Rapport

eID til ansatte i kommunal helse- og omsorgstjeneste

Status, behov og mulige tiltak

23. september 2020

Innhold

1 Sammendrag

Det er et mål å innføre nasjonale e-helseløsninger som kjernejournal og e-resept i den kommunale helse- og omsorgstjenesten. Det krever at helsepersonell og annet personell med tjenstlig behov, tar i bruk elektronisk ID (eID) med høyt sikkerhetsnivå for å identifisere seg elektronisk. Dette er en forutsetning som ikke er på plass i de fleste kommuner. Innføring av e-helseløsninger i kommunene innebærer at eID må tas i bruk av nye og større ansattgrupper enn det som er tilfellet i dag.

Arbeidsgruppens vurdering er at kommunene har behov for informasjon om hvilke krav som gjelder, hvilke løsninger som er tilgjengelig, hvilke løsninger som kan dekke behovene, og hva som er forutsetningene for å ta disse løsningene i bruk. Arbeidsgruppen mener at en veileder om valg og bruk av eID i kommunal helse- og omsorgstjeneste kan være et nyttig første steg. Videre anbefaler arbeidsgruppen at det gjøres en vurdering av om det bør legges til rette for felles anskaffelser og/eller felles kravspesifikasjon for kommunene.

2 Om rapporten

2.1 Bakgrunn

En elektronisk ID (eID) er nødvendig for å identifisere seg elektronisk, og har blitt en del av hverdagen for folk flest gjennom pålogging til digitale tjenester som Facebook, nettbutikker og nettbanken, og signering av elektroniske dokumenter. Nettbanken og en rekke andre digitale tjenester forutsetter at du beviser din unike identitet som innbygger i Norge på en sikker måte gjennom å bruke en eID på høyt sikkerhetsnivå. I dag er det kun BankID, Buypass og Commfides som tilbyr dette i det norske markedet. De fleste innbyggere i Norge er vant til å bruke eID som de har opprettet selv, som oftest fra BankID, for sikker tilgang til nettbanken og andre offentlige tjenester fra stat og kommune. I tillegg har noen en eID fra arbeidsgiver på høyt sikkerhetsnivå, som oftest fra Buypass eller Commfides, ment for bruk i jobbsammenheng. Dette gjelder for eksempel leger og annet helsepersonell som skal benytte kjernejournal eller e-resept. Overordnet er det ikke noen forskjell på en eID som den enkelte selv har anskaffet og en eID som er anskaffet og administrert av arbeidsgiver.

Kjernejournal og e-resept i kommunene er eksempler på digitale tjenester som forutsetter bruk av eID på høyt sikkerhetsnivå. Dette har aktualisert behovet for slik eID for ansatte i den kommunale helse- og omsorgstjenesten. Ut over fastleger og legevakter, har enkelte andre ansatte i kommunene i dag behov for å bruke eID for å utføre arbeidsoppgaver, men omfanget er begrenset og berører i liten grad helse- og omsorgstjenesten. Kommunene vil med denne innføringen ha behov for en enhetlig måte å understøtte bruk av eID for alle ansatte på tvers av sektorer. Det har vist seg å være utfordrende for den enkelte kommune å beslutte hvilken eID de ansatte skal bruke. Regjeringens digitaliseringsstrategi (2019-2025) peker også på at det er behov for tydelige retningslinjer. Videre har både KS og Direktoratet for e-helse i dialog med Helse- og omsorgsdepartementet løftet behovet for avklaringer knyttet til eID for ansatte.

2.2 Arbeidsgruppen

Rapporten er utarbeidet av en hurtigarbeidende arbeidsgruppe med representanter fra KS, Direktoratet for e-helse, Norsk Helsenett SF og Helse- og omsorgsdepartementet (HOD). Kommunal- og moderniseringsdepartementet og Digitaliseringsdirektoratet har bidratt med faglige innspill om eID. Arbeidsgruppen består av følgende medlemmer:

- Erik Hedlund, Norsk Helsenett SF

- Lars Ursin Lunde, Norsk Helsenett SF
- Hilde Caroline Rossland, Direktoratet for e-helse
- Lars Kristian Roland, Direktoratet for e-helse
- Randi Lilletvedt, Direktoratet for e-helse
- Geir Kristian Hansen, KS
- Marianne Sætehaug, KS
- Darlén Gjølstad, HOD
- Marit Lie, HOD

2.3 Formålet med rapporten

Formålet med rapporten er å:

- beskrive behov og status for innføring av eID i kommunene
- beskrive mulighetene som finnes innenfor eksisterende eID-løsninger
- vurdere potensialet for bruk av eID opprettet av privatperson, herunder utfordringer og muligheter for kommunen som arbeidsgiver
- foreslå tiltak som kan legge til rette for innføring av eID i kommunal helse- og omsorgstjeneste på kort sikt
- Identifisere tiltak som bør utredes nærmere

2.4 Definisjoner

Autentisering	Handling for å bekrefte identitet. Sterk autentisering er som hovedregel en form for autentisering med flere faktorer.
BankID	BankID er en eID på høyt sikkerhetsnivå som brukes av alle landets banker, og kan tas i bruk av alle virksomheter som vil ha en sikker og enkel identifisering på nett. BankID tilbys av Vipps som er en kommersiell eID-leverandør.
BuyPass	Kommersiell eID leverandør som tilbyr flere eID løsninger på betydelig og høyt sikkerhetsnivå
Commfides	Kommersiell leverandør som tilbyr eID på høyt sikkerhetsnivå.
eID	Elektronisk ID, elektronisk identitetsbevis for fysiske personer, tilsvarer elektronisk identifikasjonsmiddel i eIDAS-forordningen. eID kan anskaffes av arbeidsgiver til bruk for ansatte, eller ved at privatperson har inngått avtalen med eID-tilbyderen selv.
eIDAS-forordningen	Forordning om elektronisk identifisering og tillitstjenester for elektroniske transaksjoner i det indre markedet og som er inntatt i norsk lov.
Helse-ID	Felles påloggingsløsning for helse- og omsorgssektoren. Den legger til rette for at helsepersonell kan få engangspålogging med én elektronisk ID (e-ID) i hele helsetjenesten, og for at sektoren lettere kan dele data og dokumenter.
Innrullering	Utlevering av eID til nye brukere. Begrepet innrulling inkluderer utlevering, aktivering og utstedelse i en sammenhengende prosess. Det stilles ulike krav til kvalitet på kontroll per sikkerhetsnivå
Kjernejournal	Nasjonale e-helseløsning, en samhandlingsløsning etablert for å øke pasientsikkerheten. I den enkeltes kjernejournal er et utvalg viktige opplysninger gjort tilgjengelige for helsepersonell med tjenstlig behov, uavhengig av hvor pasienten tidligere har mottatt helsehjelp.

PKI	Public Key Infrastructure (PKI) benyttes asymmetriske kryptografiske nøkkelpar som hemmeligheter. PKI benyttes i mange anvendelser utenom eID. For eID for personer har de private nøklene tradisjonelt blitt beskyttet i en HSM modul, smartkort eller simkort
Sikkerhetsnivå	Sikkerhetsnivåene angir ulike grader av tillit til at påstanden om identitet, i en elektronisk kommunikasjon, er korrekt. Hvilket sikkerhetsnivå som skal kreves, beror på risikoen i tjenesten, herunder hvilke konsekvenser identifikasjonssvikt vil ha samt trusselbildet for den aktuelle tjeneste mv. Det er den virksomheten som eier tjenesten som bestemmer hvilket sikkerhetsnivå tjenesten deres skal ha. Sikkerhetsnivåene i eIDAS er kategorisert som «lavt», «betydelig» og «høyt». Norsk lov (selvdeklarasjonsforskriften) definerer egne norske sikkerhetsnivåer, basert på eIDAS og for bruk i Norge.
Smartkort	Er et kort med integrert mikroprosessor. Kortene har mange bruksområder, og teknologien er benyttes stadig oftere blant annet på grunn av fleksibiliteten og sikkerhetsmulighetene. Blir også ofte kalt for PKI-kort i sammenheng med eID løsninger. Da oppbevares den private nøkkelen på kortet, beskyttet normalt av en pin kode. Andre type bærere av eID er for eksempel simkort i mobiltelefon og USB-pinner.

3 Status og behov

3.1 Innføring av nasjonale e-helseløsninger og behovet for sikker pålogging

Innføringen av de nasjonale e-helseløsningene kjernejournal og e-resept til den kommunale pleie- og omsorgstjeneste er høyt prioritert i nasjonale strategier og planer. Tilgang til de nasjonale e-helseløsningene stiller krav om bruk av eID på høyt sikkerhetsnivå, dette gjelder både eksisterende tjenester som e-resept og kjernejournal, og planlagte nye tjenester som Akson journal.

I helse- og omsorgssektoren er det spesialisthelsetjenesten som er kommet lengst med å innføre bruk av eID blant ansatte. I Midt-Norge er innføringsarbeidet også kommet langt gjennom arbeidet med Helseplattformen. Alle rekvirenter av e-resept som jobber på sykehus, legekontor og legevakt bruker i dag eID på smartkort eller USB-pinne fra leverandørene Buypass eller Commfides. Smartkortet eller USB-pinnen benyttes også for tilgang til kjernejournal som brukes av over 22 000 helsepersonell.

En sentral problemstilling rundt videre innføring av e-resept og kjernejournal i kommunene, er avklaringen av hvordan anskaffelse og bruk av eID skal håndteres for ansatte i helse- og omsorgstjenesten. Et alternativ er at kommunene utstyrer ansatte med eID på høyt sikkerhetsnivå til bruk i jobbsammenheng. Et annet alternativ er å bruke eID som er anskaffet privat, for eksempel BankID.

