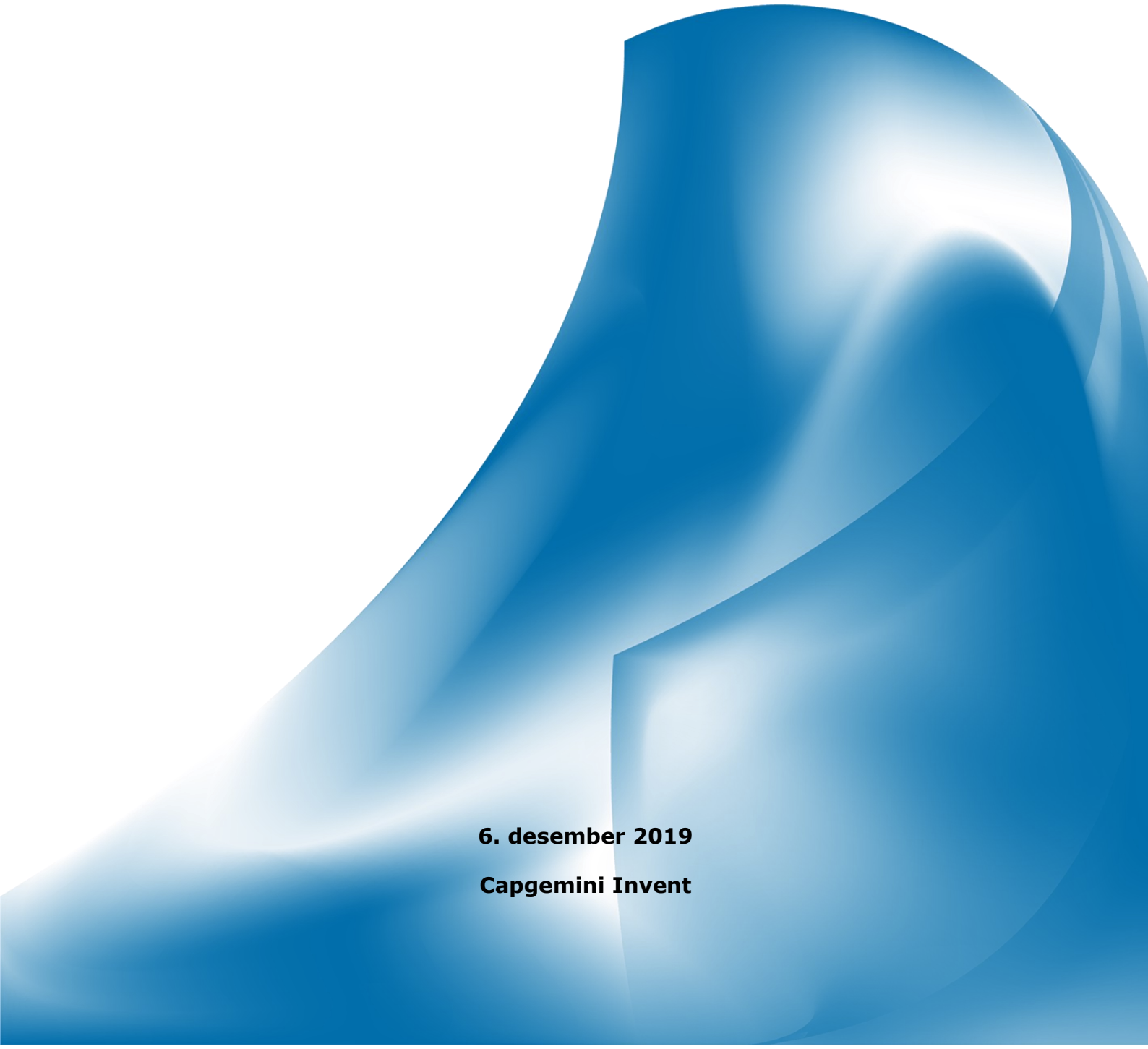
O M R Å D E G J E N N O M G A N G

ID-forvaltningen – tilleggsrapport



6. desember 2019

Capgemini Invent

Innholdsfortegnelse

Sammendrag

Formålet med områdegjennomgangen er å kartlegge om dagens ID-forvaltning er innrettet og organisert på en hensiktsmessig og kostnadseffektiv måte, og på bakgrunn av dette vurdere og foreslå alternative tiltak som vil gi økt sikkerhet, mer effektiv ressursbruk og økt brukervennlighet. Arbeidet med områdegjennomgangen for ID-forvaltningen ble igangsatt i april med leveranse av en hovedrapport 6. september. Med utgangspunkt i hovedrapporten ble leverandøren tildelt et tilleggsoppdrag med vektlegging av tre tema: *fysiske ID-bevis og utbredelse av nasjonalt ID-kort*, *eID* og *styring og struktur*. For hvert tema har oppdragsgiver spesifisert utvalgte problemstillinger som leverandøren har vurdert og det er knyttet anbefalinger til.

Anbefalingene i tilleggsoppdraget er utarbeidet for å bygge opp under anbefalt visjon for ID-forvaltningen «*én person, én identitet i Norge»,* samt anbefalte hovedmål og delmål med forventning om økt sikkerhet, brukervennlighet og ressurseffektivitet.

Tilleggsoppdraget er gjennomført i perioden september til desember 2019. Oppdragsgiver er Finansdepartementet (FIN), Justis- og beredskapsdepartementet (JD), Samferdselsdepartementet (SD), Kommunal- og moderniseringsdepartementet (KMD), samt Arbeids- og sosialdepartementet (ASD) og leverandøren er Capgemini Invent, med støtte fra advokatfirmaet BAHR AS. Vurderinger og anbefalinger som fremkommer i rapporten er leverandørens egne.

Vurderinger og anbefalinger tema 1 – Fysiske ID-bevis og nasjonalt ID-kort

For å holde oversikt over personer som er bosatt i Norge eller har en annen tilknytning til Norge tildeler norske myndigheter et identitetsnummer i form av fødselsnummer eller et midlertidig d-nummer. Identitetsnummeret registreres i Folkeregisteret, som er det sentrale personregisteret i Norge. En person registreres som «kontrollert» dersom identiteten er registrert på grunnlag av fødselsmelding eller kontrollert ved personlig oppmøte hos Skatteetaten eller utlendingsmyndighetene. For øvrig benyttes kategorien «ikke-kontrollert». Det pågår nå et arbeid med å etablere kategorien «unik» i Folkeregisteret. En «unik» identitet tilkjennegis ved ett identitetsnummer som er «låst» til én person i Norge ved bruk av biometri. Det er bare for individer registrert som «unik» at en kan være sikker på at personen er registrert med kun ett identitetsnummer i Folkeregisteret. Etablering og omfang av «unike» identiteter i Folkeregisteret har dermed stor betydning for visjonen om «én person, en identitet i Norge»

Det finnes i dag en rekke ID-bevis i omløp som i praksis aksepteres til legitimasjonsformål. Tilgangen til sikre ID-bevis varierer på tvers av ulike brukergrupper. For norske borgere er pass per i dag det eneste ID-beviset som med høy grad av sikkerhet kobler identitet til identitetsnummeret i Folkeregisteret. Utenlandske borgere med tilknytning til Norge har i dag ikke tilbud om et sikkert identitetsbevis med en slik kobling, men vil kunne få det med nasjonalt ID-kort utstedt av norske myndigheter. Utstedelse av nasjonalt ID-kort skal på lik linje med passutstedelse kunne danne grunnlag for registrering av status «unik».

Leverandøren har som del av arbeidet med tema 1 vurdert ulike alternativ for hvilke brukere som skal få tilbud om nasjonalt ID-kort og alternativ for krav til fremvisning. Behovet for bedre ID-kontroll hos utvalgte tjenesteeiere er vurdert. Det er videre vurdert hvordan EØS-/tredjelandsborgere kan oppnå status «unik» i Folkeregisteret, samt hva som gjenstår av tilrettelegging for å få registrert personer som «unike» i Folkeregisteret. I vurderingene av hvem som skal få tilbud om nasjonalt ID-kort er visjonen for ID-forvaltningen «én person, én identitet i Norge», og at enhver som får

tildelt et norsk identitetsnummer skal gis muligheten til å bevise sin knytning til tildelt identitetsnummer, gjennom et sterkt ID-bevis, tillagt stor vekt.

Nasjonalt ID-kort tilbys til alle med rett på fødselsnummer eller d-nummer, med unntak av asylsøkere. Tilbudet om nasjonalt ID-kort inkluderer borgere med begrenset opphold i Norge grunnet ikke sannsynliggjort identitet

Leverandøren anbefaler at nasjonalt ID-kort tilbys alle med rett på fødselsnummer eller d-nummer, med unntak av asylsøkere. Tilbudet omfatter norske borgere, EØS-borgere og tredjelandsborgere. Anbefalingen inkluderer borgere med begrenset opphold i Norge grunnet ikke sannsynliggjort identitet. Leverandøren anser det nasjonale ID-kortet som det beste virkemiddelet for at utenlandske brukergrupper skal kunne bevise sin tilknytning til et norsk identitetsnummer. Et bredt tilbud om nasjonalt ID-kort muliggjør at tjenesteeiere kan stille krav om fremvisning ved fysisk oppmøte som legitimasjonsgrunnlag for tilgang til tjenester.

Gjennomføre tiltak som vil bidra til høy utbredelse av det nasjonale ID-kortet

Leverandøren anbefaler flere tiltak for å stimulere til høy utbredelse av nasjonalt ID-kort. Et sentralt grep, slik anbefalt i hovedrapporten, vil være å tydeliggjøre i regelverket at norsk pass og nasjonalt ID-kort skal utgjøre de eneste gyldige fysiske ID-bevisene utstedt av norske myndigheter. Leverandøren anbefaler også at det gjennomføres en koordinert innsats på tvers av forvaltningen for å informere om og tydeliggjøre konsekvensene av et slikt regelverk. Leverandørens øvrige anbefalinger om et felles skrankepunkt og styrking av krav i utstedelsesprosessen av norske private eID-er, som beskrevet nedenfor, vil i stor grad understøtte utbredelsen av nasjonalt ID-kort.

Krav om «kontrollert» og på sikt «unik» identitet for tilgang til utvalgte offentlige ytelser og tjenester, slik det er anbefalt i hovedrapporten, vil også sikre utbredelse av nasjonalt ID-kort. Uten at det direkte har vært en del av mandatet, vurderer leverandøren at et krav til «unik» fra tjenesteeiere for utvalgte tjenester er mer målrettet enn et krav om ID-bevisene norsk pass eller nasjonalt ID-kort. Et krav til «unik» gir virkning for fysisk og elektronisk identifikasjon, uavhengig av hvilke ID-bevis som betraktes som gyldige.

Vurdere krav om norsk pass eller nasjonalt ID-kort for førstegangstildeling av skattekort

Leverandøren har vurdert ulike alternativ for å stille krav om fremvisning av nasjonalt ID-kort eller norsk pass for tilgang til sentrale tjenester og ytelser hos Skatteetaten og NAV. Det varierer i dag hvorvidt det gjennomføres ID-kontroll med fysiske ID-bevis for tilgang til tjenester og ytelser, og hvilke ID-bevis som godtas.

Leverandøren vurderer at det er tjenesteeiere selv som i siste instans må vurdere om det skal stilles krav om nasjonalt ID-kort eller norsk pass for tilgang til de enkelte tjenester og ytelser, og gi eventuelle nødvendige unntak der det er hensiktsmessig, basert på en helhetlig risikovurdering. Leverandøren begrunner dette med at belastningen et slikt krav vil medføre for bruker må vurderes opp mot risikoen ved å unnlate å stille et slikt krav, og at denne vurderingen vil være ulik for ulike tjenester og ytelser. For å tilrettelegge for muligheten til å stille krav anbefales det at tjenesteeiere gis hjemmel i sine respektive særlovgivninger til å stille krav om norsk pass eller nasjonalt ID-kort og/eller kontroll ved fysisk oppmøte som forutsetning for tjenesteytelse, der det sees behov for dette. Det er videre viktig at tjenesteeiere etablerer et tett samarbeid med pass- og ID-kortmyndigheten samt utlendingsmyndighetene om hvilke tjenester og ytelser det bør stilles krav for.

Eventuelle krav til EØS-borgere og deres familiemedlemmer må være i henhold til EØS-regelverket. Det anbefales at handlingsrommet for å stille krav til EØS-borgere og deres familiemedlemmer utredes nærmere.

Leverandøren vurderer at tildeling av skattekort kan være spesielt egnet for et krav om norsk pass eller nasjonalt ID-kort, og kan være en egnet prosess å begynne med. En annen potensielt egnet prosess kan være førstegangsutstedelse av norsk førerkort, uten at dette er vurdert nærmere i arbeidet med tilleggsoppdraget.

Avvikle EØS-registreringsordningen, betinget at ikke forordning 2019/1157 gir vesentlig utvidet handlingsrom

Et bredt tilbud om nasjonalt ID-kort til utlendinger og anbefalt tilnærming til krav vil etter leverandørens oppfatning gi grunnlag for en høy andel «unike» identiteter i Folkeregisteret. Det har spesielt betydning for å få registrert EØS-borgere som «unike». Ved dagens praksis blir det ikke tatt opp biometri av EØS-borgere i Norge. For tredjelandsborgere tas det opp biometri i søknadsprosessene hos utlendingsmyndighetene som kan generere «unike» identiteter i Folkeregisteret.

EØS-borgere (med unntak av nordiske borgere) som skal oppholde seg i Norge i mer enn tre måneder, plikter å registrere seg hos politiet gjennom EØS-registreringsordningen. Leverandøren har som et alternativ vurdert opptak av biometri gjennom EØS-registreringsordningen. Med dagens regelverk ansees opptak av biometri som urealistisk, og det er heller ikke vurdert å være verdiøkende å styrke kontrollen som gjennomføres i forbindelse med EØS-registreringsordningen. Gitt dagens regelverk og praksis anses bruksverdien for borger og forvaltningen som meget begrenset, da registreringsbeviset i liten til ingen grad kreves i andre prosesser i forvaltningen og statistikkgrunnlaget som ordningen genererer kan opptas på andre måter.

Leverandøren påpeker at en ny EU-forordning (2019/1157) potensielt kan medføre økt handlingsrom for biometriopptak i registreringsordningen. I så tilfelle bør det vurderes om EØS-registreringsordningen i stedet bør styrkes med biometriopptak. Leverandøren anbefaler derav at EØS-registreringsordningen avvikles, betinget at ikke forordning 2019/1157 gir vesentlig utvidet handlingsrom.

«Unik» baseres på pass-, ID-kort og utlendingsregisteret og det må sikres nødvendig fremdrift for juridisk og teknisk tilrettelegging

Spørsmålet om hva som skal være informasjonsgrunnlaget for «unik» er den mest sentrale gjenstående vurderingen for å kunne registrere personer som «unike» i Folkeregisteret. Utlendingsdirektoratet (UDI) og Politidirektoratet (POD) har ulike synspunkt på om søknadsprosessene i utlendingsforvaltningen bør gi grunnlag for «unik» (fra utlendingsregisteret) eller om kun utstedelse av pass og nasjonalt ID-kort kan danne dette grunnlaget (fra henholdsvis pass- og ID-kortregisteret). Leverandøren legger til grunn at det uansett skal kontrolleres for «unik» med en-til-mange søk på tvers av disse tre registrene i søknadsprosessene. Leverandøren anbefaler at det legges til rette for at status «unik» kan etableres på grunnlag av registrering i enten utlendings-, pass- eller ID-kortregisteret. Anbefalingen begrunnes i verdien av å muliggjøre høy utbredelse og bruk av status «unik», fristilt fra utbredelsen av nasjonalt ID-kort. Leverandøren har videre beskrevet hva som gjenstår av juridisk og teknisk tilrettelegging for å realisere «unik». Det anbefales spesielt at nødvendig regelverksarbeid for tilbud om nasjonalt ID-kort til utlendinger og hjemmelsgrunnlag for «unik» gis tilstrekkelig prioritet.

Styrke arbeidet med fysisk ID-kontroll

«Unike» identiteter i Folkeregisteret gir verdi isolert sett. Leverandøren vurderer likevel at verdien vil øke betraktelig i kombinasjon med en biometrisk verifisering av at personen som møter fysisk er den rettmessige eieren av ID-beviset og identitetsnummer. Manuell kontroll av fysiske ID-bevis utgjør en betydelig sikkerhetsrisiko. Leverandøren anbefaler at det etableres én offentlig teknologisk løsning for at tjenesteeiere skal kunne gjennomføre biometrisk kontroll av bruker opp mot vedkommende sitt pass og/eller nasjonale ID-kort (en-til-en søk). Løsningen skal være digital, og tjenesteeiere tar i bruk løsningen etter egen risikovurdering. Anbefalingen henger tett sammen med tilsvarende anbefalt løsning for eID, som beskrives nærmere under.

I kartleggingen har leverandøren fått forelagt lite dokumentasjon av hvordan NAV faktisk utøver ID-kontroll. Leverandøren anbefaler at det gjennomføres en systematisk gjennomgang av ID-arbeidet tilknyttet alle tjenester og ytelser i NAV for brukere i Norge og i utlandet med implementering av tilhørende tiltak.

Anbefalingene tilknyttet tema 1 nyanserer og endrer deler av anbefaling nummer 2 i hovedrapporten. Tilleggsrapporten nyanserer hovedrapportens anbefaling ved at det anbefales at norske pass og nasjonalt ID-kort skal utgjøre de eneste gyldige ID-bevisene i Norge *utstedt av norske myndigheter*, samt at hvordan det skal stilles krav til fysiske ID-bevis er ytterligere detaljert.

Vurderinger og anbefalinger tema 2 – eID

Leverandøren har som del av arbeidet med tema 2 vurdert utfordringer ved dagens tilnærming til eID, vurdert alternative løsninger for å styrke sikkerheten ved private eID-er, samt vurdert ulike roller for nasjonal eID.

En eID benyttes til verifikasjon av påstått identitet i elektronisk kommunikasjon mellom to parter. Dagens eID-løsninger for elektronisk autentisering til offentlige digitale tjenester gjennom ID-porten er i stor grad private. eID-er som benyttes til autentisering til offentlige digitale tjenester i Norge er klassifisert etter ulike sikkerhetsnivåer, der ulike sikkerhetsnivåer gir tilgang til ulike offentlige digitale tjenester. Det kreves personlig oppmøte og ID-kontroll av bruker ved utstedelse av eID-er med høyeste sikkerhetsnivå og samtlige av disse eID-ene utstedes av private tilbydere. ID-kontrollen for utstedelse gjennomføres i dag ved et stort antall lokasjoner, i bankfilialer, postkontor og post i butikk. Hvilke brukere som har tilgang til å anskaffe ulike eID-er og hvilke ID-bevis som godtas i ID-kontrollen varierer på tvers av eID-løsningene. Dagens system og tilnærming til eID anses som brukervennlig og relativt lite ressurskrevende, men har enkelte sikkerhetsutfordringer.

Leverandøren vurderer at de viktigste utfordringene ved dagens situasjon er:

1. Misbruk av eID der brukeren ikke er den rettmessige eieren grunnet svakheter i bruks- og/eller utstedelsesfasen

2. Enkelte brukergrupper har utfordringer med å få utstedt eID på høyeste sikkerhetsnivå

3. Én privat aktørs dominerende markedsposisjon skaper digital sårbarhet for det offentlige og utfordringer med fri konkurranse

Leverandøren vurderer at den første utfordringen har størst konsekvenser, selv om konsekvenser av feil og misbruk av eID er svakt dokumentert. Utfordringen skyldes to sikkerhetshull for eID. For det første gjennomføres det ingen kontroll av at bruker av

en privat eID er den rettmessige eieren av eID-en ved bruk eller fornyelse. For det andre er det betydelige svakheter ved ID-kontrollen som gjennomføres ved bankfilial eller postkontor/post i butikk ved utstedelse av private eID-er. De ansatte som gjennomfører ID-kontrollen har begrenset ID-kompetanse, det gjennomføres ingen biometrisk kontroll av bruker ved oppmøte og det stilles ulike krav til fysiske ID-bevis for utstedelse av forskjellige eID-er på samme sikkerhetsnivå. Det er en grunnleggende svakhet for eID, og for ID-forvaltningen som helhet, at det i dag ikke finnes «unike» identitetsnummer i Folkeregisteret. Én person kan ha flere identiteter, og dermed mulighet til å ha eID-er i flere ulike identiteter.

Nasjonal eID anbefales avviklet, da en supplementtilnærming gir begrenset til ingen merverdi og innføring av krav om nasjonal eID anses som risikabelt

Etter nåværende plan er det lagt opp til at det skal lanseres en nasjonal eID tilknyttet nasjonalt ID-kort mot slutten av 2021. Etter gjeldende politikk skal nasjonal eID utstedes som et supplement til eksisterende eID-løsninger i markedet.

Leverandøren har vurdert alternative roller for nasjonal eID. I tillegg til nåværende plan om å innføre nasjonal eID som et supplement til løsninger i markedet, er det vurdert innføring av krav til bruk av nasjonal eID for tilgang til enten utvalgte eller alle offentlige tjenester. Det er også vurdert å utstede nasjonalt ID-kort uten nasjonal eID.

Avklaring av rollen til nasjonal eID er krevende, som følge av mange potensielle innfallsvinkler og mye historie. Nasjonal eID har vært planlagt over lengre tid og politiet har vist manglende gjennomføringskraft i arbeidet med utrullingen av nasjonalt ID-kort med eID. Omtrent 65 prosent av investeringskostnader for nasjonal eID er påløpt eller forpliktet.

Sikkerhet og brukervennlighet vil ikke påvirkes nevneverdig så lenge nasjonal eID er et supplement til private eID-er. Dette skyldes at brukere alltid vil kunne velge de private eID-ene og velge en mindre sikker eller en mer brukervennlig løsning. Supplementtilnærmingen vil redusere digital sårbarhet marginalt og vil til en viss grad utfordre dominerende aktørs markedsposisjon. Samlet nytte fremstår likevel som meget begrenset og veier dermed ikke opp for ressursbruken supplementtilnærmingen medfører. Alternativ med krav til nasjonal eID for tilgang til offentlige tjenester vil gi mindre sikkerhetsmessige gevinster, men medfører betydelig risiko for redusert brukervennlighet og økt ressursbruk. Det anbefales derfor at nasjonal eID avvikles og at nasjonalt ID-kort utstedes uten nasjonal eID.

Styrke sikkerheten ved utstedelse av private eID-er

For å styrke sikkerheten tilknyttet utstedelse av private eID-er anbefales følgende tiltak:

- Sette krav til norsk pass eller nasjonalt ID-kort, og status «unik» i Folkeregisteret, for utstedelse av private eID-er
- Muliggjøre at ID-kontrollen som gjennomføres ved pass- og ID-kontor kan benyttes som grunnlag for utstedelse av private eID-er
- Tilrettelegge for at biometrisjekk ved hjelp av teknologiske løsninger for kontroll av bruker og fremvist ID-bevis ved utstedelse av private eID-er, med og uten fysisk oppmøte, kan gjennomføres

De tre tiltakene vil sikre at brukere kun får utstedt private eID-er i én «unik» identitet. Kun brukere med «unike» identitetsnummer, med et ID-bevis med elektronisk brikke og biometrisk informasjon som kan bevise at personen er rettmessig eier av

identitetsnummeret, gis mulighet til utstedelse av private eID-er i Norge. Videre vil de tre tiltakene, gjennom å benytte den sterke ID-kontrollen ved pass- og ID-kontor og bruk av teknologiske løsninger for biometrisjekk av bruker, begrense feilutstedelse av eID-er. De tre tiltakene vil muliggjøre at oppmøte for ID-kontroll og utstedelse av privat eID som i dag gjennomføres ved en bankfilial eller postkontor/post i butikk kan falle bort.

Implementere teknologisk løsning for biometrisk kontroll av bruker og ID-bevis tilknyttet bruk av eID-er

For å styrke sikkerheten ved bruk av eID-er anbefaler leverandøren at det offentlige har én teknologisk løsning for å kunne gjennomføre biometrisk kontroll av bruker opp mot vedkommende sitt pass eller nasjonale ID-kort ved bruk av eID-er (en-til-en søk). Løsningen skal kunne benyttes uavhengig av om bruker autentiserer seg med en norsk privat eID eller en utenlandsk eID gjennom ID-porten. Løsningen må derav være frikoblet fra de ulike eID-løsningene og må sees i tett sammenheng med anbefalingen om at tjenesteeiere skal utøve bedre ID-kontroll av fysiske ID-bevis. Det anbefales videre at det offentlige har eierskap til en slik løsning. Gitt dagens styringsstruktur i ID-forvaltningen, anbefales det at Difi anskaffer en løsning i markedet i tett samarbeid med politiet.

Anbefalingene for tema 2 om eID erstatter i sin helhet hovedrapportens anbefaling tilknyttet temaet om å styrke arbeidet med eID.

Vurderinger og anbefalinger tema 3 – Styring og struktur – et felles skrankepunkt

Myndighetsansvaret for ID-forvaltningen er delt mellom flere departementer med underliggende etater og virksomheter, hvor 11 departementer med 18 tilhørende virksomheter har en rolle. Brukere som har eller ønsker å opprette en tilknytning til Norge vil i flere situasjoner møte krav om ID-relaterte oppmøter hos ulike offentlige etater. For enkelte brukergrupper innebærer dette gjennomføring av flere oppmøter hos ulike aktører innenfor en kort tidsperiode. En EØS-borger som ønsker skattekort og nasjonalt ID-kort vil eksempelvis måtte møte til kontroll både hos politiet og på et skattekontor. Aktørene som krever ID-relaterte oppmøter deler i liten grad informasjon og informasjonen som brukerne må oppgi er i flere tilfeller overlappende.

Leverandøren har som en del av arbeidet med tema 3 vurdert samkjøring av oppmøter for registrering, fastsettelse av identitet og utstedelse av pass og nasjonalt ID-kort i et felles skrankepunkt. Prosesser med ID-relaterte oppmøter i politiet, Skatteetaten og UDI er vurdert med utgangspunkt i at et felles skrankepunkt legges til politiet og de 78 planlagte pass- og ID-kontorene. Politiets førstelinje har allerede identitetsregistrering og ID-kontroll som en kjerneoppgave, og innehar nødvendig kompetanse og infrastruktur i form av oppmøtesteder og teknisk utstyr.

Dagens skrankepunkter omfatter politiets 78 pass- og ID-kontor og 36 utlendingskontor, Skatteetatens 42 skattekontor, samt fem SUA-kontor (servicesentre for utenlandske arbeidstakere). Vurderingen inkluderer kun prosesser for ID-relaterte oppmøter som gjennomføres i Norge. Dette medfører at aktiviteter som finner sted i utlandet, på utenriksstasjonene, er holdt utenfor.

De viktigste utfordringene ved dagens skrankepunkter er:

- Unødvendig mange oppmøter, spesielt for EØS-borgere, hvor samme aktiviteter eller informasjon registreres flere ganger

- ID-relaterte skrankepunkt hos de ulike aktørene har forskjellig praksis, rutiner og retningslinjer for håndtering av ID-relaterte oppgaver

- Sammenfallende aktiviteter i ID-prosesser, dobbeltarbeid på tvers av etater og liten grad av datadeling

- Parallelle kompetansemiljøer og infrastruktur

Med bakgrunn i identifiserte utfordringer har leverandøren vurdert potensialet for å redusere ressursbruk, øke brukervennligheten og sikkerheten gjennom å samkjøre ID-relaterte oppgaver i et felles skrankepunkt.

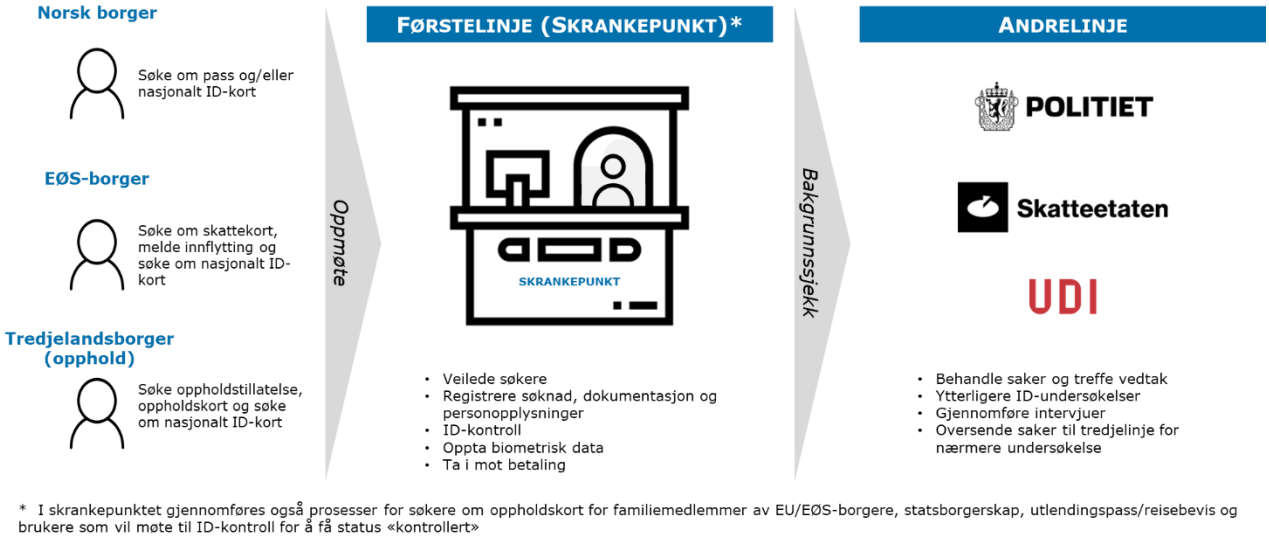
Leverandøren anbefaler å etablere et felles skrankepunkt for politiet, Skatteetaten og UDI sine ID-relaterte kjerneoppgaver knyttet til identitetsregistrering og ID-kontroll i Norge. For politiet gjelder dette prosessen tilknyttet å søke om pass og/eller nasjonalt ID-kort. For Skatteetaten gjelder det prosessene tilknyttet å søke om skattekort for de som ikke har fødselsnummer eller «kontrollert» d-nummer, melde innflytting til Norge fra utlandet samt ID-kontroll gjennomført på vegne av andre rekvirenter. For UDI gjelder det prosessene tilknyttet søknad om oppholdstillatelse, oppholdskort for familiemedlemmer av EU/EØS-borgere, statsborgerskap og utlendingspass og reisebevis.

Skrankepunktet legges til politiet og de 78 planlagte pass- og ID-kontorene. POD, underlagt JD, har ansvaret for administrativ og faglig ledelse, styring, oppfølging og utvikling av politidistriktene, herunder de felles skrankepunktene. Alle ledere og medarbeidere ved skrankepunktene vil være ansatt i politiet, og vil kunne motta alle typer saker. Det vil følgelig være et felles køsystem.

Som et felles oppmøtested for ID-relaterte oppgaver for alle brukergrupper på tvers av forvaltningen, vil skrankepunktet være et viktig virkemiddel i arbeidet for å oppnå «*én person, én identitet i Norge*». Det muliggjør dessuten en betydelig reduksjon i antall oppmøter for EØS-borgere og tredjelandsborgere da anbefalingen åpner for å utføre flere aktiviteter i ett oppmøte.

Formålet med et felles skrankepunkt er å sikre at ID-relaterte kjerneoppgaver knyttet til registrering og ID-kontroll utføres enhetlig, sikkert, effektivt og brukervennlig for definerte ID-prosesser på tvers av forvaltningen. Et felles skrankepunkt sikrer at både norske og utenlandske borgere kun trenger å oppgi informasjon én gang, får tilstrekkelig veiledning og oppnår rask søknadsbehandling, samtidig som antall fysiske oppmøter begrenses til et minimum. Skrankepunktets rutiner, retningslinjer og ansatte vil sikre enhetlig registrering av grunndata i relevante registre og utøve ID-kontroll både av norske og utenlandske borgere med betydelig spisskompetanse.

Figuren nedenfor illustrerer praksis for et felles skrankepunkt, hvilke prosesser som inkluderes per brukergruppe, samt ansvars- og oppgavefordeling mellom førstelinje (skrankepunkt) og andrelinje.



Figur 1 Illustrasjon av et felles skrankepunkt

Anbefalingen innebærer at det etableres todelt saksbehandling hvor førstelinjen veileder, mottar søknader, registrerer dokumentasjon og personopplysninger for alle typer saker. Videre gjennomfører førstelinjen ID-kontroll, opptar biometrisk data og tar imot betaling der dette er påkrevd. Det gjøres ingen form for ytterligere saksbehandling i førstelinjen. Det er kun andrelinjen som har vedtaksmyndighet i alle saker. Andrelinjen og vedtaksmyndigheten vil som i dag ligge i respektive eksisterende etater.

Et felles skrankepunkt krever tekniske tilpasninger og systemstøtte for at data skal kunne overføres mellom registre og saksbehandlingssystemer på en enkel og sikker måte. For å sikre dette må nødvendige regelverksendringer gjennomføres og personvernhensyn vurderes og ivaretas.

Leverandøren anbefaler en trinnvis implementering av et felles skrankepunkt for politiets, Skatteetatens og UDIs førstelinje. Et felles skrankepunktet opprettes først for prosessen ved pass- og ID-kontor og prosessene i skattekontorene. Dette piloteres på utvalgte lokasjoner. På et senere tidspunkt innfases prosessene ved utlendingskontorene i samme skrankepunkt.

Anbefalingen medfører at politiet ved politidistriktene gis myndighet til å rekvirere identitetsnummer, både d-nummer og fødselsnummer. Grunnlaget for rekvireringen vil fra politiets side være å utøve myndighetsoppgaver på vegne av andre aktører i skrankepunktene, og på sikt for å utstede nasjonale ID-kort til personer som får dette tilbudet. Skatteetaten er fortsatt tildelingsmyndighet av identitetsnummer.

Anbefalingen om felles skrankepunkt endrer ikke leverandørens anbefaling fra hovedrapporten om å utrede etablering av en ID-etat. Et felles skrankepunkt er et steg i riktig retning for å sikre helhetlig styring og ansvar for ID-forvaltningen i Norge. Anbefalingen om et felles skrankepunkt kan likevel implementeres uavhengig av om en ID-etat velges utredet. Et felles skrankepunkt er et av flere virkemiddel for å oppnå visjonen for ID-forvaltningen, men etter leverandørens syn vil det være nødvendig å ta i bruk sterkere grep langs styring- og strukturdimensjonen over tid.

Gevinster og utvalgte implementeringskostnader

Samlet sett vil anbefalingene bidra til økt sikkerhet og økt brukervennlighet, samt legge grunnlag for økt ressurseffektivitet i ID-forvaltningen.

Anbefalingene om *fysiske ID-bevis og utbredelse av nasjonalt ID-kort* har en stor positiv konsekvens for sikkerheten ved at anbefalingene gir grunnlag for høy utbredelse

av nasjonalt ID-kort, samt gir grunnlag for høy utbredelse av «unik» i Folkeregistret. Brukervennligheten styrkes med et bredt tilbud av nasjonalt ID-kort, spesielt for brukere som ikke har hatt tilgang på ID-bevis.

Leverandørens anbefalinger for *eID* har en stor positiv konsekvens for sikkerheten som følge av at brukere kun får utstedt private eID-er i én «unik» identitet og feilutstedelser begrenses. I tillegg vil misbruk der brukeren av en eID ikke er rettmessig eier reduseres. Økt kontroll kan for bruker ha en liten negativ konsekvens for brukervennligheten. Anbefalingen om å avvikle nasjonal eID vil ha en middels positiv konsekvens på ressursbruk, og ubetydelig/ingen konsekvens for sikkerhet og brukervennlighet. Fra et brukervennlighetsperspektiv vil anbefalingen om tilrettelegging for biometrisjekk uten oppmøte ved utstedelse av private eID-er ha stor positiv konsekvens.

Anbefalingen om *et felles skrankepunkt* har en stor positiv konsekvens for sikkerheten i ID-forvaltningen da viktige ID-relaterte kjerneoppgaver blir samlet i robuste fagmiljøer og oppgavene blir gjennomført enhetlig ved todelt saksbehandling. Anbefalingen anses å ha stor positiv konsekvens for brukervennligheten som følge av færre oppmøter for EØS-borgere og tredjelandsborger med flere mulige oppmøtelokasjoner. For øvrig muliggjør og styrker anbefalingen om et felles skrankepunkt øvrige anbefalinger i tilleggs- og hovedrapporten.

Slik beskrevet i hovedrapporten er den reelle og enhetlige dokumentasjonen av dagens sikkerhet, brukervennlighet og ressurseffektivitet i ID-forvaltningen begrenset, og samlet nytte av anbefalingene er derav krevende å estimere. Et overordnet estimat på årlige konsekvenser som følge av leverandørens anbefalinger tilknyttet etablering av felles skrankepunkt og avviklingen av EØS-registreringsordningen gir ca. 135 mill. kroner i positiv nytte for bruker og ca. 17 mill. kroner for forvaltningen per år. Ytterligere gevinster som følge av en potensiell reduksjon i eksisterende kontorstruktur, samt effektivisering av andrelinje som følge av standardisering og digitalisering er identifisert, men ikke kvantifisert.

Implementeringskostnader er overordnet identifisert, men ikke kvantifisert. Kostnader som vil påløpe i implementeringsfasen er knyttet til omstilling, ombygging/utvidelse av lokaler, IKT-utstyr og systemstøtte, kompetanseutvikling med mer.

Leverandørens vurdering er at samlet nytte vil overstige kostnader til implementering.

1 Introduksjon

Områdegjennomganger skal legge til rette for systematisk arbeid med effektivisering og forbedring innenfor utvalgte områder, og skal kunne brukes som beslutningsunderlag for strukturelle endringer i offentlig sektor. Formålet med denne områdegjennomgangen er å kartlegge om dagens ID-forvaltning er innrettet og organisert på en hensiktsmessig og kostnadseffektiv måte, og på bakgrunn av dette vurdere og foreslå alternative tiltak som vil gi økt sikkerhet, redusert ressursbruk og økt brukervennlighet.

Arbeidet med områdegjennomgangen for ID-forvaltningen ble igangsatt i april med leveranse av en hovedrapport 6. september. Med utgangspunkt i hovedrapporten ble leverandøren tildelt et tilleggsoppdrag med vektlegging av tre tema *fysiske ID-bevis og utbredelse av nasjonalt ID-kort*, *eID* og *styring og struktur*. For øvrig overordnet beskrivelse av oppdraget henvises det til hovedrapporten.

Tilleggsoppdraget har vært gjennomført med en prosjektgruppe med representanter fra Finansdepartementet (FIN), Justis- og beredskapsdepartementet (JD), Samferdselsdepartementet (SD), Kommunal- og moderniseringsdepartementet (KMD), samt Arbeids- og sosialdepartementet (ASD). ASD var deltakende i prosjektgruppen en stund etter at arbeidet med tilleggsoppdraget startet. Det er avholdt fem møter med prosjektgruppen, hvorav to møter er gjennomført som arbeidssamlinger hvor representanter fra underliggende virksomheter også har deltatt. I disse samlingene deltok Skattedirektoratet (SKD), Politidirektoratet (POD), Utlendingsdirektoratet (UDI), Direktoratet for forvaltning og ikt (Difi) og Arbeids- og velferdsdirektoratet (NAV). Prosjektstyret fra arbeidet med hovedrapporten er videreført og leverandøren har deltatt i to møter.

Leverandøren er Capgemini Invent med støtte fra advokatfirmaet BAHR AS. Medlemmene i prosjektet har deltatt i diskusjoner om vurderinger og anbefalinger, men rapporten inneholder leverandørens egne vurderinger og anbefalinger.

1.1 Mandat for tilleggsoppdraget

Følgende tema og vurderingsområder har blitt lagt til grunn fra oppdragsgiver i tilleggsoppdraget:

Tema 1 – Fysiske ID-bevis og utbredelse av nasjonalt ID-kort

- *Vurdere hvilke brukere som skal få tilbud om nasjonalt ID-kort, hvilke brukere det skal stilles krav til fremvisning for og hvilke tjenesteeiere/tjenester/ytelser et ev. krav skal gjelde for. Behovet for bedre ID-kontroll hos disse tjenesteeierne belyses nærmere*

- *Vurdere alternativ relatert til EØS-/tredjelandsborgere, herunder hvilken tilknytning til Norge som bør utløse krav om nasjonalt ID-kort. Det skal også vurderes mulighet for å bruke registrering av biometri ved utstedelse av oppholdskort for tredjelandsborgere og registreringsbevis til EØS-borgere som grunnlag for ev. registrering som «unik» i Folkeregisteret*

- *Vurdere hvilke brukergrupper og eller brukersituasjoner som vil kreve særlige løsninger (unntak) og skissere et opplegg for dette (f.eks. brukere med utfordringer med å godtgjøre identitet, borgere med tilknytning til Norge med opphold i utlandet)*

- *Beskrive hva som gjenstår av teknisk, juridisk og regulatorisk tilrettelegging for å få registrert personer som får nye pass og nasjonale ID-kort som «unike» i Folkeregisteret og gi anbefalinger om videre prosess for dette*

Tema 2 – eID

- *Vurdere forholdet mellom eID og anbefalingen om at norsk pass og nasjonalt ID-kort skal være eneste gyldige fysiske ID for tilgang til offentlige tjenester og ytelser, herunder hvordan det kan etableres en biometriknytning for eID-løsninger som gir tilgang til offentlige tjenester og ytelser*

- *Vurdere alternativ for å styrke sikkerheten ved private eID-er, herunder ID-kontroll ved utstedelse og regelmessig kontroll ved bruk av eID-er etter førstegangsutstedelse. Som ledd i dette vurdere om ID-kontrollen ved pass- og ID-kontor kan benyttes som grunnlag for utstedelse av private eID-er*

- *Vurdere utenlandske eID-løsninger for tilgang til offentlige tjenester og ytelser innenfor rammen av EØS-regelverk implementert i Norge (eIDAS-loven)*

- *Vurdere ulike eID-løsninger og rollen til en nasjonal eID opp mot private eID-løsninger. Gjeldende politikk innebærer at nasjonal eID skal være et supplement til private eIDer i markedet. Videre bør beslutningen om å utsette nasjonal eID fra ID-kort også tas høyde for i vurderingene*

- *Vurdere konsekvensene av eventuelle endringer i vederlagsmodellen for nasjonal eID*

Tema 3 – Styring og struktur

- *Utrede og vurdere samkjøring av oppmøter for registrering, fastsettelse av identitet og utstedelse av pass og nasjonalt ID-kort hos et felles skrankepunkt, trolig hos politiet. Dette gjelder særlig ID-oppgavene i POD, SKD og UDI. Konsekvensene for sikkerhet, brukervennlighet og kostnadseffektivitet av felles skrankepunkt for hhv. norske borgere, EØS-borgere og tredjelandsborgere skal redegjøres for. Vurderingen skal kunne legge grunnlag for å kunne følge opp punkt 27 i regjeringens strategi mot arbeidslivskriminalitet. Leverandøren bes synliggjøre ev. andre organisatoriske endringer som naturlig kan følge av samling i et slikt skrankepunkt*

- *Utrede og vurdere hvilke implikasjoner dette bør ha for rekvirering av identitetsnummer fra Folkeregisteret og hvilken ID-kontroll som gjennomføres i den sammenheng. Det skal også vurderes hvilke grupper av EØS-borgere som det bør kreves «kontrollert» identitet av før de får tilgang til offentlige tjenester og ytelser, ev. om det er grupper som bør få unntak fra et slikt krav*

Med utgangspunkt i de tre temaene ble det også spesifisert i mandatet at:

- *Mål om økt sikkerhet, brukervennlighet og kostnadseffektivitet skal fortsatt legges til grunn for vurderingene*

- *Vurdere om anbefalingene i hovedrapporten bør justeres eller presiseres, i lys av arbeidet med tilleggsrapporten*

- *Oppdatere og konkretisere gevinst- og gjennomføringsplan, i lys av arbeidet med tilleggsrapporten*

1.2 Struktur på leveranse, fremgangsmåte og datagrunnlag

Leverandøren har strukturert dokumentasjonen i tre hoveddeler etter oppdelingen av tema for tilleggsoppdraget. Hver del inneholder relevant nåsituasjonsbeskrivelse, relevante nåsituasjonsvurderinger og vurderinger av alternativ per tema. For hver enkelt del refereres det til hovedrapporten der hensiktsmessig, og tilleggsrapporten bygger videre på de funn og vurderinger som ble beskrevet i hovedrapporten.

Per tema er det gjennomført utvalgte kvalitative og kvantitative analyser, hvor det er blitt benyttet et bredt spekter av datakilder. Det omfattende materialet av tidligere rapporter og andre dokumenter, slik tilgjengeliggjort for hovedrapporten, er blitt noe komplettert med ytterligere rapporter og underlag. Enkelte deler av dokumentasjonen som er mottatt og benyttet er unntatt offentlighet, og er derav ikke kildehenvist. Det er videre gjennomført en rekke møter med relevante underliggende etater og virksomheter og private aktører, rettede informasjonsforespørsler, samt utvalgte befaringer.

Som i hovedrapporten er alternativene innenfor hvert tema vurdert opp mot vurderingskriteriene som gjennomgående er benyttet i områdegjennomgangen, sikkerhet, ressursbruk og brukervennlighet. Vurderingene er gjort i et femårsperspektiv. For ytterligere detaljer om fremgangsmåte og datagrunnlag, refereres det til hovedrapporten. Vurdering av de ulike alternativene gjøres etter «pluss-minusmetoden», slik beskrevet i kapittel 1.3 i hovedrapporten.[1]

I beskrivelse og vurderingene av de tre temaene er anbefalingene fra hovedrapporten lagt til grunn om noe annet ikke er spesifisert. Vurderinger og valg innenfor hvert av de tre temaene for tilleggsoppdraget kan ha gjensidig påvirkning på hverandre. I kapittel 2-4 behandles hvert enkelt av de tre temaene i all hovedsak isolert og det spesifiseres hvor det eventuelt er avhengigheter til de andre temaene. Kapittel 2-4 inneholder også oppsummerende vurderinger av ulike alternativ, men ikke anbefalinger. Anbefalingene, gjengitt i kapittel 5, er gitt samlet for de tre temaene.

[1] Direktoratet for økonomistyring, «Veileder i samfunnsøkonomiske analyser», 2018

2 Fysiske ID-bevis og utbredelse av nasjonalt ID-kort

I dette kapittelet vurderer leverandøren ulike muligheter knyttet til fysiske ID-bevis og utbredelse av nasjonalt ID-kort. I tilleggsrapporten benytter leverandøren begrepet «nasjonalt ID-kort» til å omtale nasjonalt ID-kort utstedt av norske myndigheter, med mindre annet er spesifisert eksplisitt. Kapittelet er utarbeidet i henhold til tema 1 i mandat for tilleggsoppdraget, nærmere beskrevet i kapittel 1.1.

Kapittelet fokuserer særskilt på hvilke brukergrupper som bør få tilbud om nasjonalt ID-kort og i hvilken grad det skal stilles krav om fremvisning av dette hovedsakelig tilknyttet fysiske oppmøter. Vurderingen av hvem som får tilbud ses opp mot mulighetsrommet i å benytte registrering av biometri i forbindelse med utstedelse av oppholdskort for tredjelandsborgere og styrking av EØS-registreringsprosessen. Kapittelet tar også for seg hvilken teknisk og juridisk tilrettelegging som gjenstår for å oppnå status «unik» i Folkeregisteret. Alternativ og forslag til løsninger vil vurderes opp mot kriteriene sikkerhet, brukervennlighet og ressursbruk.

Av relevant bakgrunn i hovedrapporten vises det spesielt til kapittel 2.2 om «Folkeregisteret og identitetsnummer», kapittel 2.3 om «ID-bevis og grunnidentitet», kapittel 2.6 om «Brukergrupper og brukerreiser», kapittel 2.8 om «Sakstyper og volum». Kapittel 6.1.1-6.1.3 er relevant for kvalitet og sikkerhet i tildeling og utstedelse av identitetsnummer og fysiske ID-bevis, og kapittel 6.1.6 er relevant for tematikken knyttet til «unik» i Folkeregisteret. Fra hovedrapportens del 3 er kapittel 10, 12 og 13 med vurdering av alternativ relevante. Kapittel 2.1 er komplettert med ytterligere relevant bakgrunn for tilleggsoppdraget.

2.1 Bakgrunn

2.1.1 Brukergrupper

Leverandøren viderefører den overordnede kategoriseringen av ID-forvaltningens brukere i norske statsborgere, EØS-borgere og tredjelandsborgere. Kategoriseringen er vesentlig, delvis på grunnlag av at brukergruppene er underlagt ulike rettslige rammeverk, og delvis fordi brukergruppene har ulik tilgang på ID-bevis og er underlagt ulike legitimasjonskrav som følge av deres statsborgerskap. Definisjonen av brukergruppene er nærmere beskrevet i hovedrapportens kapittel 2.6.

Norske borgere

Av den totale befolkningen i Norge per 1. januar 2019, hadde 4 743 979 norsk statsborgerskap.[2] 55 941 personer ble født i Norge i 2018. Samtidig fikk 10 269 utenlandske statsborgere norsk statsborgerskap i 2018.

EØS-borgere

Av den totale befolkningen i Norge per 1. januar 2019 var det 358 568 personer registrert med statsborgerskap i et EU/EØS[3]-land.[4] Ifølge tall fra UDI ble det gjennomført 34 033 EØS-registreringer i 2018. Tallet omhandler registreringer av EØS-borgere som skal oppholde seg i Norge i mer enn tre måneder.[5] Av gjennomførte EØS-registreringer var de to største gruppene fra Polen (26 prosent) og Litauen (13

[2] SSB.no, «Tabell 05196: Befolkning, etter statsborgerskap», 2019
[3] UDI.no, «EU/EØS-borger», u.å.
[4] SSB.no, «Tabell 05196: Befolkning, etter statsborgerskap», 2019
[5] Nordiske borgere er unntatt registreringsplikten

prosent).[6] Prosessen for gjennomføring av EØS-registrering er nærmere beskrevet i tilleggsrapportens kapittel 4.2.3.

Nordiske borgere utgjør en betydelig andel av EØS-borgere som oppholder seg i Norge, men er unntatt kravet om registrering. Antallet EØS-registreringer som gjennomføres i løpet av et år, samt antallet som innehar et EØS-registreringsbevis vil dermed ikke kunne fastslå nøyaktig hvor mange EØS-borgere som faktisk ankommer og oppholder seg i landet. EØS-registreringsbeviset viser kun at en EØS-borger har vært i Norge og oppfylt kravet til oppholdsrett på det tidspunktet EØS-registreringsbeviset ble søkt om.

Tredjelandsborgere

Av Norges totale befolkning per 1. januar 2019 var det 222 856 personer registrert med statsborgerskap i land utenfor EU/EØS[7]-landene, 2 638 statsløse personer og 171 personer med uoppgitt statsborgerskap.[8] Tredjelandsborgere som skal oppholde seg i Norge i mer enn tre måneder, eller som skal arbeide her, må søke om, og få innvilget oppholdstillatelse. Det ble i 2018 innvilget beskyttelse (asyl) til 3 570 personer. Videre ble det gitt 25 679 oppholdstillatelser i forbindelse med arbeid, utdanning og familieinnvandring.[9]

2.1.2 Gyldige ID-bevis i dag

Leverandøren har i hovedrapporten beskrevet at det finnes en rekke ID-bevis i omløp i Norge i dag, hvor mange i praksis benyttes og aksepteres til legitimasjonsformål. Som beskrevet i hovedrapporten kapittel 4 og kapittel 5 foreligger det ikke en enhetlig definisjon på tvers av lovverk rundt hva som regnes som gyldig legitimasjon i Norge. Leverandøren viser videre til hovedrapportens kapittel 2.9 for nåværende status og planlagt utrulling av nasjonalt ID-kort.

2.1.3 Særlig om oppholdskort, asylsøkerbevis og EØS-registreringsbevis som identitetsdokumenter

Dokumentene oppholdskort, asylsøkerbevis og EØS-registreringsbevis er ikke ID-bevis (jf. definisjon i hovedrapportens definisjonsliste) og har derfor i mindre grad vært gjenstand for vurdering i hovedrapporten. Dette har også vært vektlagt av UDI og politiet i tilbakemeldinger og diskusjoner med leverandøren. Likevel vil oppholdskortet, med enkelte tilpasninger i innhold, potensielt kunne inneha en rolle som ID-bevis, og vil dermed også kunne oppfylle flere av målene som er tiltenkt ved utrulling av nasjonalt ID-kort. Kortene og bevisene slik de utstedes i dag beskrives under.

Oppholdskort

Oppholdskort utstedes av politiet til tredjelandsborgere som får innvilget oppholdstillatelse i Norge. Norge er etter Schengen-avtalen pålagt å utstede oppholdskort til tredjelandsborgere med oppholdstillatelse i Norge, samt at oppholdskortet følger et felles format for alle schengen-land (schengen-standardisert).[10] Alle tredjelandsborgere som har oppholdstillatelse i Norge skal ha et oppholdskort. Oppholdskortet er gyldig like lenge som oppholdstillatelsen til eieren av

[6] Udi.no, «EØS-registreringer etter statsborgerskap og måned», 2018
[7] UDI.no, «EU/EØS-borger», u.å.
[8] SSB.no, «Tabell 05196: Befolkning, etter statsborgerskap», 2019
[9] UDI.no, «Statistikk om innvandring – Innvilgede førstegangstillatelser etter statsborgerskap og type (2018)», 2019
[10] Rådsforordning (EF) nr. 1030/2002 av 13. juni 2002 om felles format for oppholdstillatelse til tredjelandsborgere

kortet. Ved permanent oppholdstillatelse[11] er oppholdskortet gyldig i to år[12]. Kortet inneholder eierens navn, ansiktsfoto, signatur og gyldighetstid, men inneholder ikke innehavers norske identitetsnummer. Eierens fingeravtrykk er også lagret i kortet. Oppholdskortet dokumenterer at vedkommende har oppholdstillatelse i et Schengen-land, og dermed har rett til å reise fritt i Schengen-området i inntil 90 dager i løpt av en periode på 18+ dager, men er ikke i seg selv et reisebevis og eieren må derfor i tillegg ha med seg sitt pass ved reise.[13]

Det utstedes også oppholdskort for tredjelandsborgere med oppholdsrett som familiemedlem til EØS-borgere[14]. Familiemedlemmer til en EØS-borger plikter å anskaffe seg oppholdskort dersom de skal oppholde seg i Norge i mer enn tre måneder. Varigheten settes i utgangspunktet til fem år og kan forlenges til ti år, avhengig av oppholdsretten til EØS-borgeren som utøver EØS-rettigheter i Norge.

Prosessen for utstedelse av oppholdskortet beskrives nærmere i kapittel 4.2.4.

Asylsøkerbevis

Asylsøkerbevis utstedes av politiet til personer som har søkt om beskyttelse i Norge. Fra desember 2017 inneholder kortet blant annet informasjon om innehaverens navn, ansiktsfoto, statsborgerskap, fødselsdato, gyldighetstid, DUF-nummer og d-nummer. Informasjonen på kortet er basert på innehaverens oppgitte opplysninger, og det kan følgelig ikke benyttes som et gyldig ID-bevis eller reisebevis.[15] Dette står også direkte på asylsøkerbeviset.[16] Asylsøkerbeviset skrives ut på egen printer hos Politiets Utlendingsenhet, og det benyttes følgelig ikke en ekstern kortleverandør. Asylsøkerbeviset inneholder ikke elektronisk brikke, og hverken fingeravtrykk eller ansiktsfoto er lagret digitalt i asylsøkerbeviset.

EØS-registreringsbevis

EØS-registreringsbeviset utstedes av politiet til EØS-borgere ved gjennomført EØS-registrering. Det er et krav at alle EØS-borgere (med unntak av nordiske borgere) registrerer seg og får utstedt et bevis når de skal oppholde seg i Norge i mer enn tre måneder. Formålet med EØS-registrering er at utlendingsmyndighetene skal ha en viss oversikt over antallet EØS-borgere som oppholder seg i Norge. EØS-registreringsbeviset er ikke et bevis på at eieren har oppholdsrett i Norge, kun at vedkommende oppfylte kravet til oppholdsrett på registreringstidspunktet. Beviset inneholder eierens navn, adresse og dato for registrering, og har ingen utløpsdato. Registreringsbeviset utstedes kun som et alminnelig papirdokument, og inneholder ingen øvrige sikkerhetselementer. EØS-borgere som ikke registrerer seg innen tre måneder etter ankomst til Norge, kan bøtelegges.[17] Prosessen for utstedelse av EØS-registreringsbevis beskrives nærmere i kapittel 4.2.3.

2.1.4 Behovet for sterke ID-bevis til alle

[11] Nyinorge.no, «*Når du har bodd sammenhengende i Norge i tre år, kan du få en permanent oppholdstillatelse. Permanent oppholdstillatelse gir deg rett til å oppholde deg og arbeide i Norge på ubestemt tid*»
[12] Fra RS 2012-011 pkt. 2.6: «*For tredjelandsborgere med permanent oppholdstillatelse settes varigheten til to år. Dette er fordi UDI kan fatte vedtak om bortfall av en permanent oppholdstillatelse dersom en utlending har oppholdt seg utenfor Norge i mer enn to år, jf. utlendingsforskriften § 11-8 første ledd*»
[13] UDI.no, «Oppholdskort», u.å.
[14] Varig oppholdsrett, jf. oppholdsdirektivets (2004/38) artikkel 20
[15] UDI.no, «Asylsøkerbevis», u.å.
[16] UDI.no, «Asylsøkerbevis», u.å.
[17] UDI.no, «Registreringsbevis for EU/EØS-borgere», u.å.

I hovedrapporten presenterte leverandøren visjon, hovedmål og delmål for ID-forvaltningen (jf. hovedrapporten kapittel 16). Målene er nært knyttet opp mot KoIDs[18] ambisjon om «en person, en identitet i Norge», samt ambisjonen om at «enhver som har fått tildelt et norsk identitetsnummer, i form av et d-nummer eller et fødselsnummer, skal gis mulighet til å dokumentere på en troverdig måte, at han er rette eier av identitetsnummeret fysisk og digitalt, for å ivareta grunnleggende behov». Ambisjonene er også nærmere omtalt i hovedrapporten under kapittel 2.9.5.

Realisering av ambisjonene forutsetter i stor grad at personer som får tildelt et identitetsnummer i Norge i praksis får muligheten til å bevise sin identitet med et sikkert fysisk eller digitalt ID-bevis, samt at ulike instanser har mulighet til å kontrollere for dette der nødvendig.

2.1.5 Nasjonalt ID-kort som et virkemiddel for «unik» og bevis av knytning mellom person og norsk identitetsnummer

Det ble i 2016 lagt frem en utredning om knytning mellom Folkeregisteret og biometriregistrene (passregisteret, nasjonalt ID-kortregister og utlendingsregisteret) i justissektoren. Arbeidsgruppen foreslo i utredningen en knytning mellom registrene for å sikre at én identitet kunne låses til ett identitetsnummer i Folkeregisteret. Det pågående arbeidet med etableringen av «unik» i Folkeregisteret har blitt beskrevet i hovedrapporten under kapittel 2.9.4.

En vesentlig avklaring, som også er et sentralt moment i tilleggsoppdraget, er hvilke av biometriregistrene i justissektoren som skal danne grunnlaget for status «unik» i Folkeregisteret, herunder hvilke opptaksprosesser for biometriske opplysninger som skal ligge til grunn.

Behovet for «unik» på norske statsborgere vil i all hovedsak kunne dekkes av utstedelsen av norske pass. I dag utstedes det oppholdskort med ansiktsfoto- og fingeravtrykk til alle utenlandske statsborgere som har oppholdstillatelse etter tredjelandsregelverket. Tilsvarende gjelder ikke for utenlandske borgere som benytter seg av EØS-registreringsordningen. Derfor kan nasjonalt ID-kort, utover et formål om å øke utbredelsen av sterke ID-bevis i befolkningen, utgjøre et sentralt virkemiddel i å sikre at flest mulig utenlandske borgere registreres med status «unik» i Folkeregisteret. Det forutsettes her at der legges til rette for å gjennomføre en-til-mange søk på tvers av biometriregistrene ved søknader om pass, nasjonalt ID-kort og oppholdstillatelser.

Nasjonalt ID-kort kan anses å ha inneha flere formål. Utgangspunktet er at nasjonalt ID-kort skal være et praktisk ID-bevis med høy tillitt og bredest mulig bruksområde, også for brukere som ikke har, eller får, alternative ID-bevis.[19] Videre er det leverandørens forståelse at det nasjonale ID-kortet skal legge til rette for å bevise på en troverdig måte at en person er rettmessig innehaver av et gitt norsk identitetsnummer. Et slikt formål for ID-kortet er også forenlig med ambisjon 2 i KoIDs visjon for ID-forvaltningen (beskrevet over i kapittel 2.1.4). Nasjonalt ID-kort skal i den sammenheng understøtte ambisjonen om «en person, en identitet i Norge», samt ambisjonen om at «enhver som har fått tildelt et norsk identitetsnummer, i form av et d-nummer eller et fødselsnummer, skal gis mulighet til å dokumentere på en troverdig måte, at han er rette eier av identitetsnummeret fysisk og digitalt». Anvendt på utenlandske borgere er det etter leverandørens oppfatning vesentlig å påpeke

[18] Koordineringsgruppe for ID-forvaltningen (KoID) består av representanter fra Utlendingsdirektoratet, Politidirektoratet, Difi og Skattedirektoratet
[19] JfD, «Prop 66 L (2014-2015)», 2015

viktigheten av at ID-kortet benyttes for å bekrefte den identitet som innehaveren har fått lagt til grunn i Norge av norske myndigheter.

2.1.6 Tidligere vurderinger tilknyttet krav om nasjonalt ID-kort

Sammenhengen mellom tilbudet om nasjonalt ID-kort, utbredelse i befolkningen og ulike former for, eller hjemmel til, å stille krav om nasjonalt ID-kort har vært et gjennomgangstema siden planene for det nasjonale ID-kortet først ble lansert i 2005.

Basert på dokumentasjon forelagt leverandøren, arbeid med hovedrapporten og samtaler med relevante aktører er det flere sentrale poeng en diskusjon om kravsetting til nasjonalt ID-kort nødvendigvis vil måtte ta utgangspunkt i.[20] De viktigste gjengis under.

- Det er avgjørende at et krav om nasjonalt ID-kort ikke bidrar til å innskrenke en brukers rettigheter. Følgelig vil et krav om nasjonalt ID-kort kun være mulig å stille til brukere som har fått et reelt tilbud om ID-kortet, samt en reell mulighet til å anskaffe det. Videre kan det ikke gjøres urimelig byrdefullt for brukeren å møte opp og fremvise ID-beviset, der dette skal kreves

- I henhold til det EØS-rettslige ikke-diskrimineringsprinsippet vil et eventuelt krav som stilles til EØS-borgere også måtte stilles til norske borgere. Dette vil gjelde både for et obligatorisk krav om anskaffelse, og et krav for å få tilgang til rettigheter og ytelser

- Et krav om obligatorisk anskaffelse av nasjonalt ID-kort for norske borgere og/eller utenlandske borgere er i seg selv vanskelig å gjennomføre, blant annet med hensyn til å unngå en innføring av generell legitimasjonsplikt i Norge, samt utfordringer knyttet til finansiering for et påtvunget ID-bevis. Leverandøren har tidligere vurdert dette som et alternativ i hovedrapportens kapittel 10. Det ble ikke anbefalt å gå videre med alternativet, og det har vært en del av tilleggsoppdragets mandat

- Leverandøren antar at få utenlandske borgere vil velge å gå til anskaffelse av et nasjonalt ID-kort med mindre det gjøres god tilrettelegging for anskaffelse og informasjon om fordelene og/eller tjenesteeiere gis hjemmel til å stille krav om nasjonalt ID-kort. Dersom resonnementet i det foregående legges til grunn er det helt avgjørende at det åpnes for å stille en form for krav til nasjonalt ID-kort dersom kortet skal være et effektivt virkemiddel i realisering av ambisjonene for ID-forvaltningen (jf. punkt 2.1.4 og 2.1.5 over). Det samme vil i mindre grad gjelde for norske borgere, ettersom en meget stor andel av befolkningen innehar et sterkt norsk ID-bevis og har avgitt biometri gjennom et norsk pass

Tematikken rundt formålet og mulighetsrommet til å stille krav om nasjonalt ID-kort er også overordnet belyst i hovedrapporten under kapittel 10 om fysiske ID-bevis og utbredelse av nasjonale ID-kort, spesielt kapittel 10.1 og kapittel 10.2.1.

2.1.7 Praksis for tilbud og krav om nasjonale ID-kort i sammenlignbare land

[20] «UNIK», «Helhetlig ansvar for EØS-borgere», «Notat – EØS-rettslig vurdering av nasjonal ordning med ID-kort for EØS-borgere», «Nasjonalt ID-kort til utenlandske borgere», «Oppfølging av oppdrag 053 gitt i 2017 – Nasjonalt ID-kort til utenlandske borgere», informasjon forelagt i møter med relevante aktører

De fleste land i Europa utsteder i dag nasjonale ID-kort. I mange av landene som utsteder nasjonale ID-kort er det også obligatorisk for landets egne statsborgere å anskaffe et slikt nasjonalt ID-kort. Noen få europeiske land (for eksempel Sverige, Finland og Estland) utsteder også nasjonale ID-kort til utenlandske borgere etter visse vilkår. Leverandøren viser under til praksis rundt nasjonale ID-kort for utvalgte sammenlignbare land. Eventuelle krav om fremvisning av nasjonale ID-kort for tjenester og ytelser i sammenlignbare land har vært lite tilgjengelig informasjon i leverandørens kartlegging. Leverandøren bemerker videre at det pågår et arbeid for standardisering av nasjonale ID-kort innenfor EU/EØS-området, jf. europaparlaments- og rådsforordning (EU) 2019/1157 av 20. juni 2019. Forordningen stille felles krav til funksjonalitet og sikkerhetselementer for nasjonale ID-kort, herunder et krav til lagring av maskinlesbare biometriske opplysninger i ID-kortene.

Sverige

Per dags dato utstedes det svenske nasjonale ID-kort kun til svenske statsborgere. Kortet er ikke obligatorisk. Det utstedes også et eget *identitetskort* for folkeregistrerte. ID-kortet kan utstedes til alle som er folkeregistrert i Sverige, inkludert utenlandske borgere med opphold i minst ett år. Identitetskort for folkeregistrerte er heller ikke obligatorisk.

Det er nylig foreslått å utstede et *svensk statlig identitetskort*.[21] ID-kortet foreslås utstedt til svenske borgere og utenlandske borgere som er registrert i svensk folkeregister. For å bli folkeregistrert i Sverige, og dermed få muligheten til å søke om statlig identitetskort, kreves det ifølge loven at personen er bosatt i Sverige.[22]

Danmark

Danmark utsteder ikke nasjonale ID-kort etter EUs definisjon. Likevel kan alle som har en folkeregisteradresse i Danmark og er over en alder av 15 år, uavhengig av statsborgerskap, søke om dansk «legitimationskort». Kortet er ikke obligatorisk.[23]

Finland

I Finland kan nasjonale ID-kort utstedes til finske statsborgere samt utenlandske borgere med gyldig fast opphold i Finland og som godtgjør sin identitet.[24] Det er ikke obligatorisk å anskaffe ID-kortet hverken for finske statsborgere eller utenlandske statsborgere i Finland.

Estland

Estisk nasjonalt ID-kort er obligatorisk for estiske statsborgere og utenlandske statsborgere med fast opphold. Estland utsteder også eget ID-kort til EU/EØS-borgere, som er obligatorisk å anskaffe innen en måned etter å ha meldt flytting til Estland. For tredjelandsborgere med opphold i Estland er oppholdskort obligatorisk, og fungerer som gyldig ID-bevis. Estisk ID-kort til estiske statsborgere og EU/EØS-borgere, samt estisk oppholdskort, inneholder alle funksjonalitet for eID og med fingeravtrykk av innehaveren lagret i kortet. Estisk nasjonalt ID-kort koster 25 euro.[25]

Belgia

[21] «SOU 2019:14 – Ett säkert statligt ID-kort – med e-legitimation», mars 2019
[22] En person anses bosatt i Sverige dersom personen «antas å regelmessig tilbringe sin døgnhvile i landet i minst ett år», jf. § 3 i folkbokföringslagen (1991:481)
[23] Borger.dk, «Legitimationskort», u.å.
[24] Poliisi.fi, «Applying for an Identity card», u.å.
[25] Politsei.ee, «ID-card», u.å.

