SWAMID

# SWAMID

## En introduktion till SWAMID - Vad, hur och varför

Sunetdagarna hösten 2020

Pål Axelsson – Sunet
pax@sunet.se

SUNET

SWAMID

# SWAMID i en mening

- Säker inloggning till nationella och internationella tjänster för studenter, forskare, lärare och övriga anställda vid universitet och högskolor i Sverige samt anställda vid övriga organisationer anslutna till Sunet

SWAMID

# Vad är syftet med SWAMID?

- Att förenkla för en person att logga in och använda många av de tjänster personen behöver använda i sitt arbete eller för sina studier
- Att minska antalet användarkonton en person behöver i sitt arbete eller för sina studier
- Att sänka kostnaden för att hantera digitala identiteter inom och mellan organisationer
- Att säkert och kontrollerat överföra begränsade personuppgifter för att identifiera en person vid inloggning i en tjänst

SWAMID

# Vilka kan använda SWAMID?

- Medlemskap i SWAMID krävs enbart för identitetsutfärdare, det vill säga organisationer som har användare som ska logga in i tjänster
  - Endast organisationer anslutna till Sunet kan bli medlemmar i SWAMID
- De som levererar tjänster som använder SWAMID behöver inte vara medlemmar i SWAMID. Däremot måste de acceptera SWAMIDs användarvillkor
  - För att få nytta av SWAMID måste tjänsten uppfylla särskilda krav för att identitetsutfärdarna ska överföra personuppgifter i samband med inloggningen

SWAMID

# Vad är SWAMID?

- En förkortning av **Sw**edish **A**cade**m**ic **Id**entity Federation
- Ett policyramverk och två federerade inloggningsmodeller, webbinloggning via SAML och nätinloggning via eduroam
- Ett tekniskt metadataregister som kopplar ihop identitetsutfärdare och tjänster
- Ett erfarenhetsutbyte och en samverkansgrupp runt federerad webbinloggning

# Identitetsutfärdare och tjänster

- SWAMID har totalt 62 organisationer som är medlemmar i SWAMID
- Det finns idag drygt 650 olika webbtjänster registrerade i SWAMID
  - En grupp av tjänster riktar sig till enskilda organisationer, t.ex. organisationsinterna tjänster
  - En annan grupp av tjänster riktar sig till definierade användare vid flera olika organisationer, t.ex. Sunets upphandlade tjänster
  - Den tredje gruppen tjänsten riktar sig till i princip alla medlemmar i SWAMID, t.ex. Ladok, Antagning.se och Prisma
- Drygt 3000 webbtjänster för både forskare och studenter importeras från den internationella akademiska interfederationen eduGAIN

# SWAMIDs organisation

- **SWAMID Board of Trustees** - Styrgruppen för SWAMID
  - Ordförande från Sunet
  - 4 IT-chefer vid lärosätena, nomineras av ITCF
  - Representant från UHR
  - Representant från Ladokkonsortiet
  - 2 representanter från forskningsinfrastrukturer i Sverige
- **SWAMID Operations** sköter daglig verksamhet
  - Tjänsteansvarig plus tekniskt driftstöd från Sunet
  - 6 personer från olika lärosäten

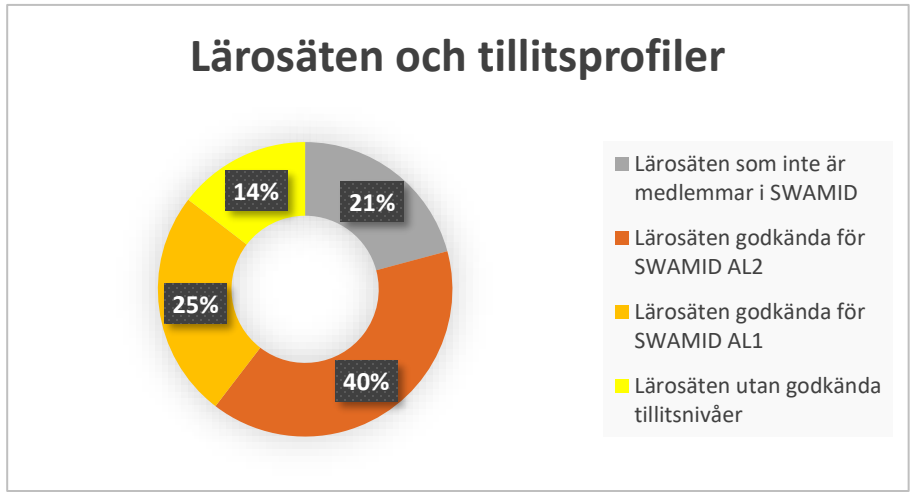
SWAMID

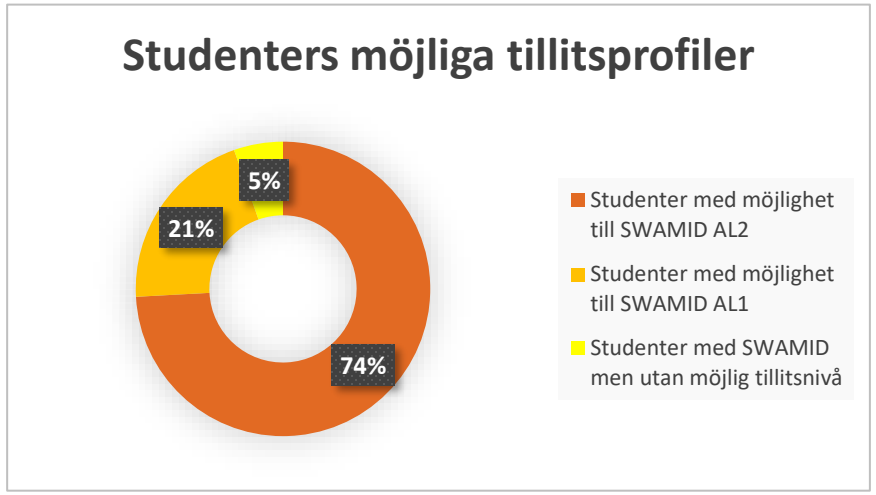
# Hur kan en tjänst lita på inloggningar?

