

Kommunal- og distriktsdepartementet
Postboks 8112 Dep

0032 OSLO

Att: Katarina de Brisis

Deres ref.:
22/7211

Vår ref.:
Mads Henriksveen

Dato:
20.januar 2023

HØRINGSSVAR – VEILEDER FOR BRUK AV EID FOR ANSATTE I OFFENTLIG FORVALTNING

Buypass viser til høringsbrev fra Kommunal- og distriktsdepartementet datert 2.desember 2022 og vil med dette komme med vårt hørings svar.

Generelt

Veilederen er blitt et veldig bra, men omfattende dokument med mye tekst. Sistnevnte medfører at det blir en del gjentakelser i ulike deler av dokumentet og en del henvisninger frem og tilbake som gjør at det kan være vanskelig å forstå alle disse sammenhengene uten å lese veilederen i sin helhet. Men det hjelper at dokumentet er strukturert slik at leseren av dokumentet raskt kan finne frem til hvilke deler av dokumentet som er relevant for seg (som arbeidsgiver eller arbeidstaker).

Vi forstår det slik at veilederen skal publiseres på nett og at dette gir muligheter for å gjøre det enklere å navigere mellom de ulike delene av veilederen.

Mye av innholdet i dokumentet er komplisert og knyttet til arbeidsrettslige forhold og personvern. Måten dette blir presentert gjør at dette blir vanskelig tilgjengelig og sammen med strukturen nevnt innledningsvis kan dette bidra til at veilederen ikke blir så hensiktsmessig som ønsket.

I det følgende kommer våre kommentarer organisert etter kapittel i veilederen.

1. Innledning

Ingen spesielle kommentarer.

2. Hva er eID?

I listen over selvdeklarte eID-ordninger side 8 bør også 'Buypass ID FIDO2' inkluderes.

I siste avsnitt under eID-leverandørene kap 2.1 side 9 er Nkom omtalt som 'Norsk kommunikasjonsmyndighet', dette skal være 'Nasjonal kommunikasjonsmyndighet'.

Kap 2.2.2 Nærmere om «ansatt-eID» og «privat eID»

Buypass vil gjerne understreke viktigheten av å skille mellom privat eID og ansatt eID. Buypass har hatt et tilbud om ansatt eID til virksomheter i mange år og vet hvor viktig det kan være for både arbeidsgiver og arbeidstaker å ha kontroll på eID brukt i arbeidssammenheng. Med en ansatt eID følger det forpliktelser og rettigheter som gjelder både arbeidsgiver og arbeidstaker der begge

parter har et forhold til eID-leverandør. Med en privat eID er dette primært et forhold mellom eID-leverandør og den ansatte som privatperson.

Under kap 2.2.2 på side 11 omtales personsertifikater som inneholder informasjon om virksomheten. Denne koblingen gjøres for å gi virksomheten "eierskap" til sertifikatene slik at disse kan administreres av dem - i henhold til gjeldende regelverk for denne type sertifikater.

Lenger ned på samme side er det også en diskusjon om privat eID og ansatt eID og det er viktig å være oppmerksom på at virksomheten (arbeidsgiver) i liten grad har anledning til å administrere en privat eID sammenliknet med en ansatt eID. Som eID-leverandør har vi ingen anledning til å gi en arbeidsgiver rettigheter til å administrere arbeidstakers private eID.

Kap 2.2.3 Elektronisk signatur

Veilederen beskriver en tett kobling mellom eID (som elektronisk identifikasjon definert under kap 2 i eIDAS-forordningen) og elektronisk signatur (som en tillitstjeneste regulert under kap 3 i eIDAS-forordningen).

Det er nok fortsatt slik at eID-løsninger i Norge, da spesielt de som er PKI-baserte, tilbyr både elektronisk identifikasjon og elektronisk signatur i en og samme løsning, men det er et klarere regulatorisk skille mellom disse to tjenestene enn det vi har vært vant til i Norge.

Elektronisk signatur slik den er definert i eIDAS-forordningen er ikke dekket under Selvdeklarasjonsforskriften i Norge.

3. Regler og krav for bruk av eID

Se kommentar over når det gjelder regulering av eID og elektronisk signatur.

4. Dette bør arbeidstaker være kjent med

Ingen spesielle kommentarer.