I Belgia utstedes det nasjonalt ID-kort til Belgiske statsborgere over 12 år. Belgiske statsborgere over 15 år plikter å anskaffe ID-kortet og bære det med seg til enhver tid. Utenlandske borgere i Belgia må på forespørsel kunne fremvise et gyldig pass eller et nasjonalt ID-kort utstedt av et annet medlemsland i EU/EØS. Belgisk nasjonalt ID-kort utstedes med eID.[26]

2.2 Tilbud om nasjonalt ID-kort

Kapittelet tar for seg hvilke brukergrupper som bør få tilbud om nasjonalt ID-kort. Leverandøren beskriver i 2.2.1 den historiske utviklingen i diskusjonen om hvem som skal få tilbud om nasjonalt ID-kort. De ulike tilnærmingene oppsummeres i kapittel 2.2.2. Leverandøren legger deretter frem alternativ med tilhørende vurdering av hvilke brukergrupper som bør få tilbud om nasjonalt ID-kort og hvilke brukergrupper som eventuelt bør unntas et tilbud (kapittel 2.2.3-2.2.5). Avslutningsvis drøftes muligheten for å oppgradere oppholdskortet til et sterkt ID-bevis gjennom å inkludere norsk identitetsnummer på kortet (kapittel 2.2.6-2.2.7).

2.2.1 Utvikling av tilbud om nasjonalt ID-kort (2007-2019)

Den første rapporten som beskrev innføringen av et nasjonalt ID-kort i Norge ble fremlagt i 2007.[27] Vedrørende hvilke grupper som skulle gis rett til å søke om nasjonalt ID-kort ble det foreslått at kortet skulle kunne «*erverves av norske statsborgere og personer med fast opphold i Norge*».

I 2014 ble ID-kortloven fremlagt.[28] I lovforslaget ble det blant annet drøftet hvilket behov utenlandske borgere har for et nasjonalt ID-kort, hvilke krav som skal stilles for godtgjøring av identitet, relevante EØS-rettslige spørsmål, samt hvilke utenlandske borgere som skal anses å ha tilknytning til Norge. Det fremkommer tydelig i lovforslaget at spørsmålene måtte utredes nærmere før endelige beslutninger ble tatt:

> *«Selv om intensjonen er at ordningen med nasjonalt ID-kort skal være et tilbud til utenlandske statsborgere, forutsetter realiseringen av kortet for denne gruppen en mer inngående drøftelse av hvilke vilkår for blant annet godtgjøring av identitet, statsborgerskap og tilknytning til Norge som må stilles for å sikre at ordningen fungerer etter hensikten. På denne bakgrunn er lovforslaget utformet slik at nærmere regler om utenlandske statsborgeres rett til å få nasjonalt ID-kort kan fastsettes i forskrift.»*

POD fikk i tildelingsbrev for 2017 i oppdrag av Justisdepartementet å «*forberede utstedelse av nasjonalt ID-kort til utenlandske statsborgere og fremlegge en plan for når og hvordan ordningen kan gjennomføres*». POD har svart på oppdraget i sin rapport «Nasjonalt ID-kort til utenlandske borgere» fra juni 2017[29], samt «Oppfølging av oppdrag 053 gitt i 2017 – Nasjonalt ID-kort til utenlandske borgere» fremlagt i oktober 2018[30]. I sistnevnte har POD utredet hvilke vilkår som anbefales lagt til grunn for å få utstedt nasjonalt ID-kort. POD har i rapporten anbefalt følgende forskriftsbestemmelse:

> *«Nasjonalt ID-kort kan utstedes til utenlandske statsborgere som utover å ha lovlig opphold har tilknytning til Norge og som godtgjør sin identitet. Med tilknytning til Norge menes utenlandsk statsborger som:*

[26] Brussels.be, «ID-card», u.å.
[27] JD, «Sluttrapport – Nasjonalt ID-kort», 2007
[28] JD, «Prop. 66 L (2014 – 2015) Lov om nasjonalt identitetskort (ID-kortloven)»
[29] POD, «Nasjonalt ID-kort til utenlandske borgere», 2017
[30] POD, «Oppfølging av oppdrag 053 gitt i 2017 – Nasjonalt ID-kort til utenlandske borgere», 19.10.2018

a) *Er folkeregistrert som bosatt i Norge, eller*

b) *Har arbeid av minst 6 måneders varighet med daglig arbeidssted i Norge, eller*

c) *Har fast eiendom i Norge, eller*

d) *På annen måte har tilknytning til Norge og kan sannsynliggjøre et særskilt behov for nasjonalt ID-kort for å legitimere seg i Norge*

EØS-borger som er registrert i Norge med hjemmel i utlendingsloven med forskrifter kan få utstedt nasjonalt ID-kort.»

Videre foreslår POD et krav om «sikker identifisering».

I «Helhetlig ansvar for EØS-borgere» (desember 2018) har en arbeidsgruppe vurdert ulike alternativ for å løse utfordringer knyttet til ID-kontroll ved innrullering i Folkeregisteret og tildeling av fødselsnummer og d-nummer. Alternativet som arbeidsgruppen mener vil gi best uttelling i form av sikkerhet, effektivitet og mulighet for gjennomføring er å utstede nasjonalt ID-kort til utlendinger. I sammenheng med anbefalt alternativ står det videre at «*det vil være formålstjenlig at omfanget av kravet til tilknytning så langt det er mulig samsvarer med vilkårene i folkeregisterloven 2-1*». Vilkårene det vises til i folkeregisterloven omfatter «*personer som er eller har vært bosatt i Norge, er født i Norge eller har fått tildelt fødselsnummer eller d-nummer*». Det står videre at «*det er vesentlig at alle som fyller vilkårene om tilknytning, ikke bare EØS-borgere, må få tilbud om nasjonalt ID-kort eller et tilsvarende ID-bevis*».

Videre ble det i mars 2019 fremlagt et forslag til forskrift om pass og nasjonale ID-kort[31]. Angående tilbud om nasjonalt ID-kort til utenlandske statsborgere er det blant annet skrevet følgende:

> *«Det nasjonale ID-kortet vil i første omgang være et tilbud til norske statsborgere, men intensjonen er å utvide tilbudet til å omfatte også utenlandske statsborgere med tilknytning til Norge, jf. forskriftshjemmelen i ID-kortloven § 14 annet ledd bokstav b. Forslag til forskriftsbestemmelser om utstedelse av nasjonalt ID-kort til utenlandske statsborgere vil bli sendt på egen høring når vilkår og fremdrift er nærmere avklart»*

Etter leverandørens forståelse er det ikke fastsatt en klar tidslinje for når et forslag til forskriftsbestemmelse om utstedelse av nasjonalt ID-kort til utenlandske borgere vil være klart.

2.2.2 Oppsummert vurdering av ulike tilnærminger til tilbud om nasjonalt ID-kort

Som det fremgår av oversikten presentert i kapittel 2.2.1 har retten til å søke om nasjonalt ID-kort lenge vært tiltenkt å på sikt omfatte utenlandske statsborgere, så vel som norske statsborgere. Leverandøren oppfatter likevel at ambisjonsnivået for hvilke utfordringer nasjonalt ID-kort skal løse til dels har økt siden forslaget om ID-kortet først ble fremlagt i 2007. Etter lanseringen av visjon for ID-forvaltningen fra KoID har diskusjonen om hvem som får tilbud om nasjonalt ID-kort i større grad omhandlet muligheten til opptak og lagring av biometriske opplysninger for en størst mulig andel av befolkningen, som et element i realiseringen av «unik» i Folkeregisteret.

Som nevnt i kapittel 2.2.1 har POD i «Oppfølging av oppdrag 053 – Nasjonalt ID-kort til utenlandske borgere» redegjort for et standpunkt for hvilken definisjon av

[31] JD, «Høring – forslag til forskrift om pass og nasjonalt ID-kort», 2019

«tilknytning til Norge» som skal ligge til grunn for utenlandske borgeres mulighet til å søke nasjonalt ID-kort. Forslaget innebærer at en utenlandsk borger skal anses å ha tilknytning til Norge dersom personen oppfyller en av flere vilkår basert på bosetting, arbeid av en viss varighet, fast eiendom eller EØS-registrering. Samtidig foreslås det en «*sikringsbestemmelse som er ment å fange opp fremtidige tilfeller som faller utenfor typetilfellene, men der det likevel er sannsynliggjort et særskilt behov*». Leverandørens forståelse er at sikringsbestemmelsen, slik den er definert, i praksis åpner for at utenlandske borgere med rett på d-nummer, men som ikke oppfyller et av vilkårene nevnt i det foregående, vil falle inn under sikringsbestemmelsen, og dermed også kunne søke om et nasjonalt ID-kort. En slik tolkning av forslaget har også fremkommet i leverandørens møter med POD.

Leverandøren viser her også til «Helhetlig ansvar for EØS-borgere» der arbeidsgruppen fremholder at kravet til tilknytning så langt det er mulig skal følge vilkårene i folkeregisterloven, og dermed også inkludere alle borgere som har fått tildelt et fødselsnummer eller d-nummer.

Basert på punktene i det foregående er det leverandørens forståelse at arbeidsgruppen som forfattet «Helhetlig ansvar for EØS-borgere», i likhet med forslaget fra POD over («oppfølging av oppdrag 053»), stiller seg bak en oppfatning om at dersom en utenlandsk borger oppfyller vilkårene som ligger til grunn for å få tildelt fødselsnummer eller d-nummer, skal vedkommende også anses å ha en slik tilknytning til Norge at vedkommende bør ha rett til å få et tilbud om nasjonalt ID-kort. Leverandøren understreker videre viktigheten av målsettingen om «én person, én identitet i Norge». Dersom målet skal realiseres ved at enhver person med et norsk identitetsnummer får et sterkt ID-bevis utstedt av norske myndigheter, vil det være svært vanskelig å nå et slikt mål med mindre alle personer som får tildelt et fødselsnummer eller d-nummer også får muligheten til å få et nasjonalt ID-kort. I det videre vil leverandøren benytte denne forståelsen som et utgangspunkt til å diskutere hvilke brukergrupper et slikt tilbud (alle med fødselsnummer eller d-nummer) vil treffe, tilhørende volumer, samt om det finnes legitime grunner til at enkelte brukergrupper burde unntas fra et tilbud om nasjonalt ID-kort.

2.2.3 Alternativ 1: Nasjonalt ID-kort tilbys norske borgere og alle utenlandske borgere med rett på norsk fødselsnummer eller d-nummer

Alternativet innebærer at en person som tilfredsstiller kravene etter folkeregisterloven om å få tildelt et norsk fødselsnummer eller d-nummer anses å ha en slik tilknytning til Norge at vedkommende også skal få et tilbud om et nasjonalt ID-kort.

Som vurderingsgrunnlag for alternativet legger leverandøren i det følgende frem vilkårene for registrering i Folkeregisteret for henholdsvis fødselsnummer og d-nummer, samt omfanget av hvilke brukergrupper som omfattes av de ulike vilkårene.

Fødselsnummer

Folkeregisterloven angir vilkårene for registrering i Folkeregisteret samt vilkårene for tildeling av norsk fødselsnummer:

> § 2-1: *I Folkeregisteret registreres alle personer som:*
>
> *a) er eller har vært bosatt i Norge,*
>
> *b) er født i Norge eller*

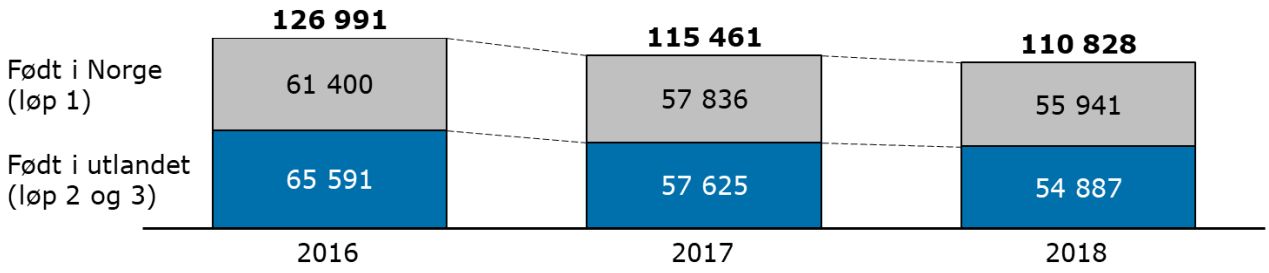
c) har fått tildelt fødselsnummer eller d-nummer

§ 2-2: *Ved første gangs registrering i Folkeregisteret tildeles en person som er **bosatt eller født i Norge**, et fødselsnummer. Fødselsnummer kan også tildeles **norsk statsborger bosatt i utlandet**. For andre personer kan det tildeles et d-nummer etter regler fastsatt i forskrift.*

*§4-2: En person som flytter til en norsk kommune, registreres som bosatt når han eller hun har lovlig opphold i norsk kommune og har til hensikt å bli her i minst **seks måneder**. Opphold av minst seks måneders varighet regnes som bosetting, selv om oppholdet er midlertidig.*

Leverandøren har i hovedrapporten kapittel 6.1.1 beskrevet overordnede volum for tildeling av fødselsnummer i Norge de siste år. Teksten gjengis i kursiv under:

I 2018 tildelte Skatteetaten 110 828 fødselsnummer totalt for alle tre løpene (ref. figur nedenfor). Av disse var 55 941 gjennom fødselsmeldinger fra helseforetak for barn født i Norge, mens 54 887 var for utenlandske borgere. Dette er noe lavere enn tildelte fødselsnummer i 2016 og 2017. Skatteetaten oppgir at de ikke sitter på klare tall på antall tildelte fødselsnummer per brukergruppe for utenlandske borgere da dette ikke oppgis i Folkeregisteret og heller ikke er relevant for Folkeregisterets formål.



Figur 2 Tildelte fødselsnummer siste tre år[32]

Av de 65 591 personene født i utlandet som fikk tildelt fødselsnummer i 2016 var 18 835 EØS-borgere, 4 804 nordiske borgere (eksklusiv Norge) og 8 311 fra Norge (norske statsborgere født i utlandet).[33] Folketallet i Norge angir totalt antall personer som regnes om bosatt i Norge. Per 1. januar 2019 utgjorde dette antallet 5 328 212 personer.[34]

D-nummer

Folkeregisterforskriften angir nærmere hvilke vilkår som gjelder for tildeling av d-nummer:

§ 2.2.3: Hvem som kan tildeles d-nummer

D-nummer kan tildeles fysisk person som ikke fyller vilkåret for å få tildelt fødselsnummer, og som er:

a) skatte- eller avgiftspliktig til Norge, herunder til Svalbard

b) i forretningsforhold med norsk finansforetak som er underlagt finansforetaksloven

c) registreringspliktig i Foretaksregisteret, Løsøreregisteret eller Konkursregisteret

[32] Skatteetaten, mottatt dokumentasjon på fødselsnummer
[33] POD, «Helhetlig ansvar for EØS-borgere», 2018
[34] SSB.no, «Befolkning», 22.02.2019

d) rolleinnehaver i juridisk enhet, jf. enhetsregisterloven § 5 annet ledd litra f og § 6 første ledd litra a–e og h, eller har tilsvarende rolle i utenlandsk deltakerlignet selskap (DLS) eller i selskap som nevnt i skatteloven § 2-4 eller som utfører rapporteringsoppgaver på vegne av slike rolleinnehavere

e) asylsøker eller person med gyldig oppholdstillatelse

f) rettighetshaver i grunnboken

g) omfattet av ordning som forvaltes av Arbeids- og velferdsetaten eller Helseøkonomiforvaltningen, eller som har rettighet utledet fra slik person

h) bosatt på Svalbard, jf. forskrift om register over befolkningen på Svalbard § 2

i) under autorisering som helsepersonell

j) utenlandsk ambassadepersonell eller utenlandske borgere i internasjonale organisasjoner og mellomstatlige konvensjonsorganer med sete i Norge som er tilmeldt til og akseptert av Utenriksdepartementet i medhold av utlendingsforskriften § 1-4 og § 1-5

Tabellen under viser antall d-nummer som har blitt rekvirert siden 2016 fordelt på de ulike rekvirentene. Det fremkommer at det ble rekvirert 107 546 d-nummer i 2018 av totalt elleve ulike rekvirenter. Skatteetaten og NAV stod for 92 prosent av rekvireringene. Ved utgangen av 2018 hadde Folkeregisteret 847 721 aktive d-nummer der 351 585 av dem hadde status «kontrollert». Rekvireringen av d-nummer er også nærmere beskrevet i hovedrapporten i kapittel 2.8.1.

Rekvirent	Antall 2016	Antall 2017	Antall 2018	Antall med norsk adresse i 2018
Skatteetaten	57 140	59 704	60 318	44 121
NAV	18 818	31 644	38 838	711
Brønnøysundregistrene	4 264	3 714	4 160	573
Utlendingsmyndighetene (PU, UNE, UDI)	2 127	2 837	2 277	1
Bank/finans	2 190	1 385	1 096	231
Kartverket	417	356	437	264
Utenriksstasjoner	0	0	388	384
Diverse[35]	0	0	26	0
Helfo	10 085	529	6	0
Total	**95 042**	**100 169**	**107 546**	**46 285**
Andel med norsk postadresse	52 prosent	45 prosent	43 prosent	-
Andel med utenlandsk postadresse	17 prosent	18 prosent	52 prosent[36]	-
Andel uten postadresse	31 prosent	36 prosent	4 prosent	-

Tabell 1 Antall rekvirerte d-nummer fordelt på aktører (2016-2018)[37]

Av de ca. 95 000 personene som fikk tildelt d-nummer i 2016 var 62 106 EØS-borgere (eksklusiv Norden) og 13 607 nordiske borgere (eksklusiv Norge).[38]

Skatteetaten har også oppgitt hvor mange av d-nummer rekvisisjonene i 2018 som ble registrert med norsk postadresse. Dette kan bidra til å gi en indikasjon på om personen d-nummeret ble rekvirert for var i landet på tidspunktet for rekvireringen. Antallet fremkommer av tabellen over. Rekvirenter som ikke er nevnt i tabellen har ikke rekvirert d-nummer med registrert norsk postadresse i 2018.[39]

2.2.4 Beskrivelse av spesielle tilfeller under alternativ 1

Leverandøren beskriver et utvalg av brukergrupper som inngår i definisjonen av «tilknytning til Norge» under alternativ 1, men som av særskilte grunner potensielt bør vurderes unntatt fra tilbudet om nasjonalt ID-kort.

Asylsøkere med uavklart oppholdsstatus

Jf. folkeregisterforskriften har også asylsøkere rett til å få tildelt d-nummer. Det finnes derimot argumenter for at denne gruppen ikke skal kunne erverve nasjonalt ID-kort før asylsøknaden er ferdig behandlet og eventuell oppholdstillatelse er innvilget. Blant annet vil det være vanskelig for utstedende myndighet å gå god for opplysningene på et ID-bevis så lenge prosessen med å verifisere personens identitet er pågående. Det

[35] Samling av rekvirenter med lavt antall rekvisisjoner som ikke lenger har egen kode i oversikt mottatt fra Skatteetaten
[36] Skatteetaten oppgir i e-post 11.11.2019 at det har vært en stor økning i andelen registrert med utenlandsk postadresse grunnet 1) overgangen til elektronisk rekvirering for NAV og Skatteetaten og tilhørende bedre tilrettelegging for registrering av utenlandsk postadresse, og 2) Økt andel av rekvisisjoner fra NAV, som i større grad enn andre rekvisisjoner inneholder utenlandsk postadresse
[37] Basert på data mottatt fra Skatteetaten, andre halvår 2019
[38] POD, «Helhetlig ansvar for EØS-borgere», 2018
[39] Informasjon forelagt leverandøren i e-post fra Skatteetaten, andre halvår 2019

er også uavklart hvorvidt personen vil få innvilget opphold og således vil ha behov for et nasjonalt ID-kort over tid.

Behovet for nasjonalt ID-kort til denne brukergruppen bør ses i sammenheng med hvor lenge en asylsøker kan regne med å vente på å få svar på sin søknad. Leverandøren er kjent med at det foreligger en overordnet ambisjon i UDI om at *«alle saker skal vurderes for vedtak innen tre uker, og at vedtak kan fattes innen 21 dager i ca. 70 prosent av sakene»*[40]. I tildelingsbrev for 2019 står det videre at *«UDI skal gradvis gjennom året realisere ambisjonene i PUMA-prosjektet om at en økt andel av førstegangsvedtak i beskyttelsessaker skal behandles innen 21 dager».*[41] UDI oppgir at median ventetid i asylsaker i perioden januar 2019 til oktober 2019 var på ca. 133 dager. I samme periode ble 41 prosent av asylsakene behandlet innen 21 dager. Det poengteres at mange saker behandles raskt, mens noen saker kan ta lang tid.[42]

Videre har enkelte asylsøkere basert på søknad rett til å ta arbeid under asylsøkerperioden, jf. utlendingsloven §94. UDI opplyser at det er relativt få personer som søker om rett til å arbeide i asylsøkerperioden. Andelen av asylsøkere som får innvilget en midlertidig arbeidstillatelse har fra 2015 til 2018 ligget mellom seks prosent og 14 prosent. Av ca. 1 800 personer som har søkt asyl i Norge i perioden januar til oktober 2019 var det kun tre prosent som søkte om og fikk innvilget en midlertidig arbeidstillatelse. UDI påpeker videre at dette kun omfatter asylsøkere som har rett til arbeid, og at andelen som faktisk er i arbeid vil sannsynligvis være enda lavere.[43]

Utenlandske borgere med begrenset oppholdstillatelse grunnet ikke sannsynliggjort identitet

En særskilt utfordring knytter seg til utenlandske statsborgere i Norge som oppholder seg i Norge på en oppholdstillatelse som er begrenset grunnet at identiteten ikke er sannsynliggjort. Brukergruppen vil inneha norske identitetsnummer og oppholde seg i Norge på ubestemt tid. Samtidig har denne brukergruppen per i dag få eller ingen muligheter til å dokumentere sin identitet overfor norske myndigheter gjennom et sterkt norsk eller utenlandsk ID-bevis. POD har i 2018 innhentet tall fra UDI som tilsier at det finnes om lag 2 200 personer i Norge som inngår i en slik kategori.[44]

Diskusjonen om nevnte brukergruppe skal få tilbud om et nasjonalt ID-kort, selv uten en sannsynlighetsovervekt for at deres identitet er fastsatt riktig, reiser større prinsipielle spørsmål. I all hovedsak omhandler dette avveiningen om kravet til sikker identifikasjon ved utstedelse av nasjonalt ID-kort til utenlandske borgere, og behovet for å sikre at én og samme utlending ikke opptrer med flere identiteter i Norge. Utstedelse av nasjonalt ID-kort til denne brukergruppen vil kunne redusere risikoen for at vedkommende opptrer under andre identiteter i det norske samfunnet. Det vil også gi denne personen mulighet til å beskytte den identiteten han har fått tildelt fra norske myndigheter. Videre vil det redusere risikoen for at andre overtar vedkommende sitt d-nummer, også etter at personen eventuelt har forlatt landet.

Leverandøren viser her til Prop. 66 L (2014 – 2015) Lov om nasjonalt identitetskort (ID-kortloven) punkt 6.3.2. Teksten har også blitt vist til i «Oppfølging av oppdrag 053»:

> *«Det kan være et selvstendig poeng for norske myndigheter at en utenlandsk statsborger får stadfestet én grunnidentitet i Norge gjennom ordningen med nasjonalt ID-kort, selv*

[40] Styringsdokument for PUMA 2020, s. 6
[41] Tildelingsbrev UDI for 2019
[42] Oppgitt i e-post fra UDI 08.11.2019. Ventetidene oppgitt gjelder for førstegangsvedtak i UDI
[43] Oppgitt i e-post fra UDI 08.11.2019
[44] POD, «Oppfølging av oppdrag 053 gitt i 2017 – Nasjonalt ID-kort til utenlandske borgere», 2018

om det ikke fullt ut kan dokumenteres at denne grunnidentiteten er den korrekte. Norske myndigheter, som for eksempel Skatteetaten, NAV, Lånekassen mv. kan ha behov for å basere sin kommunikasjon med utenlandske borgere som har lovlig opphold i Norge på en bekreftet identitet, ikke minst gjennom en tilknyttet eID.

Både i Norge og andre europeiske land gis det oppholdstillatelse til et stort antall personer som ikke har dokumentert sin identitet. Det utstedes også reisebevis for flyktninger og utlendingspass til mange i denne gruppen. Dette er ID-dokumenter som anerkjennes som reisedokumenter. For tredjelandsborgere kan et nasjonalt ID-kort komme til å bekrefte en identitet som i utgangspunktet ikke er riktig. Det dreier seg imidlertid om personer som er innvilget oppholdstillatelse i Norge og som har behov for å dokumentere den identiteten myndighetene har lagt til grunn for å kunne fungere i samfunnet»

Høyesterett har videre belyst behovet for å utstede et sterkt ID-bevis til personer som skal oppholde seg i Norge, men som ikke har sannsynliggjort sin identitet. Leverandøren viser her til HR-2017-2078-A den 31. oktober, der det i begrunnelsen for domsslutning blant annet oppgis følgende:

«En liten gruppe flyktninger med lovlig opphold her i landet, og som må forventes å bli her på ubestemt tid, mangler tilgang til viktige goder og muligheter som befolkningen for øvrig kan ta som en selvfølge. I tillegg til de betydelige ulempene i hverdagslivet, kan denne situasjonen lett tenkes å skape problemer for disse flyktningenes integrering i det norske samfunnslivet. Problemet har sin rot i usikkerheten om deres identitet. Det løses ikke ved å utstede et reisebevis hvor identiteten mest sannsynlig er uriktig. Å sørge for at denne gruppen beboere i Norge får tilgang til i alle fall de mest sentrale godene som de i dag mangler, er en oppgave for myndighetene»

Fra motsatt perspektiv kan det også argumenteres for at denne brukergruppen ikke burde inngå i et tilbud om nasjonalt ID-kort på lik linje med andre innehavere av fødselsnummer og d-nummer. Følger man kravene i ID-kortloven, slik den er utformet p.t. opplyses det at søker av nasjonalt ID-kort plikter å «godtgjøre sin identitet og statsborgerskap». POD oppgir videre i «oppfølging av oppdrag 053» at de legger til grunn at det skal forstås slik at det i kravet til godtgjøring ligger at det ikke skal foreligge noen tvil om at identiteten til søkeren kan anses verifisert.

Videre kan det også hevdes at utstedelse av nasjonalt ID-kort basert på fremleggelse av ID-dokumenter med lav notoritet, eller i tilfeller der identitet ikke er sannsynliggjort, vil bidra til å svekke tillitten til nasjonalt ID-kort som et sterkt ID-bevis. Samtidig er det et argument at personer som ankommer Norge som asylsøkere eller flyktninger vil få mindre insentiv til å fremlegge sine eksisterende ID-dokumenter (i den grad det faktisk er tilgjengelig) dersom vedkommende gis rett til et nasjonalt ID-kort uavhengig av hvilke ID-dokumenter som fremvises.

2.2.5 Leverandørens vurdering av alternativ 1

Alle utenlandske borgere som får tildelt et norsk fødselsnummer burde uten videre anses å ha en tilstrekkelig tilknytning til Norge til å få tilbud om et nasjonalt ID-kort. Leverandøren anser dette som lite problematisk, og at det også er bred aksept for dette blant aktørene i ID-forvaltningen. Dette er også en praksis som benyttes i flere andre sammenlignbare land som utsteder ID-kort til både egne statsborgere og utenlandske borgere, blant annet Finland og Estland.

I vurderingen av hvilke øvrige utenlandske borgere som bør få tilbud om nasjonalt ID-kort har leverandøren lagt til grunn at det bør være en ambisjon om «én person, én identitet» i ID-forvaltningen i Norge, samt at alle innehavere av et norsk identitetsnummer (fødselsnummer og d-nummer) bør gis muligheten til å dokumentere

at de er rette eier av identitetsnummeret. Det er i denne sammenheng, etter leverandørens vurdering, gode argumenter for at et nasjonalt ID-kort til alle som får tildelt et norsk fødselsnummer eller d-nummer vil kunne legge godt til rette for å oppnå målsetningen nevnt i det foregående. Samtlige av brukergruppene som får tildelt fødselsnummer og d-nummer vil ha et behov for å identifisere seg overfor norske myndigheter. Norske myndigheter vil tilsvarende ha et behov for å kunne identifisere vedkommende på en troverdig måte.

Så lenge det settes en klar forutsetning om at det nasjonale ID-kortet ikke knyttes til rettigheter som sådan, men kun utgjør et middel til å bevise at en person er rett innehaver av et norsk identitetsnummer, er det vanskelig å argumentere for at samtlige av brukergruppene som får tildelt et norsk d-nummer ikke som hovedregel skal kunne gis anledning til å bevise deres eierskap til tildelte d-nummer gjennom et nasjonalt ID-kort (leverandørens vurdering av unntakssituasjoner følger under). Gitt at nasjonalt ID-kort til utenlandske borgere utstedes uten reisefunksjonalitet eller andre rettighetstilknytninger, samt at ID-bevisets gyldighet begrenses til å gjelde kun i Norge, fremstår det etter leverandørens vurdering å være relativt lav risiko i å utstede dette til alle som kan få fødselsnummer eller d-nummer.

Sett i et lengre perspektiv vil et tilbud om nasjonalt ID-kort til alle med norsk fødselsnummer og d-nummer også gi et større mulighetsrom for tjenesteeiere til å stille krav om nasjonalt ID-kort uten at kravsetting medfører en innskrenkning av den enkeltes mulighet til å erverve de rettigheter som vedkommende har krav på.

Leverandørens vurdering av spesielle tilfeller under alternativ 1

Vedrørende asylsøkere med uavklart oppholdsstatus er det etter leverandørens vurdering ikke et betydelig behov for å utstede nasjonalt ID-kort til denne brukergruppen under forutsetning om at målsettingen om at minimum 70 prosent av alle asylsaker skal behandles innen 21 dager overholdes. Vurderingen underbygges av det faktum at svært få asylsøkere vil ha behov for det nasjonale ID-kortet i arbeidssammenheng (jf. statistikk fra kapittel 2.2.4).

Videre er det leverandørens vurdering at utenlandske borgere med begrenset oppholdstillatelse i Norge grunnet ikke sannsynliggjort identitet ikke kan ekskluderes fra å ta del i, og fullt ut fungere, i det norske samfunnet. Følgelig må denne brukergruppen nødvendigvis gis tilbud om et sterkt ID-bevis utstedt av norsk myndighet.

Et alternativ er at det utstedes et eget nasjonalt ID-kort til denne brukergruppen, som merkes spesielt for å indikere at innehaverens identitet ikke har vært mulig å sannsynliggjøre i tilstrekkelig grad (slik foreslått utredet av POD i «Oppfølging av oppdrag 053»). Uavhengig om personens identitet er klargjort eller ikke vil et slikt ID-kort være et sterkt bevis som knytter personens biometriske opplysninger til tildelt norsk identitetsnummer, og gi grunnlag for tjenesteeiere til å verifisere dette gjennom en sterk ID-kontroll, forutsatt at utstyr for dette er tilgjengelig. Det er dog relevant å poengtere at det i alternativet ligger en risiko for at et ID-bevis som opplyser om at identiteten til innehaveren ikke er sannsynliggjort vil kunne anses som usikkert av tjenesteeiere. Dette gjelder til tross for at kortet vil gi en sterk knytning mellom person, kort og ID-nummer gjennom biometriske opplysninger. Leverandøren stiller også spørsmål til signaleffekten det vil gi å utstede et slikt «b-kort» til en liten og utsatt andel av befolkningen.

Et annet alternativ er å utstede et nasjonalt ID-kort på like vilkår og med lik utforming som for andre borgere. Basert på tilgjengeliggjort informasjon rundt spørsmålet over er det leverandørens vurdering at nasjonalt ID-kort også bør kunne utstedes til personer med begrenset oppholdstillatelse grunnet ikke sannsynliggjort identitet, på lik

linje som for øvrige borgere. Tilsvarende som over må det være en uttrykkelig forutsetning at nasjonalt ID-kort ikke knyttes til rettigheter av noe slag, men kun utgjør et bevis på at vedkommende er rettmessig eier av et gitt norsk identitetsnummer.

Dersom det skal være et formål for det nasjonale ID-kortet å knytte en person med sitt norske identitetsnummer (jf. kapittel 2.1.5) vil ID-kortloven måtte oppdateres for å reflektere et slikt formål. Ambisjonen fordrer også at kravet til godtgjort identitet, som per i dag er strengt formulert i ID-kortloven, endres på tilsvarende grunnlag.

2.2.6 Alternativ 2: Inkludere norsk identitetsnummer i oppholdskort

Det poengteres innledningsvis at gjennomføring av alternativ 2 ikke utelukker gjennomføring av alternativ 1. Riktignok vil implementering av alternativ 2 kunne ha betydning for hvilke brukergrupper som vil ha behov for et nasjonalt ID-kort.

Alternativ 2 innebærer at oppholdskortet utstedes med innehaverens norske identitetsnummer trykket på kortet. En slik «oppgradering» av oppholdskortet vil innebære at det innehar både identitetsnummer, personalia, ansiktsfoto og biometriske opplysninger lagret digitalt i kortet, og vil således kunne fungere som et sterkt fysisk ID-bevis på lik linje med det nasjonale ID-kortet.

Slik beskrevet i kapittel 2.1.3 er Norge pliktig å utstede oppholdskort til tredjelandsborgere med oppholdstillatelse. Det er også obligatorisk for tredjelandsborgere med opphold i Norge å anskaffe kortet. Oppholdskortet vil derfor måtte utstedes uavhengig av om innehaveren også får et tilbud om nasjonalt ID-kort.

UDI har informert om at det kommer nye oppholdskort i 2020. Forut for dette vil direktoratet vurdere muligheter og kostnader tilknyttet det nye kortet, herunder hvorvidt det vil være hensiktsmessig å innlemme norsk identitetsnummer i kortet. UDI har gitt indikasjoner på at inkludering av norsk identitetsnummer vil være praktisk gjennomførbart og i henhold til lovverket for schengen-standardiserte oppholdskort.

Inkludering av identitetsnummer i oppholdskortet vil trolig innebære at det må tydeliggjøres i regelverket at oppholdskortet også skal utgjøre et gyldig ID-bevis i Norge. Dette vil i så måte utgjøre et tillegg fra leverandørens anbefaling fra hovedrapporten om at det bør tydeliggjøres i regelverket at kun norsk pass og nasjonalt ID-kort skal være gyldige ID-bevis utstedt av norske myndigheter.

Leverandøren ser følgende styrker ved alternativet:

- Alle tredjelandsborgere med opphold i Norge er påkrevd å inneha et gyldig oppholdskort. Således vil det være både praktisk for brukeren, samt kostnadsbesparende for forvaltningen, om innehavere av oppholdskortet kan benytte dette som et sterkt ID-bevis uten å i tillegg måtte gå til anskaffelse av et nasjonalt ID-kort

- Regelverksendringene og ressursene som kreves for å legge identitetsnummeret inn i oppholdskortet antas å være av begrenset omfang

Leverandøren ser følgende svakheter ved alternativet:

- Oppholdskortet vil ikke inneholde funksjonalitet for eID. Oppholdskortet vil derfor ikke kunne erstatte det nasjonale ID-kortets funksjon som sterkt elektronisk ID-bevis

- Oppholdskortet treffer kun en andel av utenlandske borgere i Norge, og vil ikke kunne benyttes som et sterkt ID-bevis av EØS-borgere, tredjelandsborgere med tilknytning til Norge men uten lovlig opphold mv.

- Til forskjell fra nasjonalt ID-kort er oppholdskortet utstedt med en annen hensikt (bevise lovlig opphold) enn et identifiseringsformål. Leverandøren vurderer derfor at en oppgradering av oppholdskortet til et gyldig ID-bevis kan medføre unødig økt kompleksitet til landskapet for hvilke ID-bevis som skal anses gyldige i Norge

2.2.7 Leverandørens vurdering av alternativ 2

Leverandøren vurderer at inkludering av identitetsnummer i oppholdskortet kan inneha enkelte fordeler. Alternativet vil til dels kunne ha en ressursbesparende effekt både for forvaltning og bruker, og vil kunne gjennomføres ved til dels enkle tilpasninger i regelverk og til en relativt lav kostnad.

Leverandører vurderer samtidig at nasjonalt ID-kort i stort vil dekke behovet til ID-bevis for tredjelandsborgere i Norge. Videre vil en oppgradering av oppholdskortet til et ID-bevis kun ha betydning for fysisk legitimering, da funksjonalitet for eID fortsatt ikke vil tas inn i oppholdskortet. Etter leverandørens syn er det fra et prinsipielt ståsted også mer hensiktsmessig at antall sterke norske ID-bevis som anses gyldige i Norge bør utvikle seg i retning av å bli færre, ikke i retning av en økning. Det er også et selvstendig poeng at det skilles mellom oppholdskortets primærformål om å bevise rett til opphold, og et adskilt formål om å bevise innehaverens identitet i Norge. Oppsummert vurderes det at identitetsnummer ikke bør innlemmes i oppholdskortet.

2.3 Krav om nasjonalt ID-kort

Flere tidligere utredninger har belyst nytten av at utstedelse av nasjonalt ID-kort gjennomføres i sammenheng med muligheten til å stille krav om nasjonalt ID-kort for å erverve rettigheter. POD har tidligere foreslått i utredninger (blant annet i utredningen POD, «UNIK», 07.07.2017) at nasjonalt ID-kort bør være en grunnleggende forutsetning for å kunne erverve rettigheter i Norge både for utenlandske borgere og for norske statsborgere. Å kunne stille krav til nasjonalt ID-kort har sammenheng med ID-kortets mulighet til å bygge opp under en høy andel av «unik» i Folkeregisteret og øke omfanget av sikre ID-bevis i omløp (jf. kapittel 2.1.5). Oppnåelse av dette er direkte knyttet opp mot ID-kortets grad av utbredelse blant norske og spesielt utenlandske borgere i Norge, der muligheten til å stille krav vil være avgjørende for å sikre stor utbredelse av nasjonalt ID-kort. Viktigheten av å kunne stille krav om nasjonalt ID-kort for å sikre høy utbredelse av ID-kortet ble også belyst i hovedrapporten under kapittel 10.1.

I informasjonsinnhentingen fra tjenesteeiere gjennomført av POD i forbindelse med «oppfølging av oppdrag 053»[45] fremkommer det videre at tjenesteeiere, herunder Skatteetaten og NAV, selv gjennomgående er interessert i å sette krav om sikker verifisering av identitet med nasjonalt ID-kort/nasjonal eID, såfremt alle deres brukere har mulighet til å få nasjonalt ID-kort.

Erverv av rettigheter vil i denne sammenheng kunne innebære et krav om fremvisning av nasjonalt ID-kort for å bli ID-kontrollert hos Skatteetaten (i forbindelse med

[45] POD, «Oppfølging av oppdrag 053 gitt i 2017 – Nasjonalt ID-kort til utenlandske borgere», oktober 2018

skattekort og rekvirering av d-nummer) og ytelser hos NAV. For å vurdere muligheten til å stille krav beskriver leverandøren først hvilke brukere som i dag påkreves et fysisk oppmøte samt fremvisning av et fysisk ID-bevis hos henholdsvis Skatteetaten (2.3.1) og NAV (2.3.2). Leverandøren beskriver deretter ulike alternativ for disse tjenesteeierne til å stille krav om nasjonalt ID-kort (2.3.3), hvilke konsekvenser dette vil ha for berørte brukergrupper (2.3.4) samt potensielle løsninger for utsatte brukergrupper (2.3.5)

2.3.1 Brukergrupper og fysisk legitimering hos Skatteetaten

Følgende oppgaver hos Skatteetaten krever fysisk oppmøte samt ID-kontroll med fremvisning av et fysisk ID-bevis i dag:

- ID-kontroll i forbindelse med utstedelse av skattekort til utenlandske borgere
- ID-kontroll i forbindelse med innflytting og gjeninnflytting til Norge fra utlandet

Skattekontoret gjennomfører også ID-kontroll *ved behov* av personer som har fått rekvirert d-nummer fra andre rekvirenter enn Skatteetaten samt ved reaktivering av inaktive d-nummer. Aktivitetene som nevnes over er nærmere beskrevet i hovedrapporten kapittel 3.1.1, samt i kapittel 4.2.8 i tilleggsrapporten.

I 2018 ble 143 763 dokumenter kontrollert i Keesing-maskin på skattekontor. Dette omfatter kontroller gjennomført i forbindelse med søknad om skattekort, melding om innflytting, ID-kontroll på vegne av øvrige d-nummer rekvirenter eller for å reaktivere et inaktivt d-nummer.[46]

Samtidig oppgir Skatteetaten at det i 2018 var 110 500 ID-kontroller utført manuelt i skranken. 70 000 av ID-kontrollene var relatert til d-nummer rekvireringer i forbindelse med søknad om skattekort og 40 000 var relatert til tildeling av fødselsnummer. Skatteetaten estimerer at av alle ID-kontrollene som ble gjennomført i 2018, var ca. 79 prosent for EØS-borgere og 21 prosent for tredjelandsborgere.[47]

Fra og med 2019 er det ikke lenger nødvendig for tredjelandsborgere å møte personlig hos Skatteetaten for å bli ID-kontrollert i forbindelse med innflytting og tildeling av skattekort. I forbindelse med vedkommende sitt oppmøte for søknad om oppholdskort sendes det automatisk en melding til Skatteetaten om at søkeren har flyttet til Norge. Personen får dermed tildelt et norsk identitetsnummer dersom søker ikke har det fra før, og blir stående som «kontrollert» i Folkeregisteret.

Unntakstilfeller for kravet om oppmøte for ID-kontroll for søknad om skattekort

Enkelte brukergrupper som er skattepliktige til Norge kan unntas fra kravet om å møte opp til ID-kontroll dersom spesielle vilkår er oppfylt. Skatteetatens liste over personer som er unntatt fra oppmøteplikten er som følger:

- Utenlandske styremedlemmer i norske selskaper som er begrenset skattepliktige til Norge
- Personer som mottar lønn fra den norske stat for arbeid utført i utlandet og som er begrenset skattepliktige til Norge

[46] Informasjon forelagt leverandøren i e-post fra Skatteetaten, andre halvår 2019
[47] Informasjon forelagt leverandøren i e-post fra Skatteetaten, andre halvår 2019

- Personer bosatt i utlandet som mottar pensjon fra Norge og som er begrenset skattepliktige til Norge
- Utenlandske statsborgere som bare arbeider på norsk kontinentalsokkel
- Sjøfolk som arbeider på NIS/NOR fartøy og som er skattemessig bosatt i utlandet
- Personer som har møtt til ID-kontroll tidligere og som har aktivt d-nummer
- Personer som har innflyttet til Norge etter 8. februar 2019 på regelverket for tredjelandsborgere og fått tildelt et fødsels- eller d-nummer

Personer som er i en situasjon der det kan være svært vanskelig å møte opp på et skattekontor og legitimere seg for å søke om skattekort, kan også søke om unntak fra oppmøteplikten. For å få fritak må det sendes skriftlig søknad til skattekontoret med bekreftet kopi av pass/gyldig ID-dokument, kopi av arbeidskontrakt med opplysninger om varighet og oppholdets karakter, utfylt skjema om skattekort for utenlandske og en begrunnelse for hvorfor det vil være svært vanskelig å møte på ID-kontroll. Skatteetaten har informert om at dette gjelder om lag 200 personer per år.

Skatteetaten oppgir at av 60 318 d-nummer som Skatteetaten rekvirerte i 2018 er det 6 488 som står som «ikke-kontrollert» i Folkeregisteret per 12. november 2019. [48] Antallet som står som «ikke-kontrollert» skyldes unntakstilfellene i kravet om oppmøtet nevnt over.

Skatteetaten oppgir videre at det i 2018 ble skrevet ut skattekort til i underkant av 50 000 personer som har fått tildelt et d-nummer (uavhengig av året d-nummeret ble tildelt) og som inngår i en kategori som er unntatt oppmøteplikten. En kategorisering av disse personene er fremstilt i tabellen under:

Kategori	Antall[49]	Unntaksgruppe
Særskilt skatteplikt Kildeskatt	16 285	Personer bosatt i utlandet som mottar pensjon fra Norge og som er begrenset skattepliktige til Norge. Utenlandske styremedlemmer i norske selskaper som er begrenset skattepliktige til Norge
Særskilt skatteplikt Petroleum	15 741	Utenlandske statsborgere som bare arbeider på norsk kontinentalsokkel
Særskilt skatteplikt Eiendom utland	14 273	Personer som er bosatt utenfor Norge som er skattepliktige for en eller flere eiendommer i Norge
Særskilt skatteplikt Utenriks	2 651	Personer som mottar lønn fra den norske stat for arbeid utført i utlandet og som er begrenset skattepliktige til Norge

Tabell 2 Antall personer som fikk tildelt skattekort i 2018 og som inngår i en kategori som er unntatt oppmøteplikten

Forklaring av kategorier:

- Kildeskatt: Ordningen gjelder først og fremst for utenlandske arbeidstakere som jobber i Norge i kortere perioder og som ikke er skattemessig bosatt i Norge. Gjelder blant annet personer som bor i utlandet og mottar styrehonorar og andre lignende godtgjørelser fra norske selskap.

[48] Informasjon forelagt i e-post fra Skatteetaten, 13.11.2019
[49] Antall personer med d-nummer som ble tildelt skattekort i 2018

- Petroleum: Skattepliktig inntekt opptjent på norsk sokkel
- Eiendom utland: Skattepliktig inntekt av fast eiendom eller løsøre i Norge
- Utenriks: Skattepliktig lønn fra den norske stat for arbeid utført i utlandet

Krav og unntak for fremvisning av legitimasjon

For å bli ID-kontrollert hos Skatteetaten må bruker møte opp personlig og fremvise norsk eller utenlandsk pass eller nasjonalt ID-kort. I tillegg har Skatteetaten etablert unntaksordninger for krav om fremvisning av legitimasjon for brukere som av ulike årsaker ikke har mulighet til å anskaffe pass eller nasjonalt ID-kort. Unntakslisten er gjengitt under[50]:

- Asylsøker og overføringsflyktning uten flyktningstatus
- Flyktning, herunder overføringsflyktning med flyktningstatus
- Person på familiegjenforening med flyktning
- Person med opphold på grunnlag av sterke menneskelige hensyn
- Person med refleksjonsperiode (offer for menneskehandel)
- Person som har fått innvilget oppholdstillatelse og ikke kan få pass fra hjemlandets myndigheter

Personer som hører til en av disse gruppene kan legitimere seg med ett av følgende identitetsdokumenter:

- Norsk Schengenstandardisert oppholdskort
- Reisebevis for flyktninger utstedt av norske myndigheter
- Norsk asylsøkerbevis, i kombinasjon med utskrift fra "UDI oppholdsstatus"
- Tidsmessig gyldig passérbrev med Schengen-visum
- Passérbrev med Schengen-visum som ikke er tidsmessig gyldig, men som har påskrift fra politiet om at det gjelder som legitimasjon overfor myndighetene som har ansvaret for Folkeregisteret
- Utlendingspass utstedt av norske myndigheter

2.3.2 Brukergrupper og fysisk legitimering hos NAV

Hvem utbetaler NAV stønader til

Arbeids- og velferdsetaten (NAV) forvalter om lag 35 prosent av statens utgifter fordelt på ca. 50 ulike trygdeytelser. NAV betjener om lag 2,8 mill. brukere og behandler over 3 mill. ytelsessaker i løpet av ett år.[51]

[50] Skatteetaten.no, «ID-kontroll», u.å.
[51] NAV, «NAVs personbrukerundersøkelse», 2018

Medlemskap i folketrygden er nøkkelen til rettigheter fra NAV. I Norge kan en person være medlem som bosatt, eller som arbeidstaker. Personen kan også være medlem i folketrygden under opphold i utlandet. Det er reglene i folketrygdloven eller trygdeavtaler Norge har inngått med andre land, som avgjør om en person er medlem eller ikke. Det er ikke avgjørende at personen er norsk statsborger, registrert i Folkeregisteret eller betaler skatt til Norge.

En kategorisering av NAV sine utbetalinger i 2018 etter størrelse er gjengitt i det følgende:

Stønader og tilskudd fra NAV	Utbetalt, mill. kr, 2018
Alderspensjon	221 068
Uføretrygd	88 108
Sykepenger	39 850
Arbeidsavklaringspenger	32 408
Foreldrepenger	19 538
Barnetrygd	14 873
Dagpenger	10 949
Grunn- og hjelpestønad	3 495
Stønad til enslig mor eller far	2 222
Ytelser til gjenlevende	2 030
Kontantstøtte	1 717
I alt stønader og tilskudd fra NAV	**438 766**

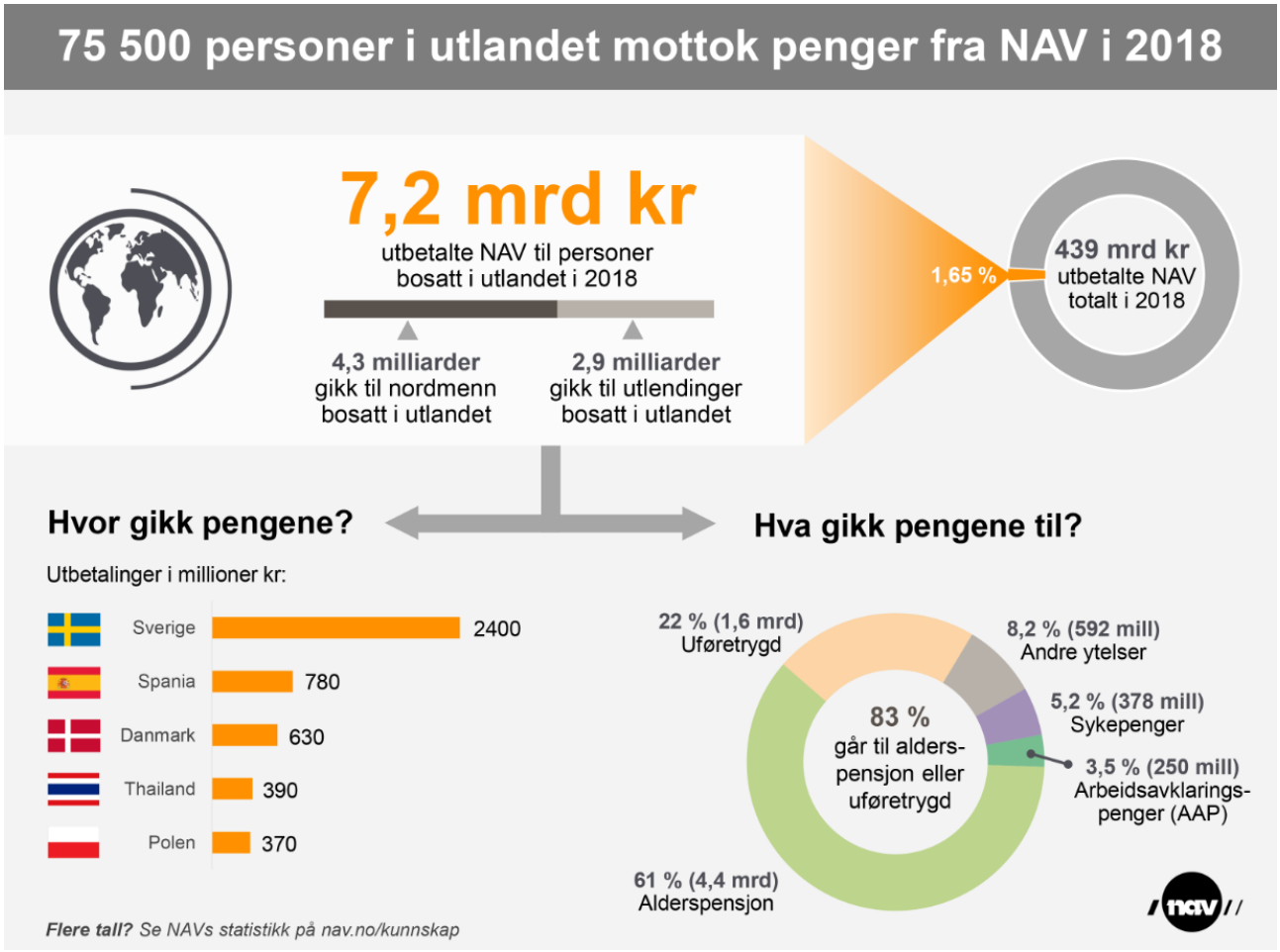
Tabell 3 Oversikt over utbetalinger fra NAV i 2018[52]

Utbetalinger fra NAV til utlandet

Utbetalinger fra NAV vil til en viss grad treffe brukere som oppholder seg i utlandet. Dette vil gjelde både norske og utenlandske statsborgere. Brukergruppen er av spesiell interesse for tilleggsoppdraget, da opphold i utlandet til dels vil legge hindringer for brukerens mulighet til å møte til fysisk ID-kontroll samt avlegge biometriske opplysninger i forbindelse med utstedelse av et nasjonalt ID-kort. Sistnevnte vil nødvendigvis måtte ligge til grunn for å oppnå status «unik» i Folkeregisteret.

NAV fører statistikk over utbetalinger til utlandet fordelt på ytelser og statsborgerskap. Statistikken viser at 75 500 personer bosatt i utlandet mottok utbetalinger fra NAV i fjor (både norske og utenlandske statsborgere). Mer enn halvparten (4,4 mrd. kroner) gikk til alderspensjonister. Norske statsborgere bosatt i utlandet mottok 4,3 mrd. kroner i 2018, mens personer med utenlandsk statsborgerskap bosatt i utlandet mottok 2,9 mrd. kroner. Kun 1,65 prosent av de samlede utbetalingene fra NAV i 2018 gikk til personer bosatt i utlandet.[53] En visualisering av NAVs utbetalinger til utlandet i 2018 er gjengitt under.

[52] NAV.no, «Utbetalt fra NAV per stønadsområde. Mill. kroner og andel til utland», oppdatert 01.04.2019
[53] NAV.no, «Utbetalinger til personer i utlandet», 30.04.2019



Figur 3 Utbetalinger til personer i utlandet fordelt på statsborgerskap og type ytelse, hentet fra NAV.no

Som nevnt over vil brukernes statsborgerskap og oppholdsland ha betydning for mulighetsrommet i å etablere status «kontrollert» og «unik» for mottagerne av utbetalingene. Omfanget av utbetalingene i 2018 for brukergruppen nevnt i det foregående, samt tilhørende antall, er gjengitt i tabellen under.

Stønader og tilskudd fra NAV	Utbetalt totalt (MNOK)	Utbetalt totalt til utlandet (MNOK)	Mottatt av utenlandsk statsborger i utlandet (MNOK)	Antall mottakere i utlandet	Antall mottakere, utenlandske statsborgere
Alderspensjon	221 068	4 395	1 644	47 671	29 146
Uføretrygd	88 108	1 605	286	8 812	2 822
Sykepenger	39 850	378	320	6 900	5 684
Arbeidsavklaringspenger	32 408	250	192	1 205	897
Foreldrepenger	19 538	147	109	1 329	998
Barnetrygd	14 873	136	110	9 330	7 597
Dagpenger	10 949	76	67	1 338	1 181
Grunn- og hjelpestønad	3 495	12	2	924	138
Stønad til enslig mor eller far	2 222	1	0	53	21
Ytelser til gjenlevende	2 030	169	133	2 294	1 715
Kontantstøtte	1 717	51	47	1 189	1 070
I alt stønader og tilskudd fra NAV	**438 766**	**7 220**	**2 911**	**75 463**	**47 601**

Tabell 4 Andel av stønader og tilskudd fra NAV utbetalt til utlandet, til henholdsvis norske og utenlandske statsborgere

Slik vist i tabellen over utbetalte NAV 2,9 mrd. kroner til ca. 47 600 utenlandske borgere bosatt i utlandet i 2018.

Hvordan identifiserer NAV sine brukere

NAVs møte med bruker foregår i voksende grad på digitale flater. Dette påvirker både behov og muligheter NAV har til rådighet for å identifisere sine brukere. I forelagt materiale har NAV oppgitt følgende:

> *Manuell saksbehandling og lokal tilstedeværelse er allerede i vesentlig grad erstattet av digitaliserte selvbetjeningsløsninger og sentralisert forvaltning. Dette er en utvikling som vil forsterkes i årene framover. Arbeids- og velferdsetaten har derfor behov for å erstatte den tidligere ID-kontrollen som lå i kjennskap til lokale forhold og personlig møte med brukeren med andre kontrollmekanismer som ivaretar behov for unik identifisering.*

Videre har NAV oppgitt følgende[54]:

> *For å frigjøre tid til tettere arbeidsrettet oppfølging av personer med et større bistandsbehov, skal brukere som ikke trenger tett veiledning og oppfølging i størst mulig grad få sitt tjeneste- og informasjonsbehov dekket av selvbetjening og internettbaserte løsninger. Økt digitalisering har gitt brukerne bedre tilgjengelighet til NAVs tjenestetilbud, og det har endret måten brukerne kommuniserer med NAV på. Flere henvendelser går via digitale kanaler, og det er færre som ringer eller oppsøker NAV-kontor.*

[54] Oppgitt i e-post fra NAV, andre halvår 2019

Krav til fysisk oppmøte

NAV har opplyst leverandøren om at det ikke foreligger en uttømmende liste over hvilke situasjoner og til hvilke ytelser/stønader en bruker vil måtte møte fysisk. NAV har derimot oppgitt en liste med *eksempler* på situasjoner der en bruker må møte fysisk på et NAV-kontor.

- Dersom bruker mangler/eller ikke har registrert oppholdstillatelse må de møte opp på NAV-kontoret med legitimasjon og bekreftelse på oppholdstillatelse
- Dersom bruker ikke har eID på nivå 4 for å kunne registrere seg som arbeidssøker på nav.no må de møte opp på NAV-kontoret med legitimasjon for manuell registrering
- Det er krav om personlig oppmøte på NAV-kontor ved førstegangs søknad om supplerende stønad og forlengelse av stønaden med legitimasjon
- Det er krav om personlig oppmøte på NAV-kontor ved farskapssaker med legitimasjon

NAV oppgir videre at de også kan foreta ID-kontroller i forbindelse med innvandring fra tredjeland der d-nummer eller fødselsnummer ikke foreligger. Videre kan ID-kontroll forekomme ved arbeidsinnvandring over tre måneder. Likevel er NAV tydelige på at de ikke anser det som sin oppgave å gjennomføre ID-kontroll i forbindelse med d-nummer rekvirering, da det formelle ansvaret er overført til Skatteetaten.[55]

Listen over situasjoner og tilhørende saker der bruker *må* møte opp fysisk er svært begrenset sammenlignet med antall sakstyper og antall saker som NAV behandler. Samtidig påpekes det at muligheten til å kunne møte opp fysisk må opprettholdes, av hensyn til brukere som av ulike grunner ikke har mulighet til å få saken sin behandlet gjennom andre kanaler (eksempelvis brukere uten mulighet til å anskaffe norsk eID på sikkerhetsnivå 4, eller brukere som har med sammensatte oppfølgingsbehov som nødvendiggjør dialog med NAV ved fysisk møte).

NAV oppgir at det ikke føres statistikk koblet til fremleggelse av ID-bevis. Det føres heller ikke direkte statistikk for antall oppmøter som gjennomføres på NAV-kontor i løpet av en gitt tidsperiode.

Enkelte undersøkelser kan likevel gi et innblikk i brukernes oppmøtemønster. Fra Personbrukerundersøkelsen i 2018 oppgir 13 prosent av de spurte at deres siste søknad til NAV ble levert fysisk på et NAV-kontor. 20 prosent oppgir å ha sendt søknaden i posten, mens 67 prosent sendte sin siste søknad til NAV gjennom nav.no. På spørsmålet «På hvilken måte har du vært i kontakt med NAV de siste seks måneder?» svarte 43 prosent at de hadde vært på et NAV-kontor. Av de som møtte på NAV-kontor i 2018 var formålet med oppmøtet hovedsakelig å «møte til forhåndsbestilt time» (59 prosent), «få svar på generelle spørsmål eller få generell informasjon» (26 prosent), «lever eller hente noe, inkl. søknad, dokumentasjon, meldekort eller annet» (21 prosent). Samtidig utgjør andelen brukere som sender eller mottar brev fra NAV litt over halvparten av brukerne. [56]

NAV oppgir videre at av 12,8 mill. innsendte søknader og vedlegg i 2018 ble ca. 1,2 mill. levert ved fysisk oppmøte på et NAV-kontor og ca. 4,5 mill. ble innsendt per post. Øvrige innsendte søknader og vedlegg ble sendt inn via digitale kanaler.[57]

[55] Fra politiets kartlegging av tjenesteeiere, «Svar fra NAV nasjonalt ID-kort»
[56] NAV, «NAVs personbrukerundersøkelse», 2018 (s. 22)
[57] Informasjon forelagt leverandøren i møter med NAV, andre halvår 2019

Retningslinjer og regelverk for gyldig legitimasjon

Plikten om å legitimere seg for en person som krever eller mottar en ytelse er hjemlet i folketrygdlovens paragraf 21.

> *Folketrygdloven § 21-3. Medlemmets opplysningsplikt: En person som krever eller mottar en ytelse, plikter å legitimere seg ved å* ***framvise pass eller annen gyldig legitimasjon*** *når arbeids- og velferdsetaten krever det. Han eller hun plikter også å legitimere seg ved kontakt med helsepersonell eller andre med sikte på erklæringer eller uttalelser mv. til etaten som grunnlag for tilståelse eller fortsatt utbetaling av ytelser*
>
> *Folketrygdloven § 21-4. Innhenting av opplysninger og uttalelser: Helsepersonell eller andre som avgir uttalelser eller erklæringer mv. av betydning for retten til ytelser, skal ved kontakt med stønadstakeren med sikte på slike uttalelser eller erklæringer, kreve at han eller hun legitimerer seg ved å framvise gyldig legitimasjon. Det skal gå fram av erklæringen eller uttalelsen at vedkommende har legitimert seg på gyldig måte. Det er likevel ikke nødvendig å kreve legitimasjon dersom stønadstakeren er kjent for den som skal avgi erklæring eller uttalelse*

Hva som fremgår over som «annen gyldig legitimasjon» spesifiseres ikke nærmere i lovteksten, eller i forespurt materiale fra NAV. Dette har også tidligere blitt omtalt i hovedrapportens kapittel 5.1.2.

På forespørsel fra leverandøren oppgir NAV at det ved søknader må legges ved kopi av ID-dokumenter. Det oppgis ikke til leverandøren hva kopi av ID-dokumenter benyttes til. Eksempelvis for barnetrygd oppgir NAV følgende:

> Det må det legges ved *kopi av arbeidsavtale, fødselsattest, ID-papirer (pass/andre ID-papirer) og tilleggsblankett*. *Sammen med søknaden om barnetrygd eller kontantstøtte legges det også ved: Attest fra hjemlandet som bekrefter at du er forelder til det barnet du søker om stønad for (fødselsattest), hvis barnet ikke er folkeregistrert i Norge. Det er Folkeregisteret eller en annen kompetent myndighet i hjemlandet som fyller ut denne attesten, ID-nummer og adresse fra hjemlandet for deg, barnet og den andre forelderen. For kontantstøtte må du i tillegg legge ved en bekreftelse fra et annet EØS-land på at du har vært dekket av en trygdeordning i minst fem år.*[58]

Rekvireringer av d-nummer

NAV rekvirerer d-nummer kun på vegne av følgende grupper:

- EØS-borgere som har rett til dagpenger fra sitt hjemland i inntil seks måneder mens de søker arbeid i Norge
- Arbeidssøkende EØS-borgere med oppholdsrett i Norge i inntil seks måneder, og som skal registrere seg som arbeidssøkere hos NAV
- Barn og/eller ektefelle av et medlem i folketrygden, når bruker søker om ytelse fra NAV
- Part og/eller barn i bidragssak som skal behandles etter norske regler om underholdsbidrag
- Personer som har behov for at NAV registrerer opplysninger om medlemskap i norsk eller utenlandsk trygdeordning fordi de er omfattet av EØS-reglene om trygd, eller av trygdeavtaler med land utenfor EØS

[58] Oppgitt i e-post fra NAV, andre halvår 2019

NAV oppgir selv at de rekvirerte 35 513 d-nummer i 2018, hvorav 96 prosent er anslått til å være rekvirert på vegne av EØS-borgere.[59] Rekvirering av d-nummer gjøres til Skatteetaten, og det registreres i den sammenheng ikke hvilken tjeneste eller ytelse som er grunnlag for hver enkelt rekvirering. Skatteetaten på sin side oppgir at NAV har rekvirert 38 838 d-nummer i 2018, samt at 37 681 av disse har status som «ikke-kontrollert» i Folkeregisteret per november 2019.[60]

D-nummer kan rekvireres av både NAV Kontor og NAV Ytelse, men nærmest alle d-nummer som NAV rekvirerer foretas av sistnevnte. I perioden juni 2018 til mai 2019 rekvirerte NAV 37 938 d-nummer, hvorav kun 1.018 ble rekvirert av NAV Kontor. NAV Ytelse rekvirerer d-nummer kun basert på innsendte dokumenter, ikke ved personlig oppmøte. Det er ikke forelagt informasjon som tilsier hvilken kontroll som gjennomføres på kopi av innsendte dokumenter. Grunnlaget for å rekvirere er dermed til dels offisielle dokumenter mottatt fra trygdemyndigheter i de landene Norge har avtale med, og dels dokumenter bruker selv sender inn. NAV oppgir videre at «*det vil sjelden være aktuelt å kreve ID-kontroll hos skattekontoret når en enhet i ytelseslinjen rekvirerer d-nummer*»[61].

NAV oppgir videre at det i noen tilfeller registreres en norsk adresse på en rekvisisjon, men det er ikke et obligatorisk felt i rekvireringen. I de tilfeller der NAV mottar utenlandsk identifikasjonsnummer, registreres dette sammen med utstederland, samt statsborgerskap. Det poengteres at dette ikke vil være gjeldende for alle rekvisisjoner. NAV har dermed ikke entydig statistikk på om personene det rekvireres d-nummer for oppholder seg i Norge eller utlandet på rekvisisjonstidspunktet.

For å rekvirere d-nummer må saksbehandler i NAV se dokumentasjon av brukers identitet før d-nummer kan rekvireres. For søknader som behandles gjennom NAV Ytelse (ca. 98 prosent av alle søknader der d-nummer blir rekvirert årlig, jf. avsnitt over), vil det være tilstrekkelig at en kopi av et gyldig ID-bevis legges ved søknaden. For borgere fra EØS-land utenom Norden godtas pass eller nasjonalt ID-kort fra hjemlandet som gyldige ID-bevis. For nordiske borgere kan NAV-kontoret i tillegg til pass eller nasjonalt ID-kort også godta gyldig førerkort og gyldig personutskrift/utdrag/attestasjon fra folkeregisteret i hjemlandet. Dokumentene skal være signert og stemplet.[62]

2.3.3 Alternativ for å stille krav om nasjonalt ID-kort for tilgang til tjenester og ytelser

Under har leverandøren skissert ulike alternativ for å stille krav om nasjonalt ID-kort for tjenester og ytelser. Alternativene er blant annet basert på forslag som har fremkommet i tidligere utredninger og rapporter om nasjonalt ID-kort, leverandørens egen hovedrapport, og samtaler med aktuelle aktører i ID-forvaltningen. Alternativene er utarbeidet med fokus på NAV og Skatteetaten som sentrale tjenesteeiere, men kan enkelt appliseres til et bredere utvalg tjenesteeiere.

