
SWAMID
Swedish Academic Identity Federation

Workshop med focus på AL-processer

Syfte

- Att praktiskt på plats stödja lärosätet med att uppnå tillitsprofilerna SWAMID AL1 och SWAMID AL2
- Att efter workshopen ha klart en ansökan med Identity Management Practice Statement (IMPS) till SWAMID AL1 eller SWAMID AL2, eventuellt kombinerat med en lista över vad som behövs för att få klart en ansökan

SWAMID

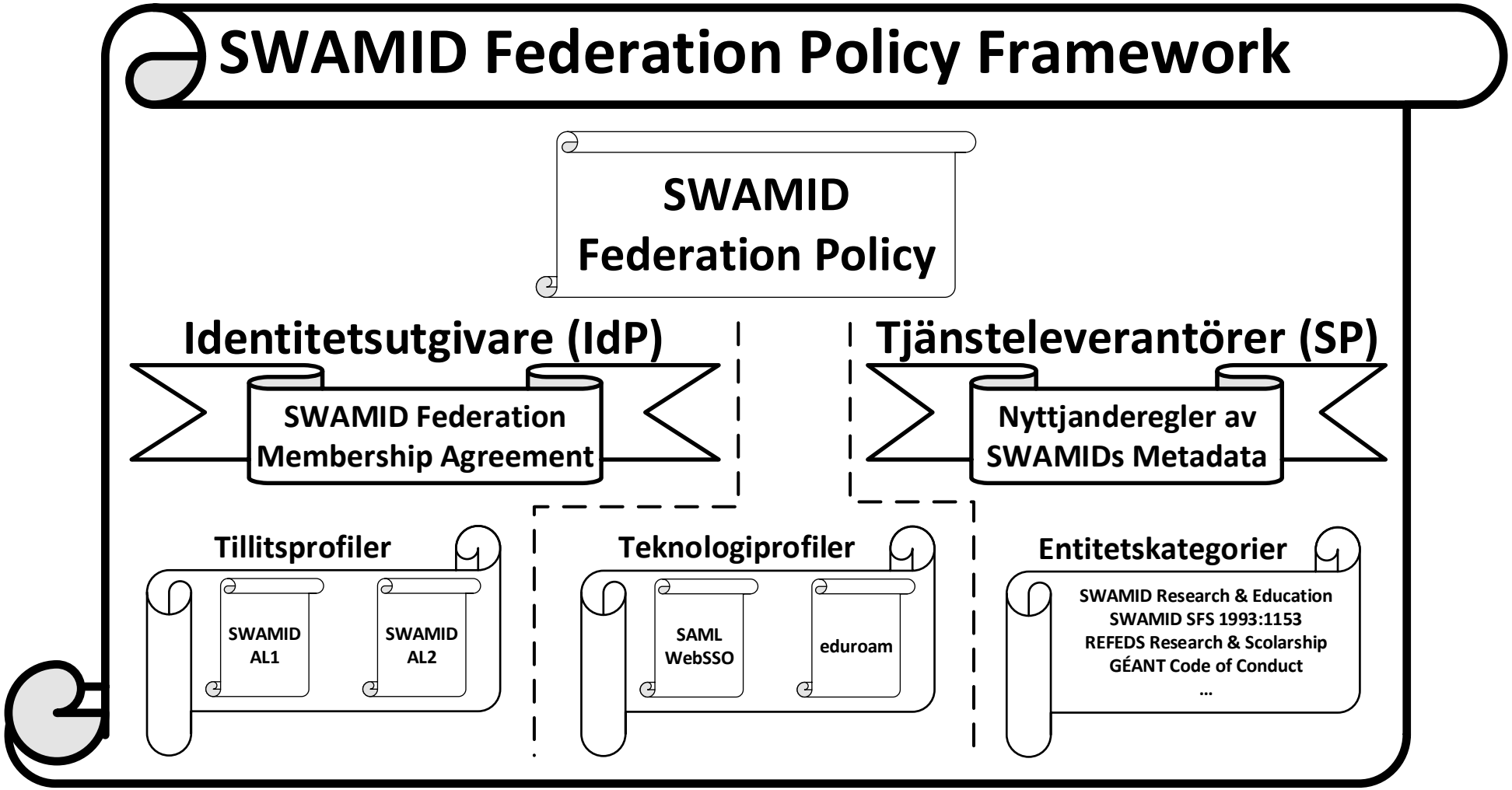
Presentation av alla deltagare

Laget runt

- Vem är du och var kommer du ifrån?
- Vad har du för förväntan på denna workshop?