3.1.1 Kjernejournal

Kjernejournal gjør at helsepersonell kan få innsyn i nødvendig informasjon om pasienten, på tvers av helse- og omsorgstjenesten. Kjernejournal inneholder informasjon om personalia, familierelasjoner med kontaktinformasjon, informasjon om hvem som er personens fastlege og besøkshistorikk. Videre inneholder kjernejournalen viktige helseopplysninger til den enkelte innbygger, som for eksempel sykdomshistorikk, informasjon om alvorlige allergier eller overfølsomhetsreaksjoner,

implantater, viktige behandlinger, sjeldne alvorlige tilstander og lignende. Under koronapandemien er det lagt til rette for at helsepersonell får tilgang til koronarelaterte prøvesvar i kjernejournal.

Det meste av informasjonen i kjernejournal hentes automatisk fra offentlige registre. I tillegg kan helsepersonell, i samråd med pasienten, registrere kritisk informasjon og spesielt viktige helseopplysninger, for eksempel allergier. Innbyggerne kan også selv legge inn noen opplysninger i kjernejournalen via innbyggerportalen helsenorge.no. Det arbeides med ny funksjonalitet som vil gi mulighet for referanse til ytterligere informasjon og mulighet til å lese bestemte journaldokumenter som er gjort tilgjengelige for deling med behandlende personell. I første omgang vil epikriser og prøvesvar for spesialisthelsetjenesten bli tilgjengeliggjort.

Kjernejournal er per mai 2020 innført ved alle sykehus, alle legevakter og ved 90 prosent av fastlegekontorene. I tillegg har alle innbyggere fått tilgang til egen kjernejournal via Helsenorge.no. Kjernejournal er ikke innført ved sykehjem og i hjemmetjenesten i kommunal helse- og omsorgstjeneste. En av de tre journalleverandørene til kommunal helse- og omsorgstjeneste har utviklet integrasjon med kjernejournal. De to andre har overfor Direktoratet for e-helse meldt at de har integrasjon med kjernejournal i sine planer for 2020. Norsk Helsenett har pågående aktiviteter for utprøving og innføring av kjernejournal i sykehjem og hjemmetjenesten. Arendal, Halden, Lillehammer, Gausdal, Ringebu og Øyer kommune er nå i gang med kjernejournal, og flere kommuner skal starte opp i 2020.

Innføring i kommunene avhenger av at kommunene har innført eID, kommunenes journalleverandører har integrert kjernejournal i løsningene og en selvbetjeningsløsning for helseID er på plass. Norsk Helsenett har anslått at om lag 50 prosent, eller totalt 25 000, av helsepersonellet ansatt i kommunene trenger eID når kommunene innfører kjernejournal.

3.1.2 E-resept

E-resept er en elektronisk samhandlingskjede for sikker overføring av reseptinformasjon som reduserer risikoen for feil i rekvirering og utlevering av legemidler. E-resept sørger for at den som rekvirerer resepten sender en elektronisk resept til reseptformidleren. Pasienten som har fått forskrevet reseptpliktige legemidler, medisinsk forbruksmateriell eller næringsmidler kan deretter henvende seg til hvilket som helst apotek for å få dette utlevert. E-reseptløsningen omfatter alle virksomheter som har en rolle ved elektronisk formidling av resepter og legemiddelopplysninger, og de systemene disse virksomhetene benytter. Løsningen omfatter rekvirenter som for eksempel fastleger, legevakter, sykehus, apotek, bandasjister, Statens legemiddelverk og Helfo. Den nasjonale reseptformidlerløsningen bidrar til at både rekvirenter, apotek og innbyggere har tilgang til en oppdatert liste over pasientens resepter.

E-resept er per mai 2020 innført for fastleger, legevakter, sykehus, avtalespesialister, apotek, bandasjister, nettapotek og for noen tannleger. Over 90 prosent av alle resepter til Norges innbyggere er elektroniske, og det arbeides med innføring for flere rekvirentgrupper som vil bidra til å øke andelen av elektroniske resepter. Den kommunale pleie- og omsorgstjenesten har ikke innført e-resept. Det anslås at ca. 50 prosent av det totale antallet ansatte som trenger tilgang etter innføring av både kjernejournal og e-resept (sentral forskrivningsmodul), trenger tilgang gjennom innføring av en kjernejournalportal. Dersom kommunen allerede har innført kjernejournal vil helsepersonellet allerede ha tilgjengelig eID.

3.2 Kommunenes behov

eID på høyt sikkerhetsnivå er en forutsetning for stadig flere tjenester som benyttes av ansatte i kommunal sektor. Behovet er ikke avgrenset til kommunale helse- og omsorgstjenester, men det er

ikke alle tjenester som har krav om eID på høyt sikkerhetsnivå. Uavhengig av dette er det viktig at valg og anbefalinger om bruk av eID-løsninger tar hensyn til funksjonelle og tekniske behov og økonomiske konsekvenser på tvers av tjenester i kommunesektoren.

Kommunene har forskjellige behov og prosesser, som stadig utvikles. Det er derfor viktig å ikke låse seg til en eller et begrenset utvalg av eID leverandører. Råd og føringer bør derfor i så stor grad som mulig være uavhengig av konkrete eID leverandører. Særlig i helse- og omsorgstjenestene, men også i andre kommunale tjenester som barnevern, sosialtjeneste og PPT, er det økende bruk av mobile flater som mobiltelefon og nettbrett. Det er derfor viktig at eID og autentiseringsløsning kan fungere på mobilt utstyr, og ikke er begrenset til autentisering ved bruk av PC.

Anskaffelse og forvaltning av eID kan for kommunene bli kostnadsdrivende, og det er derfor viktig å vurdere de ulike alternativene som finnes. Skal rask utbredelse av de nasjonale løsningene lykkes, er kostnad og om løsningene dekker kommunens behov viktige elementer.

Arendal var den første kommunen som tok i bruk kjernejournal på sykehjem og i hjemmetjenesten. De startet med PKI-kort og kortlesere på noen avdelinger. Når flere avdelinger skulle starte opp, gikk de over til å benytte eID som de ansatte skaffet selv. For mange senket dette terskelen for å logge seg på kjernejournal når de kunne benytte egen BankID. Alle ansatte har nå gått bort fra å bruke PKI-kort og kortlesere, og benytter BankID for å logge seg på. Arendal vurderer BankID som en av suksessfaktorene for innføring av kjernejournal.

Det planlegges i høst å prøve ut bruk av kjernejournal via de to andre systemene i helse- og omsorgstjenesten. Kommunene har valgt ulik tilnærming til eID. Den ene kommunen har tatt valg om å starte med eID som de ansatte har skaffet selv. I den andre kommunen vil de benytte PKI-kort anskaffet av kommunen. Dette vil gi oss viktig erfaring inn i arbeidet videre.

Det kan være effektivt for både kommunen og den ansatte å bruke en eID som forutsetter at den enkelte ansatte har en privat avtale. Det vanligste eksemplet er BankID, men det kan også være aktuelt med andre slike eID-løsninger.

3.3 Dagens eID-løsninger og krav i regelverket

Norge er blant de fremste land i verden når det gjelder utbredelse og bruk av eID. Sammen med høy kvalitet i folkeregisteret og en varig identifikator i fødselsnummer og D-nummer har det gitt oss en fordel i digitalisering av samfunnet. Bruk av eID i offentlig sektor er i hovedsak basert på kjøp fra private leverandører og samarbeid med andre samfunnssektorer som bank /finans. eID har vært helt nødvendige for å lage sikre og personaliserte tjenester på nettet.

De sikreste eID-løsningene er i hovedsak bygd rundt asymmetriske nøkler. PKI er et eksempel på dette. Med asymmetriske nøkler benyttes private, kryptografiske nøkler som hemmeligheter. Tradisjonelt har de private nøklene blitt oppbevart privat, i smartkort, USB-pinne eller simkort. I sentrallagret eID-løsninger, som BankID, lagres nøklene trygt hos eID-leverandøren. Enklere eID-løsninger er gjerne basert på bruk av passord og kodelister.

I det offentlige er det flere eID-infrastrukturer, ID-porten, helseID og Feide tilgangsstyring, som gjør det mulig å benytte eID for pålogging med tilgangsstyring i ulike løsninger og systemer.

Se nærmere omtale av eID-løsninger og eID-infrastrukturer i vedlegg.

3.3.1 Krav i regelverket

eIDAS-forordningen[1] gir i praksis felles regler for eID i hele Europa. eIDAS er innført i norsk rett gjennom lov om elektroniske tillitstjenester [2] med tilhørende forskrifter. Det norske lovverket som regulerer eID speiler dermed EU-lovgiving. Det er etablert en frivillig selvdeklareringsordningen for eID som bygger på prosesser for melding av eID på EU-nivå. Nkom er tilsynsorgan for eID i Norge. Fra 21. mai 2020 må eID-tilbydere ha selvdeklarert løsningene etter de nye sikkerhetskravene.

Selvdeklarasjonsforskriften[3] beskriver krav for å oppfylle norske sikkerhetsnivå. Kravene fra identifikasjonsnivåforskriften[4] gjenbrukes med noen norske tilpasninger, hvor den mest sentrale er kravet til entydig knytting til norsk fødsels- og d-nummer. Beskrivelsene av eID på alle sikkerhetsnivåer er også gjort teknologinøytrale og det tidligere kravet om bruk av PKI gjelder ikke lengre. Kravspesifikasjonen for PKI i offentlig sektorer vil derfor avvikles som en obligatorisk forvaltningsstandard.

