metadata.swamid.se/admin och uppdatera vilka entitetskategorierna ni stödjer i er identitetsutfärdare**


Årlig kontroll av att en identitetsutfärdare fortfarande uppfyller godkänd tillitsnivå
Pål Mikael Axelsson posted on Jan 23, 2022
Efter 10 år har nu alla utom två av SWAMIDs medlemsorganisationer blivit godkända för en eller flera tillitsprofiler. De som ännu inte är godkända måste bli det i samband med årets första möte med SWAMID Board of Trustees i början på mars, annars kommer de att stängas av från SWAMID.

I tillitsprofilernas avsnitt 3 om efterlevnad och revision står det att en medlemsorganisation årligen ska bekräfta att det som står i organisationens identitetsutgivares (IdP) Identity Management Practice Statement (IMPS) fortfarande stämmer. Det står vidare att medlemsorganisationen måste uppdatera och skicka in IMPS för godkännande innan ändringar. Den uppdaterade IMPS:en måste vara godkänd av SWAMID Board of Trustees innan ändringar genomförs i organisationens IdP och underliggande system. Från och med 2022 kommer SWAMID Operations aktivt begära att medlemsorganisationerna rapporterar enligt dessa krav.

För att underlätta uppfyllelsen av kravet kommer SWAMID Operations att skicka ut en påminnelse till alla medlemsorganisationer under året med en kopia av den IMPS som senast har blivit godkänd av SWAMID Board of Trustees. Om inte medlemsorganisationen inom rimlig tid och efter påminnelser besvarar denna begäran kommer aktuella identitetsutgivare avregistreras från SWAMID tills denna process har genomgåtts. Vi kommer att skicka ut påminnelsen till administrativa och tekniska kontakter i metadata. Kontrollera att dessa kontaktuppgifter för identitetsutfärdaren stämmer via https://metadata.swamid.se och uppdatera snarast om de inte stämmer.

SWAMID Operations
Pål Axelsson

 Vad händer i SWAMID under 2022
Pål Mikael Axelsson posted on Jan 17, 2022
I vår strävan att få SWAMID att fungera bättre och säkrare fastställde SWAMID Board of Trustees (BoT) i december den uppdaterade teknologiprofilen för SAML WebSSO efter konsultarationen som pågick mellan oktober och november 2021. Vid BoT-mötet beslutades även att alla idag registrerade entiteter (identitetsutfärdare och tjänster) i SWAMID ska ha fram till årsskiftet 2022/2023 på sig att åtgärda eventuella felaktigheter i metadata som identifierats baserat på den uppdaterad teknologiprofilen. De som inte åtgärdar felaktigheterna innan årsskiftet kommer att avregistreras från SWAMIDs metadata under januari 2023. Under denna övergångsperiod avvecklas också SWAMIDs gamla entitetskategorier SWAMID Research & Education och SWAMID SFS 1993:1153.

För att underlätta arbetet med att åtgärda felaktigheterna i metadata samt att generellt förenkla metadataadministrationen har SWAMID Operations tagit fram ett verktyg för självadministration av metadata. Det nya verktyget ska alltid användas, från och med januari 2022, vid registrering och uppdatering av metadata i SWAMID. Det nya självserviceverktyget är tillgängligt via SeamlessAccess-inloggningsknappen på https://metadata.swamid.se. Metadataverktyget kommer att presenteras på ett webinar torsdagen den 20:e januari, se https://wiki.sunet.se/x/_4uvBg.

