SWAMID

SWAMID

Vad är på gång inom SWAMID?

Sunetdagarna hösten 2020

SWAMID Operations
operations@swamid.se

SUNET

SWAMID

Agenda

- Tillitsprofiler i SWAMID – Pål Axelsson, Sunet
- Hur väl uppfyller identitetsutfärdare registrerade i SWAMID de nya rekommendationerna för entitetskategorier – Björn Mattsson, BTH
- Vad innebär förändringen av entitetskategorier för tjänsterna som är beroende av dem? – Eskil Swahn, LU
- Uppgradera Shibboleth IdP till version 4 – Paul Scott, KaU
- ADFS Toolkit 2.0 – Johan Peterson, LiU

Tillitsprofiler i SWAMID

- SWAMID Board of Trustees beslutade om införande av ny revision runt SWAMID federationspolicy och tillitsprofiler i juni 2020
  - Genomgick konsultationsperiod under april-maj inkl. zoommöte
- Alla medlemmar med identitetsutfärdare registrerad i SAML eller eduroam måste vara godkända för minst SWAMID AL1
  - SWAMID Board of Trustees beslutade även om en övergångsperiod till 2021-12-31
  - Samtliga medlemsorganisationer som inte uppfyller kravet 2022-01-01 kommer att stängas av från SWAMID
- Ny tillitsprofil SWAMID AL3 med höga krav på identifiering av användare och som alltid kräver multifaktorinloggning

Vilka uppfyller inte kravet idag 14 oktober?

- Universitet och högskolor som inte uppfyller kravet idag – 7 st
  - Enskilda Högskolan Stockholm, Ersta Sköndal Bräcke Högskola, Handelshögskolan i Stockholm, Högskolan i Halmstad, Högskolan i Skövde, Kungliga Musikhögskolan samt Stockholms konstnärliga högskola
- Övriga medlemsorganisationer som inte uppfyller kravet idag – 9 st
  - Institut Mittag-Leffler, KK-Stiftelsen, Kungliga Biblioteket, Kungliga Vetenskapsakademien, NORDUnet, Rymdstyrelsen, Stockholm International Peace Research Institute, Universitets- och högskolerådet samt Vetenskapsrådet
- Listan hämtad från SWAMIDs medlemslista
  - https://wiki.sunet.se/display/SWAMID/SWAMID+Members

Vad ska vi göra för att uppfylla kravet?

- Kontakta SWAMID Operations för metodstöd och inledande möte
- Bestäm er för vilken eller vilka tillitsprofiler ni vill bli godkända för
  - Identifiera eventuella områden där förbättringar behövs
- Skriv organisationens Identity Management Practice Statement (IMPS) baserat på SWAMIDs malldokument
  - Mallar finns på https://wiki.sunet.se/display/SWAMID/SWAMIDs+Assurance+Profiles
- Skicka in IMPS till SWAMID Operations för granskning innan 31 maj 2021
  - Granskningen medför i princip alltid att IMPS med tilläggsdokument behöver uppdateras en eller flera gånger innan SWAMID Operations lämnar för beslut i SWAMID Operations

Entitetskategorier - Identitetsutfärdare

- Identitetsutfärdare (Identity Providers) inom SWAMID ska senast 2020-08-31 ha implementerat SWAMID:s nya rekommendationer för entitetskategorier för att deras användare även i framtiden ska kunna logga in i tjänster på samma sätt som tidigare
- De gamla entitetskategorierna SWAMID Research and Education och SWAMID SFS 1993:1153 ersätts med de internationella standarderna REFEDS Research and Scholarship (R&S) och GÉANT Data Protection Code of Conduct (CoCo)

SWAMID

Krav för entitetskategorierna

- REFEDS Research and Scholarship (R&S)
  - Kan användas av tjänster som tydligt stödjer forskning och utbildning
  - Begränsad uppsättning av personuppgifter överförs vid inloggning
    - Namn, e-postadress, unik identifierare och om student eller anställd
- GÉANT Data Protection Code of Conduct (CoCo)
  - Tjänsten definierar i metadataregistret vilka personuppgifter som tjänsten måste få för att kunna erbjuda tjänst till en användare
    - Lista med standardiserade personuppgifter finns på SWAMIDs Wiki
  - Tjänsten måste publicera en integritetspolicy (eng. privacy policy) som beskriver vilka personuppgifter som hanteras och hur de används

SWAMIDs testverktyg Release-check

- SWAMID testverktyg för att verifiera attributrelease
  - https://release-check.swamid.se/
- Följande tester finns
  - Test 0 - Visar infon som finns i Metadata om IdP
  - Test 1 – SP utan entity category. Inget skall släppas
  - Test 2 – R&S namn, email och eduPersonPrincipalName
  - Test 3 – CoCo som begär delmängd av attribute
  - Test 4 – CoCo som begär annan delmängd av attribute
  - Test 5 – CoCo SP som ej tillhör SWAMID. Skall EJ släppa personnummer
  - Fler kan komma senare 😊