Sikkerhetsnivå lavt gir enkel pålogging og tilfredsstiller nivået for mange tjenester. Det gir en viss sikkerhet for at personen er rette vedkommende. Eksempler er løsninger basert på:

- Innlogging med passord som er aktivert ved hjelp av melding til personens e-postadresse i kontaktregisteret, eller til folkeregistrert adresse
- Innlogging med brukerkonto som er aktivert gjennom e-post eller SMS-sendt adresse fra kontaktregisteret.
- Et program (app) på mobil enhet som er knyttet til personen gjennom engangskode sendt personens mobilnummer i kontaktregisteret
- Passord, program (app) på mobil enhet eller brukerkonto som er blitt knyttet til personen gjennom innlogging med annen eID i tråd med dette rammeverket

Sikkerhetsnivå betydelig tilfredsstiller behovet for de fleste tjenester. Eksempler på løsninger:

- MinID, opprettet med engangspassord sendt til folkeregistrert adresse
- Tofaktorinnlogginger som måtte tilbys av markedet, men som ikke tilfredsstiller nivå høyt

Sikkerhetsnivå høyt tilfredsstiller også behovet for tjenester med særlig høye krav til sikkerhet. Eksempler på løsninger:

- eID som er utstedt ved manuell identitetskontroll (pass/ID-kort sjekkes ved fysisk fremmøte mot personen), tofaktorløsning, ev. med bruk av privatnøkkel[5]
- eID som er utstedt ved automatisert identitetskontroll (pass/ID-kort sjekkes mot bilde/video som tas av personen), tofaktorløsning med sterk knytning til telefonen og til passord

Tjenesteeier må gjøre egne vurderinger av trusselbildet for tjenesten, herunder vurdere risikoen for sikkerhetsbrudd og konsekvenser ved å kreve et bestemt sikkerhetsnivåer. Eksempler på hvordan sikkerhetsnivåene kan brukes:

- Lavt nivå: Mange tjenester, blant annet skolepålogging som gir innsyn i egne lekser og karakterer. Innsyn for å se skattelisteopplysninger, åpne folkeregisteropplysninger. Innsending av skjema (barnehagesøknad etc.), statistikkoppgaver.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
[2] https://lovdata.no/dokument/NL/lov/2018-06-15-44
[3] https://lovdata.no/dokument/SF/forskrift/2019-11-21-1578
[4] https://lovdata.no/dokument/SF/forskrift/2019-11-21-1577
[5] Per 2020 tilfredsstilles dette kravet av BankID, Buypass og Commfides

- Betydelig nivå: De fleste tjenester med taushetsbelagte opplysninger, blant annet innsyn i selvangivelser. Vaksineoversikter.
- Høyt nivå: Tjenester som gir innsyn i taushetsbelagte opplysninger med særlig beskyttelsesbehov, herunder stigmatiserende opplysninger, forretningskritisk informasjon, sikkerhetskritisk informasjon og de fleste helseopplysninger.

3.3.2 eIDAS og annerkjennelsesplikt på tvers av landegrensene

eIDAS-lovgivingen pålegger medlemslandene anerkjennelsesplikt for eID på betydelig eller høyt sikkerhetsnivå fra et annet medlemsland dersom landet benytter slik eID for pålogging til egne tjenester. For å legge til rette for bruk av eID fra andre land, er ID-porten utvidet med et eIDAS-knutepunkt som formidler påloggingsforespørsler til brukerens hjemland. Brukersteder benytter ID-porten på vanlig måte.

En liste over meldte eID-ordninger er tilgjengelig på:
https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

4 eID for ansatte i kommunal helse- og omsorgstjeneste

Når kommunene skal ta i bruk eID bør ulike alternativer vurderes for å finne løsninger som enklest kan innfri kommunenes behov. For noen kommuner kan det være aktuelt å kombinere flere alternativer ut fra behov i ulike arbeidsprosesser og roller som personellet skal ivareta brukervennlighet, sikkerhet, gjenbruk og tverrsektorielle behov, og økonomiske og administrative konsekvenser. Tabell 4.1 nedenfor inneholder forslag til vurderingskriterier.

Tabell 4.1 Forslag til vurderingskriterier

Vurderingskriterier	Beskrivelse
Behov og anvendelighet, inkludert: - **Brukervennlighet** - **Implementeringstid og realiserbarhet** - **Potensialet for gjenbruk på andre tjenesteområder**	Veilederen bør inneholde en vurdering av generell behovsdekning opp mot ulike løsningsalternativer Brukervennlighet til de ulike eID-løsningene avhenger av arbeidsoppgavene til den enkelte ansatte og hver kommune må vurdere behov og hvilke tilgang på eID utstyr dette krever. Noen generelle bruksmønstre bør vurderes opp mot de enkelte alternativene. Veilederen bør beskrive om alternativene er praktisk realiserbart og tilgjengelige i dag. Har alternativet allerede etablerte eID-er eller må det utstedes nye eID for alle ansatte som har behov for å bruke eksterne tjenester? Vurdering av implementeringstid for løsningen. Veilederen bør beskrive om løsningen også kan benyttes for andre tjenesteområder i en kommune uten store nye investeringer? Vil fremtidige tiltak kreve nye løsninger eller kan valgt alternativ gjenbrukes?
Sikkerhetsvurdering	Veilederen bør inneholde en overordnet sikkerhetsvurdering av de ulike løsningsalternativene.
Kostnads- og investeringsbehov	Veilederen bør kartlegge hva som potensielt trengs av investeringer og forvaltningskostnader for de ulike alternativene på et overordnet nivå.

Videre beskrives noen erfaringer og betraktninger knyttet til tabellen.

4.1 Behov og anvendelighet

Brukervennlighet til de ulike eID-løsningene avhenger av arbeidsoppgavene til den enkelte ansatte. Ulike arbeidsprosesser vil påvirke hvilken løsning som er best egnet. Kartlegging av noen generelle bruksmønstre under behovsutredningen av eID i den enkelte kommune, vil gi tydelig retning på hvilke(n) løsning som er mest brukervennlig. Det vil være ulike behov ut fra om den ansatte skal logge seg inn på mange ulike enheter i løpet av dagen, hyppighet på innlogging, brukervennlighet og krav til påloggingstid, og om den ansatte jobber på et kontor eller har en mobil arbeidsplass.

Videre må det tas hensyn til hvor anvendelig løsningen er for kommunal sektor, når det gjelder implementering og administrering. Dette omfatter også mulighet for reserveløsninger når bruker har gjenglemt, mistet eller fått ødelagt nødvendig utstyr. Videre må det ved bruk av eID som krever bruk av privat mobil, brikke eller kort, tas hensyn til hvordan dette vil fungere praktisk for helsepersonell i pasientnært arbeid på sykehjem og hjemmetjenesten. Det kan tenkes at det for noen brukergrupper vil være mest hensiktsmessig å benytte mobile løsninger, mens det for andre vil være mest hensiktsmessig å benytte kort e.l.

Eksisterende utstyr som brukes i tjenesten er i liten grad tilrettelagt for å kunne lese kort eller USB-pinne. Det er også tidkrevende å administrere kort eller USB-pinne til alle ansatte, inkludert kortlesere ute i virksomhetene. Installasjon krever ofte oppgradering av programvare på tynnklienter. En fordel med eID-løsninger hvor den ansatte selv har avtaleforholdet med identitetstilbyderen, er at de fleste allerede har en egen eID. Det er derfor et stort potensial for økt brukerdekning ved å åpne opp for bruk av ansattes egne eID. En annen fordel er at disse eID-ene blant annet kan leveres som mobil-apper, bankID på mobil, bankID-brikke, og kodekort.

4.2 Sikkerhetsvurderinger

eID-løsninger som er selvdeklarert og NKOM godkjent på sikkerhetsnivå høyt som utstedes i henhold til norske offentlige krav og EU standard innfrir de høyeste krav til sikkerhet i norsk helsesektor. Alle eID-løsninger som omtales i kapitel 3.4 under *Selvdeklarerte løsninger på høyt sikkerhetsnivå* vil kunne brukes for tilgang til de nasjonale e-helseløsningene med hensyn til sikker identitet.

BankID og *BankID på mobil* er løsninger som leverer eID på sikkerhetsnivå høyt og er derfor kvalifisert for å kunne brukes mot de nasjonale e-helseløsningene. Dette er en to-faktorløsning, i tillegg blir eID-en utlevert ved personlig oppmøte og legitimering, for å unngå at kodegeneratoren til BankID havner i feil hender. For å kunne ta i bruk BankID på mobil må personen allerede ha en nettbankavtale med BankID og kodebrikke. Personen kan bare aktivere BankID på mobil fra banken som tildelte BankID. Når BankID på mobil er aktivert, vil mobiltelefonen fungere som et alternativ til BankID med kodebrikke. BankID tilbyr en trygg autentiseringsmekanisme på stadig flere brukersteder som gjør at brukeren trenger å huske færre brukerkontoer og slipper å spre brukernavn og passord over flere brukerdatabaser.

Påloggingsløsningene helseID og ID-porten har støtte for å kunne velge ulike eID som brukeren kan logge inn med for å benytte eksterne tjenester. Begge løsningene har gode sikkerhetsmekanismer innebygget og baserer seg på internasjonale sikre protokoller. For å støtte ansatt eID som eventuelt en kommune etablerer på nivå høyt, vil helseID være en viktig felleskomponent for å oppnå dette på en sikker måte. I tillegg vil en slik ansatt eID kunne gi automatiske pålogging til eksterne tjenester ved at helseID går god for at den ansatte allerede er logget inn med en eID på høyt nivå ("Single Sign-on").