- En grundtanke med SWAMID är att den som äger en tjänst ska kunna lita på att lärosäten och andra organisationer hanterar användare och inloggningar tillräckligt bra
- För att definiera vad som är tillräckligt bra finns tre olika tillitsprofiler, SWAMID AL1, SWAMID AL2 och SWAMID AL3
- Alla identitetsutfärdare måste uppfylla minst en av dessa tillitsprofiler
  - Alla organisationer uppfyller inte detta idag men måste göra det senast 2021-12-31
- Medlemsorganisationen visar hur de uppfyller tillitsprofilerna genom att skriva ett särskilt dokument som granskas av SWAMID

# Lärosäten och deras användare

- 38 av 48 lärosäten med examinationsrätt enligt högskoleförordningen är medlemmar i SWAMID
- Dessa 38 lärosäten täcker 99,7% av alla anställda och studenter



SWAMID

# Tillitsprofilen SWAMID AL1

Tillitsprofilen innebär i korthet att

- det är en person som innehar och använder kontot, kallas även för obekräftad användare
  - Minsta nivå är att personen går att kontakta via verifierad e-postadress
  - Oftast vet man mer men inte tillräckligt för SWAMID AL2
- informationen knuten till kontot kan vara uppgiven av och ansvaras för av användaren själv
- organisationens identitetshanteringssystem uppfyller minst kraven i SWAMID AL1

# Tillitsprofilen SWAMID AL2

Tillitsprofilen innebär i korthet att

- kraven utökas från SWAMID AL1
- högre krav ställs på att organisationen vet vem personen är som innehar och använder kontot, kallas även för bekräftad användare
  - Minsta nivå är utskick av engångskod till folkbokföringsadress
- organisationen alltid ansvarar för information om användare till skillnad från i SWAMID AL1

# Tillitsprofilen SWAMID AL3

Tillitsprofilen innebär i korthet att

- kraven utökas från SWAMID AL2
- ännu högre krav ställs på att organisationen vet vem personen är som innehar och använder kontot, kallas även för verifierad användare
  - Minsta nivå är noggrann kontroll av identitetshandling inkl. beslutade rutiner runt kontroll
- Inloggning måste alltid ske med multifaktor

SWAMID

# Varför ställa krav på personidentifiering?

- GDPR... Rätt person ska ha tillgång till sina egna personuppgifter och uppgifter som är knutna till sig, t.ex. studieresultat
- Vissa tjänster har högre krav på att det är rätt individ som använder tjänsten

- Vilken tillitsprofil en tjänst har behov av är en riskbedömning och avvägning mellan säkerhet och användbarhet, ofta finns hjälp att hämta i informationssäkerhetsklassificering av tjänsten

SWAMID

# Utländska distansstudenter?

- Det är nästan omöjligt att göra samma nivå av identifiering för utländska distansstudenter i början av studierna som för studenter i Sverige
- Vissa distansstudenter besöker aldrig lärosätet

- För studenter med svenskt personnummer eller som finns på plats på lärosätet använd SWAMID AL2
- För distansstudenter utan svenskt personnummer använd den lägre nivån SWAMID AL1 (lägre krav på identifiering)

SWAMID

# Multifaktorinloggning i SWAMID

- Säkrare inloggning där förutom lösenord även minst ytterligare en inloggningsfaktor krävs
  - Kan även i vissa fall vara pinkod + inloggningskort (smarta kort)
- Den andra inloggningsfaktorn måste vara något man har, t.ex. en särskild app i telefonen som ger en engångskod eller en hårdvarupinne ansluten i samma enhet som webbläsaren
- Inom SWAMID godkänns inte SMS och appar som visar knapp för att acceptera inloggning som andra faktor
  - Skyddar bra mot lösenordsfiske men inte vid högre säkerhetskrav

SWAMID

# Överföring av personuppgifter

- När en person loggar in i en tjänst överförs personuppgifter från personens identitetsutfärdare till tjänsten
- Inom SWAMID används en standardiserad modell för att hantera vilka personuppgifter som överförs vid inloggningen för att
  - minimera vilka uppgifter som överförs
  - göra denna minimering på ett skalbart och effektivt sätt
- Modellen kallas entitetskategorier och är en markering i SWAMIDs metadataregister som används för automatiserade beslut

SWAMID

# Vilka entitetskategorier används?

- REFEDS Research and Scholarship
  - 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
  - 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

SWAMID

# Vill du veta mer?

- Det finns fler sessioner om SWAMID och närliggande tjänster under Sunetdagarna
- SWAMID har omfattande information på Sunets Wiki
  - https://www.swamid.se
- Anmäl dig till SWAMIDs öppna e-postlista saml-admins
  - https://wiki.sunet.se/display/SWAMID/Contact+SWAMID
- Vid frågor och funderingar ta kontakt med SWAMID Operations
  - operations@swamid.se