
SWAMID
Swedish Academic Identity Federation

SWAMID

Multifaktorinloggning via SWAMID

SWAMID Operations
Pål Axelsson, Sunet
Eskil Swahn, Lunds universitet

SUNET

SWAMID

Varför multifaktorinloggning via SWAMID?

- Lösenordsinloggning är alltmer utsatt för flera olika hot, t.ex. lösenordsfiske och lösenordstestning
- Datainspektionen har ställt krav på att endast avsedda mottagare ska kunna ta del av känsliga personuppgifter i det för lärosätena gemensamma systemet Nais
  - Datainspektionen exemplifierar uppfyllande med e-legitimation
  - Många anställda på lärosätena vill inte använda en privat e-legitimation i tjänsten

SWAMID

Vilka olika behov av inloggningsskydd finns?

- Lösenord (eller annan enskild faktor)
- Egenregistrerad multifaktor för att ta bort lösenordshoten
  - Identifiering enbart genom befintlig lösenordsinloggning
- Personverifierad multifaktor för att säkerställa att det är rätt person som loggar in
  - Organisationen/identitetsutgivaren kopplar multifaktorn till användaren
  - Identifiering via samma metoder som kontoutdelning för SWAMID AL2 eller
  - Identifiering via särskild identitetskontroll för att säkerställa rätt individ

Vad är Nais?

SWAMID

- *Nationellt administrations- och informations-system för samordnare*
- Ett nationellt konsortiebaserat system för handläggning av särskilt pedagogiskt stöd på universitet och högskolor
- Studenterna kan enkelt via systemet ansöka om stöd utifrån sin studiesituation
- Innehåller känsliga personuppgifter som är nödvändiga för att handlägga studenters ansökan om särskilt stöd
- **Nais kommer att för handläggare kräva personverifierad multifaktor med särskild identitetskontroll** *(troligtvis från 1 december 2018)*

SUNET

SWAMID

Egenregistrerad multifaktor

- Stärker inloggningen så att du vet att ingen annan använder ditt användarkonto
- Löses idag oftast genom att lösenordet kompletteras med en särskild autentiseringsapp i mobilen, s.k. Authenticator
- Finns idag i de större privata tjänsterna
  - Tvåstegsverifiering hos Google, tvåstegsverifiering i Office 365 och tvåfaktorsautentisering i Facebook
- eduID har stöd för detta genom standarden U2F
  - Proof of Concept vid Sunetdagarna i höstas, i drift sedan i fredags

SWAMID

Personverifierad multifaktor

- Stärker inloggningen så att den tjänst du loggar in i vet att det är du som loggar in
- SWAMID definierar i en särskild profil vilka krav som finns för personverifierade multifaktorer (ännu ej klar)
  - Organisationen och användaren måste vara godkänd för SWAMID AL2
  - Multifaktorn måste uppfylla vissa tekniska och säkerhetsmässiga krav
  - Att personverifierad multifaktor har använts signaleras via den internationella federativa standarden REFEDS MFA
  - Att särskild identitetskontroll har genomförts signaleras via attributet eduPersonAssurance (dvs som SWAMID AL1 resp SWAMID AL2)

SWAMID

Krav och rekommendationer för personverifierade multifaktorer i SWAMID?

SUNET

SWAMID

Vad innebär multifaktorinloggning?

För att logga in använder man inte bara lösenord utan en kombination av minst två av faktortyperna

- Något man vet
  - Exempel: Lösenord eller pinkod
- Något man har
  - Exempel: Google Authenticator, Yubikey och Smartcard
- Något man är *(endast i kombination med något man har)*
  - Exempel: Fingeravtryck och ansiktsigenkänning
- ~~Något man gör *(väldigt svår att använda på ett säkert sätt samt endast i kombination med något man har)*~~
  - ~~Exempel: Hur man skriver på tangentbordet och tittar på skärmen~~

SUNET

Krav på personverifierade multifaktorer i SWAMID

- Multifaktorn måste uppfylla minst samma nivå av inloggningssäkerhet som kraven i aktuell tillitsprofil men samtidigt tillföra ökat skydd
- Multifaktorn måste bindas till en fysisk enhet
- Multifaktorn får inte vara kopierings- eller kloningsbar
- Multifaktorn måste skyddas mot gissningsattacker
- Klientbaserade krypteringsnycklar måste lagras säkert i den enhet som hanterar multifaktorn
- Serverbaserade krypteringsnycklar, om de används, måste lagras säkert i verifieringsservern

SWAMID

Multifaktor men på olika sätt…

- Fullständig multifaktor
  - Multifaktorn består av något man har där användaren måste låsa upp användningen med en pinkod eller via fingeravtryck för att använda multifaktorn
- Kombinerad multifaktor (lösenord + andra faktor)
  - Användaren loggar in med användaridentitet och lösenord och kompletterar sedan med en fristående andra faktor av typen något man har