ID-porten støtter "Single Sign-On" mellom offentlige tjenester. Ved bruk av ID-portens eID-tilbydere via helseID bør applikasjonen sikre at en bruker ikke kan gå videre fra en innlogget helsetjeneste der brukeren er logget inn som ansatt med helseID, til en annen offentlig tjeneste der brukeren er innbygger, uten å måtte logge inn på nytt. Dette for at ikke opplysninger kommer på avveie, ved at andre tar over maskinen. Helsenorge.no godtar ikke "Single Sign-on" til helsenorge.no for innbyggere på liknende grunnlag, dersom en person er logget inn på for eksempel altinn.no, og åpner helsenorge.no, så vil helsenorge.no kreve en ny innlogging.

En av de største truslene for bruk av sikker eID er brukerens eget miljø. Det er viktig å være oppmerksom på at for å oppnå et høyt sikkerhetsnivå på bruk av eID må det stilles krav til systemsikkerhet hos den enkelte bruker som å holde PC og/eller mobil oppdatert, sikre PC og/eller mobil enhet med passord, bruke anti-virus og alltid logge ut etter endt sesjon. Uavhengig av teknisk løsning er man avhengig av at den enkelte bruker også beskytter både passord, kodebrikker og andre sikkerhetselementer ved bruk av eID. Utlån av egen personlig eID til nære relasjoner er en mulig risiko for kommuner som tar i bruk personlig eID må vurdere.

Bruk av personlig eID i en ansattrelasjon kan medføre et større tilgjengelighetskrav til løsningen enn det innbyggerbruk krever. Det er derfor viktig at en kommune gjør en vurdering av om eID-løsningenes tilgjengelighet er tilfredsstillende.

Det pågår et arbeid ledet av Direktoratet for e-helse for å utarbeide en felles tillitsmodell for identitets- og tilgangsstyring som på sikt kan påvirke hvilket sikkerhetsnivå som vil være akseptabelt på tvers av aktørene i helsesektoren, men det er usikkert om det vil føre til endringer i krav til sikkerhetsnivå i helse- og omsorgstjenesten. Det vil sannsynligvis også ta noen år før eventuelle endringer vil kunne innføres. På kort sikt er alternativet derfor å ta utgangspunkt i dagens krav i sektoren.

4.3 Kostnader og investeringsbehov

Kostnader ved eID er spesielt avhengig av kommunens valg av eID-løsning og hvor mange eID som trenger anskaffes. Dersom kommunen åpner for at ansatte kan benytte personlig eID inn i aktuelle løsninger kan nødvendige investeringskostnader reduseres betraktelig. Med en god veileder vil hver enkelt kommune unngå tidsbruk til kartlegging og utredning av løsninger.

En kommune som har besluttet å anskaffe eID til de ansatte vil ha følgende kostnadselementer

1. Tidsbruk for gjennomføring av anskaffelsesaktiviteter for å inngå avtale med aktuell eID-tilbyder
    a. Definere behovet og kravene: hvilke løsninger skal benytte eID, hvor mange ansatte skal ha e-ID
    b. Konkurransegjennomføring: Innhenting og vurdering av tilbud, og inngåelse av avtaler/kontrakt
2. Innkjøp av eID til aktuelle ansatte og tidsbruk for bestilling og innrullering
3. Innkjøp og oppsett av teknisk utstyr, aktuelt ved kortbaserte eID løsninger hvor det er behov for å anskaffe kortlesere til den enkelte "arbeidsstasjon"
4. Installasjon og teknisk tilrettelegging for eID i kommunens infrastruktur

I tillegg kommer driftskostnader:

1. Fornyelse av eID, flere av dagens løsninger har redusert varighet og krever fornyelse for eksempel hvert tredje år. Flere av kostnadselementene ved investering er aktuelle på nytt.
2. Innkjøp av eID til nyansatte og ansatte som har mistet eller ødelagt eID-en
3. Fornyelse av teknisk utstyr som er i ustand

4. Brukskostander, enkelte eID-løsninger har brukskostnader for eksempel BankID på mobil for Telenor kunder.

Boks 4.1 Kostnader til eID ved innføring av kjernejournal i kommuner – ett eksempel

I tabellen nedenfor presenteres et eksempel på beregning av kostnader til eID ved innføring av kjernejournal. I eksemplet er det gjort en sammenligning mellom innkjøp av PKI-kort for ansatte og bruk av BankID på mobil. Eksemplet er basert på omtrentlige estimater for investering og kostnader ved årlig bruk.

Grunnlagstall som benyttes i beregningen	**Liten kommune** < 5000 innbygg.	**Mellomstor kommune** 5 000-20 000 innbygg.	**Stor kommune** 20 000-100 000 innbygg.	**Nasjonalt** alle innbygg.
Gjennomsnittlig antall helsepersonell som trenger tilgang til kjernejournal-portal	20	50	180	25 000
Gjennomsnittlig antall pasientmottak til sykehjem og hjemmetjenester, forventet minste antall pålogging til kjernejournal	160	520	1 860	275 000
Estimater for kostnader til investering og årlig bruk eID ved innføring av kjernejournal, kroner				
eID, alternativ PKI-kort*	**36 000**	**67 500**	**225 000**	**34 250000**
Anskaffelse kort, 700 kroner per ansatt	15 000	35 000	125 000	18 000 000
Anskaffelse kortleser, 500 kroner (1 per 10 ansatte)	1 000	2 500	10 000	1 250 000
Estimert tidsbruk bestilling og innrullering, 1 time per ansatt	10 000	20 000	70 000	10 000 000
Teknisk tilrettelegging for kortleser i infrastruktur, per kommune	10 000	10 000	20 000	5 000 000
eID, alternativ BankID på mobil* *Forutsetter at den enkelte ansatte har BankID og personlig mobil*				
Kostnad årlig innlogging ved pasientmottak og utskrivelse, over mobil for Telenor-kunder, 0,49 kroner per innlogging	150	500	2 000	270 000
Total kostnad	**150**	**500**	**2 000**	**270 000**

* Det kan potensielt komme en kostnad til kommunen for bruken av ID-porten, avhengig av totalbruken. Kostnaden er basert på antall transaksjoner. Se Kva kostar ID-porten?:https://samarbeid.difi.no/felleslosninger/id-porten. Det forventes ikke et høyt antall transaksjoner per kommune for bruken av kjernejournal.

5 Arbeidsgiver- og arbeidstakerrettslige problemstillinger

Arbeidsgiver har en styringsrett som innebærer at arbeidsgiver har en rett til å organisere, lede, kontrollere og fordele arbeidet. Denne styringsretten må som utgangspunkt antas å omfatte rett til å kreve at arbeidstaker legitimerer seg, der det er nødvendig for å utføre arbeidet. Det vil omfatte «tradisjonell» legitimasjon i form av pass, førerkort eller annen godkjent legitimasjon, og også eID. Denne styringsretten kan være begrenset av arbeidstaker ev. rett til å reservere seg mot å anskaffe eID, jf. eforvaltningsforskriften § 9. Styringsretten setter trolig ikke retten til å reservere seg til side.

Rett til å reservere seg gjelder anskaffelse av eID og ikke bruk av eID. Dersom arbeidstaker har eID, vil arbeidsgiver ha anledning til å pålegge arbeidstaker å benytte eID. Hvor mange som benytter eID i dag gir en indikasjon på omfanget av eventuelle reservasjoner.

Når det gjelder muligheten for tariffregulering av anskaffelse av eID så åpner personvernforordningen artikkel 88 for at dette kan gjøres. Det er imidlertid ikke klart at tariffpartene faktisk kan pålegge bruk av eID, også for de som aktivt har reservert seg i medhold av eforvaltningsforskriften. Denne åpner ikke uttrykkelig for tariffregulering, som i realiteten ville fratatt den enkelte mulighet til å reservere seg fra å etablere eID.

Det neste spørsmålet vil være om arbeidsgiver i forbindelse med inngåelse av en ny arbeidsavtale kan stille krav om bruk av eID. I en rekke stillinger stilles det krav for eksempel om at arbeidstaker har en form for sikkerhetsgodkjenning, førerkort osv. Ved ansettelser i stillinger hvor det er nødvendig med eID for å utføre arbeidet, vil dette være et kvalifikasjonskrav ved tilsetting. Bruk av eID i arbeidet vil da også kunne være et vilkår ved tilsettingen. Det kan være arbeidstakere som allerede er tilsatt og som har reservert seg mot eID, og derfor ikke kan utføre alle de oppgaver som i utgangspunktet ligger til stillingen ved en innføring av eID på arbeidsplassen. Arbeidsgiver vil da måtte finne måter å tilrettelegge for arbeidstaker, for eksempel ved at arbeidstaker blir satt til å utføre andre oppgaver.