SUNET

SWAMID



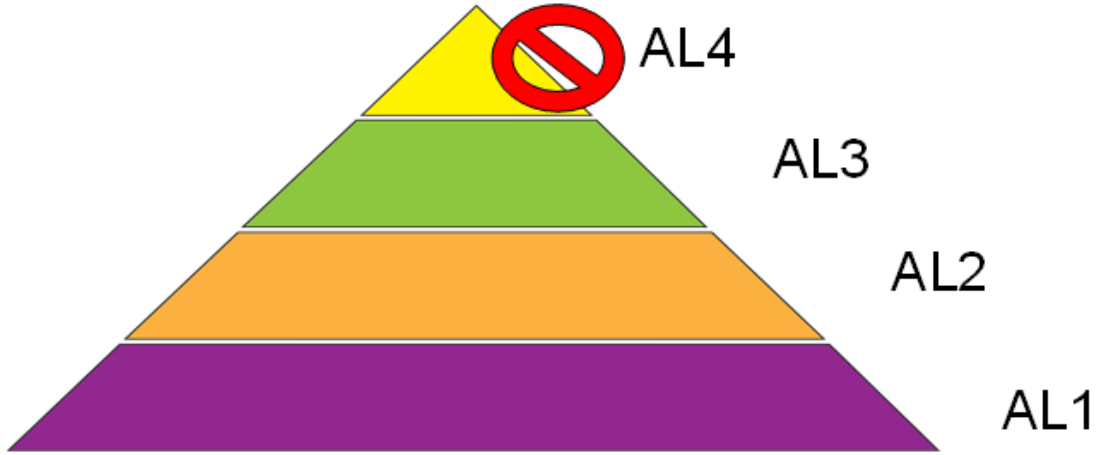
SUNET

SWAMID

Introduktion till tillitsnivåer

SUNET

Tillitspyramiden



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.

https://www.sunet.se/swamid/policy/al1/

SWAMID

SWAMID Identity Assurance Level 1 Profile

Tillitsprofilen SWAMID AL1 innebär tre saker:

- Att det är en person som innehar och använder kontot, detta kallas även för obekräftad användare.
- Informationen knuten till kontot är oftast uppgiven av och ansvaras för av användaren själv.
- Lärosätets identitetshanteringssystem uppfyller minst kraven i SWAMID AL1.

SUNET

https://www.sunet.se/swamid/policy/al2/

SWAMID

SWAMID Identity Assurance Level 2 Profile

Tillitsprofilen SWAMID AL2 innebär tre saker:

- Utökning av SWAMID AL1.
- Ställer högre krav på att lärosätet vet vem personen är som innehar och använder kontot, detta kallas även för bekräftad användare.
- Lärosätet ansvarar för personinformationen till skillnad från i SWAMID AL1.
- Lärosätets identitetshanteringssystem uppfyller minst kraven i SWAMID AL2.

SUNET

Vad skiljer SWAMID AL1 och SWAMID AL2?

- Godkännande och revisionsförfarande
- Högre krav på vem som innehar och använder användarkontot
- Högre krav på lösenord och lösenordsåterställning
- Högre krav på hantering av attribut
- Högre krav på loggning

Observera! En organisation kan ha vissa användare på SWAMID AL1 och andra på SWAMID AL2 så länge de kan signalera vem som är vad.