SWAMID

Identitetsutfärdare med stöd för R&S

- Identitetsutfärdare som stödjer R&S samt markerar detta i metadata
  - BTH, DU, eduID.se, FHS, GU, HB, HHS, HiG, HJ, HKR, HV (Shibboleth), IRF, KaU, KI, Konstfack, KTH, LiU (x2), LNU, LTU, LU (x2), MaU, MDH, MiUN, OrU (Gammal Shibboleth), SLU, SMHI, SU, UmU, UU och VR
- Identitetsutfärdare som stödjer R&S men utan markering i metadata
  - Chalmers, EHS, GIH, HH, HV, KKH, KVA, RiSE, SH, Sunet, Uniarts och Vinnova
- Identitetsutfärdare som stödjer R&S men skickar för många attribut
  - Antagning.se, NORDUnet, SHH och OrU (Ny Shibboleth)

SWAMID

Identitetsutfärdare utan stöd för R&S

- Identitetsutfärdare som testat men inte uppfyller kraven (antingen inga eller för få attribut skickas)
  - KB (Shibboleth) och UHR
- Identitetsutfärdare inte som testat och information ej tillförlitlig
  - ESBH, HiS, HV (ADFS), KB (ADFS), KMH, NRM, RKH och SiCS

SWAMID

Identitetsutfärdare med stöd för CoCo

- Identitetsutfärdare som fullt ut stödjer CoCo samt markerar detta i metadata
  - BTH, DU, HB, HiG, HJ, KaU, Konstfack, KTH, LiU (ADFS), LNU, LTU, LU (x2), MiUN, SU, UU och VR
- Identitetsutfärdare som stödjer CoCo men utan personnummer samt markerar detta i metadata
  - eduID.se, FHS, HHS, IRF, LiU (Shibboleth) och UmU
    - Dessa följer CoCo men användarna kan få problem baserat på avsaknad av personnummer!

SWAMID

Identitetsutfärdare med stöd för CoCo

- Identitetsutfärdare som fullt ut stödjer CoCo men utan markering i metadata
  - GU, HH, HV (Shibboleth), EHS, KKH, KTH, MDH, SLU och Uniarts
- Identitetsutfärdare som stödjer CoCo men utan personnummer och utan markering i metadata
  - GIH, KI, OrU (Gammal Shibboleth), RiSE, SH, SMHI och Vinnova
    - Dessa följer CoCo men användarna kan få problem baserat på avsaknad av personnummer!

SWAMID

Identitetsutfärdare utan stöd för CoCo

- Identitetsutfärdare som testat men inte uppfyller kraven (antingen inga eller för få attribut skickas)
  - Antagning.se, ESBH, HiS, HKR, KB (Shibboleth), KVA, NORDUnet, ORU (Ny Shibboleth), Sunet och UHR
- Identitetsutfärdare inte som testat och information ej tillförlitlig
  - Chalmers, HV (ADFS), KB (ADFS), KMH, NRM, RKH, SHH och SiCS

SWAMID

Entitetskategorier för tjänster (nästa steg)

- Tjänster (Service Providers) i SWAMID har fram till 2021-03-31 på sig att ersätta Research & Education och SFS med Research and Scholarship och/eller GÉANT Dataprotection Code of Conduct
- Ingen nyregistrering av de gamla entitetskategorierna!
- SWAMID Operations kommer att kontakta alla registrerade kontaktpersoner
  - Inaktuella kontaktpersoner kommer att leda till att tjänster kommer sluta att fungera i praktiken samt i förlängningen tas bort ur SWAMID

- Ett webinar om detta under november

SWAMID

Vad behöver man göra som tjänsteleverantör?

- Kontrollera villkor för de internationella entitetskategorierna
  - Research & Scholarship är något annorlunda än Research & Education
  - Krav på metadata kan aktualiseras vid byte av entitetskategori
  - Privacy policy är en stark rekommendation för R&S och ett absolut krav för CoCo (på engelska!)
- Kontrollera och förstå hur attributrelease för resp. entitetskategori
  - R&S är förbestämt, CoCo innebär att tjänsten måste specificera vilka attribut som den behöver
- Tänk igenom geografiskt område (CoCo inom EU/EES, R&S även utanför EU)

SWAMID

Länkar om entitetskategrier

- https://wiki.sunet.se/display/SWAMID/Entity+Category+attribute+release+in+SWAMID
- https://wiki.sunet.se/display/SWAMID/Example+of+a+standard+attribute+filter+for+Shibboleth+IdP+v3.4.0+and+above
- https://wiki.sunet.se/display/SWAMID/How+to+consume+SWAMID+metadata+with+ADFS+Toolkit
- https://wiki.sunet.se/display/SWAMID/Service+Provider+Privacy+Policy+Template

SWAMID

Shibboleth IdPv4

- Shibboleth IdP 3.4.X är EOL och support slutar 2020-12-31. Detta på grund av att Spring 4.3 är EOL
  - https://github.com/spring-projects/spring-framework/wiki/Spring-Framework-Versions#supported-versions

- SWAMIDs rekommendation är att gör en uppgradering av befintlig IdP, inte en nyinstallation. Uppgraderingen kommer att kräva ett lite längre driftavbrott, troligtvis 30 minuter.