Tilrettelegging av arbeid skjer i stor utstrekning i dag, og det er ikke holdepunkt for at tilrettelegging som skyldes at arbeidstakere reserverer seg mot eID vil kunne få et omfang som ikke er håndterbart. Det er trolig en helt marginal problemstilling at arbeidstakere reserverer seg mot bruk av eID. Denne rapporten vurderer fordeler og ulemper med bruk av eID som er opprettet av privatperson, og det er klart at den potensielle ulempen ved at enkelte arbeidstakere kan tenkes å reservere seg, ikke er særlig betydelig. Det er fremstår som rimelig klart at de omtalte fordelene med eID som er opprettet av privatperson vil oppveie for denne eventuelle ulempen. eID i form av BankID er i utgangspunktet gratis å anskaffe og benytte. Det er som utgangspunkt ingen kostnader, men dersom det er forutsatt at BankID skal benyttes på en privat mobiltelefon med et privat abonnement, kan det for arbeidstaker være noen kostnader forbundet med slik bruk. Våre undersøkelser tilsier at denne kostnaden trolig er helt marginal. Kostnadene ved slik bruk trolig er mindre enn 10 kroner i måneden selv ved svært utstrakt bruk. Dersom arbeidsgiver ønsker å kompensere slike dokumenterte utgifter, vil det være anledning til å gjøre det.

Det er ikke innenfor arbeidsgivers styringsrett å kreve at arbeidstaker stiller nødvendig utstyr, der slikt utstyr er nødvendig for å utføre arbeidet. Utgangspunktet er at arbeidsgiver stiller nødvendig utstyr. Det ligger for eksempel ikke innenfor arbeidsgivers styringsrett å kreve at arbeidstaker stiller med privat mobiltelefon. Det må derfor klart skilles mellom krav om eID og krav om utstyr.

6 Forslag til tiltak

Arbeidsgruppen viser til at kommunene i sammenheng med innføring av kjernejournal og e-resept har behov for avklaringer om bruk av eID på høyt sikkerhetsnivå for ansatte i helse- og omsorgstjenesten. Behovet er ikke avgrenset til kommunale helse- og omsorgstjenester, men ikke alle har samme krav om høyt sikkerhetsnivå for et så stort antall brukere som denne tjenesten. Dette er bakgrunnen for at arbeidsgruppen anbefaler at det i første omgang utarbeides en veileder for bruk av eID løsninger i helse- og omsorgstjenesten. Dette er et tiltak som raskt kan gjennomføres, og som sammen med pågående tiltak for å støtte innføring av nasjonale e-helseløsninger, svarer på behov i sektoren. Det kan også være aktuelt å vurdere felles anskaffelser og felles kravspesifikasjon som virkemiddel for å styrke innføringen av eID. Videre pågår det et arbeid i regi av Kommunal- og moderniseringsdepartementet med retningslinjer for bruk av ansatt eID som også er relevant for helse- og omsorgstjenesten.

6.1 Veiledning til kommunene om bruk av eID-løsninger

6.1.1 Nasjonal veileder om bruk av eID i kommunal helse- og omsorgstjeneste

Arbeidsgruppen mener at en nasjonal veileder om bruk av eID-løsninger for ansatte i kommunal helse- og omsorgstjeneste kan være et aktuelt tiltak. Helse- og omsorgstjenesten har et særlig behov for informasjon og veiledning i sammenheng med det pågående arbeidet med å innføre nasjonale e-helseløsninger i kommunene. Det bør legges til rette for at veilederen kan danne mønster for tilsvarende veiledning for andre sektorer, eller at den skal kunne utvides til å omfatte andre sektorer etter hvert.

En slik veileder bør ta utgangspunkt i de kravene som gjelder for tilknytning til de nasjonale e-helseløsningene. Kommunene vil også ha behov for eID på andre tjenesteområder, og det bør så langt det er mulig legges til rette for valg som understøtter behov på tvers av sektorer. Det er likevel viktig å ivareta hensynet til behov for avklaringer i sammenheng med pågående innføring av nasjonale e-helseløsninger i kommunene.

En nasjonal veileder bør inneholde omtale av:

- praktisk og pedagogisk informasjon om eID – hva er det og hvorfor trenger vi det?
- kommunenes behov for eID til ansatte, både i helse- og omsorgssektoren og tverrsektorielt
- krav til eID for å ta i bruk de nasjonale e-helseløsningene og sikkerhetsvurderinger knyttet til de ulike eID-løsningene
- tilgjengelige eID-løsninger for ansatte i kommunal helse- og omsorgstjeneste med vurdering av brukervennlighet (mobile løsninger, smittevernhensyn mv.), kostnader og investeringsbehov, håndtering av kostnader ved bruk av personlig eID og andre avtale- og arbeidsrettslige problemstillinger, mm
- HelseID og ID-porten – hva det er og hvorfor det er nyttig og/eller nødvendig for kommunen
- praktiske råd og veiledning om innføring og bruk av ulike eID-løsninger – hvordan kommunen går fram ved bestilling av eID til ansatte, hvilke vurderinger som gjøres, hva som trengs av kartlegging av behov og bruksmønstre, hva som kreves av vedlikehold og administrasjon mm
- eksempler og erfaringer fra andre kommuner som har tatt i bruk eID-løsninger i helse- og omsorgssektoren eller andre sektorer

Siden veilederarbeidet foreslås avgrenset til helse- og omsorgssektoren, anbefaler arbeidsgruppen at arbeidet forankres i styringslinjen til Helse- og omsorgsdepartementet. Det innebærer at Direktoratet for e-helse må ha en sentral rolle som myndighetsorgan på e-helseområdet. Det samme gjelder Norsk Helsenett SF som dataansvarlig for de nasjonale e-helseløsningene. KS må ha en sentral rolle som representant for kommunene for å sikre at veilederen treffer kommunenes behov. Arbeidet må baseres på en nærmere kartlegging av behovene i den kommunale helse- og omsorgstjenesten, og det vil være behov for bred involvering av kommunesektoren for å kartlegge status og sikre at veilederen treffer de behovene kommunene har for avklaringer. I tillegg bør Digitaliseringsdirektoratet involveres for å sikre god samordning med eksisterende løsninger og pågående arbeid som treffer bredere enn helse- og omsorgstjenesten, for å møte kommunesektorens behov.

Som en del av innføring av kjernejournal på sykehjem og i hjemmetjenestene, foregår det erfaringsdeling mellom kommunene når det gjelder bruk av eID i kjernejournal. Dette erfaringsgrunnlaget bygges det videre på i videre utbredelse av de nasjonale e-helseløsningene og kan tas inn i veilederen.

6.1.2 Strategi for bruk av eID og e-signatur i offentlig sektor

Arbeidsgruppen viser i tillegg til regjeringens Digitaliseringsstrategi for offentlig sektor 2019-2025 der det fremgår at: "retningslinjer for bruk av ansatt-ID bør inngå som en del av strategi for bruk av eID og e-signatur i offentlig sektor". Kommunal- og moderniseringsdepartementet vil følge opp dette i arbeidet med ny strategi for bruk av eID i offentlig sektor. Selv om arbeidet vil ha en bredere tilnærming, vil det også være relevant for helse- og omsorgssektoren.

6.2 Felles anskaffelse og felles kravspesifikasjon

Det er krevende for hver enkelt kommune å anskaffe eID. Det krever kompetanse om behov, sikkerhet, tilgjengelige løsninger mv. Arbeidsgruppen har derfor vurdert at det kan være behov for å legge til rette for økt bruk av felles anskaffelser og/eller utarbeidelse av felles kravspesifikasjon.

Felles anskaffelser er gjennomført på enkelte områder tidligere. For eksempel har KS lagt til rette for en felles anskaffelse av elektroniske medisindispensere under koronapandemien. En slik felles anskaffelse sparer den enkelte kommune for tid, samtidig som det letter situasjonen for leverandørene som opplever stor pågang. Det er også en fordel å samle opp behov fra flere kommuner slik at leverandørene kan tilby produkter i et større volum.

Felles kravspesifikasjon som kommunene kan gjenbruke i anskaffelser er også et tiltak som kan gi nytte for kommuner som skal anskaffe løsninger for eID. Gjennom å utarbeide et felles sett med krav, én gang, kan det bli enklere for både kommunene og leverandørene å gjennomføre anskaffelser og finne gode løsninger som dekker kommunenes behov. Det er også ønskelig at produktutviklingen skjer i henhold til kommunenes behov.

6.3 Andre nasjonale tiltak som pågår og har relevans for arbeid med eID

Det er et mål at de nasjonale e-helseløsningene skal innføres og tas i bruk av alle relevante aktører i helse- og omsorgstjenesten. De nasjonale e-helseløsningene er i stor grad tatt i bruk i spesialisthelsetjenesten, av fastleger, legevakter og apotek. Så langt har de nasjonale e-helseløsningene ikke vært tilgjengelig i systemene til de øvrige kommunale helse- og omsorgstjenestene. Sykehjem og hjemmetjenestene i kommunene får etter planen tilgang til kjernejournal i løpet av 2020. Det pågår arbeid for å legge til rette for at de kommunale helse- og omsorgstjenestene kan ta i bruk e-resept. Når tjenestene får tilgang til de nasjonale e-helseløsningene, oppstår behovet for å ta i bruk eID. Kjernejournal er det første systemet som utløser behov for eID for større grupper ansatte i helse- og omsorgstjenesten i kommunene.

Det nasjonale e-helsearbeidet er nå i en fase der det er nødvendig å synliggjøre avhengigheter og forutsetninger for innføring, både mellom eksisterende nasjonale e-helseløsninger og mellom disse løsningene og Akson. KS har pekt på behovet for forutsigbare og realistiske planer for sektorens bruk av funksjonalitet for helhetlig samhandling og som viser sammenheng mellom de ulike nasjonale e-helsetiltakene. Det er viktig å synliggjøre på hvilket tidspunkt de ulike aktørene skal og kan ta i bruk hvilke løsninger og hvilken funksjonalitet, og avhengigheter mellom de ulike innføringsløpene. Helse- og omsorgsdepartementet har i brev av 29. april bedt Direktoratet for e-helse utarbeide et helhetlig veikart for utvikling og innføring av de nasjonale e-helseløsningene. Veikartet skal utarbeides i samarbeid med aktørene i helse- og omsorgssektoren, herunder Helsedirektoratet, Norsk Helsenett SF, de regionale helseforetakene, og KS og kommunesektoren.

