

# Styringsrådet for Digitaliseringsdirektoratets fellesløsninger, (tidligere i regi av Difi)

## SAKSFRAMLEGG

---

Forum:

Styringsrådet for DigDirs felleskomponenter

Møtedato: 22. september 2021

---

### **Sak 21/16 Oppfølging og status etter hendelsen 1. oktober 2020**

#### 1. Oppsummering

Saksfremlegget oppsummerer viktige anbefalinger og tiltak etter hendelsen 1. okt. 2020.

Saken legges fram til orientering og for ev. innspill

#### 2. Hva saken gjelder

Som følge av sikkerhetshendelsen i ID-porten 1. okt. 2020 har Digdir iverksatt flere tiltak som forbedrer håndtering av hendelser, og innført avbøtende tiltak for å hindre nye sikkerhetshendelser. Saksfremlegget gjør rede for hovedtiltakene og er ment som informasjon til Styringsrådet.

Håndteringen av hendelsen i etterkant har fungert godt. Samarbeidet med virksomhetene og deres berørte brukere har vært godt. Det ble tidlig avklart, med ekstern bistand, at ID-porten kjørte stabilt og sikkert etter tilbakerulling av produksjonssettingen som førte til feilen. ID-porten har siden vært i stabil og sikker drift, og det har ikke skjedd liknende hendelser i løpet av året som har gått.

Derfor har hovedfokus i oppfølgingen blitt rettet mot tiltak som kan bidra til å avdekke feil tidligere, samt tiltak som bidrar til å redusere sannsynligheten for hendelser fremover. Mnemonic er engasjert for å gjennomføre en evaluering av hendelsen og gi anbefalinger om hvilke områder og tiltak Digdir bør vurdere for å forbedre prosesser rundt utvikling og forvaltning av ID-porten.

Følgende er gitt som hovedanbefalinger:

##### 1. **Forbedre risikostyring i utviklingsarbeidet:**

Risikoer bør identifiseres og håndteres tidlig ved å bruke teknikker for å nyansere risikobildet. Videre må risikoene kommuniseres, og beslutninger må forankres på riktig nivå i organisasjonen.

##### 2. **Forbedre testrutiner slik at de reflekterer risikoene i produksjonsmiljøet:**

Bank ID og Bank ID på mobil er de mest brukte eID-ene i ID-porten. Digitaliseringsdirektoratet bør derfor gjennomføre mer omfattende testing og kvalitetssikring av disse.

##### 3. **Implementering av tekniske integritetskontroller i ID-porten:**

Digitaliseringsdirektoratet har i sin interne klassifisering vurdert at ID-porten krever høyeste nivå for sikring av integritet. Det bør derfor settes større fokus på å innføre gjennomgående tekniske integritetskontroller.

##### 4. **Tilpasse og forbedre utviklingsprosessen for å møte høye sikkerhetskrav:**

Utviklingsprosessen til Digitaliseringsdirektoratet er ikke tilpasset hvordan utviklingen gjøres i praksis eller de høye sikkerhetskravene til ID-porten, noe som fører til prosessavvik og avvik fra sikkerhetskravene. Prosessen bør videreutvikles slik at endringer i ID-porten er i henhold til disse kravene.

Det er tatt grep ilt. vinteren og våren 2021 for å sikre at risiko håndteres i tråd med eksisterende prosesser. Deriblant prosedyrer knyttet til håndtering og vurdering av risiko ved produksjonssettinger av endringer.

## **Styringsrådet for Digitaliseringsdirektoratets fellesløsninger, (tidligere i regi av Difi)**

Et lengre løp er startet for å møte anbefalingene i evaluering etter hendelsen. Et eget prosjekt følger opp videreutvikling av prosesser og kontinuerlig forbedringsarbeid for en sikrere utvikling av ID-porten. Prosjektet ser konkret på prosesser for bedre håndtering av trusler og risiko gjennom hele utviklingsløpet. Arbeidet retter seg mot to områder. Det ene er eksisterende ID-porten med eksisterende applikasjoner og driftsplattform. Det andre området er den moderniserte ID-porten på ny driftsplattform, som for tiden er under etablering. Moderniseringen av ID-porten er i seg selv et risikoreduserende tiltak, dette prioriteres høyt. Prosjektet gjennomføres med støtte fra Mnemonic.

Prosesser og praksis for kontinuerlig forbedringsarbeid skal være implementert i løpet av 2021. Sentralt i prosessforbedringen er også testrutiner som bedre reflekterer risikoene i produksjonsmiljøet. Dette henger sammen med implementering av nye eID-avtaler i november 2021. Som del av anskaffelsen av eID-er er det tatt høyde for å gjøre mer omfattende testing. Slik møtes anbefalingene som er gitt i evalueringen etter hendelsen.

Digdir er også i kontakt med eksterne utviklingsmiljøer for innspill til prosessforbedringen, her tar vi gjerne videre dialog med flere. Målet er å hente erfaringer og beste praksis fra andre i vårt videre arbeid med prosessutvikling.

Saksframlegg utarbeidet av Halvard Gjerde og legges frem av Jon Håkon Odd

Leikanger, 15.09.2021