Godkännande och revisionsförfarande

SWAMID AL1

- Egenkontroll
- Lämna in IMPS och checklista för SWAMID AL1
- SWAMID Operations granskar checklistan och läser igenom IMPS

SWAMID AL2

- Extern granskning
- Lämna in IMPS med länkade eller bifogade handlingar
- SWAMID Operations granskar IMPS inkl. handlingar

SWAMID

Att skriva en Identity Management Practice Statement (IMPS)

SUNET

https://wiki.swamid.se/display/SWAMID/SWAMID+Identity+Assurance

SWAMID

Innan vi börjar…

- Ladda ner IMPS-mallen från sidan SWAMID Identity Assurance på https://wiki.swamid.se
- Leta upp länkar eller dokument till organisationens
  - användarregler,
  - lösenordspolicy,
  - tjänstedefinition för identitetsutgivaren (IdP) eller användarhanteringssystem (IAM) och
  - policy för hantering av personuppgifter för identitetsutgivaren (IdP).
  - (eller motsvarande)

SUNET

1. Inledning

- Under det här avsnittet skriver men en kort text som beskriver organisationen och varför den är med i SWAMID.
- Exempel:
  ”Grönköpings högskola är som svenskt lärosäte beroende av att på ett säkert och enkelt sätt kunna ge sina anställda och studenter tillgång till nationella och internationella IT-resurser. Detta ges genom medlemskap i SWAMID. Högskolan ser därför ett fortsatt medlemskap som en förutsättning för sin verksamhet.”

4.1 Enterprise and Service Maturity

- Avsnittet är lika för SWAMID AL1 och SWAMID AL2!
- Definierar tydligt vilken organisation som uppfyller tillitsprofilen.
- Visar att de som sköter identitetshanteringssystemet vid lärosätet är medvetna om vilka lagar och förordningar som styr denna verksamhet, finns en exempeltext för utbildningsmyndigheter.
- Beskriver att organisationen har fastslagna rutiner för avveckling hårddiskar, band och andra lagringsmedia som innehåller känslig information.

SWAMID

4.2 Notices and User Information

- Avsnittet är lika för SWAMID AL1 och SWAMID AL2!
- Visa var organisationens användarregler finns.
  - Har organisationen inga finns ett exempel på enkla användarregler på SWAMIDs Wiki.
- Beskriv hur användarna godkänner organisationens användarregler, både första gången och om reglerna uppdateras.
- För att andra ska kunna förstå vad en identitetsutgivare är ska det finnas en tjänstedefinition, exempel finns på SWAMIDs Wiki.
- Personuppgifter överförs i samband med inloggningar till tjänsten, det måste finnas en integritetspolicy.

SWAMID

4.3 Secure Communications

- Avsnittet är lika för SWAMID AL1 och SWAMID AL2!
- Beskriv hur lärosätet har satt upp sin tekniska miljö för identitetsutgivaren och aktuella undersystem, t.ex. Active Directory, så att ingen känslig information är avlyssningsbar vid överföring.
- Tänk särskilt på att inte skriva någon hemlig information i texten eftersom IMPS automatisk blir allmän handling vid inskickande till SWAMID eftersom SWAMID är en del av SUNET som är en avdelning under Vetenskapsrådet som är en myndighet.

SUNET

4.4 Security-relevant Event (Audit) Records

- Detta avsnitt gäller bara SWAMID AL2!
- Beskriv hur ni sparar viktig säkerhetsloggar runt administration och användning av identitetsutgivaren och underliggande system.
- Tänk särskilt på att inte skriva någon hemlig information!

5.1 Credential Operating Environment

- SWAMID AL2 har högre krav än SWAMID AL1 men rekommendationen är att alla användare uppfyller kraven i SWAMID AL2 när det gäller lösenord.
- Beskriv lösenordspolicy, hur användare avråds från att dela lösenordet med andra samt vilka rutiner och tekniska hinder som finns för missbruk av lösenord.
- Tänk särskilt på att inte skriva någon hemlig information!

