



## Kommunal- og moderniseringsdepartementet

Postboks 8112 Dep

0032 Oslo

Politidirektoratet

Deres referanse:

Vår referanse:

Dato:

22/238470 - 21

30.01.2023

## Politidirektoratets hørings svar - Høring om forslag til veileder for bruk av eID for ansatte i offentlig forvaltning

### Innledning

Politidirektoratet viser til Kommunal- og moderniseringsdepartementets høringsbrev av 2. desember 2022. Høringsfristen var i utgangspunktet 20. januar 2023. Politidirektoratet har imidlertid fått bekreftet utsatt høringsfrist til 30. januar 2023.

Politidirektoratet har forelagt høringen for Kripos, Oslo, Øst og Trøndelag politidistrikter, samt Politiets IT-enhet (PIT), og har mottatt innspill fra Kripos og Øst politidistrikt. Mottatte innspill følger vedlagt dette hørings svaret.

### Kort om høringen

Kommunal- og moderniseringsdepartementet har utarbeidet et utkast til en veileder med retningslinjer for bruk av eID for ansatte i offentlig forvaltning. Den foreslåtte veilederen er en oppfølging av oppdrag nr. 5 i Statsbudsjettet 2022 – Tildelingsbrev fra Digitaliseringsdirektoratet, og er ment å gi nødvendig informasjon for arbeidsgivere og arbeidstakere. Veilederen inneholder en sjekklister for de viktigste vurderingene som bør gjøres i forbindelse med bruk av eID.

Formålet med veilederen er å gi arbeidsgivere og arbeidstakere tilgang til oversiktlig informasjon om bruk av eID i offentlig forvaltning, herunder tilgang til retningslinjer og sjekklister for de konkrete vurderingene som bør foretas. Det er et mål om at forholdene rundt bruk av eID i arbeidsforhold skal oppleves forståelige for arbeidsgivere og arbeidstakere. Veilederen tar utgangspunkt i og beskriver den faktiske og rettslige situasjonen slik den er i dag. Det er altså en deskriptiv og ikke en normativ veileder.

Veilederen omtaler bl.a. hvilke regler og krav som gjelder for bruk av eID i offentlig sektor, hvilke tekniske løsninger som er tilgjengelig på de to høyeste sikkerhetsnivåene, og hva som er forutsetningene for å ta disse løsningene i bruk. Videre omtales ulike arbeidsrettslige- og personvernrettslige temaer.

### Politidirektoratet

---

## Politidirektoratets merknader

Politidirektoratet er i utgangspunktet positiv til at det utarbeides en veileder som gir retningslinjer for bruk av eID for ansatte i offentlig forvaltning, og som har som formål at arbeidsgivere og arbeidstakere skal ha tilgang til oversiktlig informasjon om bruk av eID i offentlig forvaltning. Direktoratet er likevel av den oppfatning at flere viktige punkter bør presiseres og tas inn i veilederen av bl.a. sikkerhets- og personvernmessige årsaker, og av hensyn til tydelighet og brukervennlighet. Vi viser særlig til innspillet fra Kripos, og vurderer i likhet med dem at det kan være hensiktsmessig med nærmere redegjørelse i et møte med Kripos.

### Generelle merknader:

- Veilederen er for overordnet til at den gir en verdi som veileder til arbeidsgivere som ikke har betydelig kunnskap om eID og løsninger, og de dilemmaer som er på dette fagområdet.
- Veilederen bør skille tydelig på om det er arbeidsgiver som eier tjenesten, eller om tjenesten eies av andre (for eksempel NAV). Eier arbeidsgiver tjenesten selv, har de helt andre virkemidler og problemstillinger enn om tjenesten eies av andre. Herunder kan det nevnes forholdet til skillet mellom behandlingsansvar og databehandleransvar etter GDPR, valgmuligheter og kontrollmuligheter. Her vil det være hensiktsmessig med noen eksempler.
- Veilederen skiller mellom offentlige og private eID'er i teksten. Vi kan ikke se at det har noen betydning om det er offentlig eller private som står bak eID-utstedelsen i dette tilfellet. Det er av større betydning å fokusere på sikkerhetsnivåer. Slike formuleringer vil også være mer varig over tid.
- Politidirektoratet ser lite spor av hvilke vurderinger som er gjort i forhold til risiko for misbruk av eID'en. Dette er svært bekymringsfullt da vi ser en økning i misbruk av eID. Veilederen bør rettlede arbeidsgivere i forhold til hvilket misbrukspotensiale de har i tjenestene de selv eier, og i tjenester deres ansatte bruker og som eies av andre. Særlig er det viktig å få frem misbrukspotensialet ved BankID ettersom det kan være utstedt flere BankID'er på en og samme person. Også det motsatte kan forekomme, der den ansatte får sin egen eID misbrukt av arbeidsgiver eller kollegaer bør redegjøres for, herunder hvilke tiltak som kan iverksettes for å redusere slik risiko.
- Omtalen av virksomhetssertifikater kan med fordel være mer utfyllende. Ofte forstår ikke den ansatte hvorfor det er nødvendig med personlig ID i stedet for innlogging med organisasjonsnummer e.l. Dataminimeringsprinsippet taler også for at innlogging med personlig ID er unødvendig i tilfeller hvor det er tilstrekkelig å verifisere brukeren som en ansatt i den aktuelle virksomheten.
- Vedrørende tidspunkt for lansering: Vi stiller spørsmål ved om det er hensiktsmessig å lansere en veileder nå, før arbeidene med eID-strategi, digital lommebok og pilot på ansattportalen er ferdigstilt.
- Kripos har påpekt at enkelte momenter i den fremtidige utviklingen innenfor eID kan ha betydning for politiets skjulte metoder og ivaretagelsen av sikkerheten til politiansatte med et særlig behov for beskyttelse. Dette aktualiseres særlig ved et eventuelt pålegg om bruk av privat eID som ansatt offentlig forvaltning. Kripos legger til grunn at også andre offentlige etater kan oppleve et eventuelt pålegg om bruk av privat eID som en sikkerhetsutfordring. Se nærmere om sammenhengen i Kripos sitt høringsinnspill som følger vedlagt. Kripos stiller gjerne til et møte med Kommunal- og