Både Direktoratet for e-helse og Norsk Helsenett SF er gjennom oppdrag i 2020 bedt om å bistå i arbeidet med å styrke innføringen i kommunene, herunder utarbeide innføringsplaner for de nasjonale e-helseløsningene. Videre samarbeider Helse- og omsorgsdepartementet og KS om en mulig samarbeidsavtale om innføring av nasjonale e-helseløsninger i kommunene. Et av de aktuelle

samarbeidstiltakene er å sikre gode anbefalinger om hvordan e-ID, helseID og andre nødvendige løsninger kan håndteres i kommunal sektor. KS e-helse kompetansenettverk skal også bistå det nasjonale prosjektet i innføring.

Kommunal sektor har de siste årene begynt å gjøre mer sammen på digitaliseringsområdet, og har gjennom KS etablert samstyringsmekanismer for digitaliseringsarbeidet. KS sin rolle med å koordinere og samordne digitaliseringsarbeidet i kommunal sektor er under utvikling. Det er etablert en samstyringsmodell for digitalisering i kommunal sektor, KommIT-rådet med underliggende utvalg. KS og kommunene har etablerte nettverkssamarbeid regionalt (regionale digitaliseringsnettverk) og nasjonalt (KS e-helse kompetansenettverk og Nasjonalt velferdsteknologiprogram) for å bidra til økt gjennomføringskraft i det nasjonale e-helsearbeidet. Slike nettverk kan legge til rette for å dele kompetanse og erfaringer mellom kommunene, også på eID-området. I Nasjonal helse- og sykehusplan 2020-2023, Meld. St. 7 (2019-2020), løftes behovet for å understøtte digitaliseringen i kommunene. Videreutvikling av innføringsapparatet for eksisterende nasjonale e-helseløsninger i kommunene i samarbeid med KS er et av virkemidlene som trekkes fram for å bidra til å øke innføringstakten og redusere risiko i digitaliseringsarbeidet i kommunene.

Det pågår videre et arbeid med felles tillitsmodell i regi av Direktoratet for e-helse, jf. kapittel 4.2, som vil inkludere utredning av om krav til sikkerhetsnivå for eID kan nedjusteres noe ved etablering av en felles tillitsmodell i helse- og omsorgssektoren. Dette er arbeid med et langsiktig perspektiv og justeringer av krav må eventuelt følges opp når det foreligger anbefalinger.

Boks 6.1 Forslag til oppfølging

- Utarbeide en nasjonal veileder om bruk av eID i kommunal helse- og omsorgstjeneste. Arbeidet forankres i styringslinjen til Helse- og omsorgsdepartementet og gjennomføres i samarbeid mellom Direktoratet for e-helse, Norsk Helsenett SF, KS og Digitaliseringsdirektoratet. Det bør vurderes hvordan nasjonalt utvalg for fag og arkitektur (NUFA) og andre fora i den nasjonale styringsmodellen for e-helse kan trekkes inn i arbeidet.
- Gjennomføre en nærmere kartlegging av behovet i kommunene med utgangspunkt i KS e-komp og andre relevante nettverk i regi av KS
- Veilederarbeidet ses i sammenheng med arbeidet med ny strategi for bruk av eID i offentlig sektor
- Vurdere om felles anskaffelse og felles kravspesifikasjon kan være egnet tiltak for å forenkle innføring av eID i kommunal helse- og omsorgstjeneste.
- eID synliggjøres som forutsetning for innføring av nasjonale e-helseløsninger i veikart, innføringsplaner, samarbeidsavtale mv.

7 Økonomiske og administrative konsekvenser

Arbeidet med å utforme og formidle en veileder vil ha begrensede økonomiske og administrative konsekvenser. Det samme gjelder arbeidet med å gjennomføre en nærmere kartlegging og vurdering av behov i helse- og omsorgssektoren, utrede en eventuell felles anskaffelse og kravspesifikasjon, og synliggjøre eID som forutsetning for innføring av nasjonale e-helseløsninger i pågående arbeid og planer. Økonomiske og administrative konsekvenser for kommunene ved innføring av eID avhenger av valg av løsning og vil blant annet være et tema i veilederarbeidet.

Vedlegg 1: Dagens eID-løsninger

Norge er blant de fremste i verden når det gjelder utbredelse og bruk av eID. Sammen med høy kvalitet i folkeregisteret og én varig identifikator i fødselsnummer og D-nummer har det gitt oss en fordel i digitalisering av samfunnet. Bruk av eID i offentlig sektor er i hovedsak basert på kjøp fra private leverandører og samarbeid med andre samfunnssektorer som bank og finans. eID har vært helt nødvendige for å lage personaliserte tjenester på nettet.

Enklere eID-løsninger er gjerne basert på bruk av passord og kodelister. Sikrere løsninger er i hovedsak bygd rundt en infrastruktur med offentlige og private asymmetriske nøkler. PKI (Public Key infrastructure) er et eksempel på dette. Med asymmetriske nøkler benyttes private, kryptografiske nøkler som hemmeligheter. Tradisjonelt har de private nøklene blitt oppbevart privat, i smartkort, USB-pinne eller Sim-kort. I sentrallagret eID-løsninger, som for eksempel BankID, lagres nøklene trygt hos eID-leverandøren.

Løsninger på høyt sikkerhetsnivå

BankID og BankID på Mobil er eID-løsninger som tilbys av bankene i Norge og er basert på en felles infrastruktur som er utviklet av banknæringen i fellesskap. BankID er en personlig elektronisk legitimasjon for sikker identifisering på nettet. BankID fungerer i alle norske banker og på offentlige tjenester. I tillegg kan BankID benyttes til å signere avtaler og til å identifisere den enkelte på ulike tjenester. For å få BankID må innbygger legitimere seg med pass og oppmøte. BankID skiller mellom PersonBankID som kan benyttes til innlogging i nettbank og på andre brukersteder hvor BankID kan benyttes, og AnsattBankID som kan brukes når en ansatt signerer for bedriften og som knytter fødselsnummer opp mot bedriftens organisasjonsnummer.

Med BankID identifiserer innbyggeren seg gjennom å bruke fødselsnummer sammen med koden fra en kodebrikke eller applikasjon, og et personlig passord. Med BankID på mobil benyttes mobilnummer, fødselsdato og en selvvalgt pinkode. BankID på mobil tilbys av alle operatører og nesten alle banker, og har tilsvarende bruksområde som vanlig BankID. Noen mobiloperatører tar betalt for bruk av BankID på mobil. I dag har ca. 4 millioner nordmenn BankID, enten med kodebrikke og/eller applikasjon eller på mobil. BankID brukes av alle landets banker, offentlige digitale tjenester og av stadig flere virksomheter i ulike bransjer. BankID kan benyttes for å signere elektronisk på vegne av bedrift eller arbeidsplass. På samme måte som signering av en avtale med penn på vegne av bedriften, kan den ansatte benytte egen BankID ved signering av en avtale elektronisk. Elektronisk signering er likestilt med fysisk signatur.

BuyPass AS er en kommersiell eID-leverandør som tilbyr flere eID løsninger på betydelig og høyt sikkerhetsnivå. BuyPass er en stor leverandør til helsesektoren. BuyPass smartkort er en PKI basert eID på høyt sikkerhetsnivå. I kortet lagres nøkler for BuyPass eID på høyt nivå, men også sektorspesifikke eller bedriftsinterne eID-løsninger kan lagres. Kortet kan også tilrettelegges for fysisk tilgangsstyring som dørlåser med mer. BuyPass-kort kan personaliseres med bilde og personalia og fungerer derfor også som ID-kort for ansatte. Kortet kan bestilles fra BuyPass på nett eller via administrasjonsløsninger, men også produseres på brukerstedet. Det siste krever spesialutstyr og opplæring av personell. For å bruke BuyPass smartkort på PC eller annet utstyr må brukeren ha tilgang til kortleser. Mellom 3-400 000 bruker BuyPass-ID på høyt nivå. BuyPass-ID i Mobil er en applikasjon løsning hvor mobiltelefonen brukes til innlogging. Den er basert på sentral lagrede PKI nøkler. Simkort benyttes ikke i løsning. For de som har Buypass-kort fra før er det enkelt å aktivere BuyPass-ID i mobil. Nye brukere må gjennom en innrullering som i hovedtrekk er den samme som for BuyPass-kort. Buypass har startet arbeidet med passordløs eID på høyt sikkerhetsnivå, bygd på fido2 teknologi. Fido2 beskrives nærmere i vedlegg 3 teknologisk utvikling.

Commfides er en privat leverandør som tilbyr eID på høyt sikkerhetsnivå rettet mot bedriftsmarkedet. Helsesektoren er en viktig kunde. eID fra Commfides er en PKI-basert eID som lagres på chip i en USB-pinne eller smartkort. Ved bruk av USP-pinne er det ikke nødvendig med kortleser, men enheten må støtte nødvendig programvare og ha en USB-port. eID for Commfides kan bestilles på nettet eller via tilrettelagte bedriftsløsninger. PKI sertifikatene inneholder knytting til bedriften. eID fra Commfides kan på ulike vis integreres mot bedriftens prosesser. Som for Buypass tilbys løsninger for å utstede kortet lokalt i tillegg til bestilling på nettet.

