MFA i Nais

Krav på multifaktorsinloggning för Nais

Nais är ett ärendehanteringssystem där studenter med en varaktig funktionsnedsättning kan ansöka om att få särskilt pedagogiskt stöd i sina studier vid svenska universitet och högskolor. Systemet underlättar det administrativa och personalkrävande arbetet för lärosätena kring dokumentation och kommunikation med studenterna. Nais används av 32 lärosäten i Sverige.

Datainspektionen (DI) har i ett tillsynsärende (dnr 2407-2016) kring Nais och BTH bl a konstaterat att Nais ”inte uppfyller säkerhetskraven i 31§ personuppgiftslagen beträffande åtkomst till känsliga personuppgifter över öppet nät”. DI förelägger därför BTH att ”vidta åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av personuppgifter i Nais, exempelvis genom att använda e-legitimation för samtliga användare som har åtkomst till uppgifter som rör studenternas personliga förhållanden via internet.” DI resonerar vidare kring kravet: ”När sådana personuppgifter kommuniceras via internet ska den personuppgiftsansvarige därför använda stark autentisering vid åtkomst till uppgifterna, exempelvis e-legitimation, engångslösenord eller motsvarande.” Observera att detta krav gäller samordnare och administratörer. Studenter omfattas inte av detta krav.

För mer information se utskick till SA- och IT-chefer vid aktuella lärosäten och Tillsyn enligt personuppgiftslagen (1998:204) - angående behandling av personuppgifter i Nais.

Status:

- 2018-03-25: SWAMID har tagit fram en testtjänst för att identitetsutgivare ska kunna testa sin implementation av personverifierad multifaktorinloggning - https://mfa-check.swamid.se/
- 2018-09-12: SWAMID har tagit fram en policy för personverifierad multifaktorinloggning via SWAMID - https://www.sunet.se/swamid/policy/al2mfa/
- 2018-12-03: eduID har driftsatt stöd för personverifierad säkerhetsnyckel som andra faktor vid inloggning.
- 2019-03-13: UHR slog på kravet för personverifierad multifaktorinloggning i Nais.

Sunet och UHR samarbetar

För att logga in i Nais använder handläggare och administratörer sina lärosätesinloggningar via SWAMID. UHR och Sunet samarbetar därför för att få en lösning på plats för förhöjd inloggningssäkerhet i Nais. På dessa wikisidor kommer vi att presentera resultatet av detta arbete.

I Datainspektionens tillsyn ställs krav på att säkerställa att endast avsedda mottagare av ärendena som ska handläggas kan ta del av dem. För att uppnå detta genom SWAMID kommer Nais att ställa följande krav vid handläggares inloggning:

1. Inloggning sker med hjälp av i SWAMID definierad profil för personverifierad multifaktorinloggning där andra faktorn, alternativt hela multifaktorn, har tillhandahållits användaren i samband med kontroll av godkänd identitetshandling.
2. Inloggningen i identitetsutgivaren måste ske samtidigt som användaren vill logga in i Nais, dvs. åsidosättande av Single Sign On.
3. Användaren som loggar in i Nais måste uppfylla kraven för tillitsprofilen SWAMID AL2, även känt som bekräftad användare.