moderniseringsdepartementet for å redegjøre nærmere for aktuelle og konkrete problemstillinger. Politidirektoratet viser til innspillet fra Kripos og er enig i Kripos' synspunkter.

#### Kommentarer til de enkelte delene av utkastet til veileder:

- Innledningsvis omtales både Feide og MinID, uten at vi kan se at disse er omtalt senere i veilederen. Er de ikke aktuelle som bruk i arbeidsforhold så bør de utgå for å få veilederen mer presis og enkel. I motsatt fall bør de mer inn i beskrivelsen.
- Begrepslisten bør være alfabetisk. Det kan også være nyttig med en liste over aktuelle eID'er og en beskrivelse av de respektive beskafterheter hver enkelt av dem har og kanskje trekke frem hva som gjør dem egnet til å bruke som ansatt-eID. Commfides og Buypass er her vesentlig forskjellig fra BankID, da disse kan anskaffes av virksomheter og tilbys ansatte som en ansatt-eID. BankID har ikke denne egenskapen, noe som skiller dem vesentlig fra de andre to. Etter vår vurdering er BankIDs egenskap på dette området beskrevet feil i veilederen.
- Side 24, 2. kulepunkt: Det er uheldig å foreslå en økonomisk kompensasjon i bytte mot bruk av personlig eID. Økonomisk kompensasjon bør kun være aktuelt der slik bruk innebærer utgifter for arbeidstaker.
- Side 24, 3. kulepunkt: Her legges det til grunn som et utgangspunkt at bruk av personlig eID ikke kan pålegges og står i konflikt med styringsretten. Ettersom dette beror på en tolkning av loven og ikke fremgår direkte av lov eller rettspraksis bør det i høringen utvises forsiktighet med å komme med slike slutninger.
- Kap. 5.1, 5. avsnitt (side 25): Her igjen konkluderes det med at bruk av styringsretten til å pålegge bruk av personlig utstyr for identifikasjon er "snever". Dette er et uheldig språkbruk og går for langt i å konkludere rammene for arbeidsgiver styringsrett.
- Kap. 5.2.1, 3. avsnitt (side 26): Konkrete regler for bruk og anskaffelse av eID bør være lik for alle arbeidstakere, og dermed ikke avtales individuelt eller fastsettes i kollektive avtaler. Slike regler bør fastsettes ensidig i reglement og være en del av arbeidsavtalen på lik linje med andre reglementer. Høringen bør ikke legge opp til individuelle eller kollektive avtaler om dette.
- Kap. 5.4, "steg 3" (side 30): Høringsbrevet går for langt i å antyde økonomisk kompensasjon samtidig som det også presiserer at det må vurderes om bruk av private eiendeler kan pålegges gjennom styringsretten. Dersom det kan pålegges gjennom styringsretten må en økonomisk kompensasjon være utelukket, og bør ikke omtales som en del av en frivillig løsning.
- Øst politidistrikt har særlig påpekt følgende, som Politidirektoratet slutter seg til:
  - o Veilederen bør inneholde et flytskjema til støtte for de virksomheter som har behov for å innføre e-ID (veilederen bærer noe preg av "tungt" språk).
  - o Fagord eller fremmedord, eks " legaldefinert" under kap. 2.2.2 bør unngås slik at lekfolk kan forstå innholdet uten å slå opp i ordliste.
  - o Dersom det i dokumentet henvises til eksempelvis lov og forskrift, eller andre kapitler i dokumentet, bør det settes inn hyperlink.
  - o Kap 2. avsnitt 6: Det bør fremkomme at "BankID på mobil" erstattes av "BankID på app"

- Kap 2.1: Sikkerhetsnivåene bør også tallfestes (nivå 1-4) slik at det blir samsvar mellom informasjon i veileder og informasjon fra dagens tilbydere.
- Kap 3.3 Henvisning til SPH. Årstallet 2022 bør tas ut da SPH oppdateres årlig.

Med hilsen

**Kristine Langkaas**  
*Seksjonssjef*

**Synnøve Wik Bårdsen**  
*Rådgiver*

*Dokumentet er elektronisk godkjent uten signatur.*

Vedlegg:

Høringsinnspill - veileder for bruk av eID for ansatte i offentlig forvaltning - Øst politidistrikt

Høringsinnspill - veileder for bruk av eID for ansatte i offentlig forvaltning - Kripos