I helsesektoren er BankID, Buypass og Commfides tilgjengelig gjennom ID-porten og koblingen til helseID.

Selvdeklarerte løsninger på betydelig sikkerhetsnivå

MinID [6]utstedes av Digitaliseringsdirektoratet for bruk i offentlig sektor. Den tidligste versjonen av løsningen ble etablert i 2006. MinID har omtrent lik utbredelse som BankID, men bruken er lavere. I MinID benyttes både pinkode-kort eller engangsmeldinger på SMS i tillegg til passord. MinID kan bestilles på direktoratets nettsider. MinID sendes til brukerens folkeregistrerte adresse. MinID kan brukes både av innbyggeren og ansatte i offentlig sektor. I helsesektoren er MinID tilgjengelig gjennom ID-porten og koblingen til helseID.

Buypass har levert tippekort til Norsk tipping spillere i en årrekke. Kortet fungerer som en eID på mellomhøyt sikkerhetsnivå og er PKI basert. Ca. 2,1 mill. i befolkningen har spillekort fra BuyPass. Kortet er likt BuyPass ordinære smartkort og kan oppgraderes til høyt sikkerhetsnivå.

Løsninger på lavere sikkerhetsnivå

I kommunene finnes det i dag mange løsninger for håndtering av identitet og autentisering av ansatte, som bruk av Microsoft Active Directory internt i kommunen, men de har vanligvis lavere sikkerhetsnivå enn det som kreves av de nasjonale e-helseløsningene.

Feide er utdanningssektorens løsning for elever og ansatte. Feide omfatter både pålogging og tilgangsstyring. For påloggingen benyttes Feide eID. I utgangspunktet tilbys brukernavn og passord for pålogging på lavere sikkerhetsnivå. Det tilbys også sterkere autentisering for ansatte med engangskode fra SMS eller godkjenner-klient (Google Authenticator). Feide har stor utbredelse i utdanningssektoren med svært hyppig bruk, men oppfyller ikke høyt sikkerhetsnivå.

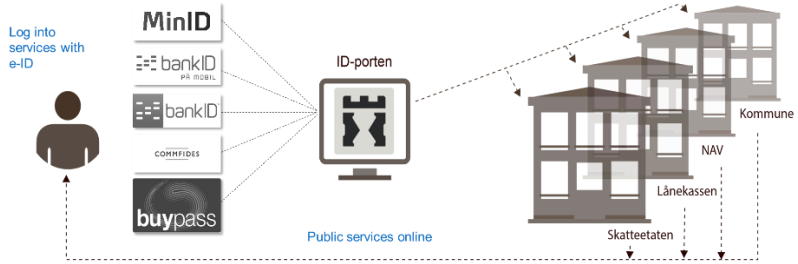
[6] MinID som beskrevet her er ikke en eID-løsning som er godkjent på sikkerhetsnivå betydelig, men tilsvarer tidligere nivå 3. Det er noen forskjeller mellom nivå 3 og sikkerhetsnivå betydelig. Digdir har imidlertid selvdeklarert en ny MinID som har en annen innrulleringssprosess enn den som er beskrevet her.

Vedlegg 2: Offentlige infrastrukturer for pålogging

I det offentlige er det flere relevante eID-infrastrukturer som gjør den mulig å benytte eID for pålogging samt å koble denne til tilgangsstyring.

ID-porten

ID-porten er en felles innloggingsløsning for mange offentlige tjenester på internett, for bruk av alle innbyggere i Norge. Gjennom Digitaliseringsrundskrivet er sentralforvaltningen instruert om å ta i bruk ID-porten for «digitale tjenester som krever innlogging og autentisering».



Figur 2.? ID-porten

HelseID

HelseID er en felles innloggingsløsning for helsesektoren, for bruk av ansatte i helse- og omsorgstjenesten. HelseID introduserer ikke en ny eID, men legger til rette for gjenbruk av eID-er som er i bruk i sektoren. For pålogging med høyt sikkerhetsnivå gjenbruker helseID den nasjonale felleskomponenten ID-porten, samtidig som det legges til rette for at helsetjenesten også kan gjenbruke eID-løsninger som de allerede anvender på tilstrekkelig sikkerhetsnivå. HelseID består av ulike funksjoner som i praksis ofte kombineres for å tilby en totalfunksjonalitet og for å realisere ulike bruksscenarioer. I hovedsak kan funksjonaliteten deles inn i fire områder:

1. Brukerautentisering

HelseID kan bidra til å *autentisere* (verifisere/bekrefte) helsepersonellets digitale identitet. HelseID vil da i samspill med identitetstilbyderen autentisere at helsepersonellet er den vedkommende gir seg ut for å være. I tillegg kan HelseID berike helsepersonellets identitetsdetaljer med informasjon fra nasjonale registre, slik som HPR-nummer fra Helsepersonellregisteret.

Typiske bruksformål for denne funksjonalitet er å kunne gi helsepersonell tilgang til et lokalt fagsystem eller en nasjonal nettjeneste med helseopplysninger. De aktuelle fagsystemene og nettjenestene overlater da pålogging til helseID, og slik sett tilbyr helseID "pålogging-som-en-tjeneste". Dette gir en enhetlig brukeropplevelse uavhengig av fagsystem og helsevirksomhet, og legger samtidig til rette for engangspålogging ("Single Sign-On").

2. System- og virksomhetsautentisering

HelseID kan *autentisere* (verifisere/bekrefte) at et system er det det gir seg ut for å være. I dette ligger blant annet å verifisere hvilken virksomhet som er ansvarlig for det aktuelle systemet, samt å vurdere ulike egenskaper ved systemet.

Et typisk bruksformål for denne funksjonaliteten er system-til-system kommunikasjon, der ulike systemer trenger å kunne stole på hverandres "identitet" før informasjonsutveksling finner sted, og eventuelt for å kunne gjennomføre egen tilgangskontroll.

3. Systemautorisering

HelseID kan *autorisere* (vurdere og beslutte) om et aktuelt system skal gis tilgang til å kommunisere med en aktuell tjenestetilbyder og dennes API. Vurderingen gjøres typisk basert på hva tjenestetilbyderen på forhånd har konfigurert i HelseID at det aktuelle systemet har tillatelse til. Denne funksjonaliteten kalles også "sikring av API", ettersom HelseID beskytter tilgangen til API-et.

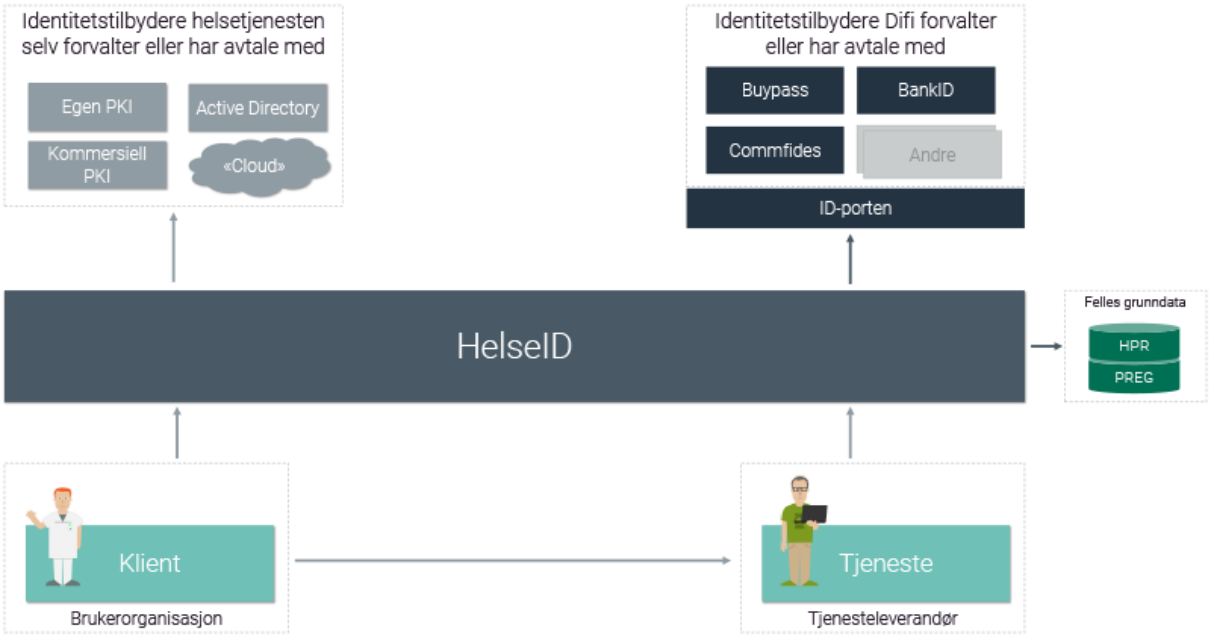
4. Portal for eID-tilbydere

HelseID tilbyr en portal for eID-tilbydere. Her kan helsepersonell velge mellom ulike tilbydere av eID-er som er støttet av HelseID (utvalget kan begrenses av helsevirksomheten). Typiske tilbydere her er kommersielle aktører som BuyPass, BankID og Commfides, men det jobbes også med potensielle sektorinterne identitetstilbydere, slik som regionale helseforetak.

Dette konseptet kalles "eksternalisert identitet", og muliggjør at helsepersonell og helsevirksomheter får valgfrihet i hvilken eID de ønsker å bruke.