For samtlige av alternativene er det vesentlig å påpeke at ingen av alternativene vil kunne gjennomføres på en kort tidshorisont, da nødvendige endringer i regelverk og handlingsmønster hos tjenesteeiere og bruker vil være tidkrevende. Det er også en forutsetning for alle alternativ at det, uavhengig av hvordan det stilles krav om

[59] Oppgitt i e-post fra NAV, andre halvår 2019
[60] Informasjon forelagt i e-post fra Skatteetaten, 13.11.2019. Skatteetaten opplyser at differanse i oppgitte d-nummer rekvireringer mellom Skatteetaten og NAV kan skyldes at statistikk er hentet ut på forskjellige tidspunkter
[61] NAV, «Rutine for rekvirering av d-nummer», 24.05.2018
[62] NAV, «Rutine for rekvirering av d-nummer», 24.05.2018

nasjonalt ID-kort, tydeliggjøres i regelverket at norsk pass og nasjonalt ID-kort som utgjør gyldige norske ID-bevis i Norge.

Alternativ 1: Krav om norsk pass eller nasjonalt ID-kort for tilgang til tjenester og ytelser hos NAV og skattekort fra Skatteetaten

Alternativet innebærer at norsk pass eller nasjonalt ID-kort blir en uttrykkelig forutsetning for tilgang til ytelser hos NAV eller for å søke om skattekort hos Skatteetaten. Dette innebærer videre at eksempelvis utenlandske borgere som har krav på stønad fra NAV og som oppholder seg i utlandet må ha møtt på et pass- og ID-kontor (eventuelt på en utenriksstasjon) forut for ervervelse av ytelser hos NAV. For utenlandske borgere vil anskaffelse av det nasjonalt ID-kortet også være en forutsetning for å søke om skattekort i Norge.

Som beskrevet tidligere i tilleggsrapporten stod NAV og Skatteetaten for over 90 prosent av d-nummer rekvireringer i 2018. Effekten av å stille krav om nasjonalt ID-kort for deres brukere vil derfor sørge for at den store majoriteten av nye d-nummer i Folkeregisteret tildeles til personer som ikke har et annet norsk identitetsnummer fra før. Samtidig vil det medføre en byrde for andelen av personene det rekvireres d-nummer for som befinner seg i utlandet å potensielt måtte reise til Norge (eller en norsk utenriksstasjon) for å avgi biometrisk informasjon.

Vurdering av alternativ 1

Alternativet vil etter leverandørens vurdering kunne gi stor uttelling fra et sikkerhetsperspektiv. I praksis vil det sørge for at de aller fleste som får et norsk identitetsnummer blir «unike» over tid, samt at de gis et ID-bevis som beviser deres knytning til tildelt identitetsnummer. Likevel er det etter leverandørens vurdering flere grunner til at alternativ 1 anses krevende å implementere.

For det første er det utfordrende for utenforstående å evaluere hvilke av tjenesteeiernes brukere utgjør en stor nok risiko for å nødvendiggjøre et krav om pass eller nasjonalt ID-kort, samt for hvilke tjenester og ytelser dette skal gjelde for. Det er tjenesteeieren selv som vil ha best forutsetninger til å gjøre denne vurderingen. Samtidig er det tjenesteeieren selv som i all hovedsak eier risikoen for ID-misbruk. Det vil også for brukergrupper kunne fremstå som et uforholdsmessig tiltak å stille krav om et spesifikt ID-kort eller avgitt biometri i saker som ikke innebærer noen vesentlig risiko for ID-misbruk.

For det andre er det videre klart at både Skatteetaten og NAV tildeler d-nummer og yter tjenester til en ikke-ubetydelig andel brukere som oppholder seg i utlandet. For en andel av personene det gjelder vil et krav om nasjonalt ID-kort eller norsk pass og derav «unik» kunne fremstå som et uforholdsmessig tiltak.

Alternativ 2: Krav om norsk pass eller nasjonalt ID-kort hos Skatteetaten og NAV der det i dag kreves fremvisning av et fysisk ID-bevis ved fysisk oppmøte eller ved søknad i post

Alternativet innebærer at bruker må fremvise enten norsk pass eller nasjonalt ID-kort i tilfeller der bruker avkreves fremvisning av et fysisk ID-bevis i dag eller der bruker legger ved kopi av fysisk ID-bevis i søknad per post. Alternativet innebærer videre at ved alle situasjoner der bruker i dag møter opp hos Skatt/NAV og kan benytte ulike ID-bevis som legitimasjon, vil det i det videre kun være norsk pass eller nasjonalt ID-kort som aksepteres som gyldige ID-bevis.

Omfanget av brukere som møter og fremviser fysiske ID-bevis hos Skatteetaten og NAV i dag er nærmere beskrevet i kapittel 2.3.1 og 2.3.2. Tiltaket vil treffe EØS-borgere

som søker skattekort hos Skatteetaten ved fysisk oppmøte. Det vil derimot ikke ha betydning for brukere som er unntatt oppmøteplikten for ID-kontroll ved søknad om skattekort. For NAV vil implementering av alternativet ha betydning for andelen brukere som møter opp på NAV-kontor og som avkreves et fysisk ID-bevis. Dette utgjør riktignok en svært liten andel av NAVs totale brukerhenvendelser, og vil ikke treffe NAVs brukere som oppholder seg i utlandet, samt brukere som baserer seg på digitale kanaler for kontakt med NAV.

Vurdering av alternativ 2

En styrke ved alternativet er at det vil redusere utfordringer knyttet til bruk av svake fysiske ID-bevis til legitimasjonsformål (herunder førerkort og bankkort med bilde). Således vil det legge til rette for at kontroller som gjennomføres ved fysisk oppmøte blir sikrere. Det vil også bidra som insentiv til anskaffelse av nasjonalt ID-kort.

Leverandøren ser også flere begrensninger ved alternativet. For det første vil alternativ 2 kun treffe et mindre antall av NAV sine brukere. Antallet antas også å være fallende i takt med økt digitalisering.

For det andre stiller leverandøren også spørsmål om hvor effektivt et slikt tiltak vil være fra et sikkerhetsperspektiv. Av samlet antall oppmøter hos NAV vil få oppmøter innebære en så stor risiko for ID-misbruk at det fordrer en sterk ID-kontroll, ettersom mange oppmøter på NAV skyldes oppfølging og veiledning av stønadsmottageren. For brukere som søker om en ytelse per post er det også usikkert hvor mye sikrere en vedlagt kopi av et nasjonalt ID-kort vil være sammenlignet med en kopi av et utenlandsk pass eller nasjonalt ID-kort fra søkers hjemland.

For det tredje vil et oppmøte hos Skatteetaten for ID-kontroll ved søknad om skattekort potensielt være overflødig dersom bruker allerede har møtt på et ID-kontor for å anskaffe nasjonalt ID-kort. Hos Skatteetaten er det i all hovedsak utenlandske arbeidstakere som vil treffes av en implementering av alternativ 2. Dersom en utenlandsk borger først må anskaffe et nasjonalt ID-kort forut for en søknad om skattekort kan det diskuteres hvorvidt behovet for å møte opp på skattekontoret og fremvise et fysisk ID-bevis bortfaller. Således gir det liten merverdi å stille et krav til fysisk legitimering ved dette oppmøtet. Dette må ses i sammenheng med vurderinger og tilhørende anbefalinger fra kapittel 4 om «et felles skrankepunkt».

Alternativ 3: Krav om fremvisning av fysiske ID-bevis settes av tjenesteeiere etter en helhetlig vurdering av ambisjoner for ID-forvaltningen, risiko og belastning for bruker

Alternativet innebærer at tjenesteeiere, herunder NAV og Skatteetaten, vurderer etter risiko hvilke tjenester og ytelser, samt for hvilke brukere det vil være hensiktsmessig å stille krav om norsk pass eller nasjonalt ID-kort ved fysisk legitimering.

Tjenesteeiere «tvinges» dermed ikke til å stille et universelt krav om pass eller nasjonalt ID-kort for samtlige av sine brukere. Tjenesteeiere kan fortsette å akseptere andre fysiske ID-bevis i de tilfeller der sterk ID-kontroll ikke er nødvendig av hensyn til risiko, eller tilfeller der det er urimelig å forvente at en bruker anskaffer seg et nasjonalt ID-kort.

Selv om alternativet ikke innebærer at det fra statlig hold detaljstyres hvilke krav tjenesteeierne skal kunne sette, er det en essensiell del av alternativet at andre prosesser iverksettes i parallell for å underbygge en høy utbredelse av nasjonalt ID-kort. Prosessene beskrives kort under.

Tjenesteeiere og rekvirenter gis hjemmel til å stille krav om nasjonalt ID-kort og kontroll ved fysisk oppmøte for sine brukere der det anses som proporsjonalt i henhold til risiko og byrde for bruker. Et eksempel til etterfølgelse kan være forslaget fra NFD til endringer aksjelovgivningen mv., som for øyeblikket er ute på høring.[63] Høringsnotatet belyser behovet for sikker identifisering fra perspektivet til blant annet foretaksregisteret, og foreslår at foretaksregisteret gis hjemmel til å kreve kontroll av identitet blant annet med krav om fysisk oppmøte i forbindelse med rekvirering av d-nummer.

Det gjennomføres en kollektiv og koordinert innsats for å tydeliggjøre at det er norsk pass og nasjonalt ID-kort som anses som gyldige ID-bevis i Norge (ikke førerkort og bankkort med bilde). Dette tydeliggjøres for eksempel i regjeringens strategi for ID-forvaltningen (anbefaling 1 i hovedrapporten) og som felles føringer i relevante tildelingsbrev

Igangsette initiativ til å informere tjenesteeiere og brukere om hvilken nytte et krav om nasjonalt ID-kort vil ha, både for den enkelte tjenesteeier og bruker, men også i et større bilde mot målsettingen om høy andel «unik» i Folkeregisteret

Etablere et nært samarbeid mellom pass- og ID-kortmyndigheten, utlendingsmyndighetene og relevante tjenesteeiere. I tjenesteeiernes vurderinger av hvilke brukere det skal stilles krav til bør dette gjøres i tett dialog med nevnte aktører. Samarbeid vil være viktig for å få en best mulig forståelse av risikobildet, og således hvor sikkerhetskravene vil være mest nødvendig.

Vurdering av alternativ 3

I motsetning til alternativ 1 og 2 utgjør alternativ 3 en mer fleksibel tilnærming. Alternativet tar høyde for at det ikke vil være rimelig å avkreve et nasjonalt ID-kort av alle (utenlandske borgere) som har rett på tjenester og ytelser i Norge.

Videre er det en vesentlig styrke ved alternativet at brukervennligheten i større grad blir ivaretatt. For tjenester eller brukere der risikoaspektet anses som lavt, eller i brukerdialog der behovet for sterk ID-kontroll er minimalt, vil det være langt mer brukervennlig for bruker å kunne benytte andre ID-bevis som vedkommende har anskaffet fra før.

Selv uten at tjenesteeiere tvinges til å stille krav til alle er det etter leverandørens vurdering avgjørende at det iverksettes tiltak for å stimulere tjenesteeiere til å stille krav om norsk pass eller nasjonalt ID-kort til flest mulig. Prosesser for dette er beskrevet som en del av alternativ tre, og vil etter leverandørens vurdering sørge for at forvaltningen over tid beveger seg i retning av visjonen for ID-forvaltningen.

Den sentrale ulempen ved alternativet, etter leverandørens vurdering, er at effekten av nasjonalt ID-kort som et virkemiddel for å oppnå høy andel status «unik» i Folkeregisteret svekkes. Slik det er skissert gir alternativet ingen garanti for at utenlandske borgere vil gå til anskaffelse av det nasjonale ID-kortet, og således ingen garanti for en høy andel «unik» i Folkeregisteret for utenlandske borgere. Hvor stor innvirkning denne svakheten vil ha, avhenger av i hvilken grad tjenesteeiere vil velge å stille krav om nasjonalt ID-kort til utlendinger.

[63] NFD, «Forslag til endringer i aksjelovgivningen mv. (tilknytningskrav for styremedlemmer og daglig leder mv.)», 2019

2.3.4 Konsekvenser av å stille krav

Gjeldende EØS-rett tilknyttet muligheten til å stille krav om nasjonalt ID-kort for erverv av tjenester og ytelser i Norge

En viktig avklaring knyttet til alternativene presentert i kapittel 2.3.3 over er hvorvidt det vil være i henhold til EØS-retten å kreve et nasjonalt ID-kort av utenlandske borgere for tilgang til rettigheter og ytelser i Norge. Det vil også måtte avklares om det har betydning at samme krav også stilles overfor norske borgere. Avklaring av spørsmålene er relevant for leverandørens vurderinger og anbefalinger, men leverandøren påpeker at det ikke inngår i leverandørens mandat å gjennomføre en komplett juridisk vurdering av disse spørsmålene. I følgende delkapittel begrenser derfor leverandøren seg til å gjengi relevant forelagt dokumentasjon på problemstillingen.

Mulighetsrommet til å stille krav om nasjonalt ID-kort til utenlandske borgere må vurderes blant annet ut ifra EØS-retten. Særlig relevant er reglene om fri bevegelighet for personer som finnes i EØS-avtalen del III og direktiv 2004/38/EF[64]. Dette er implementert i norsk rett ved utlendingsloven kapittel 13. Direktivet sier blant annet at EØS-borgere kan reise til en annen EØS-stat og oppholde seg og arbeide der inntil tre måneder uten å måtte oppfylle andre krav enn å vise et gyldig identitetsbevis eller pass utstedt i en EØS-stat.

I materiale forelagt leverandøren er spørsmålene over drøftet i et notat fra lovavdelingen fra 2014.[65] I notatet fremholder lovavdelingen i JD at en ordning om krav til utenlandske borgere om identifisering med nasjonalt ID-kort for tilgang til tjenester (fra NAV) vil kunne utgjøre en restriksjon på reglene om fri bevegelighet. Ordningen vil således måtte begrunnes i et legitimt hensyn, samt at ordningen må anses å være egnet, nødvendig og forholdsmessig. Lovavdelingen konkluderer med at ordningen antagelig vil kunne begrunnes i *hensynet* til «bevarelsen av trygdesystemets økonomiske likevekt» og bekjempelse av bedrageri. Lovavdelingen anser det derimot som vanskelig å argumentere for at et nasjonalt ID-kort vil være *nødvendig* og *forholdsmessig* i en slik grad at det gir grunnlag for å kunne avkreve EØS-borgere et nasjonalt ID-kort for mottak av skattekort og mottak av ytelser fra NAV. Notatet er tydelig på at krav som stilles til EØS-borgere og ikke samtidig stilles til norske statsborgere vil være direkte diskriminering i strid med EØS-avtalen. Notatet tar ikke stilling til om et krav som både omfatter norske borgere og utenlandske borgere vil tilfredsstille EØS-kravene. Lovavdelingen trekker frem i notatet at vurderingen vanskeliggjøres grunnet stor usikkerhet (på gjeldende tidspunkt) rundt formål og format på det nasjonale ID-kortet samt hvem ID-kortet skulle utstedes til.

Det sentrale spørsmålet om hvilke forutsetninger som kan eller må ligge til grunn for å kunne avkreve nasjonalt ID-kort av EØS-borgere i henhold til EØS-regelverket blir dermed ikke i sin helhet avklart i notatet.

4. januar 2016 leverte advokatfirmaet Simonsen Vogt Wiig en utredning om Norges forpliktelser etter Unionsborgerdirektivet.[66] Utredningen tar blant annet for seg hvilke vilkår som må overholdes etter EØS-regelverket og hvordan vilkårene kan tolkes. Således er innholdet i rapporten relevant for mulighetsrommet til å stille krav om nasjonalt ID-kort.

[64] Europa-parlamentet og Rådet, «Direktiv 2004/38/EF av 29. april 2004 om EØS-borgere og deres familiemedlemmers rett til å bevege og oppholde seg fritt på medlemsstatenes område», 2004
[65] JD, «EØS-rettslig vurdering av nasjonalt ordning med ID-kort for EØS-borgere», 06.11.2014
[66] Simonsen Vogt Wiig, «*Legal study on Norway's obligations under the EU Citizenship Directive 2004/38/EC*», 04.01.2016

Rapporten «Helhetlig ansvar for EØS-borgere»[67] har i eget kapittel beskrevet hvilke absolutte rammer som må ligge til grunn for eventuelle løsningsalternativ. Rapporten henviser til utredningene nevnt over, og trekker frem momenter av særlig relevans for spørsmålet om krav til EØS-borgere. Blant annet vises det til følgende:

> *«Reglene om fri bevegelighet innebærer at det er **forbudt å innføre restriksjoner på den frie bevegeligheten** (rett til innreise og opphold), **såfremt begrensningen/restriksjonen ikke kan begrunnes i hensynet til offentlig orden, sikkerhet og folkehelse.** Det er videre et vilkår at begrunnelsen med hensyn til offentlig orden, sikkerhet og folkehelse er knyttet til den enkelte EØS-borgers personlige forhold, altså at en bestemt person utgjør en slik alvorlig trussel som nevnt i artikkel 27 i direktivet at han nektes å utøve rettighetene etter direktivet. Det skal foretas en sak-til-sak-vurdering, **og tiltaket kan ikke ha en generell preventiv karakter**, jf. artikkel 27 i direktivet.»*

I rapporten står det videre:

> *Direktiv 2004/38/EF om fri personbevegelighet inneholder en rekke bestemmelser om EØS-borgerens rett til å ferdes og oppholde seg i EØS-området. Formålet med direktivet er å gjøre det enklere for EØS-borgere og deres familiemedlemmer å bevege seg på tvers av EØS-landene for å arbeide, studere, drive næringsvirksomhet med mer. En rød tråd i direktivet er at **det skal legges stor vekt på den frie bevegeligheten og mindre vekt på kontrollhensynet**, og formaliteter eller administrative tiltak som kan begrense denne friheten skal holdes på et minimum – slik at den frie ferdselen tilnærmet blir som å ferdes innad i et medlemsland. **Ved innføring av administrative tiltak er det av betydning om restriksjonen er egnet og nødvendig for å oppnå det formål som ligger bak ordningen.** Det avgjørende etter EU-domstolens praksis vil ofte være om det finnes **mindre inngripende reguleringsmuligheter** blant de tiltakene som er egnet til å ivareta det aktuelle hensynet. Restriksjonen må i tillegg være **forholdsmessig** sett hen til det som ønskes oppnådd.*

I tillegg til momentene over knyttet til fri bevegelighet viser rapporten til behovet for å overholde grunnprinsippet om forbud mot nasjonalitetsbestemt forskjellsbehandling (ikke-diskrimineringsprinsippet). I likhet med retten til fri personbevegelighet er det nødvendig at ikke-diskrimineringsprinsippet overholdes med mindre annet kan begrunnes i hensynet til offentlig orden, offentlig sikkerhet og folkehelse.

Leverandøren har i arbeidet med tilleggsoppdraget vært kjent med utredningene nevnt i det foregående. Som nevnt innledningsvis er en komplett juridisk vurdering av om hvorvidt et nasjonalt ID-kort utstedt av norske myndigheter kan avkreves en EØS-borger for tilgang til rettigheter i Norge ikke direkte en del av leverandørens mandat. Leverandøren har i drøftingen av ulike alternativ i tilleggsoppdraget lagt til grunn at et krav om nasjonalt ID-kort vil ligge innenfor norske myndigheters handlingsrom etter EØS-regelverket, såfremt det stilles krav om enten norsk pass eller nasjonalt ID-kort også til norske statsborgere. Dette er en gjennomgående forutsetning som ligger til grunn i mange av rapportene som er tilgjengeliggjort for leverandøren.[68] Samtidig er det leverandørens vurdering at utredningene og rapportene nevnt i delkapittelet over ikke i nødvendig grad har avklart hva mulighetsrommet er. Det vil være sentralt at spørsmålet blir gjenstand for en nærmere juridisk vurdering i det videre arbeidet.

[67] POD/SKD/UDI, «Helhetlig ansvar for EØS-borgere», desember 2018
[68] «UNIK», «Helhetlig ansvar for EØS-borgere», «Nasjonalt ID-kort til utenlandske borgere» og «Oppfølging av oppdrag 053 gitt i 2017 – Nasjonalt ID-kort til utenlandske borgere»

Personer på korte opphold i Norge

Nasjonalt ID-kort vil i Norge utstedes ved samme utstedelseslokasjoner som norske pass. Slikt sett vil ventetiden for å søke om pass og nasjonale ID-kort i Norge være sammenlignbare. Leverandøren er ikke forelagt statistikk over gjennomsnittlig ventetid for utstedelse av pass, men er kjent med tilfeller der det kan ta opptil flere måneder å få time til å bestille norsk pass. Lange passkøer, særlig i høysesong for søknader, er nærmere beskrevet i hovedrapportens kapittel 5.

Dersom nasjonalt ID-kort blir en forutsetning for utenlandske borgeres tilgang til tjenester og ytelser i Norge er det avgjørende at ventetiden for utstedelse av det nasjonale ID-kortet ikke vil utgjøre en «flaskehals» for rettigheten til å arbeide. Som et eksempel utgjør arbeidsinnvandrere en stor andel av personer som kommer til Norge årlig. Dersom det nasjonale ID-kortet utgjør en forutsetning for å arbeide (gjennom et vilkår for utstedelse av skattekort) er det essensielt at arbeidsinnvandrer ikke må vente ukesvis, eller månedsvis, for å kunne søke om kortet. Korte ventetider for det nasjonale ID-kort vil for flere tjenesteeiere nærmest være en forutsetning for om de vil kunne stille krav om ID-kortet. Dersom et krav implementeres er det derfor viktig at det ses i sammenheng med politiets kapasitet til å utstede ID-kort.

Dersom personer på korte opphold i Norge avkreves et nasjonalt ID-kort vil det også være nærliggende at prosessen for å anskaffe ID-kortet samkjøres med andre prosesser som vedkommende må gjennomføre (eksempelvis rekvirering av identitetsnummer eller søknad om skattekort). Dette for å redusere tidsbruken for bruker og sørge for at vedkommende kommer raskt i gang. I kapittel 4 vurderes ulike tilnærminger til et felles skrankepunkt for utvalgte ID-relaterte oppmøter og således presenterer mulige løsninger på en slik problemstilling.

Utenlandske borgere med opphold i utlandet

Et krav om nasjonalt ID-kort for tilgang til tjenester og ytelser vil være spesielt krevende å overholde for personer som har tilknytning til Norge uten å oppholde seg i landet. Utstedelse av nasjonalt ID-kort forutsetter fysisk oppmøte på en lokasjon der nasjonalt ID-kort utstedes. For personer med opphold i utlandet vil det være rimelig å anta at det i mange tilfeller vil måtte påregnes lang reisevei for å møte opp ved søknad om nasjonalt ID-kort. For NAV kan dette omfatte opptil ca. 75 000 personer årlig, derav ca. 47 000 er utenlandske borgere (jf. kapittel 2.3.2). Av totalt ca. 60 000 d-nummer som Skatteetaten rekvirerte i fjor var det ca. 6 000 personer som var unntatt oppmøteplikten for ID-kontroll (jf. kapittel 2.3.1), i all hovedsak personer som oppholder seg i utlandet.

2.3.5 Potensielle løsninger for utsatte brukergrupper

Personer på korte opphold i Norge

For personer på korte opphold i Norge (og/eller personer med raskt behov for nasjonalt ID-kort) vil det måtte etableres særskilte løsninger. Ett tiltak vil være å sikre nødvendig kapasitet til politiet for å sikre rask og effektiv utstedelse av nasjonalt ID-kort.

Utenlandske borgere med opphold i utlandet

Det vil være sentralt å utrede hvorvidt nasjonalt ID-kort skal kunne utstedes til utenlandske borgere på utenriksstasjoner, på lik linje med utstedelsen av norske pass i utlandet i dag. Muligheten må ses i lys av et langt høyere kostnadsnivå for utstedelse av ID-bevis i utlandet. Samtidig kan det bli en utfordring å sørge for tilstrekkelig kompetanse for verifisering av identitet og utenlandske dokumenter på alle

utenriksstasjoner som kan medføre en sikkerhetsutfordring. På den annen side vil byrden som pålegges bruker være betydelig mindre dersom brukeren har anledning til å søke om nasjonalt ID-kort i det landet brukeren befinner seg i.

2.4 Vurdering av dagens ID-kontroll hos sentrale tjenesteeiere og behovet for styrket kontroll

Skatteetaten

I hovedrapporten kapittel 6.1.1 og 6.1.2 har leverandøren beskrevet kvalitet og sikkerhet i forbindelse med tildeling av henholdsvis fødselsnummer og d-nummer. ID-kontrollen som gjennomføres av Skatteetaten i den sammenheng inngår her. ID-kontrollen er også delvis omtalt i hovedrapportens kapittel 5.1.2 (*krav til legitimasjon for tjenester og ytelser).*

NAV

I hovedrapportens kapittel 6.1.2 har leverandøren beskrevet forhold knyttet til kvalitet og sikkerhet hos blant annet NAV. Kapittelet tar for seg kvalitet og sikkerhet knyttet til d-nummer rekvirering, og beskriver ikke øvrige situasjoner der NAV har behov for å identifisere sine brukere. Hvilke legitimasjonskrav som NAV legger til grunn for vedtak om ytelser er overordnet beskrevet i hovedrapportens kapittel 5.1.2 (*krav til legitimasjon for tjenester og ytelser).*

Basert på videre arbeid i forbindelse med tilleggsoppdraget bemerker leverandøren at NAVs retningslinjer for hvilke fysiske ID-bevis som anses som gyldige til legitimeringsformål (både ved fysisk oppmøte og ved søknader per post) fremstår som svært uklare. Kunnskapen om hvordan dette faktisk blir gjennomført i praksis fremstår videre som mangelfull. Uavhengig av spørsmålet om hvilke krav som skal stilles vurderer leverandøren at det kan være fordelaktig at etaten etablerer og implementerer tydeligere retningslinjer og praksis for hvilken fysisk legitimasjon som skal regnes som gyldig i ulike situasjoner.

Leverandørens vurdering av behov for bedre ID-kontroll

Dersom det stilles krav om «kontrollerte» og på sikt «unike» identitetsnummer (jf. anbefaling fem i hovedrapporten) vil dette ha noe begrenset verdi uten at tjenesteeiere samtidig har muligheten for å kontrollere at personen som møter er rettmessige eier av ID-beviset. Hjelpemidler for biometrisk kontroll, noe hverken Skatteetaten, NAV eller andre aktører i offentlig sektor har per dags dato, vil vesentlig styrke en slik kontroll.

Under presenteres to eksempler som illustrerer viktigheten av utstyr for biometrisk kontroll:

- *Tjenesteeier krever status «unik» uten utstyr for biometrisk kontroll:* Statens vegvesen kan kreve at en utenlandsk borger som ønsker å få norsk førerkort (enten førstegangsutstedelse eller innbytte av sitt hjemlands førerkort) har et norsk identitetsnummer og står oppført med status «unik» i Folkeregisteret. Vedkommende møter da på trafikkstasjon for å søke om utstedelse/innbytte, fremviser sitt nasjonale ID-kort. Saksbehandler i skranken sammenligner ansiktsfoto i ID-kortet med kortets angivelige eier. Dersom vedkommende innfrir vilkårene for norsk førerkort sendes dette til oppgitt adresse etter en gitt tidsperiode. Sikkerheten i ID-kontrollen som er gjennomført for utstedelsen av det norske førerkortet hviler dermed på saksbehandlerens evne til å

sammenligne ansiktsfoto på ID-kortet opp mot utseendet til personen som har møtt opp

- *Tjenesteeier krever status «unik» og verifiserer ID-kort mot person med biometrisk utstyr:* Prosess-stegene er tilsvarende som over, men saksbehandler benytter utstyr for å verifisere at fremlagt nasjonalt ID-kort er autentisk og ikke meldt tapt, samt benytter ansiktsgjenkjenningsteknologi som verifiserer brukers identitet ved å sammenligne personens fysiske utseende opp mot ansiktsbiometri lagret i det nasjonale ID-kortet. Hjelpemidler som kan benyttes til et slikt formål er eksempelvis politiets Taps og verifikasjonstjeneste (TOVE) alternativ 1 eller applikasjonen IDmee. Disse verktøyene og deres bruksområde er nærmere beskrevet i kapittel 3 om eID, blant annet i delkapittel 3.1.5 og 3.5.2

Hva gjelder fysiske ID-kontroller har Skatteetaten og NAV per i dag svært begrensede forutsetninger for å avdekke en imposter[69]. Leverandøren viser her til kapittel 2.1.5, der det poengteres at det nasjonale ID-kortet skal muliggjøre en sterk knytning mellom en persons norske identitetsnummer, personens biometriske opplysninger og personens status som «unik» i Folkeregisteret. Verifiseringen av denne knytningen vil dog ikke kunne styrkes uten at kontrolløren gis forutsetninger for å gjøre en biometrisk kontroll av person opp mot biometriske opplysninger lagret i fremlagt ID-bevis. Leverandøren anerkjenner at opplysningen om «unik» og/eller et krav om fremvisning av norsk pass eller nasjonalt ID-kort vil begge isolert sett kunne ha en verdi for tjenesteeier. Verdien vil øke betraktelig ved en biometrisk verifisering i kontrollsituasjoner. Etter leverandørens vurdering er det derfor nødvendig å implementere hjelpemidler eller utstyr for biometrisk kontroll i skrankepunktet dersom imposter-problematikken skal adresseres.

2.5 Tilrettelegging for «unik» i Folkeregisteret

2.5.1 Vurdering av opptak av biometri gjennom EØS-registreringsordningen

Følgende delkapittel er knyttet til tema 1 punkt 2 i oppdragets mandat (jf. tilleggsrapportens kapittel 1.1). I mandatet har leverandøren fått i oppdrag å vurdere muligheten for å benytte registreringsbevis til EØS-borgere som grunnlag for registrering som «unik» i Folkeregisteret. Kapittelet baserer seg på dialog med relevante aktører og dokumentasjon forelagt leverandøren.

Spørsmålet om biometriopptak kan inngå i EØS-registreringsordningen har tidligere vært drøftet i en rekke utredninger. De viktigste gjengis under.

Tidligere utredninger

I rapporten «Nasjonalt ID-kort til utenlandske borgere» (30. juni 2017) utarbeidet av POD omtales muligheten for å «*skjerpe kravet til identifisering for EØS-registrering*». Rapporten påpeker behovet for sikker ID-verifisering ved EØS-registrering, og anbefaler at det bør forutsettes at EØS-borger legger frem pass eller nasjonalt ID-kort fra hjemlandet. Samtidig vises det til EU-direktiv 2004/38/EF om hvilke begrensninger som foreligger for dokumentasjonskravet for registrering og utstedelse av registreringsbevis.

I rapporten «Helhetlig ansvar for EØS-borgere» (desember 2018), utarbeidet av POD, UDI og SKD i felleskap, ble EØS-registreringsordningen vurdert med tanke på ordningens relevans i å bekjempe arbeidslivskriminalitet. Rapporten konkluderer med

[69] En person som utgir seg for å være an annen

at EØS-registreringsordningen «*ikke er egnet til å avdekke om en person er registrert i Folkeregisteret med fødsels- eller d-nummer fra før*». Dette begrunnes blant annet i at EØS-regelverket ikke gir anledning til å registrere biometri i forbindelse med EØS-ordningen, samt at regelverket angir restriksjoner på å innføre ordninger som ikke også gjelder for norske borgere. Rapporten påpeker videre at ordningen anses som lite treffende, da den ikke dekker nordiske borgere eller EØS-borgere som oppholder seg i landet under tre måneder. Med henvisning til direktivt 2004/38/EF fremheves det i rapporten at «*det er etter dette antatt at det ikke er adgang til å rutinemessig kreve avlagt biometri for å kunne registrere seg eller utøve sine rettigheter etter direktivet. Dette er også lagt til grunn av departementet i Prop. 90L (2015-2016), punkt 10.7.1».*

Juli 2017 leverte en arbeidsgruppe bestående av SKD, UDI og POD en rapport ved navn «UNIK». I rapporten utredet arbeidsgruppen hva som skulle til for å overføre status «unik» fra biometriregistrene i justissektoren til Folkeregisteret. POD og UDI anbefaler i rapporten at muligheten for å utstede nasjonale ID-kort til EØS-borgere i stedet for – eller som tillegg til – registreringsbeviset utredes nærmere.

Leverandørens kartlegging

Utover forelagt materiale har leverandøren gjennomført møter med relevante aktører for å kartlegge i hvilken grad biometriopptak kan inngå i EØS-registreringen og følgelig danne grunnlag for «unik» i Folkeregisteret for EØS-borgere.

I møte med UDI ble representanter for direktoratet forespurt om å redegjøre for sitt standpunkt på temaet. UDI var tydelige på at EØS-registreringsprosessen slik den nå gjennomføres innehar en svært begrenset bruksverdi. Videre så de ingen mulighet for å benytte biometri som del av EØS-registreringsprosessen av hensyn til EØS-regelverket.

I møte med POD fremholdes det at EØS-regelverket antagelig må endres dersom biometriopptak gjennom registreringsordningen skal la seg gjøre. Tilsvarende ble det i møte med ASD oppgitt at det er helt uaktuelt å oppta biometri i forbindelse med EØS-registreringsordningen.

Etter samtaler med Skatteetaten fremkommer det at det per i dag er et krav om å fremvise EØS-registreringsbevis ved melding om innflytting til Norge for EØS-borgere. Det opplyses videre at det pågår et arbeid for å fjerne kravet om å fremvise registreringsbeviset ved innflytting, og erstattes av at Skatteetaten selv vurderer om personen oppfyller kravet til lovlig opphold.[70]

I møte med innvandringsavdelingen i JD det fremmet et ønske om å styrke EØS-registreringsprosessen med skjerpet kontroll, herunder med verifisering av eksisterende ID-bevis med biometri, uten at biometriske opplysninger opptas og lagres. Innvandringsavdelinger var likevel tydelige på at EØS-registreringsordningen i sin nåværende form innehar svært begrenset bruksverdi, og at ordningen bør styrkes dersom den skal videreføres.

Leverandøren bemerker at EU har vedtatt Europaparlaments- og rådsforordning (EU) 2019/1157 av 20. juni 2019 om økt sikkerhet i nasjonale ID-kort, registreringsbevis og oppholdskort til familiemedlemmer av EØS-borgere. Forordningen omhandler i hovedsak nasjonale ID-kort, men lister også hvilke informasjonselementer som skal fremkomme av registreringsbeviset i fremtiden. Forordningen omtaler opptak av fingeravtrykk i forbindelse med registreringsbeviset, men det er meget uklart for

[70] Oppgitt i e-post til leverandøren, andre halvår 2019

sentrale aktører i ID-forvaltningen og leverandøren hvilket handlingsrom dette faktisk gir.

Leverandørens vurdering av EØS-registreringsordningen

Det er leverandørens vurdering at opptak av biometri av EØS-borgere i forbindelse med EØS-registreringsordningen ikke er gjennomførbart i henhold til EØS-regelverket slik det praktiseres i dag. For å danne grunnlag for status «unik» i Folkeregisteret for EØS-borgere vil man derfor måtte se til andre muligheter enn EØS-registreringsordningen. Dette standpunktet underbygges av tidligere utredninger og dokumentasjon som leverandøren er forelagt, og av samtlige aktører som leverandøren har innhentet synspunkter fra. Leverandøren bemerker at forordning 2019/1157 potensielt kan åpne for økte kontrolltiltak i forbindelse med registreringsordningen i fremtiden. Leverandøren erfarer at JD anser formuleringen i forordningen som svært uklar, og at det p.t. foreligger betydelig usikkerhet rundt hvilken anvendelse forordningen vil ha. Leverandøren legger til grunn at JD vil se nærmere på innholdet i forordningen i det videre arbeidet.

Videre er det leverandørens vurdering at EØS-ordningen slik den gjennomføres i dag innehar svært begrenset bruksverdi. Det foreligger i dag et krav om å fremvise registreringsbeviset ved melding om innflytting hos Skatteetaten. Leverandøren vurderer likevel at det foreligger andre, og potensielt bedre måter å bevise lovlig opphold på, uten at det avkreves et oppmøte av bruker i forkant hos en annen aktør i forvaltningen. Det understrekes videre at det pågår et arbeid i Skatteetaten om å fjerne kravet til fremvisning av registreringsbeviset. Dette må også sees i sammenheng med vurderingene tilknyttet et felles skrankepunkt, jf. kapittel 4. Utover dagens krav fra Skatteetaten erfarer leverandøren at registreringsbeviset i liten til ingen grad kreves i andre prosesser i forvaltningen, og statistikkgrunnlaget som ordningen generer kan opptas på andre måter. Leverandøren stiller derfor spørsmål ved om ordningens årlige ressursbruk, samt krav til oppmøte og tidsbruk fra bruker, kan rettferdiggjøres med dagens formål med ordningen.

Flere aktører har påpekt at registreringsordningen potensielt kan styrkes for å gi større bruksverdi. Et tiltak er at kontrollen som gjennomføres i forbindelse med ordningen oppgraderes med utstyr for biometrisk kontroll. Tiltaket innebærer ikke at EØS-borger avgir biometri som del av registreringen, men åpner for at saksbehandler kan *kontrollere* søkers biometri opp mot biometrien som er elektronisk lagret i personens fremlagte ID-bevis gjennom såkalte en-til-en søk. Tiltaket kan også tenkes å åpne for at vedkommende registreres med status «kontrollert» i Folkeregisteret. Tjenesteeiere får dermed bedre forutsetninger for å kunne stille krav om «kontrollert» i henhold til sine sikkerhetsbehov.

Etter leverandørens vurdering vil også styrking av ID-kontrollen i EØS-registreringsordningen ha svært liten verdi. Dette skyldes blant annet at de aller fleste EØS-borgere som oppholder seg i Norge over tid vil bli kontrollert i forbindelse med søknad om skattekort eller melding om innflytting hos Skatteetaten. Videre vil ordningen fortsatt ikke treffe nordiske borgere, som er unntatt kravet om registering. Leverandøren bemerker også at det etter EØS-regelverket er svært begrenset hvilke ID-bevis som kan avkreves i forbindelse med registrering.

Overordnet vurderer leverandøren at EØS-registreringsordningen har liten nytteverdi i sin nåværende form, at ordningen påfører et unødig ressursbruk for forvaltningen samt tidsbruk for brukere, samt at noen verdiøkende oppgradering anses som lite realistisk.

2.5.2 Vurdering av gjenstående teknisk og juridisk tilrettelegging for «unik»

Følgende delkapittel tar for seg hva som gjenstår av teknisk og juridisk tilrettelegging for å få registrert personer som «unike» i Folkeregisteret, jf. oppdragets mandat. Kapittelet baserer seg på dialog med relevante aktører og dokumentasjon forelagt leverandøren.[71] Kapittelet er videre basert på et arbeidsmøte med KoID (SKD, POD, UDI og Difi) 18.10.2019, med påfølgende referat som aktørene utarbeidet i samarbeid med leverandøren.

Beskrivelse av pågående prosjekter og synspunkter tilknyttet registergrunnlag for status «unik»

JD gjorde i 2016 en forstudie i samarbeid med FIN, ASD og KMD om muligheten for å gjøre en knytning mellom Folkeregisteret og biometriregistrene i justissektoren for å styrke kvaliteten på opplysningene i Folkeregisteret og sørge for at det aktuelle fødsels- eller d-nummer kun er knyttet til en person, benevnt som "unik". Dette dannet bakgrunn for et felles oppdragsbrev til POD, UDI og SKD 07.12.2016.[72] Oppdraget hadde sammenheng med flere andre prosjekter som pågikk på den tiden (og som fremdeles pågår), herunder Modernisering av Folkeregisteret (SKD), ABIS[73] (POD), Nye pass og ID-kort (POD), nasjonalt ID-kort til utlendinger (POD), IKT-modernisering og økt biometriopptak i utlendingssaker (UDI i samarbeid med POD og UD) og anskaffelse av biometriopptaksutstyr (POD). Det gjengis følgende status for et utvalg av aktiviteter i prosjektene:

- Folkeregisteret vil være klare til å ta imot informasjon om «unik» fra 2020 og vil tilby dette som tjeneste til brukerne av Folkeregisteret når alle med rettigheter og plikter i landet gis mulighet til å bli «unike»

- ABIS-passregisterdelen vil for passregisteret være klare til å overføre historiske data fra våren 2020 og nye forekomster når nytt saksbehandlingssystem for pass tas i bruk, etter planen skal Politidirektoratet/Kripos lansere dette i løpet av 2020

- ABIS-ID-kortregisterdelen vil være klare til å overføre opplysninger fra nasjonalt ID-kort register når saksbehandlingssystemet tas i bruk, etter planen skal Politidirektoratet/Kripos lansere dette i løpet av 2020

- ABIS-Utlendingsregisterdelen vil være klare til å overføre opplysninger når utvidet opptak av biometri starter opp. Det foreligger avhengigheter til tilpasninger som utføres av ATT-prosjektet[74]. Trolig vil utvidet opptak av biometri starte juni 2020

- Nye pass og ID-kort er det prosjektet som blant annet skal sørge for saksbehandlingssystem og prosess for økt kvalitet i ID-kontrollen og ensartet krav til informasjonssikkerhet i alle prosesser som støtter opp under utstedelse av pass og nasjonale ID-kort (skrankepunkter, IKT-systemer, leverandører, PIT mv). Etter planen skal Politidirektoratet lansere dette i løpet av 2020

- Anskaffelse av biometriopptaksutstyr for politidistriktene (pass- og ID-myndigheten samt utlendingsforvaltningen) ble ferdigstilt i 2019

[71] Relevante kilder: *JD/FIN/KMD/ASD, «Knytning mellom Folkeregisteret og biometri i Passregisteret, Nasjonalt ID-kortregister og Utlendingsregisteret», 14.06.2016; POD, «UNIK», 07.07.2017; JD, «Høring om forslag til endringer i utlendingsloven m.m. om opptak og lagring av biometri i utlendingssaker», 15. juli 2019*
[72] JD, «Nærmere undersøkelse av knytning Folkeregisteret-biometriregistrene i justissektoren», 07.12.2016
[73] Automated Biometric Identification System (ABIS). Prosjektet henviser til tekniske tilpasninger for å muliggjøre søk på tvers av flere biometriregistre
[74] *ABIS Tilpasning av Tjenester* (ATT)

- Nasjonalt ID-kort til utlendinger anses som ferdig utredet av Politidirektoratet og forslag ble sendt JD oktober 2018

Det foreligger en uenighet mellom POD og UDI hvorvidt «unik» skal dannes på grunnlag av to eller tre registre. Dersom det besluttes at alle utlendinger med en tilknytning til riket (vurdert av leverandøren i kapittel 2.2.3) skal få nasjonalt ID-kort kan overføring av "unik"-status for utenlandske borgere skje på bakgrunn av registrering i kun to registre (passregisteret og ID-kortregisteret). Alternativt kan også overføring av status «unik» skje på bakgrunn en registering i utlendingsregisteret i forbindelse med søknad om oppholdstillatelse. Basert på samtaler og forelagt informasjon fremstår det fra leverandørens ståsted at enkelte i POD fremholder at det heller ikke bør søkes på tvers av alle tre registre ved søknad om pass eller nasjonalt ID-kort. Posisjonen står i motsetning til oppfatningen fra andre miljøer i POD, UDI, JD og ASD.

Enkelte miljøer i Politidirektoratet har uttrykt bekymring for at registrering i utlendingsregisteret (utover registering i pass- og ID-kortregistrene) også skal kunne danne grunnlag for status «unik». Dette skyldes delvis en oppfatning av at tre registre vil medføre at det er to ulike juridiske formål (Pass- og ID-kortutstedelse og registrering av utlendingers opphold, herunder avklaring av identitet) som ligger til grunn for et nytt avledet formål ("unik"). Det fremholdes at det innebærer at det vil være ulik kvalitet, prosesser, regelverk og til dels utstyr. POD poengterer videre at det da vil være to virksomheter som følger opp internkontroll og virksomhetsstyring (POD for pass- og ID-kortmyndigheten, og UDI for oppholdssaker, asylsaker og visumsaker).

UDI er uenige av oppfatningen som fremstilles over. UDI fremholder at kvaliteten på biometriopptakene i utlendingsforvaltningen vil være lik som biometriopptak for pass og nasjonale ID-kort. UDI poengterer at opptakene som gjøres i utlendingsforvaltningen skal benyttes i oppholdskort, reisebevis og utlendingspass, som har samme krav til innhold som de ordinære passene og fremtidige nasjonale ID-kort. UDI påpeker at utstyr som benyttes ved opptak i Norge er likt, og der det benyttes annet utstyr skal dette imøtekomme kravene nevnt over.

UDI ser heller ikke at det har noen betydning for spørsmålet om benyttelse av to eller tre registre om formålet som ligger til grunn for opptak av biometrien er ulikt. Det poengteres at formålet for opptak av biometri i utlendingssaker er identifisering og senere verifisering av identitet, i tillegg til saksopprettelse. Samtidig understrekes det at det også i passloven er ulike formål, jf. passloven § 8a. UDI fremholder at det uansett løsning er forutsetning at det foreligger tilstrekkelig hjemmel for å kunne overføre opplysninger om «unik» til Folkeregisteret.

UDI mener derfor at det bør utredes nærmere mellom hvordan «unik» skal etableres, og at det i denne vurderingen også bør tas hensyn til hva «unik» skal benyttes til og hvilke rettigheter og plikter som knyttes til statusen. UDI mener videre det også må vurderes hvordan forvaltningen kan sikre rask tilgang til statusen «unik» for publikum i Norge.

Aktørene har videre gitt uttrykk for at ettersom det er SKD som vil bli eier av "unik" og skal innestå for videreformidling av informasjonen, bør det være SKD som tar beslutning om de ønsker opplysningene kun basert på utstedelse av norske pass og nasjonale ID-kort, eller også fra registreringer i utlendingsregisteret.

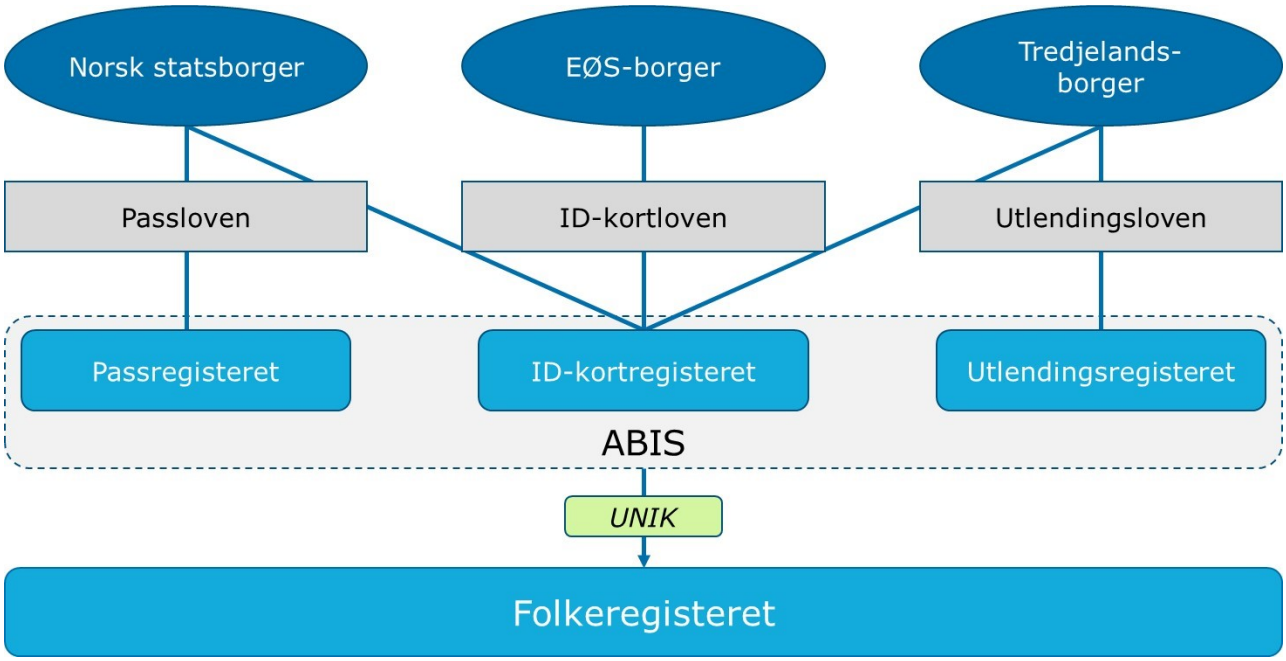
<u>Leverandørens vurdering av registergrunnlag for «unik»</u>

Leverandøren påpeker at det er viktig å avklare hvorvidt det er en forutsetning for «unik» at vedkommende har fått utstedt pass eller nasjonalt ID-kort, eller om status «unik» også skal baseres på registrering i utlendingsregisteret. Dette er den viktigste beslutningen som må gjøres for å komme videre med «unik».

Leverandørens vurdering er at det uansett registergrunnlag for «unik» skal legges til grunn et premiss om at det skal kontrolleres for «unik» på tvers av alle tre registrene i søknadsprosessene. Dette for å forhindre at en person kan operere med en identitet i utlendingsregisteret og en annen identitet i pass- eller ID-kortregisteret.

Leverandøren ser at det av flere årsaker kan virke forenklende å begrense grunnlaget for status «unik» til registrering kun i pass- og ID-kortregisteret. For utenlandske borgere vil det innebære et 1:1 forhold mellom utstedte nasjonale ID-kort og status «unik». Internkontroll og virksomhetsstyring kan begrenses til POD. Det vil også minimere forskjeller i prosessen for biometriopptak, og de forskjeller som eventuelt foreligger i utstyr for biometriopptak.

Samtidig har ikke leverandøren sett dokumentasjon eller undersøkelser som tilsier at biometriske opplysninger i utlendingsregisteret skal være av vesentlig lavere kvalitet enn i pass- og ID-kortregisteret. Leverandøren oppfatter heller ikke at det foreligger forskjeller av betydning i utstyret som benyttes for opptak av biometri i utlendingsforvaltningen og til pass- og ID-kort. De forskjeller som eventuelt eksisterer bør etter leverandørens syn kunne håndteres på andre måter, og vil også i stor grad kunne adresseres av leverandørens vurderinger knyttet til et felles skrankepunkt. Uavhengig av det foregående ser leverandøren flere fordeler ved å åpne for å benytte registrering i utlendingsregisteret til status «unik». Primært anses det som en styrke at det vil bidra til å øke andelen av status «unik» i Folkeregisteret, uavhengig av utbredelsen på det nasjonale ID-kortet. Leverandøren påpeker her at status «unik» vil kunne inneha verdi selv uten at vedkommende innehar et nasjonalt ID-kort. Videre vil det kunne bidra til at tredjelandsborgere oppnår status «unik» raskere, og vil også åpne for at både tjenesteeiere og brukere kan nyttiggjøre seg informasjonsverdien i status «unik» uten å være bundet til nasjonalt ID-kort. Samlet sett ser leverandøren størst fordeler ved at registergrunnlaget for «unik» består av pass-, ID-kort og utlendingsregisteret, forutsatt at det uansett skal gjennomføres en-til-mange søk på tvers av alle tre registrene i søknadsprosessene.



Figur 4 Samspillet mellom brukergrupper, mulige biometriregistre og status «unik» i Folkeregisteret – hentet fra Forstudiet gjennomført av JD med flere i 2016

Vurdering av juridisk tilrettelegging

Av juridisk tilrettelegging gjenstår det å etablere hjemmelsgrunnlaget for søk på tvers mellom pass- og ID-kortregisteret og utlendingsregisteret. Et forslag til endringer i utlendingsforskriften, som har vært på høring, foreslår blant annet at utlendingsmyndigheten i forbindelse med behandling av søknader etter utlendingsloven vil kunne gjennomføre en-til-mange søk i pass- og ID-kortregisteret.[75] Tilsvarende hjemler vil også måtte innlemmes i passloven og ID-kortloven. Leverandøren påpeker videre at det vil være viktig å avklare tilbudet om nasjonalt ID-kort til utlendinger for å fastslå omfanget av hvilke brukergrupper som vil kunne oppnå status «unik». Nødvendig forskriftsarbeid gjenstår på dette punktet.

Utover muligheten til å søke på tvers i ulike registre er det per i dag forskjellige reguleringer i henholdsvis passloven, ID-kortloven og utlendingsloven med tilhørende forskrifter rundt prosesser og rutiner for opptak av biometri og til hvilket formål biometriske opplysninger skal opptas. Skatteetaten uttaler at nevnte regelverk vil måtte reflektere et konkret formål om å danne grunnlag for «unik» identitet i Folkeregisteret. Hvilke lovverk som vil måtte endres må ses i sammenheng med hvilke registre som eventuelt vil ligge til grunn for «unik». Dersom det skal stilles visse krav til prosess, kvalitet og sikkerhet i biometriopptak vil dette følgelig også måtte fremkomme tydelig fra de respektive lovtekstene.

Det gjenstår også å gjennomføre tilhørende forskriftsarbeid fra folkeregistermyndigheten. Per dags dato avventes dette arbeidet i påvente av avklaringer knyttet til hvilke biometriregistre som vil ligge til grunn for status «unik». Forskriftsarbeidet er anslått til å ta maksimalt seks måneder å ferdigstille.

Vurdering av teknisk tilrettelegging

Av teknisk tilrettelegging er det primært politiets arbeid med nødvendige tilpasninger for å kunne foreta biometrisøk på tvers i ABIS som gjenstår.

Det pågår videre et arbeid med å etablere en teknisk løsning for en-til-mange søk i pass- og ID-kort registeret. En-til-mange søk er utviklet og testet for utlendingsforvaltningen, og vil bli satt i produksjon i løpet av 2020. For å muliggjøre en-til-mange søk av høy kvalitet må eksisterende biometridatabaser også «vaskes» forut for innlemmelse i ABIS. UDI gjennomførte «vask» av historiske foto i 2017-2018. POD har igangsatt det tekniske arbeidet med «vask» av eksisterende biometridatabaser. Arbeidet estimeres ferdigstilt i første kvartal 2020. Øvrige tekniske tilpasninger i ABIS vil være klart høsten 2020 til utstedelse av nasjonalt ID-kort.

Selve grensesnittet mellom justissektoren hvor «unik» genereres og Folkeregisteret anses å være relativt uproblematisk. Skatteetaten har tidligere estimert kostnaden til om lag 10 mill. kroner og har oppgitt at grensesnittet kan implementeres på vesentlig kortere tid enn seks måneder. Skatteetaten opplyser at estimatene forutsetter at det settes av tilstrekkelig tid og ressurser til arbeidet, samt at den estimerte kostnaden for grensesnittet ikke ligger innenfor kostnadsrammen til prosjekt modernisert Folkeregister.

POD opplyser at kostnader og ytterligere teknisk og manuell tilrettelegging som påløper i justissektoren vil avhenge av tilbudet til nasjonalt ID-kort og prosesser som må gjennomføres med henhold til kontroll mot registrering i utlendingsregisteret. Det opplyses at tilhørende arbeidsbelastning avhenger blant annet av kvaliteten på biometriopptakene og algoritmenes egnethet. Hvor krevende et søk på tvers av tre

[75] JD, «Høring om forslag til endringer i utlendingsloven m.m. om opptak og lagring av biometri i utlendingssaker», 15. juli 2019 (s. 7)

biometriregistre blir trengs det erfaring fra før det kan estimeres behov for manuelle kontrollprosesser hos Kripos (3.linje). POD har ikke beregnet kostnaden eller tidsestimat for å utarbeide et grensesnitt mot Folkeregisteret.

Det foreligger uklarheter knyttet til hvordan det skal tilrettelegges for «unik» i Folkeregisteret for barn. Det er vanskelig å oppta biometriske opplysninger av for eksempel spebarn. Videre er det utfordrende at personers biometriske opplysninger endrer seg over tid i ung alder, noe som kan påvirke treffsikkerheten i algoritmene for ansiktsgjenkjenning. Det er spesielt Difi som har fremhevet denne problematikken. Videre tekniske tilrettelegging for «unik» må ta høyde for denne problematikken.

2.5.3 Konsekvenser for «unik» av å ikke stille krav om norsk pass eller nasjonalt ID-kort for EØS-borgere

Utenlandske ID-bevis kan i dag benyttes som legitimasjonsformål i en rekke situasjoner. For eksempel kan en tysk statsborger benytte sitt tyske pass eller sitt tyske nasjonale ID-kort som gyldig legitimasjon ved ID-kontroll hos Skatteetaten.

Leverandøren er også kjent med nye forordninger som legger føringer for å styrke sikkerheten til identitetskort til unionsborgere.[76] Forordningen har til hensikt å innføre felles standarder for nasjonale ID-kort på tvers av EU, og på den måten bekjempe kriminalitet i EU/EØS området. Blant annet tilsier forordningen at alle nasjonale ID-kort utstedt av et medlemsland må inneholde maskinlesbar biometriske opplysninger.

Videre viser leverandøren til delkapittel 2.3.4 angående muligheten til å stille krav om nasjonalt ID-kort utstedt av norske myndigheter for tilgang til tjenester og ytelser i Norge. Leverandøren poengterer at det inntil videre er uavklart hvorvidt et slikt krav vil være i strid med prinsippene om fri bevegelighet og ikke-diskriminering.

I lys av dette anser leverandøren det som nødvendig å forklare hvilke implikasjoner det vil kunne ha dersom det ikke vil være mulig å stille krav til EØS-borgere om å inneha et nasjonalt ID-kort utstedt av norske myndigheter for å få tilgang til tjenester og ytelser i Norge. Leverandøren legger frem enkelte muligheter og utfordringer under.

<u>Muligheter:</u>

Etter forordning 2019/1157 vil alle europeiske nasjonale ID-kort på sikt måtte inneha funksjonalitet for å lagre ansiktsfoto og fingeravtrykk i ID-kortet. I så måte vil ID-kortene kunne benyttes til en en-til-en sammenligning ved eksempelvis opprettelse av identitetsnummer ved oppmøte i Norge, samt andre kontrollsammenhenger. En utenlandsk borger kan kobles til et norsk identitetsnummer ved at vedkommende sitt utenlandske identitetsnummer/dokumentnummer lagres i Folkeregisteret. Vedkommende sitt eierskap til det norske identitetsnummeret kan i teorien dermed verifiseres ved fremvisning/kontroll av personens utenlandske nasjonale ID-kort.

<u>Utfordringer:</u>

Leverandøren anser det som en klar ulempe at et slikt scenario vil innebære at det i meget begrenset grad vil opptas og lagres biometriske opplysninger av EØS-borgere med tilknytning til Norge. Kun EØS-borgere som velger å anskaffe et nasjonalt ID-kort utstedt av norske myndigheter, til tross for at de kan benytte pass eller nasjonalt ID-kort fra sitt hjemland, vil oppnå status «unik». Dette vil i stor grad undergrave visjonen om «én person, én identitet i Norge», og vil i praksis innebære at det ikke vil være

[76] Europaparlaments- og rådsforordning (EU) 2019/1157 av 20. juni 2019

mulig å oppnå status «unik» for EØS-borgere. Gitt at det ikke oppnås status «unik» for denne brukergruppen vil, etter leverandørens vurdering, den reelle verdien av status «unik» som konsept være betydelig svekket. Det skyldes at eventuelle krav om «unik» vil være mer krevende å stille. Verdien av biometrisøk som skal foretas på tvers av de tre biometriregistrene vil også begrenses, da biometrien tilknyttet et stort antall norske identitetsnummer vil falle utenfor.

3 Elektronisk ID (eID)

I dette kapittelet vurderer leverandøren dagens eID-løsninger som benyttes for tilgang til offentlige tjenester og ytelser, og vurderer alternative løsninger for det offentlige for økt sikkerhet, brukervennlighet og ressurseffektivitet ved digital autentisering gjennom eID-er. Kapittelet er utarbeidet i henhold til tema 2 i mandatet for tilleggsoppdraget, nærmere beskrevet i kapittel 1.1.

Hovedrapporten redegjorde for bruk av eID-er for tilgang til offentlige tjenester og ytelser, inkludert omfanget av digital autentisering med eID i dag og tilknyttet ressursbruk, samt en oversikt over pågående arbeid med nasjonal eID tilknyttet nasjonalt ID-kort. Videre drøftet hovedrapporten utfordringer ved dagens eID-løsninger og alternative forbedringer og løsninger til utfordringer ved eksisterende private eID-er og nåværende plan for nasjonal eID.

På enkelte områder vil det være grad av gjentagelse fra hovedrapporten, og leverandøren viser spesielt til kapittel 2.8.2 og 2.9.2 i hovedrapporten for nåsituasjonsbeskrivelse og pågående arbeid med eID, kapittel 7.1.3 for ressursbruk tilknyttet ID-porten og dagens eID-er, kapittel 11 for vurdering av alternativ knyttet til eID, samt kapittel 16.1.3 for anbefalingen om å styrke arbeidet med eID. Kapittel 3.1 er komplettert med ytterligere relevant bakgrunn for tilleggsoppdraget. Tilleggsrapportens mandat vektlegger offentlige digitale tjenester og ytelser, men i beskrivelsen av misbruk av eID beskriver leverandøren også omfanget i digitale tjenester i privat sektor.

I hovedrapporten anbefalte leverandøren å tydeliggjøre at norsk pass og nasjonalt ID-kort er gyldige fysiske ID-bevis, samt å stille krav til norsk pass eller nasjonalt ID-kort for tilgang til offentlige tjenester og ytelser. Leverandøren anser det som et grunnleggende prinsipp at sikkerheten ved tilgang til offentlige tjenester og ytelser må være like god ved fysiske ID-bevis og eID, for å sikre at ikke en av «veiene» blir mer utsatt for misbruk. Dette er lagt til grunn i alle vurderingene tilknyttet eID.

Figur 5 Tilsvarende sikkerhet for tilgang til offentlige tjenester og ytelser med fysiske ID-bevis og eID

Majoriteten av beskrivelsene av utfordringer og alternative løsninger i kapittel 3.3 - 3.6 er gjort med utgangspunkt at det eksisterer etablerte private eID-er og at nasjonal eID vil bli utstedt som et supplement til markedet, hvor brukerne i stort vil ha et valg om hvilken eID-løsning de ønsker å benytte for å identifisere seg digitalt til offentlige tjenester.

I vurderingen av sikkerhet for alternative løsninger til dagens eID-tilnærming i kapittel 3.5 og alternativ for nasjonal eID i kapittel 3.6 vurderer leverandøren effekten av de ulike alternativene på sikkerhet ved utstedelse av eID-er, ved bruk av eID-er og effekten på samfunnssikkerheten samlet sett. For vurdering av effekten på brukervennlighet ved de ulike alternativene er det brukeren av eID-en og dens opplevelse av løsningen som er i fokus, samt brukers ressursbruk ved utstedelse og bruk av løsningen. Brukers opplevde sikkerhet ved utstedelse og bruk av eID-er er

inkludert i vurderingen av sikkerhet beskrevet over. Ressursbruken som de ulike alternative løsningene medfører vurderes ut fra effekten på det offentliges samlede ressursbruk, samt private aktørers ressursbruk.

3.1 Bakgrunn

3.1.1 Dagens eID-løsninger og ID-porten

Slik beskrevet i hovedrapporten kapittel 2.8.2 har det over lengre tid vært tilrettelagt for løsninger for elektronisk autentisering både i offentlig og privat sektor i Norge. Siden 2010 har det i rundskriv fra KMD blitt stilt krav til tjenesteeiere om å benytte ID-porten som løsning for offentlige digitale tjenester som krever innlogging og autentisering med eID. Dagens eID-løsninger for elektronisk autentisering til offentlige digitale tjenester er i stor grad private. Gjennom ID-porten kan brukere i dag benytte en rekke eID-er for autentisering mot det offentlige: MinID (lansert 2008), Buypass (2010), Commfides (2011), BankID (2012) og BankID på mobil (2015). BankID og BankID på mobil benytter i utgangspunktet ulike infrastrukturer, men begge forutsetter bankforhold og beskrives kombinert videre i kapittel 3. Difi har ansvaret for ID-porten, samt utstedelse og drift av den offentlige eID-en MinID[77]. eID-løsninger som benyttes i ansattforhold innen eksempelvis helse- og utdanningssektoren er ikke en del av omfanget i mandatet for tilleggsrapporten og vurderes dermed ikke.

eID-er som brukes for autentisering til offentlig digitale tjenester i Norge er klassifisert etter fire ulike sikkerhetsnivåer, slik beskrevet i hovedrapporten kapittel 2.8.2, der de ulike sikkerhetsnivåene gir tilgang til ulike offentlige digitale tjenester. Den offentlige eID-en MinID gir tilgang til tjenester som krever sikkerhetsnivå 3, mens de private eID-ene fra BankID, Buypass og Commfides alle gir tilgang til tjenester på sikkerhetsnivå 4. I sammenheng med innføring av eIDAS-forordningen, gjennom lov om elektroniske tillitstjenester og tilhørende forskrifter, er begrepsbruken for de ulike sikkerhetsnivåene under utvikling, slik beskrevet i hovedrapporten kapittel 2.8.2. Tabellen under viser antallet offentlige digitale tjenester som er tilgjengelig gjennom ID-porten, samt andelen som krever autentisering med henholdsvis sikkerhetsnivå 3 og 4. Tabellene indikerer at befolkningen velger autentiseringsmekanismer med nivå 4, selv om kravet i mange tilfeller er nivå 3.

Innlogginger i ID-porten	Totalt	Andel innlogginger på sikkerhetsnivå 3	Andel innlogginger på sikkerhetsnivå 4
Innlogginger i ID-porten (totalt i 2018)	139,4 mill.[78]	16 prosent	84 prosent

Tabell 5 Antall innlogginger i ID-porten i 2018[79]

Tjenester i ID-porten	Totalt	Andel med krav til sikkerhetsnivå 3	Andel med krav til sikkerhetsnivå 4
Antall tilgjengelige tjenester i ID-porten (ved utgangen av 2018)	2 496[80]	79 prosent	21 prosent

Tabell 6 Offentlig digitale tjenester i ID-porten[81]

[77] Basert på samtaler med representanter i Difi, første halvår 2019
[78] Difi.no, «Nøkkeltall og statistikk – Fellesløsninger», 2019
[79] Basert på data mottatt fra Difi, andre halvår 2019
[80] Difi.no, «Nøkkeltall og statistikk – Fellesløsninger», 2019
[81] Basert på data mottatt fra Difi, andre halvår 2019

Tabellene over viser totalt antall innlogginger i ID-porten i 2018, samt antall tilgjengelige tjenester i ID-porten ved utgangen av 2018. I løpet av 2019 har antall innlogginger i ID-porten økt sammenlignet med 2018, og det er per oktober 2019 gjennomført over 147 mill. påloggінger i ID-porten. Tilsvarende har antall tilgjengelige tjenester i ID-porten økt til 4 126 per oktober 2019.[82]

Det kreves personlig oppmøte og ID-kontroll av bruker ved utstedelse av eID-er med sikkerhetsnivå 4. Oppmøte og ID-kontroll av bruker for utstedelse av eID på sikkerhetsnivå 4 gjennomføres i dag ved bankfilialer, postkontor og post i butikk. Det finnes omtrent 2 340 oppmøtesteder for utstedelse av eID, hvorav 940[83] bankfilialer og 1 400[84] postkontor eller post i butikk. Ved postkontor og post i butikk benytter utstedere av private eID-er seg av PUM[85]-tjenesten, som er en tjeneste for personlig utlevering og dokumentasjon av mottakers identitet.[86] Hensikten med det personlige oppmøtet er å sikre at eID-en blir utlevert til rettmessig eier. For eID-er med sikkerhetsnivå 3 er det ikke krav til personlig oppmøte eller ID-kontroll av bruker ved utstedelse.[87]

3.1.2 Overordnet beskrivelse av utstedelsesprosessen for dagens eID-er

Utstedelse av MinID

Den offentlige eID-en MinID kan bestilles av alle som har et fødselsnummer eller d-nummer, og både utstedelsen og bruk av MinID er gratis for bruker og kostnadene dekkes over statsbudsjettet. For å registrere en MinID må brukeren først bestille PIN-kodebrev som blir sendt til folkeregistrert adresse. Etter at brukeren har mottatt PIN-kodebrevet kan MinID opprettes ved bruk av koder fra PIN-kodebrevet, og brukeren velger deretter selv et passord som skal benyttes ved innlogging med MinID.

