SWAMID

Swedish Academic Identity Federation

Multifaktorinloggning i SWAMID

En kort introduktion samt vad säger SWAMIDs policy ramverk

SWAMID

Vad betyder multifaktorinloggning?

- Vid inloggning använder användaren minst två olika oberoende faktortyper varav den ena är alltid något man har.
- Multifaktortyper
  - Något man vet – Kunskap (eng. Knowledge)
  - Något man har – Besittning (eng. Possession)
  - Något man är – Medfött (eng. Inherence, aka. Biometri)
- Ej äkta multifaktortyper
  - Lokalisering och tid (eng. Location and time)
  - Kan endast användas för filtrering ej som enskild faktor

SWAMID

Olika sätt för att få säker inloggning

- Full multifaktor – En besittningsfaktor som kräver en kunskapsfaktor eller biometrifaktor för aktivering
  - Exempel är Smartcard
- Kombinerade multifaktor – En besittningsfaktor utan ytterligare krav för aktivering som används tillsammans med fristående kunskapsfaktor eller biometrifaktor
  - Exempel är Yubikey plus lösenord
- Federerad multifaktor – Använder multifaktor hos annan tjänst
  - Exempel är eduID och Freja eID+

SWAMID

Mitt lärosäte och multifaktorinloggning?

- De flesta lärosäten använder idag en enklare form av multifaktorinloggning för att skydda e-post och andra tjänster från stöld av användarkonton
- Denna enklare form uppfyller inte alltid kraven som ställs vid säker inloggning men fungerar som lösenordsförbättrare
- Säker inloggning innebär i korthet
  - Kryptografiskt säker
  - Ej flytt- eller kopieringsbar mellan enheter
  - Inbyggt skydd mot nätfiske och socialt bedrägeri

SWAMID

eduID som multifaktorinloggning

- eduID stödjer idag inloggning via två enskilda faktorer där den ena är lösenord och den andra är en säker kryptografisk nyckel som antingen lagras på en fysisk säkerhetsnyckel eller en säkerhetsnyckel lagrad säkert i enhetens säkerhetsmodul
  - Exempel på fysisk nyckel är YubiKey
  - Exempel på nyckel i säkerhetsmodul är Passkey
- En användare kan ha en eller flera registrerade säkerhetsnycklar
- Som backup för säkerhetsnyckel kan även inloggning via Freja eID+ användas
  - Används även vid registrering och återställning av säkerhetsnyckel

SWAMID

SWAMIDs regelverk och MFA

SWAMID

MFA i SWAMIDs tillitsprofiler

- Tillitsprofilerna AL1 och AL2 tillåter att MFA används (5.1.1)
- Tillitsprofilen AL3 kräver att MFA används (5.1.1)
- Inloggningsfaktorer ska vara oberoende, dvs. det går inte att använda enbart den ena för att återställa den andra (5.1.1)
  - Vid första etablering av MFA är det ok att använda enbart lösenordet för inloggning
- Användarreglerna måste innehålla tydlig uppmaning att användarna inte får låna ut sin MFA till någon annan (5.1.3)
  - Samma krav som för lösenord
- MFA måste delas ut enligt samma krav som för kontoaktivering (5.2.5)
- Byte av MFA måste tillåtas (5.3.1 – 5.3.2)
  - Manuella administrativa rutiner via personligt besök tillåts
- MFA måste kunna återställas och spärras (5.3.3 & 5.4.2)

Glöm inte att uppdatera IMPS!

SWAMID

Begränsning av MFA-metoder

- I avsnitt 5.1.1 i tillitsprofilerna finns det definierat vilka typer av MFA-metoder som är godkända för signalerad MFA i SWAMID
- Inom SWAMID godkänns inte SMS, motringning och appar som endast visar knapp för att acceptera inloggning
  - Skyddar bra mot lösenordsfiske men inte socialt bedrägeri
- Inom 2-5 år kommer högre krav på skydd mot socialt bedrägeri (nätfiskeresistentare multifaktorinloggning)
  - Sexsiffriga OTP-koder och push begäran om sifferkod blir ej ok
  - Avvaktar nya möjligheter i ADFS genom MFA med hjälp av Azure

SWAMID

MFA i teknologiprofilen SAML WebSSO

- Om multifaktorinloggning begärs av en tjänst måste den genomföras med någon av de metoder som finns definierade i avsnitt 5.1.1 i SWAMIDs tillitsprofiler (5.4.5)
  - Begäran av multifaktorinloggning sker via RequestedAuthnContext i inloggningsbegäran (5.4.4)
  - Om IdP inte kan hantera begärd RequestedAuthnContext får inte inloggning genomföras (5.4.6)
  - IdP måste skicka tillbaka använd AuthnContext i inloggningssvaret till tjänsten (5.4.7)
- Om tjänsten begär ny inloggning via ForceAuthn måste fullständig ny inloggning genomföras, inte bara med en av faktorerna (5.4.9)
  - Vid ny inloggning måste AuthnInstant sättas till aktuell tidpunkt (5.4.8)

SWAMID

Begäran och signalering av MFA

SWAMID

MFA-signalering via REFEDS MFA-profil

- SWAMID använder REFEDS MFA Profile för att signalera krav på MFA-inloggning (https://refeds.org/profile/mfa)
- En tjänst begär MFA via värdet https://refeds.org/profile/mfa i AuthnContextClassRef i RequestedAuthnContext
  - Tjänsten kan begära mer än en metod för inloggning t.ex. https://refeds.org/profile/mfa och PasswordProtectedTransport
  - Endast en av metoderna ska användas och det finns ingen inbördes ordning även om det rekommenderas att man går i listans ordning
- IdP får endast använda begärda metoder och måste svara i AuthnContextClass vilken som använts

SWAMID

Single Sign-On eller inte?

- I SWAMIDs till federationsramverk finns ignet krav på att en ny multifaktorinloggning ska genomföras utan det är upp till tjänsten att begära detta
- Begäran om åsidosättande av Single Sign-On görs av tjänsten via att sätta parametern ForceAuthn till 1 eller true vid inloggningsbegäran
- Om ForceAuthn begärs måste inom SWAMID en fullständig inloggning ske, inte bara en av faktorer vid multifaktorinloggning

SWAMID

Frågor och kommentarer?

SWAMID

Nu börjar hackatonet!

SWAMID

SWAMID

Swedish Academic Identity Federation