Den internationella samarbets- och standardiseringsorganisationen REFEDS kommer under 2022 uppdatera sina entitetskategorier för att ännu bättre kunna ge användarna tillgång till de tjänster de behöver logga in i samtidigt som aktuell dataskyddslagstiftning beaktas. Detta betyder att SWAMID kommer att uppdatera SWAMIDs rekommendationer runt entitetskategorier senare i år. Det kommer att tillkomma fyra nya entitetskategorier: en för personaliserad åtkomst till tjänster, en för pseudonymiserad åtkomst till tjänster, en för anonymiserad åtkomst till tjänster samt en GDPR-anpassad Data Protection Code of Conduct. Skillnaden mellan de tre första är hur mycket personuppgifter som skickas av identitetsutgivaren till tjänsten. SWAMID Operation kommer under året att uppdatera wikisidorna om entitetskategorier för att beskriva hur de nya entitetskategorierna ska användas i framtiden. Det kommer också hållas webinarer om hur de nya entitetskategorierna konfigureras i av SWAMID stödda identitetsutgivare (Shibboleth IdP och ADFS). Vidare kommer SWAMIDs testverktyg att utökas med tester för de nya entitetskategorierna så snart de är beslutade av REFEDS.

SWAMID kommer under året fortsätta utveckla ADFS Toolkit för att följa de nya standarderna från REFEDS men också hantera standardiserad multifaktorinloggning enligt REFEDS standardsignalering och SWAMIDs tillitsprofiler. Version 2.1.0 kommer att släppas under första kvartalet. SWAMID kommer även här att genomföra webinarer för att beskriva hur ADFS Toolkits kan användas inom SWAMID.

SWAMID kommer som vanligt att delta under Sunetdagarna i vår och i höst. Vårens Sunetdagar kommer genomföras digitalt under andra hälften av mars, program kommer när det närmar sig.

Välkomna till 2022!
SWAMID Operations

 Är din tjänst beroende av personnummer, läs detta!
Pål Mikael Axelsson posted on May 20, 2021
I princip har alla IdP-administratörer gjort sitt jobb när det gäller förändringen av entitetskategorier i SWAMID och nu är det dags för er som administrerar tjänster i SWAMID att göra samma sak.

Enligt SWAMIDs metadata finns det idag runt 100 tjänster som via entitetskategorin SFS 1993:1153 får tillgång till personnummer för användarna som loggar in. Det finns några få nationella tjänster från t.ex. UHR och Ladok men de flesta är lärosäteslokala. Några av de lärosäteslokala hanteras dessutom av externa tjänsteleverantörer på uppdrag av resp. lärosäte. Vanliga typer av tjänster är kontoaktiveringsportaler och CMS men det finns även andra typer. De flesta lärosäteslokala tjänsterna begränsar från vilken identitetsutfärdare inloggning är möjlig, t.ex. lärosätets egna eller eduID och Antagning.se.

Vad händer nu? Detta brev är en första varning om att de tjänster som inte har bytt från den gamla entitetskategorin SFS 1993:1153 till Géant Data Protection Code of Conduct (CoCo) inte lägre att få tillgång till personnummer efter 2021-12-31 om inte en förändring görs. Observera att detta datum inte kommer att flyttas framåt! Detta gör att ni som har tjänster som får personnummer i samband med inloggning och som ännu gjort detta arbete måste nu planera in aktiviteter under hösten runt bytet av entitetskategorier.

För att kontrollera om ni är berörda av denna förändring finns nedanstående lista men ni kan även gå till https://metadata.swamid.se/?showSP&entityID och klicka på ert entityId. Den resulterande sidan med information om er tjänst ser ni vilka entitetskategorier som er tjänst har registrerade. Observera att SWAMIDs gamla entitetskategori Research and Education också avvecklas 2021-12-31 och därför är det bra om ni ser till så att alla attribut ni måste ha för att tjänsten ska fungera för användaren hanteras samtidigt via entitetskategorin CoCo.

Om ni vet att ert lärosäte har tjänster som är beroende av personnummer vid inloggning med hjälp av SWAMID sprid denna information till personer som arbetar med tjänsterna.

För mer information om kraven för att få använda entitetskategorin CoCo se https://wiki.sunet.se/display/SWAMID/4.1+Entity+Categories+for+Service+Providers#id-4.1EntityCategoriesforServiceProviders-G%C3%89ANTDataprotectionCodeofConduct.

