

Nais

Införande av multifaktorinloggning(MFA)



Kort presentation Nais

Nationellt informations- och administrationssystem för samordnare av pedagogiskt stöd

Om Nais

- Nais stödjer den verksamhet som arbetar med pedagogiskt stöd till studenter med funktionsnedsättning/funktionsvariation
- Nais är ett nationellt system. Varje lärosäte äger och ansvarar dock för det egna lärosätets personuppgifter, och kan inte ta del av ett annat lärosätes uppgifter
- 33 högskolor och universitet i Sverige använder Nais
- I Nais hanteras ca. 8000 ansökningar per år
- Huvudsakliga användare i Nais:
 - Studenter med behov av pedagogiskt stöd vid studier
 - Samordnare för pedagogiskt stöd på lärosätena

Bakgrund till beslut om införande av MFA

Nais

Bakgrund till beslut om införande av MFA

- 2016 inkom ett klagomål till Datainspektionen (DI) gällande Nais. DI beslutade mot bakgrund av klagomålet att inleda ett tillsynsärende.
- I juni 2017 konstaterade DI i ett beslut bl.a. att Nais ”inte uppfyller säkerhetskraven i 31§ personuppgiftslagen beträffande åtkomst till känsliga personuppgifter över öppet nät”.
- DI konstaterade också att man bör införa ”stark autentisering vid åtkomst till uppgifterna i Nais”, vilket innebär både säker inloggning via multifaktor och att multifaktorn är tilldelad till användaren mot legitimationskontroll.

Bakgrund till beslut om införande av MFA

- En åtgärdsplan tog fram med anledning av beslutet
- Av åtgärdsplanen framgick bl.a att frågan gällande MFA för Nais skulle utredas under 2017 och att införande skulle ske under 2018
- UHR kontaktade SWAMID Operations för att diskutera ett samarbete och för att ta fram ett lösningsförslag gällande MFA för Nais

Bakgrund till beslut om införande av MFA

- Styrgruppen för Nais tog i januari 2018 beslut om att införa MFA för samordnare och administratörer vid inloggning i Nais under 2018
- Man beslutade sig för två olika sätt att logga in:
 - Inloggning via eduID med säkerhetsnyckel
 - Säkerhetsnyckeln och användarens identitet måste bekräftas med Freja eID+
 - Lärosätets egna MFA-anpassade IdP

Införandeprojektet

Nais

Införandeprojektet

- UHR och Sunet träffades kontinuerligt under 2018 för att diskutera
 - Testmiljö och teknisk rådgivning för anpassning av lärosätenas IdP:er
 - Nödvändiga förändringar för att anpassa Nais
 - Tidsplan och införandedatum
 - Information till lärosätena om det nya inloggningsförfarandet:
 - till IT- och SA-chefer
 - till samordnare och administratörer
- Beslut om att skjuta på införandet till första kvartalet 2019
 - I oktober 2018 beslutade styrgruppen för Nais att skjuta på införandet till första kvartalet 2019
 - undvika ett införande under december något som inte skulle vara optimalt för verksamheten
 - ha möjlighet att informera/demonstrera hur man skapar eduID-konto och verifierar sig själv och sin säkerhetsnyckel på den utbildningsdag för Nais som hölls i februari 2019

Anpassning av Nais

Emil Nikander, utvecklare, konsult från Netlight

Anpassning av Nais

- Uppdatering av Shibboleth SP programvara till senaste version 3.
- Anpassning av inloggningen genom att separera inloggningsförfarande för studenter och övrig personal i Shibboleth2.xml.
- Checkar av nya attribut som Nais kräver att en IDP skickar med för att verifiera att både användaren tillsammans med IDP uppfyller kraven för multi faktor autentisering.
- Tidsvalidering för att säkerställa att en inloggningen som tar för lång tid till systemet inte ska godkännas.
- Ny felhantering vid olika typer av scenarios där ovanstående krav inte är uppfyllda.

Reflektioner från införandet

Nais

Reflektioner från införandet

- Framgångsrikt med korta kontaktvägar mellan Sunet och UHR under hela införandeprojektet
- Viktigt med utförliga manualer till samordnare och administratörer för att skapa eduID-konto och lägga till säkerhetsnyckel
- Bra med lång tid för samordnare och administratörer att gå igenom processen för att skapa eduID-konto (och verifiera sig själv och säkerhetsnyckel) i kombinationen med flera påminnelser
– (hela processen går på en dag)
- Viktigt med direkt support från UHR under införandedagen
- Att Sunet köpte in säkerhetsnycklar som distribuerades till lärosätena av UHR = smidigt för UHR och lärosätena
- Fundering: UHR borde kanske ha haft tillgång till en egen stagingmiljö för eduID. UHR:s utvecklare använde sig av samma stagingmiljö som eduID:s utvecklare använde.

Frågor?

Nais

Tack!
www.uhr.se