Nya entitetskategorier och signalera tillitsnivåer till tjänster

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**