Et typisk eksempel er at helsepersonell via sitt fagsystem ønsker tilgang til helseopplysninger fra en tjenestetilbyder sitt API. Da kombineres hovedsakelig brukerautentisering med både system- og virksomhetsautentisering. Det gjøres for å kunne gi tjenestetilbyderen pålitelig informasjon om både helsepersonellet som ønsker tilgang, hvor henvendelsen kommer fra, og om systemet har rett til å kalle tjenestetilbyderens API. I tillegg, og som del av brukerautentiseringen, vil helsepersonellet benytte portalen for eID-tilbydere for å autentisere seg hos ønsket identitetstilbyder.

For at kommune skal kunne slå opp i Kjernejournal må de bruke HelseID, dette på grunn av krav til sikkerhet som er satt for systemet. For eksempel har Kjernejournal behov for å ha kontroll på hvor henvendelsen kommer fra, og har vurdert at tjenesten HelseID løser dette kravet best.



Figur 1 Aktørskisse for HelseID

Feide tilgangsstyring

Feide er den nasjonale løsningen for sikker innlogging og datadeling i utdanning og forskning. Med Feide som eID benytter elever, studenter, forskere og undervisere ett og samme brukernavn og passord til å logge inn på alle tjenester som har Feide som innloggingsløsning. Det betyr at de slipper å huske brukernavn og passord for ulike tjenester. Feide opprettes og endres av organisasjonen den enkelte tilhører, f.eks. NTNU eller Oslo kommune, og brukerinformasjon administreres og lagres lokalt hos organisasjonen. Hvis passord skal endres, gjøres ikke dette for hver tjeneste brukeren benytter, men én gang av organisasjonen.

Høsten 2018 ble Feide og Dataporten slått sammen til én tjeneste, og denne har fått navnet Nye Feide. Nye Feide har tidligere også blitt omtalt som Feide 2.0. Tjenesten har ny funksjonalitet som sørger for enkel og sikker deling av data, bedre brukeropplevelse ved innlogging og styrket personvern, samtidig som den tilrettelegger for innovasjon og utvikling av nye utdanningstjenester. Feide leveres av Uninett AS som samarbeider med Utdanningsdirektoratet og Unit om forvaltningen av tjenesten.

Vedlegg 3: Teknologisk utvikling og muligheter framover

De siste 10-15 årene har tilnærming til eID vært stabil. Det er nå i endring. Ny teknologi gir nye muligheter i alle deler av en eIDs livssyklus denne kan gjerne deles i tre deler: 1) innrullering, 2) identifikasjonsfaktorer og 3) autentisering.

Innrullering av nye brukere

Det store kostnadene og brukertersklene ved eID er gjerne knyttet til innrullering av nye brukere. På høyt sikkerhetsnivå har kravet vært kontroll av ID-dokumenter ved personlig oppmøte, mens det på betydelig sikkerhetsnivå har vært utsendelse til folkeregistret adresse. Det nye regelverket åpner imidlertid for nye muligheter med digital ID-kontroll, innrullering med annen eID på høyt sikkerhetsnivå, bruk av identifikasjonsfaktorer og enklere autentiseringsprosesser.

Moderne maskinlæring har gjort mulig å lage algoritmer for digital ID-kontroll som kan sammenligne personer med bilder og video like godt som et menneske. Metodene kan fremover trolig gjøre en bedre jobb enn de fleste menneskelige kontrollører. Chipen i modere ID-dokumenter som pass og ID-kort inneholder høy oppløselige bilder som kan benyttes til slik sammenligning. Digdir har sammen med Nav laget en midlertidig versjon av MinID som benytter digital Id-kontroll for å gi eID til hjemreiste gjestearbeidere.

Regelverket åpner også for at en annen eID kan benyttes for innrullering i eID på samme sikkerhetsnivå. Slik kan for eksempel BankID benyttes til innrullere offentlig ansatte i en eID-løsning som kun benyttes for ansattbruk. Mekanismen brukes allerede av BuyPass.

Identifikasjonsfaktorer

Ny teknologi gjør det mulig å lage identifikasjonsfaktorer (hemmeligheter) som kan brukes i en eID. Glemte passord er en av de store utfordringene med dagens eID løsninger. Alternative tilnærminger som mønsteret og elementer som er lettere å huske har vært forsøkt for å erstatte passordet, men det har så langt hatt begrenset suksess.

Tidligere har metodene vært begrenset til pinkodekort, kodekalkulatorer og smartkort, men nå omgir vi oss nå med mange enheter som kan benyttes som bærer av eID. Moderne programvare gjør det mulig å lage apper på telefonen som er motstandsdyktige nok mot angrep og enkelt kan tas i bruk. Moderne telefoner kan bindes til bruker gjennom biometri som lagres i telefon. Sammen med andre sikkerhetsmekanismer blir det vanskelige for andre å benytte telefonen til autentisering. Andre enheter som smartklokker vil trolig fremover oppdage om den bæres av rett bruker ved hjelp av biometri. Yubico er et eksempel hardwarenøkler som er enkle i bruk og lett kan rulles ut i organisasjonen, og som heller ikke krever kortleser som dagens smart kort: https://www.yubico.com/.

Biometri har tidligere vært vanskelig å bruke i eID-løsninger fordi avleserutstyr som kamera, fingeravtrykkleser eller andre sensorer ikke har vært tilgjengelig for brukeren når han skal identifisere seg. Det har vært stor utvikling i sensorer særlig på mobiltelefoner hvor ansikts- og fingeravtrykkbiometri nå brukes som standard for å låse opp telefonen eller til andre funksjoner. Det har også blitt vanlig å benytte slike løsninger til for eksempel tilgang til nettbank. I Frankrike etableres nå en offentlig eID-løsning hvor bekreftet ansiktsbilder lagres lokalt i telefonen som en del av eID-løsningen. Disse benyttes som biometrisk sammenligning av brukeren. Sentralt lagret biometri vil gi enkle og brukervennlige løsninger, men det har så langt ikke vært mulig å realisere på grunn av personvernbekymringer.

Autentisering

Ny teknologi gjør det også mulig å forenkle selve autentiseringsprosessen. En av de store svakhetene med internetteknologien er manglende standarder for autentisering direkte mot web-lesere. Det har derfor vært nødvending å lage tilpassede autentiseringsløsninger som for eksempel ID-porten. Arbeidet som er lagt ned i Fido-standardene gjør det mulig å autentisere seg direkte i nettjenester uten mellomsteg. En mekanisme kan derfor enkelt gjenbrukes over svært mange nettløsninger. Fido-løsninger kombinert med hardware-nøkler kan gi en svært enkel brukeropplevelse og anvendelige løsninger: https://fidoalliance.org/fido2/

Nye leverandører i det norske markedet
Ferja eID er en eID-leverandør som er veletablert for eksempel i Sverige. Ferja eID er en appbasert løsning hvor brukeren kan oppgraderes til høyere sikkerhets etter hvert som det er nødvendig. Det gjør det enkelt å ta løsningen i bruk og dyre prosesser rundt innrullering gjennomføres først når det kreves av tjenesten. Ferja eID er tilrettelagt digital ID-kontroll og kan også fungere som et digitalt ID-kort på mobiltelefonen. Ferja ID etablerer seg nå i Norge og forventes å selvdeklarere løsningen sin på Høyt nivå innen kort tid.

Nasjonalt ID-kort skal lanseres i løpet av 2020. I første omgang blir kortet tilgjengelig for norske statsborgere. Fra flere er det ønske om å gi kortet til statsborgere fra andre land med tilknytning til Norge, men det er ikke besluttet politisk. eID på nasjonalt ID-kort er utsatt og det er uklart når eller om det det blir lansert. Det er ikke rimelig å forvente at det blir tilgjengelig for sektoren i løpet av kort tid. eID på nasjonalt ID-kort er planlagt som en PKI-løsning, hvor nøkler lagres lokalt på selve kortet. Løsninger for mobiltelefon er ikke presentert, men kortet støtter NFC-lesning. Løsning vil være gratis for sektoren, men den ansatte må betale gebyr for nasjonalt ID-kort. Det er viktig å merke seg er at ikke alle automatisk får Nasjonalt ID-kort. Det er frivillig å ha et nasjonalt ID-kort.

Buypass har startet arbeidet med passordløs eID på høyt sikkerhetsnivå bygd på fido2-teknologi. Forslaget benytter flere ulike nye teknologier og er ment å forenkle brukeropplevelse i helsesektoren. Nye nettlesere har innebygg støtte for autentisering basert på fido2 webauth-standarden. Løsningen fra Buypass utnytter dette og kan derfor lett integreres direkte mot tjenester i sektoren. Istedenfor smartkort benyttes Yubico nøkler som støtter Fido2. Nøklene kan kommunisere med utstyr på ulike måter som USB og NFC. Det er derfor lettere å bruke dem mot forskjellige enheter enn smartkortlesere. Brukeren vil heller ikke være avhengig av å benytte sin egen telefon i arbeidet. Forslaget fra BuyPass benytter også en passleser-app for innrullering av brukeren slik at personlig oppmøte ikke trenger å gjennomføres. Nøklene fra Yubico må ikke personaliseres på forhånd og kan kjøpes inn direkte av virksomheten og leveres ut til brukeren.

Flere internasjonale leverandører tilbyr eID-løsninger. Både Google, Microsoft og Facebook har sikre og brukervennlige løsninger, men de vil være vanskelige å bruke i sektoren. De forholder seg ikke til norsk regelverk og kan derfor ikke lett kobles til norske sikkerhetsnivåer. Det er heller ikke kobling til norske identifikatorer og det er vanskelig å gjenkjenne brukerne på tvers av systemer.