
SWAMID
Swedish Academic Identity Federation

SWAMID

Vad händer i SWAMID

Pål Axelsson
SWAMID Operations, SUNET
pax@sunet.se

SUNET

SWAMID

Kort om SWAMID

- **Swedish Academic Identity Federation**
- **SWAMID är en del av SUNET**
- **Endast organisationer med identitetshanterare är medlemmar i SWAMID (57 st)**
- **Federationen hanterar både WebSSO via SAML och Wifi via eduroam**

SWAMID

WebSSO via SAML

- 63 identitetsutgivare
  - 50 Shibboleth, 10 ADFS, 1 SSP, 2 pySAML
- 655 tjänster
- Federation över gränserna – eduGAIN
  - 48 akademiska medlemsfederationer med totalt 2433 identitetsutgivare och 1584 tjänster i interfederationen

SWAMID

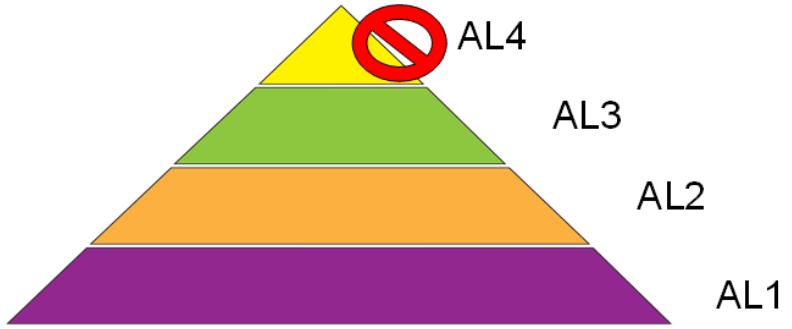
WebSSO via SAML

- **Bilaterala avtal och manuell attributrelease skalar inte!**
- **Tjänster med behov av basala personuppgifter såsom teknisk unik identifierare, namn och e-postadress får attributrelease via generaliserade entitetskategorier**
- **Tjänster med behov av personnummer får via lagstöd attributrelease via entitetskategorier efter särskilt beslut**

SUNET

I SWAMID är tillit allt!

- **Tillit inom SWAMID är inte riskhantering utan faktiska krav på organisation och användarhantering!**
- **11 medlemmar är godkända för SWAMID AL1 & SWAMID AL2**
- **15 medlemmar är godkända för enbart SWAMID AL1**



AL1: Vet att det är en person (obekräftad). Personuppgifterna är självuppgivna.
- Exempel: Facebook och Google

AL2: Vet vem personen är (bekräftad). Uppgifterna är delvis hämtade från annan källa.
- Exempel: Universitet eller högskola.

AL3: Vet mycket väl vem personen är (verifierad). Personen har uppvisat legitimation och personuppgifter är delvis hämtade från annan källa.
- Exempel: Svensk E-legitimation.

SWAMID

En evighet går fort…

…eller att byta signeringsnyckel för federationen

SUNET

SWAMID har bytt signeringsnyckel

För 10 år sedan var 10 år en evighet!

SWAMID

December 2016: Nyckelsigneringsparty

- **Planering är nödvändig och viktig…**
- Publik händelse med utsedd extern revisor
  - Nyckelsigneringsprocessen: https://wiki.swamid.se/display/SWAMID/Nyckelrullning+2016+-+Nyckelceremoni
  - Inspelning av nyckelsigneringen: https://youtu.be/vANObw7NE2E
- För att skapa n ny signeringsnyckel för SWAMIDS metadata skapades en särskild teknisk miljö med särskild hårdvara för slumptal. Mjukvarukomponenterna är tillgängliga för alla
  - https://github.com/SUNET/keykeeper
  - Den nya nyckel finns sparad i HSM och all signering sker med hjälp av HSM

SUNET

SWAMID

En evighet är allti en evighet…

20 år är den nya evigheten!

Vi hoppas att SAML har gått ur tiden om 20 år…

SUNET

SWAMID

Våren 2017: Byta till den nya signeringsnyckeln

- Information, information och information…
  - Tre webinarer riktade till identitetsutfärdare
  - Fem e-postbrev till olika nivåer i organisationerna som äger identietsutfärdarna
  - Tre publika e-postbrev till identitetsutfärdare och tjänster
- Hur gick det?
  - Alla utom en identietsutfärdare var korrekt konfigurerade när den gamla signeringsnyckeln upphörde den första maj
  - Alla utom ett par handfull tjänster var korrekt konfigurerade när den gamla signeringsnyckeln upphörde den första maj
- **Information is everything…**

SUNET

SWAMID

Vad händer framöver?

- **SWAMID tittar på den framtida federationstekniken OpenId Connect Federation**
- **SUNET kommer att titta på identitetshantering för mindre organisationer och eventuellt tillhandahålla en tjänst till mindre lärosäten och forskningsorganisationer**
- **SWAMID kommer att använda e-legnämndens entitetskategori loa2-pnr för överföring av person-/samordningsnummer till myndighetssystem**

SUNET

SWAMID

Swedish Academic Identity Federation

SWAMID