SWAMID

5.2 Credential Issuing

- Kraven för identifieringsmetoderna skiljer mellan SWAMID AL1 och SWAMID AL2.
- Beskriv i löpande text identitetsutgivarens DNS-domän, hanteringen av användarnamn/konton och ändring av självuppgiven information.
- Identifieringsmetoder, egna bilder.
- Krav på identitetsgranskningen, egen bild.
- För SWAMID AL2 tillkommer krav på att registrera och spara användares ändrade tillitsnivå.

SUNET

Identifieringsmetoder SWAMID AL1

On-line

- Inloggning med attributrelease från identitetsutgivare godkänd för SWAMID AL1 eller SWAMID AL2.
- Brev till självuppgiven e-postadress med tidsbegränsad engångskod och CAPTCHA.

In-person

- Besök vid servicedesk, eller motsv., utan krav på id-kontroll.

Off-line

- Brev till självuppgiven adress med tidsbegränsad engångskod.

Annan motsvarande metod

- Granskas av SWAMID Operations.

Identifieringsmetoder SWAMID AL2

On-line

- Inloggning med attributrelease från identitetsutgivare godkänd för SWAMID AL2.

In-person

- Besök vid servicedesk, eller motsv., med krav på godkänd id-handling.

Off-line

- Brev till folkbokföringsadress med tidsbegränsad engångskod.
- Brev till utrikesadress på hushållsräkning med tidsbegränsad engångskod där namn på hushållsräkning stämmer överens med namn på godkänd id-handling.

Annan motsvarande metod

- Granskas av SWAMID Operations.

SWAMID

Krav på identitetsgranskningen

- För SWAMID AL1 krävs att den person som verifierar en person vid besök i servicedesk, eller motsv., är godkänd för SWAMID AL1 eller SWAMID AL2 samt har inloggning på motsvarande nivå.
- För SWAMID AL2 krävs att den person som verifierar en person vid besök i servicedesk, eller motsv., är godkänd för SWAMID AL2 samt har inloggning på motsvarande nivå.
- Gäller även systemadministratörer eller andra som arbetar med identitetshanteringssystemet vid organisationen.

SUNET

5.3 Credential Renewal and Re-issuing

- SWAMID AL2 har högre krav än SWAMID AL1!
- Beskriv hur användarna kan byta lösenord samt hur de gör för att återställa dem om de glömt sitt lösenord.
- Lösenordsåterställning kan använda samma metoder som vid användaridentifiering i föregående avsnitt.
- Vid lösenordåterställning är det ok för SWAMID AL1 att skicka tidsbegränsad engångskod via e-post eller SMS medans för SWAMID AL2 krävs bägge i kombination.
- För SWAMID AL2 ska även beskrivas hur användaren kan tvingas att byta lösenord.

5.4 Credential Revocation

- Avsnittet är lika för SWAMID AL1 och SWAMID AL2!
- Beskriv hur användarens inloggning kan stängas av och hur användarna gör för att aktivera inloggningen igen.
- För återaktivering krävs att samma metoder som användes vid användaridentifiering används igen.
- Vid avstängning beroende avslutad anställning eller saknad studieaktivitet är det ok med automatisk återaktivering om det är inom en begränsad fastslagen tidsperiod, t.ex. inom samma termin, så länge som det tydligt beskrivs.

5.5 Credential Status Management

- Avsnittet är lika för SWAMID AL1 och SWAMID AL2!
- Det måste finnas en sparad historik över manuell och automatiserad administration av alla användare, beskriv denna.
- Ange förväntad tillgänglighet av identitetsutgivaren när det gäller tillgänglighet. Hänvisa gärna SLA eller motsvarande.

5.6 Credential Validation/Authentication

- Avsnittet är lika för SWAMID AL1 och SWAMID AL2!
- Om SWAMIDs rekommendationer följs utryck detta tydligt.
- I de fall där avsteg från SWAMIDs rekommendationer görs beskriv detta också.

SWAMID

Avslutning

SUNET

SWAMID

Avslutning

Laget runt

- Har ni fått förväntat resultat av workshopen?
- Vad är nästa steg för er?
- Vad tyckte ni om denna form på workshop?
- Är det någon annan workshop ni tycker att vi ska anordna?

SUNET