Utdannings-
direktoratet

Sterk autentisering i skolesektoren?

KiNS-konferansen - 21.04.2022

Feide med sterk autentisering

- *Status siden 21.10.2021*
- *Planer for veien videre*

Rune Nordang/Seniorrådgiver – Udir/Avdeling Digitale fellesløsninger 2

Sikker og trygg deling av data i skolesektoren!

Hva er status etter KiNS-konferansen i oktober 2021?

Status aktivering - **sterk autentisering** for Feide

21.10.2021		Per 11.04.2022
136 av 356 **kommuner**		**229** av 356 **kommuner**
5 av 11 **fylkeskommuner**		**10** av 11 **fylkeskommuner**
47 av 346 **friskoler***		**99** av 346 **friskoler***

*Alle kommuner og fylkeskommuner bruker Feide, mens **239** av totalt 346 privatskoler har tatt i bruk tjenesten per 19.04.2022.

Planer for veien videre

Sterk autentisering i Feide idag:

Innloggings-/autentiseringsprosessen:

- Hvordan vet du at den som logger inn er den samme som fikk utlevert innloggingsopplysningene?
  - Lav: brukernavn og en faktor, ofte passord
  - Betydelig: en tilleggsfaktor, ofte en engangskode, nøkkel e.l.

Utleveringsprosessen:

- Hvor vet du at den som fikk utlevert innloggingsopplysningene er den som *faktisk* skulle ha dem?
  - Lav: Anta at det er riktig person
  - Betydelig: Kontrollere at det er riktig person (forenklet)

I dag må begge aksene være oppfylt for å oppnå et nivå.

- Vurderer å splitte opp innloggings-/autentiseringsprosessen og utleveringsprosessen i to separate verdier.
- Vurderer å støtte sikkerhetsnivå 4/Høyt (gjennom eksterne ID-løsninger). Om du bruker ID-porten, vil du kunne autentisere deg på nivå 4/høy der, men i og med at Feide ikke støtter 4/høy ennå, så anser vi det som en innlogging på nivå 3/betydelig.

Planer for veien videre

eID-strategi

Digdir

digdir.no

Behov for økt utbredelse av eID og tilgang til offentlige digitale tjenester for unge

UTFORDRING

Unge har utfordringer med å utstedt eID på høyt sikkerhetsnivå og mangler derfor tilgang til offentlige tjenester som de har rett til

KONSEKVENSER OG UTDYPNING

- Manglende eID på høyt sikkerhetsnivå gjør at unge ikke får tilgang til digitale helsetjenester som de har rettigheter til og at de ikke kan benytte disse tjenestene uten innsyn fra foreldre
- Generell lav utbredelse av eID blant unge er til hinder for lansering av nye tjenester
- Lav sikkerhet i Feide utgjør en risiko, også med tanke på potensiell anvendelse utenfor utdanning
- Unge har i dag Feide fra ung alder, men må anskaffe andre eID-er for å få tilgang til andre digitale offentlige digitale hvilket oppleves som lite sømløst

Unge brukeres alder

6 år	13 år	13/15 år	15 år
• Kommunen utsteder Feide til unge i grunnskolen • Feide benyttes for tilgang til skolesystemer og læringsmateriale Feide	• MinID utstedes kan bestilles av unge fra det året de fyller 13 år • MinID brukes av unge ved søknad til videregående skole MinID	• Unge kan få utstedt BankID og Buypass fra de 13 år gamle • Enkelte banker har en aldersgrense på 15 år for utstedelse av BankID bankID buypass	• Fylkeskommunen utsteder en ny Feide til unge i videregående skole • Tilsvarende funksjonalitet som Feide i grunnskolen Feide

Behov

- Unge har behov for brukervennlige, mobile og tilgjengelige eID-løsninger og en sømløs tilnærming til eID gjennom livet
- Det er behov for økt utbredelse av eID til unge slik at de kan få tilgang til tjenester de har krav på og opptre som digitale borgere

Planer for veien videre

eID-strategien – del II

Andre innspill og behov identifisert i behovsanalysen

Videføring av Feide-kvaliteter

- Innen utdanningssektoren pekes det på behov for å beholde Feide som løsning for elever og lærere da den oppleves å fungere godt til formålet den har i dag
- Eventuelle forbedringer og endringer i eID for ansatte må være kompatible med Feide, slik at eksisterende kvaliteter videreføres

Økt sikkerhet ved bruk av eID

- Flere virksomheter trekker frem et behov for å øke sikkerheten ved bruk av eID, eksempelvis ved innføring av sikkerhetssupplerende løsninger som kreves ved for eksempel låneopptak
- Eksempler på sikkerhetssupplerende løsninger som er foreslått er økt interaksjon og ytterligere kontroll mellom usteder og eier av eID, mulighet for bruker til deaktivere eID-en i en periode

Virksomhetsautorisasjon

- Innen helsesektoren pekes det på et stort behov for virksomhetssertifikater for sikring av API-er mellom applikasjoner i ulike virksomheter, eksempelvis når en helseansatt jobber i på tvers av flere ulike systemer i løpet av en dag
- Videre trekkes kryptering og signering av elektronisk meldingsutveksling frem som et behov, da det er viktig å sikre sensitivt informasjonsinnhold som sendes

TILGJENGELIGE METODER FOR STERK AUTENTISERING

Engangspassord på SMS

- Sluttbruker må benytte mobiltelefon til å motta engangspassord ved innlogging.
- Vertsorganisasjonen belastes de løpende kostnadene Feide har ved å sende ut SMS til brukere ved vertsorganisasjonen.
- Rutine for registrering må verifisere at oppgitt mobilnummer tilhører sluttbruker.

Kode via godkjenner-applikasjon

Sluttbruker må benytte en klient som støtter en bestemt implementasjon av tidsbaserte engangspassord, kalt Godkjennerklient, f.eks.

- 1Password
- Duo Mobile
- Google Authenticator
- Microsoft / Azure Authenticator
- Yubico Authenticator med YubiKey

Det er ingen løpende kostnader knyttet til bruken av denne metoden. Rutine for registrering må sørge for at hemmelig nøkkel blir lagt inn på sluttbrukerens klient

ID-porten

Alle metodene benyttet av ID-porten støttes automatisk.

Vertsorganisasjonen belastes de løpende kostnadene Feide blir viderefakturert av Digitaliseringsdirektoratet for innlogginger ved vertsorganisasjonen som gjøres via ID-porten.

Feide-innlogging med AzureAD

Gjør det mulig å benytte Microsoft-konto til å logge på tjenester som bruker Feide som innloggingsløsning. Merk: Krever lokal LDAP for Feide.

Piloter

Flere metoder for sterk autentisering vil komme

- Ansattporten for offentlig sektor
- MFA gjennom Google Workspace

Sikker innlogging og datadeling!