SWAMID

Exempel på fullständiga multifaktorer

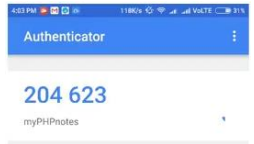
- Smartcard *(eller Personal Identity Verification (PIV) card)*
  - Det klassiska PKI-baserade inloggningskortet med kortläsare
  - Kräver kortläsare med koppling till datorn och särskild kontroll av att det är ett kort och inte på datorn lagrade certifikat som används
- Multifaktor OTP
  - Inloggningsservern skickar en kontrollkod till användaren som denne matar in på OTP-dosan tillsammans med sin personliga pinkod för att få en svarskod som användaren sedan skriver in på inloggningsservern

SWAMID

Exempel på den andra faktorn

- Universal 2nd Factor (FIDO U2F)

  - En liten hårdvarubaserad nyckel med hög säkerhetsnivå som aktiveras med enkel tryckning på nyckeln
  - Webbläsarstödet är f.n. begränsat till Chrome, Opera och Firefox (manuell aktivering) men Edge kommer att få stöd under året
- Tidsbaserad enfaktor OTP (TOTP)
  - Användaren installerar och konfigurerar en Authenticatorapp som visar en engångskod som ändras ofta (normalt var trettionde sekund)
  - Enkel för användarna att använda och förstå men Authenticator och inloggningsservern delar på en gemensam hemlighet



SUNET

SWAMID

Dåliga exempel på andra faktorn

- OTP via SMS
  - SMS kan idag dyka upp på fler enheter än den avsedda, t.ex. på mobiltelefonen och datorn samtidigt
  - SIM-kortet kan flyttas över till annan mobiltelefon
- Automatiserad uppringning
  - Telefonsamtal kan kopplas över till en eller flera telefoner

Får absolut inte användas för personverifierad multifaktor

SWAMID

Hur kräver och kontrollerar en webbtjänst personverifierad multifaktorinloggning i SWAMID?

SUNET

Hur begär en tjänst personverifierad multifaktorinloggning?

SWAMID

Tjänsten begär i sin inloggningsförfrågan

- att personverifierad multifaktorinloggning ska används
  - I Shibboleth SP sätter man authnContextClassRef=”https://refeds.org/profile/mfa” i SAML2 SessionInitiator
- att ny inloggning ska genomföras, dvs. inte lita på SSO
  - I Shibboleth SP sätter man ForceAuthn=”true” i SAML2 SessionInitiator

Alternativt direkt via URL i en webbserver som använder Shibboleth SP:
https://sp.example.org/Shibboleth.sso/Login?forceAuthn=true&authnContextClassRef=
https%3A%2F%2Frefeds.org%2Fprofile%2Fmfa&target=https%3A%2F%2Fsp.example.org%2FservicePage

Hur kontrollerar en tjänst att personverifierad multifaktorinloggning har genomförts? 1(2)

SWAMID

Tjänsten kontrollerar efter lyckad inloggning

- att multifaktor har använts för inloggningen
  - Med Shibboleth SP och Apache kontrollera Shib-AuthnContext-Class==”https://refeds.org/profile/mfa”
- att identitetsutfärdaren uppfyller kraven för SWAMID AL2
  - Med Shibboleth SP konfigurera att metadata för assurance certification hämtas upp som ett attribut
  - Kontrollera sedan att detta attribut innehåller ”http://www.swamid.se/policy/assurance/al2”
  - samt vid behov kraven för särskild identitetskontroll för MFA
    - Kontrollera sedan att detta attribut innehåller värdet för att lärosätet hanterar identitetsverifierad MFA

…

Hur kontrollerar en tjänst att personverifierad multifaktorinloggning har genomförts? 2(2)

SWAMID

Tjänsten kontrollerar efter lyckad inloggning

...

- att inloggningen är ny (max 60 sekunder plus definierad max klockdrift)
- att användaren uppfyller kraven för SWAMID AL2
  - Kontrollera sedan att attributet eduPersonAssurance innehåller värdet ”http://www.swamid.se/policy/assurance/al2”
  - samt att vid behov kraven för särskild identitetskontroll för MFA
    - Kontrollera sedan att attributet eduPersonAssurance innehåller värdet för att användaren använder identitetsverifierad MFA

Notera att SWAMIDs identifierare för identitetsverifierad MFA ännu ej är definierad

SUNET

SWAMID

Vad är nästa steg?

SUNET

Vad är på gång nu?

SWAMID

- SWAMID Operations håller på att skriva en formell profil för personverifierad multifaktorinloggning i SWAMID
  - Denna profil bygger på det som presenterats idag och kommer att skickas ut för diskussion innan slutet av april
- SWAMID Operations har intentionen att ta fram en exempelinstallation baserad på TOTP och Shibboleth IdP
- eduID kommer att fram en lösning för personverifierad multifaktor med hjälp av FIDO U2F *(se nästa presentation)*

SWAMID

Swedish Academic Identity Federation

SWAMID