Utstedelse av BankID

BankID eies av Vipps AS, men utstedes av banken brukeren har et bankforhold med. Bankene utsteder en BankID kodebrikke til bruker, og bruker kan deretter autentisere seg digitalt med denne for å få utstedt BankID på mobil. Ved utstedelse kreves personlig oppmøte og ID-kontroll av brukerens pass. For banker med filialer kan brukeren møte opp i filial for ID-kontroll, mens banker som ikke har filialer benytter seg av ID-kontroll ved et postkontor eller post i butikk gjennom Postens PUM-tjeneste. Det er gratis for bruker å få utstedt BankID og brukeren blir i utgangspunktet ikke belastet for å bruke BankID til sikker digital autentisering. Telenor[88] belaster alle sine kunder for bruk av BankID på mobil med 0,49 kroner per autentisering, mens Telia[89] kun belaster sine bedriftskunder for bruk av BankID på mobil tilsvarende. Bruk av BankID med kodebrikke er derimot gratis for alle brukere.

Siden 1. mars 2007 har det i BankID-reglene (nå forvaltet av Bits AS) vært krav til fremvisning av pass ved utstedelse av BankID. I reglene stilles det ikke krav til etterkontroll med pass av kunder som fikk utstedt BankID før 1. mars 2007. Enkelte banker vil, som en del av arbeidet mot hvitvasking, likevel kreve at kunder som har fått utstedt BankID før 1. mars 2007 og ikke har legitimert seg med pass, møter opp i

[82] Difi.no, «Nøkkeltall og statistikk – Fellesløsninger», 2019
[83] Finansnorge.no, «Antall ekspedisjonssteder», 2017
[84] Postennorge.no, «Fakta om konsernet», 2019
[85] PUM er forkortelse for «personlig utlevering mottakingsbevis»
[86] Bring.no, «Personlig utlevering mottakingsbevis (PUM)», u.å.
[87] Difi, «Sikkerhet og informasjonskapsler – Ulike sikkerhetsnivå», 2019
[88] Telenor.no, «BankID – Priser for bruk av BankID på mobil», u.å.
[89] Telia.no, «Prisinformasjon – Telefoni og mobil», u.å.

en bankfilial for gjennomføring av en ID-kontroll med pass.[90] Enkelte banker har utstyrt filialene sine med Keesing-maskiner for å sjekke ektheten til fremvist pass. Postkontorer og post i butikk har også tilsvarende maskiner for ekthetssjekk av pass.

Utstedelse av Buypass

Buypass AS utsteder eID-er til både privatpersoner og til bedrifter/ansatte. I helsevesenet utsteder virksomhetene selv tilpassede Buypass-løsninger på sikkerhetsnivå 4 til ansatte som har behov for en slik løsning. Som i hovedrapporten fokuserer leverandøren også i tilleggsrapporten på eID-er utstedt til privatpersoner. Buypass tilbyr to løsninger til privatkunder, «Buypass ID på smartkort» og «Buypass ID i mobil». Buypass ID på smartkort koster brukeren 669 kroner ved utstedelse og har en gyldighet på tre år. Dersom kunden trenger en smartkortleser koster dette 100 kroner. Buypass ID i mobil koster brukeren 298 kroner ved utstedelse og har i praksis evig gyldighet ettersom eID-en fornyes ved jevnlig bruk. Begge løsningene bestilles på nett og utleveres gjennom PUM-tjeneste ved postkontor eller post i butikk, der den obligatoriske ID-kontrollen ved oppmøte gjennomføres.

Tabellen under viser en oversikt over godkjente fysiske ID-bevis som kan fremvises ved oppmøte og ID-kontroll for utstedelse av BankID og Buypass.

	BankID[91]	Buypass[92]
Godkjente fysiske ID-bevis ved utstedelse	- Norsk pass - Utenlandsk pass - *«Andre dokumenter som etter en konkret risikobasert vurdering anses som gyldig legitimasjon med samme sikkerhetsnivå som norsk pass»*	- Norsk pass - Utenlandsk pass - Norsk utlendingspass og reisebevis - Norsk bankkort med legitimasjonsdel (bilde m.m.) - Norsk førerkort utstedt fra og med 01.01.1998 - Postens ID-kort - Europeiske identitetskort (Identity Card)

Tabell 7 Godkjente fysiske ID-bevis for utstedelse av BankID og Buypass

3.1.3 Nasjonal eID

Nasjonal eID tilknyttet det nasjonale ID-kortet er beskrevet i kapittel 11.2.1 i hovedrapporten. Utstedelsen av nasjonal eID vil følge utstedeselsprosessen for pass og nasjonalt ID-kort, med ID-kontroll og opptak og kontroll av biometri ved et pass- og ID-kontor. Det vil gjennomføres ekthets- og tapskontroll av fremvist ID-bevis, en-til-en biometrikontroll mellom brukeren som møter opp og fremvist ID-bevis, samt en-til-mange søk av brukers biometri. Utstedelsesprosessen vil sikre status «unik» for alle som får utstedt nasjonal eID og dermed forhindre at en person får utstedt nasjonal eID i andre identiteter, samt at det ikke utstedes nasjonal eID til fiktive personer. Planer og rammer for Nasjonal eID ble lagt i 2007.[93] Planene ble konkretisert i 2010-2011, finansiert av Stortinget i 2013 og vedtatt av regjeringen etter behovsundersøkelse blant offentlige tjenesteeiere, private tjenesteeiere, eID-er i markedet og sluttbrukere i 2016[94].

[90] Finansnorge.no, «BankID og kontroll av pass», 18.01.2019
[91] Bits, «Regler om BankID», 2018
[92] Buypass.no, «Buypass ID på smartkort – Legitimasjonskontroll på Posten», u.å. og Posten.no, «Legitimasjon og fullmakter – Dokumenter som er godkjent som legitimasjon», u.å.
[93] JD, «Sluttrapport – Nasjonalt ID-kort», 2007
[94] POD og Difi, «Beslutningsgrunnlag for eID på nasjonalt ID-kort», 2016

POD beskriver at Nasjonal eID består av flere sammensatte tjenester i politiet, som er lagt sammen med pass og ID-kort og på den måten får synergieffekter av hverandre. Blant annet utnyttes felles miljø for sertifikatinfrastruktur som er kjernen i eID-myndighetsutøvelsen sammen med utstedelsesprosessen for pass og nasjonalt ID-kort. POD informerer videre at andre tjenester som muliggjør nasjonal eID er status og oppslagstjenester, autentiserings- og signeringstjeneste, publikumstjeneste og brukerstøtte. I tillegg kommer produksjonstjenesten som er felles for pass og ID-kort. Det hele er en del av en anskaffelse i markedet.

Nasjonal eID skal utstedes sammen med det nasjonale ID-kortet til norske borgere over 13 år, og vil ha en gyldighet på fem år. Brukere kan ved utstedelse velge om de ønsker å reservere seg mot nasjonal eID, og følgelig få utstedt et nasjonalt ID-kort uten nasjonal eID. Nasjonal eID skal finansieres av brukeren gjennom utstedelsesgebyret for nasjonalt ID-kort. Utstedelsesgebyret for nasjonalt ID-kort er i PODs gebyrmodell satt til 570 kroner, og brukere som reserverer seg mot nasjonal eID vil ikke få fratrekk i gebyret. I gebyrmodellen er det lagt opp til at omtrent 70 kroner av gebyret til nasjonal ID-kort går til dekning av kostnader for nasjonal eID. Årlige investeringskostnader til nasjonal eID er i gebyrmodellen omtrent 7 mill. kroner, mens årlige forvaltningskostnader til nasjonal eID er omtrent 12 mill. kroner. Leverandøren er gjort kjent med at det per november 2019 har påløpt omtrent 28 mill. kroner i investeringskostnader tilknyttet nasjonal eID, og at samlede planlagte investeringskostnader til nasjonal eID beløper seg til omtrent 82 mill. kroner. Nasjonal eID skal etter utstedelse være gratis i bruk både for brukeren og tjenesteeierne, og gebyret vil dekke alle kostnader tilknyttet utstedelse og bruk av nasjonal eID.

Nasjonalt ID-kort planlegges utstedt også til utlendinger og det pågår utredninger om hvilke utenlandske borgere som skal få tilbud om nasjonalt ID-kort. Det pågår også utredninger om hvorvidt det nasjonale ID-kortet til utlendinger skal ha en nasjonal eID tilknyttet, og et viktig aspekt er hvorvidt dette kommer i konflikt med eIDAS-reguleringen.

Nasjonal eID skal kunne levere funksjonalitet for autentisering og signering. I nåværende planlagt versjon vil nasjonal eID ha tofaktor-autentisering med PIN-kode og passord, tilsvarende eksisterende eID-er på sikkerhetsnivå 4. Ifølge POD vurderes det om sikkerhetsfunksjonaliteten skal utvides for å muliggjøre trefaktor-autentisering med sjekk av biometriske opplysninger som er lagret i det nasjonale ID-kortet opp mot bruker av den nasjonale eID-en. POD vurderer at dette vil åpne for nye bruksområder og dekke det totale risikobildet ved å tilby en-til-en biometrisk kontroll. POD anser at nasjonal eID med trefaktor-autentisering i så fall vil kunne anvendes både i digitale tjenester og ved fysisk skrankepunkt.

3.1.4 ID-kontroll ved bruk og fornyelse av dagens eID-er

Dagens eID-er kan etter fullført utstedelse benyttes til digital autentisering for tilgang til offentlige og private tjenester. Hver gang en eID på sikkerhetsnivå 4 benyttes gjennomføres det en kontroll i form av en tofaktor-autentisering bestående av noe brukeren vet (PIN-kode eller passord) og noe brukeren har (kodebrikke, smartkort, BankID på mobil etc.). Utover denne kontrollen gjennomføres det ingen ytterligere fysisk ID-kontroll av brukeren, og fornyelser av dagens eID-er bygger dermed kun på ett historisk fysisk oppmøte. BankID har en gyldighet på to år, men fornyes automatisk ved jevnlig bruk og har i praksis evig gyldighet. Buypass ID i mobil er gyldig i tre år og fornyes automatisk ved jevnlig bruk slik som BankID og har dermed i praksis evig gyldighet. Buypass ID på smartkort har en gyldighet på tre år før det må fornyes. Smartkortet kan fornyes via Buypass sine nettsider og sendes i posten, hvilket betyr at

det ikke gjennomføres noen ID-kontroll ved fornyelse av smartkortet og løsningen har dermed i praksis evig gyldighet. MinID er etter utstedelse gyldig til evig tid.

3.1.5 Beskrivelse av løsninger med funksjonalitet for sjekk av biometriske trekk

Det pågår arbeid både i offentlig og privat sektor med å utvikle og utrede løsninger med funksjonalitet for sjekk av biometriske trekk hos en bruker og kontroll mot fremvist pass eller nasjonalt ID-kort. POD har sett på muligheter for en slik løsning, Vipps AS har utviklet appen IDmee og leverandøren er kjent med at det er mange andre tilbydere av lignende løsninger og at markedet er i rask utvikling.

POD har utredet alternativ for en taps- og verifikasjonstjeneste (TOVE) og leverandøren har fått oversendt følgende beskrivelse og status for tjenesten:

> *«Et tapsregister for sterke ID-dokumenter tilgjengeliggjort utenfor politiet er omtalt første gang i Handlingsplanen for ID fra 2012. Øremerkede midler til en taps- og verifikasjonstjeneste kom med oppdrag 055 i Tildelingsbrev 2017.*
>
> *Tjenesten skal etableres tidsriktig ved utstedelse av "nye pass og nasjonale ID-kort", og legge til rette for at offentlige og private aktører kan foreta ekthetskontroll av et fremvist ID-dokument, være seg norsk pass, nasjonalt ID-kort eller tilsvarende utenlandske dokumenter. I tillegg vil de kunne kontrollere om de norsk-utstedte pass og nasjonale ID-kort er meldt tapt eller stjålet.*
>
> *En isolert tapsstatus og verifikasjon av ID-dokumentets elektroniske brikke (ekthetskontroll) uten bruk av biometri vil løse enkelte symptomer, men ikke i tilstrekkelig grad til å bidra til å løse essensen i problemene knyttet til konsekvenser av ID-misbruk i det norske samfunnet. POD er bedt om å utrede mulighetene for å ta i bruk biometri slik at en person kun kan benytte en identitet i Norge.*
>
> *Tjenesten kan på sikt ta inn i seg ulike elementer for å dekke samfunnets behov som "Remote authentification" ved digitalisering og her vil eID knyttet direkte til norske nasjonale ID-kort være essensielt.*
>
> *TOVE er ved ferdigstillelsen av konseptfase, og går i høst i gang med planleggingsfase for etablering av taps- og verifikasjonstjeneste, samt utrede fremtidig bruk av biometri.»*

Slik leverandøren forstår det vil POD lansere TOVE som alternativ 0+ (tapstatus og verifikasjon av elektronisk brikke i ID-bevis) tidsriktig med lanseringen av nasjonale ID-kort i 2020. Formålet med å etablere tjenesten TOVE er at politiet bidrar til å bedre forutsetningene for at offentlige og private aktører kan gjennomføre god ID-kontroll.

TOVE alternativ 0+ vil bestå av en tapsstatustjeneste for norske pass og nasjonale ID-kort som vil tilgjengeliggjøres på politiets nettsider og gjennom grensesnitt, og vil kunne benyttes av offentlige og private aktører. Samtidig vil POD tilgjengeliggjøre grensesnitt for at offentlige og private aktører skal kunne foreta en verifisering av den elektroniske brikken i fysiske ID-bevis mot deres registre. Tjenesten vil kunne kontrollere ektheten av norske pass og nasjonale ID-kort, samt tilsvarende utenlandske fysiske ID-bevis. POD vil kun tilgjengeliggjøre verifikasjonstjenesten, og det er opp til hver enkelt aktør å legge til rette for bruk av tjenesten.

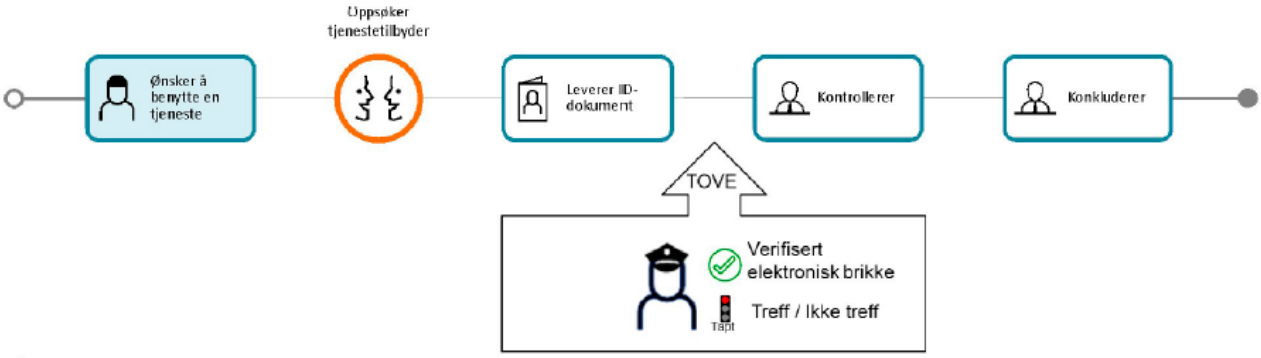
Kriminalitetsbildet, brukernes behov og det teknologiske mulighetsrommet har endret seg de siste årene, og POD har i sitt arbeid med alternativvurderingen av TOVE sett på muligheter for å utvide funksjonaliteten til å omfatte en tjeneste for ID-kontroll der brukeren som fysisk person kobles til ID-dokumentet ved hjelp av biometri, omtalt som TOVE alternativ 1. Alternativ 1 vil ha de samme funksjonalitetene som alternativ 0+,

men vil i tillegg kunne gjennomføre en biometrisjekk av om personen som fremviser et fysisk ID-bevis er rettmessig eier av beviset, ved å kontrollere ansiktsfoto og fingeravtrykk lagret i ID-beviset mot bruker som fremviser ID-beviset. POD anbefaler å gå videre med en løsning som gjør at *«eksterne aktører kan koble seg på politiets grensesnitt med egne løsninger ved sine skrankepunkt, samt at tjenesten TOVE tilgjengeliggjøres som en online og mobil løsning utenfor skrankepunkt for bruk i felt».*[95]

	TOVE alternativ 0+ Tapstatus og verifikasjon av elektronisk brikke	**TOVE alternativ 1** Tjeneste for ID-kontroll
Funksjonalitet	- Tjeneste for tapsstatus tilgjengeliggjøres for offentlige og private aktører på politiets nettsider - Grensesnitt for verifisering av ekthet ved hjelp av elektronisk brikke i fysisk ID-bevis tilgjengeliggjøres for offentlige og private aktører	- Funksjonalitet fra alternativ 0+ - Tjeneste for gjennomføring av biometrikobling (1:1) mellom bruker og fysisk ID-bevis tilgjengeliggjøres for offentlige aktører - Grensesnitt for gjennomføring av biometrikobling (1:1) mellom bruker og fysisk ID-bevis tilgjengeliggjøres for private aktører

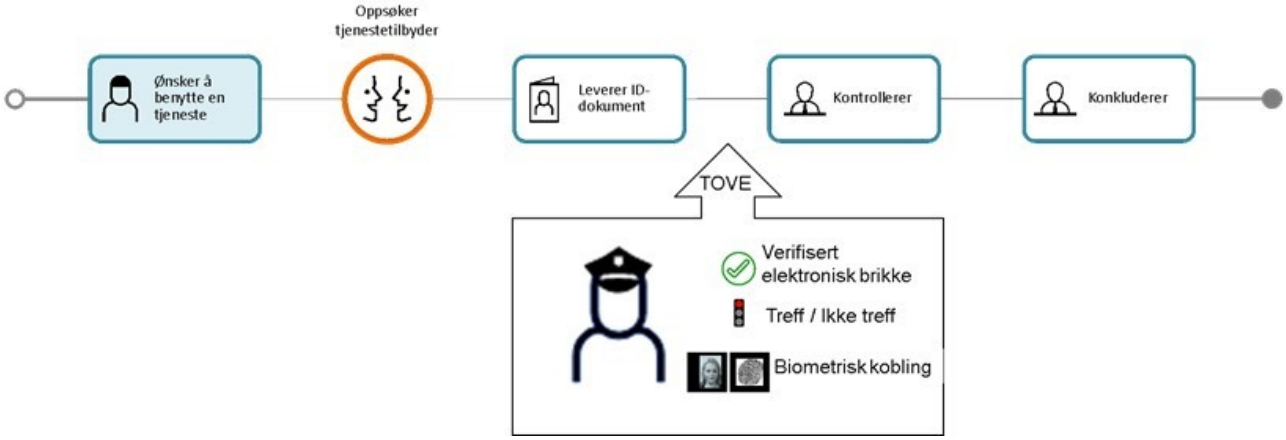
Tabell 8 Overordnet beskrivelse av funksjonalitetene ved de ulike alternativene for TOVE[96]

Figurene under viser PODs overordnede visualiseringer av de to alternativene for TOVE beskrevet over. POD har videre identifisert et sett med bruksområder for TOVE, uavhengig av hvilket alternativ som implementeres. Identifiserte bruksområder (ikke prioritert rekkefølge) er opprettelse av kundeforhold i bank, ID-kontroll ved utlevering av BankID, innrullering i Folkeregisteret, kontroll på arbeidsplasser i arbeidet med arbeidslivskriminalitet og verifisering av ID ved utstedelse av førerkort.[97]



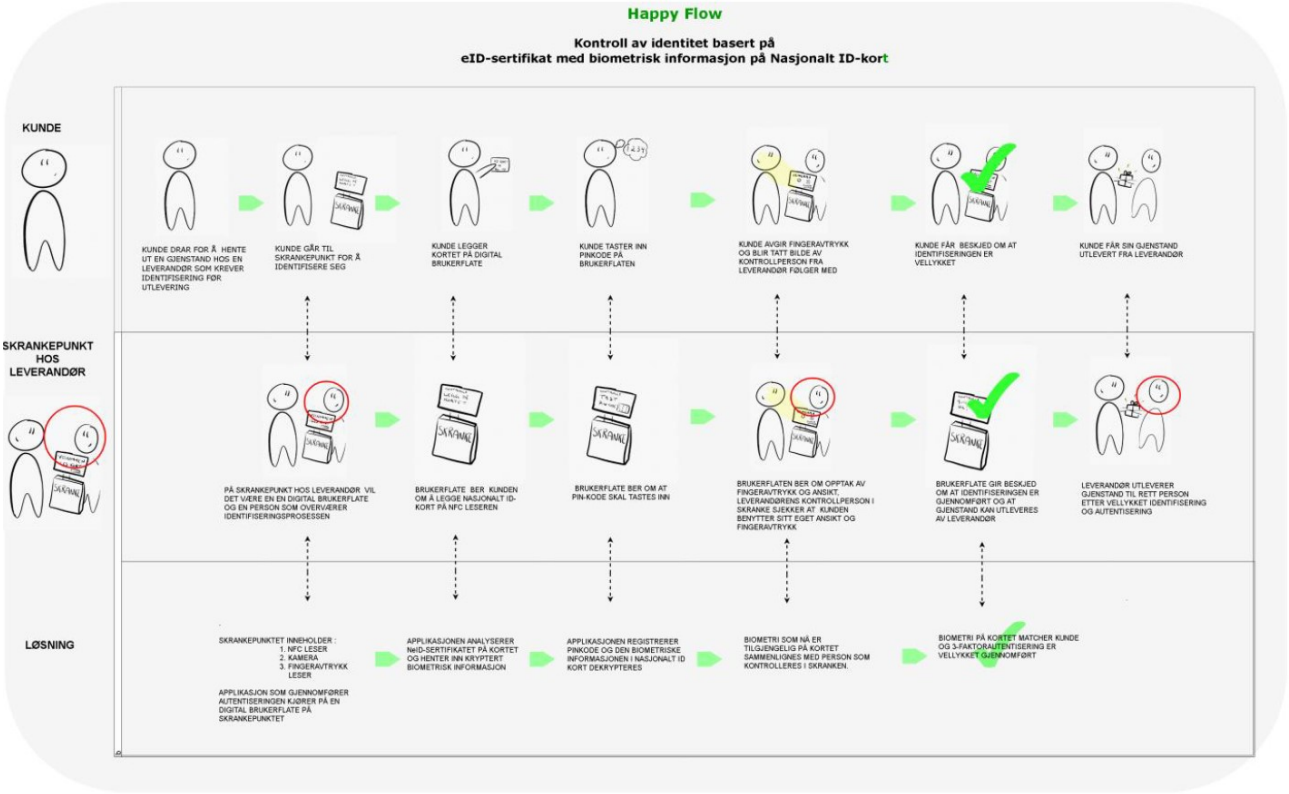
Figur 6 Overordnet visualisering av ID-kontroll med TOVE alternativ 0+[98]

[95] POD, «Alternativvurdering TOVE, Versjon 1.1», 2019
[96] POD, «Alternativvurdering TOVE, Versjon 1.1», 2019
[97] POD, «Alternativvurdering TOVE, Versjon 1.1», 2019
[98] Skjermbilde hentet fra: POD, «Alternativvurdering TOVE, Versjon 1.1», 2019



Figur 7 Overordnet visualisering av ID-kontroll med TOVE alternativ 1[99]

Slik beskrevet i kapittel 3.1.3 vurderes det om funksjonaliteten for nasjonal eID skal utvides til å kunne gjennomføre en trefaktor-autentisering, med sjekk av biometriske opplysninger som er lagret i det nasjonale ID-kortet mot bruker av den nasjonale eID-en. Leverandøren har blitt forelagt følgende konseptuelle beskrivelse, se figur under, som viser et tenkt scenario for hvordan trefaktor-autentisering med nasjonal eID kan gjennomføres i et skrankepunkt. Slik leverandøren forstår det, eksisterer det ikke eksempler på øvrige bruksområder eller andre konseptuelle eller mer detaljerte beskrivelser av løsningen.



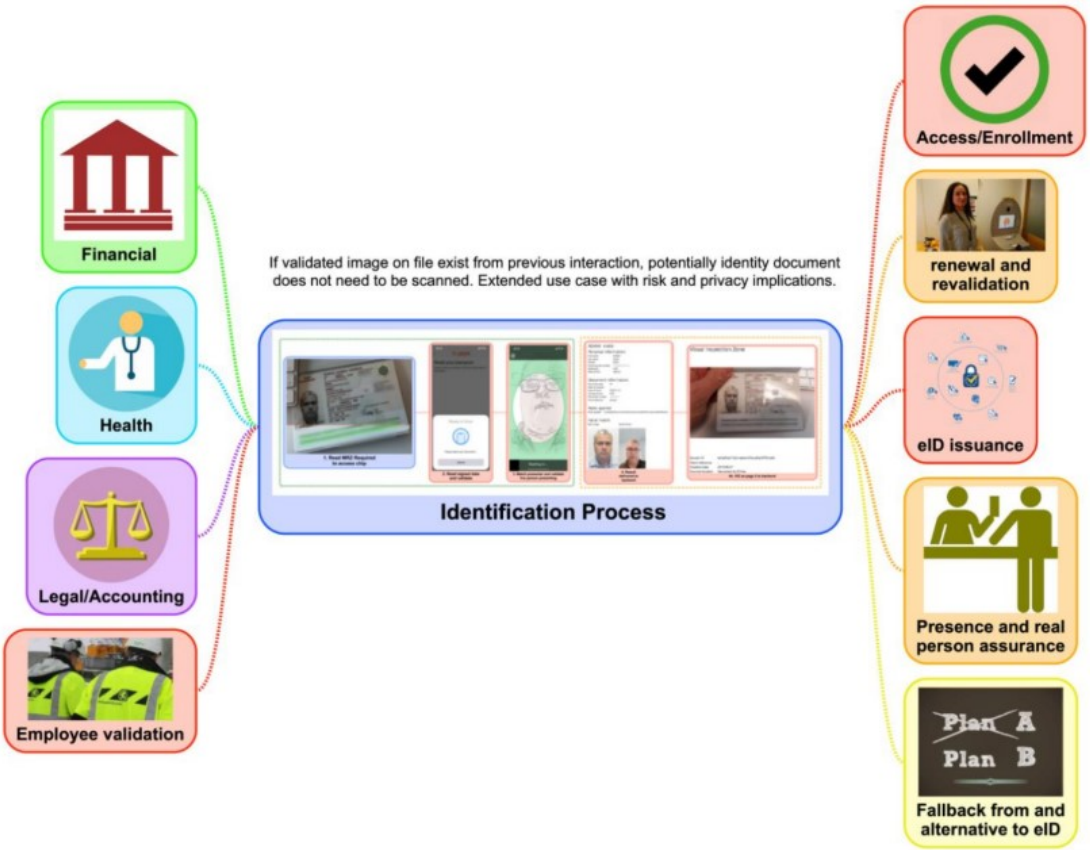
Figur 8 Konseptuell beskrivelse av trefaktor-autentisering med nasjonal eID i skrankepunkt

Vipps AS har utviklet appen IDmee som kan verifisere ektheten til et pass med elektronisk brikke ved hjelp av kamera og NFC-leser i en smarttelefon, samt gjøre en sjekk mellom ansiktsbiometrien til brukeren av appen og ansiktsfoto som ligger lagret i den elektroniske brikken i passet som blir ekthetssjekket. IDmee er slik leverandøren

[99] Visualisering mottatt fra POD, andre halvår 2019

forstår det hovedsakelig en tjeneste for å kunne forenkle opprettelsen av kundeforhold i bank, men vil også kunne ha andre bruksområder, slik beskrevet i figuren under. Vipps har per dags dato en demoversjon av løsningen tilgjengelig og har etablert et samarbeid med DNB, Difi og BITS for å teste løsningen på 6 000 DNB-kunder.[100] Figurene under illustrerer henholdsvis bruk av IDmee-appen for sjekk av ekthet og biometri, og mulige bruksområder for løsningen.

Figur 9 Illustrasjon ekthetssjekk og kontroll av ansiktsbiometri ved bruk av IDmee[101]



Figur 10 Illustrasjon av mulige bruksområder for IDmee[102]

[100] DNB på Linkedin.com, «Passcanning = effektivisering», 25.09.2019
[101] Skjermbilde hentet fra: Idmee.no, «White paper – What we solve», 18.09.2019
[102] Skjermbilde hentet fra: Idmee.no, «White paper – What we solve», 18.09.2019

3.1.6 Om synliggjort feil og misbruk av dagens eID

Slik beskrevet i kapittel 6 i hovedrapporten er det lite dokumentert kvantifisert informasjon på samfunnsøkonomiske konsekvenser av feil og misbruk av ID. Dette gjelder også helhetlige konsekvenser av feil og misbruk av eID. POD begrunner manglende statistikk på ID-kriminalitet med at ID-kriminalitet er et verktøy for andre kriminalitetsformer, og at misbruk av ID og eID ikke blir registrert som egen kriminalitetsform. Slik poengtert i hovedrapporten kapittel 7 registrerer ikke politiet sin tidsbruk mot bestemte aktiviteter, hvilket gjør det krevende å se omfanget av politiets egen ressursbruk og innsats mot ID-kriminalitet.

I privat sektor eksisterer det til en viss grad data på omfanget av misbruk av eID-er. Finanstilsynet rapporterte i sin Risiko- og sårbarhetsanalyse (ROS) for 2018 at tapstall knyttet til bruk av nettbank var omtrent 27 mill. kroner.[103] Det foreligger ikke tall på antall saker som misbruket er fordelt på. Selv om det er flere eksempler på misbruk av eID-er med hensikt om økonomisk svindel, eksempelvis i Lime-saken[104], og misbruket kan utgjøre en betydelig utfordring for samfunnet, eksisterer det slik forklart over ikke samlet statistikk på utfordringen. Bildet under viser samlet svindelstatistikk knyttet til nettbank i 2018 fordelt på type saker.

Svindeltype nettbank	**2018**
Angrep ved bruk av ondartet programkode på kundens PC eller sikkerhetsmekanisme (trojaner)	1 305
Tapt/stjålet sikkerhetsmekanisme	1 954
Phishing og falske BankID-brukersteder	16 858
Annet/Ukjent	6 723
Totalt	**26 840**

Figur 11 Tapstall knyttet til bruk av nettbank[105]

Finanstilsynet skriver videre i sin ROS-analyse at «d*et har vært en økning i antall låneavtaler som inngås gjennom misbruk av andres digitale signatur (BankID), i særlig grad utført av personer i nær relasjon til den som blir svindlet».* [106] I tilfeller der misbruket skjer i nære relasjoner har ikke nødvendigvis personen som misbruker eID-en tilegnet seg nødvendig innloggingsinformasjon på en uærlig måte, ettersom det er flere tilfeller der en eier av eID gir personer i nær relasjon nødvendige innloggingsdetaljer slik at de kan disponere eID-en på vegne av rettmessig eier. Det er dermed vanskelig å avdekke misbruket ettersom eieren i liten grad selv benytter eID-en og ikke har oversikt over hva den benyttes til og om den eventuelt misbrukes.

Et annet eksempel er misbruk av ID-bevis og eID-er i arbeidslivskriminalitetssaker, der eID-er utstedt til utenlandske arbeidstakere som oppholder seg i Norge i en kortere periode blir overtatt og misbrukt av bakmenn når de utenlandske arbeidstakerne forlater Norge. POD informerer om at de er kjent om flere tilfeller av slike «ID-karuseller». Identitetene blir gjenbrukt av ulovlig og «svart avlønnede arbeidstakere», og ofte er det flere personer som jobber under samme identitet. Bakmenn har imidlertid kontroll over arbeidstakernes eID og identitetsnummer. POD oppgir at det i malerbransjen, transportbransjen og rengjøringsbransjen er eksempler hvor

[103] Finanstilsynet.no, «Korrigerte tapstall for svindel med betalingskort og nettbank for 2018», 25.10.2019
[104] Oslo tingrett, «TOSLO-2015-105037-3», 2018
[105] Skjermbilde hentet fra: Bits As, «Bits AS har dessverre oppdaget feil i rapporterte tall for svindel for 2018», 25.10.2019
[106] Finanstilsynet, «Risiko- og sårbarhetsanalyse (ROS) 2018», 2019

næringsdrivende melder om at det nesten er umulig å konkurrere på pris med lovlig arbeidskraft. POD oppgir videre at flere kriminelle nettverk innen bygg- og anleggsbransjen er domfelt for hvitvasking av til sammen over 100 mill. kroner, ved hjelp av til sammen 550 falske/misbrukte identiteter.

3.2 eIDAS – Status og implikasjoner for offentlige digitale tjenester

Slik beskrevet i hovedrapporten kapittel 2.9.2 pågår det et arbeid med å få på plass et mer helhetlig reguleringsregime for eID for medlemsland i EU/EØS. eIDAS-forordningen legger til rette for økt elektronisk samhandling mellom næringsdrivende, borgere og offentlige myndigheter på tvers av landegrensene i EU/EØS og har som mål å bidra til sterkere økonomisk vekst i det indre marked.

For at en eID skal kunne benyttes for autentisering til offentlige tjenester i andre europeiske land må eID-en meldes i henhold til en av de definerte sikkerhetsnivåene i eIDAS-forordningen, slik beskrevet i hovedrapporten kapittel 2.8.2. Det eksisterer imidlertid noen uklarheter rundt tolkningen av annerkjennelsesplikten av utenlandske eID-løsninger i eIDAS-forordningen.[107] Leverandøren forstår, etter innspill fra flere aktører i ID-forvaltningen, at annerkjennelsesplikten til utenlandske meldte eID-er først vil gjelde dersom også norske eID-er er meldt. Dersom en norsk eID meldes på eIDAS sikkerhetsnivå «høyt» innebærer det at alle utenlandske eID-er som også er meldt på eIDAS «høyt» vil kunne benyttes, og må aksepteres, for autentisering til de norske offentlig tjenester som den norske eID-en gir tilgang til.[108] Konsekvensen av å melde eksempelvis BankID på eIDAS «høyt» blir dermed at det offentlige må godkjenne autentisering via alle andre europeiske eID-er meldt på eIDAS «høyt» for tilgang til de offentlige tjenester som BankID gir tilgang til gjennom ID-porten. Brukeren av den utenlandske eID-en må ha fått tildelt et norsk fødselsnummer eller d-nummer og ha rettigheter til å få tilgang til offentlige tjenester og ytelser gjennom ID-porten, for at brukeren skal kunne autentisere seg med sin utenlandske eID. Eksempelvis kan dette benyttes av:

- En spanjol med avledede rettigheter, d-nummer og som er bosatt i Spania, kan benytte sin spanske eID meldt på eIDAS «høyt» for digital kommunikasjon med NAV

- En polakk som arbeider ett år i Norge og som har fått fødselsnummer, kan benytte sin polske eID meldt på eIDAS «høyt» for digital kommunikasjon med Skatteetaten

I Norge er det KMD som har myndighet til å fastsette hvilket organ som skal være meldingsmyndighet overfor Europakommisjonen og melde norske eID-er i henhold til sikkerhetsnivåene satt i eIDAS.[109] Den nye selvdeklarasjonsforskriften likestiller norske sikkerhetsnivåer for eID med sikkerhetsnivåene benyttet i eIDAS-forordningen, slik at en eventuell melding av eID-en i henhold til eIDAS-forordningen gjøres enklere.[110] Private utstedere av eID har seks måneder på seg til å melde sine eID-er til de norske sikkerhetsnivåene etter at den nye selvdeklarasjonsforskriften trådte i kraft. Etter dette er gjennomført vil organet som har meldingsmyndighet sende inn dokumentasjon til Europakommisjonen for å melde norske eID-er. Ifølge Difi vil det ta omtrent seks måneder fra dokumentasjonen leveres, til Europakommisjonen har fullført eIDAS-

[107] NFD, «Prop. 71 LS (2017-2018), Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester), og samtykke til EØS-komiteens beslutning nr. 22/2018 om innlemmelse av forordningen i EØS-avtalen», 2017-2018
[108] Basert på samtaler med Difi, andre halvår 2019
[109] Lovdata, «Delegering av myndighet etter lov om elektroniske tillitstjenester», 08.11.2019
[110] Lovdata, «Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon (selvdeklarasjonsforskriften)», 21.11.2019

meldingen. Difi regner med at de norske eID-ene vil være meldt i henhold til eIDAS innen ultimo 2020/primo 2021.[111] Leverandøren er kjent med det planlegges å melde BankID, Buypass og Commfides på eIDAS-sikkerhetsnivå «høyt», og at nasjonal eID vil meldes på samme sikkerhetsnivå.

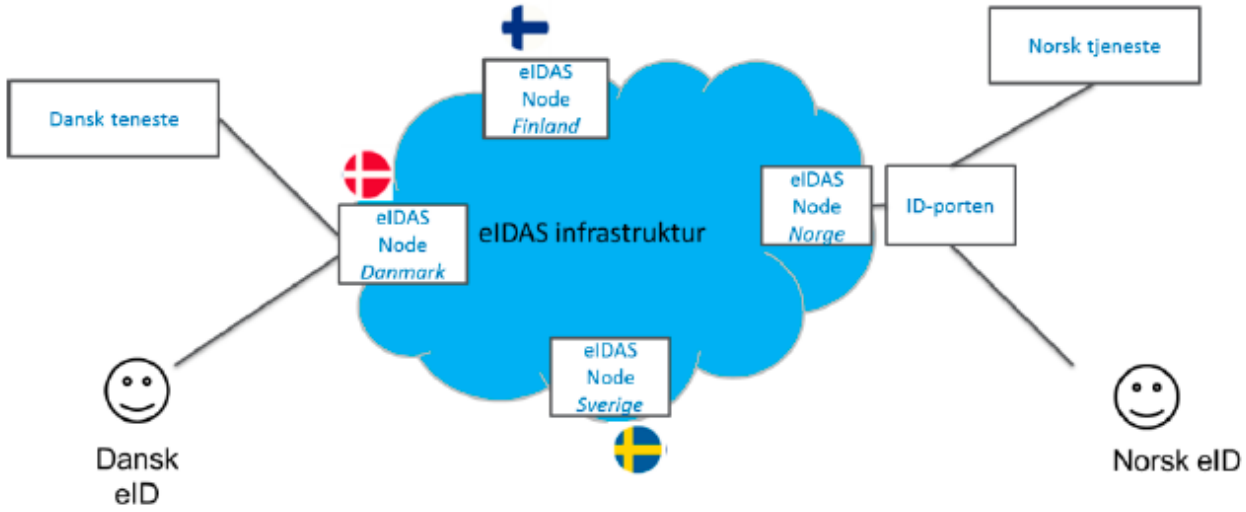
Innføring av eIDAS-forordningen åpner for bruk av utenlandske eID-er for tilgang til norske offentlige tjenester gjennom ID-porten, og kan således medføre nye utfordringer. Leverandøren anser at flere av de alternative løsningene beskrevet under i kapittel 3.5 i stor grad vil kunne omgås ved bruk av en utenlandsk eID, ettersom flertallet av løsningene er rettet mot å tette sikkerhetshull ved utstedelse av norske private eID-er. Utfordringer som bruk av utenlandske eID-er medfører kan imidlertid begrenses ved at det innføres løsninger for sjekk av biometri for å øke sikkerheten ved bruk av både norske og utenlandske eID-er, slik beskrevet i kapittel 3.5.5. Krav om «unike» identitetsnummer for tilgang til en tjeneste eller ytelse kan også implementeres for å styrke sikkerheten tilknyttet autentisering med utenlandske eID-er.

Problemstillingen beskrevet over kan potensielt unngås dersom Norge ikke melder noen norske eID-er, og dermed ikke åpner for bruk av utenlandske eID-er for autentisering og tilgang til norske offentlige tjenester. Det er opp til hvert enkelt land om de ønsker å melde sine eID-løsninger, og det eksisterer ingen juridisk forpliktelse til å melde eID-løsninger.[112] Leverandøren anser imidlertid at det potensielt kan medføre en politisk belastning dersom Norge velger å ikke melde eID-er i henhold til eIDAS-forordningen, og anerkjenner at en slik tilnærming kan være krevende gitt Norges EØS-medlemskap. Ifølge Difi er det i realiteten ikke et alternativ å ikke melde inn norske eID-løsninger, da melding fra alle EU/EØS-land er et premiss for å kunne realisere den potensielle gevinsten av økt elektronisk samhandling på tvers. Innføring av eIDAS vil kunne gi gevinster i form av at eksempelvis borgere som har utvandret fra Norge, men som fortsatt har krav på tjenester og ytelser fra det offentlige, vil kunne benytte en utenlandsk eID for å autentisere seg digitalt og få tilgang til de tjenester og ytelser brukeren har krav på. Leverandøren har ikke blitt gjort kjent med arbeid som konkretiserer ytterligere gevinster ved innføring av eIDAS-forordningen og melding av norske eID-er.

Norske myndigheter kan vurdere identitetsgrunnlaget til den enkelte utenlandske bruker for tilgang til offentlige tjenester og ytelser. Eksempelvis har ikke Tyskland et folkeregister med identitetsnummer, og det kan derfor være utfordrende å koble identiteten en tysk eID-bruker oppgir og får lagret i Norge med identiteten brukeren har i Tyskland. I et slikt tilfelle kan den enkelte tjenesteeier potensielt begrense brukerens tilgang til enkelte tjenester grunnet tvil rundt brukerens identitet i Norge.

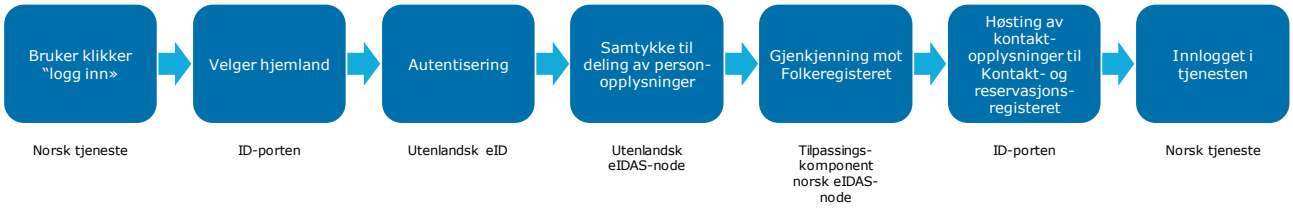
Figuren under er hentet fra en rapport skrevet av Skatteetaten og Difi i forbindelse med et felles eIDAS-prosjekt som ble gjennomført i 2017. Figuren viser overordnet hvordan eIDAS-infrastrukturen ser ut, med et nettverk av sammenkoblede eIDAS-noder der hvert land opererer minst en node i nettverket.[113]

[111] Basert på samtaler med Difi, andre halvår 2019
[112] NFD, «Prop. 71 LS (2017-2018), Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester), og samtykke til EØS-komiteens beslutning nr. 22/2018 om innlemmelse av forordningen i EØS-avtalen», 2017-2018
[113] Skatteetaten og Difi, «eIDAS-innlogging med europeisk eID til norske tjenester», 2017



Figur 12 Overordnet arkitektur for eIDAS-infrastrukturen[114]

Figuren under viser hvordan innloggingsflyten vil se ut når en utenlandsk borger skal autentisere seg til en norsk offentlig tjeneste ved å benytte eID fra sitt hjemland[115].



Figur 13 Steg i innloggingsflyten når utenlandsk eID benyttes på norsk tjeneste[116]

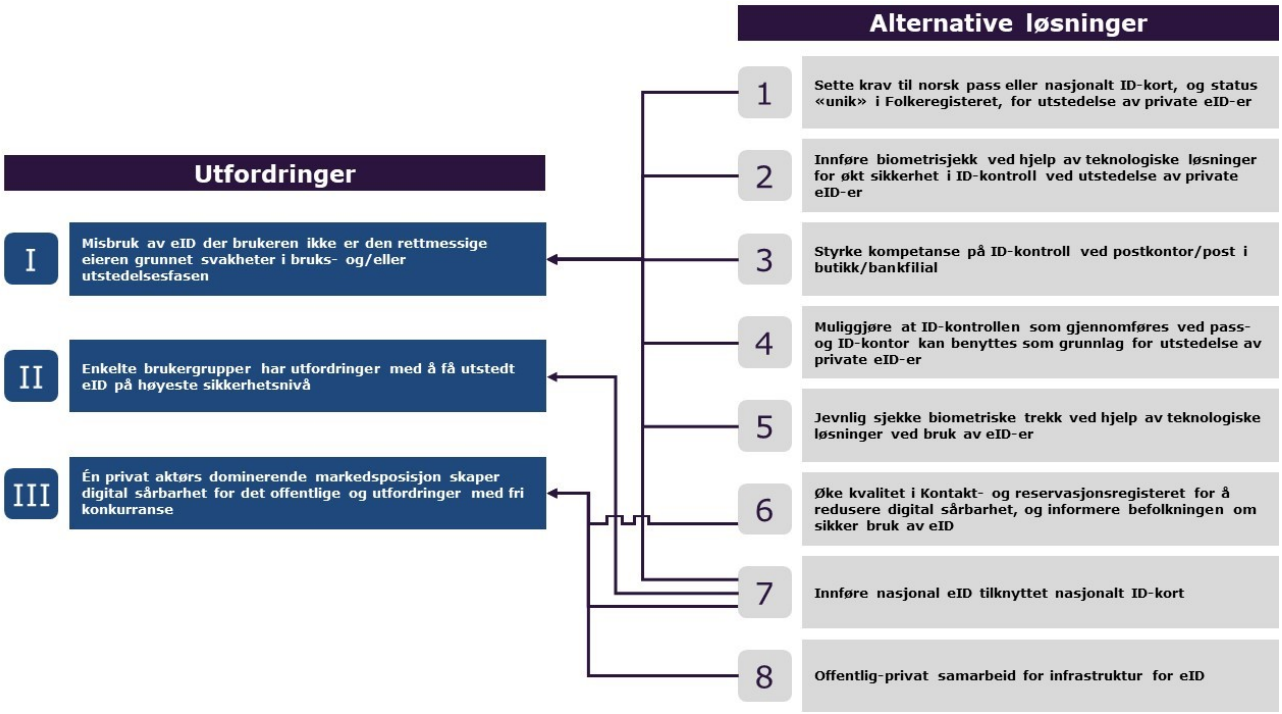
Leverandøren har i begrenset grad identifisert tungtveiende argumenter for å avvente melding av norske eID-løsninger i henhold til eIDAS-forordningen, sett opp mot de potensielle fordelene melding av norske eID-løsninger kan gi. Leverandøren har ikke tatt stilling til behovet for eller risikoen ved å være et foregangsland innen grensekryssende bruk av eID. Leverandøren vurderer videre at det er hensiktsmessig å følge nøye med på antall innlogginger og innloggingsmønstre med utenlandske eID-er når det åpnes for bruk av disse.

3.3 Utfordringer og alternative løsninger for dagens eID-er

I hovedrapporten kapittel 11 belyste leverandøren overordnede utfordringer ved dagens eID-løsninger og anbefalte forbedringer. Basert på mandatet for tilleggsoppdraget har leverandøren bygget videre på dette arbeidet og ytterligere undersøkt og konkretisert utfordringer og alternative løsninger.

Basert på informasjon og erfaringer fra både offentlige og private aktører presenteres under en oversikt over utfordringer ved dagens eID-er og alternative løsninger. Hverken utfordringer eller alternative løsninger er rangert i figuren, og er nærmere forklart i kapittel 3.4 og 3.5.

[114] Skjermbilde hentet fra: Skatteetaten og Difi, «eIDAS-innlogging med europeisk eID til norske tjenester», 2017
[115] Skatteetaten og Difi, «eIDAS-innlogging med europeisk eID til norske tjenester», 2017
[116] Hentet fra: Skatteetaten og Difi, «eIDAS-innlogging med europeisk eID til norske tjenester», 2017



Figur 14 Oversikt over utfordringer og alternative løsninger

De ulike aktørene i ID-forvaltningen har ulike oppfatninger om hva som er de største utfordringene ved dagens eID-tilnærming. Majoriteten fremhever at utfordring I er den største utfordringen, selv om det er uenighet om hvor stor utfordringen reelt sett er, sammenlignet med øvrige utfordringer i ID-forvaltningen som helhet. POD har påpekt overfor leverandøren at utfordring I består av tre ulike utfordringer; én person kan ha flere identitetsnummer i Folkeregisteret, én person kan få ustedt eID i en annen persons identitet og en person kan benytte en annen persons eID. Leverandøren adresserer alle de tre utfordringene i vurderingene av alternative løsninger i kapittel 3.5.

Alternativ løsning 7 innebærer innføring av nasjonal eID tilknyttet nasjonalt ID-kort og behandles separat i kapittel 3.6. Alternativ løsning 8 innebærer opprettelse av et offentlig-privat samarbeid for infrastruktur for eID og behandles separat i kapittel 3.8.

3.4 Utfordringer ved dagens eID-tilnærming

I det følgende beskrives utfordringer som leverandøren har identifisert som de mest sentrale for dagens eID-tilnærming.

Det er en grunnleggende utfordring for eID, og for ID-forvaltningen som helhet, at det i dag ikke er sikret «unike» identiteter i Folkeregisteret. Utfordringen bygger således på utfordringer relatert til opprettelsen av identitetsnummer i Folkeregisteret, slik spesielt dekket i kapittel 6 og 12 i hovedrapporten, og er til dels uavhengig av eID. Selv om dette i hovedsak er et registerkvalitetsproblem, har det konsekvenser for dagens eID-tilnærming. Manglende unikhet betyr at én person kan ha flere identiteter, og dermed mulighet til å ha eID-er i flere ulike identiteter. Mulighetsrommet for misbruk ved at én person har flere eID-er i ulike identiteter er i stor grad det samme som ved at én person har flere gyldige fysiske ID-bevis i ulike identiteter, men bruk av digital autentisering gir enklere mulighet til å misbruke offentlige tjenester og ytelser. Denne problemstillingen er i liten grad drøftet i de videre vurderingene i dette kapittelet og ivaretas av øvrige anbefalinger i leverandørens hovedrapport, samt anbefalinger

relatert til et felles skrankepunkt. Leverandøren presiserer at oppgaven til en eID er å bekrefte en identitetspåstand, og at identifiseringen av en person og tilhørende tildeling av identitetsnummer er beskrevet og vurdert i hovedrapporten.

3.4.1 Utfordring I: Misbruk av eID der brukeren ikke er den rettmessige eieren grunnet svakheter i bruks- og/eller utstedelsesfasen

I dagens system eksisterer det etter leverandørens oppfattelse noe begrensede kontrollmekanismer for å forhindre at en eID utstedes til feil person, altså en person som utgir seg for å være en annen ved ID-kontrollen for utstedelse av eID-en. Videre er det begrensede kontrollmekanismer som kan kontrollere om brukeren av eID-en er den rettmessige eieren av eID-en påfølgende utstedelse. De to grunnleggende sikkerhetshullene som muliggjør disse utfordringene er beskrevet under.

Manuell ID-kontroll hos Posten/bankfilial ved utstedelse av private eID-er, herunder svakheter i ID-kompetanse, ingen biometrisk kontroll og ulike krav til fysiske ID-bevis

For utstedelse av private eID-er kreves det i dag personlig oppmøte og fremvisning av et godkjent fysisk ID-bevis for ID-kontroll ved et av de 2 340 oppmøtestedene, slik beskrevet i kapittel 3.1.1 og 3.1.2. ID-kontrollen gjennomføres av et meget bredt omfang av medarbeidere, hvorav mange er deltidsansatte, eksempelvis ved post i butikk. Strukturen setter naturlige begrensninger på hvorvidt det er mulig å bygge god kompetanse på ID-kontroll hos så mange medarbeidere ved et stort antall oppmøtesteder. Videre er ID-kontrollen som gjennomføres i hovedsak manuell, hvilket betyr at det ikke benyttes utstyr som kontrollerer og sammenligner biometriske trekk av den som møter opp til ID-kontroll og ID-beviset som fremvises. Enkelte kontrollsteder benytter seg av en Keesing-maskin eller tilsvarende som kan lese av passet og sjekke ekthet, men kontrollen av rettmessig eier av fremlagt legitimasjon er fortsatt manuell. Leverandøren er gjort kjent med at slike maskiner relativt ofte returnerer et svar om at et pass er ekte selv om det er falskt, eller omvendt.

Slik beskrevet i kapittel 3.1.2 stilles det ulike krav til fremvisning av fysiske ID-bevis for utstedelse av de ulike private eID-er. Ettersom løsningene fra BankID og Buypass begge gir tilgang til offentlige tjenester på sikkerhetsnivå 4, er det problematisk at kravet til fysisk ID-bevis, og dermed sikkerhetsgrunnlaget ved utstedelse, ikke er likt. Følgelig er det problematisk at ulike krav til fysiske ID-bevis ved utstedelse av eID bryter med det grunnleggende prinsippet om at sikkerheten ved tilgang til offentlige tjenester og ytelser må være like god ved fysiske ID-bevis og eID, slik beskrevet innledningsvis.

Ingen biometrisk kontroll eller lignende ved bruk og fornyelse av at bruker av privat eID er rettmessig eier av eID-en

Det gjennomføres i dag ingen biometrisk kontroll av om brukeren av en eID er den rettmessige eieren. Dersom en person får tilgang til den nødvendige informasjonen som behøves for å autentisere seg med en annens eID, kan eID-en dermed misbrukes uten at det kontrolleres om brukeren er den rettmessige eieren. Som beskrevet i kapittel 3.1.2 har private eID-er i dag i praksis evig gyldighet, hvilket betyr at dersom en person har fått tilgang til en annen brukers eID kan den utføre misbruk til evig tid, så fremt rettmessig eier av eID ikke melder kodebrikke/smartkort mistet og får sperret eID-en. Dette skiller seg fra tilgang til tjenester og ytelser ved bruk av et fysisk ID-bevis, der brukeren kontrolleres hver gang, selv om ID-kontrollen kan hevdes å være mindre sikker.

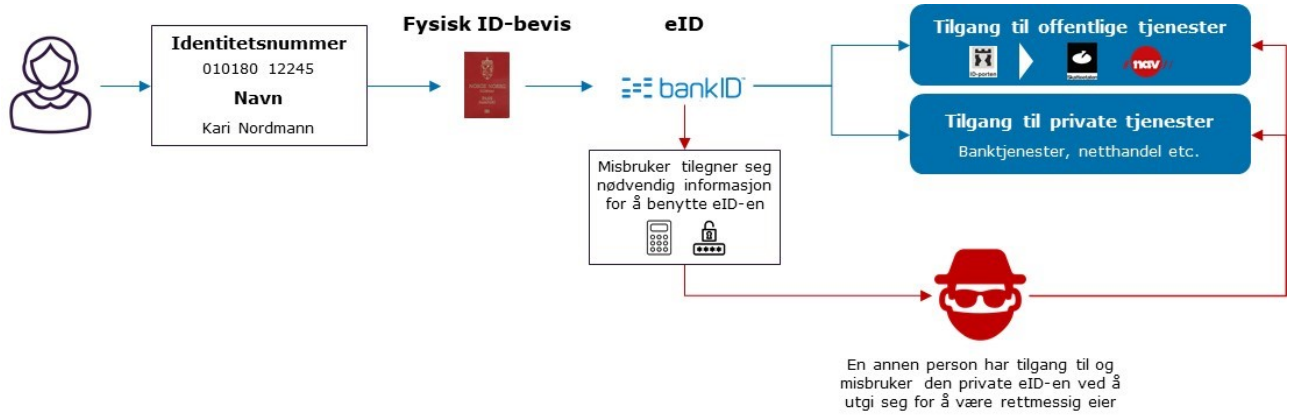
Selv om det i teorien er mulig å misbruke en eID til evig tid, anser leverandøren at den største risikoen ved manglende biometrisk kontroll er ved misbruk av private eID-er til tjenester som innebærer potensielle store økonomiske belastninger for bruker, slik som opptak av lån eller overføring av penger fra rettmessig eiers kontoer. Dette er misbruk som mest sannsynlig vil gjøres så fort som mulig etter at en misbruker har fått tilgang til en annen brukers eID.

Konsekvenser av sikkerhetshullene

Utfordringen ved at en eID utstedes til feil person er mulig dersom en person har tilegnet seg en annen brukers ekte ID-bevis, har forfalsket et ID-bevis for å operere under en annen brukers identitet eller benytter et ID-bevis som ligner personen som misbrukes, og dette ikke blir oppdaget i ID-kontroll ved utstedelse av eID-en. Konsekvensen av en slik feilutstedelse er at en person har muligheten til å autentisere seg digitalt i en annen persons identitet, og få tilgang til og misbruke offentlige og private tjenester i denne identiteten. Leverandøren er imidlertid gjort kjent med at Difi erfarer at majoriteten av misbruk tilknyttet eID-er skjer i bruksfasen og ikke som et resultat av feilutstedelser beskrevet over. POD påpeker riktignok at feilutstedelser av eID kan være en viktig kilde til misbruk og fremhever flere eksempler på dette.

Misbruk av eID der bruker ikke er rettmessig eier av eID-en er utfordrende å avdekke. Avdekking av misbruket skjer først ved at enten den rettmessige eieren av eID-en selv oppdager misbruket eller ved at utstederen av eID-en oppdager unormal bruk av eID-en. Slik beskrevet i kapittel 3.1.6 ble det i 2018 rapportert om tapstall knyttet til bruk av nettbank på omtrent 27 mill. kroner.[117] Finanstilsynet skriver videre om økt misbruk i nære relasjoner, særlig ved inngåelse av låneavtaler der bruker av eID ikke er rettmessig eier.

Figuren under viser en skisse der en person har den nødvendige informasjonen (identitetsnummer, passord og kodebrikke eller mobiltelefon med BankID på mobil) for å misbruke eID-en til den rettmessige eieren. Et tenkt scenario under kan være at personen som har tilgang til og misbruker eID-en tar opp lån i den rettmessige eierens navn og overfører mottatt lån til en konto som misbrukeren selv disponerer. Andre mulige scenarioer er at misbrukeren endrer rettmessig eiers utbetalingskonto for ytelser fra NAV eller for tilbakebetaling av skattepenger i forbindelse med skatteoppgjøret, til en konto som misbrukeren selv disponerer.



Figur 15 Eksempel på misbruk av eID der brukeren av eID-en ikke er rettmessig eier

[117] Finanstilsynet.no, «Korrigerte tapstall for svindel med betalingskort og nettbank for 2018», 25.10.2019

3.4.2 Utfordring II: Enkelte brukergrupper har utfordringer med å få utstedt eID på høyeste sikkerhetsnivå

På prinsipielt grunnlag ser leverandøren det som en utfordring at det i praksis er de private utstederne av eID som regulerer brukerens mulighet til å kunne identifisere seg på høyeste sikkerhetsnivå for tilgang til offentlige og private tjenester.

Som nevnt i hovedrapporten kapittel 2.8.2 er BankID den klart mest brukte eID-en for autentisering til offentlige tjenester gjennom ID-porten, med ca. 82 prosent av alle autentiseringene i 2018. Den offentlige eID-en MinID gir tilgang til autentisering på sikkerhetsnivå 3 og ble benyttet i ca. 16 prosent av autentiseringene. Buypass ble kun benyttet ved ca. to prosent av autentiseringene i ID-porten i 2018. Selv om det kun er 21 prosent av tjenestene i ID-porten som krever autentisering med eID på sikkerhetsnivå 4, ble det i 2018 benyttet eID-er med sikkerhetsnivå 4 ved 84 prosent av alle autentiseringer.[118] Det vil si at størsteparten av alle autentiseringer til offentlige tjenester gjennom ID-porten gjøres med private eID-er, uavhengig av definert sikkerhetsnivå.

Basert på dagens regelverk kan det være utfordrende for enkelte brukergrupper å få utstedt en privat eID med mulighet for autentisering på sikkerhetsnivå 4. Eksempelvis vil personer med kriminell historie kunne ha utfordringer med å opprette bankforhold, grunnet bankenes fokus på antihvitvask, og får dermed ikke tilgang til den dominerende aktørens løsninger. En person som ikke kvalifiserer for et bankforhold eller banken ikke ønsker som kunde vil heller ikke få BankID. Personer som ikke får opprettet bankforhold, kan likevel få utstedt en eID fra Buypass så fremt de oppfyller kravene til fysisk ID-bevis beskrevet i kapittel 3.1.2.

Det er i hovedsak to grupper som ikke har mulighet til å få utstedt en eID på høyeste sikkerhetsnivå i dag, barn under 13 år og personer som ikke har et gyldig fysisk ID-bevis og ingen mulighet til å bevise sin identitet.

BankID har en aldersgrense på 13 år, men aldersgrensen varierer blant bankene og enkelte banker opererer med 15 og 18 års aldergrense.[119] Buypass har en aldersgrense på 13 år for sine eID-løsninger.[120] Følgelig kan ikke barn under 13 år autentisere seg digitalt på høyeste sikkerhetsnivå og de er avhengig av at dette gjøres av den/de som har foreldreansvar for barnet, eksempelvis ved tilgang til barnets helseopplysninger gjennom Helsenorge sine sider.[121] Det er i liten grad lagt frem et behov for at barn under 13 år skal ha en eID på sikkerhetsnivå 4, og leverandøren har følgelig ikke vektlagt dette i vurderingene av alternative løsninger i kapittel 3.5.

Det er en mindre gruppe bestående av personer som ikke har et gyldig fysisk ID-bevis og ingen mulighet til å bevise sin identitet, som ikke kan få utstedt en eID på høyeste sikkerhetsnivå. Per 2018 utgjorde denne gruppen omtrent 2 200 personer med begrenset oppholdstillatelse i Norge, på bakgrunn av at de ikke har tilstrekkelig sannsynliggjort sin identitet.[122]

[118] Basert på data fra Difi, andre halvår 2019. Gjelder for antall tjenester ved utgangen av 2018 og antall autentiseringer gjennomført i 2018
[119] BankID.no, «Aldersgrense i bankene», u.å.
[120] Buypass.no, «Aldersgrense og andre betingelser», u.å.
[121] Helsenorge.no, «Slik representerer du andre på helsenorge.no», 2019
[122] POD, «Oppfølging av oppdrag 053 gitt i 2017 – Nasjonalt ID-kort til utenlandske borgere», 2018. Problemstillinger med denne gruppen er nærmere belyst i kapittel 2.2

3.4.3 Utfordring III: Én privat aktørs dominerende markedsposisjon skaper digital sårbarhet for det offentlige og utfordringer med fri konkurranse

Som beskrevet i hovedrapporten kapittel 2.8.1 og 2.8.2 har BankID ca. 4 mill. brukere og ble benyttet ved 82 prosent av alle autentiseringer til offentlige tjenester gjennom ID-porten i 2018. Slik videre beskrevet i hovedrapporten kapittel 11.1 anser leverandøren at en situasjon med én såpass dominerende aktør kan være utfordrende dersom BankID skulle få langvarige tekniske problemer med å levere sine tjenester, få nye eiere eller øke prisene på tjenesten sin betraktelig.

Avhengighet av tilgjengeligheten til BankID som autentiseringssystem er en digital sårbarhet for bankene finanssektoren i dag, og det samme gjelder for autentisering til offentlige tjenester på høyeste sikkerhetsnivå.[123] Det offentlige har få alternativ dersom BankIDs tjenester ikke er tilgjengelige, utover å benytte MinID og data fra Kontakt- og reservasjonsregisteret for å sikre alternativ tilgang til offentlige tjenester.

Videre utgjør BankIDs dominerende markedsposisjon en prisrisiko for det offentlige, og utviklingen i næringen tilsier at det er en risiko for at Vipps AS øker prisene for bruk av BankID i fremtiden. Det offentlige har i tillegg manglende strategisk kontroll over infrastrukturen og de private eID-ene, og de private aktørene har i utgangspunktet full kontroll over infrastrukturen de benytter for autentisering med sine løsninger.

Leverandøren ser også utfordringer ved at ansatte ofte benytter en eID utstedt til dem som privatperson for å autentisere seg digitalt i jobbsammenheng. I dagens eID-tilnærming skilles det ikke tydelig på hvem personen er som privatperson og hvem personen er i jobbsammenheng i slike tilfeller. Leverandøren har imidlertid ikke blitt forelagt informasjon som tilsier at dette er en stor utfordring ved dagen eID-tilnærming, og utfordringen er derav ikke vektlagt i vurderingen av alternative løsninger i kapittel 3.5.

3.5 Alternative løsninger til identifiserte utfordringer

I det følgende beskrives og vurderes alternative løsninger som kan bidra til å løse de identifiserte utfordringene ved dagens eID-tilnærming. Alternativene er vurdert i tilhørende tabeller etter kategorisering om alternativet løser beskrevne utfordringer på en «*mindre god*», «*god*» eller «*meget god*» måte, og vurdert ift. vurderingskriteriene sikkerhet, brukervennlighet og ressursbruk. Alternativene er beskrevet isolert, men kan kombineres på ulike måter for best å løse de identifiserte utfordringene.

3.5.1 Alternativ løsning 1: Sette krav til norsk pass eller nasjonalt ID-kort, og status «unik» i Folkeregisteret, for utstedelse av private eID-er

Alternativet innebærer å innføre krav om norsk pass eller nasjonalt ID-kort ved utstedelse av private eID-er. Alternativet vil sikre at brukere som får utstedt nye private eID-er har status «unik» i Folkeregisteret, ettersom den biometriske informasjonen som behøves for å oppnå «unik» registreres og sjekkes ved utstedelse av norske pass og nasjonalt ID-kort fra og med slutten av 2020, slik beskrevet i kapittel 2.5.2. Alternativet fordrer et bredt tilbud for nasjonalt ID-kort, slik beskrevet i kapittel 2.2.3.

Alternativet vil bidra til at det ikke blir mulig for en person å inneha fysiske ID-bevis for flere identiteter som godkjennes for utstedelse av private eID-er, og dermed bidra

[123] Lysne et al., «NOU 2015:13, Digital sårbarhet – sikkert samfunn», 2015

til å redusere muligheten for å anskaffe og benytte flere ulike eID-er i flere identiteter. ID-kontrollen som gjennomføres ved utstedelse av private eID-er vil bli marginalt sikrere ettersom kun to fysiske ID-bevis er mulig å benytte. Videre vil PODs lansering av TOVE alternativ 0 og tilgjengeliggjøring for private aktører bidra til å øke sikkerheten i ID-kontrollen som gjennomføres ved postkontor, post i butikk og bankfilialer.

I den nye selvdeklarasjonsforskriften stilles det krav til pass eller nasjonalt ID-kort, norske eller utenlandske, for utstedelse av private eID-er.[124] Dette betyr at utenlandske pass og nasjonale ID-kort godtas som ID-bevis ved utstedelse, og følgelig vil ikke private eID-er som er utstedt på grunnlag av disse bevisene sikre status «unik» for brukeren. Videre vil ikke kontrollørene kunne bygge like god kompetanse på kontroll av ID-bevis da er stort antall ulike ID-bevis er godkjent.

Alternativet vil potensielt være til ulempe for utenlandske brukere som ønsker å anskaffe seg en privat eID, ved at de først må få utstedt et nasjonalt ID-kort. Melding av norske private eID-er til eIDAS vil imidlertid bety at utenlandske brukere kan benytte meldte eID-er fra sitt hjemland, hvilket betyr at de ikke behøver å anskaffe et nasjonalt ID-kort og en privat eID for tilgang til offentlige tjenester.

Alternativet vil kun bidra til å løse utfordringer for eID-er som enda ikke er utstedt, og vil ikke løse utfordringer for allerede utstedte eID-er i bruk.

Sikkerhet	• Sikrer at alle brukere som får utstedt en privat eID har avlagt biometri og har status «unik». Dermed betydelig vanskeligere å anskaffe og benytte flere ulike eID-er i flere identiteter for en person • ID-kontrollen som gjøres ved utstedelse vil bli sikrere ettersom kun to fysiske ID-bevis er mulig å benytte, hvor kontrollører lettere kan bygge kompetanse på gjenkjenning av falske bevis. Samtidig utføres ID-kontroll av et meget bredt spekter av ansatte på et meget stort omfang av utstedelsessteder • Gir ingen forbedring i misbruk der brukeren av eID-en ikke er den rettmessige eieren, selv om identitetsnummeret er klassifisert som «unik» • Samlet sett en god løsning for å løse deler av utfordring I tilknyttet svakheter i sikkerheten ved utstedelsen av private eID-er
Brukervennlighet	• Potensiell ulempe for utenlandske brukere å måtte anskaffe et nasjonalt ID-kort for å få utstedt en privat eID
Ressursbruk	• Potensiell økning i ressursbruken ved pass- og ID-kontor ved stor etterspørsel etter nasjonale ID-kort

Tabell 9 Vurdering av alternativ løsning 1

3.5.2 Alternativ løsning 2: Innføre biometrisjekk ved hjelp av teknologiske løsninger for økt sikkerhet i ID-kontroll ved utstedelse av private eID-er

Alternativet innebærer å innføre biometrisjekk av brukere og sammenligning med fremvist gyldig ID-bevis ved utstedelse av private eID-er. Biometrisjekken vil gjøres ved at ansiktsbiometrien til bruker blir sammenlignet med ansiktsfoto som ligger lagret i pass eller nasjonalt ID-kort som fremvises, og bidrar til å sikre at brukeren som får utstedt eID-en er det rettmessige eieren av eID-en.