5. Dette bør arbeidsgiver vurdere - Bruk av eID i et arbeidsrettslig perspektiv

Arbeidsgiver må være oppmerksom på skillet mellom bruk av eID internt (PC, nettverk, applikasjoner etc) og eksternt (typisk tjenester via ID-porten, HelselD, eResept etc).

En vurdering av totalbehovet må tidlig inn hos arbeidsgiver for å vurdere hva som er hensiktsmessig for å dekke krav til compliance, sikkerhet, funksjonalitet, brukervennlighet (blant annet en eller flere eID til samme ansatt), tekniske muligheter/begrensninger, kostnader etc

Kap 5.2 Hva bør avtales mellom arbeidsgiver og arbeidstaker?

I nest siste avsnitt (under 5.2.2.2) sies det at en ansatt eID ment for bruk i forvaltningen ikke skal brukes for andre formål.

En ansatt eID er også en personlig eID på et sikkerhetsnivå som gjør at den kan brukes for andre formål. En slik begrensning må derfor reguleres i avtale mellom arbeidsgiver og arbeidstaker.

Dersom arbeidsgiver ønsker at ansatte skal bruke sin private eID og samtidig begrense bruken av denne, så må det håndteres innenfor de systemer og tilganger den ansatte benytter i jobbsammenheng – i den grad dette er mulig. Arbeidsgiver har ingen mulighet til å begrense bruk av privat eID utenfor jobb.

Kap 5.4 Sjekkliste for arbeidsgiver

Under steg 1 og andre kulepunkt under 'Inngå dialog med ansatte' står det at arbeidsgiver skal avklare om den ansatte allerede har en eID og ønsker å bruke denne.

Her er det viktig at arbeidsgiver er oppmerksom på forholdet mellom intern og ekstern bruk (se også kommentar under 5 over). Ved kun ekstern bruk (via ID-porten o.l.) kan privat eID vurderes benyttet, men ved intern bruk for pålogging PC, nettverk, applikasjoner etc må arbeidsgiver av tekniske, praktiske og kostnadmessige hensyn velge på vegne av alle ansatte.

6. Dette bør arbeidsgiver vurdere - Personvernet til arbeidstaker

I kulepunkt 2 på side 31 hevdes det at det normalt er innenfor formålet at privat eID benyttes mer generelt også i arbeidsøyemed.

Dersom eID skal brukes for internt bruk (se kommentar under 5) så kan det diskuteres om det er dekning for denne påstanden.

7. Sjekkliste

Under steg 2 på side 39 hevdes det under 'Effektivitetshensyn' at det er tidsbesparende å ta i bruk eksisterende privat eID fremfor å anskaffe nye ansatt eID-er.

Dette er en påstand det ikke er dekning for. Hvis eID for intern bruk kan det tvert imot være helt motsatt. Kanskje sågar ikke teknisk mulig med bruk av privat eID. Formuleringen må endres og samtidig må det tillegges noe om vurdering av hva som er hensiktsmessig ut ifra krav/ønsker som skal tilfredsstilles innenfor compliance, sikkerhet, funksjonalitet, interne/eksterne tjenester m.m.

Se også kommentar under 5 over.

8. Hvordan bruke denne veilederen

Ingen spesielle kommentarer.

9. Spørsmål og svar

Her følger en del relevante spørsmål som Buypass får:

- Hvorfor registreres fullt fødselsnummeret (11 siffer)?
- Hva lagres av data om meg?
- Hvorfor må man vise gyldig legitimasjon?
- Hva om man ikke har slik legitimasjon?
- Hva er gyldig legitimasjon?
- Hva er smartkort?
- Hva er PKI?
- Hva er kryptering?
- Hva er digitale sertifikater?
- Hva er elektronisk signatur?

Oppsummering

Buypass er generelt positive til innholdet i veilederen, men vi vil spesielt peke på ett forhold som kommenteres spesielt.

Det er vesentlige forskjeller mellom en privat eID og ansatt eID når det gjelder arbeidsgivers muligheter til å administrere eID, samt hva som er teknisk mulig for å oppnå ønsket funksjonalitet.

Arbeidsgiver må derfor tidlig ta stilling til påkrevd/ønsket funksjonalitet for bruk av eID hos de ansatte, samt være oppmerksom på forskjellen mellom privat eID og ansatt eID.

Med vennlig hilsen
Buypass AS

Gunnar Lindstøl
Administrerende direktør