SWAMID

Swedish Academic Identity Federation

Rekommenderad attributrelease i SWAMID

Vad är på gång och varför?

2022-10-20

SWAMID

För SWAMID finns följande programpunkter under Sunetveckorna

- *Torsdag 13 oktober 09.00 -09.45: Metadata i SWAMID*
  Ett trekvarts år med SWAMIDs nya metadataverktyg, vilka är erfarenheterna och vad har förändrats.
  Vid årsskiftet måste alla identitetsutgivare och tjänster som är registrerade i SWAMID uppfylla SWAMIDs beslutade teknologiprofil för SAML WebSSO. Hur kan metadataverktyget hjälpa till med detta?
- Torsdag 20 oktober 10.00 -10.45: Rekommenderad attributrelease i SWAMID - Vad är på gång och varför?
  SWAMID är en infrastruktur för att möjliggöra att användare kan använda inloggningen i sin egen organisation för att logga in i webbaserade tjänster i sin egen och i andra organisationer. För att detta ska fungera måste organisationens identitetsutgivare skicka attribut, dvs. information om användaren, till tjänsten. Inom SWAMID har vi länge använt en metod som kallas entitetskategorier och nu kommer det nya GDPR-vänliga kategorier.
- Torsdag 20 oktober 11.00-11.45: Rekommenderad attributrelease i SWAMID - Hur gör vi?
  Del 2 om attributrelease beskriver hur vi tekniskt implementerar och testar de nya entitetskategorierna för både Shibboleth och ADFS.
- Torsdag 27 oktober 10.00 -10.45: Vad är på gång i SWAMID?
  Under de senaste åren har mycket fokus lagts på att uppdatera SWAMID policyramverk men nu skiftar fokus till tekniska förbättringar i SWAMIDs tekniska infrastruktur. Vi kommer bland annat att presentera vårt arbete med nytt och kompletterande sätt att hämta metadata samt planerna på en helt ny QA-miljö som ersätter SWAMIDs testmiljö.

Alla presentationer från SWAMID-passen kommer att publiceras på programsidan för Sunetdagarna efter respektive pass.

SWAMID

Det identitetsfederativa dilemmat

- Tjänster behöver information om användarna för att kunna låta dem logga in men identitetsutfärdarna vill vara i kontroll över vilka personuppgifter en tjänst får tillgång till
- Detta hindrar ofta anställda, primärt forskare, att logga in i de tjänster de behöver för att kunna genomföra sitt arbete, alternativt studier för studenter
- De som hindras i inloggningen tar ofta inte kontakt med supporten utan försöker hitta andra mindre säkra vägar in i tjänsten
- Inom SWAMID har vi varit bra på att minimera detta dilemma och nu tar vi nästa steg med nya entitetskategorier som är ännu mer GDPR vänliga

SWAMID

Entitetskategorier för attributrelease

- I SWAMID använd entitetskategorier för att underlätta attributrelease från identitetsutfärdare till tjänst
  - Kortfattat det är en markering i tjänstens metadata att de behöver definierade attribut från identitetutgivaren
- Entitetskategorierna används för att både förenkla och minimera överföringen av personuppgifter till en tjänst
- Tekniskt stöd för SWAMIDsnuvarande rekommenderade entitetskategorier finns i
  - SWAMIDsaktuella exempelfilter och -resolver för Shibboleth
  - ADFSToolkit v2.2.0

SWAMID

Vilka entitetskategorier används i SWAMID och eduGAIN?

- REFEDS Anonymous Access Entity Category
- REFEDS Pseudonymous Access Entity Category
- REFEDS Personalized Entity Category
- REFEDS Data Protection Code of Conduct Entity Category (CoCo v2)
- Géant Data Protection Code of Conduct Entity Category (CoCo v1)
- REFEDS Research and Scholarship Entity Category (R&S)
- European Student Identifier Entity Category

SWAMID

REFEDS Anonymous Access Entity Category

- Kategorin avser tjänster som erbjuder en servicenivå baserad på bevis på framgångsrik autentisering samt möjliggör ingen personifiering baserat på en användaridentifierare
- Tjänsten signalerar tydligt att de inte har behov av personlig information
- Attribut som ska överföras är:
  - schacHomeOrganization
  - eduPersonScopedAffiliation

SWAMID

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
- Attribut som ska överföras är:
  - **pairwise-id**
  - **eduPersonAssurance**
  - schacHomeOrganization
  - eduPersonScopedAffiliation

SWAMID

REFEDS Personalized 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
- Attribut som ska överföras är:
  - **subject-id**
  - **mail**
  - eduPersonAssurance
  - eduPersonScopedAffiliation
  - **displayName**
  - **givenName**
  - **sn**
  - schacHomeOrganization