[124] Lovdata, «Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon (selvdeklarasjonsforskriften)», 21.11.2019

Slik beskrevet i kapittel 3.1.5 kan eksempelvis Vipps sin løsning IDmee, POD sin TOVE-løsning (alternativ 1) eller nasjonal eID med trefaktor-autentisering benyttes for å gjennomføre en slik biometrisk kontroll. Videre vil bruk av IDmee eller TOVE alternativ 1 bidra til å kunne verifisere ektheten til ID-beviset som fremvises. Taps- og verifikasjonstjenesten i TOVE vil i tillegg øke sikkerheten ved at det kontrolleres om fremvist pass eller nasjonalt ID-kort er meldt tapt eller mistet. Ettersom denne tjenesten vil gjøres tilgjengelig for både offentlige og private aktører vil det potensielt være mulig å integrere en slik kontroll også i en IDmee-løsning eller andre tilsvarende private tjenester. POD vurderer muligheter for å bygge inn ekthetssjekk og kontroll av om fremvist ID-bevis er meldt tapt eller savnet i en nasjonal eID med trefaktor-autentisering.

Alternativet vil kun bidra til å løse utfordringer for eID-er som enda ikke er utstedt, og vil ikke løse utfordringer for allerede utstedte eID-er i bruk. Løsninger som er bygget på tankesettet beskrevet over og underlagt statlig eierskap burde etter leverandørens oppfatning kunne benyttes for å oppnå status «kontrollert» i Folkeregisteret. Løsninger som er eid av private aktører, slik som IDmee, burde imidlertid ikke kunne benyttes for å oppnå status «kontrollert». Andelen identitetsnummer med status «kontrollert» i Folkeregisteret vil kunne økes relativt raskt ved at brukere selv benytter en løsning for å kontrollere sin egen identitet, sammenlignet med om alle brukere skal måtte møte opp ved et pass- og ID-kontor for å gjennomføre en ID-kontroll.

Figur 16 Eksempel på tenkt bruk av TOVE/IDmee for biometrisjekk av bruker ved utstedelse av privat eID

Sikkerhet	• Økt sikkerhet ved at den rettmessige eieren er den som får utstedt den private eID-en • Bruk av løsninger som TOVE alternativ 1 eller IDmee vil øke sikkerheten ved at det sjekkes om fremvist ID-bevis er ekte • Bruk av TOVE alternativ 1 vil øke sikkerheten ved at det sjekkes om fremvist ID-bevis er meldt tapt/mistet • Bidra til å øke andelen identitetsnummer med status «kontrollert» dersom de teknologiske løsningene godkjennes som grunnlag for dette • Gir ingen forbedring i misbruk der brukeren av eID-en ikke er den rettmessige eieren, selv om identitetsnummeret er klassifisert som «unik» • God løsning for å løse deler av utfordring I tilknyttet misbruk av eID der brukeren ikke er rettmessig eier
Brukervennlighet	• Ingen vesentlige endringer
Ressursbruk	• Redusert ressursbruk knyttet til ID-kontroll ved postkontor/post i butikk/bankfilial ved at bruker selv gjennomfører biometrisk sjekk og behovet for oppmøte faller bort

Tabell 10 Vurdering av alternativ løsning 2

Alternativet kan også potensielt gjennomføres uten personlig oppmøte, noe som kan øke brukervennligheten betydelig og redusere samlet ressursbruk, men kan redusere sikkerheten sammenlignet med personlig oppmøte som beskrevet over.

Leverandøren anser det som hensiktsmessig at det offentlige eier en teknologisk løsning som ligger utenfor eID-løsningene, med funksjonalitet for sjekk av biometriske trekk hos bruker og kontroll mot fremvist pass eller nasjonalt ID-kort. Løsningen burde kunne sjekke ektheten av den elektroniske brikken i fremvist ID-bevis, samt kunne kontrollere om ID-beviset er meldt tapt eller mistet. Den offentlige løsningen burde videre kunne benyttes både ved autentisering med eID gjennom ID-porten og ved fysisk fremmøte med kontroll av fysiske ID-bevis og fysisk person. Private tjenesteeiere kan tenkes å ha tilsvarende teknologiske løsninger som kjøpes i det private markedet, og etter leverandørens vurdering må det ikke nødvendigvis være et offentlig ansvar å tilby en slik løsning til private tjenesteeiere.

Dersom denne løsningen innføres uten at alternativ løsning 1 innføres, vil ikke en biometrisk kontroll av brukere som benytter et utenlandsk fysisk ID-bevis kunne bekrefte at det er knytning mellom brukeren som får utstedt eID-en og identitetsnummeret brukeren er registrert med i Folkeregisteret.

3.5.3 Alternativ løsning 3: Styrke kompetanse på ID-kontroll ved postkontor/post i butikk/bankfilial

Alternativet innebærer å styrke ID-kontrollen som gjennomføres ved postkontor, post i butikk og i bankfilialer ved å styrke kompetansen til de ansatte som gjennomfører ID-kontrollene. Posten og banknæringen er ansvarlige for at deres ansatte som gjennomfører ID-kontroll gjennomgår opplæring. En styrking av denne ID-kontrollkompetansen kan for eksempel gjøres ved at ansatte må gjennom et kurs i regi av Nasjonalt ID-senter (NID). NID gjennomfører i dag et 1-2 dagers kurs for ansatte i førstelinjen ved de nye pass- og ID-kont

orene, samt et mer omfattende kurs for ansatte i andrelinjen. Ved at ansatte ved postkontor, post i butikk og bankfilial som skal gjennomføre ID-kontroll gjennomfører kompetansebyggende tiltak, sikres økt kompetanse.

Alternativet vil kun bidra til å løse utfordringer for eID-er som enda ikke er utstedt, og vil ikke løse utfordringer for allerede utstedte eID-er i bruk.

Sikkerhet	• Krevende til umulig å nå ut til alle ansatte som gjennomfører ID-kontroll på de 2 340 oppmøtestedene, med meget begrenset potensial for økning i sikkerhet i ID-kontrollen som gjennomføres ved postkontor/post i butikk/bankfilial • Gir ingen forbedring i misbruk der brukeren av eID-en ikke er den rettmessige eieren, selv om identitetsnummeret er klassifisert som «unik» • Mindre god løsning for å løse deler av utfordring I tilknyttet svakheter i sikkerheten ved utstedelsen av private eID-er
Brukervennlighet	• Ingen vesentlige endringer
Ressursbruk	• Svært ressurskrevende å gjennomføre kurs for svært mange ansatte ved postkontor/post i butikk/bankfilial over hele landet

Tabell 11 Vurdering av alternativ løsning 3

3.5.4 Alternativ løsning 4: Muliggjøre at ID-kontrollen som gjennomføres ved pass- og ID-kontor kan benyttes som grunnlag for utstedelse av private eID-er

Alternativet innebærer å muliggjøre at ID-kontrollen som gjennomføres ved et pass- og ID-kontor benyttes og legges til grunn for utstedelse av private eID-er, slik beskrevet i hovedrapporten kapittel 11.2.2. Alternativ løsning 1 om krav til norsk pass eller nasjonalt ID-kort og status «unik» i Folkeregisteret gjelder fortsatt, men alternativet som beskrives her er et verktøy for å gjennomføre det fysiske oppmøtet for utstedelse av private eID, sikre status «unik» og ikke være avhengig av at ID-kontroller gjennomføres ved postkontor, post i butikk eller bankfilial. Størsteparten av den norske befolkningen er i dag innom et pass- og ID-kontor med jevne mellomrom for utstedelse og fornyelse av pass, og i fremtiden nasjonalt ID-kort. Endringen alternativet medfører vil være størst for utenlandske borgere, som i større grad enn i dag må dra innom et pass- og ID-kontor. Alternativet innebærer også at brukere som ikke ønsker å få utstedt eller fornyet pass eller nasjonalt ID-kort, kan dra til et pass- og ID-kontor for å bli ID-kontrollert med hensikt å oppnå status «unik» og benytte dette til utstedelse av en privat eID. Alternativet støtter oppunder tankegangen om et felles skrankepunkt som beskrives i kapittel 5, og bygger på et bredt tilbud om nasjonalt ID-kort slik beskrevet i kapittel 2. Et eventuelt vederlag til politiet fra private tilbydere av eID som benytter seg av dette alternativet må etter leverandørens vurdering utredes nærmere.

Den påfølgende prosessen og tekniske innretningen som beskrives under for å legge til grunn ID-kontrollen fra et pass- og ID-kontor kan løses på flere måter, og er derfor kun ment som et eksempel.

Alternativet innebærer at brukeren på pass- og ID-kontoret får et valg om de ønsker at ID-kontrollen skal kunne benyttes og legges til grunn av private utstedere av eID. Dersom brukeren godtar dette vil den motta en engangskode/token som kan benyttes ved utstedelse av privat eID. Brukeren kontakter utsteder av privat eID, for eksempel via utsteders hjemmeside, og benytter engangskoden/token for å identifisere seg. Utstederen sjekker brukerens informasjon i Folkeregisteret, om brukeren har status «unik» og får samtidig tilgang til en nøkkel som matches med engangskoden/token til bruker. På denne måten vet utsteder at brukeren har blitt ID-kontrollert ved et pass- og ID-kontor og at den har status «unik» i Folkeregisteret. Brukeren får utstedt eID-en i form av et smartkort, aktiveringskode eller kodebrikke tilsendt per post til folkeregistrert adresse. Brukeren aktiverer til slutt eID-en ved å benytte sin engangskode/token.

Figuren under viser et eksempel på en brukerreise der ID-kontrollen ved et pass- og ID-kontor benyttes som grunnlag for utstedelse av privat eID.

Figur 17 Eksempel for brukerreise der ID-kontroll utført ved pass- og ID-kontor benyttes som grunnlag for utstedelse av privat eID

Alternativet vil kun bidra til å løse utfordringer for eID-er som enda ikke er utstedt, og vil ikke løse utfordringer for allerede utstedte eID-er i bruk.

Sikkerhet	• Økt sikkerhet ved at alle private eID-er er utstedt med grunnlag i ID-kontroll utført av ansatte med høy ID-kompetanse ved et pass- og ID-kontor • Status «unik» for alle brukere som får utstedt en privat eID • God løsning for å løse deler av utfordring I tilknyttet svakheter i sikkerheten ved utstedelsen av private eID-er
Brukervennlighet	• Betydelig redusert brukervennlighet ved at antall oppmøtesteder for gjennomføring av ID-kontroll reduseres fra 2 340 steder til 78
Ressursbruk	• Redusert ressursbruk knyttet til ID-kontroll ved postkontor/post i butikk/bankfilial • Potensielt økt ressursbruk ved pass- og ID-kontor ved at flere norske og utenlandske borgere har behov for å gjennomføre ID-kontroll
Annet	• Forutsetter avklaring om hvorvidt ID-kontrollen skal gjennomføres mot et vederlag fra private tilbydere av eID

Tabell 12 Vurdering av alternativ løsning 4

3.5.5 Alternativ løsning 5: Jevnlig sjekke biometriske trekk ved hjelp av teknologiske løsninger ved bruk av eID-er

Alternativet bygger på alternativ løsning 2, beskrevet i kapittel 3.5.2, og innebærer å gjennomføre en jevnlig biometrisjekk av eID-brukere og sammenligning med brukers pass eller nasjonale ID-kort ved bruk av eID-er. Løsningen vil også kunne benyttes ved bruk av nasjonal eID med tofaktor-autentisering. Biometrisjekken vil gjøres ved at ansiktsbiometrien til bruker blir sammenlignet med ansiktsfoto som ligger lagret i pass eller nasjonalt ID-kort som brukeren har, og bidrar til å sikre at brukeren av eID-en er den rettmessige eieren av eID-en. Leverandøren anser at en slik løsning på sikt vil bidra til å sikre «unik» for brukere som benytter et norsk pass eller nasjonalt ID-kort for å gjennomføre biometrisjekken. Årsaken er at brukere ikke kan benytte norske pass og nasjonale ID-kort som er utgått for å gjennomføre biometrisjekken, og brukerne vil dermed måtte gå til anskaffelse av et nytt norsk pass eller nasjonalt ID-kort og dermed oppnå status «unik», for å kunne gjennomføre biometrisjekken og få tilgang til tjenester.

Tilsvarende som for alternativet beskrevet i kapittel 3.5.2 er PODs TOVE-løsning alternativ 1 og Vipps AS sin IDmee-løsning potensielle eksempler på løsninger som kan benyttes for å gjennomføre en slik biometrisjekk av bruker. Leverandøren har blitt gjort kjent med at det finnes en rekke potensielle tilbydere av denne typen løsninger og at markedet er i rask utvikling. Ett eksempel på et bruksområde for en slik løsning er at NAV er opptatt av å kunne verifisere om trygdemottakere i utlandet faktisk lever. En biometrisk kontroll via en digital tjeneste slik beskrevet over kan dekke dette behovet. Andre bruksområder er at Skatteetaten kan benytte en slik løsning for å kontrollere at én person ikke får utstedt skattekort i flere ulike identiteter og dermed forhindre tilfeller av skatteunndragelse, eller at Statens vegvesen kan kontrollere at personer som fornyer førerkort eller bytter inn et førerkort fra et EU/EØS-land er den rettmessige eieren av førerkortet.

Biometrisjekken kan eksempelvis gjøres som en tilleggsprosess i ID-porten for tilgang til utvalgte tjenester, slik visualisert i figuren under. Biometrisjekk som tilleggsprosess kan innføres enten basert på en risikobasert vurdering avhengig av tjenesten som

brukeren ønsker tilgang til, eller som en jevnlig sjekk fra ID-porten sin side. Leverandøren ser fordeler med en biometrisjekk som en tilleggsprosess, da det muliggjør bedre kontroll av utenlandske eID-er for tilgang til offentlige tjenester ved at disse brukerne benytter et ID-bevis med elektronisk brikke og biometrisk informasjon lagret i ID-beviset.

Alternativet vil både styrke sikkerheten for allerede utstedte eID-er og for eID-er som vil utstedes i fremtiden.

Figur 18 Kontroll av at bruker av eID er rettmessig eier ved sjekk biometriske trekk gjennom TOVE/IDmee

Sikkerhet	• Økt sikkerhet ved kontroll om brukeren av eID-en er den rettmessige eieren • Bruk av IDmee eller TOVE alternativ 1 vil øke sikkerheten ved at det sjekkes om brukeren innehar og benytter et ekte ID-bevis • Bruk av TOVE alternativ 1 vil øke sikkerheten ved at det sjekkes om benyttet ID-bevis er meldt tapt/mistet • Meget god løsning for å løse deler av utfordring I tilknyttet misbruk av eID-er der bruker ikke rettmessig eier
Brukervennlighet	• Noe redusert brukervennlighet ved at brukeren må ha pass eller nasjonalt ID-kort tilgjengelig for gjennomføring av biometrisjekk ved elektronisk autentisering for utvalgte tjenester
Ressursbruk	• Ingen vesentlige endringer

Tabell 13 Vurdering av alternativ løsning 5

3.5.6 Alternativ løsning 6: Øke kvalitet i Kontakt- og reservasjonsregisteret for å redusere digital sårbarhet, og informere befolkningen om sikker bruk av eID

Det offentlige har tilgang til innbyggernes digitale kontaktinformasjon gjennom Kontakt- og reservasjonsregisteret som forvaltes av Difi som en fellesløsning for offentlige virksomheter.[125] Den digitale kontaktinformasjon kan benyttes av offentlige virksomheter for å sende ut post og dokumenter elektronisk til befolkningen, hvor MinID kan benyttes som pålogging.[126] Når en bruker logger seg på med eID til en offentlig tjeneste blir brukerens digitale kontaktinformasjon registrert i Kontakt- og reservasjonsregisteret.[127] Brukere kan reservere seg mot digital kommunikasjon fra det offentlige, og vil dermed kun motta post og dokumenter per post.[128]

[125] Difi.no, «Difis fellesløsninger – Kontakt- og reservasjonsregisteret», 2019
[126] Difi.no, «Difis fellesløsninger – Kontakt- og reservasjonsregisteret», 2019
[127] Norge.no, «Oppdater kontaktinformasjon», 2019
[128] Norge.no, «Reservasjon», 2019

Ved å benytte den digitale kontaktinformasjonen som er registrert i Kontakt- og reservasjonsregisteret kan det offentlig effektiv kommunisere med store deler av befolkningen. Alternativet som beskrives her innebærer å øke kvaliteten i Kontakt- og reservasjonsregisteret slik at det offentlige raskt kan komme i kontakt med en størst mulig andel av befolkningen. I et tilfelle der eksempelvis BankID og Buypass sine løsninger ikke er tilgjengelig over lengre tid kan det offentlige benytte kontaktinformasjon fra registeret for å sende ut for eksempel engangskoder til befolkningen slik at de kan logge inn til offentlige tjenester. Dette vil redusere den digitale sårbarheten som eksisterer ved at det offentlige i stor grad er avhengig av én privat aktørs infrastruktur for eID. Leverandøren bemerker at eksempelvis utsendelse av engangskoder kun er en midlertidig løsning som kan benyttes dersom det skulle oppstå en situasjon der en stor del av befolkningen ikke har mulighet til å logge inn til offentlige tjenester med sine eID-er.

Videre innebærer alternativet å informere befolkningen om sikker bruk av eID for å bevisstgjøre om konsekvensen av misbruk. Dagens eID-løsninger har en relativt høy teknisk sikkerhet, og i mange misbrukstilfeller har brukeren selv gitt bort innloggingsdetaljer til sin eID, vitende eller uvitende, til personer som kan misbruke eID-en. Informasjon til befolkningen om sikker bruk av eID og oppfordring til å holde innloggingsdetaljer for eID skjult for andre, kan potensielt bidra til å redusere misbruk av eID-er.

Sikkerhet	• Redusert digital sårbarhet ved at størst mulig del av befolkningen kan nåes via digital kommunikasjon, og derav redusere utfordring II • Redusert misbruk av eID-er der brukeren har delt sine innloggingsdetaljer, vitende eller uvitende • Mindre god løsning for å løse deler av utfordring I tilknyttet misbruk av eID-er der bruker ikke rettmessig eier
Brukervennlighet	• Ingen vesentlige endringer
Ressursbruk	• Gjennomføring krever lite ressursbruk fra det offentlige

Tabell 14 Vurdering av alternativ løsning 6

3.5.7 Samlet vurdering av alternative løsninger til identifiserte utfordringer

Basert på vurderingene av de alternative løsningene i kapittel 3.5.1–3.5.6 anser leverandøren at følgende fire alternative løsninger har betydelige styrker for å løse utfordringer identifisert i kapittel 3.4.

- Alternativ løsning 1: Sette krav til norsk pass eller nasjonalt ID-kort, og status «unik» i Folkeregisteret, for utstedelse av private eID-er
- Alternativ løsning 2: Innføre biometrisjekk ved hjelp av teknologiske løsninger for økt sikkerhet i ID-kontroll ved utstedelse av private eID-er
- Alternativ løsning 4: Muliggjøre at ID-kontrollen som gjennomføres ved pass- og ID-kontor kan benyttes som grunnlag for utstedelse av private eID-er
- Alternativ løsning 5: Jevnlig sjekke biometriske trekk ved hjelp av teknologiske løsninger ved bruk eID-er

Innføring av alternativ løsning 1 vil sikre at brukere som får utstedt nye private eID-er har status «unik» i Folkeregisteret, og bidra til at det ikke blir mulig for en person å inneha fysiske ID-bevis i flere identiteter og redusere muligheten for at brukere kan anskaffe og benytte flere ulike eID-er i flere identiteter.

Innføring av alternativ løsning 2 vil bidra til å øke sikkerheten i ID-kontrollen ved at ektheten til det fremviste ID-beviset kontrolleres, det sikres at det er rettmessig eier som får utstedt den private eID-en, samt at én person forhindres fra å få utstedt private eID-er i flere ulike identiteter.

Innføring av alternativ løsning 4 vil gi økt sikkerhet ved at private eID-er utstedes med grunnlag i ID-kontroll utført av ansatte med høy ID-kompetanse ved et pass- og ID-kontor, samt at alle brukere som får utstedt en privat eID har status «unik» Folkeregisteret.

Innføring av alternativ løsning 5 vil øke sikkerheten ved bruk av private eID-er ved at det kontrolleres for at brukeren av den private eID-en er den rettmessige eieren, samt at løsningen vil kontrollere at ID-beviset som benyttes for å gjennomføre kontrollen er ekte. Ved TOVE alternativ 1 vil det i tillegg sjekkes om ID-beviset som benyttes for å gjennomføre kontrollen er meldt tapt eller mistet.

Alternativ løsning 1, 2 og 4 vil kun øke sikkerheten for utstedelse av norske eID-er, og vil ikke ha noen effekt på sikkerheten ved bruk av utenlandske eID-er dersom det åpnes for dette ved at norske eID-er meldes i henhold til eIDAS-forordningen. Alternativ løsning 5 vil derimot øke sikkerheten ved bruk av både norske eID-er og utenlandske eID-er, ettersom løsningen vil gjennomføres som en tilleggsprosess ved autentisering til offentlige tjenester gjennom ID-porten.

Alternativ løsning 3 om å styrke kompetansen på ID-kontroll ved postkontor/post i butikk/bankfilial anses ikke som et virkningsfullt alternativ for å øke sikkerheten ved utstedelse av private eID-er. Alternativ løsning 6 som innebærer å øke kvaliteten i Kontakt- og reservasjonsregisteret vil kun i begrenset grad redusere den digitale sårbarheten, og informasjon til befolkningen om sikker bruk av eID anses som et mindre virkningsfullt alternativ for å redusere misbruk av eID-er. Generelle informasjonskampanjer med videre bør trolig allikevel gjennomføres.

3.6 Vurdering av alternativ for nasjonal eID

Gitt at nasjonal eID har vært under planlegging og utvikling over lengre tid og at nåværende plan er at den vil lanseres mot slutten av 2021, setter dette visse begrensninger for vurderingen av de ulike alternativene under. Vurdering av alternativ for nasjonal eID er en krevende problemstilling, med mange potensielle innfallsvinkler og mye historie. Det finnes videre et relativt omfattende bakgrunnsmateriale og analyser, som det blant aktørene i ID-forvaltningen eksisterer ulike perspektiv på relevansen av.[129] Det er i dag et etablert marked for private eID-er, der én aktør har en dominerende posisjon med en eID-løsning som er svært utbredt og mye brukt ved tilgang til offentlige tjenester gjennom ID-porten. Leverandøren anser at det prinsipielt sett kunne vært fornuftig at det offentlige hadde et ansvar for å tilby sikker digital autentisering med eID til befolkningen. Et slikt frivillig eller obligatorisk tilbud hadde vært enklere å implementere om befolkningen ikke hadde et tilbud slik de har i dag. En tilnærming med krav hadde også vært vesentlig enklere om det for dagens eID-løsninger hadde vært vesentlige utfordringer i brukervennligheten, meget store dokumenterte sikkerhetsutfordringer eller høyt ressursbruk for bruker og forvaltning.

[129] POD og Difi, «Beslutningsgrunnlag for eID på nasjonalt ID-kort», 2016

Dagens situasjon medfører at et slikt prinsipielt tankesett kan være krevende å anvende.

Det har de siste årene vært en betydelig utvikling i eID-markedet, og det er krevende å forutse utviklingen i eID-markedet, både nasjonalt og internasjonalt. Eksempelvis har det i de seneste år vært en stor utvikling innen betalingstjenester med et tydelig grensesnitt mot ID- og tillitstjenester, eksempelvis tilknyttet «Payment services directive» (PSD2). Det er videre krevende å forutse både hvilke eID-løsninger private aktører, inkludert banknæringen, vil behøve og hvordan private tilbydere av eID vil utvikle sitt tilbud i fremtiden. Leverandøren anser videre at sterk volumutvikling i antall digitale autentiseringer[130] og digitalisering av tjenester[131] vil fortsette fremover, samt at det potensielt vil bli en fremvekst av nye globale aktører som leverandører av autentiseringsløsninger (eksempelvis fra Google, Apple, Facebook eller Amazon) eller fra telekommunikasjonsaktører. Gitt at markedet for eID-løsninger er under utvikling er det også krevende å forutse offentlig forvaltnings bruk av og behov for ulike eID-løsninger på lang sikt (mer enn ti år). Leverandøren legger til grunn at det i fremtiden vil være behov for digital autentisering i kommunikasjon med det offentlige for brukere, men anser at det er krevende å forutse hvilken form slike løsninger vil ta.

Gitt leverandørens mandat om å vurdere rollen til nasjonal eID opp mot private eID-løsninger beskrives og vurderes i det følgende alternativ for nasjonal eID, inkludert gjeldende politikk om å utstede nasjonal eID som et supplement til eksisterende eID-er i markedet. Vurderingene gjøres opp mot sikkerhet, brukervennlighet og ressursbruk, i tråd med mandatet for tilleggsoppdraget. Følgende alternativ for nasjonal eID er vurdert:

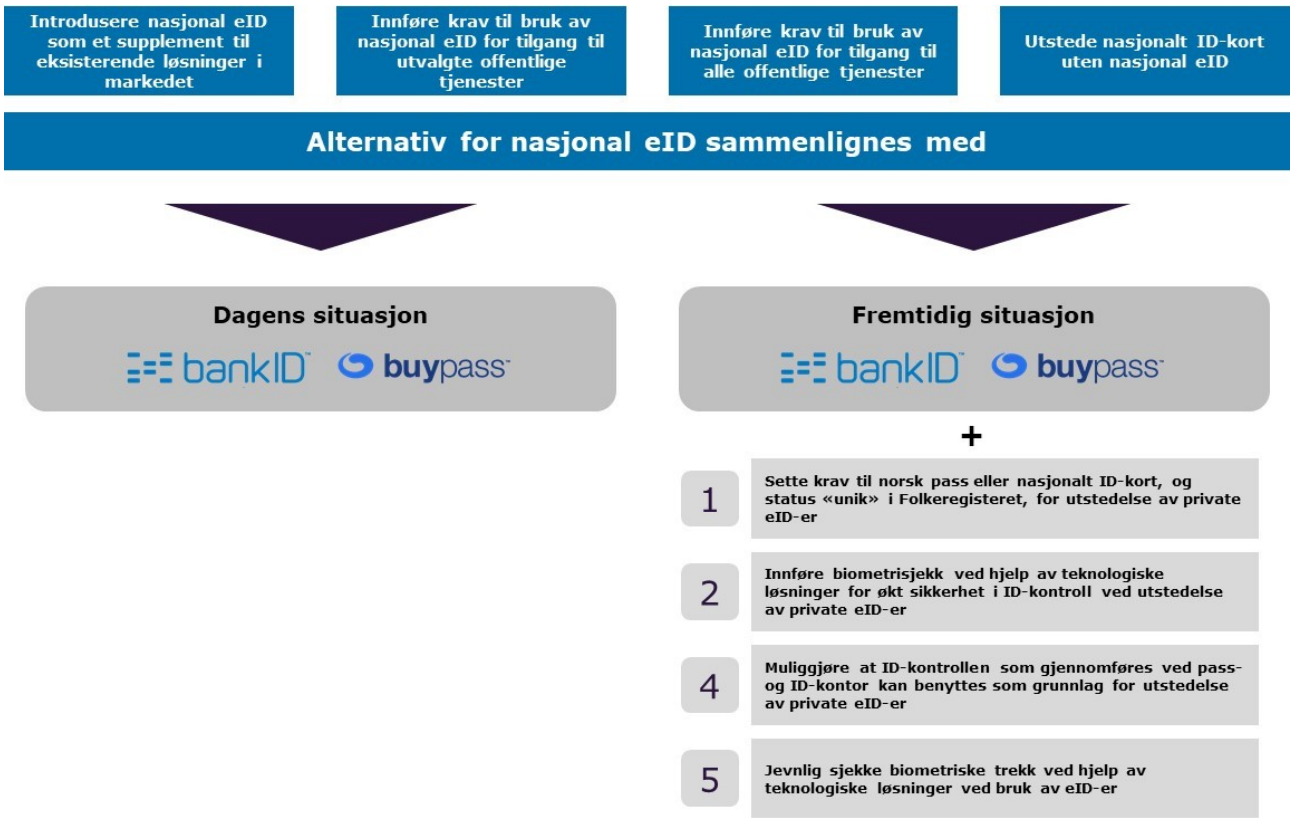
- Introdusere nasjonal eID som et supplement til eksisterende løsninger i markedet
- Innføre krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester
- Innføre krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester
- Utstede nasjonalt ID-kort uten nasjonal eID

Slik beskrevet i kapittel 3.5.7 anser leverandøren at innføring av fire følgende alternative løsninger vil gi betydelige styrker for både private eID-er og nasjonal eID og bidra til å løse utfordringer identifisert i kapittel 3.4:

- Alternativ løsning 1: Sette krav til norsk pass eller nasjonalt ID-kort, og status «unik» i Folkeregisteret, for utstedelse av private eID-er
- Alternativ løsning 2: Innføre biometrisjekk ved hjelp av teknologiske løsninger for økt sikkerhet i ID-kontroll ved utstedelse av private eID-er
- Alternativ løsning 4: Muliggjøre at ID-kontrollen som gjennomføres ved pass- og ID-kontor kan benyttes som grunnlag for utstedelse av private eID-er
- Alternativ løsning 5: Jevnlig sjekke biometriske trekk ved hjelp av teknologiske løsninger ved bruk av eID-er

[130] Antallet innlogginger i ID-porten har med over 400 prosent siden 2012. Kilde: Difi.no, «Nøkkeltall og statistikk», 2019
[131] Antallet tilgjengelige offentlige tjenester i ID-porten har 17-doblet seg siden 2012. Kilde: Difi.no, «Nøkkeltall og statistikk», 2019

Leverandøren vil i dette kapittelet vurdere alternativene for nasjonal eID nevnt over ved å sammenligne dem med henholdsvis **dagens situasjon** for private eID-er og en **fremtidig situasjon** der de utvalgte alternative løsningene 1, 2 og 4 nevnt over implementeres for private eID-er og alternativ løsning 5 for private eID-er og nasjonal eID. Figuren under viser sammenligningsgrunnlaget som leverandøren benytter for å vurdere de ulike alternativene for nasjonal eID.



Figur 19 Oversikt over sammenligningsgrunnlag for vurdering av alternativ for nasjonal eID

Implementering av de alternative løsningene i fremtidig situasjon i figuren vil medføre noe økt ressursbruk for det offentlige, men i vurderingen av alternativ for nasjonal eID vil ikke den økte ressursbruken ha innvirkning på evaluering av alternativene. Leverandøren antar videre at den teknologiske løsningen for sjekk av biometriske trekk vil kunne benyttes både ved bruk av nasjonal eID og private eID-er.

Vurdering av de ulike alternativene for nasjonal eID gjøres etter «pluss-minusmetoden», slik beskrevet i kapittel 1.[132] Hvert alternativ gis en konsekvens som er endringen sammenlignet med henholdsvis dagens situasjon for private eID-er og fremtidig situasjon, og vurderes ved hjelp av en skala basert på plusser og minuser.

[132] Direktoratet for økonomistyring, «Veileder i samfunnsøkonomiske analyser», 2018

3.6.1 Vedrørende forvaltningens rolle for utstedelse av ID-bevis i det fysiske og digitale rom

I følge NOU 2019:5 skal forvaltningen sikre befolkningens grunnleggende velferd og tilby fellestjenester. Dette for å sikre at infrastruktur og tjenester finnes, samt fremme likhet mellom innbyggere. Det varierer mellom sektorer, over tid og med politisk ledelse i hvilken grad tjenestetilbud gis av det offentlige eller av det private.[133]

I det fysiske rom belager forvaltningen seg i dag på en kombinasjon av egenutstedte fysiske ID-bevis som pass og førerkort, samt private ID-bevis som bankkort, hvorav alle disse ID-bevisene betraktes som gyldige for de fleste tjenester og ytelser. Dette er nærmere beskrevet i hovedrapporten. Med anbefalingen om tydeliggjøre at norsk pass og nasjonalt ID-kort utgjør gyldige ID-bevis utstedt av norske myndigheter, vil forvaltningen belage seg på egenutstedte ID-bevis. For ID-bevis utstedt både av forvaltningen og av private/banker er ofte private aktører leverandører av selve ID-dokumentene og ansvarlig for forsendelsen til forbruker. Eventuelle forskjeller i utstedelsen ligger i hvem som har ansvar for prosessene, myndighetsutøvelse og regulering.

Slik beskrevet i kapittel 3.1.1 belager forvaltningen seg i stor grad på private eID-løsninger utover MinID for autentisering. Forvaltningen har riktignok eierskap til regulering og ID-porten for felles innlogging og autentisering til offentlige tjenester. Slik beskrevet i hovedrapporten er denne tilnærmingen velfungerende. Identitetstildeling med tilhørende identitetsnummer og identitetsforvaltning i Folkeregisteret er definert som en statlig oppgave.

Det er riktignok mulig å argumentere for at forvaltningen bør ha en lik rolle for utstedelse av ID-bevis i det fysiske og digitale rom. Det vil si at staten har samme tilnærming for fysiske og elektroniske ID-bevis, enten ved å fullstendig belage seg på egenutstedte ID-bevis og/eller private ID-bevis. Leverandøren har ikke noe prinsipielt synspunkt tilknyttet en slik argumentasjon.

Leverandøren bemerker imidlertid at det er særdeles sjeldent staten som rettssubjekt går inn i et eksisterende marked med hensikt å tilby supplerende løsninger eller for å stimulere til økt konkurranse. Leverandøren har ikke identifisert gode eksempler på dette. Det finnes riktignok en lang rekke historiske eksempler på at staten har deregulert et marked, eksempelvis post- og pakketransport, luftfart, gods- og persontogtransport, telefoni, drift av vei, og apotek. Videre er forvaltningens tjenesteproduksjon i mange tilfeller skilt ut i rettssubjekt utenfor staten, og i mange tilfeller delprivatisert og/eller solgt. Det finnes også enkelte eksempler der det offentlige har hatt motsatt tilnærming ved å fullstendig ta over tjenesteproduksjon fra private aktører, særlig i kommunal sektor.

3.6.2 Introdusere nasjonal eID som et supplement til eksisterende løsninger i markedet

Helt siden arbeidet med nasjonal eID startet opp har det vært lagt til grunn at nasjonal eID skal utstedes som et supplement til eksisterende eID-løsninger i markedet, hvilket fortsatt er gjeldende politikk, og leverandøren er ikke gjort kjent med at det underveis i arbeidet har eksistert en annen strategi for nasjonal eID.[134] Det vil si at nasjonal eID skal kunne benyttes på lik linje med eksisterende eID-løsninger på høyeste sikkerhetsnivå i ID-porten, som BankID og Buypass, og dermed gi brukerne en

[133] Backer et al., «NOU 2019:5 Ny forvaltningslov — Lov om saksbehandlingen i offentlig forvaltning», 2019
[134] JD, «Sluttrapport – Nasjonalt ID-kort», 2007

ytterligere valgmulighet for hvilken eID de ønsker å benytte for sikker digital autentisering til offentlige tjenester.[135] Det vil videre være opp til hver enkelt privat tjenesteeier å avgjøre om de ønsker å integrere nasjonal eID med sine tjenester.[136]

Gitt øvrige vurderinger i kapittel 2 antas det i vurderingen av alternativet at en betydelig andel norske borgere, EØS-borgere og tredjelandsborgere over en femårsperiode vil disponere en nasjonal eID. Samtidig antar leverandøren at en betydelig andel kun vil disponere private eID-er da mange norske borgere vil benytte pass som ID-bevis, samt at private eID-er vil dominere samlet bruk i samfunnet for sikker digital autentisering. I det følgende vurderer leverandøren styrker og utfordringer ved en slik tilnærming.

Vurdering – sikkerhet

*Sammenlignet med **dagens situasjon** vil en supplementtilnærming for nasjonal eID ha ubetydelig/ingen konsekvens med tanke på sikkerhet, da nasjonal eID kun vil ha økt sikkerhet i utstedelsesprosessen, og brukere står fritt til å benytte eksisterende eID-løsninger.*

Nasjonal eID i tilknytning til nasjonalt ID-kort vil bety at eieren av eID-en har status «unik» i Folkeregisteret og tjenesteeiere kan potensielt benytte denne informasjonen for å vite at brukere som autentiserer seg med nasjonal eID har gjennomgått en sterk ID-kontroll ved et pass- og ID-kontor. Opptak av biometri og status «unik» ved utstedelse vil også sikre at én person kun kan få utstedt én nasjonal eID i én identitet, hvilket vil bidra til å øke sikkerheten ved utstedelse av nasjonal eID. Brukere som velger å anskaffe og benytte nasjonal eID tilknyttet det nasjonale ID-kortet vil dermed ha en god mulighet til å bevise sin identitet både fysisk og digitalt. Leverandøren presiserer at sikkerheten kun vil styrkes for brukere som disponerer og benytter en nasjonal eID.

En supplementtilnærming betyr at befolkningen står fritt til å velge om de ønsker å benytte eksisterende eID-løsninger eller nasjonal eID for å identifisere seg digitalt. Brukere som velger å benytte en annen eID vil dermed unngå å gjennomgå ID-kontrollen med økt sikkerhet ved et pass- og ID-kontor for utstedelse av nasjonal eID, og samtidig ha tilgang til de samme offentlige, og potensielt private, tjenester. Så lenge det eksisterer andre eID-løsninger i markedet og nasjonal eID innføres supplement, vil bidraget til samlet sikkerhet være særdeles begrenset.

Selv om sikkerheten ved utstedelsen av det nasjonale ID-kortet med eID vil være sterkere enn ved dagens private eID-er, vil ikke sikkerheten ved bruk av den nasjonale eID-en være sterkere enn for eksisterende eID-løsninger. En nasjonal eID vil kunne misbrukes av en person som ikke er rettmessig eier, slik som for eksisterende eID-er, så lenge det ikke eksisterer kontrollmekanismer som kan avdekke slik misbruk.

Nasjonal eID er videre tiltenkt å kunne benyttes for å utstede private eID-er.[137] Leverandøren anser at en slik løsning kan ha en positiv effekt på sikkerheten ved utstedelsen av private eID-er, men en supplementtilnærming for nasjonale eID vil sette vesentlige begrensninger for økt sikkerhet. For at sikkerheten skal øke må det eventuelt stilles et krav til at private eID-er kun skal kunne utstedes gjennom bruk av nasjonal eID og det må være stor utstedelse og bruk av nasjonal eID for at løsningen skal ha effekt på sikkerheten i utstedelsesprosessen. Dersom det kun er et alternativ å bruke

[135] POD og Difi, «Beslutningsgrunnlag for eID på nasjonalt ID-kort: Forholdet til nivå 4 e-IDer i markedet, delleveranse 5», 2016
[136] POD og Difi, «Beslutningsgrunnlag for eID på nasjonalt ID-kort: Forholdet til nivå 4 e-IDer i markedet, delleveranse 5», 2016
[137] POD og Difi, «Beslutningsgrunnlag for eID på nasjonalt ID-kort: Konseptbeskrivelse, delleveranse 3», 2016

nasjonal eID for utstedelse av private eID-er, vil brukere kunne få utstedt private eID-er på samme måte som det gjøres i dag, med lavere sikkerhet i utstedelsesprosessen.

Slik beskrevet i kapittel 3.4.3 vil avhengighet av en dominerende aktørs infrastruktur være en digital sårbarhet ved dagens løsning for eID-er og tilgang til offentlige tjenester på høyeste sikkerhetsnivå.[138] Denne digitale sårbarheten vil reduseres ved at nasjonal eID tilbys som en alternativ løsning til eksisterende eID-løsninger. Nasjonal eID vil kunne fungere som en reserveløsning eksempelvis ved langvarige driftsproblemer hos private løsninger. Styrken i et slikt argument fordrer imidlertid stor utbredelse av nasjonalt ID-kort med eID. I tillegg argumenterer Difi for at MinID benyttes i perioder der eksempelvis BankID ikke er tilgjengelig, hvilket reduserer den digitale sårbarheten ved å være avhengig av én infrastruktur. Kontakt- og reservasjonsregisteret kan også benyttes som reserveløsning, og muliggjør eksempelvis utsendelse av engangspassord til brukere dersom BankID skulle være utilgjengelig over en lengre periode.

Ettersom en supplementtilnærming ikke vil stille noen krav til bruk av nasjonal eID, er det en risiko for at utbredelsen og bruken av en nasjonal eID blir lav. Reduksjonen i digital sårbarhet ved å innføre nasjonal eID som en alternativ infrastruktur og eID-løsning vil videre være begrenset ved lav utbredelse og bruk av nasjonal eID.

*Sammenlignet med **fremtidig situasjon** for private eID-er vil en supplementtilnærming for nasjonal eID ha ubetydelig/ingen konsekvens for sikkerheten samlet sett, da utstedelsen av private eID-er vil være omtrent like sikker som for nasjonal eID og nasjonal eID ikke tilfører noe til sikkerheten i bruksfasen. Den digitale sårbarheten reduseres imidlertid noe ved å introdusere nasjonal eID som supplement*

Nasjonal eID vil som beskrevet over ha høyere sikkerhet i utstedelsesprosessen, men i fremtidig situasjon med gjenbruk av ID-kontroll fra pass- og ID-kontor, krav om norsk pass eller nasjonalt ID-kort og biometrisjekk av bruker ved utstedelse av private eID-er vil sikkerheten i utstedelsesprosessen for private eID-er være omtrent like høy.

Videre vil det i fremtidig situasjon jevnlig sjekkes biometriske trekk ved hjelp av teknologiske løsninger ved bruk av både nasjonal eID og private eID-er, slik at sikkerheten ved bruk ikke vil øke ved introduksjon av nasjonal eID som et supplement isolert sett.

Den digitale sårbarheten som eksisterer ved å være avhengig av en dominerende aktørs infrastruktur vil kun reduseres noe ved at nasjonal eID introduseres som et supplement til eksisterende løsninger, da et slikt argument fordrer stor utbredelse av nasjonal eID.

Vurdering – brukervennlighet

*Sammenlignet med **dagens situasjon og fremtidig situasjon** vil en supplementtilnærming for nasjonal eID ha ubetydelig/ingen konsekvens for brukervennligheten for eID-er, da nasjonal eID anses å ha lavere brukervennlighet enn eksisterende eID-løsninger, men brukere står fritt til å benytte eksisterende løsninger.*

Leverandøren er ikke gjort kjent med eller sett dokumentasjon på brukerreiser eller bruksområder for nasjonal eID som tyder på at brukervennligheten ved løsningen vil være slik at brukere vil velge å benytte den nasjonale eID-en fremfor eksisterende løsninger. Leverandøren anser at den foreslåtte løsningen for nasjonal eID vil være mindre brukervennlig ettersom bruker må ha med seg det nasjonale ID-kortet for å

[138] Lysne et al., «NOU 2015:13, Digital sårbarhet – sikkert samfunn», 2015

autentisere seg, og potensielt gå til anskaffelse av en smartkortleser til PC dersom brukerens mobil ikke har støtte for NFC[139]. Gitt manglende planlagt ressursbruk til videreutvikling av nasjonal eID, manglende gjennomføringskraft i gjennomføring av NPID-programmet, samt stadige teknologiske nyvinninger vurderer leverandøren at det er usannsynlig at POD vil klare å levere like brukervennlige løsninger som private eID-leverandører over tid.

Slik beskrevet i kapittel 3.4.2 er det enkelte brukergrupper som i dag ikke har mulighet til å få utstedt private eID-er. Nasjonal eID vil imidlertid ikke løse denne utfordringen, da *«Buypass og Commfides vil kunne ha samme dekning som eID på nasjonalt ID-kort»*.[140] Aldersgrensen for nasjonal eID vil være 13 år, tilsvarende BankID og Buypass.[141] Følgelig vil barn under 13 år ikke ha mulighet til å identifisere seg sikker digitalt selv etter lansering av nasjonal eID. Videre vil personer som ikke har et gyldig fysisk ID-bevis og per dags dato ikke har mulighet til å bevise sin identitet, kunne få utstedt et nasjonalt ID-kort som følge av vurderinger gitt i kapittel 2. Ved at denne brukergruppen får et nasjonalt ID-kort kvalifiserer de også de til å få utstedt en privat eID, da de kan bevise sin identitet gjennom det nasjonale ID-kortet. Brukergruppen vil imidlertid kunne få utstedt nasjonalt ID-kort med nasjonalt eID i ett og samme oppmøte, hvilket betyr at brukervennligheten for disse brukerne øker ved å innføre nasjonal eID. Samlet sett vil nasjonal eID i begrenset grad bidra til å muliggjøre sikker digital autentisering for brukergruppene beskrevet i kapittel 3.4.2, og vil ha liten effekt på brukervennligheten i denne sammenheng.

For enkelte brukergrupper vil det imidlertid kunne være mer brukervennlig å få utstedt en nasjonal eID samtidig som en får utstedt et pass eller nasjonalt ID-kort, og dermed slippe et ekstra oppmøte ved en bankfilial eller postkontor/post i butikk.

Vurdering – ressursbruk

*Sammenlignet med **dagens situasjon og fremtidig situasjon** vil en supplementtilnærming for nasjonal eID ha middels negativ konsekvens for det offentliges ressursbruk, da innføring, drift, vedlikehold og videreutvikling av nasjonal eID vil medføre betydelige kostnader.*

Ved å tilby nasjonal eID som et supplement vil det offentlige etablere en infrastruktur som vil fungere parallelt med eksisterende løsningers infrastruktur. Det kan argumenteres for at det er ineffektivt og ressurskrevende å bygge en parallell infrastruktur for å tilby nasjonal eID. POD argumenterer for at store deler av investeringskostnaden til nasjonal eID allerede er tatt, og at det er begrenset behov for ytterlige investeringskostnader for å kunne lansere nasjonal eID. Videre argumenter POD for at det er store synergier ved å utnytte felles miljø for sertifikatinfrastruktur som er kjernen i eID-myndighetsutøvelsen sammen med utstedelsesprosessen for pass og nasjonalt ID-kort.

Videre er leverandøren kjent med at private tilbydere har vesentlige årlige kostnader til drift og videreutvikling av sine infrastrukturer. Etter leverandørens vurdering er kostnader til årlig drift av infrastrukturen for nasjonal eID betydelig underestimert i PODs gebyrmodell, sammenlignet med erfaringer fra private tilbydere. I tillegg inngår ikke kostnader til videreutvikling av løsningen i gebyrmodellen. Leverandøren anser at det er en risiko for at manglende midler til videreutvikling vil føre til at nasjonal eID som løsning ikke vil være et reelt alternativ til eksisterende eID-løsninger i fremtiden eller at ytterligere kostnader vil påløpe for å besørge videreutvikling.

[139] Near Field Communication
[140] POD og Difi, «Beslutningsgrunnlag for eID på nasjonalt ID-kort: Forholdet til nivå 4 e-IDer i markedet, delleveranse 5», 2016
[141] JD, «Høring – forslag til forskrift om pass og nasjonalt ID-kort», 2019

Innføringsdatoen for nasjonale ID-kort har blitt utsatt flere ganger og kostnadene har økt betydelig fra de opprinnelige estimatene. Dette gjelder også for nasjonal eID og gir leverandøren i liten grad tillit til at planlagte kostnadsestimat for fremtidig drift, forvaltning og ingen videreutvikling reelt sett vil overholdes.

Samlet vurdering

Tabellen under oppsummerer leverandørens vurdering av å innføre nasjonal eID som et supplement til eksisterende løsninger i markedet, sammenlignet med henholdsvis dagens situasjon og fremtidig situasjon for private eID-er.

Alternativ	Sammenlignet med	Konsekvens		
		Sikkerhet	Bruker-vennlighet	Ressursbruk
Introdusere nasjonal eID som et supplement til eksisterende løsninger i markedet	Dagens situasjon	0	0	--
	Fremtidig situasjon	0	0	--

Tabell 15 Vurdering av å introdusere nasjonal eID som et supplement til eksisterende løsninger i markedet

3.6.3 Innføre krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester

Alternativet innebærer å stille krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester. Et slikt krav vil medføre at digital autentisering til de aktuelle tjenestene ikke er mulig å gjennomføre med de eksisterende eID-løsningene i markedet. For å avgjøre hvilke offentlige tjenester som skal omfattes av et slikt krav, anser leverandøren det som hensiktsmessig at tjenesteeierne selv gjennomfører en risikobasert vurdering av de offentlige tjenester som er tilgjengelig gjennom ID-porten i dag.

Gitt krav om nasjonal eID for tilgang til utvalgte offentlige tjenester antas det i vurderingen av alternativet at en betydelig andel norske borgere, EØS-borgere og tredjelandsborgere vil disponere en nasjonal eID for å kunne få tilgang til de utvalgte tjenestene. Videre antas det at en betydelig andel av befolkningen vil disponere en privat eID, og at private eID-er vil benyttes til majoriteten av tjenester som ikke er omfattet av et krav til bruk av nasjonal eID. Leverandøren antar i tillegg at andelen av offentlige tjenester som vil være omfattet av et krav til bruk av nasjonal eID vil være relativt lavt, og at private eID-er vil dominere samlet bruk i samfunnet for sikker digital autentisering. I det følgende vurderer leverandøren styrker og utfordringer ved å innføre krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester.

Vurdering – sikkerhet

*Sammenlignet med **dagens situasjon** vil innføring av et krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester ha middels positiv konsekvens for sikkerheten samlet sett, da sikkerheten vil øke noe for de tjenestene som er omfattet av et krav til bruk av nasjonal eID og den digitale sårbarheten reduseres.*

Ved å innføre krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester vil tjenesteeier og det offentlige være sikker på at brukeren som har tilgang til tjenesten har gjennomført en ID-kontroll ved et pass- og ID-kontor, avgitt biometri og har status

«unik». Flere aktører i ID-forvaltningen argumenter for at dette vil øke sikkerheten ved tilgang til de utvalgte tjenestene, og at det kan være formålstjenlig å vite at brukere som har tilgang har status «unik» og ikke opptrer med eID-er i flere identiteter.

Selv om sikkerheten ved utstedelsen av nasjonal eID vil være sterkere enn for eksisterende eID-er i markedet, er det viktig å bemerke at nasjonal eID ikke vil øke sikkerheten ved bruk. Nasjonal eID vil være like utsatt for misbruk der brukeren av eID-en ikke er rettmessig eier som de eksisterende eID-ene i markedet. Videre vil utstedelse av private eID-er gjennom bruk av nasjonal eID være utsatt for misbruk der en person kan benytte en annens nasjonale eID for å få utstedt en privat eID.

Slik beskrevet i kapittel 3.2 planlegges nasjonal eID meldt på eIDAS sikkerhetsnivå «høyt». Dette medfører at utenlandske eID-er meldt på eIDAS «høyt» kan benyttes, og må anerkjennes, for autentisering til de norske offentlige tjenester som nasjonal eID gir tilgang til. Et krav om nasjonal eID for tilgang til utvalgte offentlige tjenester vil dermed kunne omgås av brukere som har en utenlandsk eID på eIDAS «høyt», og vil i praksis kun ha en effekt for brukere som ikke har en utenlandsk eID på eIDAS «høyt». Dersom nasjonal eID ikke meldes i henhold til eIDAS-forordningen og det likevel settes krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester faller denne problemstillingen bort, men medfører at EØS-borgere ikke kan benytte en meldt eID fra sitt hjemland for tilgang til de utvalgte offentlige tjenestene.

Dersom nasjonal eID i en lengere periode er utilgjengelig for bruk grunnet eksempelvis tekniske problemer, vil de utvalgte tjenester som er omfattet av et krav være utilgjengelige for alle brukere og den digitale sårbarheten er dermed høy. Leverandøren anser det imidlertid som sannsynlig at det gjennom ID-porten kan åpnes for bruk av private eID-er eller MinID for tilgang til de utvalgte tjenestene dersom nasjonal eID skulle være utilgjengelig. Følgelig vil den digitale sårbarheten som eksisterer ved å være avhengig av en dominerende aktørs infrastruktur reduseres ved at det settes krav til nasjonal eID for utvalgte tjenester, og sikkerheten vil øke samlet sett.

Fra POD og Difi sin behovsundersøkelse for nasjonal eID fra 2016 fremkommer det at fire av 25 offentlige tjenesteeiere som besvarte undersøkelsen, Skatteetaten, Helsedirektoratet, Statens innkrevingssentral og politiet, ser et behov for et *«sikkerhetsnivå utover sikkerhetsnivå 4»*.[142] Behovsundersøkelsen virker ikke å ha beskrevet sikkerhetsnivåene i tilstrekkelig grad for at etatene på en god måte skal kunne uttale seg om behovet for en eID på et høyere sikkerhetsnivå enn nivå 4. Behovsundersøkelsen skisserer heller ikke hva et eventuelt sikkerhetsnivå utover sikkerhetsnivå 4 kan tenkes å inneholde eller bidra med i sikkerhetsøyemed.

Skatteetaten begrunner blant annet behovet med at det ved dagens eID-løsninger ikke er noen *«god sammenheng mellom fysisk person og digital ID»* og at *«det er en styrke å ha biometri og eID i samme kort»*. Utstedelse av nasjonal eID med opptak av biometri og en-til-mange søk vil sikre status «unik» for personen som får utstedt den nasjonale eID-en, men det vil ikke være noen knytning mellom den fysiske personen og den nasjonale eID-en i bruksfasen slik løsningen er skissert i dag. Helsedirektoratet begrunner behovet med at norske sikkerhetsnivåer må harmonere med de sikkerhetsnivåer som benyttes i eIDAS-forordningen. Slik beskrevet i kapittel 3.2 likestiller den nye selvdeklarasjonsforskriften norske sikkerhetsnivåer med de benyttet i eIDAS-forordningen. Politiet og Statens innkrevingssentral begrunner behovet med at det eksisterer svakheter i utstedelsesprosessen for private eID-er og at det forekommer misbruk ved bruk av private eID-er. Dette er utfordringer som er beskrevet i kapittel 3.4 og adressert med alternative løsninger i kapittel 3.5.

[142] POD og Difi, «Beslutningsgrunnlag for eID på nasjonalt ID-kort: Kartlegging – offentlige tjenesteeiere, delleveranse 8», 2016

Leverandøren har i møter med flere sentrale tjenesteeiere ikke oppfattet et behov for et høyere sikkerhetsnivå enn sikkerhetsnivå 4, utover de utfordringer som er beskrevet i kapittel 3.4. Tjenesteeierne er opptatt av å løse de utfordringer som beskrives i kapittel 3.4, men ingen av tjenesteeierne, med unntak av politiet, har slik leverandøren forstår det et spesifikt ønske om et krav om nasjonal eID for å løse disse utfordringene.

*Sammenlignet med **fremtidig situasjon** for private eID-er vil innføring av et krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester ha liten positiv konsekvens for sikkerheten samlet sett, da sikkerheten for private eID-er øker og den digitale sårbarheten reduseres.*

Nasjonal eID vil som beskrevet over ha høy sikkerhet i utstedelsesprosessen og et krav om bruk av nasjonal eID for tilgang til utvalgte tjenester vil sikre at kun brukere som har gått gjennom den sikre utstedelsesprosessen har tilgang til tjenestene. I fremtidig situasjon der ID-kontrollen fra pass- og ID-kontor kan benyttes som grunnlag for utstedelse av privat eID-er eller krav om norsk pass eller nasjonalt ID-kort og biometrisjekk av bruker innføres ved utstedelse av private eID-er, vil imidlertid sikkerheten i utstedelsesprosessen for private eID-er være omtrent like høy.

Videre vil det i fremtidig situasjon jevnlig sjekkes biometriske trekk ved hjelp av teknologiske løsninger ved bruk av både nasjonal eID og private eID-er, slik at sikkerheten ved bruk ikke vil øke ved å innføre krav om nasjonal eID for tilgang til utvalgte tjenester isolert sett.

For de offentlige tjenestene som omfattes av et krav til bruk av nasjonal eID vil den digitale sårbarheten øke ettersom kun nasjonal eID er tilgjengelig for digital autentisering. Leverandøren anser det imidlertid som sannsynlig at det gjennom ID-porten kan åpnes for bruk av private eID-er for tilgang til de utvalgte tjenestene dersom nasjonal eID skulle være utilgjengelig. Følgelig vil den digitale sårbarheten som eksisterer ved å være avhengig av én dominerende aktørs infrastruktur reduseres ved at det settes krav til nasjonal eID for utvalgte tjenester, og sikkerheten vil øke samlet sett.

Vurdering – brukervennlighet

*Sammenlignet med **dagens situasjon og fremtidig situasjon** vil innføring av et krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester ha stor negativ konsekvens for brukervennligheten, da all autentisering til de utvalgte tjenestene må gjøres med nasjonal eID som etter leverandørens vurdering fremstår som en lite brukervennlig eID-løsning og som det er lav etterspørsel etter.*

Leverandøren ser en stor risiko i brukerdimensjonen ved å innføre et krav om bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester. Et krav om at samtlige påloggingar til de utvalgte offentlige tjenestene skal gjennomføres med nasjonal eID krever at en stor andel av befolkningen «konverteres» fra å bruke eksisterende eID-løsninger. Eksisterende løsninger oppleves fra et brukerperspektiv å fungere godt, mens nasjonal eID etter leverandørens vurdering fremstår som mindre brukervennlig, sik beskrevet i kapittel 3.6.2. Et krav om bruk av nasjonal eID for utvalgte tjenester vil potensielt påtvinge lavere brukervennlighet for en stor andel av befolkningen, avhengig av hvilke og hvor mange offentlige tjenester som vil omfattes av et krav. POD og Difi sin sluttbrukerundersøkelse viser at 82 prosent av respondentene ønsker å benytte samme eID til all innlogging ved både offentlige og private tjenester, og at BankID er den foretrukne eID-løsningen.[143]

[143] POD og Difi, «Beslutningsgrunnlag for eID på nasjonalt ID-kort: Kartlegging – sluttbrukere, delleveranse 11», 2016

Dersom nasjonal eID ikke blir benyttet for sikker digital autentisering og tilgang til andre tjenester enn de utvalgte offentlige tjenestene, kan potensielt bruken av nasjonal eID ende med å ikke være tilstrekkelig til å sikre at befolkningen blir komfortable med å benytte løsningen. Den nasjonale eID-en kan dermed ende med å bli en løsning som oppfattes å ha svært lav brukervennlighet og som kun vil benyttes av brukere i de få tilfeller der det stilles et krav om det. Gitt manglende planlagt ressursbruk til videreutvikling av nasjonal eID, manglende gjennomføringskraft i gjennomføring av NPID-programmet, samt stadige teknologisk nyvinninger vurderer leverandøren at det er usannsynlig at POD vil klare å levere like brukervennlige løsninger som private eID-leverandører over tid.

Vurdering - ressursbruk

*Sammenlignet med **dagens situasjon og fremtidig situasjon** vil innføring av et krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester ha middels negativ konsekvens for det offentliges ressursbruk, da innføring, drift, vedlikehold og videreutvikling av nasjonal eID vil medføre betydelige kostnader.*

Ved å sette krav til bruk av nasjonal eID for utvalgte offentlige tjenester vil det offentlige etablere en infrastruktur som i stor grad vil fungere parallelt med eksisterende løsningers infrastruktur for de tjenester som ikke er omfattet av kravet, hvilket er ressurskrevende og potensielt ineffektivt. Slik beskrevet i kapittel 3.6.2 vurderer leverandøren at kostnader til årlig drift av infrastrukturen for nasjonal eID er betydelig underestimert i PODs gebyrmodell, sammenlignet med erfaringer fra private tilbydere. I tillegg inngår ikke kostnader til videreutvikling av løsningen i gebyrmodellen. Leverandøren anser at det er en risiko for at manglende midler til videreutvikling vil føre til at nasjonal eID som løsning ikke vil ha tilstrekkelig sikkerhet i fremtiden eller at ytterligere kostnader vil påløpe for å besørge videreutvikling.

Et krav om nasjonal eID for utvalgte offentlige tjenester vil potensielt føre til økt ressursbruk for det offentlige da det er kritisk at nasjonal eID som eneste godkjente løsning har god tilgjengelighet og kan håndtere periodevis stor pågang fra brukere for autentisering til utvalgte tjenester.

Samlet vurdering

Tabellen under oppsummerer leverandørens vurdering av å innføre krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester, sammenlignet med henholdsvis dagens situasjon og fremtidig situasjon for private eID-er.

Alternativ	Sammenlignet med	Konsekvens		
		Sikkerhet	Bruker-vennlighet	Ressursbruk
Innføre krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester	Dagens situasjon	++	---	--
	Fremtidig situasjon	+	---	--

Tabell 16 Vurdering av å innføre krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester

3.6.4 Innføre krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester

Alternativet innebærer å sette krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester. Et slikt krav vil medføre at digital autentisering til offentlige tjenester ikke lenger er mulig å gjennomføre med de eksisterende eID-løsningene i markedet.

Gitt krav om bruk av nasjonal eID for tilgang til alle offentlige tjenester antas det i vurderingen av alternativet at majoriteten av norske borgere, EØS-borgere og tredjelandsborgere som har rett på offentlige tjenester og ytelser vil disponere en nasjonal eID. Videre antas det at en betydelig andel av befolkningen vil disponere en privat eID og at disse vil benyttes for majoriteten av digitale autentiseringer til private tjenester. I det følgende vurderer leverandøren styrker og utfordringer ved å innføre krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester.

Vurdering – sikkerhet

*Sammenlignet med **dagens situasjon** vil innføring av et krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester ha liten positiv konsekvens på sikkerheten samlet sett, da alle digitale autentiseringer til offentlige tjenester vil gjøres med en nasjonal eID som er koblet til et identitetsnummer som har status «unik». Den digitale sårbarheten reduseres imidlertid ved å innføre krav til nasjonal eID for alle tjenester.*

Slik beskrevet i kapittel 3.6.2 og 3.6.3 vil utstedelsesprosessen for nasjonal eID være sikrere enn for de eksisterende eID-løsningene i markedet. Utstedelsesprosessen vil sikre at brukeren har status «unik», samt at én person kun kan få utstedt én nasjonal eID, i én identitet.

Et krav om bruk av nasjonal eID for tilgang til alle offentlige tjenester vil videre tette sikkerhetshullene som eksisterer ved at private eID-er, som har en lavere sikkerhet i utstedelsesprosessen, kan benyttes på lik linje med nasjonal eID for tilgang til alle offentlige tjenester. Sikkerheten ved bruk av nasjonal eID vil imidlertid være sårbar for misbruk der brukeren av nasjonal eID ikke er den rettmessige eier.

Utstedelse av private eID-er gjennom nasjonal eID vil kunne sikre at én person kun kan få utstedt private eID-er koblet til ett unikt identitetsnummer, men dette fordrer imidlertid at det er et krav om at utstedelse av private eID-er kun kan gjøres gjennom nasjonal eID. Ettersom sikkerheten ved bruk av nasjonal eID ikke er høyere enn for dagens eksisterende løsninger, vil det imidlertid være rom for misbruk der en ikke-rettmessig eier benytter en annen persons nasjonale eID for å få utstedt en privat eID.

Innføring av et krav om bruk av nasjonal eID for tilgang til alle offentlige tjenester vil øke den digitale sårbarheten ved sikker digital autentisering til offentlige tjenester dersom nasjonal eID i en lengere periode er utilgjengelig grunnet eksempelvis tekniske problemer. Leverandøren anser det imidlertid som sannsynlig at det gjennom ID-porten kan åpnes for bruk av private eID-er eller MinID for tilgang til de utvalgte tjenestene dersom nasjonal eID skulle være utilgjengelig. Følgelig vil den digitale sårbarheten som eksisterer ved å være avhengig av en dominerende aktørs infrastruktur reduseres ved at det settes krav til nasjonal eID for alle tjenester, og sikkerheten vil øke samlet sett.

På en annen side vil imidlertid en innføring av krav til bruk av nasjonal eID for alle offentlige tjenester gjøre at modellen til ID-porten om å tilby innlogging med ulike eID-er fra private og offentlige tilbydere faller bort. Alternativet vil dermed potensielt føre til at ID-porten legges ned og erstattes av autentiseringsmekanismen og signeringsfunksjonaliteten ved nasjonal eID. Dersom ID-porten legges ned vil ikke det offentlige ha mulighet til å åpne for bruk av private eID-er dersom nasjonal eID i en lengere periode er utilgjengelig grunnet eksempelvis tekniske problemer, hvilket vil føre til at den digitale sårbarheten øker.

Dersom nasjonal eID meldes på eIDAS «høyt», slik det er planlagt å gjøre, vil imidlertid utenlandske eID-er kunne benyttes for tilgang til offentlige tjenester og kravet om nasjonal eID vil kun ha en sikkerhetseffekt for brukere som ikke har en utenlandsk eID på eIDAS «høyt». Dersom nasjonal eID ikke meldes i henhold til eIDAS-forordningen, og det likevel settes krav til bruk av nasjonal eID for tilgang alle offentlige tjenester,

faller denne problemstillingen bort, men medfører at EØS-borgere ikke kan benytte en meldt eID fra sitt hjemland for tilgang til offentlige tjenester.

*Sammenlignet med **fremtidig situasjon** for private eID-er vil innføring av et krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester ha liten positiv konsekvens for sikkerheten samlet sett, da utstedelsen av private eID-er vil være omtrent like sikker som for nasjonal eID og nasjonal eID ikke tilfører noe til sikkerheten i bruksfasen. Den digitale sårbarheten reduseres imidlertid ved å innføre krav til nasjonal eID for alle tjenester.*

Nasjonal eID vil som beskrevet over ha høy sikkerhet i utstedelsesprosessen, men i fremtidig situasjon der ID-kontrollen fra pass- og ID-kontor kan benyttes som grunnlag for utstedelse av privat eID-er eller krav om norsk pass eller nasjonalt ID-kort og biometrisjekk av bruker innføres ved utstedelse av private eID-er, vil imidlertid sikkerheten i utstedelsesprosessen for private eID-er være omtrent like høy.

Videre vil det i fremtidig situasjon jevnlig sjekkes biometriske trekk ved hjelp av teknologiske løsninger ved bruk av både nasjonal eID og private eID-er, slik at sikkerheten ved bruk ikke vil øke ved å innføre krav om nasjonal eID for tilgang til alle offentlige tjenester isolert sett.

Slik beskrevet over vil den digitale sårbarheten reduseres også i en fremtidig situasjon dersom det settes krav til bruk av nasjonal eID for offentlige tjenester, da det kan åpnes for bruk av private eID-er og MinID dersom nasjonal eID er utilgjengelig, gitt at ID-porten ikke legges ned.

Vurdering – Brukervennlighet

*Sammenlignet med **dagens situasjon og fremtidig situasjon** vil innføring av et krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester ha meget stor negativ konsekvens for brukervennligheten, da det er en betydelig risiko i å konvertere hele befolkningen fra private eID-er til nasjonal eID.*

Leverandøren ser en meget stor risiko i brukerdimensjonen ved å innføre et krav om bruk av nasjonal eID for å løse utfordringer i utstedelsesprosessen som i utgangspunktet er relativt begrenset. Dagens eID-løsninger har stor utbredelse og bruk i befolkningen, med over 139 mill. pålogginger gjennom ID-porten i 2018. Dersom samtlige pålogginger gjennom ID-porten skal gjennomføres med nasjonal eID kreves det at hele befolkningen «konverteres» fra å bruke eksisterende eID-løsninger, som fra et brukerperspektiv oppleves å fungere godt, til å bruke nasjonal eID.

Slik beskrevet i kapittel 3.6.2 fremstår den foreslåtte løsningen for nasjonal eID å være mindre brukervennlig enn eksisterende løsninger i markedet, og et krav til nasjonal eID for alle offentlige tjenester vil dermed redusere brukervennligheten for hele befolkningen ved digital autentisering til offentlige tjenester. Gitt manglende planlagt ressursbruk til videreutvikling av nasjonal eID, manglende gjennomføringskraft i gjennomføring av NPID-programmet, samt stadige teknologisk nyvinninger vurderer leverandøren at det er usannsynlig at POD vil klare å levere like brukervennlige løsninger som private eID-leverandører over tid.

