Utdannings-
direktoratet

Utdannings-
direktoratet

MFA i skolen, hvorfor så mye støy!

Feide for grunnskolen

Hva tilbyr Feide av sterk autentisering og hva gjør Feide for å møte dagens og fremtidige behov på dette feltet?

Øystein Larsen/IT-sikkerheitsansvarlig, Utdanningsdirektoratet
Rune Nordang/Senior rådgiver – Udir/DIF1/Feide

Feide for grunnskolen

Hva tilbyr Feide av sterk autentisering og hva gjør Feide for å møte dagens og fremtidige behov på dette feltet?

Hva er sterk autentisering i Feide?

- Gjenbruker kriteriene som benyttes i resten av offentlig sektor
  - Rammeverk for autentisering og uavviselighet i og med offentlig sektor (FAD2008)
  - eIDASs identifikasjonsnivåforskrift (EU2015)

- Siden 2016 støtter Feide sikkerhetsnivå 2/Lav og 3/Betydelig
- Vurderer å støtte sikkerhetsnivå 4/Høyt (gjennom eksterne ID-løsninger)

Hva er sterk autentisering i Feide?

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. Feide vurderer å splitte de opp i to separate verdier.

Hvorfor sterk autentisering for Feide?

- Fordi **passord ikke er godt nok**!
- **Sikre brukersituasjon** – et **passord kan fanges opp** av andre rundt deg der du logger på tjenester (klasserom/grupperom, «kikke-over-skuldra» osv.
- **Samme passord** brukes ofte **på flere tjenester** – samme **mønster** i bruk av passord.
- **Passord på avveie** som følge av **lekkasje** fra andre steder hvor passordet brukes, **skadevare** på PC som plukker opp brukernavn og passord, «**man-in-the-middle»-angrep** og **phising** (angriper som lurer brukeren til å utføre en handling)

TO-FAKTOR-AUTENTISERING ER EN MYE SIKRERE LØSNING OG KONSEKVENSENE VED AT BRUKERNAVN OG PASSORD KOMMER PÅ AVVEIE ER LANGT MINDRE!

Hvorfor sterk autentisering for Feide?

FORDI

- Styrke sikkerheten rundt identitetsbekreftelsen – gi deg sikkerhet for at det er bare du som når de tjenestene du skal ha tilgang til og som gir deg tilgang til dine data/informasjon om deg.

METODER

- **Passord** - eksempel på noe du **VET / Kjennskapsfaktor**
- **Bankkort** - eksempel på noe du **HAR / Besittelse**
- **Fingeravtrykk** – eksempel på noe du **ER / Iboende**

HVORFOR ER DETTE VIKTIG VED BRUK AV FEIDE?

- Mange ulike brukergrupper og flere blir det! Og ulike brukersituasjoner utfordrer sikkerheten!
- Vertsorganisasjoner og risikovurderinger – hvor sikkerhet inngår som et sentralt område i ROS-analysen. Sikre brukerne mot at uvedkommende får tilgang til tjenesten og at brukerne har trygghet på innsiden.

Hvorfor **sterk autentisering** for Feide?

Hvilken løsning kan man velge?

- Det legges ikke føringer fra Datatilsynet hvilken løsning man velger, så lenge sikkerheten blir ivaretatt. Sikkerheten i to-faktor varierer. En må derfor nøye vurdere løsningen man ønsker å benytte.
- To-faktor representerer et viktig tiltak for å sikre og ivareta personvern knyttet til bruk av passord (ref. ROS/Risiko- og sårbarhetsanalyser, internkontroll)

Hvorfor **sterk autentisering** for Feide?

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.

Piloter

Flere metoder for sterk autentisering vil komme

- MFA gjennom AzureAD innlogging
- Ansattporten for offentlig sektor
- MFA gjennom Google Workspace?

Status aktivering - **sterk autentisering** for Feide

I grunnopplæringen har:

136 av 356 **kommuner**
5 av 11 **fylkeskommuner**
47 av 347 **friskoler**

- aktivisert sterk autentisering.

Og nye kommer stadig til!

Sikker innlogging og datadeling!