Arbetsplan för MFA i Nais

Vem gör vad?

För att multifaktorinloggning i Nais ska fungera genom SWAMID behöver SWAMID och lärosätena göra förändringar i sina infrastrukturer för identitetshantering. Det behöver även göras ändringar i Nais för att tekniskt kräva och därefter kontrollera de högre inloggningskraven.

Vad ska SWAMID göra

1. SWAMID kommer att följa REFEDS Multi-Factor Authentication (MFA) Profile som teknikprofil för regelverket runt personverifierad multifaktorinloggning. SWAMID Operations kommer dock att komplettera teknikprofilen med regelverk om vilka utdelningsmetoder och vilka säkerhetsfaktorer som SWAMID Operations bedömer uppfyller REFEDS Multi-Factor Authentication (MFA) Profile baserat på svenska förhållanden.
2. SWAMID kommer att införa en tillitsmarkering i metadata som indikerar att en identitetsutgivare (IdP) uppfyller de funktionella och tekniska kraven för att genomföra en korrekt autentisering med multifaktoinloggning enligt SWAMIDs regelverk för personverifierad multifaktorinloggning där multifaktorn har tillhandahållits användaren i samband med identitetskontroll med godkänd identitetshandling.
3. SWAMID kommer att tillhandahålla en teknisk valideringstjänst för att administratörer av en identitetsutgivare ska kunna validera att de tekniskt uppfyller SWAMIDs regelverk för personverifierad multifaktorinloggning.
    - Valideringstjänsten kommer att finnas på adressen https://mfa-check.swamid.se/.
4. SWAMID kommer att tillhandahålla instruktioner för hur tjänsteleverantör (SP) ska implementera stöd för personverifierad multifaktorinloggning.

Vad ska ett lärosäte göra

1. Lärosätet måste vara godkänt för tillitsprofilen SWAMID AL2 (observera som vanligt att alla användare inte måste uppfylla kraven utan man kan ha användare som är SWAMID AL2 och andra som är SWAMID AL1 inom samma lärosäte, för mer information se SWAMID Identity Assurance på SWAMIDs wiki).
2. Lärosätet måste vara godkänt för SWAMIDs regelverk för personverifierad multifaktorinloggning där den andra faktorn, alternativt hela multifaktorn, har tillhandahållits i samband med identitetskontroll.
3. Lärosätet måste implementera multifaktorinloggning i sin identitetsutfärdare baserat på SWAMIDs regelverk för multifaktorinloggning.
4. Lärosätet måste i sin identitetsutfärdare stödja krav på återautentisering (eng. Re-Authentication, forceAuthn i SAML2 Service Provider Request Initiation Protocol and Profile) för tjänster som kräver multifaktorinloggning.
    - SWAMIDs instruktioner för hur tjänster ska implementera multifaktorinloggning kommer att ställa krav på återautentisering för att starta och avsluta en inloggningssession på ett säkert sätt.

Om inte lärosätet av en eller annat skäl kan genomföra det som de måste göra innan kravet på multifaktor i Nais kommer att införas kommer Sunets tjänst eduID tillhandahålla multifaktorinloggning men då måste användaren använda ett eduID-konto för att logga in i Nais.

Vad ska UHR göra i Nais

1. Nais får endast hantera inloggning via SAML2, inte äldre versioner av SAML.
    - Både krav på multifaktor och återautentisering går endast att utföra med SAML2.
2. I inloggningsförfrågan från Nais till ett lärosätes identitetsutfärdare (IdP) ska Nais ställa krav på:
    a. att användare måste logga in med multifaktor genom att tekniskt signalera krav på REFEDS-MFA för inloggningen och
    b. att användaren måste logga in på nytt oberoende om denna redan sedan tidigare hade en giltig inloggning i identitetsutfärdare n (IdP) eller inte.
3. När godkänd inloggning är genomförd ska Nais tekniskt kontrollera följande innan användaren släpps in i Nais:
    a. att lärosätet uppfyller kraven för SWAMID AL2,
    b. att lärosätet uppfyller kraven för SWAMID AL2-MFA-HI,
    c. att användaren uppfyller kraven för SWAMID AL2,
    d. att användaren uppfyller kraven för SWAMID AL2-MFA-HI,
    e. att inloggningen i lärosätets identitetsutfärdare (IdP) har skett med multifaktor via REFEDS MFA och
    f. att inloggningen i lärosätets identitetsutfärdare (IdP) inte är äldre än 1 minut (plus utrymme för klockdrift).