Resultatet fra POD sin sluttbrukerundersøkelse om at 82 prosent av respondentene ønsker å benytte samme eID til all innlogging ved både offentlige og private tjenester, vil fordre at nasjonal eID må benyttes til alle private tjenester med krav om digital autentisering på høyeste sikkerhetsnivå.[144] Slik beskrevet i kapittel 3.6.2 er ikke

[144] POD og Difi, «Beslutningsgrunnlag for eID på nasjonalt ID-kort: Kartlegging – sluttbrukere, delleveranse 11», 2016

leverandøren gjort kjent med eller sett dokumentasjon på brukerreiser eller bruksområder for nasjonal eID som tyder på at brukervennligheten ved løsningen vil være god nok til at brukere vil velge å benytte den nasjonale eID-en fremfor eksisterende løsninger i markedet.

Dersom nasjonal eID ikke blir benyttet for sikker digital autentisering og tilgang til andre tjenester enn de offentlige, kan potensielt bruken av nasjonal eID ende med å ikke være tilstrekkelig til å sikre at befolkningen blir komfortable med å benytte løsningen. Det kan imidlertid argumenteres for at i underkant av 30[145] innlogginger gjennom ID-porten per innbygger i løpet av et år kan sies å være tilstrekkelig for å sikre at befolkningen blir komfortable med å bruke nasjonal eID for sikker digital autentisering.

Vurdering – Ressursbruk

*Sammenlignet med **dagens situasjon og fremtidig situasjon** vil innføring av et krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester ha liten negativ konsekvens for det offentliges ressursbruk, da innføring, drift og vedlikehold av nasjonal eID potensielt kan være ressursbesparende for det offentlige, mens ressursbruk til videreutvikling av løsningen kan bli betydelig.*

Ved å sette krav til bruk av nasjonal eID for alle offentlige tjenester vil det offentlige etablere en infrastruktur som i stor grad vil fungere parallelt med eksisterende løsningers infrastruktur, gitt at disse opprettholdes for digital autentisering til private tjenester, hvilket er ressurskrevende og potensielt ineffektivt. Slik beskrevet i kapittel 3.6.2 vurderer leverandøren at kostnader til årlig drift av infrastrukturen for nasjonal eID er betydelig underestimert i PODs gebyrmodell, sammenlignet med erfaringer fra private tilbydere. I tillegg inngår ikke kostnader til videreutvikling av løsningen i gebyrmodellen. Leverandøren anser at det er en risiko for at manglende midler til videreutvikling vil føre til at nasjonal eID som løsning ikke vil ha tilstrekkelig sikkerhet i fremtiden eller at ytterligere kostnader vil påløpe for å besørge videreutvikling. Dersom estimatene i PODs gebyrmodell imidlertid skulle vise seg å være korrekte, kan innføring, drift og vedlikeholds av nasjonal eID vise seg å være ressursbesparende for det offentlige sammenlignet med dagens situasjon.

Et krav om nasjonal eID for alle offentlige tjenester vil potensielt føre til økt ressursbruk for det offentlige da det er kritisk at nasjonal eID som eneste godkjente løsning har god tilgjengelighet og kan håndtere periodevis stor pågang fra brukere for autentisering til offentlige tjenester. I tillegg vil et krav om bruk av nasjonal eID for alle offentlige tjenester potensielt medføre betydelig opplæringskostnader og ressurskrevende tiltak for å sikre utbredelse i befolkningen, hvilket vil øke det offentliges ressursbruk.

Leverandøren vurderer i tillegg at eksisterende ressurser i Difi som er planlagt å utføre brukerstøtte for nasjonal eID ikke vil være tilstrekkelig dersom hele befolkningen skal benytte nasjonal eID for alle offentlige tjenester. Følgelig kan ressursbruk og tilhørende kostnader tilknyttet brukerstøtte for nasjonal eID vise seg å bli betydelig for det offentlige.

Samfunnsøkonomisk sett kan et krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester være positivt, men gevinsten vil være begrenset/ikke eksisterende dersom det opprettholdes private infrastrukturer for de eksisterende eID-løsningene. Samtidig fordrer argumentet om redusert digital sårbarhet ved innføring av krav til nasjonal eID for alle offentlige tjenester at de private infrastrukturene opprettholdes, slik at den samfunnsøkonomiske gevinsten vil være begrenset/ikke eksisterende.

[145] Overslag av antall innlogginger i ID-porten i 2018 per innbygger

Samlet vurdering

Tabellen under oppsummerer leverandørens vurdering av å innføre krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester, sammenlignet med henholdsvis dagens situasjon og fremtidig situasjon for private eID-er.

Alternativ	Sammenlignet med	Konsekvens		
		Sikkerhet	Bruker-vennlighet	Ressursbruk
Innføre krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester	Dagens situasjon	+	----	-
	Fremtidig situasjon	+	----	-

Tabell 17 Vurdering av å innføre krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester

3.6.5 Utstede nasjonalt ID-kort uten nasjonal eID

Alternativet innebærer å utstede nasjonalt ID-kort uten eID, og medfører at dagens løsning med å benytte eksisterende eID-er for digital autentisering til offentlige og private tjenester videreføres. Gitt øvrige vurderinger i kapittel 2 antas det i vurderingen av alternativet at en betydelig andel av norske borgere, EØS-borgere og tredjelandsborgere over en femårsperiode vil ha et norsk pass eller nasjonalt ID-kort. I det følgende vurderer leverandøren styrker og utfordringer ved å utstede nasjonalt ID-kort uten nasjonal eID.

Vurdering – sikkerhet

*Sammenlignet med **dagens situasjon** vil utstedelse av nasjonalt ID-kort uten nasjonal eID ha ubetydelig/ingen konsekvens for sikkerheten samlet sett, da dagens sikkerhetshull for private eID-er fortsatt vil eksistere.*

Videreføring av dagens situasjon vil bety at utfordringer identifisert i kapittel 3.4 gjelder, og det vil være svakheter i sikkerheten både i utstedelsesprosessen og bruksfasen av private eID-er. Utstedelse av nasjonalt ID-kort uten nasjonal eID vil ikke føre til noen endringer i sikkerheten for private eID-er.

Den digitale sårbarheten som eksisterer ved at innlogging til offentlige tjenester i stor grad gjennomføres ved bruk av én privat eID-løsning vil fortsatt eksistere dersom nasjonalt ID-kort utstedes uten nasjonal eID. Det vil like fullt være mulig å innføre tiltak for å redusere den digitale sårbarheten. Difi argumenterer for at MinID i dag i stor grad fungerer som en reserveløsning dersom eksempelvis BankID skulle være utilgjengelig. Kontakt- og reservasjonsregisteret kan også benyttes som reserveløsning, og muliggjør eksempelvis utsendelse av engangspassord til brukere dersom BankID skulle være utilgjengelig.

*Sammenlignet med **fremtidig situasjon** for private eID-er vil utstedelse av nasjonalt ID-kort uten nasjonal eID ha ubetydelig/ingen konsekvens for sikkerheten samlet sett, da sikkerheten ved utstedelse og bruk av private eID-er vil styrkes i fremtidig situasjon.*

Krav til norsk pass eller nasjonalt ID-kort og teknologiske løsninger for biometrisjekk ved utstedelse av private eID-er vil sikre at alle brukere som får utstedt private eID-er har status «unik», at hver bruker kun kan få utstedt privat eID i én identitet og at en bruker ikke kan få utstedt en annen persons eID. Benyttelse av ID-kontrollen som

gjennomføres ved et pass- og ID-kontor som grunnlag for utstedelse av private eID-er vil gi tilsvarende økning i sikkerheten, og vil i tillegg innebære at brukere som skal få utstedt en privat eID gjennomgår tilsvarende ID-kontroll som ved utstedelse av pass og nasjonalt ID-kort.

Slik beskrevet i kapittel 3.6.2 vil ikke nasjonal eID isolert sett løse utfordringer relatert til sikkerheten i bruksfasen. Implementering av teknologiske løsninger for sjekk av biometri ved bruk av eID-er, uavhengig om det er for nasjonal eID eller private eID-er, vil derimot bidra til å løse denne utfordringen og vil redusere misbruk der brukeren av eID-en ikke er rettmessig eier.

Slik som i vurderingen av sikkerhet sammenlignet med dagens situasjon over, vil ikke utstedelse av nasjonalt ID-kort uten nasjonal eID redusere den digitale sårbarheten som eksisterer ved at innlogging til offentlige tjenester i stor grad gjennomføres ved bruk av én privat eID-løsning.

Det kan argumenteres for at utstedelse av nasjonalt ID-kort uten nasjonal eID vil bidra til å videreføre posisjonen til en dominerende markedsaktør, som også i sikkerhetsøyemed kan være en utfordrende situasjon. På samme måte som for den digitale sårbarheten, kan det tenkes at det offentlige kan iverksette tiltak for å oppnå mer strategisk kontroll over den dominerende eID-løsningen eller stimulere til mer konkurranse i markedet.

Vurdering – brukervennlighet

*Sammenlignet med **dagens situasjon og fremtidig situasjon** vil utstedelse av nasjonalt ID-kort uten nasjonal eID ha ubetydelig/ingen konsekvens for brukervennligheten, da eksisterende brukervennlige løsninger vil videreføres for sikker digital autentisering til offentlige tjenester.*

Utstedelse av nasjonalt ID-kort uten nasjonal eID viderefører dagens brukervennlighet, da brukere fortsatt vil benytte eksisterende eID-løsninger. Slik beskrevet i hovedrapporten kapittel 2.8.2 er BankID den klart mest brukte eID-en for tilgang til offentlige tjenester gjennom ID-porten, med ca. 82 prosent av alle autentiseringene i 2018.[146]

Slik beskrevet i kapittel 3.6.2 vil ikke nasjonal eID løse utfordringen med at enkelte brukergrupper har utfordring med å få utstedt en privat eID i dag. Utstedelse av nasjonalt ID-kort uten eID vil følgelig ikke føre til redusert brukervennlighet for disse brukergruppene, og ved at denne brukergruppen får et nasjonalt ID-kort kvalifiserer de også til å få utstedt en privat eID, da de kan bevise sin identitet gjennom det nasjonale ID-kortet.

Fra POD og Difi sin sluttbrukerundersøkelse for nasjonal eID fra 2016 fremkommer det at 93 prosent av respondentene er *«helt enig»* eller *«ganske enig»* i at BankID er lett å bruke, og at 91 prosent av respondentene er *«helt enig»* eller *«ganske enig»* i at BankID er en praktisk løsning for pålogging. For BankID på mobil fremkommer det at 95 prosent av respondentene er *«helt enig»* eller *«ganske enig»* i at BankID på mobil er lett å bruke, og at 96 prosent av respondentene er *«helt enig»* eller *«ganske enig»* i at BankID på mobil er en praktisk løsning for pålogging. Videre viser sluttbrukerundersøkelsen at 82 prosent av respondentene ønsker å benytte samme eID til all innlogging ved både offentlige og private tjenester, og at BankID er den foretrukne eID-løsningen.[147]

[146] Basert på data fra Difi, første halvår 2019
[147] POD og Difi, «Beslutningsgrunnlag for eID på nasjonalt ID-kort: Kartlegging – sluttbrukere, delleveranse 11», 2016

Vurdering – ressursbruk

*Sammenlignet med **dagens situasjon og fremtidig situasjon** vil utstedelse av nasjonalt ID-kort uten nasjonal eID ha middels positiv konsekvens for det offentliges ressursbruk, da kostnader til innføring, drift, vedlikehold og videreutvikling av nasjonal eID vil unngås eller betydelig reduseres.*

Utstedelse av nasjonalt ID-kort uten nasjonal eID kan potensielt ha ressursmessige gevinster, først og fremst ved at det offentlige ikke binder opp fremtidige drifts-, forvaltnings- og utviklingskostnader til nasjonal eID. Årlige drifts- og forvaltningskostnader til nasjonal eID er i PODS gebyrmodell estimert til omtrent 12 mill. kroner. Slik beskrevet i kapittel 3.6.2 inngår ikke kostnader til videreutvikling av nasjonal eID i PODs gebyrmodell. Private tilbydere fremhever imidlertid at deres kostnader til videreutvikling av eID-løsninger er betydelige. Ved å utstede nasjonalt ID-kort uten nasjonal eID vil det unngå potensielt betydelige kostnader til videreutvikling av nasjonal eID for å sikre en levedyktig og sikker løsning med stor utbredelse og bruk.

Ved å utstede nasjonalt ID-kort uten nasjonal eID må POD terminere kontrakten med leverandøren av felles driftsplattform for nasjonal eID og kø- og timebestilling. Leverandøren har fått opplyst at det ved en slik terminering vil påløpe en engangskostnad på mellom 5 og 10 mill. kroner. Slik beskrevet i kapittel 3.1.3 har det per november 2019 påløpt omtrent 28 mill. kroner i investeringskostnader tilknyttet nasjonal eID. POD har i tillegg ytterligere betalingsforpliktelser på omtrent 26 mill. kroner, hvilket betyr at totale irreversible investeringskostnader til nasjonal eID er på totalt 54 mill. kroner. De totale planlagte investeringskostnadene for nasjonal eID på 82 mill. kroner vil dermed kunne nedjusteres med 28 mill. kroner dersom nasjonalt ID-kort utestedes uten nasjonal eID.

Videre vil utstedelse av nasjonalt ID-kort uten nasjonal eID potensielt kunne føre til redusert ressursbruk i POD og PIT grunnet redusert behov for forvaltning, drift og videreutvikling av nasjonal eID. Eksisterende ressurser i Difi som er planlagt å utføre brukerstøtte for brukere av nasjonal eID vil ikke lenger være bundet til denne oppgaven, hvilket vil redusere det offentliges ressursbruk ytterligere.

Samlet vurdering

Tabellen under oppsummerer leverandørens vurdering av å utstede nasjonalt ID-kort uten nasjonal eID, sammenlignet med henholdsvis dagens situasjon og fremtidig situasjon for private eID-er.

Alternativ	Sammenlignet med	Konsekvens		
		Sikkerhet	Bruker-vennlighet	Ressursbruk
Utstede nasjonalt ID-kort uten nasjonal eID	Dagens situasjon	0	0	++
	Fremtidig situasjon	0	0	++

Tabell 18 Vurdering av å utstede nasjonalt ID-kort uten nasjonal eID

3.6.6 Avsluttende vurdering

Tabellen under oppsummerer leverandørens vurdering av de fire alternativene for nasjonal eID, sammenlignet med henholdsvis dagens situasjon og fremtidig situasjon for private eID-er. Begrenset gjennomføringsevne hos ansvarlig aktør, store forsinkelser med nasjonalt ID-kort og nasjonal eID og betydelig ressursbruk over lang tid, kombinert med dagens store utbredelse og bruk av brukervennlige private eID-løsninger, gjør at innføring av nasjonal eID vil gi begrenset nytte etter leverandørens syn. Det er særlig argumenter om begrenset økning i sikkerhet, redusert brukervennlighet og usikker fremtidig ressursbruk ved nasjonal eID som er utslagsgivende for at leverandøren anser det som lite hensiktsmessig at det offentlige skal ha et ansvar for sikker digital autentisering gjennom nasjonal eID. Etter leverandørens syn bør identifiseringen av brukere være det offentliges ansvar, mens autentisering av brukere gjennom eID-løsninger kan settes ut til andre aktører. På en annen side bør viktigheten av en mindre økning i sikkerhet i form av forbedret digital sårbarhet og endring av dominerende aktørs posisjon vektes opp mot økt ressursbruk og redusert brukervennlighet ved innføring av nasjonal eID.

Alternativ	Sammenlignet med	Konsekvens		
		Sikkerhet	Bruker-vennlighet	Ressursbruk
Introdusere nasjonal eID som et supplement til eksisterende løsninger i markedet	Dagens situasjon	0	0	--
	Fremtidig situasjon	0	0	--
Innføre krav til bruk av nasjonal eID for tilgang til utvalgte offentlige tjenester	Dagens situasjon	++	---	--
	Fremtidig situasjon	+	---	--
Innføre krav til bruk av nasjonal eID tilgang til alle offentlige tjenester	Dagens situasjon	+	----	-
	Fremtidig situasjon	+	----	-
Utstede nasjonalt ID-kort uten nasjonal eID	Dagens situasjon	0	0	++
	Fremtidig situasjon	0	0	++

Tabell 19 Samlet vurdering av alternativ for nasjonal eID

3.7 Vurdering av konsekvenser av eventuelle endringer i vederlagsmodellen for nasjonal eID

Slik beskrevet i kapittel 11.2.2 i hovedrapporten anser leverandøren det som en mulighet å endre vederlagsmodellen for nasjonal eID og innføre en transaksjonskostnad for å i større grad opprettholde konkurransen i markedet ved innføring av nasjonal eID. Leverandøren beskrev videre i kapittel 11.2.2 i hovedrapporten at en transaksjonskostnad for nasjonal eID vil kunne bidra til å dekke inn fremtidige økte kostnader til drift ved stor bruk av nasjonal eID og kostnader til videreutvikling av nasjonal eID. POD argumenterer for at det i stor grad kun er faste kostnader knyttet til nasjonal eID og at stor bruk av nasjonal eID ikke vil medføre ytterligere kostnader for det offentlige. Videre argumenter POD for at en eventuell

uforutsett økning i kostnadene ved nasjonal eID kan dekkes ved å øke utstedelsesgebyret for nasjonalt ID-kort.

Valgt utforming av vederlagsmodellen avhenger i stor grad av om det settes krav til bruk av nasjonal eID for tilgang til offentlige tjenester eller ikke. Dersom det innføres et krav til bruk av nasjonal eID for tilgang til alle offentlige tjenester anser leverandøren at gratis bruk av nasjonal eID for tjenesteeiere, i alle fall offentlige tjenesteeiere, kan være en hensiktsmessig løsning.

Den viktigste styrken ved en modell med gratis anvendelse av nasjonal eID er at det gir gode forutsetninger og insentiver for utstrakt bruk av nasjonal eID hos offentlige og private tjenesteeiere. Dette gjelder spesielt ved stor utbredelse av nasjonal eID i befolkningen. Leverandøren vurderer at det vil være meget attraktivt for både private og offentlige tjenesteeiere å tilby digital autentisering gjennom nasjonal eID dersom det er gratis for tjenesteeierne. For mange tjenesteeiere er ikke autentisering via eID en vesentlig kostnad samlet sett og arbeidet med hovedrapporten har vist at bevisstheten tilknyttet disse kostnadene er meget lav. Det antas allikevel at gratis bruk vil gi tjenesteeierne et meget kraftig insentiv til å påvirke hvilken eID brukerne benytter. Videre anser leverandøren at en modell med gratis bruk av nasjonal eID vil være relativt enkel å drifte for det offentlige. Det vil eksempelvis ikke påløpe kostnader til å beregne faktureringsgrunnlag eller innkreving, og behovet for oppfølging av tjenesteeiere vil være meget begrenset.

En svakhet ved modellen med gratis anvendelse av nasjonal eID er at den kan skape en skjev konkurransesituasjon sammenlignet med dagens situasjon for private eID-er. Commfides har en lignende modell med gratis anvendelse for tjenesteeiere, men løsningen utstedes i stor grad til bedriftskunder og brukes dermed meget sjeldent for tilgang til offentlige tjenester i ID-porten. I tillegg har Commfides betydelig høyere utstedelsesgebyrer sammenlignet med nasjonal eID, og bedriftskundene kjøper en helhetlig løsning med mulighet for at utstedelse gjennomføres av ansatte i virksomheten, og ikke kun en eID-løsning. Tilbydere av eID-løsninger kan imidlertid selv velge ønsket forretningsmodell og leverandøren er ikke forelagt dokumentasjon som indikerer at forretningsmodellen som er valgt for nasjonal eID er ulovlig. Gratis anvendelse av nasjonal eID vil gi tjenesteeiere insentiv til å velge å tilby digital autentisering med nasjonal eID for tilgang til sine tjenester. Leverandøren anser at dette potensielt kan bidra til å bremse digitalisering og videreutvikling av eID-løsninger dersom en stor andel tjenesteeiere velger å benytte nasjonal eID, da nasjonal eID for leverandøren fremstår å være en mindre brukervennlig løsning og grunnet PODs manglende estimater for kostnader til videreutvikling av løsningen.

Ved høy utbredelse og høyt antall autentiseringer gjennom nasjonal eID for private og offentlige tjenesteeiere sitter det offentlige med all risiko for at kostnadene tilknyttet til drift, forvaltning og videreutvikling blir høyere enn estimatene lagt til grunn ved gebyret ved utstedelse. Leverandøren har ikke blitt forelagt eksempler som viser hvordan kostnadene vil utvikle seg i en slik situasjon, men antar at eksempelvis kostnader til brukerstøtte og øvrig drift og forvaltning vil kunne bli betydelige. Kontantstrømmen fra vederlagsmodellen sikrer heller ikke grunnlag for midler til videreutvikling av nasjonal eID slik leverandøren forstår det. Når behovene for videreutvikling kommer må kostnadene etter leverandørens forståelse tas fra øvrig drift i politiet, gis som separate bevilgninger eller tas ut i økte gebyrer.

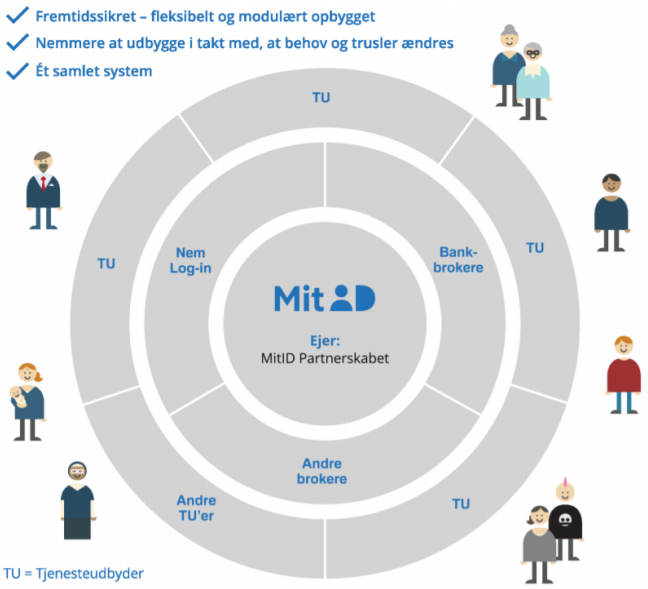
3.8 Vurdering av offentlig-privat samarbeid for infrastruktur for eID

Som et alternativ til dagens situasjon og innføring av nasjonal eID, beskriver leverandøren i dette kapittelet kort muligheten for et offentlig-privat samarbeid for

infrastruktur for eID. Alternativet er delvis inspirert av Danmarks pågående arbeid med MitID og medfører at det vil etableres én kjerneinfrastruktur for eID. Et begrenset antall tilbydere er påkoblet og kan konkurrere om brukeropplevelse for både utstedelse og bruk av sine løsninger. Alternativet er også delvis inspirert av modellen som staten har valgt for utsendelse av digital post til befolkningen gjennom digital postkasse. De to tilbyderne av digital postkasse, Posten med Digipost og e-Boks AS, konkurrerer om brukere på brukeropplevelse og tilleggstjenester.[148]

Teknisk og kommersielt sett kan et offentlig-privat samarbeid i utgangspunktet løses på mange ulike måter, men kan eksempelvis innebære å endre eierskapet til deler av eksisterende infrastruktur og/eller sertifikatdatabaser hos private tilbydere. For BankID vil dette umiddelbart medføre at løsningen får 4,2 mill. brukere, 800 mill. transaksjoner årlig og tilgang til ca. 1 600 private tjenester, i tillegg til offentlige tjenester gjennom ID-porten.

Danmark vil i løpet av 2021 introdusere MitID, der flere ulike tjenestetilbydere vil kunne utstede eID-er til brukere basert på grunnleggende informasjon om personidentiteter som er tilgjengelig for alle tilbydere.



Figur 20 Overordnet skisse for MitID[149]

Et offentlig-privat samarbeid vil være et alternativ til å etablere en nasjonal eID som en fjerde løsning i konkurranse med etablerte og velfungerende løsninger som BankID, Buypass ID og Commfides. Norge er et av markedene som har kommet lengst når det gjelder utbredelse og bruk av eID-er. Gjennom et offentlig-privat samarbeid kan det offentlige utnytte dagens utbredelse og samtidig stimulere til konkurranse og innovasjon. Dette kan videre bidra til å endre den dominerende markedsposisjonen som BankID har i dag, da flere tilbydere vil ha mulighet til å utstede egne eID-løsninger til brukere basert på en felles kjerneinfrastruktur. Videre vil alternativet forhindre etablering av parallelle og kostnadskrevende infrastrukturer for eID, hvilket vil skje dersom både infrastruktur for nasjonal eID, eventuelle nye tilbydere, og eksisterende private infrastrukturer opprettholdes.

[148] Norge.no, «Spørsmål og svar – Skaff deg ein digital postkasse», 2019
[149] Skjermbilde hentet fra: Digitaliseringsstyrelsen, «Opfølgende informationsmøde for interesserede brokere», 17.09.2019

Leverandøren vurderer imidlertid at et offentlig-privat samarbeid og en felles kjerneinfrastruktur krever betydelig utredningsarbeid, og en eventuell påfølgende kommersiell dialog med et gitt antall aktører, før det kan realiseres. En forutsetning for realisering av et offentlig-privat samarbeid er at det etableres og sikres prosesser og mekanismer tilknyttet kontroll ved utstedelse og bruk av eID-er som hindrer at én person kan få utstedt og benytte eID-er i flere ulike identiteter. Videre anser leverandøren at et slikt samarbeid potensielt vil ta betydelig tid å implementere, sammenlignet med de alternative løsninger som ble vurdert i kapittel 3.5.

4 Styring og struktur – et felles skrankepunkt

I dette kapittelet utreder og vurderer leverandøren samkjøring av ID-relaterte oppmøter for registrering, fastsettelse av identitet og utstedelse av pass- og nasjonalt ID-kort i et felles skrankepunkt. Kapittelet er utarbeidet i henhold til tema 3 i mandat for tilleggsoppdraget, nærmere beskrevet i kapittel 1.1.

Kapittelet fokuserer særskilt på de ulike skrankepunktene i ID-forvaltningen og ID-relaterte oppmøter med tilhørende oppgaver. Kapittelet tar videre for seg formål med et felles skrankepunkt, samt alternativ og forslag til organisering av et felles skrankepunkt. Alternativene vurderes opp mot kriteriene sikkerhet, brukervennlighet og ressursbruk.

Av relevant bakgrunn i hovedrapporten vises det spesielt til kapittel 2.4 om «Prosess fra fastsetting av ID til ID-kontroll», kapittel 2.6 om «Brukergrupper og brukerreiser» og kapittel 2.8 om «Sakstyper og volum». Det vises videre til kapittel 3.1.1 om «Aktørbilde i ID-forvaltningen med administrativ styringslinje», kapittel 3.1.2 om «Geografisk tjenestestedstruktur» og kapittel 3.1.3 om «ID-forvaltningens saksgang fra et aktørperspektiv». Det vises til kapittel 6.1.1-6.1.4 for en beskrivelse av kvalitet og sikkerhet i utvalgte ID-prosesser. Fra hovedrapportens del 3 er kapittel 14 om vurdering av alternativ knyttet til fysiske oppmøter, samt kapittel 15 om vurdering av alternativ knyttet til styring og struktur relevant. Når det gjelder del 4 og anbefalinger er kapittel 16.1.6 om å redusere brukers behov for fysiske oppmøter og kapittel 16.1.7 om å nærmere utrede eierskap og etablering av en ID-etat relevante.

I hovedrapporten anbefalte leverandøren å redusere brukers behov for fysiske oppmøter gjennom å tilrettelegge for økt deling av data og gjenbruk av ID-kontroll ved et skrankepunkt. Tilleggsrapporten går mer i dybden på ID-relaterte oppmøter som finner sted i de ulike skrankepunktene til relevante aktører og vurderer muligheter og alternativ for å samle hele eller deler av slike oppmøter i et felles skrankepunkt.

4.1 Bakgrunn

4.1.1 Forutsetninger

Som følge av mandatet og nødvendige forenklinger i arbeidet har leverandøren utarbeidet noen viktige forutsetninger som gjelder for kapittel 4:

- Kun prosesser for ID-relaterte oppmøter som gjennomføres i Norge er vurdert. Dette medfører at aktivitetene i prosessene som finner sted i utlandet, på utenriksstasjonene, ikke er inkludert i vurderingene
- Alle prosessene er vurdert med tanke på at et potensielt felles skrankepunktet ligger hos politiet
- Alternative løsninger som innebærer å beholde skrankepunktorganiseringen slik den er i dag med ulike former for forbedringer vurderes ikke
- Oppmøter for fornyelser av ID-bevis og øvrige tillatelser er ikke fremvist i prosesser, regnet med i antall oppmøter og heller ikke hensyntatt ved beregning av brukertid og ressursbruk. Det vises for øvrig til hovedrapportens kapittel 5 for aspekter tilknyttet dette

- Skrankepunktet er vurdert å være et fysisk oppmøtested, men det er på sikt mulig å tenke seg et felles digitalt skrankepunkt hvor tjenester knyttet til ID samles i en felles portal. Dette vil være tett knyttet opp mot aktiviteter i det fysiske skrankepunktet. Tilleggsrapporten vurderer kun et fysisk skrankepunkt

4.1.2 Førstelinje, andrelinje og skrankepunkt

Det finnes flere definisjoner av førstelinje, andrelinje og skrankepunkt, og det varierer hvilke aktiviteter som inngår i begrepsdefinisjoner. Ulike definisjoner er beskrevet i avsnittene nedenfor.

Ved politiets pass- og ID-kontor: kontrollinje vs. vedtakslinje. Med nytt saksbehandlingssystem innføres det en ny prosedyre med todelt saksbehandling i kontrollinje og vedtakslinje.[150] *«Skrankepunktene (pass- og ID-kontorene) i politidistriktene vil utgjøre politiets kontrollinje. Oppgavene i kontrollinjen vil blant annet omfatte veiledning av søkere, registrering av søknader, opptak av foto og fingeravtrykk og kontroll/verifisering av søkers og eventuell verges identitet, kontroll av dokumenter og oversendelse av søknader til vedtakslinjen. Vedtakslinjen vil blant annet behandle saker og treffe vedtak, oversende saker til Kripos for nærmere undersøkelser (treff i ansiktsgjenkjenning, dokumentgransking), utrede saker som skal følges opp i straffesakssporet, anmelde mulige straffbare forhold og forberede klagesaker til Politidirektoratet».*

Politiets utlendingsforvaltning og UDI: førstelinje vs. andrelinje. Utføring av alle aktiviteter som foregår på politiets utlendingskontorer på vegne av UDI betraktes som førstelinje.[151] Begrepet andrelinje benyttes for sakene som sendes videre til ytterligere behandling av politiet og/eller UDI.

Fra førstelinjeprosjektets sluttrapport om ansvarfordeling i utlendingsforvaltningen:[152] *«Begrepet "førstelinje" defineres typisk som det fysiske kontaktpunktet til brukeren. I utlendingsforvaltningen er det en rekke oppgaver i den forberedende saksbehandlingen som forutsetter et fysisk kontaktpunkt fordi det kreves personlig oppmøte.»*

Skattekontorene: førstelinje vs. andrelinje. Førstelinje brukes for å beskrive det fysiske kontaktpunktet til brukeren, mens andrelinje omfatter øvrige aktiviteter.

Det eksisterer få til ingen kjente eller allmennbrukte definisjoner av et skrankepunkt. Leverandøren har valgt følgende definisjon:

> *Et skrankepunkt er et fysisk oppmøtested hvor brukere møter opp for å legitimere seg og søke om tilgang til en tjeneste eller ytelse. I skrankepunktet er det en eller flere skranker som skiller personene som betjener og personene som betjenes.*

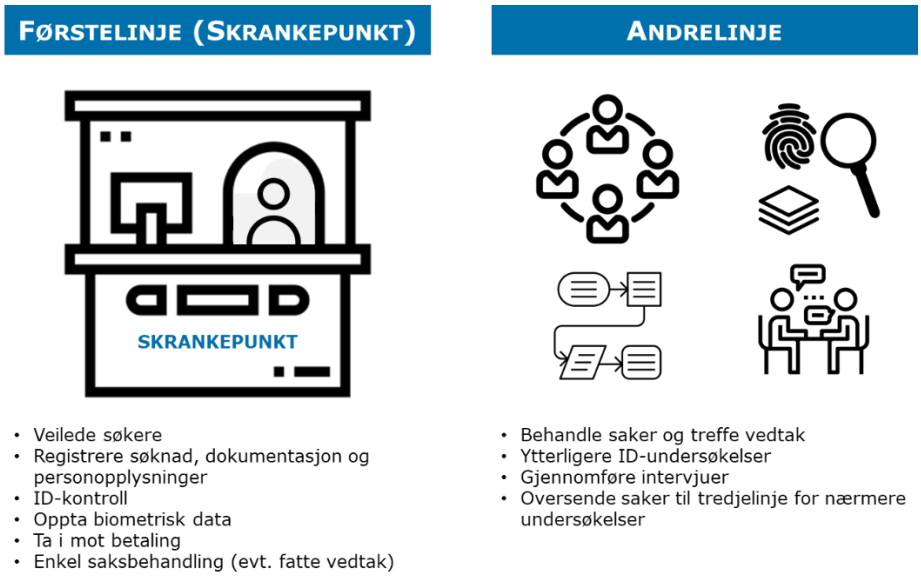
Bruk av begrepene i beskrivelse av nåsituasjonen

Leverandøren har, for å standardisere og forenkle, valgt å benytte definisjonene førstelinje (skrankepunkt) og andrelinje i beskrivelsen av nåsituasjonen og de ulike prosessene. Det understrekes at dette skillet med tilhørende ansvars- og oppgavedeling kun gjelder i beskrivelsen av nåsituasjonen, det vil si i kapittel 4.1, 4.2 og 4.3.

[150] JD, «Høring – forslag til forskrift om pass og nasjonalt ID-kort», 2019
[151] Informasjon mottatt av politiet og UDI, andre halvår 2019
[152] UDI, «Førstelinjeprosjektets sluttrapport – Anbefalinger om fremtidig oppgave- og ansvarsfordeling i utlendingsforvaltningen», 2009

Førstelinjen omfatter alle aktiviteter som gjennomføres i et skrankepunkt ved brukers oppmøte som enkel/forberedende saksbehandling inkludert gjennomføring av ID-kontroll, registrering av søknad, dokumentasjon og personopplysninger, opptak av biometriske data og betaling. Andrelinjen omfatter alle aktiviteter som foregår utenfor selve skrankepunktet, som ytterligere saksbehandling, ID-undersøkelser og intervjuer.

En overordnet beskrivelse av oppgaver i førstelinje (skrankepunkt) og andrelinje gitt dagens organisering og som er lagt til grunn i nåsituasjonsbeskrivelsen er illustrert i figuren nedenfor.



Figur 21 Overordnet beskrivelse av oppgaver i førstelinje (skrankepunkt) og andrelinje

4.1.3 ID-kontroller

På tvers av forvaltningen brukes ulike begreper tilknyttet ID-kontroll, og en gjennomføring av en ID-kontroll inneholder nødvendigvis ikke de samme aktivitetene da dette vil avhenge av hvilken type ID-kontroll det dreier seg om. Leverandøren forklarer de mest sentrale definisjonene av ID-kontroll under:

- Minimumskontroll: Innebærer en personkontroll (sjekke pass eller annet ID-dokument opp mot søkeren) og en dokumentkontroll (enkel sjekk av om dokumentet er ekte). I utlendingsforvaltningen følges blant annet en sjekkliste fra POD og veileder fra NID.[153] Kontrollen utføres i førstelinje

- Utvidet kontroll: Innebærer en mer omfattende kontroll av dokumentene etter sjekkliste, blant annet fra POD i utlendingsforvaltningen.[154] Kontrollen kan utføres både i første- og andrelinje avhengig av om skrankepersonell har kompetanse eller utstyr til å utføre de nødvendige undersøkelsene

- Teknisk kontroll: Innebærer å «*sjekke om det er korrekt myndighet som har utstedt dokumentet, at alle felt i dokumentet er utfylt, at det ikke ser ut til at dokumentet er manipulert på noen måte og at det ser ekte ut*»[155]. Kan utføres både i første- og andrelinje

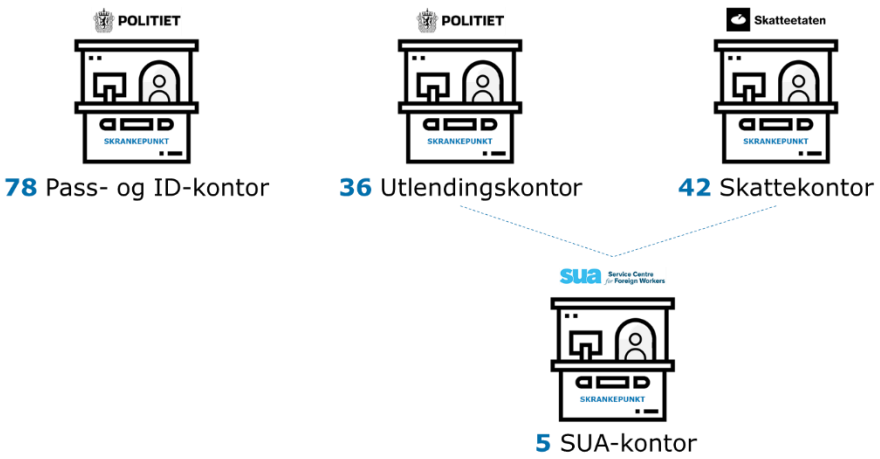
[153] Som definert i UDIs RS 2011-040
[154] Som definert i UDIs RS 2011-040
[155] NID, «Kartlegging av ID-arbeid – Del 1 Politi og utenriksstasjoner», 2013

- Taktisk kontroll: Innebærer å undersøke om det er sannsynlig at personen som møter opp fysisk og presenterer dokumentet er den samme som det er bilde av i dokumentet, om det er sannsynlig at vedkommende er rette innehaver av dokumentet og de personopplysningene som fremkommer i dokumentet, samt en vurdering av hvordan personen fremstår og om hun/han kjenner innholdet i dokumentet.[156] Kan utføres både i første- og andrelinje

ID-dokumenter som skal kontrolleres i disse tilfellene kan være nasjonalitetspass og andre reisedokument som nasjonale ID-kort fra andre land, samt andre typer ID-dokument som for eksempel statsborgerbevis eller fødsels- og vigselsattester eller utskrift fra folkeregister i et annet land.

4.1.4 Overordnet om vurderte skrankepunkt

Leverandøren har basert på mandat, mottatt dokumentasjon og samtaler med aktører vurdert fire skrankepunkt i ID-forvaltningen som relevante for vurderingene i tilleggsoppdraget: pass- og ID-kontor, utlendingskontor, skattekontor og SUA-kontor (servicesentre for utenlandske arbeidstakere, med skranker både for utvalgte utlendingssaker og for skattesaker). I det følgende er de ulike skrankepunktenes oppgaver inn mot ID-relaterte oppmøter overordnet forklart. Kapittel 4.2 forklarer de ulike oppmøtene som gjennomføres på skrankepunktene mer detaljert.



Figur 22 Oversikt over relevante skrankepunkt

Pass- og ID-kontor

Politidistriktenes passforvaltning med pass- og ID-kontor er en del av politiets førstelinje og behandler søknader om pass. Kurante saker behandles direkte i skrankepunkt, mens tvilssaker går videre til behandling i andrelinje. På mindre søkersteder behandles i tillegg andre forvaltningssaker, for eksempel våpen, førerkort og brukthandelbevilling.

Når nasjonale ID-kort lanseres fra 2020 vil pass- og ID-kontorene også behandle disse sakene.

[156] NID, «Kartlegging av ID-arbeid – Del 1 Politi og utenriksstasjoner», 2013 og informasjon mottatt av Skatteetaten

Politiets utlendingskontor

Politidistriktenes utlendingsforvaltning med utlendingskontorer utgjør UDIs førstelinje i Norge for søknader om oppholdstillatelse, søknader om norsk statsborgerskap, søknader om utlendingspass/reisebevis og EØS-registreringer.[157] Politiet behandler en stor del av søknadene selv, etter delegert vedtaksmyndighet fra UDI, men kan ikke avslå søknader.[158] Saker som politiet ikke kan behandle selv, blir sendt til UDI.

Skattekontor

Skatteetatens ID-relaterte førstelinje er plassert på skattekontor som gjennomfører ID-kontroller, i tillegg til på SUA-kontorene. Skattekontorene gjennomfører ID-kontroll for personer som trenger skattekort, utenlandske borgere med d-nummer som har behov for status «kontrollert» i Folkeregisteret eller for personer som skal melde innflytting og gjeninnflytting til Norge.[159] I tillegg gjennomføres enkelte oppgaver relatert til skatt og endringer av informasjon i Folkeregisteret, samt øvrige serviceoppgaver.

SUA-kontor

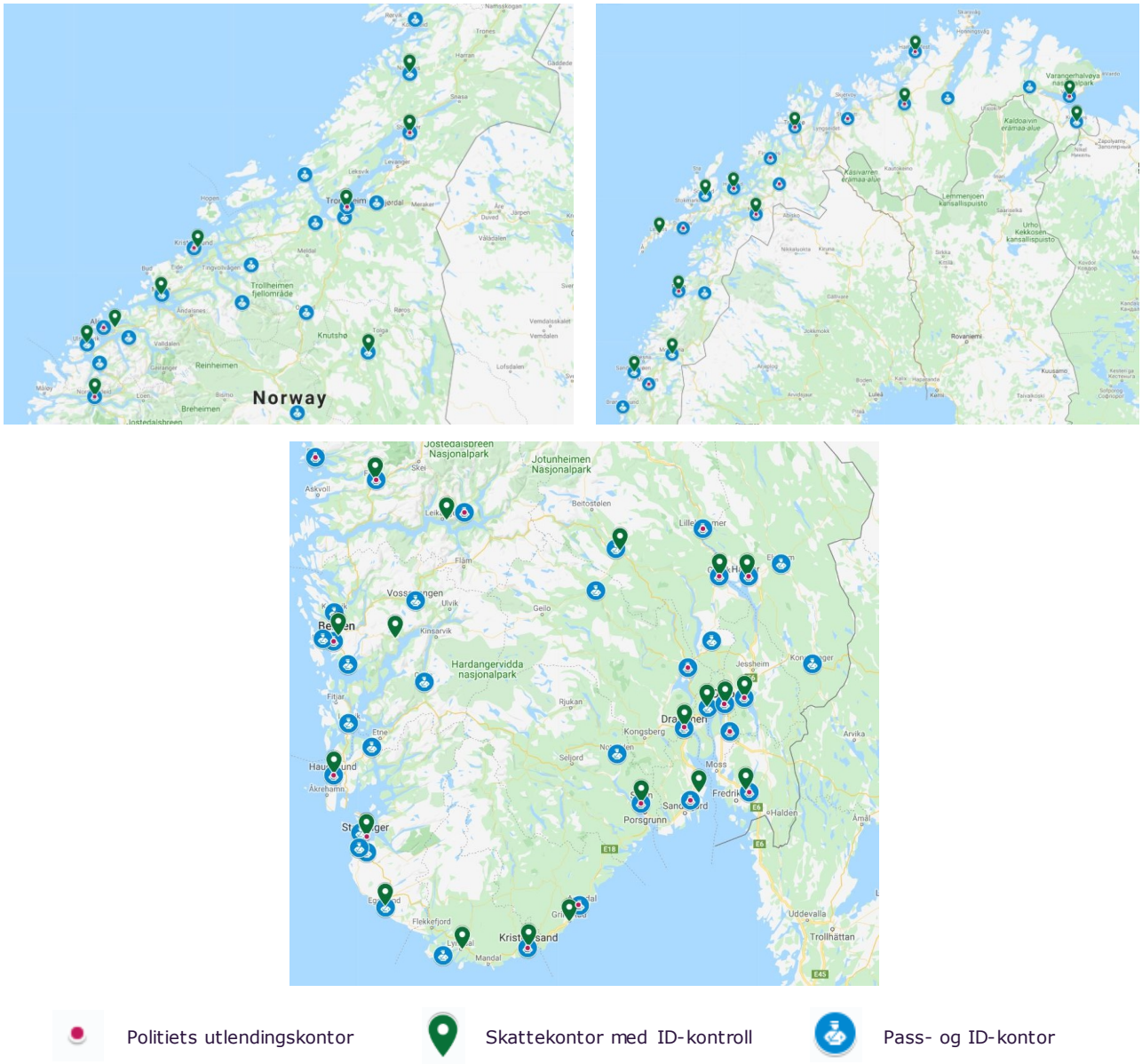
På SUA-kontorene samarbeider politiet, Skatteetaten, UDI og Arbeidstilsynet om å gi god veiledning og rask søknadsbehandling til utlendinger som kommer til Norge for å jobbe. Hensikten er at brukerne skal kunne gå inn én dør og skaffe seg det de trenger for å kunne komme raskt ut i arbeid. Hovedoppgavene til politiets skrankepunkt ved SUA-kontorene er å behandle søknader om oppholdstillatelse, bestille oppholdskort og utstede registreringsbevis til EØS-borgere. For Skatteetatens skrankepunkt ved SUA-kontorene er hovedoppgavene å behandle søknader om skattekort, tildele d-nummer og fødselsnummer til brukere, samt å ta imot søknad om og registrere innflytting til Norge.

Politiet og Skatteetaten har separate køer og skrankepunkter på SUA-kontorene, men brukere som først er i politiets skranke og deretter ønsker en tjeneste av Skatteetaten (noe som ofte er tilfellet), prioriteres i køen til Skatteetaten. I noen tilfeller må søkeren møte på to forskjellige dager for å få gjennomført begge tjenestene da det kan være kapasitetsutfordringer. Det er betydelig forskjeller i ventetid mellom etatene og de ulike SUA-kontorene. Oslo skiller seg spesielt negativt ut på grunn av stort volum søkere.

4.1.5 Grad av samlokalisering for dagens skrankepunkt

I hovedrapportens kapittel 3.1.2 ble tjenestestedstrukturen for skattekontor, SUA-kontor og pass- og ID-kontor forklart og i tillegg ble det illustrert hvordan disse geografisk er plassert i forhold til hverandre. Figuren nedenfor viser oppdatert tjenestestedstruktur for skattekontor, pass- og ID-kontor og utlendingskontor. I tillegg er det SUA-kontor i fem byer: Oslo, Stavanger, Bergen, Trondheim og Kirkenes.

[157] Informasjon mottatt fra politiet, andre halvår 2019
[158] UDI, «RS 2010-089 Delegering av vedtaksmyndighet fra UDI til politiet - utlendingsloven § 65 annet ledd, jf. utlendingsforskriften §§ 13-1, 13-2, 13-3, 13-5 og 13-6, og delegering av myndighet til å avvise søknader som ikke er fremsatt på riktig måte», 2019
[159] Skatteetaten, «Skattekontorer som utfører ID-kontroll», u.å.



Figur 23 Oversikt over geografisk plassering av utlendingskontor, skattekontor med ID-kontroll og pass- og ID-kontor

Oversikten viser en relativt høy grad av samlokalisering mellom pass- og ID-kontor, utlendingskontor og skattekontor. Av totalt 41 oppmøtesteder for utlendingskontor (inkl. SUA) er 34 samlokalisert med pass- og ID-kontor på politistasjoner. Av totalt 47 skattekontor (inkl. SUA) som gjennomfører ID-kontroll er 31 samlokalisert med eller plassert én km fra et pass- og ID-kontor, mens 90 prosent av skattekontorene ligger maks 15 km i radius unna et pass- og ID-kontor. Det vil si at det er stor grad av geografisk nærhet mellom pass- og ID-kontorene og skattekontorene/SUA-kontorene.

At to eller flere skrankepunkt er samlokalisert betyr ikke at det er et felles skrankepunkt. Eksempelvis gjennomføres prosesser for utlendingskontorene og pass- og ID-kontorene i dag i stor grad med forskjellige medarbeidere, i ulike systemer og basert på ulike regelverk. Utover å dele adresse kan samlokaliseringen gi begrensede synergier, men dette er noe som varierer mellom politidistrikter.

I samtaler med forvaltningen har fordeler ved samlokalisering blitt drøftet, og politistasjonene på Grålum og i Tromsø har blitt trukket frem som eksempler på hvordan samlokalisering fungerer på en god måte. På Grålum (Øst politidistrikt) vises det til et tett samarbeid om ID-relaterte oppgaver mellom utlendingsseksjonen og forvaltningsseksjonen, noe som gir positive utslag for kompetanse, publikum, utstyr og

ressurser.[160] Seksjonene hevder videre at samlokaliseringen bidrar til bedre sikkerhet, ressursutnyttelse, service og tilgjengelighet for brukerne.

Videre er det viktig å presisere at SUA-kontorene har samlokaliserte skrankepunkter, men at de etter leverandørens definisjon ikke er felles skrankepunkt.

4.1.6 Endringer i kompetanse og antall oppmøter ved utstedelse av nasjonale ID-kort til utenlandske borgere

Som beskrevet i kapittel 2 skal nasjonale ID-kort på sikt også utstedes til utenlandske borgere. Pass- og ID-kontorene har per i dag kjernekompetanse på identitetsfastsettelse og dokumentkontroll av norske borgere. Utstedelse av nasjonale ID-kort til utlendinger vil stille krav til både økt og endret kompetanse ved pass- og ID-kontor. Per i dag er dette kompetanse som ansatte ved utlendingskontorene i stor grad besitter. Dette gjelder blant annet dyptgående kunnskap om utenlandske dokumenter, moduser og generell landkunnskap som kan brukes i samtaler med utlendinger ved behandling av saker.

Utstedelse av nasjonalt ID-kort til utlendinger vil videre kreve et ekstra oppmøte for utlendinger, gitt dagens struktur og organisering med utstedelse på pass- og ID-kontor. I tillegg til oppmøte hos politiets utlendingskontor og/eller skattekontor (eventuelt oppmøte i to separate skranker på SUA), vil utlendingen måtte møte opp på et pass- og ID-kontor for å kunne skaffe seg et nasjonalt ID-kort.

Poengene synliggjort over resulterer i både behov og mulighet for å tenke nytt rundt dagens kompetanse og skrankepunktorganisering med tanke på sikkerhet, brukervennlighet og ressursbruk. Dette er tatt med videre inn i leverandørens vurdering.

4.2 Prosesser med ID-relaterte oppmøter

I dette kapittelet illustreres og beskrives relevante eksisterende prosesser slik de gjennomføres i dag knyttet til ID-relaterte oppmøter i politiet, Skatteetaten og UDI. Prosessen for søknad om pass og/eller nasjonalt ID-kort viser fremtidig prosess ved pass- og ID-kontorene. Prosessene kan helt eller delvis vurderes til å bli en del av et felles skrankepunkt. Prosessene er fremstilt på et overordnet nivå med delprosesser og tilhørende aktiviteter bygget på dokumentasjon mottatt fra involverte aktører.

4.2.1 Overordnet prosessoversikt

En oversikt over relevante ID-prosesser som krever oppmøte vises i tabellen nedenfor. Tallene gjelder hovedsakelig antall førstegangssøknader om ikke annet er spesifisert.

[160] Informasjon fra presentasjon holdt av Øst politidistrikt ved besøk på Grålum politistasjon, andre halvår 2019

Etat/enhet	Oppmøte-sted	Prosess	Brukergruppe	Omfang (ca.) 2018
Politiet	Pass- og ID-kontor	Søknad om pass og/eller nasjonalt ID-kort	Norske borgere	705 000 søknader[161]
Politiets utlendings-enhet	Utlendings-kontor eller SUA	EØS-registrering	EØS-borgere	38 400 innkomne saker (20 400 på SUA)
		Søknad om oppholdstillatelse og utstedelse av oppholdskort	Tredjelandsborgere	65 600 søknader om opphold[162]
		Søknad om oppholdskort for familiemedlemmer av EU/EØS-borgere	Tredjelandsborgere	1 500 innleverte saker
	Utlendings-kontor	Søknad om statsborgerskap	EØS-borgere og tredjelandsborgere	18 950 innkomne saker
		Søknad om utlendingspass og reisebevis	Tredjelandsborgere (hovedsakelig asylsøkere)	20 000 innkomne saker[163]
Skatte-etaten	Skattekontor eller SUA	Søknad om skattekort for personer som ikke har fødselsnummer eller «kontrollert» d-nummer	EØS-borgere og tredjelandsborgere	144 000 kontroller gjennomført totalt[164] (29 000 på SUA)
		Melde innflytting til Norge fra utlandet	EØS-borgere, tredjelandsborgere, norske borgere	(12 100 på SUA)
	Skattekontor	ID-kontroll gjennomført på vegne av andre rekvirenter i tilfeller der det kreves status «kontrollert» eller bruker ønsker å bli «kontrollert»	EØS-borgere og tredjelandsborgere	200 kontroller

Tabell 20 Prosesser for ID-relaterte oppmøter med oppmøtested, brukergrupper og omfang

Prosessene over viser ID-relaterte oppmøter med tilhørende oppgaver i politiet, Skatteetaten og UDI. Andre prosesser som innebærer et krav eller valg om et ID-relatert oppmøte er bevisst holdt utenfor oversikten og ikke nærmere vurdert. Dette gjelder:

- Saksbehandling og øvrige oppgaver i politiet, Skatteetaten og UDI som ikke er knyttet til ID, men som er andre typer forvaltningsoppgaver
- Prosesser/oppmøter i Skatteetaten (der det er et valg å møte opp) der volumet av saker er lavt og primært gjøres digitalt. Dette gjelder blant annet erklæring av farskap[165], bytting av navn, ekteskapsprøving, melding om dødsfall og mottak av attester

[161] Inkludert fornyelser
[162] Inkluderer familieinnvandringssøknader, alle typer arbeidssøknader, utdanningssøknader og permanente tillatelser
[163] Inkludert fornyelser
[164] Skatteetaten har ikke data på antall saker fordelt på de ulike prosessene, kun det totale tallet på antall ID-kontroller gjennomført
[165] Dette kan også gjøres av lege eller jordmor i forbindelse med svangerskapskontroll/fødsel eller ved NAV-kontor

- Asylsøkerprosessen da denne i hovedsak gjennomføres i PUs førstelinje, samt at prosessen har flere særegenheter. PU og UDI jobber med å inngå et tettere samarbeid for ny asylsaksflyt ved samlokalisering på mottakssenteret i Råde[166]

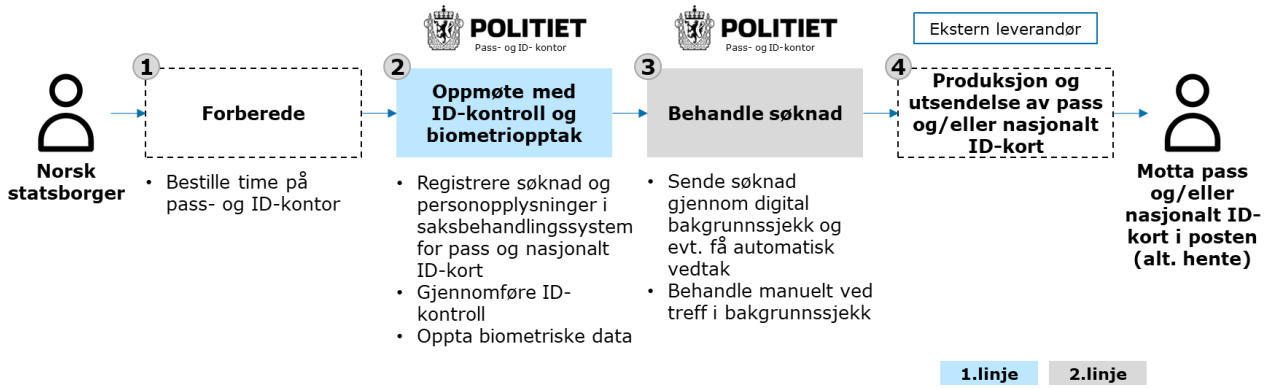
- Prosesser som delvis håndteres av politidistriktene, men som ikke medfører oppmøte i skrankepunkt som mottak av overføringsflyktninger, saker om utvisning og avslags- og tilbakekallssaker. Disse sakene kan kreve oppmøte, men dette finner i så fall sted i andrelinjen til politiet eller UDI etter leverandørens definisjoner

- Utstedelse av sjøfartsbok. Gjennomføres per i dag av NAV. Sjøfartsboken skal erstattes av et ID-kort for sjøfolk og vil etter planen utstedes av pass- og ID-kontor fra 2020

I følgende kapitler gjennomgås prosessene som fremstilt i tabellen over med illustrasjon og beskrivelse. Beskrivelsene er basert på svar mottatt på utsendt dataforespørsel til politiet, Skatteetaten og UDI, samt samtaler og oppfølging.

4.2.2 Søknad om pass og/eller nasjonalt ID-kort

Det understrekes igjen at denne prosessen (som den eneste) ikke fremstiller eksisterende prosess for utstedelse av pass, men fremtidig prosess for utstedelse av pass og/eller nasjonalt ID-kort fra 2020.



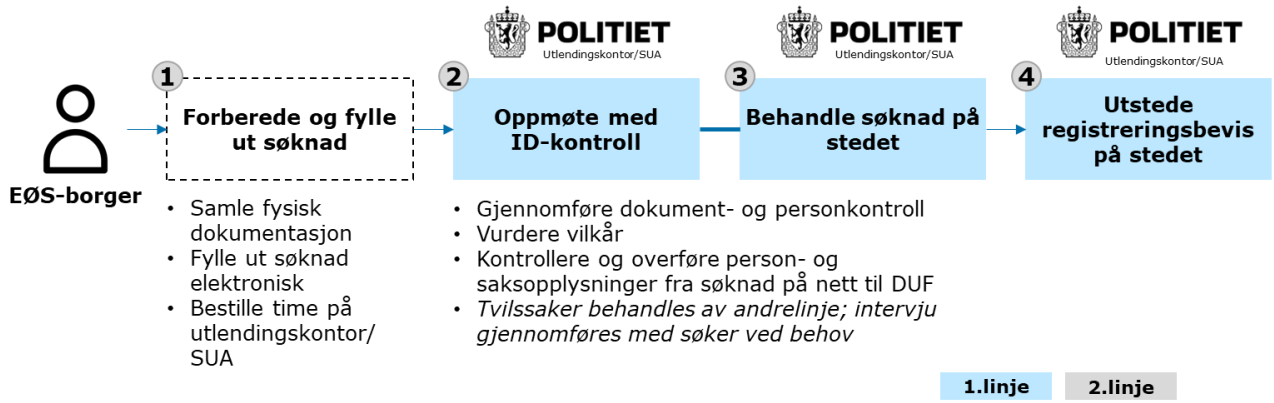
Figur 24 Prosess for søknad om pass

Ved utstedelse av pass og/eller nasjonalt ID-kort kreves det ett oppmøte der det foretas en ID-kontroll i skranken ved et pass- og ID-kontor. Nivået på ID-kontrollen som gjennomføres følger kravet i passloven, ID-kortloven og den kommende forskriften om pass og nasjonalt ID-kort om at søker må godtgjøre sin identitet for å ha rett til pass og/eller nasjonalt ID-kort. Kravet innebærer at det ikke skal være tvil om at søkeren er den vedkommende utgir seg for å være. Det opptas også biometriske data og opplysninger om søkeren blir registrert i saksbehandlingssystem for pass og nasjonalt ID-kort og lagres i saksarkiv og i passregisteret/ID-kortregisteret.

Det brukes i gjennomsnitt 20 minutter per søker i skrankepunktet. Alle søknader går så videre til andrelinje gjennom en digital bakgrunnssjekk. Kurante saker vedtas automatisk, uten ytterligere manuell behandling i andrelinje, mens saker med treff i bakgrunnssjekk eller flagging fra førstelinje behandles manuelt. Dette antas å gjelde ca. fem prosent av søknadene. Søker kan velge å møte opp fysisk for å hente passet og/eller det nasjonale ID-kortet eller å få det tilsendt i posten.

[166] JD, «Supplerende tildelingsbrev 2019 Utlendingsdirektoratet (UDI) – nr. 4», 2019

4.2.3 EØS-registrering



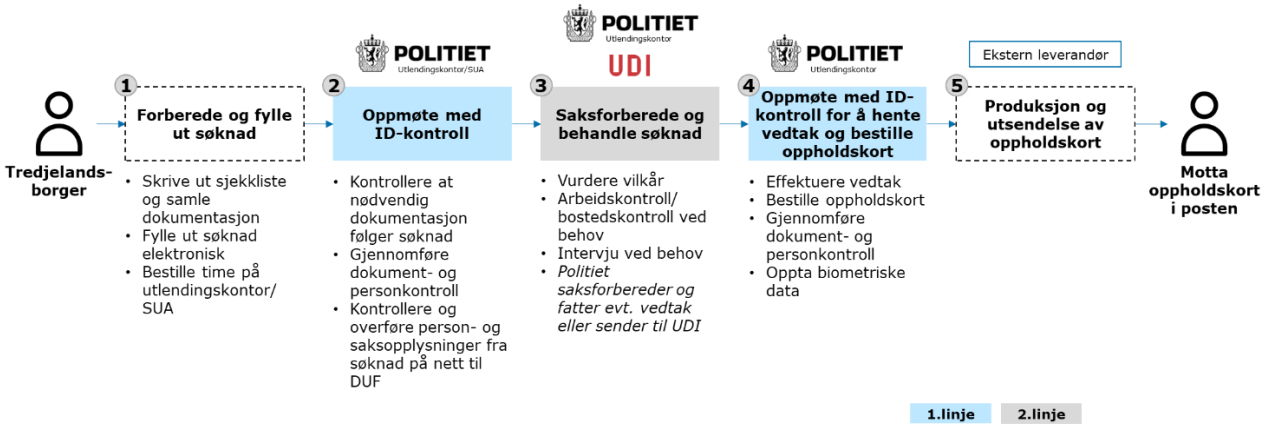
Figur 25 Prosess for EØS-registrering

Ved EØS-registering kreves det ett oppmøte der det foretas en ID-kontroll i skranken på utlendingskontor eller SUA-kontor. Majoriteten av ID-kontrollene som utføres i skrankepunktet er minimumskontroller, men det gjennomføres også utvidede kontroller for et betydelig antall saker. Ved utvidet kontroll gjennomføres kontrollen ofte av politidistriktenes andrelinje på ID eller saken blir sendt til tredjelinje. I forbindelse med oppmøtet i skrankepunktet kontrolleres og overføres person- og saksopplysninger fra søknad på nett til Datasystemet for utlendings- og flyktningsaker (DUF).

Det brukes i gjennomsnitt 12,5 minutter per EØS-borger i skrankepunktet, men noen av sakene kan ta betydelig lengre tid avhengig av ulike faktorer som for eksempel ID-tvil, tvil om arbeidsforhold etc. Tilnærmet alle søknadene blir behandlet direkte i skrankepunktet, noe som tilsier at en svært liten andel sendes videre til saksbehandling i andrelinje i UDI.

4.2.4 Søknad om oppholdstillatelse og utstedelse av oppholdskort

Det er mulig for brukere å søke om oppholdstillatelse fra utlandet via utenriksstasjonene, men gitt forutsetningene i kapittel 4.1.1 er prosessen kun tegnet opp og forklart for brukere som søker fra Norge.



Figur 26 Prosess for søknad om oppholdstillatelse og utstedelse av oppholdskort

Ved søknad om oppholdstillatelse og utstedelse av oppholdskort kreves det to oppmøter. Under første oppmøte gjennomføres det en ID-kontroll i skranken på et utlendingskontor eller et SUA-kontor. Majoriteten av ID-kontrollene som utføres i

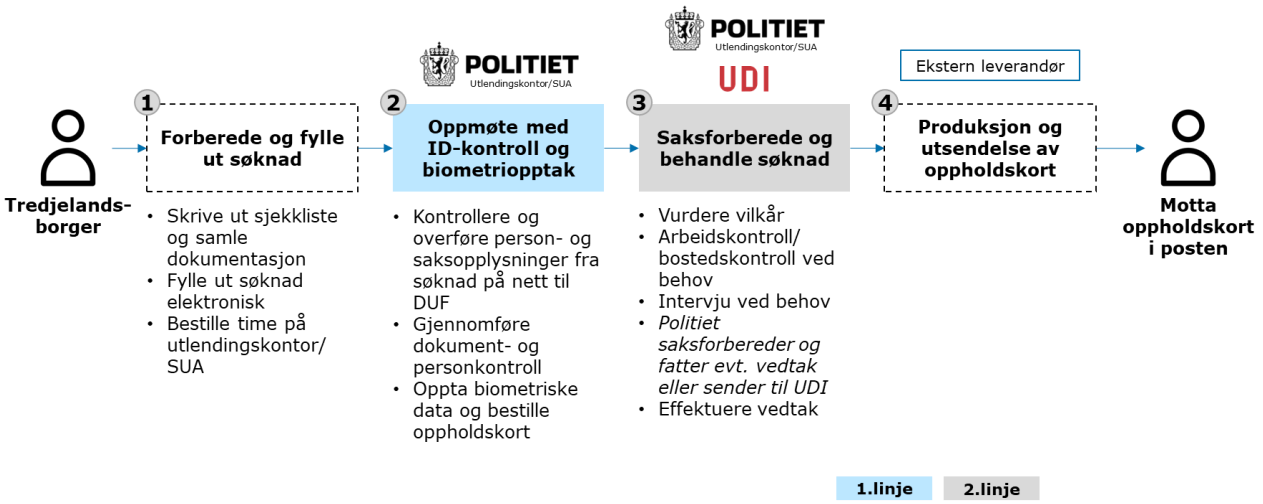
skrankepunktet er minimumskontroller, men det gjennomføres også utvidede kontroller for et betydelig antall saker. Under det første oppmøtet i skrankepunktet kontrolleres og overføres person- og saksopplysninger fra søknad på nett til DUF. Ved det andre oppmøtet effektueres vedtaket og det opptas biometriske data til oppholdskortet (utlendingspass/reisebevis kan også bestilles samtidig om bruker har behov for dette). I forbindelse med det andre oppmøtet i skrankepunktet sendes det også automatisk en melding til Skatteetaten om at søkeren har flyttet til Norge, og søkeren får dermed tildelt et fødselsnummer eller eventuelt et d-nummer i denne prosessen om søker ikke har dette fra før, som blir stående som «kontrollert» i Folkeregisteret.[167]

Det brukes i gjennomsnitt 12,5 til 15 minutter per søker i skrankepunktet ved det første oppmøtet, men politiet poengterer at tidsbruken som er satt av i noen politidistrikt er lengre (opp mot 30 minutter). Mer tid i skrankepunkt betyr at skrankepersonell gjør mer av den forberedende saksbehandlingen direkte i skrankepunkt før den sendes til andrelinje i politiet. Ved det andre oppmøtet brukes det i gjennomsnitt 12,5 til 15 minutter. Samlet sett er den totale tiden i skrankepunktet på ca. 30 minutter. Kun et fåtall saker blir behandlet i skrankepunktet i sin helhet. Majoriteten av saker blir sendt til behandling utenfor skrankepunkt, men fortsatt hos politiet. Etter saksforberedelse utenfor skrankepunkt fatter politiet vedtak i de sakene de har fått delegert vedtaksmyndighet, mens øvrige saker ekspederes til UDI. Saksforberedelse kan være alt fra å innhente ytterligere dokumentasjon til å gjennomføre forvaltningsintervjuer.

Det er i løpet av 2020 planlagt å fjerne effektueringsoppmøtet ved søknad om opphold da dette ikke er nødvendig for å produsere oppholdskort, fordi politiet skal ta opp biometriske data allerede ved første oppmøte når det søkes om oppholdskort. [168] Dette vil redusere antall oppmøter i oppholdssaker fra to til ett ved innføring.

4.2.5 Søknad om oppholdskort for familiemedlemmer av EU/EØS-borgere

Hvis en tredjelandsborger er familiemedlem av en EU/EØS-borger i Norge kan borgeren søke om å bli registrert etter EU/EØS-regelverket.