Lista på tjänster och tillhörande test- och utvecklingsmiljöer som berörs:

- dev.lararlyftet-validering.se/shibboleth
- http://adfs.ju.se/adfs/services/trust
- http://fs.liu.se/adfs/services/trust
- http://fs.test.ad.liu.se/adfs/services/trust
- http://test.account.hj.se/adfs/services/trust
- http://ths.instructure.com/saml2
- http://uppsala.instructure.com/saml2
- https://acc.valda.uhr.se/shibboleth
- https://acc-nais.uhr.se/shibboleth
- https://account.hh.se/Shibboleth
- https://account.ki.se/shibboleth
- https://account.mdh.se/shibboleth
- https://account.tst.ki.se/shibboleth

- https://accountcheckout.lnu.se
- https://account-idac.ki.se/shibboleth
- https://account-utv.hh.se/Shibboleth
- https://activate.du.se/shibboleth
- https://activate-test.du.se/shibboleth
- https://administrationsverktyg.test.umu.se/shibboleth
- https://administrationsverktyg.umu.se/shibboleth
- https://aktivera.su.se/Shibboleth.sso
- https://aktivera-test.su.se/Shibboleth.sso
- https://antagningsp2-1.slu.se/shibboleth
- https://app.sh.se
- https://client200-151.its.umu.se/shibboleth
- https://client200-180.its.umu.se/shibboleth
- https://client200-190.its.umu.se/shibboleth
- https://demo.antagning.se/aws-sp
- https://demo.antagning.se/aws-sp-en
- https://dev.nais.uhr.se/shibboleth
- https://dev.valda.uhr.se/shibboleth
- https://devpassport.lu.se/activateaccount/shibboleth
- https://emrex.its.umu.se/gui-sp
- https://emrex-test.its.umu.se/shibboleth
- https://fidustest.skolverket.se/shibboleth
- https://idp.comanage.sunet.se/Saml2SP/sp
- https://idpaas-dev.swamid.se/Saml2SP/sp
- https://juridicum.blackboard.com/auth-saml/saml/SSO
- https://konto.bth.se/sp
- https://konto.hb.se/Shibboleth
- https://konto.hig.se:443/idm
- https://konto.weblogin.uu.se/shibboleth
- https://konto-test.test.hb.se/Shibboleth
- https://ladok3-demo-01.its.umu.se/gui-sp
- https://lartorget.sll.se/luvit/shibboleth
- https://lartorget.sll.se/shibboleth
- https://nyainloggning.hv.se/Shibboleth
- https://nyainloggning.slu.se/shibboleth-sp
- https://nyainloggning-test.hv.se/Shibboleth
- https://openexam.bmc.uu.se/simplesaml
- https://passportprod.lu.se/activateaccount/shibboleth
- https://passporttest.lu.se/activateaccount/shibboleth
- https://pera.cs.lth.se/shibboleth
- https://pingpong.ki.se/shibboleth
- https://portal.mdh.se/shibboleth
- https://portaltest.mdh.se/shibboleth
- https://prep.math.su.se/shibboleth
- https://sam.cs.lth.se/shibboleth
- https://selfservice.hb.se/Shibboleth
- https://selfservice-test.test.hb.se/Shibboleth
- https://shib1.oru.se/shibboleth
- https://sp.it.gu.se/shibboleth
- https://sp.swamid.se/shibboleth
- https://sp-nya.bth.se/shibboleth
- https://student.ladoktest13.utv.ladok.se/student-sp
- https://student.utbildning.ladok.se/student-sp
- https://test.fidus.sunet.se/shibboleth
- https://test.valda.i.uhr.se/shibboleth
- https://test.valda.uhr.se/shibboleth
- https://test-ki.pingpong.net/shibboleth
- https://test-lartorget.sll.se/shibboleth
- https://test-nais.i.uhr.se/shibboleth
- https://umdac-utv1.ad.umu.se/shibboleth
- https://uportalhb-test.ldc.lu.se/Shibboleth.sso
- https://valda.uhr.se/shibboleth
- https://webapp-utv.ita.mdh.se/shibboleth
- https://webkonto.student.hig.se/shibboleth
- https://weblogon.ltu.se/shibboleth
- https://www.antagning.se/aws-sp
- https://www.nais.uhr.se/shibboleth
- https://www.servicedesk.its.umu.se/shibboleth
- https://www.test.antagning.se/aws-sp
- https://www.test.universityadmissions.se/aws-sp-en
- https://www.universityadmissions.se/aws-sp-en
- test.lararlyftet-validering.se/shibboleth
- www.lararlyftet-validering.se/shibboleth



