
SWAMID
Swedish Academic Identity Federation

SWAMID

Webinar 2018-05-24
Profil för 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

SWAMID

Vad innebär multifaktorinloggning?

För att logga in använder man inte bara lösenord utan en kombination av något man har plus ytterligare en faktortyp

- Något man har
  - Exempel: Authenticator app i mobilen, Yubikey och Smartcard
- Något man vet
  - Exempel: Lösenord eller pinkod
- Något man är
  - Exempel: Fingeravtryck och ansiktsigenkänning
- ~~Något man gör~~ ~~*(väldigt svår att använda på ett säkert sätt)*~~
  - ~~Exempel: Hur man skriver på tangentbordet, hur man tittar på skärmen och var man finns någonstans~~

SUNET

SWAMID

Multifaktor men på olika sätt…

- 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
- Fullständig multifaktor
  - Multifaktorn består av något man har där användaren måste låsa upp användningen med en pinkod eller via fingeravtryck för att använda multifaktorn

SWAMID

Egenregistrerad multifaktor

- Stärker inloggningen så att du som användare vet att ingen annan använder ditt användarkonto
- Löses idag oftast genom att lösenordet kompletteras med en särskild autentiseringsapp i mobilen, s.k. Authenticator, eller SMS
- Finns idag i de större privata tjänsterna
  - Tvåstegsverifiering hos Google, tvåstegsverifiering i Office 365, tvåfaktorsautentisering i Facebook, inloggningsverifiering på Twitter och säkerhetsnyckel i PayPal
- eduID har stöd genom standarden FIDO U2F (hårdvarunyckel)
  - Fungerar f.n. endast med Chrome och Opera samt till viss del i Firefox

SWAMID

Personverifierad multifaktor

- Stärker inloggningen så att den tjänst du loggar in i vet att det är du som loggar in
- Särskild profil i SWAMID om vilka krav som finns för personverifierad multifaktor
  - Organisationen och användaren måste vara godkänd för SWAMID AL2
  - Två nivåer, SWAMID AL2 resp SWAMID AL2 med explicit identitetskontroll
  - Multifaktorn måste uppfylla vissa tekniska och säkerhetsmässiga krav
  - Att personverifierad multifaktor har använts signaleras via den internationella federativa standarden REFEDS MFA

SWAMID

Förslag till profil för personverifierad multifaktorinloggning I SWAMID

SUNET

Vad innebär den nya profilen?

SWAMID

- Både användare och organisation måste vara godkända för tillitsprofilen SWAMID AL2
- Inloggning måste ske med hjälp av mer än en faktortyp
  - Något man vet + något man har, alternativt
  - Något man är + något man har
- Hantering av multifaktor (andra faktor eller full multifaktor) måste ske så att organisationen är säker på rätt person har fått multifaktorn
  - Det räcker inte med att användaren endast loggar in med lösenord för att registrera en multifaktor (egenregistrerad multifaktor)

Profilens begränsningar

SWAMID

- Hanterar endast personverifierad multifaktorinloggning
- All inloggning måste *inte* ske med multifaktor utan den tjänster som kräver personverifierad multifaktorinloggning kräver det vid inloggning
- Alla användare inom organisationen behöver *inte* använda personverifierad multifaktorinloggning utan endast de som använder tjänster som kräver det
- Innehåller inga krav runt Single-Sign On (SSO) men en tjänst kan alltid kräva ny inloggning vid åtkomst till tjänsten

Säkerhetsmässiga krav på personverifierade multifaktorer i SWAMID 1(2)

SWAMID

- Profilen använder definitionerna i NIST 800-63B för att definiera vilka multifaktorer som är godkända inkl. andra säkerhetskrav
- Lösenord + andra faktor
  - Single-Factor OTP Device, *exempel Google Authenticator och Microsoft Authenticator med OTP*
  - Single-Factor Cryptographic Software, *exempel FIDO2 (WebAuthn + CTAP)*
  - Single-Factor Cryptographic Device, *exempel U2F och FIDO2 (WebAuthn + CTAP)*
- Full multifaktor
  - Multi-Factor OTP Device
  - Multi-Factor Cryptographic Software
  - Multi-Factor Cryptographic Device, *exempel traditionellt inloggningskort med pinkod (smart card)*

Säkerhetsmässiga krav på personverifierade multifaktorer i SWAMID 2(2)

SWAMID

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

Dela ut multifaktor till rätt person

SWAMID

- Den andra faktorn eller den fulla multifaktorn måste kopplas till rätt person med mer än bara lösenordsinloggning
- Profilen innehåller två nivåer
  - SWAMID AL2-MFA – Samma metoder som för SWAMID AL2
  - SWAMID AL2-MFA-HI – Kräver att identitetskontroll görs
- En person kan ha fler än en andra faktor eller full multifaktor kopplad till sig men alla bör vara verifierade på samma nivå

Byta, lägga till eller ta bort multifaktor

SWAMID

- Användare måste kunna byta ut sin multifaktor
  - Självservice genom att använda multifaktor
  - Genom att först ta bort nuvarande multifaktor och därefter få en ny enligt definierade rutiner för utdelande av multifaktor
- Användarens multifaktor måste gå att ta bort ifrån användaren antingen beroende på den inte längre ska användas eller om det inträffat en säkerhetsincident med multifaktorn inblandad

SUNET

Inloggning med multifaktor med stöd av profilen

SWAMID

- SP kräver inloggning med multifaktor genom att signalera i REFEDS MFA i authnContextClassRef
- IdP signalerar att inloggning skett med multifaktor genom att ange REFEDS MFA i authnContextClass
- Om multifaktorinloggningen uppfyller kraven för SWAMID AL2-MFA-HI signaleras detta genom tillägg av värde i eduPersonAssurance
- SP kontrollerar sedan att alla krav den har för inloggningen uppfylls av användaren och dess IdP

SWAMID

Exempel på användning av profilen

SUNET

Exempel 1 på användning av denna profil

Systemet Nais hanterar känsliga personuppgifter för studenter med särskilda behov

- *Nais kräver att organisationen är godkänd för SWAMID AL2*
- *Nais kräver att användaren är godkänd för SWAMID AL2*
- Nais kräver att organisationen är godkänd för SWAMID AL2-MFA-HI
- Nais kräver att användaren är godkänd för SWAMID AL2-MFA-HI
- Nais kräver att inloggning skett med multifaktor
- Nais kräver att ny inloggning har genomförts i samband med inloggning i Nais, dvs åsidosätta SSO (återautentisering)

Exempel 2 på användning av denna profil

SWAMID

Forskningslagring kräver att det är rätt person som loggar in

- Systemet kräver att organisationen är godkänd för SWAMID AL2-MFA
- Systemet kräver att användaren är godkänd för SWAMID AL2-MFA
- Systemet kräver att inloggning skett med multifaktor
- Systemet kräver *inte* att ny inloggning har genomförts i samband med inloggning i systemet

SUNET

SWAMID

Frågor och diskussion…

SUNET

SWAMID

Swedish Academic Identity Federation

SWAMID