Figur 27 Prosess for søknad om oppholdskort for familiemedlemmer av EU/EØS-borgere

Ved søknad om oppholdskort for familiemedlemmer av EU/EØS-borgere kreves det ett oppmøte der det foretas en ID-kontroll i skranken på et utlendingskontor eller et SUA-

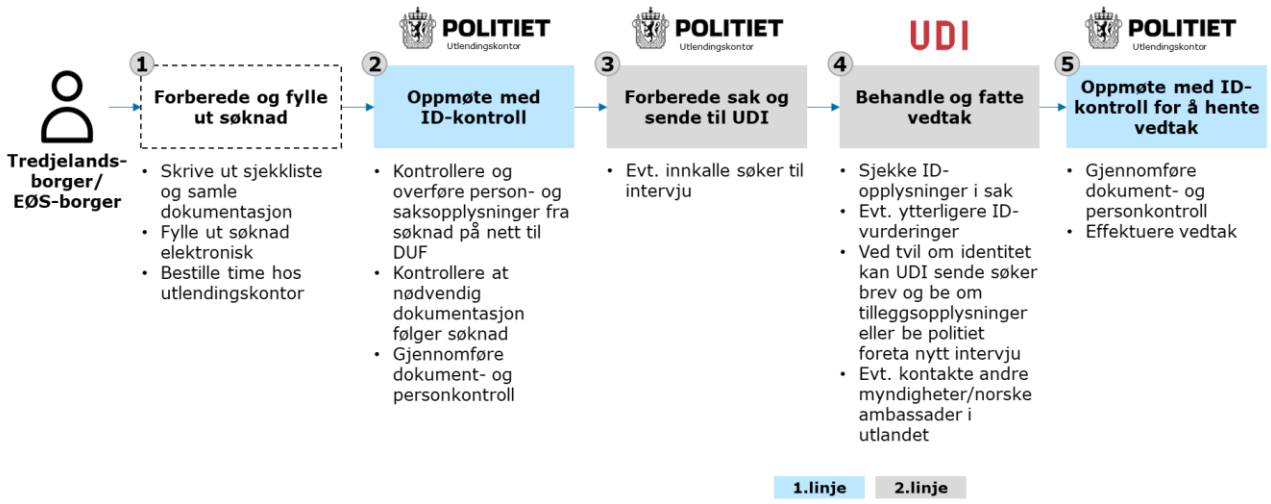
[167] Fremgår av informasjonsutvekslingsavtale mellom Skattedirektoratet og UDI
[168] Informasjon mottatt på e-post fra UDI, andre halvår 2019

kontor. Som ved EØS-registreringsprosessen og oppholdsprosessen over, er majoriteten av ID-kontrollene som utføres i skrankepunktet minimumskontroller, men det gjennomføres også utvidede kontroller for et betydelig antall saker. Under oppmøtet i skrankepunktet kontrolleres og overføres person- og saksopplysninger fra søknad på nett til DUF og det opptas biometriske data.

Det brukes i gjennomsnitt 12,5 til 15 minutter per søker i skrankepunktet, men det poengteres at tidsbruken som er satt av i noen politidistrikt er lengre (opp mot 30 minutter). Kun et fåtall saker blir behandlet i skrankepunktet i sin helhet. Førstegangs- og fornyelsessaker blir sendt til behandling utenfor skrankepunktet, og saksbehandlingen foretas hos politiets andrelinje. Politiet fatter vedtak i de saker politiet har vedtakskompetanse, øvrige saker ekspederes til UDI etter saksforberedelse.

Familiemedlemmer av EØS-borgere må melde flytting sammen med sitt EØS-registrerte familiemedlem på et skattekontor (prosess er beskrevet i kapittel 4.2.9).

4.2.6 Søknad om statsborgerskap



Figur 28 Prosess for søknad om statsborgerskap

Ved søknad om statsborgerskap kreves det to oppmøter. Ved første oppmøte gjennomføres det en ID-kontroll i skranken på utlendingskontor. Som ved prosessene over, er majoriteten av ID-kontrollene som utføres i skrankepunktet minimumskontroller, men det gjennomføres også utvidede kontroller for et betydelig antall saker. I forbindelse med det første oppmøtet i skrankepunktet kontrolleres og overføres person- og saksopplysninger fra søknad på nett til DUF. Ved det andre oppmøtet utføres ID-kontroll på nytt, vedtak effektueres og statsborgerskapsvedtaket utleveres søker.

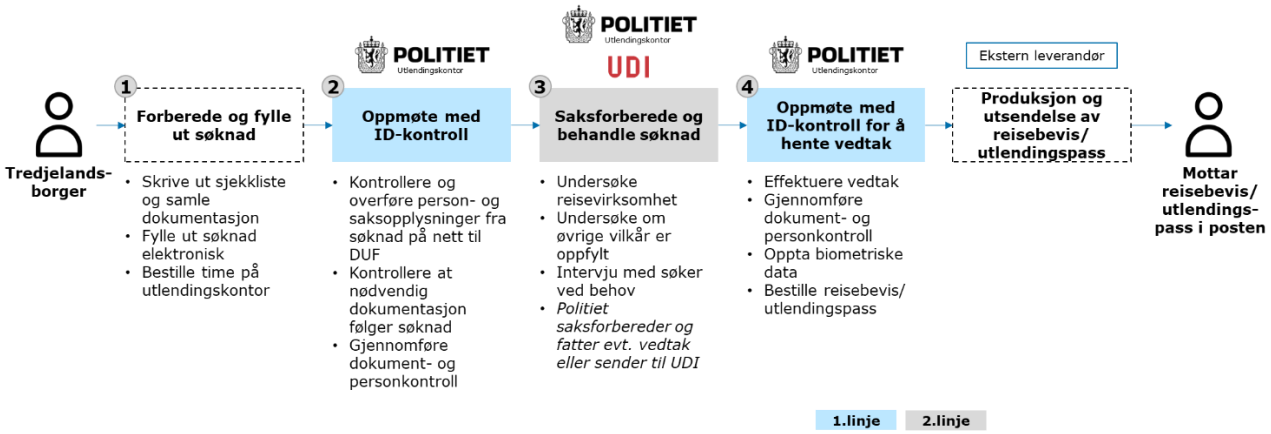
Det brukes i gjennomsnitt 12,5 minutter per søker i skrankepunktet hver gang, hvilket samlet sett gir en total tid på 25 minutter brukt i skrankepunkt per bruker. Alle søknader blir sendt til behandling hos politiet i andrelinje for saksforberedelse. Etter saksforberedelsen utenfor skrankepunktet sendes alle saker videre til UDI i andrelinje som behandler saken og fatter vedtak.

Det vil i løpet av 2020 være automatiserte vedtak i statsborgerskapssaker, noe som vil effektivisere saksbehandlingen av statsborgerskapssaker i andrelinjen i UDI, men ikke ha innvirkning på antall oppmøter.[169]

[169] Informasjon mottatt på e-post fra UDI, andre halvår 2019

Når en søker har fått innvilget norsk statsborgerskap kan personen også søke om norsk pass eller nasjonalt ID-kort med reiserett. Dette krever enda et nytt oppmøte på et pass- og ID-kontor, etter prosessen beskrevet for pass- og ID-kontorene i kapittel 4.2.2.

4.2.7 Søknad om utlendingspass og reisebevis

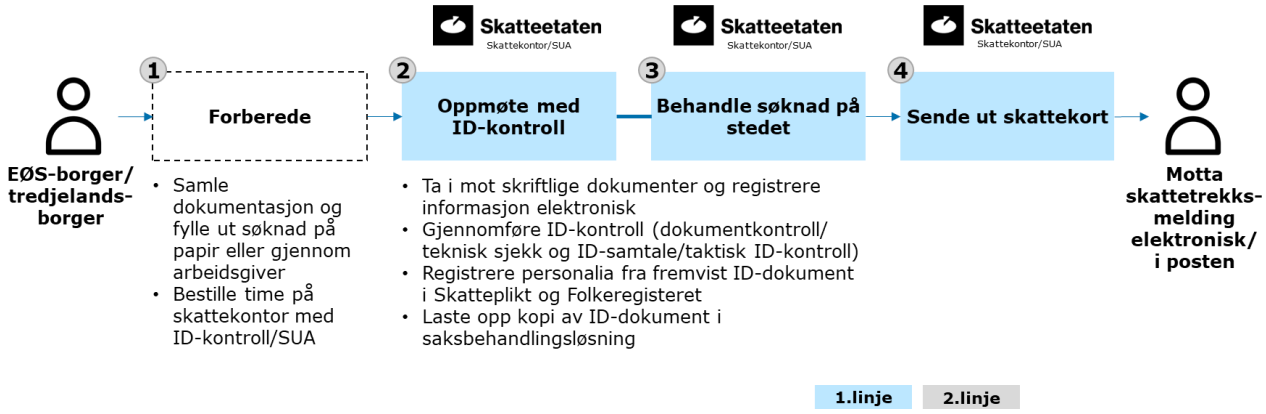


Figur 29 Prosess for søknad om utlendingspass og reisebevis

Ved søknad om utlendingspass eller reisebevis for flyktninger kreves det to oppmøter. Ved det første oppmøte gjennomføres det en ID-kontroll i skranken på et utlendingskontor. Som ved prosessene over, er majoriteten av ID-kontrollene som utføres i skrankepunktet minimumskontroller, men det gjennomføres også utvidede kontroller for et betydelig antall saker. I forbindelse med det første oppmøtet i skrankepunktet kontrolleres og overføres person- og saksopplysninger fra søknad på nett til DUF. Ved det andre oppmøtet uføres ID-kontroll, vedtaket effektueres og søker avgir biometrisk data. Det bestilles deretter et reisebevis/utlendingspass til søker.

Det brukes i gjennomsnitt 12,5 minutter per søker i skrankepunktet hver gang, noe som gir en tid på 25 minutter totalt for tid brukt i skrankepunkt per bruker. Alle søknader bli sendt til behandling hos politiet i andrelinje for saksforberedelse. Saksforberedelse kan være alt fra å innhente ytterligere dokumentasjon til å gjennomføre forvaltningsintervjuer. Etter saksforberedelsen utenfor skrankepunkt fatter politiet vedtak i de sakene politiet har fått delegert vedtaksmyndighet, mens øvrige saker ekspederes til UDI som fatter vedtak.

4.2.8 Søknad om skattekort for personer som ikke har fødselsnummer eller «kontrollert» d-nummer



Figur 30 Prosess for søknad om skattekort for personer som ikke har fødselsnummer eller «kontrollert» d-nummer

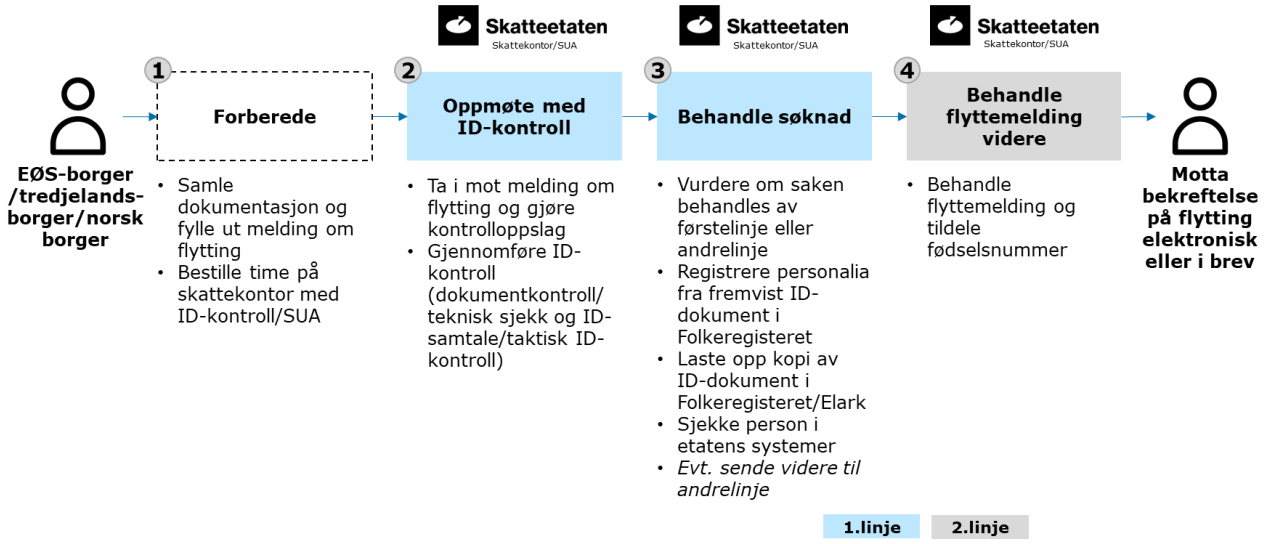
Ved utstedelse av skattekort til personer som ikke har fødselsnummer eller «kontrollert» d-nummer kreves det ett oppmøte ved et skattekontor eller på SUA-kontor (gjelder også for borgere med inaktivt d-nummer som må reaktivere det). Ved oppmøtet gjennomføres en ID-kontroll av personen som søker. Det kontrolleres også om personen har arbeidsadgang og det gjøres kontroll av arbeidskontrakt eller evt. annen dokumentasjon som kan sannsynliggjøre behovet for skattekort.

ID-kontrollen består vanligvis av en visuell sammenligning av borgeren og ansiktsfoto på fremvist ID-dokument, skanning av ID-dokument for ekthetssjekk og undersøkelse av ID-dokumentet med UV-lys og lupe. Under oppmøtet registreres brukerens personalia i Skatteplikt og Folkeregisteret. Et identitetsnummer rekvireres og identitetsnummeret får status «kontrollert» i Folkeregisteret.

Det er tildelt 15 minutter i timebestillingen per person per sak i skranken for kurante saker, der ca. fem minutter brukes til ID-kontroll og ca. 10 minutter brukes til saksbehandling direkte i skrankepunkt. I realiteten tar ofte hele saksbehandlingen 20-25 minutter, og resterende saksbehandling som det ikke blir tid til når søker er til stede gjennomføres i skrankepunkt i etterkant av oppmøtet. Alle saker blir behandlet direkte i skrankepunktet[170], og kun ca. to prosent av saker har ID-relaterte spørsmål som rettes til andrelinje via telefon, mail eller Skype. Hvis dokumentet synes å være falskt, eller søker fremstår å være imposter, blir saken overført til politiets andrelinje for videre behandling.

[170] Skatteetaten har ingen andrelinje for behandling av skattekort

4.2.9 Melde innflytting til Norge fra utlandet



Figur 31 Prosess for å melde innflytting til Norge fra utlandet

Ved melding om innflytting til Norge kreves det ett oppmøte ved et skattekontor eller på SUA-kontor. ID-kontrollen er den samme som ved søknad om skattekort beskrevet over. Som del av saksbehandlingen kontrolleres personalia i fremvist ID-dokument opp mot personalia på registreringsbevis eller oppholdskort, utfylt innflyttingsmelding og eventuelt allerede registrerte opplysninger i Folkeregisteret. Manglende personalia registreres i Folkeregisteret, og en kopi av fremvist ID-dokument lagres i Elark[171]. Dersom det er avvikende opplysninger mellom ID-dokument og informasjon som fremkommer i oppholdskort eller registreringsbevis eller innflyttingsmeldingen må det avklares hva som er rett informasjon før saken kan ferdigbehandles.

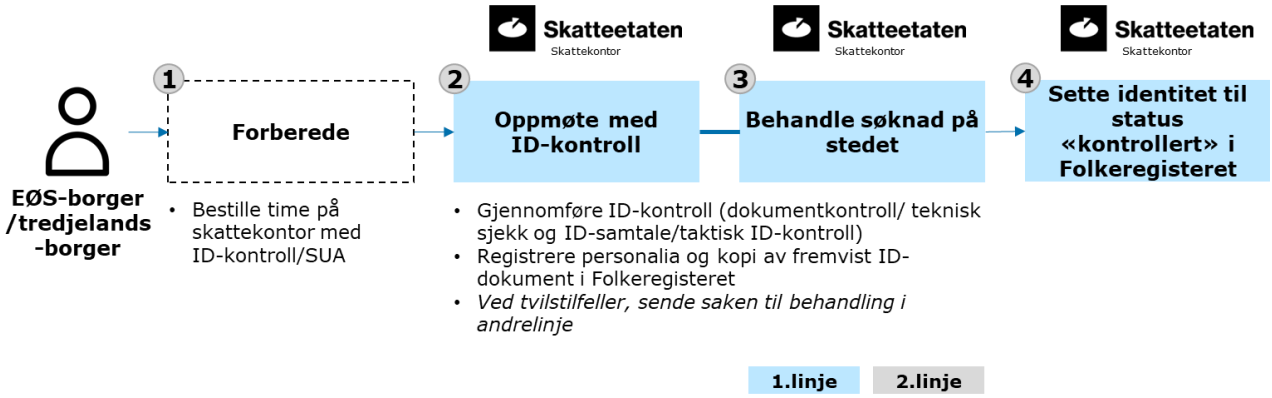
Det er tildelt 15 minutter i timebestillingen per person per sak i skranken for kurante saker, der ca. fem minutter brukes til ID-kontroll. Saksbehandleren i skrankepunktet har videre ca. 10 minutter til å motta innflyttingsmeldingen, kontrollere at alle opplysninger er fylt ut, gjøre nødvendige kontrolloppslag og vurdere om fremlagt dokumentasjon er tilstrekkelig for at brukeren oppfyller hensikten med å skulle bosettes i Norge. I realiteten tar ofte hele saksbehandlingen 20-25 minutter, og resterende saksbehandling som det ikke blir tid til når søker er til stede gjennomføres i skrankepunkt i etterkant av oppmøtet. Ved melding om innflytting er det flere systemer som må sjekkes, så behandlingstiden i skranken er ofte lengre enn ved søknad om skattekort som beskrevet over. Dersom saken er ukurant kan bruker bes om å komme tilbake med ytterligere dokumentasjon eller saken kan sendes til andrelinje. Per i dag går i gjennomsnitt 43 prosent av sakene til andrelinje for videre behandling.[172]

For EØS-borgere er det per i dag krav om å fremlegge registreringsbevis for å melde innflytting.[173] Dersom borgeren har mistet sitt bevis og ikke har en kopi fra politiet gjør Skatteetaten en utskrift fra OHS som er en oppholdsstatustjeneste fra UDI. Skatteetaten gjør uansett alltid et oppslag i OHS for å sikre at EØS-borgeren er registrert. For tredjelandsborgere som har fått oppholdstillatelse sendes det, som nevnt i kapittel 4.2.4, automatisk melding til Skatteetaten om at borgeren flytter til Norge

[171] Skatteetatens sak-, journal- og arkivsystem
[172] Det påpekes at dette tallet er tatt ut fra enkelte SUA-kontorer og ikke er et snitt over de 42 ID-kontorene samlet
[173] Leverandøren har blitt opplyst på e-post fra Skatteetaten, andre halvår 2019, om at det pågår et arbeid mellom Skatteetaten og FIN om å gå bort fra kravene om å fremlegge registreringsbevis og heller skulle vurdere lovlig opphold og hvorvidt dette er oppfylt i forbindelse med melding om innflytting

når det bestilles oppholdskort hos politiet. Borgeren trenger derfor ikke møte på skattekontor for å melde flytting.[174]

4.2.10 ID-kontroll gjennomført på vegne av andre rekvirenter i tilfeller der det kreves status «kontrollert» eller bruker ønsker å bli «kontrollert»



Figur 32 Prosess for gjennomføring av ID-kontroll på vegne av andre rekvirenter

Ved ID-kontroll gjennomført på vegne av andre rekvirenter kreves ett oppmøte ved et skattekontor. ID-kontrollen er den samme som ved søknad om skattekort beskrevet over. Som en del av ID-kontrollen registreres brukers personalia fra fremvist ID-dokument i Folkeregisteret og en kopi av ID-dokumentet lastes opp i Elark.

Det brukes i snitt ca. 15 minutter per søker i skrankepunkt for kurante saker, der ca. fem minutter brukes til ID-kontroll og ca. 10 minutter til resterende saksbehandling direkte i skrankepunkt. Tilnærmet alle sakene blir behandlet direkte i skrankepunktet, og kun ca. to prosent av saker har ID-relaterte spørsmål som rettes til andrelinje via telefon, mail eller Skype.

4.2.11 Oppsummering av prosesser og oppmøter per brukergruppe med dagens prosesser

I hovedrapportens kapittel 5.1.5 og 5.1.6 ble det fremstilt overordnede brukerreiser for utstedelse av identitetsnummer og ID-bevis for norske borgere, EØS-borgere og tredjelandsborgere. For oppsummering av prosesser og oppmøter i dette kapitlet er det delvis tatt utgangspunkt i disse prosessene.

Tabellen nedenfor gir en oversikt over antall fysiske oppmøter for utvalgte brukergrupper, samt hvilke prosesser oppmøtene er tilknyttet gitt dagens situasjon inkludert planlagte endringer. Antall oppmøter gjelder for saker som er kurante og ikke krever ytterligere oppmøter i skrankepunkt (ytterligere oppmøter kan eksempelvis være oppmøte for å levere manglende dokumentasjon). Oppmøter for fornyelser av ID-bevis og øvrige tillatelser er ikke inkludert i antall oppmøter.

[174] Skatteetaten, «Melding om flytting til Norge», u.å.

Brukergruppe	Antall oppmøter	Prosesser tilknyttet oppmøtene	Kommentarer
Norsk borger	**1**	• Søknad om pass og/eller nasjonalt ID-kort	
EØS-borger[175]	**4**	• EØS-registrering • Søknad om skattekort for personer som ikke har fødselsnummer eller «kontrollert» d-nummer • Melde innflytting til Norge fra utlandet • Søknad om nasjonalt ID-kort	Noen EØS-borgere kan gjennomføre søknad om skattekort og melding av innflytting i ett oppmøte. Likevel gjør mange det i to oppmøter da EØS-borgere må ha registreringsbevis for å melde innflytting og det er lang ventetid mange steder for å registrere seg.
Tredjelands-borger (opphold)	**2**	• Søknad om opphold (levere søknad) • Søknad om nasjonalt ID-kort	Det registreres innflytting i forbindelse med søknad om oppholdskort og søker får automatisk et identitetsnummer.
Tredjelands-borger (opphold) som er familiemedlem av EØS-borger	**3**	• Søknad om oppholdskort for familiemedlemmer av EU/EØS-borgere • Melde innflytting til Norge fra utlandet (sammen med registrert EØS-borger) • Søknad om nasjonalt ID-kort	Bruker må møte opp på et utlendingskontor, et skattekontor og et pass- og ID-kontor.
Tredjelands-borger/EØS-borger (norsk statsborgerskap)	**3**	• Søknad om norsk statsborgerskap (levere søknad) • Søknad om norsk statsborgerskap (hente vedtak) • Søknad om pass og/eller nasjonalt ID-kort	Bruker vil sannsynligvis ha fått nasjonalt ID-kort før han/hun blir norsk statsborger, men kan som norsk borger anskaffe nasjonalt ID-kort med reiserett.
Tredjelands-borger (utlendingspass/ reisebevis)	**2**	• Søknad om utlendingspass/reisebevis (levere søknad) • Søknad om utlendingspass/reisebevis (hente vedtak)	Den største gruppen av søkere er asylsøkere med innvilget asylsøknad og denne brukergruppen får ikke tilbud om å søke nasjonalt ID-kort som drøftet i kapittel 2.2.5.

Tabell 21 Oversikt over fysiske oppmøter og tilhørende prosesser for ulike brukergrupper

Sammenfallende aktiviteter i prosessene

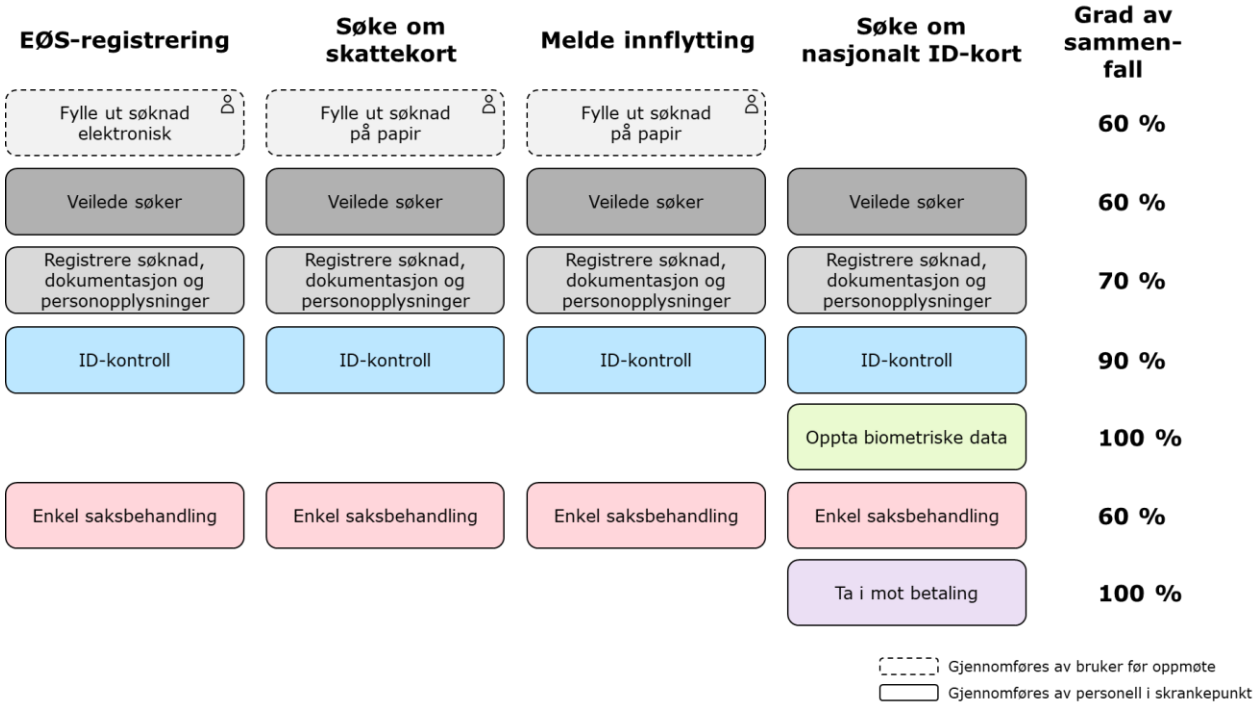
EØS-borgere og tredjelandsborgere må, som tabellen over viser, møte opp fysisk ved et skrankepunkt minst to til fire ganger for å gjennomføre nødvendige prosesser. Flere av prosessene har sammenfallende aktiviteter og informasjonskrav noe som medføre

[175] Om borgeren møter på SUA-kontor kan dette potensielt redusere antall oppmøter til 2, men borger må fortsatt gjennom tre prosesser

at søker oppgir samme informasjon flere ganger i de tilfeller hvor data ikke deles på tvers av aktører og systemer.

EØS-borger

Figuren nedenfor viser prosessene en EØS-borger ofte må gjennomføre og aktivitetene som gjennomføres i skrankepunktet ved hver prosess. Leverandøren vurderer likheten i aktivitetene på tvers av prosessene, noe prosenttallene til høyre i skissen reflekterer. ID-kontroll, mottak av betaling og opptak av biometriske data antas å være tilnærmet like aktiviteter på tvers av prosessene. For resterende aktiviteter; utfylling av søknad, veiledning, registrering og enkel saksbehandling, vurderer leverandøren at kjernen i aktivitetene er av samme art. Likevel vurderes total likhet i aktivitetene på tvers av prosessene til å være 60-70 prosent på grunnlag av at det kreves ulik dokumentasjon, opplysninger og kompetanse i de ulike prosessene.



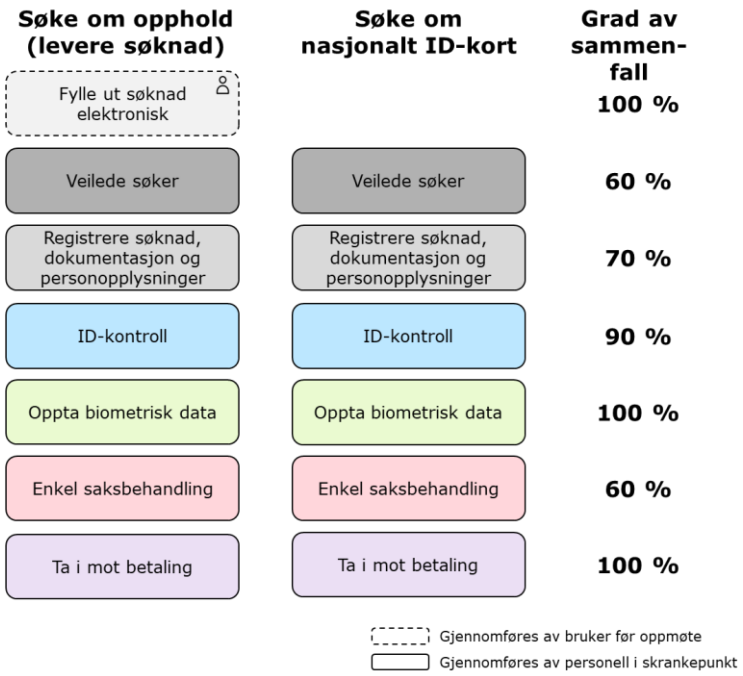
Figur 33 Aktiviteter og likhet for en EØS-borger i utvalgte prosesser

Det er tungvint og lite effektivt at bruker må oppgi samme informasjon flere ganger. Dette gjelder spesielt i forbindelse med EØS-registrering og søknad om skattekort der samme informasjon må oppgis henholdsvis elektronisk og på papir.

Tredjelandsborgere

Figuren nedenfor fremstiller prosessene en tredjelandsborger som søker opphold ofte må gjennomføre og aktivitetene som gjennomføres i skrankepunktet ved hver prosess.[176] Også for tredjelandsborgere er det en viss grad av likhet i aktivitetene på tvers av prosessene som gjennomføres. På samme møte som for EØS-borgere antas ID-kontroll, mottak av betaling og opptak av biometriske data å være tilnærmet like aktiviteter på tvers av prosessene. Utfylling av søknad gjøres for tredjelandsborgere som søker opphold kun én gang. For veiledning, registrering og enkel saksbehandling vurderes det som for EØS-borgere at kjernen i aktivitetene er av samme art, men at total likhet er 60-70 prosent grunnet krav om ulik dokumentasjon, opplysninger og kompetanse i de ulike prosessene.

[176] Søkere av opphold er brukt som eksempel da dette er den største gruppen tredjelandsborgere



Figur 34 Aktiviteter og likhet for en tredjelandsborger som søker opphold i utvalgte prosesser

4.3 Styrker og utfordringer ved dagens organisering av skrankepunkt i ID-forvaltningen

Nedenfor følger leverandørens vurdering av de viktigste styrkene og utfordringene ved dagens ansvars- og oppgavefordeling i og mellom de ulike skrankepunktene. Styrkene og utfordringene forutsetter at alle vedtatte planer og tiltak på ID-området gjennomføres.

	Styrker	Utfordringer
Sikkerhet	- Nytt, mer sikkert saksbehandlings-system for utstedelse av pass og nasjonale ID-kort er planlagt implementert - Oppmøtekrav for førstegangs-utstedelse og fornyelse av ID-bevis - Politiets førstelinje dekker store deler av utlendingsforvaltningen - Flere fagmiljø med høy kompetanse innenfor egne ansvarsområder - Hver enkelt rekvirent vurderer begrunnet behov for d-nummer	- ID-kontroll utføres av mange aktører med varierende kvalitet og krav til kompetanse - Manglende felles begrepsbruk, rutiner og retningslinjer for samme type aktiviteter - Ulik praksis for å registrere informasjon - Status «kontrollert» for d-nummer kreves ikke tilstrekkelig ofte - Biometri kontrolleres ikke av andre aktører enn politiet
Bruker-vennlighet	- Samlokalisering av flere tjenester som krever oppmøter på SUA-kontor - Biometriprosjektet til UDI gir etter implementering kun ett oppmøte for tredjelandsborgere som søker opphold etter tredjelandsregelverket	- Kravet til oppmøter hvor like aktiviteter eller opplysninger registreres flere ganger medfører et høyt antall oppmøter for EØS-borgere - Lang behandlingstid for enkelte prosesser - Lang ventetid for timebestilling
Ressurs-bruk	- Hver aktør har kontroll over egen ressursbruk og ressurser allokeres hvor behovet er størst - Skatteetaten utnytter ID-kontrollen fra utlendingsforvaltningen - Saksbehandling ved pass- og ID-kontorene er blitt mer effektiv	- Sammenfallende oppgaver i ID-prosessene og dobbeltarbeid på tvers av etater (registrering, ID-kontroll etc.) - Parallell infrastruktur i skrankepunktene - Parallelle kompetansemiljøer i politiet - Krevende å styre ressursinnsats ved sesongvariasjoner - Lav bevissthet tilknyttet ressursbruk - Generelt for lite fokus på deling av data[177] og «kun en gang» for bruker
Annet	- Relativt enkle styringslinjer (ID-oppgaver gjøres på vegne av aktøren selv, og ikke på vegne av andre) - Etatene har ulike myndighetsoppgaver med robuste og tydelig definerte regelverk	- Noe uklarheter og uenigheter om ansvar- og rollefordeling - Manglende tillit til oppgaveutførelse og kompetanse på tvers av aktører

Tabell 22 Viktigste styrker og svakheter for sikkerhet, brukervennlighet, ressursbruk og annet

Oppsummering

Styrkene over samsvarer godt med leverandørens tidligere vurdering knyttet til styrkene ved dagens ID-forvaltning, kapittel 8.2 i hovedrapporten. Leverandøren vurderer de viktigste styrkene ved dagens skrankepunkt til å være:

- Tydelig ansvars- og rollefordeling med enkle styringslinjer: ID-oppgaver gjøres i stort på vegne av aktøren selv, etter egne risikovurderinger
- Noe tverrgående samarbeid: samlokalisering av flere tjenester som krever oppmøter på SUA-kontor

Utfordringene vurdert i hovedrapporten, kapittel 8.3 følger også utfordringene skissert over. Leverandøren vurderer de viktigste utfordringene ved dagens skrankepunkt til å være:

[177] Nettsted regjeringen.no: Starter arbeid med stortingsmelding om datadrevet økonomi og innovasjon, Pressemelding 02.12.2019

- Unødvendig mange oppmøter, spesielt for EØS-borgere, hvor samme aktiviteter eller informasjon registreres flere ganger
- ID-relaterte skrankepunkt hos de ulike aktørene har forskjellig praksis, rutiner og retningslinjer for håndtering av ID-relaterte oppgaver
- Sammenfallende aktiviteter i ID-prosessene, dobbeltarbeid på tvers av etater og liten grad av datadeling
- Parallelle kompetansemiljøer og infrastruktur

Som påpekt i hovedrapporten er det med bakgrunn i de identifiserte utfordringene et potensial for forenkling og for å redusere ressursbruk, øke brukervennlighet og øke sikkerhet.

4.4 Formål og alternative løsninger for et felles skrankepunkt

4.4.1 Formål med et felles skrankepunkt

Et felles skrankepunkt for ID-relaterte oppgaver kan være et viktig virkemiddel i arbeidet for å oppnå visjonen for ID-forvaltningen *«Én person, én identitet i Norge»,* samt hovedmålet og delmålene som skissert i hovedrapportens kapittel 16.1.1. Leverandøren har definert følgende formål med et felles skrankepunkt:

Formålet med et felles skrankepunkt er å sikre at ID-relaterte kjerneoppgaver knyttet til registrering og ID-kontroll utføres enhetlig, sikkert, effektivt og brukervennlig for definerte ID-prosesser på tvers av forvaltningen. Et felles skrankepunkt sikrer at både norske og utenlandske borgere kun trenger å oppgi informasjon én gang, får tilstrekkelig veiledning og oppnår rask søknadsbehandling, samtidig som antall fysiske oppmøter begrenses til et minimum. Skrankepunktets rutiner, retningslinjer og ansatte vil sikre enhetlig registrering av grunndata i riktige registre og utøve ID-kontroll både av norske og utenlandske borgere med betydelig spisskompetanse.

4.4.2 Overordnet om alternativene

Leverandøren har gjennom prosessen med tilleggsoppdraget gått fra flere mulige tilnærminger for samkjøring av ID-relaterte oppmøter i et felles skrankepunkt til å ende opp med to reelle alternativ som tilfredsstiller forutsetningen om alternative løsninger i kapittel 4.1.1. Dette er gjort i dialog med prosjektgruppen.

Leverandøren legger til grunn at de felles skrankepunktene legges til de 78 planlagte pass- og ID-kontorene. Politiets førstelinje er et naturlig valg som felles skrankepunkt, da de har identitetsregistrering og ID-kontroll som en av sine kjerneoppgaver, og innehar nødvendig kompetanse og infrastruktur i form av oppmøtesteder og teknisk utstyr. Leverandøren er kjent med risikoen ved at oppgaveporteføljen til politiet er svært stor og at det er fare for at mer kritiske ansvarsområder prioriteres, men dette er ikke nærmere vurdert i denne sammenhengen.[178]

Begge alternativene bygger på samme prinsipper hva gjelder ansvars- og arbeidsdeling mellom første- og andrelinje, men antall prosesser som inkluderes i skrankepunktet er forskjellig. I de felles skrankepunktene vil alle ansatte kunne motta alle typer saker og det vil følgelig være et felles køsystem hvor de fleste timene må bestilles på forhånd.

[178] Dette aspektet ble drøftet i hovedrapportens kapittel 15.2.4, september 2019

Todelt saksbehandling i første- og andrelinje

I kapittel 4.1.2 la leverandøren til grunn en definisjon av første- og andrelinje med tilhørende ansvars- og oppgavedeling for beskrivelse av nåsituasjonen og nåværende prosesser i kapittel 4.1–4.3. For å beskrive alternative løsninger for et felles skrankepunkt enhetlig har leverandøren videre brukt definisjonene første- og andrelinje, men i en litt annen form. Ansvars- og oppgavedelingen mellom første- og andrelinje er i beskrivelsen av alternativene som følger noe annerledes enn i nåsituasjonsbeskrivelsen.

Alternativene bygger på en todelt saksbehandling for ID-forvaltningen med fokus på å heve eksisterende sikkerhets- og kvalitetsnivå. Denne type saksbehandling er allerede planlagt innført på pass- og ID-kontorene ved behandling av søknader om nye pass og nasjonale ID-kort fra 2020. Bakgrunnen for dette er å styrke sikkerheten i saksbehandlingen med mål om å sikre at alle norske pass utstedes etter enhetlige prosesser.[179] Todelingen tydeliggjør ansvars- og oppgavedeling mellom første- og andrelinje og hvilke aktiviteter som gjennomføres hvor. Todelt saksbehandling er ikke et nytt fenomen for forvaltningen og praktiseres allerede, selv om det innholdsmessig ikke alltid praktiseres likt.

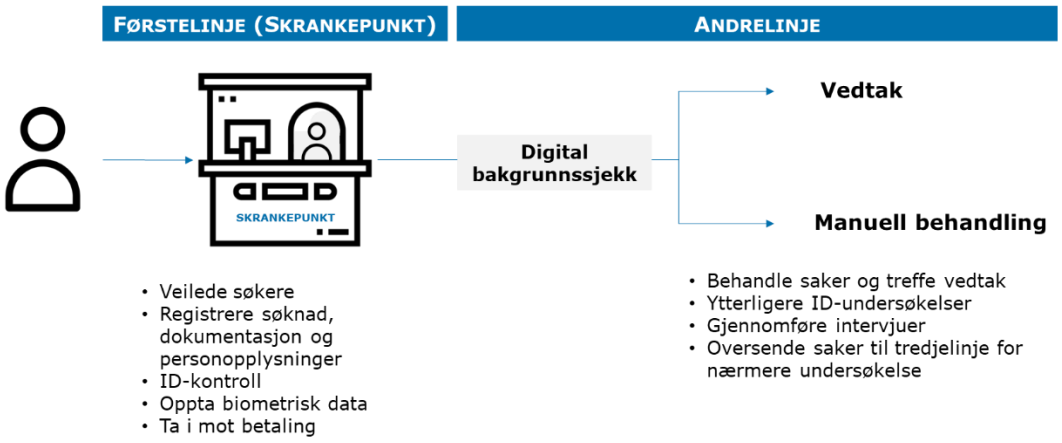
Med dette som utgangspunkt har leverandøren lagt til grunn at ansvars- og oppgavedelingen i første- og andrelinjen fordeler seg som følger:

- Førstelinjen veileder, mottar søknader, registrerer dokumentasjon og personopplysninger for alle typer saker som legges til et felles skrankepunkt. Videre gjennomfører førstelinjen ID-kontroll, opptar biometrisk data og tar imot betaling der dette er påkrevd. Dette er aktiviteter som gjennomføres i et felles skrankepunkt. Det gjøres ingen form for ytterligere saksbehandling i førstelinjen. Når aktivitetene er gjennomført oversendes saken fortrinnsvis digitalt til andrelinjen i enten politiet, UDI eller Skatteetaten avhengig av sakstype og hvilke prosesser som er inkludert i skrankepunktet.

- Andrelinjen mottar sak registrert i førstelinjen som er relatert til eget virksomhetsområde. Alle saker gjennomgår en automatisk kontroll via en bakgrunnssjekk (fortrinnsvis digital automatisert løsning) der kurante saker med alle vilkår oppfylt går rett gjennom og får positivt vedtak, mens saker som flagges for oppfølging fra førstelinjen eller får treff i bakgrunnssjekk sendes til manuell saksbehandling. Det er kun andrelinjen som har vedtaksmyndighet i alle saker.

Figuren nedenfor illustrerer ansvars- og oppgavedeling i første- og andrelinje. Disse prinsippene er lagt til grunn for felles skrankepunkt i begge alternativene.

[179] JD, «Høring - forslag til forskrift om pass og nasjonalt ID-kort», 2019



Figur 35 Todelt saksbehandling i første- og andrelinje

Systemstøtte og ID-kontroll

For å sikre en enhetlig behandling i et felles skrankepunkt, er det en forutsetning at ID-kontroll utøves på samme måte for like formål og at nødvendige opplysninger om søker registreres likt og med enhetlig begrepsbruk i aktuelle saksbehandlingssystemer og/eller registre som brukes videre i saksbehandlingen i andrelinje. Nødvendige opplysninger kan variere etter sakstype.

En annen viktig forutsetning for realiseringen av et felles skrankepunkt er at utførelsen av arbeidsoppgavene understøttes av nødvendig systemstøtte med et godt integrasjonsgrunnlag. Dette må understøtte formålet med et felles skrankepunkt slik at opplysninger og data kan overføres på tvers av systemene på en sikker og enkel måte. Systemene må understøtte moderne IT-arkitekturprinsipper slik at de kan fungere optimalt i samhandling med hverandre. Videre må førstelinjen ha tilgang til å søke på tvers av relevante registre. For å sikre dette må nødvendige regelverksendringer gjennomføres og personvernhensyn vurderes og ivaretas. Leverandøren går ikke videre inn på dette, men forutsetter at dette kan gjennomføres i beskrivelser og drøfting av alternativene.

I tillegg til prosessene beskrevet som aktuelle å inkludere i et felles skrankepunkt, vil det være hensiktsmessig å legge til rette for å gjenbruke ID-kontroll og annen relevant informasjon innhentet i skrankepunktet (ansiktsfoto, signatur etc.) for andre aktører, eksempelvis for utstedere av private eID-er og Statens vegvesen for utstedelse av førerkort. Se videre kapittel 3.5.4 for beskrivelse og drøfting av en slik løsning for utstedere av private eID-er og hovedrapportens kapittel 14.2.1 for drøfting rundt gjenbruk av ID-kontroll hos Statens vegvesen.

Beskrivelse av alternativene

I de neste to delkapitlene beskriver og utdyper leverandøren to ulike alternativ for et felles skrankepunkt:

> *Alternativ 1: Et felles skrankepunkt for politiets førstelinje på pass- og ID-kontorene og Skatteetatens førstelinje på skattekontorene*
>
> *Alternativ 2: Et felles skrankepunkt for politiets førstelinje på pass- og ID-kontorene, Skatteetatens førstelinje på skattekontorene og UDIs førstelinje på utlendingskontorene*

Alternativene beskrives og vurderes ut ifra ulike aspekter som leverandøren anser som sentrale for videre vurdering opp mot sikkerhet, brukervennlighet og ressursbruk:

- Formål, myndighet og regelverk
- Styring
- Brukerreiser og brukertid
- Organisering og ressurser
- Kompetanse og kvalitet
- Oppsummering med styrker og svakheter for sikkerhet, brukervennlighet og ressursbruk

Beskrivelsene og vurderingene sammenlignes med dagens organisering og prosesser (inkl. prosess for utstedelse av både pass og nasjonale ID-kort fra 2020 og planlagte endringer i prosessene i utlendingsforvaltningen). Det antas at alle brukergrupper søker nasjonalt ID-kort utenom asylsøkere med innvilget asyltillatelse da denne brukergruppen ikke gis tilbud om nasjonalt ID-kort som omtalt i kapittel 2.2.5. Denne forutsetningen avhenger følgelig videre av hvilke krav som settes til de ulike brukergruppene i kapittel 2.3. Det legges i begge alternativene til grunn at EØS-registreringsordningen avvikles som drøftet i kapittel 2.5.1.

Alternativene medfører at politiet ved politidistriktene gis myndighet til å rekvirere identitetsnummer, både d-nummer og fødselsnummer.[180] Dette kan gjøres på samme måte som for utlendingsmyndighetene per i dag.[181] Grunnlaget for rekvireringen vil fra politiets side være å utøve myndighetsoppgaver på vegne av andre aktører i skrankepunktene, og på sikt for å utstede nasjonale ID-kort til personer som får dette tilbudet. Skatteetaten er fortsatt tildelingsmyndighet av identitetsnummer.

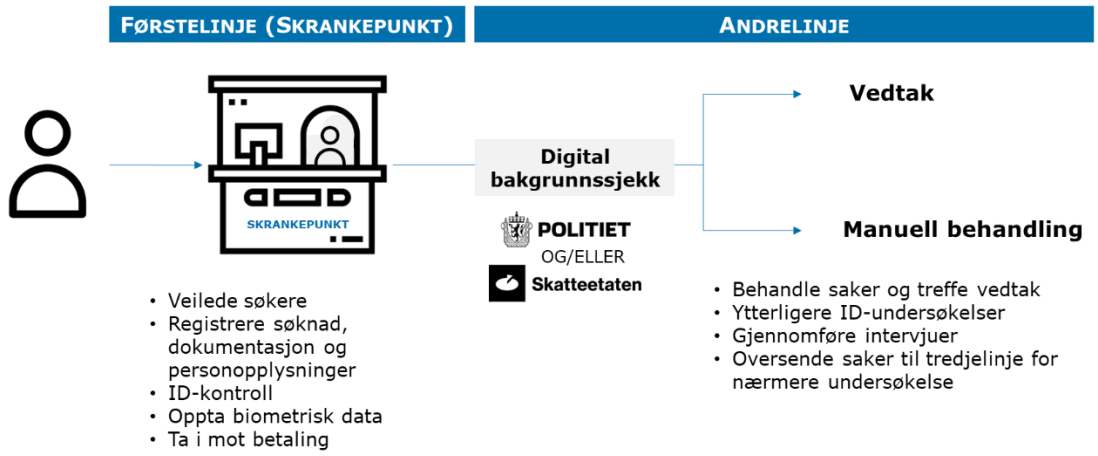
4.4.3 Alternativ 1: Et felles skrankepunkt for politiets førstelinje på pass- og ID-kontorene og Skatteetatens førstelinje på skattekontorene

Alternativet innebærer at aktivitetene, som gjennomføres av førstelinjene ved henholdsvis pass- og ID-kontorene og skattekontorene, gjennomføres i et felles skrankepunkt. Ansvars- og oppgavedeling i første- og andrelinje følger beskrivelsen i delkapittelet over. Følgende prosesser beskrevet i kapittel 4.2 inngår i et felles skrankepunkt:

- *Søknad om pass og/eller nasjonalt ID-kort (fra pass- og ID-kontor)*
- *Søknad om skattekort for personer som ikke har fødselsnummer eller «kontrollert» d-nummer (fra skattekontor)*
- *Melde innflytting til Norge fra utlandet (fra skattekontor)*
- *ID-kontroll gjennomført på vegne av andre rekvirenter i tilfeller der det kreves status «kontrollert» eller bruker ønsker å bli «kontrollert» (fra skattekontor)*

Skrankepunktet legges til de 78 planlagte pass- og ID-kontorene. Søknad om pass og/eller nasjonalt ID-kort sendes videre for behandling til politiets andrelinje, mens de tre andre søknadsprosessene sendes videre til Skatteetatens andrelinje. Alternativet innebærer ingen endringer i førstelinjen for utlendingskontorene.

[180] PU er per i dag eneste enhet innen politiet som har myndighet til å rekvirere d-nummer
[181] Utlendingsmyndighetene sender melding til Skatteetaten når en person får innvilget oppholdstillatelse og Skatteetaten tildeler identitetsnummer på bakgrunn av meldingen



Figur 36 Organisering og aktiviteter i første- og andrelinje i alternativ 1

Formål, myndighet og regelverk

Slik beskrevet i hovedrapporten er myndighetsansvar innenfor ID-forvaltningen fordelt på flere sektorer. Eksempelvis ligger folkeregistermyndigheten til SKD og skattekontorene, mens ID-kortmyndigheten og passmyndigheten i hovedsak er lagt til politiet. Alternativ 1 omfatter ikke endring eller overføring av myndighetsansvar mellom POD og SKD eller etablering av en ny myndighet på direktoratsnivå.

Alternativ 1 påvirker imidlertid myndigheten som ligger til skattekontorene da de er registermyndighet i første instans, jf. § 1-3 i folkeregisterloven. I praksis vil endringen fungere på samme måte som myndigheten som er delegert til utlendingskontorene i dag, blant annet gjennom utlendingsloven, forskrift, rundskriv og databehandleravtaler.[182] Dette er beskrevet nærmere under styring.

Regelverkene som ligger til grunn for de ulike myndighetsområdene som inngår i et felles skrankepunkt er relativt omfattende og komplekst. Gjennomgang av utvalgt regelverk, herunder lov, forskrift og rundskriv viser til dels svært ulike formål og ulik praktisering innenfor for eksempel registrering av data:

> ***Passmyndigheten: Formålet med passloven*** *er å regulere utstedelse av norske pass. Loven hjemler opprettelsen av passregisteret. Formålet med pass er å lette borgernes reisevirksomhet. En rett til pass styrker den grunnleggende retten til å forlate ethvert land, også ens eget. Loven gjelder kun for norske statsborgere, ettersom norsk statsborgerskap er et grunnvilkår for å kunne få norsk pass.* [183]
>
> *Som utgangspunkt er det kun passmyndigheten, Kripos og grensekontrollmyndighet som skal ha tilgang til passregisteret, jf. passloven § 8. I tillegg kan opplysninger i passregisteret brukes til nærmere bestemte oppgaver, jf. § 8 a, eksempelvis til søk etter savnet person, identifisering av død person, identifisering av person som skal innbringes i henhold til politiloven § 8, identifiseringsarbeid i medhold av utlendingsloven og ved forebygging og etterforskning av handlinger som kan medføre høyere straff enn fengsel i seks måneder.*
>
> *ID-kortregisteret kan kobles mot passregisteret, jf. ID-kortloven § 9. Det følger av forarbeidene at «koblingen til passregisteret muliggjør automatiserte søk mellom opplysningene i registrene». JD forvalter passloven og ID-kortloven (ikke trådt i kraft).*
>
> ***Folkeregistermyndigheten: Formålet med folkeregisterloven*** *er å legge til rette for sikker, korrekt og effektiv registrering av grunnleggende*

[182] Informasjon mottatt på e-post fra UDI, andre halvår 2019
[183] Lov 19. juni 1997 nr. 82 om pass (passloven). Beskrevet i hovedrapportens kapittel 4.1.6, september 2019

personopplysninger om den enkelte, herunder hvilke personer som er bosatt i Norge. Loven skal sikre at registreringspliktige personer tildeles et unikt identifikasjonsnummer. Loven skal bidra til at opplysningene i Folkeregisteret skal kunne brukes til myndighetsoppgaver og offentlig forvaltning, forskning, statistikk og til å ivareta grunnleggende samfunnsbehov. [184]

Folkeregisterloven regulerer vilkårene som må være oppfylt for utlevering av opplysninger fra registeret. Folkeregistermyndigheten har på sin side hjemmel i folkeregisterloven § 7-1 til å innhente fra andre myndigheter, uten hinder av taushetsplikt, opplysninger som er nødvendige for registerføringen. Folkeregisterforskriften § 7-1-1 bestemmer at en rekke konkrete offentlige myndigheter og virksomheter skal dele informasjon med folkeregistermyndigheten. FIN forvalter folkeregisterloven.

Et felles skrankepunkt for politiet og Skatteetaten krever regelverksendringer i om lag fem regelverk med tilhørende forskrifter. Leverandørens vurdering av omfanget er at det er behov for større endringer i regelverket, og at minst to departementer må involveres, men behovet må utredes nærmere. Dette for å legge til rette for «kun én gang» og sammenhengende tjenester med brukeren i sentrum.[185]

Skrankepunktet skal ivareta myndighetenes behov for fysiske oppmøter i ID-forvaltningen. Det er nødvendig å etablere hjemler for sikker deling av data mellom myndighetene slik at opplysningene som innhentes, registreres, kontrolleres og utleveres, kan benyttes til flere formål hos de respektive myndighetene på tvers av instanser og sektorer. Personvernhensyn spiller en viktig rolle i ID-forvaltningen og har stor betydning for utformingen av regelverket. Myndighetenes ivaretakelse av personvernet er utfordrende fordi til dels ulike hensyn skal balanseres. Dette må understøttes av tilstrekkelig systemstøtte slik at vedtakslinjer i neste instans har tilgang til nødvendige saksopplysninger. Det er avgjørende med et godt integrasjonsgrunnlag som kan understøtte formålet med et felles skrankepunkt slik at opplysninger og data kan overføres på tvers av systemene på en sikker og enkel måte.

Styring

Styrings- og ansvarsforholdene mellom POD og SKD endres ved å etablere et felles skrankepunkt. Det gir større kompleksitet i fag- og styringslinjene og trolig økt behov for koordinering mellom de to etatene.

POD, underlagt JD, har ansvaret for administrativ og faglig ledelse, styring, oppfølging og utvikling av politidistriktene, herunder de felles skrankepunktene.

SKD vil fortsatt være sentral folkeregistermyndighet og behandlingsansvarlig for Folkeregisteret, og FIN vil fortsatt ha ansvar for overordnet styring av SKD. Myndigheten som er lagt til skattekontorene i første instans påvirkes ved at ansvar, oppgaver, medarbeidere og ressurser for definerte prosesser på skattekontorene overføres til pass- og ID-kontorene.

Delegering av myndighet til forvaltningsorganer som er underordnet et sideordnet forvaltningsorgan reiser særlige problemstillinger som må håndteres.[186] Pass- og ID-kontorene skal utøve oppgaver for SKD på lik linje med dagens samhandling mellom politidistriktenes utlendingskontorer (førstelinje) og UDI (andrelinje). Det vil være behov for koordinering og samordning mellom POD og SKD som tar hensyn til ny arbeidsdeling mellom etatene. Det er avgjørende med ulike samordningsmekanismer

[184] Lov 9. desember 2016 nr. 88 om folkeregistrering (folkeregisterloven) § 1-2. Beskrevet i hovedrapportens kapittel 4.1.5, september 2019
[185] Én digital offentlig sektor. Digitaliseringsstrategi for offentlig sektor 2019–2025
[186] Backer et al., «NOU 2019:5 Ny forvaltningslov — Lov om saksbehandlingen i offentlig forvaltning», 2019

og god systemstøtte for å sikre måloppnåelse når første- og andrelinje er plassert i ulike etater. Samordning av styringssignaler i tildelingsbrev skjer mellom departementer der statsråder har et politisk og konstitusjonelt ansvar for aktuelle politikkområder. En forutsetning for enhetlige, sikre, effektive og brukervennlige felles skrankepunkt er at POD gir felles overordnede føringer til politidistriktene om hvordan pass- og ID-kontorene skal samhandle og samordne basert på erfaringer og beste praksis i etaten.

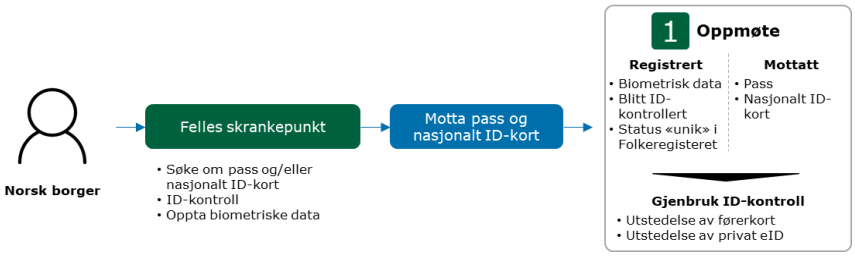
Som beskrevet i hovedrapporten er det en risiko ved å plassere ansvaret for skrankepunktet hos politiet at oppgaveporteføljen deres er svært stor og det er fare for at andre mer kritiske ansvarsområder prioriteres.[187] Videre har gjennomføringsevnen knyttet til implementeringen av nye pass og ID-kort av ulike årsaker vært lav. Det er også en fare for at ved å plassere ansvaret hos politiet, så vil kvalitet og sikkerhet vektlegges i noe større grad enn brukervennlighet og ressurseffektivisering. Det er derfor viktig å etablere overordnede mål for skrankepunktet som balanserer de ulike hensynene tilstrekkelig. En sentral forutsetning for at et felles skrankepunkt blir et vellykket tiltak er at skrankepunktenes rutiner, retningslinjer, opplæring, utstyr og de ansattes kompetanse implementeres enhetlig i de ulike politidistriktene.

Brukerreiser og brukertid

Som det fremgår av kapittel 4.2.11 medfører dagens organisering av skrankepunkt i gjennomsnitt ett oppmøte for en norsk borger, fire oppmøter for en EØS-borger og to eller tre oppmøter for en tredjelandsborger som søker opphold, statsborgerskap, oppholdskort for familiemedlemmer av EU/EØS-borgere eller utlendingspass/reisebevis.[188] Et felles skrankepunkt har i alternativ 1 primært innvirkning på brukervennligheten for EØS-borgere. Brukerreiser med antall oppmøter er fremstilt for de ulike brukergruppene nedenfor.

Norsk borger

Alternativet påvirker ikke antall oppmøter for norske borgere sammenlignet med dagens situasjon. Brukergruppen har fortsatt, på lik linje med dagens situasjon, ett oppmøte i forbindelse med søknad om pass og/eller nasjonalt ID-kort.

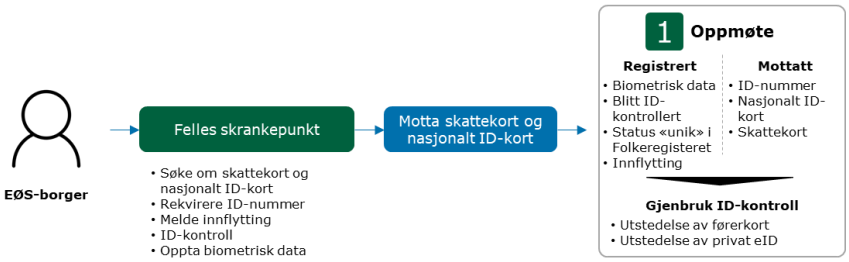


Figur 37 Antall oppmøter for en norsk borger ved alternativ 1

EØS-borger

For EØS-borgere blir brukervennligheten markant bedre ved realisering av alternativ 1. Avvikling av EØS-registreringsordningen og muligheten til å gjennomføre flere aktiviteter i et felles skrankepunkt, reduserer antall oppmøter fra fire til ett. EØS-borgeren slipper i tillegg å registrere den samme informasjonen flere ganger. Antall oppmøtesteder øker fra 42 skattekontor til 78 felles skrankepunkt.

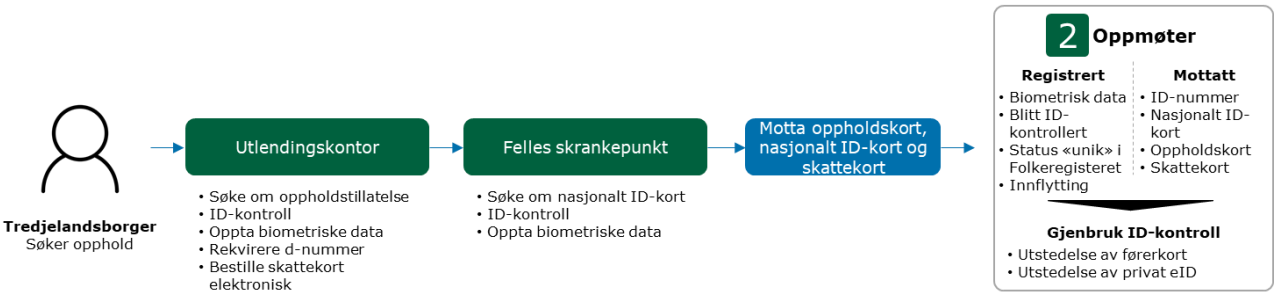
[187] Dette aspektet ble drøftet i hovedrapportens kapittel 15.2.4, september 2019
[188] Dette tallet gjelder antall oppmøter for førsteganssøknader tilknyttet relevante prosesser. Tallet vil være høyere i et livsløp



Figur 38 Antall oppmøter for en EØS-borger ved alternativ 1

Tredjelandsborger

Alternativet har liten effekt på brukervennligheten for tredjelandsborgere i stort da utlendingsforvaltningen ikke er en del av felles skrankepunkt i alternativ 1. Tredjelandsborgere møter opp som tidligere på utlendingkontorene for å gjennomføre relevant prosess, som å søke opphold eller statsborgerskap som beskrevet kapittel 4.2.11. Figuren under viser prosessen for oppholdssøkere som et eksempel på at antall oppmøter er uendret i alternativ 1.



Figur 39 Antall oppmøter for en tredjelandsborger ved alternativ 1

Alternativet vil imidlertid ha effekt på brukervennligheten til familiemedlemmer av EØS-borgere (en liten gruppe tredjelandsborgere oppsummert i tabell i kapittel 4.2.1) hvor antall oppmøter reduseres fra tre til to da de slipper å møte opp separat på skattekontor for å melde innflytting.

Verdi av tidsbesparelse for brukergrupper

Beregning av tidsbesparelser omfatter endring i tid som følge av at alternativet realiseres, ikke total tidsbruk for brukergruppene. Som vist i brukerreisene over er det ingen tidsbesparelse for norske borgere eller tredjelandsborgere (med unntak for tredjelandsborgere som er i familie med EØS-borgere) i alternativ 1 sammenlignet med dagens situasjon. Det er like mange oppmøter som ved dagens situasjon for begge disse brukergruppene.

Alternativet medfører tid spart for EØS-borgere, da det ikke kreves separate oppmøter for EØS-registrering, skattekort og innflytting. Dette fordi EØS-registreringen avvikles og de to andre prosessene gjøres i ett og samme oppmøte og skrankepunkt samtidig som bruker søker om nasjonalt ID-kort. Tidsbruken reduseres også for familiemedlemmer til EØS-borgere som er tredjelandsborgere, da innflytting gjennomføres i forbindelse med søknad om nasjonalt ID-kort. De må riktignok fortsatt møte på utlendingskontor for å søke oppholdskort for familiemedlemmer av EØS-borgere.

Tabellen nedenfor oppsummerer spart tid for EØS-borgere. Tidsbesparelsen totalt for EØS-borgere[189] ved å gå fra fire til ett oppmøte[190] er estimert til omtrent 95 mill. kroner per år. Dette er basert på totalt antall saker i 2018 og en antagelse om en gjennomsnittlig tidsverdi på 365 NOK[191] per time. Tidsbesparelsen vil følgelig variere med antall saker fra år til år.

I dag er det satt av tjue minutter per bruker i skrankepunkt ved søknad om pass- og nasjonalt ID-kort. Leverandøren legger videre til grunn at prosessen for utstedelse av nasjonalt ID-kort, søknad om skattekort og melding om innflytting kan gjennomføres i løpet av 25 minutter, noe som gir brukeren økt tidsbruk på fem minutter. Leverandøren anser dette som gjennomførbart i et felles skrankepunkt. Tydeliggjøring av første- og andrelinjeoppgaver reduserer omfanget av saksbehandling og øker effektivitet i skrankepunktet som følge av enklere deling av data og opplysninger på tvers av prosesser samt gjenbruk av ID-kontroll. Det understrekes likevel at tid i skrankepunkt varierer etter kompleksitet i saker og at det ikke i alle tilfeller vil være realistisk å beregne 25 minutter per oppmøte.

Økt tid på fem minutter i forbindelse med oppmøtet i felles skrankepunkt gir reduksjon i tidsverdi på i underkant av 5 mill. kroner for alle oppmøter. Leverandøren legger til grunn at 144 000 EØS-borgere som tidligere har møtt hos Skatteetaten for ID-kontroll vil bruke fem minutter ekstra tid i felles skrankepunkt.[192] Det er riktignok reduksjon i reisetid tilknyttet fjernede oppmøter som er drivende for tidsverdien.

Prosess	Brukertid[193]	Antall i 2018	Estimat tidsverdi
EØS-registrering	Bestilling av time: 5 min Reisetid: 60 min Tid ved utlendingskontor: 22,5 min Totalt: 1,5 timer	38 400	21 mill. kroner
Søknad om skattekort for personer som ikke har fødselsnummer eller «kontrollert» d-nummer	Bestilling av time: 5 min Reisetid: 60 min Tid ved skattekontor: 25 min Totalt: 1,5 timer	144 000[194]	79 mill. kroner
Melde innflytting til Norge fra utlandet	Bestilling av time: 5 min Reisetid: 60 min Tid ved skattekontor: 25 min Totalt: 1,5 timer		
Tidsverdi			100 mill. kroner
Ekstra tid brukt i felles skrankepunkt	5 minutter	144 000	- 5 mill. kroner
Total tidsverdi			**95 mill. kroner**

Tabell 23 Estimert samlet verdi av spart tidsbruk per år ved gjennomføring av alternativ 1 for EØS-borgere (og familiemedlemmer av EU/EØS-borgere ved innflytting)

For alle brukergrupper spares det ytterligere tid om ID-kontrollen som gjennomføres i et felles skrankepunkt gjenbrukes av Statens vegvesen og aktører for utstedelse av

[189] Heretter i denne beskrivelsen brukt om EØS-borgere og familiemedlemmer av EØS-borgere som er tredjelandsborgere for prosess om innflytting
[190] Fra tre til to oppmøter for familiemedlemmer av EØS-borgere som er tredjelandsborgere
[191] Som i hovedrapportens kapittel 5.1.8 er det lagt til grunn en gjennomsnittlig tidsverdi per time på 365 kroner i 2018. Denne verdien er basert på norske borgere, men det legges til grunn samme tidsverdi per time for andre borgere
[192] De 38 400 som EØS-registrerer seg vil være en del av de 144 000 som møter opp hos Skatteetaten for en ID-kontroll for skattekort eller innflytting
[193] I hovedrapportens kapittel 5.1.5 ble det satt noen antagelser for tidsbruk og gjennomsnittlig kjøretid i forbindelse med oppmøter. Disse antagelsene gjenbrukes i tilleggsrapporten. Da det er færre skattekontor og utlendingskontor enn antall pass- og ID-kontor har leverandøren økt gjennomsnittlig reisetid fra 41 til 60 minutter tur/retur. Ellers er tid brukt i skrankepunkt som oppgitt under de respektive prosessene i kapittel 4.2, og lagt til en gjennomsnittlig ventetid på 10 minutter
[194] Totalt antallet for både søknad om skattekort og innflytting. Tallet inkluderer også innflytting for personer som er familiemedlemmer av EU/EØS-borgere

eID. Leverandøren viser til hovedrapportens kapittel 5.1.5 og vedlegg 8 for fremstilling og beregninger relatert til dette.