SWAMID

Hierarki mellan Anonymous, Pseudonymous och Personalized

- Om en tjänst har mer än en av entitetskategorierna i metadata så är det den med minst attributrelease som vinner
  - Om Anonymous och Personalized ska Anonymous användas
- Detta följer av minimalitetsprincipen i GDPR

- Det finns ingen motsvarande hierarki mellan Anonymous, Pseudonymous eller Personalized och Code of Conduct
  - Undantaget är attributen pairwise-id och subject-id eftersom endast en av dem ska släppas samtidigt

SWAMID

REFEDS Data Protection Code of Conduct Entity Category (CoCo v2)

- Kategorin avser tjänster som antingen inte uppfyller kraven för övriga kategorier eller har behov andra attribut än de som erbjuds i dessa
- Entitetskategorin fungerar på samma sätt som CoCo v1 men baseras på GDPR istället för EU:s dataskyddsdirektiv (SFS uL)
- Ersätter på sikt CoCo v1 men bägge kommer att existera parallellt under lång tid
- Listan på förväntade attribut att stödja finns på SWAMID swiki, https://wiki.sunet.se/x/-4AFAQ

SWAMID

Attributen pairwise-id och subject-id

- De nya användaridentifierarna definierades 2019 som ett tillägg i standarden för SAML2
  - OASIS SAML V2.0 Subject Identifier Attributes Profile Version 1.0
- pairwise-id ersätter eduPersonTargetedID (ePTID, deprecated)
- subject-id ersätter eduPersonPrincipalName (ePPN) men bägge kommer att existera parallellt under lång tid
- Bortsätt från tekniska skillnader är den största skillnaden att pairwise-id och subject-id aldrig får återanvändas för någon annan person
  - De tekniska skillnaderna hanteras av Shibboleth och ADFS Toolkit

SWAMID

Att signalera tillit via eduPersonAssurance

- Attributet eduPersonAssurance används för att signalera användarens tillitsnivå enligt SWAMID (inkl. underliggande)
- Om användaren har en tillitsnivå ska även motsvarande värden för samt aktuella värden för REFEDS Assurance Framework inkluderas i signaleringen
  - SWAMIDspolicyramverk ger oss per automatik aktuella värden
- En identitetutfärdare får inte signalera en högre tillitsnivå än de är godkända för
- Exempelresolver för Shibboleth och ADFS Toolkit lägger till samtliga värden baserat på användarens tillitsnivå

SWAMID

Vilka tjänster känner vi till som kräver tillit?

SWAMID Assurance Levels

- Ladok, införande i flera faser
  - AL2 för nationell översikt, årskiftet
  - AL2 för anställda, halvårsskiftet
  - AL2 för svenska studenter, nästa årsskifte
- Nais - Samordning av riktat pedagogisk stöd
  - AL3 för alla handläggare

REFEDS Assurance Framework

- EuroHPC-centrat Lumi via MyAccessID
  - Användare informeras om krav på tillitsnivå från 15 januari
  - Användare kan inte logga in utan tillitssignalering efter 1 mars
- National Institute of Health (NIH) i USA kräver RAF medium för åtkomst till vissa tjänster hos dem
  - Medicinska forskare i Sverige berörs

SWAMID

Signalering för SWAMID AL1

eduPersonAssuranceska innehålla

- http://www.swamid.se/policy/assurance/al1
- https://refeds.org/assurance
- https://refeds.org/assurance/ID/unique
- https://refeds.org/assurance/ID/eppn-unique-no-reassign
- https://refeds.org/assurance/IAP/low
- https://refeds.org/assurance/ATP/ePA1m

SWAMID

Signalering för SWAMID AL2

eduPersonAssuranceska innehålla

- Samtliga värden som signaleras för SWAMID AL1
- http://www.swamid.se/policy/assurance/al2
- https://refeds.org/assurance/profile/cappuccino
- https://refeds.org/assurance/IAP/medium
- https://refeds.org/assurance/IAP/local~~-~~enterprise

SWAMID

Signalering för SWAMID AL3

eduPersonAssuranceska innehålla

- Samtliga värden som signaleras för SWAMID AL1
- Samtliga värden som signaleras för SWAMID AL2
- http://www.swamid.se/policy/assurance/al3
- https://refeds.org/assurance/profile/espresso
- https://refeds.org/assurance/IAP/high

- Observera att SWAMID AL3 endast får signaleras vid multifaktorinloggning

SWAMID

Nästa steg?

- Efter pausen fortsätter vi med införande i Shibboleth och ADFS Toolkit samt kort uppdatering runt SWAMIDstestverktyg release-check
- Välkomna tillbaka 11.00 eller passa på att ställ 100 frågor…

SWAMID

SWAMID

Swedish Academic Identity Federation