SWAMID

Shibboleth IdPv4

- De olika stegen:
  - Man måste har anpassat attribute-resolver och attribute-filter för och 3.4.0 uppåt
  - Inga DEPRECATED varningar i loggarna!
  - Java 11
  - Jetty 9.4 inklusive nya jetty-base (SWAMID tillhandahåller en jetty-base tarboll)
  - Rensa gamla jar-filer, uppdatera eventuella databas-connector jar-filer
  - Uppgradera Shibboleth

- Instruktioner kommer snart till wiki:n för Centos och Debian

SWAMID

ADFS Toolkit

- v2.0.0 RC5 ute på PowerShell Gallery
  - Kräver nyaste PowerShell Get i servern plus särskilt hämtning
- Stödjer de förändrade entitetskategorierna
- Bättre hantering för manuella ändringar av SP:s
- SHA1/SHA256
  - Stöd för auktorisering
  - Hantera en enskild SP
  - Hantera alla SP:s i en domän
  - Hantera alla SP:s

SUNET

ADFS Toolkit – Hur skapas attributrelease?

- Attributes added to release list
- Attributes added/overwritten to/in release list
- Attributes added/overwritten to/in release list
- Attributes added/overwritten to/in release list

SWAMID

ADFS Toolkit – Ny filstruktur

- ADFS Toolkit får egen konfigurationsfil, `config.ADFSTk.xml`
- Lärosätets konfigurationsfil flyttas till `/institution`, kallas Institution Config, `config.Swamid.xml`
- Federationen får konfigurationsfiler under `/federation/SWAMID`
  - Entitetskategorier, `SWAMID_entityCategories.ps1`
  - Standardsvar vid nyskapande/uppgradering av Institution Config, `SWAMID_defaultConfigFile.xml`, `SWAMID-TEST_defaultConfigFile.xml`

SWAMID

ADFS Toolkit – Vad annat är nytt?

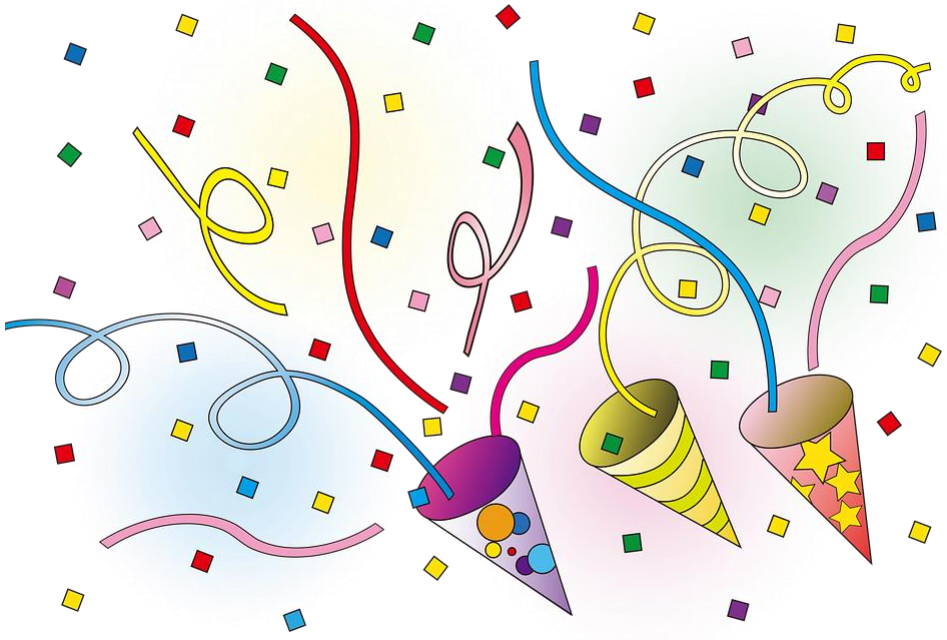
- Nytt sätt för att beräkna SP-hash från metadatat
- Bättre hantering av manuellt ändrade SP:s (prefix)
- Nya hanterade attribut
  - eduPersonPrimaryAffiliation
  - Persistent-id
    - Val mellan Persistent-id och Transient-id läses från metadatat
- Hälsokontroll vid körning (RC6/2.0.0)
  - Kontrollerar så att all kod är signerad
  - Kontrollerar så att versionen av Institution Config är kompatibel
  - `-criticalHealthChecksOnly` för att undanta kodsigneringskontrollen

SUNET

SWAMID

ADFS Toolkit – Vad ytterligare är nytt?

- Get-ADFSTkToolsIssuanceTransformRules
  - Hjälper dig skapa SAML2 regler för icke-SWAMID SP:s
- Planen är att v2.0.0 ska släppas inom en månad!



SUNET

SWAMID

Vill du veta mer?

- Vid frågor och funderingar ta kontakt med SWAMID Operations
  - operations@swamid.se

SUNET