Ny site: metadata.swamid.se

Björn Mattsson posted on Mar 11, 2021
SWAMID har nu publicerat en ny web-site för att presentera Metadata.

På https://metadata.swamid.se/ går det att se samtliga av SWAMID publicerade IdP/SP:er
Mycket info finns där redan men mer kommer säkert att dyka de närmaste månaderna beroende på efterfrågan.

 ADFS Toolkit 2.0.0
Johan Peterson posted on Feb 14, 2021
Nu finns ADFS Toolkit 2.0.0 i skarp version!

Efter en lång tids utveckling och testande har vi äntligen kunnat släppa den nya versionen av ADFS Toolkit. 🙂
Det är mycket som hänt sedan 1.0.0.0 och modulen har betydligt fler konfigureringsmöjligheter än tidigare och är mer robust och uppgraderingsbar.

Vi uppmanar alla som kör en Release Candidate att uppdatera till den skarpa versionen.

För att läsa mer om vad som ändrats, läs release notes på GitHub:
https://github.com/fedtools/adfstoolkit/releases/tag/v2.0.0

Dokumentation kring hur man installerar eller uppgraderar finns också på GitHub:
https://github.com/fedtools/adfstoolkit

Läs igenom instruktionerna noga innan uppgradering. Det är lite olika steg som behöver göras vid uppgradering från 1.0.0.0 till 2.0.0.
Vidare uppgraderingar kommer gå betydligt lättare!

Upplever du några problem eller har funderingar, kontakta operations@swamid.se

 Stora problem för era studenter om ni inte fixat er identitetsutfärdare
Pål Mikael Axelsson posted on Nov 11, 2020
Inloggning med hjälp av SWAMIDs infrastruktur används idag i väldigt många tjänster, t.ex. Ladok, Prisma, Box och det nationella antagningssystemet. För att inloggningen ska fungera behöver vissa personuppgifter såsom attribut överföras från identitetsutfärdare (IdP) till tjänsten (SP). Inom SWAMID använder vi s.k. entitetskategorier för att organisera hanteringen av dessa attribut. Sedan Sunetdagarna hösten 2019 har SWAMID genomfört flera aktiviteter för att underlätta lärosätenas, och övriga organisationers, hantering av dessa entitetskategorier, med speciellt fokus på Microsoft-miljöer.

I arbetet med att göra överföringen av attribut mer strömlinjeformad och mer i andan av gällande personuppgiftslagstiftning beslutades det hösten 2019 att de gamla entitetskategorierna SWAMID Research and Education och SFS 1193:1153 (även kallat R&S respektive SFS) avvecklas och ersätts med utökad och tydligare användning av REFEDS Research and Scholarship (R&S) och GÉANT Data Protection Code of Conduct (CoCo). All användning av personnummer överförs till CoCo beroende dels på att personnummer används i fler tjänster än studentrelaterade och att CoCo ställer tydliga krav på att tjänsten tydligt måste informera användarna om hur personuppgifterna används.

