SWAMID

SWAMID

En introduktion samt vad är aktuellt

Sunetdagarna 2023
Pål Axelsson – Sunet
pax@sunet.se

SUNET

SWAMID

SWAMID i en mening

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

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 SWAMIDs infrastruktur behöver inte vara medlemmar i SWAMID men uppfylla vissa kriterier
  - Tjänsten uppfylla vissa anslutningskriterier, t.ex. tillhöra en medlemsorganisation eller att minst en medlemsorganisation använder tjänsten
  - Följa det tekniska regelverket för aktuell identitetsfederationsteknologi

SWAMID

Vad är SWAMID?

- En förkortning av **Sw**edish **A**cade**m**ic **Id**entity Federation
- Ett policyramverk och federerade inloggningsteknologier
  - Webbinloggning via SAML
  - Webbinloggning via OpenID Connect (pilot påbörjas under 2023)
  - Nätinloggning via eduroam
- Tekniskt metadataregister som kopplar ihop identitetsutfärdare och tjänster
- Erfarenhetsutbyte och samverkansgrupp runt federerad inloggning

Identitetsutfärdare och tjänster

- SWAMID har totalt 62 organisationer som är medlemmar i SWAMID
- Det finns idag drygt 520 olika webbtjänster registrerade i SWAMID
  - Tjänster som riktar sig till definierade användare vid flera olika organisationer, t.ex. Sunets upphandlade tjänster
  - Tjänster som riktar sig till i princip alla medlemmar i SWAMID, t.ex. Ladok, Antagning.se och Prisma
  - Tjänster som riktar sig till enskilda organisationer, t.ex. organisationsinterna tjänster
- Drygt 3500 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
  - Representant från forskningsinfrastrukturer i Sverige
- **SWAMID Operations** sköter daglig verksamhet
  - Tjänsteförvaltare plus specialister och teknikstöd från Sunet (3 personer)
  - Specialister på deltid från olika lärosäten (5 personer)

SWAMID

Hur kan en tjänst lita på inloggningar?

- Grundtanken 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
- Medlemsorganisationen visar hur de uppfyller tillitsprofilerna genom att skriva ett särskilt dokument som granskas och godkänns av 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
- information knuten till kontot kan vara uppgiven 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 är alltid ansvarig för information om användare

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
  - Identifieringsnivå är noggrann kontroll av identitetshandling, inkl. beslutade rutiner runt denna kontroll, alternativt svensk e-legitimation på LoA3-nivå
- Inloggning måste alltid ske med multifaktor enligt SWAMIDs regelverk

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 studenter som finns på plats på lärosätet använd SWAMID AL2
- För distansstudenter utan svenskt personnummer använd antingen identifiering via eduID på AL2-nivå eller den lägre nivån SWAMID AL1

SUNET

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

Multifaktorinloggning i SWAMID

- Säkrare inloggning där inte enbart lösenord räcker
- Minst två olika sorters faktorer där den säkrare måste vara något man har och den andra är antingen lösenord eller biometri
- Inom SWAMID godkänns inte SMS, motringning och appar som endast visar knapp för att acceptera inloggning
  - Skyddar bra mot lösenordsfiske men inte vid högre säkerhetskrav
- Inom 2-5 år kommer högre krav mot nätfiskeresistentare multifaktorinloggning
  - Sexsiffriga OTP-koder och push med en av tre sifferkoder försvinner först

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? 1(2)

- REFEDS Anonymous Access
  - Begränsade anonymiserade personuppgifter överförs vid inloggning
    - Student eller anställd samt organisation
- REFEDS Pseudonymous Access
  - Begränsade pseudonymiserade personuppgifter överförs vid inloggning
    - Unik pseudononymiserad identifierare som ej går att spåra mellan tjänster, om student eller anställd, organisation och tillitsnivå
- REFEDS Personalized Access
  - Begränsade personuppgifter överförs vid inloggning
    - Unik identifierare som går att spåra mellan tjänster, e-postadress, namn, om student eller anställd, organisation och tillitsnivå

Vilka entitetskategorier används? 2(2)

- 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 samt om student eller anställd
- GÉANT/REFEDS Data Protection Code of Conduct v1 och v2
  - 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

Vad är på gång runt metadatahantering

- Metadataverktyget vidareutvecklas kontinuerligt, nu senast aktiverades behörighetshantering
- Årlig kontroll och validering av metadata kommer att börja skickas ut
- Årlig kontroll och validering av Identity Management Practice Statement

SUNET

Att hämta metadata från SWAMID

- Idag hämtar alla metadataaggregat från https://mds.swamid.se/md
  - Att ladda hem fulla aggregat med flera tusen entiteter tar mycket tid att hämta hem och ladda in i SAML-klienterna
  - Att hämta fulla aggregat medför att SAML-klienten behöver ha mycket minne
- Nytt är att SWAMID nu har stöd för att hämta metadata via Metadata Query Protocol vid behov istället för aggregat
  - Minnesmängd och starttid för SAML-klienterna minskar
  - SWAMID kommer att skapa dokumentation och hålla workshop i höst

SWAMID

Vill du veta mer?

- Det finns fler sessioner om SWAMID och närliggande tjänster under Sunetdagarna
- SWAMID har omfattande information på Sunets Wiki
  - https://wiki.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

SUNET