Från och med 1 september i år har vi börjat flytta över tjänster från de gamla entitetskategorierna till de två som vi behåller och uppdaterar användningen av. Detta kommer att innebära att användare vid organisationer som ännu inte infört uppdaterat stöd för R&S och CoCo i sin identitetsutfärdare (IdP) inte längre kommer att kunna logga in i de tjänster som har flyttats över till den nya hanteringen. Användarnas problem kommer att smyga sig på tjänst för tjänst och kommer för lärosätena att bli väldigt tydlig när tjänster såsom Ladok och det nationella antagningssystemet flyttas. I och med detta får inte heller några nya tjänster de gamla entitetskategorierna (R&E respektive SFS).

Identitetsutgivarna för Antagning.se och eduID.se hanterar idag korrekt de entitetskategorier som kommer att användas i SWAMID framöver och därför har vi nu påbörjat arbetet tillsammans med de som äger tjänsterna att flytta över tjänster som kräver personnummer till entitetskategorin CoCo. Detta betyder att samtliga kontoaktiveringstjänster vid lärosätena som kräver personnummer snarast behöver flytta från den gamla SFS-kategorin till CoCo. Samtidigt måste alla identitetsutfärdare som har användare som loggar in i Antagning.se, Universityadmissions.se och Ladok för studenter se till så att de stödjer överföring av personnummer via entitetskategorin GÉANT Data Protection Code of Conduct (CoCo).

För att kontrollera att er identitetsutfärdare (IdP) är konfigurerad korrekt finns SWAMIDs testverktyg:

- https://release-check.swamid.se/

För er som har studenter och personal som loggar in i Ladok så finns ett specifikt test för just Ladok:

- https://ladok.release-check.swamid.se/

Om ni har några frågor och funderingar kontakta SWAMID Operations på operations@swamid.se.

 Shibboleth IdP v4 uppgradering
Paul Scott posted on Nov 10, 2020
SWAMID operations har tagit fram ett "How-to" dokument för uppgradering av Shibboleth Identity Provider till version 4.

Shibboleth IdP v3 är end-of-life vid årsskiftet 2020-12-31 på grund av att Spring framework 4.3 som den använder är också end-of-life.

SWAMIDs rekommendation är att göra en uppgradering av befintlig IdPn och inte en nyinstallation. För att uppgradera måste man ha redan anpassat sina attribute-resolver och attribute-filter till nyare syntax (för v3.4). I samband med uppgraderingen måste man också byta Java och Jetty till nyare versioner. Därför ska man räkna med ett litet längre driftavbrott (vår erfarenhet är runt 30 minuter).

Läs mer: Shibboleth IdPv4 uppgradering


Chrome version 80 ändrar beteende runt webbkakor (SameSite)
Pål Mikael Axelsson posted on Jan 23, 2020

Shibboleth konsortiet har publicerat en sammanfattning av deras testning av Chrome SameSite förändringen. Det finns på [1].

SWAMID operations rekommenderar att läsa igenom informationen. Man kan testa det nya beteendet med Google Chrome genom att sätta [2] till enabled i Chrome 79. Från och med Chrome 80 blir denna inställningen default.

Det finns en patch för ADFS som man måste installera för Windows Server 2016. Information om patchen finns på [3].

Det är för stunden svårt att begripa vad konsekvenserna kommer att bli under februari. Det finns en risk att det sker förändringar hos Service Providers som kommer att medföra olika beteende beroende på användares val av webbläsare, framför allt mellan de som kör Chrome 80+ resp Safari på macOS 10.14 och äldre samt Safari på iOS 12 och äldre. En beredskap för att det kan komma att rapporteras in udda användarproblem rekommenderas därför.

[1] https://wiki.shibboleth.net/confluence/display/IDP30/SameSite
[2] chrome://flags/#same-site-by-default-cookies
[3] https://support.microsoft.com/sv-se/help/4534271/windows-10-update-kb4534271


Förändrad best practice för attributrelease inom SWAMID
Pål Mikael Axelsson posted on Nov 11, 2019
Inom SWAMID har vi länge använt villkorsstyrd automatiserad attributrelease genom s.k. entitetskategorier för att på ett standardiserat sätt överföra personuppgifter i samband med inloggningen från hemmaorganisationens identitetsutfärdare till den webbtjänst som användaren försöker logga in i. SWAMID Operations har under en längre tid jobbat med att ta fram en ny best practice för hur identitetsutgivare släpper attribut till olika webbtjänster för att göra detta både enklare och tydligare. På Sunetdagarna i Falun under hösten presenterade vi SWAMIDs nya best practice.

I korthet innebär förändringen att SWAMIDs egna entitetskategorier SWAMID Research & Education och SWAMID SFS 1993:115 kommer att avvecklas och ersättas med REFEDS Research and Scholarship (R&S) och GÉANT Dataprotection Code of Conduct (CoCo). Vi har flyttat överföring av personnummer till entitetskategorin CoCo dock med vår rekommenderade begränsning att personnummer endast släpps till tjänster registrerade i SWAMID.

Tidplan för förändringen

- 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 Research & Education och SWAMID SFS 1993:1153 inlagda i metadata.
- Från och med 2020-10-31 kommer metadata vara rensat från de avvecklade entitetskategorierna.

I korthet betyder detta att före 1 maj nästa år bör ni ha uppdaterat ert system så att ni kan hantera SWAMIDs nya best practice. Ni behöver inte ta bort SWAMIDs gamla entitetskategorierna förrän vi säger till i slutet på nästa år.

Hur vet jag som tjänsteleverantör om min tjänst är berörd av förändringen av SWAMIDs Best Practice?

På wikisidan SWAMID Service Providers including interfederations finns en lista på samtliga tjänster som är tillgängliga inom SWAMID. Det enklaste sättet att ta reda på om ni berörs av förändringen är att leta upp er tjänst i listan och därefter titta i kolumnen Entity Categories. Står det researchandeducation eller sfs19931153 berörs ni av förändringen.

Vad behöver jag som tjänsteleverantör göra för att fortsätta få attribut?

Om ni idag har en tjänst registrerad i SWAMID som får attributrelease genom de gamla entitetskategorierna SWAMID Research & Education och SWAMID SFS 1993:1153 behöver ni titta på vilken av entitetskategorierna REFEDS Research and Scholarship (R&S) och GÉANT Dataprotection Code of Conduct (CoCo) som passar er bäst. På wikisidan Entity Categories for Service Providers finns det beskrivet vad som gäller för de bägge entitetskategorierna. Är det så att ni i er tjänst måste använda personnummer så är det GÉANT Dataprotection Code of Conduct som gäller. Under perioden 2020-05-01 till 2020-10-31 måste ni som använder SWAMIDs gamla entitetskategorier uppdatera till de två som kommer att finnas i framtiden.

Hur gör vi i vår identitetsutfärdare för att följa den nya best practice?

- För Shibboleth IdP har SWAMID Operations tagit fram nya exempelfiler på SWAMID s wiki för attributresolver och attributfilter tillsammans med en uppdaterad rekommendation av hur personnummer hanteras.
- För ADFS håller SWAMID Operations på att ta fram en ny version av ADFStoolkit, mer information kommer när den är klar.

SWAMIDs nya testverktyg för entitetskategorier

SWAMID Operations håller även på att skapa ett nytt testverktyg för att testa att man som identitetsutfärdare följer den nya rekommendationen. Denna finns redan i beta på adressen https://release-check.swamid.se/ men allt fungerar ännu inte, t.ex saknas sista testet samt informationstexter som beskriver test och resultat.

Vad händer nu?

Mer information kommer att skickas ut framöver och vi kommer att hålla minst ett webinar framöver.

SWAMID har på wikisidan Entity Category attribute release in SWAMID gjort en tydlig tabell över vilka attribut som ingår i vilka entitetskategorier. Observera att CoCo är lite krångligare eftersom endast attribut som begärs ska släppas.