Organisering og ressurser

Organisering

Felles skrankepunkt legges, som nevnt i kapittel 4.4.2, til de 78 planlagte pass- og ID-kontorene i politidistriktene. Alle ledere og medarbeidere ved skrankepunktene vil være ansatt i politiet. Det er ikke behov for å endre utformingen av pass- og ID-kontorene, etter utrulling av biometrikiosker og annet teknisk utstyr for ID-kontroll og dokumentgransking, for å kunne utføre aktivitetene knyttet til skatterelaterte prosesser på samme sted. Det vil derimot være nødvendig å vurdere dimensjonering og utvidelse av bemanning og kapasitet nærmere ved hvert enkelt kontorsted for å sikre at det er tilstrekkelig antall skranker for å håndtere nye oppgaver og prosesser. Dette gjelder også for å kunne håndtere utstedelse av nasjonalt ID-kort for utlendinger.

Behovet for skranker eller direkte kontakt med bruker på de 42 skattekontorene som i dag utfører ID-relaterte oppgaver blir sterkt redusert i dette alternativet. Dagens klare strategi og praksis medfører at de fleste av Skatteetatens tjenester kan gjennomføres uten et fysisk oppmøte. På Skatteetatens hjemmesider oppfordres bruker til å ta kontakt gjennom chat, Facebook eller på telefon for andre tjenester enn for oppmøter relatert til skatteprosessene nevnt i kapittel 4.2.8–4.2.10. I tråd med styrt utvikling og pågående arbeid med å digitalisere og automatisere Skatteetatens tjenester har leverandøren grunn til å tro at behovet for fysiske oppmøter på de 42 skattekontorene vil reduseres til et minimum eller opphøre på mellomlang sikt. De nasjonale divisjonene i Skatteetaten som utøver register- og skattemyndighet i andrelinjen påvirkes i mindre grad av endringene. Grensesnittet mellom første- og andrelinjen endres og vil kreve god samhandling og koordinering med pass- og ID-kontorene. Videre effektivisering og endring i andrelinjen kommer som følge av styrt utvikling og pågående arbeid med å digitalisere og automatisere Skatteetatens tjenester.

Store deler av formålet til SUA-kontorene bortfaller ved realisering av alternativet som følge av at EØS-registreringsordningen avvikles og EØS-borgere vil møte i felles skrankepunkter for å gjennomføre tjenestene de har behov for i ett oppmøte. Tredjelandsborgere som søker opphold for arbeid samt oppholdskort vil fortsatt dra nytte av å kunne møte opp på et SUA-kontor. En sterkt redusert oppgaveportefølje medfører at ressurseffektiviteten ved å opprettholde SUA-kontorene må vurderes.

Som nevnt i kapittel 4.1.5 er 34 av 41 utlendingskontor i dag samlokalisert med pass- og ID-kontor. Det ble også synliggjort gevinster og driftsfordeler ved lokasjoner der pass- og ID-kontor og utlendingskontor er samlokalisert. Leverandøren vurderer at samlokalisering av alle utlendingskontor med felles skrankepunkt er en fordel for alternativet. Dette vil også være hensiktsmessig for deling av kunnskap og kompetanse. Samlokalisering av felles skrankepunkt og utlendingskontor kan for tredjelandsborgere tenkes å fungere som SUA-kontorene gjør i dag der brukere som møter både på utlendingskontor og i felles skrankepunkt prioriteres i køene. Dette for å redusere byrden for tredjelandsborgere og sikre at de ikke må møte opp flere ganger (de må fortsatt møte i to skranker og avgi informasjon to ganger). Arbeidstilsynet kan også vurderes samlokalisert med felles skrankepunkt og utlendingskontor i de byene der SUA-kontorene er plassert i dag for å opprettholde eksisterende tilbud.

Ressurser

Leverandøren understreker at de største gevinstene ved gjennomføring av etablering av et felles skrankepunkt vil knytte seg til økt sikkerhet og brukervennlighet.

Realisering av alternativ 1 bidrar til redusert ressursbruk for forvaltningen på flere områder:

- Antall oppmøter med ID-kontroller på skattekontorene reduseres med 144 000 per år og medfører et behov for ca. 22 færre årsverk ved skattekontorene isolert.[195] Dette tilsvarer en kostnadsbesparelse på ca. 15 mill. kroner.[196] Som nevnt i kapittel 4.2.11 er fornyelser av ID-bevis og øvrige tillatelser i et livsløpsperspektiv ikke inkludert i vurderingen i tilleggsoppdraget

- EØS-registreringsordningen avvikles, noe som medfører at 38 400 (tall for 2018) registreringer per år ikke gjennomføres. Dette medfører et behov for fem færre årsverk ved utlendingskontorene isolert.[197] Dette tilsvarer en kostnadsbesparelse på ca. 3 mill. kroner[198]

- Økning i tid satt av per bruker i et felles skrankepunkt fra 20 til 25 minutter gir behov for ca. syv flere årsverk isolert ved de felles skrankepunktene.[199] Dette tilsvarer en kostnadsøkning på ca. 6 mill. kroner[200]

- Todelt saksbehandling hvor ansvars- og oppgavefordelingen mellom første- og andrelinje rendyrkes og implementeres. Prosesser standardiseres, retningslinjer og rutiner tydeliggjøres og gir mer effektiv ressursbruk

- Mer effektiv saksbehandling gjennom deling av data og praktisering av «kun en gang» som i stort betyr at bruker kun skal måtte trenge å oppgi informasjon en gang. I et skrankepunkt hvor flere parallelle prosesser gjennomføres på samme tid vil dette være ressursbesparende.

Alternativet vil også kunne redusere ressursbruk sett fra et bruker- og samfunnsperspektiv. I tillegg til vesentlige sikkerhetsgevinster som følge av enhetlig registrering av grunndata i riktige registre og utøvelse av ID-kontroll vil det være hensiktsmessig å gjenbruke ID-kontroll og annen relevant informasjon innhentet i skrankepunktet (ansiktsfoto, signatur etc.) for andre aktører, eksempelvis for utstedere av private eID-er og Statens vegvesen for utstedelse av førerkort.

Implementeringskostnader relatert til alternativet og den omstillingen det krever inkluderer blant annet følgende kostnadsområder:

- *Ombygging/utvidelse av lokaler* omfatter kostnader for å sikre at det er tilstrekkelig med kapasitet og skranker som tilfredsstiller krav til fysisk sikring for å håndtere nye oppgaver og prosesser etter at behovet er vurdert nærmere ved hvert enkelt kontorsted

- *IKT-utstyr og systemstøtte* omfatter tekniske tilpasninger og integrasjoner mellom ulike registre og saksbehandlingssystemer slik at for eksempel saksbehandlere i skranken ikke jobber i flere parallelle systemer, men at data deles sikkert og effektivt

- *Budsjett-/rammeoverføringer* omfatter budsjettmessige konsekvenser ved flytting av for eksempel budsjett og årsverk mellom etater

[195] Legges til grunn 15 minutter brukt per søker i skrankepunktet på skattekontorene og ett årsverk på 1650 timer
[196] Basert på data mottatt av Skatteetaten om personalkostnader i arbeid med hovedrapporten, første halvår 2019
[197] Legges til grunn 12,5 minutter brukt per søker i skrankepunktet på utlendingskontoret og ett årsverk på 1650 timer
[198] Basert på data mottatt av POD om personalkostnader i arbeid med hovedrapporten, første halvår 2019
[199] Lagt til grunn 144 000 oppmøter av EØS-borgere og familiemedlemmer av EØS-borgere som er tredjelandborgere
[200] Basert på data mottatt av POD om personalkostnader i arbeid med hovedrapporten, første halvår 2019

- *Innplassering av medarbeidere* omfatter kostnader knyttet til at omstillingsprosessen gjennomføres i samsvar med lov- og avtaleverk, retningslinjer for personalpolitikk og omstillingsavtaler

- *Kompetanseutvikling* omfatter kostnader knyttet til krav til opplæring og relevant trening for alle saksbehandlere ved skrankepunktene for eksempel høyere og/eller mer enhetlige sikkerhetskrav ved ID-kontroller

- *Omstillingsvirkemidler* for nedbemanning omfatter kostnader knyttet til å realisere effektiviserings- og gevinstpotensialet

- *Rundskriv, rutiner og retningslinjer* omfatter kostnader knyttet til å oppdatere dokumentasjon i henhold til enhetlige kvalitets- og sikkerhetskrav på tvers av sektorer, bortfall av synergier mellom første- og andrelinje og eventuelle informasjonstiltak internt og eksternt

- *Lov- og forskriftsendringer* omfatter kostnader knyttet til regelverksprosesser

Grunnet mangel på tallgrunnlag og ressursbruk tilknyttet dette er implementeringskostnadene kategorisert som ikke-kvantifiserbare effekter hvor det må gjøres ytterligere foranalyser for å kunne etablere kostnadsestimater.

Kompetanse og kvalitet

Det etableres et robust fagmiljø for utførelse av relativt like aktiviteter som per i dag finner sted i førstelinjen på henholdsvis pass- og ID-kontorene og skattekontorene. Alternativet medfører at det gis faglige og tekniske forutsetninger for bedre ID-kontroll ved søknad om skattekort og ID-kontroller gjennomført på vegne av andre rekvirenter der det kreves status «kontrollert» eller bruker selv ønsker å bli «kontrollert», samt ved innflytting ved at disse prosessene finner sted samtidig med utstedelse av nasjonalt ID-kort. En forutsetning for enhetlige, sikre, effektive og brukervennlige felles skrankepunkt er at POD gir felles overordnede føringer til politidistriktene om hvordan og etter hvilke rutiner og retningslinjer aktivitetene skal gjennomføres og hvilken kompetanse de ansatte skal inneha. Det bør videre være fokus på å bygge ut kompetanse spesifikt tilknyttet disse aktivitetene. Totalt gir dette økt kvalitet og økt sikkerhet i prosessene.

I andrelinjene vil det fortsatt være fokus på å spisse og tilegne kompetanse innen eget forvaltningsområde knyttet til respektive aktørers relevante prosesser. Det vil være behov for tett samhandling, kompetansedeling og dialog på tvers av første- og andrelinje.

Det er i forbindelse med nytt saksbehandlingssystem ved pass- og ID-kontorene satt minimumskrav til kompetanse for saksbehandlere.[201] Dette skal gi enhetlig behandling av søknader og sikre økt kvalitet i aktivitetene som gjennomføres. Leverandøren vurderer at de samme kompetansekravene bør gjelde for alle aktiviteter som skal gjennomføres i et felles skrankepunkt. Det er ingen krav til politifaglig bakgrunn for å jobbe ved pass- og ID-kontorene.

Det vil i tillegg til egne kompetansekrav i de felles skrankepunktene være svært sentralt at det deles kompetanse på tvers av felles skrankepunkt og utlendingskontorene slik at ansatte ved de felles skrankepunktene har tilstrekkelig kunnskap om utenlandske dokumenter, moduser og landkunnskap for å utstede nasjonale ID-kort også til

[201] Politidirektoratet, Kompetansekrav – Saksbehandlere pass og nasjonalt ID- 8

utenlandske borgere. Dette understøtter at pass- og ID-kontorene bør være samlokalisert med utlendingskontorene som diskutert tidligere.

Oppsummering – styrker og svakheter for sikkerhet, brukervennlighet og ressursbruk

Tabellen nedenfor oppsummerer styrker og svakheter ved det presenterte alternativet.

Sikkerhet	+ Todelt saksbehandling gjør at sikkerheten i ID-forvaltningen øker sett fra både myndigheters og brukers perspektiv + Robuste fagmiljøer med eksperter på ID-kontroll og registrering av saker + Forebygger kriminalitet ved en sikrere prosess for kontroll og registrering av identitet og utstedelse av ID-bevis ÷ Begrenset påvirkning for prosessene i utlendingskontorene
Brukervennlighet	+ Betydelig færre oppmøter for EØS-borgere og for familiemedlemmer av EØS-borgere som er tredjelandsborgere og registrering av opplysninger skjer kun én gang + Markant økning i oppmøtesteder for brukere med ID-relaterte behov på skattekontorene, øker fra 42 skattekontor til 78 felles skrankepunkt ÷ Ingen endring i antall oppmøter for de fleste tredjelandsborgere
Ressursbruk	+ Viktige ID-oppgaver i skrankepunktet samles og blir utført enhetlig + Bedre kapasitetsutnyttelse ved å samle fagmiljøer, gjenbruke av ID-kontroll og økt deling av data ÷ Fortsatt parallelle kompetansemiljøer i første-, andre- og tredjelinje ÷ Potensielt bortfall av enkelte synergier mellom første- og andrelinje
Annet	+ Hver aktør beholder vedtaksmyndighet for eget virksomhetsområde ÷ Ulike kulturer på tvers av Skatteetaten og politiet, og innad i politiet, som kan være krevende å integrere ÷ Økt kompleksitet i fag- og styringslinjene mellom politiet og Skatteetaten kan skape større behov for koordinering på tvers ÷ Krever potensielt omfattende regelverksendringer

Tabell 24 Vurdering av alternativ 1

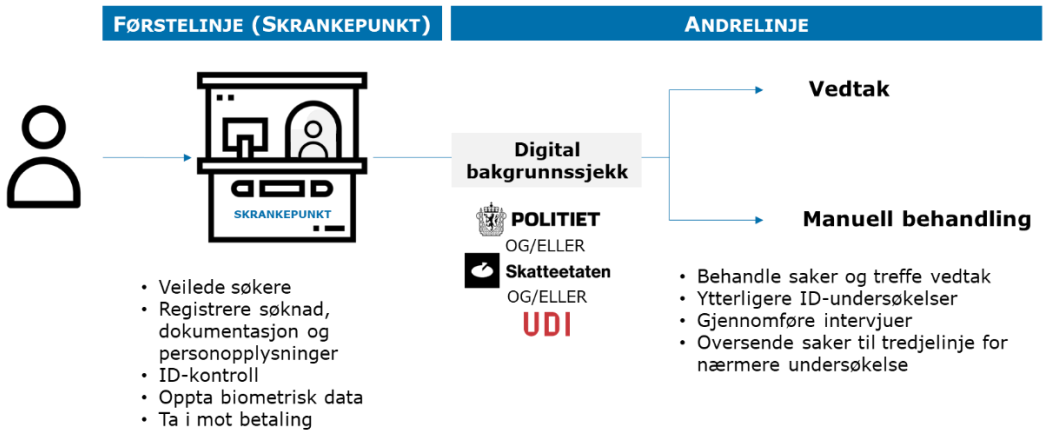
4.4.4 Alternativ 2: Et felles skrankepunkt for politiets førstelinje på pass- og ID-kontorene, UDIs førstelinje på utlendingskontorene og Skatteetatens førstelinje på skattekontorene

Alternativet innebærer at aktivitetene, som gjennomføres av førstelinjene ved henholdsvis pass- og ID-kontorene, skattekontorene og utlendingskontorene, gjennomføres i et felles skrankepunkt. Ansvars- og oppgavedeling i første- og andrelinje følger beskrivelsen i kapittel 4.4.2. Alle prosesser beskrevet i kapittel 4.2 inngår i et felles skrankepunkt:

- *Søknad om pass og/eller nasjonalt ID-kort (fra pass- og ID-kontor)*
- *Søknad om skattekort for personer som ikke har fødselsnummer eller «kontrollert» d-nummer (fra skattekontor)*
- *Melde innflytting til Norge fra utlandet (fra skattekontor)*
- *ID-kontroll gjennomført på vegne av andre rekvirenter i tilfeller der det kreves status «kontrollert» eller bruker ønsker å bli «kontrollert» (fra skattekontor)*
- *Søknad om oppholdstillatelse og utstedelse av oppholdskort (fra utlendingskontor)*

- *Søknad om oppholdskort for familiemedlemmer av EU/EØS-borgere (fra utlendingskontor)*
- *Søknad om statsborgerskap (fra utlendingskontor)*
- *Søknad om utlendingspass og reisebevis (fra utlendingskontor)*

Skrankepunktet legges til de 78 planlagte pass- og ID-kontorene. Søknad om pass og/eller nasjonalt ID-kort sendes videre for behandling i politiets andrelinje, søknader tilknyttet de tre prosessene i Skatteetaten vil sendes videre til behandling i Skatteetatens andrelinje, mens de fire siste søknadstypene sendes videre til andrelinjen i enten politiet eller UDI avhengig av sakstype.



Figur 40 Organisering og aktiviteter i første- og andrelinje i alternativ 2

I det følgende vurderes og drøftes ulike aspekter ved alternativ 2. Mange av punktene har noe av det samme innholdet som alternativ 1, og leverandøren henviser derfor opp til respektive punker under kapittel 4.4.3 der dette er hensiktsmessig for å unngå gjentagelser.

Formål, myndighet og regelverk

Slik beskrevet i hovedrapporten er myndighetsansvar innenfor ID-forvaltningen fordelt på flere sektorer. Eksempelvis ligger folkeregistermyndigheten til SKD og skattekontorene, mens ID-kortmyndigheten og passmyndigheten i hovedsak er lagt til politiet. Utlendingsmyndigheten involverer flere forvaltningsorganer som politiet, utenriksstasjoner, UDI og UNE.

Som i alternativ 1 omfatter ikke alternativ 2 endring av myndighetsansvar mellom POD, SKD og UDI eller etablering av en ny myndighet på direktoratsnivå.

Alternativ 2 påvirker imidlertid myndigheten som ligger til skattekontorene da de er registermyndighet i første instans, jf. § 1-3 i folkeregisterloven. I praksis vil endringen fungere på samme måte som myndigheten som er delegert til utlendingskontorene i dag, blant annet gjennom utlendingsloven, forskrift, rundskriv og databehandleravtaler. Dette er beskrevet nærmere under styring.[202]

Gjennomgang av utvalgt regelverk, herunder lov, forskrift og rundskriv viser som tidligere nevnt til dels svært ulike formål og ulik praktisering. I tillegg til formålene til passloven og folkeregisterloven som beskrevet i alternativ 1, har utlendingsloven følgende formål:

[202] Informasjon mottatt på e-post fra UDI, andre halvår 2019

Utlendingsmyndighetene: Formålet med utlendingsloven *er å gi grunnlag for regulering av og kontroll med inn- og utreise, og utlendingers opphold i riket, i samsvar med norsk innvandringspolitikk og internasjonale forpliktelser. Loven skal legge til rette for lovlig bevegelse over landegrensene, og ivareta rettssikkerheten til utlendinger som reiser inn i eller ut av riket, som oppholder seg her, eller som søker en tillatelse etter loven. Loven skal gi grunnlag for vern for utlendinger som har krav på beskyttelse etter alminnelig folkerett eller internasjonale avtaler som Norge er bundet av.*[203]

Utlendingsloven regulerer ulike grunnlag for opphold i Norge. I den forbindelse registreres alle utlendinger i en egen utlendingsdatabase (UDB). Fingeravtrykk tatt med hjemmel i utlendingsloven lagres i et eget utlendingsregister. UDI er behandlingsansvarlig for registeret. Kripos er databehandler. Kapittel 11 i loven bestemmer saksbehandlingsregler med blant annet opplysningsplikt og behandling av personopplysninger i alle saker. JD forvalter utlendingsloven med tilhørende forskrifter. De særlige reglene om EØS- og EFTA-borgere har ASD forvaltningsansvaret for.

Et felles skrankepunkt for politiet, Skatteetaten og UDI krever regelverksendringer i om lag fem til ti regelverk med tilhørende forskrifter. Leverandørens vurdering av omfanget er at det er behov for større endringer i regelverket i alternativ 2 hvor flere myndigheter og minst tre departementer må involveres. Videre er utlendingsloven mer omfattende og prosessovergripende enn folkeregisterloven. Behovet for harmonisering av regelverk, hjemler, begrepsbruk og semantikk må utredes nærmere for å legge til rette for «kun én gang» og sammenhengende tjenester med brukeren i sentrum.[204]

Skrankepunktet skal ivareta myndighetenes behov for fysiske oppmøter i ID-forvaltningen. Det er nødvendig å etablere hjemler for sikker deling av data mellom myndighetene slik at opplysningene som innhentes, registreres, kontrolleres og utleveres, kan benyttes til flere formål hos de respektive myndighetene på tvers av instanser og sektorer. Personvernhensyn spiller en viktig rolle i ID-forvaltningen og har stor betydning for utformingen av regelverket. Myndighetenes ivaretakelse av personvernet er utfordrende fordi til dels ulike hensyn skal balanseres. Dette må understøttes av tilstrekkelig systemstøtte slik at vedtakslinjer i neste instans har tilgang til nødvendige saksopplysninger. Det er avgjørende med et godt integrasjonsgrunnlag som kan understøtte formålet med et felles skrankepunkt slik at opplysninger og data kan overføres på tvers av systemene på en sikker og enkel måte.

Styring

I likhet med alternativ 1 endres styrings- og ansvarsforholdene mellom POD og SKD ved å etablere et felles skrankepunkt. Det gir større kompleksitet i fag- og styringslinjene og trolig økt behov for koordinering mellom to av etatene. Det er færre endringer relatert til fag- og styringslinjene mellom POD og UDI utover at grensesnittet mellom pass- og ID-kontorene og utlendingskontorene i politiet påvirkes.

POD, underlagt JD, har ansvaret for administrativ og faglig ledelse, styring, oppfølging og utvikling av politidistriktene, herunder de felles skrankepunktene.

SKD vil som i alternativ 1 fortsatt være sentral folkeregistermyndighet og behandlingsansvarlig for Folkeregisteret, og FIN vil fortsatt ha ansvar for overordnet styring av SKD. Myndigheten som er lagt til skattekontorene i første instans påvirkes ved at ansvar, oppgaver, medarbeidere og ressurser for definerte prosesser på skattekontorene overføres til pass- og ID-kontorene.

[203] Lov 15. mai 2008 nr. 35 om utlendingers adgang til riket og deres opphold her (utlendingsloven). Beskrevet i hovedrapportens kapittel 4.1.4, september 2019
[204] Én digital offentlig sektor. Digitaliseringsstrategi for offentlig sektor 2019–2025

Pass og ID-kontorene skal utøve oppgaver for SKD og UDI på lik linje med dagens samhandling mellom politidistriktenes utlendingskontorer (førstelinje) og UDI (andrelinje). Det vil være behov for koordinering og samordning som tar hensyn til ny arbeidsdeling mellom etatene. Det er avgjørende med ulike samordningsmekanismer og god systemstøtte for å sikre måloppnåelse når første- og andrelinje er plassert i ulike etater. Som tidligere nevnt er det en forutsetning at POD gir felles overordnede føringer til politidistriktene om hvordan pass- og ID-kontorene og utlendingskontorene skal samhandle og samordne basert på erfaringer og beste praksis i etaten.

Som beskrevet i hovedrapporten er det en risiko ved å plassere ansvaret for skrankepunktet hos politiet at oppgaveporteføljen deres er svært stor og det er fare for at andre mer kritiske ansvarsområder prioriteres.[205] Videre har gjennomføringsevnen knyttet til implementeringen av nye pass og ID-kort av ulike årsaker vært lav. Det er også en fare for at ved å plassere ansvaret hos politiet, så vil kvalitet og sikkerhet vektlegges i noe større grad enn brukervennlighet og ressurseffektivisering. Det er derfor viktig å etablere overordnede mål for skrankepunktet som balanserer ulike hensyn tilstrekkelig. En sentral forutsetning for at et felles skrankepunkt blir et vellykket tiltak er at skrankepunktenes rutiner, retningslinjer, opplæring, utstyr og de ansattes kompetanse implementeres enhetlig i de ulike politidistriktene.

Brukerreise og brukertid

Alternativ 2 vil gi økt brukervennlighet for både EØS-borgere og tredjelandsborgere, mens brukervennligheten til norske borgere vil være upåvirket. Brukerreisen for norske borgere og EØS-borgere vil være de samme som illustrert i figur 37 og 38 i alternativ 1.

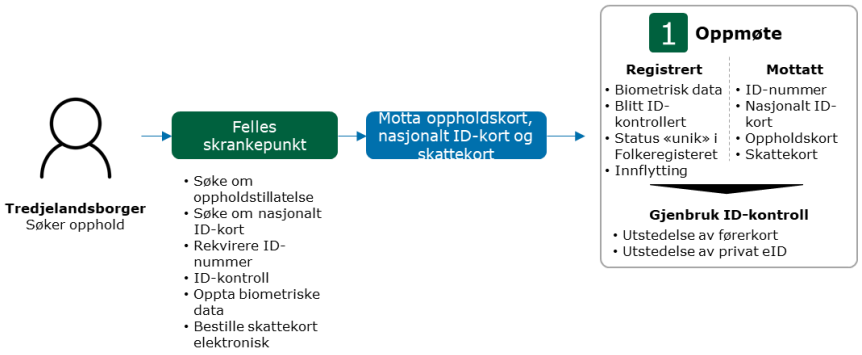
Tredjelandsborgere

Alternativet har betydelig effekt på brukervennligheten for tredjelandsborgere. Muligheten for å gjennomføre flere aktiviteter i et felles skrankepunkt vil redusere antall oppmøter fra tre til to for søkere om statsborgerskap eller to til ett for søkere om opphold eller oppholdskort for familiemedlemmer av EU/EØS-borgere.

I forbindelse med å søke opphold gis det også mulighet til å søke om nasjonalt ID-kort ved oppmøte i et felles skrankepunkt. Søkere om statsborgerskap kan søke om pass eller nasjonalt ID-kort med reiserett samtidig som de henter vedtak om innvilget statsborgerskap. Antall oppmøtesteder øker fra 41 utlendingskontor til 78 felles skrankepunkt. Familiemedlemmer av EØS-borgere (en liten gruppe tredjelandsborgere oppsummert i tabell i kapittel 4.2.1) vil kunne gjøre alle relevante prosesser i ett oppmøte (søke oppholdskort for familiemedlemmer av EØS-borgere, melde flytting og søke om nasjonalt ID-kort).

Figuren nedenfor viser som eksempel brukerreise for en tredjelandsborger som søker opphold ved realisering av alternativ 2.[206]

[205] Dette aspektet ble drøftet i hovedrapportens kapittel 15.2.4, september 2019
[206] Tredjelandsborgere som søker opphold er brukt som eksempel da dette er den største gruppen tredjelandsborgere



Figur 41 Brukerreise for tredjelandsborgere som søker opphold ved realisering av alternativ 2

Verdi av tidsbesparelse for brukergrupper

Beregning av tidsbesparelser omfatter endring i tid som følge av at alternativet realiseres, ikke total tidsbruk for brukergruppene. Alternativ 2 gir ingen spart tidsverdi for norske borgere på lik linje som alternativ 1. For EØS-borgere gjelder samme sparte tidsverdi som i alternativ 1. Tidsbesparelsen totalt for EØS-borgere er omtrent 95 mill. kroner per år.[207]

Det spares også tid for tredjelandsborgere. Søkere om oppholdstillatelse og utstedelse av oppholdskort sparer ett oppmøte ved å kunne søke om nasjonalt ID-kort samtidig som de søker oppholdstillatelse. Søkere om statsborgerskap sparer ett oppmøte da de kan søke om pass eller nasjonalt ID-kort med reiserett samtidig som de henter vedtak om statsborgerskap. Søkere om oppholdskort for familiemedlemmer av EØS-borgere sparer to oppmøter sammenlignet med dagens situasjon ved å kunne søke oppholdskort, melde innflytting og søke om nasjonalt ID-kort ved samme oppmøte. For søkere om utlendingspass/reisebevis antas det at antall oppmøter er uendret da denne gruppen ikke får tilbud om nasjonale ID-kort (som omtalt i kapittel 2.2.5) og det er dermed ikke lagt til grunn noen tidsbesparelse for disse sakene.

Tabellen nedenfor oppsummerer redusert tidsbruk for tredjelandsborgere. Tidsbesparelsen totalt for tredjelandsborgere ved reduksjon i antall oppmøter er estimert til 40 mill. kroner per år. Totalt antall tidsbesparelse for EØS-borgere og tredjelandsborgere er dermed estimert til rundt 135 mill. kroner per år.[208] Dette er basert på totalt antall saker i 2018 og en antagelse om en gjennomsnittlig tidsverdi på 365 NOK[209] per time. Tidsbesparelsen vil følgelig variere med antall saker fra år til år.

I dag er det satt av tjue minutter per bruker i skrankepunkt ved søknad om pass- og nasjonalt ID-kort. Leverandøren legger videre til grunn at alle nødvendige tjenester/prosesser en bruker har behov for kan gjennomføres i løpet av 25 minutter, noe som gir brukeren økt tidsbruk på fem minutter. Leverandøren anser dette som gjennomførbart i et felles skrankepunkt. Tydeliggjøring av første- og andrelinjeoppgaver reduserer omfanget av saksbehandling og øker effektivitet i skrankepunktet som følge av enklere deling av data og opplysninger på tvers av prosesser samt gjenbruk av ID-kontroll. Det understrekes likevel at tid i skrankepunkt varierer etter kompleksitet i saker og at det ikke i alle tilfeller vil være realistisk å beregne 25 minutter per oppmøte. Språklige utforinger, kontroll av underlagsdokumenter fra ulike land eller innhenting av ulik informasjon som det er behov for i videre saksbehandling, kan medføre behov for lengre tid i skrankepunktet.

[207] Dette tallet er inkludert tidsbesparelse for reduksjon i ett oppmøte for familiemedlemmer av EØS-borgere som er tredjelandsborgere
[208] I kapittel 4.4.5 ble det beregnet en total tidsbesparelse for EØS-borgere på omtrent 95 mill. kroner
[209] Som i hovedrapportens kapittel 5.1.8 er det lagt til grunn en gjennomsnittlig tidsverdi per time på 365 kroner i 2018. Denne verdien er basert på norske borgere, men det legges til grunn samme tidsverdi per time for andre borgere

Økt tid på fem minutter i forbindelse med oppmøtet i felles skrankepunkt gir reduksjon i tidsverdi på ca. to mill. kroner for tredjelandsborgere. Leverandøren legger da til grunn at både søkere om oppholdstillatelse og søkere som skal hente statsborgerskapsvedtak vil måtte bruke fem minutter ekstra i et felles skrankepunkt for å gjennomføre alle prosesser.[210] Det er riktignok reduksjon i reisetid tilknyttet fjernede oppmøter som er drivende for tidsverdien.

Prosess	Brukertid[211]	Antall saker i 2018	Estimat tidsverdi (ca.)
Søkere om oppholdstillatelse og utstedelse av oppholdskort			
Søke om oppholdstillatelse	Bestilling av time: 5 min Reisetid: 60 min Tid ved utlendingskontor: 22,5 min Totalt: Ca. 1,5 time	65 600	36 mill. kroner
Søkere om oppholdskort for familiemedlemmer av EØS-borgere			
Søke om oppholdskort	Bestilling av time: 5 min Reisetid: 60 min Tid ved utlendingskontor: 22,5 min Totalt: Ca. 1,5 time	1 500	1 mill. kroner
Søkere om statsborgerskap			
Hente statsborgerskaps-vedtak	Bestilling av time: 5 min Reisetid: 60 min Tid ved utlendingskontor: 22,5 min Totalt: Ca. 1,5 time	10 268[212]	6 mill. kroner
Tidsverdi			42 mill. kroner
Ekstra tid brukt i felles skrankepunkt	5 minutter	75 868[213]	- 2 mill. kroner
Total tidsverdi for tredjelandsborgere			**40 mill. kroner**

Tabell 25 Estimert samlet verdi av spart tidsbruk per år ved gjennomføring av alternativ 1 for tredjelandsborgere

For alle brukergrupper spares det ytterligere tid om ID-kontrollen som gjennomføres i et felles skrankepunkt gjenbrukes av Statens vegvesen og aktører for utstedelse av eID. Leverandøren viser til hovedrapportens kapittel 5.1.5 og vedlegg 8 for fremstilling og beregninger relatert til dette.

Organisering og ressurser

Organisering

Som i alternativ 1 legges felles skrankepunkt til de 78 planlagte pass- og ID-kontorene i politidistriktene. Alle ledere og medarbeidere ved skrankepunktene vil være ansatt i politiet. Det er ikke behov for å endre utformingen av pass- og ID-kontorene, etter utrulling av biometrikiosker og annet teknisk utstyr for ID-kontroll og dokumentgransking, for å kunne utføre aktivitetene knyttet til skatterelaterte prosesser på samme sted. Det vil derimot være nødvendig å vurdere dimensjonering og utvidelse av bemanning og kapasitet nærmere ved hvert enkelt kontorsted for å sikre at det er

[210] Søkere om oppholdskort for familiemedlemmer av EØS-borgere vil også bruke fem minutter ekstra i skrankepunktet, men dette er allerede beregnet inn i total tidsbesparelse for EØS-borgere som vist i alternativ 1

[211] I hovedrapportens kapittel 5.1.5 ble det satt noen antagelser for tidsbruk og gjennomsnittlig kjøretid i forbindelse med oppmøter. Disse antagelsene gjenbrukes i tilleggsrapporten. Da det er færre skattekontor og utlendingskontor enn antall pass- og ID-kontor har leverandøren økt gjennomsnittlig reisetid fra 41 til 60 minutter tur/retur. Ellers er tid brukt i skrankepunkt som oppgitt under de respektive prosessene i kapittel 4.2, lagt til en gjennomsnittlig ventetid på 10 minutter

[212] Det påpekes at dette tallet varierer fra tallet oppgitt i tabell i kapittel 4.2.1 da tallet i tabellen er innleverte søknader om statsborgerskap, mens dette tallet er innvilgede statsborgerskap. Kilde: SSB, «Overgang til norsk statsborgerskap», 2019

[213] Ikke inkludert familiemedlemmer av EØS-borgere som er tredjelandsborgere da de fem ekstra minuttene ved ett oppmøte i felles skrankepunkt er medberegnet i total tidsverdi for EØS-borgere

tilstrekkelig antall skranker for å håndtere nye oppgaver og prosesser. Dette gjelder også for å kunne håndtere utstedelse av nasjonalt ID-kort for utlendinger.

Alternativet innebærer samme konsekvenser for skattekontorene og utførelsen av Skatteetatens tjenester som drøftet i alternativ 1.

Formålet til SUA-kontorene vil i sin helhet bortfalle ved realisering av alternativ 2 da alle prosesser som i dag utføres på disse kontorene vil legges til de felles skrankepunktene. Arbeidstilsynet kan vurderes samlokalisert med felles skrankepunkt i de byene der SUA-kontorene er plassert i dag for å opprettholde eksisterende tilbud.

Når det gjelder utlendingskontorene vil det i alternativ 2 være redusert behov for skranker eller direkte kontakt med bruker på dagens 41 utlendingskontor. Grensesnittet mellom første- og andrelinjen endres og vil kreve god samhandling og koordinering med pass- og ID-kontorene. På lik linje som skissert for Skatteetaten vil det være mulig å benytte endringsmomentet til videre digitalisering og effektivisering av prosessene i andrelinjen.

Ressurser

Leverandøren understreker at de største gevinstene ved gjennomføring av etablering av et felles skrankepunkt vil knytte seg til økt sikkerhet og brukervennlighet.

Realisering av alternativ 2 bidrar til redusert ressursbruk for forvaltningen på flere områder:

- Antall oppmøter med ID-kontroller på skattekontorene reduseres med 144 000 per år og medfører et behov for ca. 22 færre årsverk ved skattekontorene isolert.[214] Dette tilsvarer en kostnadsbesparelse på ca. 15 mill. kroner.[215] Som nevnt i kapittel 4.2.11 er fornyelser av ID-bevis og øvrige tillatelser i et livsløpsperspektiv ikke inkludert i vurderingen i tilleggsoppdraget

- EØS-registreringsordningen avvikles, noe som medfører at 38 400 (tall for 2018) registreringer per år ikke trenger å gjennomføres.[216] Antall oppmøter på utlendingskontor for øvrige tredjelandsprosesser reduseres med 77 368 per år. Dette tilsvarer totalt et behov for ca. 17 færre årsverk isolert ved utlendingskontorene.[217] Det tilsvarer en kostnadsbesparelse på ca. 11 mill. kroner[218]

- Økning i tid satt av per bruker i et felles skrankepunkt fra 20 til 25 minutter gir behov for 11 flere årsverk ved de felles skrankepunktene isolert.[219] Dette medfører en kostnadsøkning på ca. 9 mill. kroner

- Todelt saksbehandling hvor ansvars- og oppgavefordelingen mellom første- og andrelinje rendyrkes og implementeres. Prosesser standardiseres, retningslinjer og rutiner tydeliggjøres og gir mer effektiv ressursbruk

[214] Legges til grunn 15 minutter brukt per søker i skrankepunktet på skattekontorene og ett årsverk på 1650 timer
[215] Basert på data mottatt av Skatteetaten, første halvår 2019
[216] Legges til grunn 12,5 minutter brukt per søker i skrankepunktet for EØS-registrering på utlendingskontoret og ett årsverk på 1650 timer
[217] Legges til grunn 15 minutter brukt per søker i skrankepunktet på utlendingskontoret for øvrige prosesser og ett årsverk på 1650 timer
[218] Basert på data fra POD om personalkostnader mottatt i arbeid med hovedrapporten, første halvår 2019
[219] Lagt til grunn 144 000 oppmøter av EØS-borgere og familiemedlemmer av EØS-borgere som er tredjelandborgere og 123 000 oppmøter av øvrige tredjelandsborgere

- Mer effektiv saksbehandling gjennom deling av data og praktisering av «kun en gang» som i stort betyr at bruker kun skal måtte trenge å oppgi informasjon en gang. I et skrankepunkt hvor flere parallelle prosesser gjennomføres på samme tid vil dette være ressursbesparende

Alternativet vil også kunne redusere ressursbruk sett fra et bruker- og samfunnsperspektiv. I tillegg til vesentlige sikkerhetsgevinster som følge av enhetlig registrering av grunndata i riktige registre og utøvelse av ID-kontroll vil det være hensiktsmessig å gjenbruke ID-kontroll og annen relevant informasjon innhentet i skrankepunktet (ansiktsfoto, signatur etc.) for andre aktører, eksempelvis for utstedere av private eID-er og Statens vegvesen for utstedelse av førerkort.

Implementeringskostnaden relatert til alternativet og den omstillingen det krever er betydelig mer omfattende da det berører flere enheter, medarbeidere, prosesser og systemer, og inkluderer blant annet følgende kostnadsområder:

- *Ombygging/utvidelse av lokaler* omfatter kostnader for å sikre at det er tilstrekkelig med kapasitet og skranker som tilfredsstiller krav til fysisk sikring for å håndtere nye oppgaver og prosesser etter at behovet er vurdert nærmere ved hvert enkelt kontorsted

- *IKT-utstyr og systemstøtte* omfatter tekniske tilpasninger og integrasjoner mellom ulike registre og saksbehandlingssystemer slik at for eksempel saksbehandlere i skranken ikke jobber i flere parallelle systemer, men at data deles sikkert og effektivt

- *Budsjett-/rammeoverføringer* omfatter budsjettmessige konsekvenser ved flytting av for eksempel budsjett og årsverk mellom etater

- *Innplassering av medarbeidere* omfatter kostnader knyttet til at omstillingsprosessen skal gjennomføres i samsvar med lov- og avtaleverk, retningslinjer for personalpolitikk og omstillingsavtaler

- *Kompetanseutvikling* omfatter kostnader knyttet til krav til opplæring og relevant trening for alle saksbehandlere ved skrankepunktene for eksempel høyere og/eller mer enhetlige sikkerhetskrav ved ID-kontroller

- *Omstillingsvirkemidler* for nedbemanning omfatter kostnader knyttet til å realisere effektiviserings- og gevinstpotensialet

- *Rundskriv, rutiner og retningslinjer* omfatter kostnader knyttet til å oppdatere dokumentasjon i henhold til enhetlige kvalitets- og sikkerhetskrav på tvers av sektorer, bortfall av synergier mellom første- og andrelinje og eventuelle informasjonstiltak internt og eksternt

- *Lov- og forskriftsendringer* omfatter kostnader knyttet til regelverksprosesser

Grunnet mangel på tallgrunnlag og ressursbruk tilknyttet dette er implementeringskostnadene kategorisert som ikke-kvantifiserbare effekter hvor det må gjøres ytterligere foranalyser for å kunne komme opp med kostnadsestimater.

Kompetanse og kvalitet

Alternativet medfører som for alternativ 1 at det etableres et robust fagmiljø for utførelse av relativt like aktiviteter som per i dag finner sted i førstelinjen på henholdsvis pass- og ID-kontorene, skattekontorene og utlendingskontorene. Alternativet medfører at det gis faglige og tekniske forutsetninger for bedre ID-kontroll

ved alle prosesser. En forutsetning for enhetlige, sikre, effektive og brukervennlige felles skrankepunkt er at POD gir felles overordnede føringer til politidistriktene om hvordan og etter hvilke rutiner og retningslinjer aktivitetene skal gjennomføres og hvilken kompetanse de ansatte skal inneha. Det bør videre være fokus på å bygge ut kompetanse spesifikt tilknyttet disse aktivitetene. Totalt gir dette økt kvalitet og økt sikkerhet i prosessene.

I andrelinjene vil det fortsatt være fokus på å spisse og tilegne kompetanse innen eget forvaltningsområde knyttet til respektive aktørers relevante prosesser. Det vil være behov for tett samhandling, kompetansedeling og dialog på tvers av første- og andrelinje.

På samme måte som i alternativ 1 vurderer leverandøren at kompetansekrav som innføres for saksbehandlere av søknader om pass og/eller nasjonalt ID-kort også i dette alternativet bør gjelde for alle aktiviteter som skal gjennomføres i et felles skrankepunkt.

Det vil være svært sentralt at det deles kompetanse på tvers av de ansatte og at ansatte i andrelinje med mer dyptgående kunnskap tilknyttet hvert forvaltningsområde og hver prosess kan kontaktes via telefon, chat eller lignende og kan bidra med spisset kompetanse.

Oppsummering med styrker og svakheter for sikkerhet, brukervennlighet og ressursbruk

Tabellen nedenfor oppsummerer styrker og svakheter ved det presenterte alternativet.

Sikkerhet	+ Todelt saksbehandling gjør at sikkerheten i ID-forvaltningen øker sett fra både myndigheters og brukers perspektiv + Robuste fagmiljøer med eksperter på ID-kontroll, biometriopptak og registrering av saker + Forebygger kriminalitet ved en sikrere prosesser for registrering av identitet og utstedelse av ID-bevis + Samling av ID-relatert kompetanse på ulike fagområder
Brukervennlighet	+ Betydelig færre oppmøter for EØS-borgere og tredjelandsborgere og registrering av opplysninger skjer kun én gang + Markant økning i oppmøtesteder for brukere med ID-relaterte behov på skattekontorene og utlendingskontorene, øker fra 42 skattekontor og 41 utlendingskontor til 78 felles skrankepunkt + Mange aktiviteter finner sted i et oppmøte og kan påvirke tidsbruk for bruker i skranke
Ressursbruk	+ Viktige ID-oppgaver i skrankepunktet samles og blir utført enhetlig + Bedre kapasitetsutnyttelse ved å samle fagmiljøer, gjenbruke av ID-kontroll og økt deling av data ÷ Fortsatt parallelle kompetansemiljøer i andre- og tredjelinje ÷ Potensielt bortfall av enkelte synergier mellom første- og andrelinje
Annet	+ Hver aktør beholder vedtaksmyndighet for eget virksomhetsområde ÷ Ulike kulturer på tvers av Skatteetaten og politiet, og innad i politiet, som kan være krevende å integrere ÷ Økt kompleksitet i fag- og styringslinjene mellom politiet og Skatteetaten kan skape større behov for koordinering på tvers ÷ Krever potensielt omfattende regelverksendringer

Tabell 26 Vurdering av alternativ 2

4.4.5 Tiltak 27 i regjeringens strategi mot arbeidslivskriminalitet

I regjeringens reviderte strategi mot arbeidslivskriminalitet er det listet opp en rekke tiltak for å bekjempe kriminalitet. Tiltak 27 (tiltak 24 før revidering) omhandler *ID-kontroll ved utstedelse av d-nummer og helhetlig ansvar for EØS-borgere* og er beskrevet som følger:

> *Justis- og beredskapsdepartementet skal sammen med Finansdepartementet og Arbeids- og sosialdepartementet utrede om én etat skal ha et mer helhetlig ansvar for ID-forvaltningen for EØS-borgere. Justis- og beredskapsdepartementet og Finansdepartementet skal også vurdere om politiet skal overta ID-kontrollen ved rekvirering av D-nummer (identifikasjonsnummer som gis til alle utlendinger som oppholder seg i Norge under seks måneder). Dette skal ses i sammenheng med blant annet politiets registreringsordning for EØS-borgere og database over stjålne/tapte utenlandske ID-dokumenter.*
>
> *Politidirektoratet, Utlendingsdirektoratet og Skattedirektoratet har fått i oppdrag å identifisere alternativer som gir en sikrere og mer effektiv identitetsforvaltning overfor EØS-borgere i Norge, og har avgitt en arbeidsgrupperapport. Justis- og beredskapsdepartementet og Finansdepartementet vil vurdere oppfølgingen av arbeidsgrupperapporten.*

På bakgrunn av tiltaket avga POD, SKD og UDI en arbeidsgrupperapport for å identifisere alternativ for en sikrere og mer effektiv identitetsforvaltning overfor EØS-borgere. «Helhetlig ansvar for EØS-borgere» (EØS-rapporten) vurderte fem ulike alternativ for dette. Ingen av disse alternativene er direkte sammenlignbare med alternativene som foreslås i områdegjennomgangens tilleggsrapport, men noen likhetstrekk kan identifiseres med alternativ 5 «Én ansvarlig etat» fra EØS-rapporten. Det legges både i EØS-rapporten og i begge alternativene i tilleggsrapporten i kapittel 4.4.3 og 4.4.4 vekt på felles skrankepunkt, sikre ID-prosesser og effektivitet for borgeren. EØS-rapporten gikk dog ikke nærmere inn på hvordan «Én ansvarlig etat» kunne realiseres, men anbefalte gjennomføring av en undersøkelse for å avdekke forbedringspotensialet. Områdegjennomgangens hovedrapport anbefalte i kapittel 16.1.7 etablering av en ID-etat, og det er i tilleggsrapporten detaljert og utdypet i større grad med konkrete forslag for førstelinjen og et felles skrankepunkt.

Alternativene i tilleggsrapporten legger begge samme grunnlag for å følge opp tiltak 27 i regjeringens strategi mot arbeidslivskriminalitet. De vil gi en sikrere og mer effektiv identitetsforvaltning overfor EØS-borgere i Norge fordi de behandles enhetlig i en samlet førstelinje. Politiet gis et mer helhetlig ansvar for oppgaveutøvelse knyttet til EØS-borgerne da de felles skrankepunktene vil være EØS-borgernes kontaktpunkt i det eneste oppmøtet de trenger å gjennomføre. Videre svarer anbefalingen i kapittel 16.1.7 fra hovedrapporten også ut tiltak 27 ved at en etat får et helhetlig ansvar for ID-forvaltningen.

4.4.6 Implikasjoner for rekvirering av identitetsnummer og krav om status «kontrollert»

Både alternativ 1 og 2 medfører som presisert i slutten av kapittel 4.4.2 at politiet ved politidistriktene gis myndighet til å rekvirere identitetsnummer, både d-nummer og fødselsnummer.[220] Dette kan gjøres på samme måte som utlendingsmyndighetene gjør per i dag.[221] Grunnlaget for rekvireringen vil fra politiets side være å utøve myndighetsoppgaver på vegne av andre aktører i skrankepunktene, og på sikt for å utstede nasjonale ID-kort til personer som får dette tilbudet. Skatteetaten er fortsatt

[220] PU er per i dag eneste enhet innen politiet som har myndighet til å rekvirere d-nummer
[221] Utlendingsmyndighetene sender melding til Skatteetaten når en person får innvilget oppholdstillatelse og Skatteetaten tildeler identitetsnummer på bakgrunn av meldingen

tildelingsmyndighet av identitetsnummer. Øvrige etater og virksomheter som har rekvirentstatus vil som i dag selv vurdere begrunnet behov for å rekvirere d-nummer.

Leverandøren anbefalte i hovedrapporten krav om «kontrollert» og på sikt «unik» identitet for å motta offentlige tjenester og ytelser. Leverandøren stiller seg fortsatt bak denne anbefalingen.

Leverandøren vurderer at Skatteetaten, som i dag, generelt bør kreve status «kontrollert» (eventuelt «unik» på sikt i den grad det er mulig) for utstedelse av skattekort. Noen brukergrupper er likevel unntatt kravet om å møte til ID-kontroll ved utstedelse av skattekort, som nevnt og opplistet i kapittel 2.3.1 om *unntakstilfeller for kravet om oppmøte for ID-kontroll for søknad om skattekort*. Leverandøren vurderer videre at det bør gjøres en systematisk gjennomgang av alle brukergrupper som er unntatt kravet om oppmøte basert på en konsekvens- og risikovurdering, for å på nytt vurdere om det kan kreves fysisk oppmøte av flere. Spesielt bør gruppen *«personer som er i en situasjon der det vil være svært byrdefullt for vedkommende å møte opp på skattekontoret og legitimere seg»* gjennomgås, og det bør vurderes om det kan kreves «kontrollert» av flere som per i dag unntas kravet på dette grunnlaget.

For andre rekvirenter enn Skatteetaten vurderer leverandøren at det bør etableres hjemler i rekvirentenes regelverk om at det generelt kreves status «kontrollert» ved et fysisk oppmøte i felles skrankepunkt for å få tilgang på respektive rekvirenters tjenester og ytelser. Det vil likevel være nødvendig å utarbeide en liste over brukergrupper som kan unntas kravet om oppmøte, på samme måte som det Skatteetaten har i dag. Dette bør gjøres basert på en konsekvens- og risikovurdering. Tjenesteeiere «tvinges» dermed ikke til å stille et universelt krav om «kontrollert» for alle EØS-borgere.

En slik gjennomgang med konsekvens- og risikovurdering krever at man går detaljert gjennom grunnlag for alle rekvisisjoner per rekvirent og om det er reelt å kreve at ulike brukergrupper må møte opp fysisk. Leverandøren har ikke fått tilgang på tilstrekkelig datagrunnlag for å kunne gjennomføre en slik detaljert gjennomgang.

For å kunne gjennomføre vurderingen bør det etableres et nært samarbeid mellom politiet og relevante tjenesteeiere. Dialog er viktig for å få en best mulig forståelse av risikobildet, og således hvor innstramming av sikkerhetskrav er mest nødvendig og gir størst effekt basert på det til enhver tid gjeldende kriminalitetsbilde. Dette følger samme prinsipp som skissert for krav om nasjonalt ID-kort i kapittel 2.3.3, alternativ 3.

4.4.7 Avsluttende vurdering

Et felles skrankepunkt er et av flere virkemidler for å oppnå visjonen for ID-forvaltningen. Tabellen under oppsummerer leverandørens vurdering av de to alternativene for et felles skrankepunkt sammenlignet med dagens situasjon. Det er særlig argumenter om bedre brukervennlighet og sikkerhet som trekkes frem. På en annen side bør implementeringskostnaden vektes opp mot begrenset ressurseffektvisering.

Et felles skrankepunkt kan implementeres uavhengig av om en ID-etat velges utredet. Et felles skrankepunkt er et steg i riktig retning for å sikre helhetlig styring og ansvar for ID-forvaltningen i Norge. Det er et av flere virkemiddel for å oppnå visjonen for ID-forvaltningen, men etter leverandørens syn vil det være nødvendig å ta i bruk sterkere grep langs styring- og strukturdimensjonen over tid.

Alternativ	Konsekvens		
	Sikkerhet	Brukervennlighet	Ressursbruk
Et felles skrankepunkt for politiets førstelinje i pass- og ID-kontorene og Skatteetatens førstelinje i skattekontorene	++	++	+
Et felles skrankepunkt for politiets førstelinje på pass- og ID-kontorene, UDIs førstelinje på utlendingskontorene og Skatteetatens førstelinje på skattekontorene	+++	+++	+

Tabell 27 Samlet vurdering av alternativ 1 og 2

5 Anbefalinger, konsekvenser og gevinster

Leverandørens anbefalinger er gitt med utgangspunkt i mandatet for tilleggsoppdraget og bygger videre på anbefalinger gitt i hovedrapporten. Effekten av de samlede anbefalingene vil være økt brukervennlighet, økt sikkerhet og økt ressurseffektivitet i ID-forvaltningen i et samfunnsmessig perspektiv.

5.1 Anbefalinger

5.1.1 Anbefalinger fysiske ID-bevis og utbredelse av nasjonalt ID-kort

Nasjonalt ID-kort tilbys til alle med rett på fødselsnummer eller d-nummer, med unntak av asylsøkere. Tilbudet om nasjonalt ID-kort inkluderer borgere med begrenset opphold i Norge grunnet ikke sannsynliggjort identitet.

Leverandøren anbefaler at nasjonalt ID-kort kan utstedes til alle med rett på norsk fødselsnummer eller d-nummer. Tilbudet inkluderer borgere som bor i Norge med begrenset oppholdstillatelse grunnet ikke sannsynliggjort identitet. Leverandøren begrunner anbefalingen i behovet for «én person, én identitet i Norge», og at enhver som får tildelt et norsk fødselsnummer eller d-nummer skal gis muligheten til å bevise sin knytning til tildelt identitetsnummer gjennom et sterkt ID-bevis. Leverandøren anser det nasjonale ID-kortet som det beste virkemiddelet for at utenlandske brukergrupper skal kunne bevise sin tilknytning til ett norsk identitetsnummer. Oppholdskortet vil også kunne oppnå et slikt formål ved innlemmelse av norsk identitetsnummer i kortet, men leverandøren har ikke identifisert tungtveiende argumenter for at dette skal være et prioritert tiltak på mellomlang sikt.

Leverandøren anbefaler at asylsøkere gjøres til unntak for et slikt tilbud. Dette begrunnes i at det er uavklart hvorvidt personer i brukergruppen vil bo i Norge over tid, samt at det for den store majoriteten av asylsøkere ikke vil foreligge et stort behov for et nasjonalt ID-kort i løpet av en relativt kort asylsøkerperiode.

Implementere anbefalte tiltak for å sikre høy utbredelse av nasjonalt ID-kort, og ytterligere vurdere mulighet til å stille krav om nasjonalt ID-kort for tildeling av skattekort.

Leverandøren anbefaler at det gjennomføres tiltak for å sikre høy utbredelse av nasjonalt ID-kort for utenlandske borgere. Slik anbefalt i hovedrapporten anbefaler leverandøren fortsatt at det tydeliggjøres i regelverket at nasjonalt ID-kort og norsk pass utgjør de eneste gyldige offentlige utstedte ID-bevisene i Norge. Utover dette er det etter leverandørens syn flere andre tiltak som vil sørge for høy utbredelse av nasjonalt ID-kort:

- Tjenesteeiere må gis hjemmel til å stille krav om norsk pass eller nasjonalt ID-kort samt kontroll ved fysisk oppmøte for sine brukere der det anses som proporsjonalt i henhold til risikovurdering og byrde for bruker. Et eksempel til etterfølgelse kan være forslaget fra NFD til endringer aksjelovgivningen mv.[222] Høringsnotatet belyser behovet for sikker identifisering fra perspektivet til blant annet foretaksregisteret, og foreslår at foretaksregisteret gis hjemmel til å kreve kontroll av identitet blant annet med krav om fysisk oppmøte i forbindelse med rekvirering av d-nummer

[222] NFD, «Forslag til endringer i aksjelovgivningen mv. (tilknytningskrav for styremedlemmer og daglig leder mv.)», 2019

- Gjennomføre en kollektiv og koordinert innsats for å tydeliggjøre at det er norsk pass og nasjonalt ID-kort som anses som gyldige norske ID-bevis i Norge (ikke førerkort og bankkort med bilde). Dette stadfestes for eksempel i regjeringens strategi for ID-forvaltningen (anbefaling 1 i hovedrapporten) og som felles føringer i relevante tildelingsbrev

- Igangsette initiativ til å informere tjenesteeiere og brukere om hvilken nytte et krav om nasjonalt ID-kort vil ha, både for den enkelte tjenesteeier og bruker men også i et større bilde mot målsettingen om høy andel «unik» i Folkeregisteret

- Etablere et tett samarbeid mellom pass- og ID-kortmyndigheten, utlendingsmyndighetene og relevante tjenesteeiere rundt hvilke tjenester og ytelser som det bør stilles krav for

- Implementering av tiltaket om å styrke kravene til utstedelse av norsk eID vil kunne ha stor effekt i utbredelsen av det nasjonale ID-kortet

- Leverandørens anbefaling om etablering av et felles skrankepunkt vil etter leverandørens vurdering være et sentralt tiltak i å understøtte utbredelsen av nasjonalt ID-kort. Samkjøring av utstedelsen av ID-kortet med oppmøtet for andre ID-relaterte prosesser i felles skrankepunkt reduserer terskelen betydelig for bruker å anskaffe ID-kortet

Vedrørende spørsmålet om krav om nasjonalt ID-kort for tilgang til tjenester og ytelser er det leverandørens anbefaling at det er tjenesteeiere som i siste instans vurderer eventuelle krav om fysiske ID-bevis i henhold til en risikovurdering, og gir eventuelle nødvendige unntak der hensiktsmessig. Jf. tidligere anbefaling om at nasjonalt ID-kort tilbys alle med rett på norsk fødselsnummer eller d-nummer vil tjenesteeiere dog ha *mulighet* til å stille et krav til alle sine brukere. Leverandøren begrunner anbefalingen i at det vil være vanskelig å kunne forvente at tjenesteeiere stiller et universelt krav om pass eller nasjonalt ID-kort for samtlige av sine tjenester og brukere. Et slikt krav vil i mange tilfeller utgjøre en urimelig belastning for bruker, samt ofte ikke være i henhold til tilhørende risiko.

Uavklarte spørsmål i henhold til EØS-regelverket vil potensielt også utgjøre en utfordring dersom det stilles krav til EØS-borgere og deres familiemedlemmer om fremvisning av et nasjonalt ID-kort utstedt av norske myndigheter for tilgang til tjenester og ytelser i Norge. Det vil i det videre arbeidet måtte avklares hvorvidt et slikt krav vil være forenlig med EØS-regelverket.

Leverandøren påpeker at selv for utvalgte tjenester og ytelser hos NAV vil et krav om legitimering med norsk pass eller nasjonalt ID-kort, der det kreves fysisk oppmøte, treffe få brukere i dag. Kravet vil treffe enda færre i fremtiden, etter hvert som digitaliseringen av tjenester fortsetter. For utstedelsen av skattekort er det leverandørens syn at et krav om fremvisning av nasjonalt ID-kort kan være et effektivt virkemiddel for å sørge for utbredelse av nasjonalt ID-kort og høy andel «unik» for EØS-borgere som skal arbeide i Norge. Leverandøren vurderer at førstegangsutstedelse av norsk førerkort er en annen prosess hvor det kan være spesielt egnet å stille krav om norsk pass eller nasjonalt ID-kort, uten at dette er vurdert nærmere av leverandøren i arbeidet med tilleggsoppdraget. Leverandøren legger likevel til grunn at Skatteetaten (og eventuelt Statens vegvesen) må vurdere om tiltaket er proporsjonalt med risiko, hvilke unntak som må gjelde av hensyn til byrden for bruker, samt om krav vil stå seg etter Norges forpliktelser overfor EØS-avtalen.

Leverandøren vurderer videre at et krav til «unik» fra tjenesteeiere for utvalgte tjenester er mer målrettet enn et krav om de fysiske ID-bevisene norsk pass eller

nasjonalt ID-kort. Dette har også vært omtalt som en anbefaling i hovedrapporten. Dette har ikke vært en direkte del av mandatet for tema 1 i tilleggsoppdraget, selv om det er en tett tilknyttet problemstilling. Ett krav til «unik» gir virkning både for fysisk og elektronisk identifikasjon, uavhengig av hvilke ID-bevis som betraktes som gyldige.

Avvikle EØS-registreringsordningen, betinget at ikke forordning 2019/1157 gir vesentlig utvidet handlingsrom

Leverandøren har ikke identifisert nevneverdig bruksverdi av informasjonen som opptas i forbindelse med EØS-registreringsordningen i sin nåværende form. Informasjonen som opptas kan opptas på andre måter, spesielt sett i lys av anbefalingen tilknyttet et felles skrankepunkt. Gitt dagens regelverk og praksis anses opptak av biometri i forbindelse med EØS-registreringsordningen som urealistisk, og det anses heller ikke å være verdiøkende å styrke kontrollen som gjennomføres i forbindelse med registreringsordningen. Leverandøren legger likevel til grunn at handlingsrommet for biometriopptak i registreringsordningen i henhold til ny forordning 2019/1157 må avklares nærmere i det videre arbeidet. Leverandøren vurderer dermed at dagens registreringsordning ikke kan rettferdiggjøre ressursbruken i forvaltningen samt den tidsbruk som påløper i forbindelse med oppmøte for bruker. Ordningen anbefales følgelig avviklet, betinget at ikke forordning 2019/1157 gir vesentlig utvidet handlingsrom. I så tilfelle bør det vurderes om EØS-registreringsordningen i stedet bør styrkes med biometriopptak før det konkluderes å avvikle ordningen.

«Unik» baseres på pass-, ID-kort og utlendingsregisteret og det må sikres nødvendig fremdrift for juridisk og teknisk tilrettelegging

Leverandøren anbefaler at det iverksettes tiltak for å sikre framgang i realiseringen av «unik». Spesielt viktig vil det være å avklare om det er en forutsetning for «unik» at vedkommende har fått utstedt pass eller nasjonalt ID-kort, eller om status «unik» også bør kunne baseres på registrering i utlendingsregisteret. Uavhengig av valgt alternativ legger leverandøren til grunn at søker vil kontrolleres ved en-til-mange søk på tvers av alle tre biometriregistre i søknadsprosesser tilknyttet pass-, ID-kort- og utlendingsregisteret.

Leverandøren anbefaler at det legges til rette for at status «unik» kan etableres på grunnlag av registrering i enten utlendings-, pass- eller ID-kortregisteret. Anbefalingen begrunnes i at tiltaket vil være fordelaktig for å øke andelen av status «unik» i Folkeregisteret, uavhengig av utbredelsen på det nasjonale ID-kortet. Leverandøren påpeker at status «unik» vil kunne ha verdi selv uten at vedkommende innehar et nasjonalt ID-kort. Videre vil dette kunne bidra til at tredjelandsborgere oppnår status «unik» raskere, og vil også åpne for at både tjenesteeiere og brukere kan nyttiggjøre seg informasjonsverdien i status «unik» uten å være bundet til nasjonalt ID-kort. Leverandøren har ikke blitt forelagt dokumentasjon som underbygger at biometriopptak i utlendingsforvaltningen ikke skal være av tilstrekkelig kvalitet for å etablere status «unik». Leverandørens anbefaling om «ett felles skrankepunkt» vil også bidra til mer strømlinjeformet styring av biometriopptak i de ulike søknadsløpene, noe som til dels svekker grunnlaget for å begrense status «unik» til å kun baseres på registrering i pass- og ID-kortregistrene. Leverandøren vurderer at argumentene overgår de positive effektene det kan ha i økt kvalitet, forenkling og kontroll å begrense grunnlaget for status «unik» til registrering i pass- og ID-kortregisteret.

Leverandøren anbefaler videre at øvrig teknisk og juridisk tilrettelegging beskrevet i kapittel 2.5.2 følges opp og gjennomføres. Det anbefales spesielt at nødvendig regelverksarbeid for tilbud om nasjonalt ID-kort til utlendinger og hjemmelsgrunnlag for «unik» gis tilstrekkelig prioritet.

Styrke arbeidet med fysisk ID-kontroll

Leverandøren anbefaler at det etableres én offentlig teknologisk løsning for at tjenesteeiere skal kunne gjennomføre biometrisk kontroll av bruker opp mot vedkommende sitt pass og nasjonale ID-kort. Løsningen skal være digital, og tjenesteeiere tar i bruk løsningen etter egen risikovurdering. Leverandøren anser dette som et viktig tiltak for å få full effekt av status «unik» og muliggjøre en sterk fysisk ID-kontroll der nødvendig. Anbefalingen vil følgelig begrense misbruk der brukeren av fysiske ID-bevis ikke er den rettmessige eieren av ID-beviset. Slik beskrevet i kapittel 3.1.5 er både TOVE alternativ 1 og IDmee eksempler på slike løsninger, og anbefalingen henger sammen med tilsvarende løsning for eID.

I kartleggingen har leverandøren fått forelagt lite dokumentasjon av hvordan NAV faktisk utøver ID-kontroll. Leverandøren anbefaler at det gjennomføres en systematisk gjennomgang av ID-arbeidet tilknyttet alle tjenester og ytelser i NAV for brukere i Norge og i utlandet med implementering av tilhørende tiltak. Tiltak i NAV sees i sammenheng med øvrige anbefalte tiltak.

For ytterligere beskrivelse og vurderinger som er lagt til grunn for anbefalingene tilknyttet fysiske ID-bevis og utbredelse av nasjonalt ID-kort se kapittel 2.

5.1.2 Anbefalinger eID

Nasjonal eID anbefales avviklet, da en supplementtilnærming gir begrenset til ingen merverdi og innføring av krav om nasjonal eID anses som risikabelt

Innføring av nasjonal eID er en krevende problemstilling, men basert på leverandørens kartlegging fremstår samlet nytte av nasjonal eID som begrenset. Det er i tilleggsrapporten vurdert ulike roller for nasjonal eID, herunder en nasjonal eID som supplement til eksisterende løsninger, krav om bruk av nasjonal eID for tilgang til enten et utvalg offentlige tjenester eller for alle offentlige tjenester, samt utstedelse av nasjonalt ID-kort uten nasjonal eID.

Flere av de største utfordringene tilknyttet eID i dag, løses ikke ved en supplementtilnærming for nasjonal eID. Ved at nasjonal eID innføres som et supplement til eksisterende løsninger vil brukere fortsatt kunne benytte eksisterende løsninger, og følgelig vil ikke innføring av nasjonal eID ha noen effekt på sikkerheten samlet sett. Nasjonal eID har økt sikkerhet ved utstedelsesprosessen, men ingen endring i sikkerhet tilknyttet bruk. Sikkerheten ved utstedelse øker imidlertid kun for de som anskaffer og bruker den nasjonale eID-en og ikke for brukere som benytter øvrige private eID-er. Den digitale sårbarheten reduseres noe, men ikke vesentlig. En supplementtilnærming vil videre gi noe redusert brukervennlighet for de brukere som velger å benytte nasjonal eID, men effekten på brukervennlighet vil samlet sett være uendret da brukere står fritt til å benytte eksisterende løsninger. Ressursbruken vil øke ved en supplementtilnærming for nasjonal eID og det stilles spørsmål ved behov for fremtidig ressursbruk da behov for videreutvikling av løsningen ikke er hensyntatt. Samtidig vurderer leverandøren videre nytteverdien av øvrige anbefalinger tilknyttet eID, til å være større enn å innføre en supplementtilnærming av nasjonal eID isolert sett.

I leverandørens vurdering av alternative roller for nasjonal eID fremstår innføring av krav til bruk av nasjonal eID lite hensiktsmessig, spesielt om kravet settes for et lite utvalg offentlige tjenester. Et krav til bruk av nasjonal eID vil være risikabelt med tanke på å sikre nødvendig utbredelse av løsningen og god tilgang til offentlige tjenester for brukere. Leverandøren anser at et krav om bruk av nasjonal eID vil være svært ressurskrevende og at det ikke vil svare til nytten som oppnås ved et krav. Det er

videre risikabelt å sette krav til å benytte en løsning som fremstår å ha lav brukervennlighet sammenlignet med eksisterende løsninger.

Samlet sett vurderer leverandøren at en supplementtilnærming for nasjonal eID gir liten til ingen merverdi for sikkerhet og brukervennlighet og at ressursbruken vil øke. Innføring av krav til bruk av nasjonal eID er risikabelt med tanke på utbredelse og brukervennlighet, og vil kreve betydelig ressursbruk for det offentlige. Nasjonal eID har vært planlagt over lengre tid og politiet har vist manglende gjennomføringskraft i arbeidet med utrullingen av nasjonalt ID-kort med eID. Leverandøren anbefaler følgelig at nasjonal eID avvikles og at eksisterende eID-løsninger forbedres slik anbefalt under.

Leverandøren gir ingen anbefaling om eventuelle endringer i vederlagsmodellen for nasjonal eID, da nasjonal eID anbefales avviklet. På samme grunnlag ser leverandøren mindre grunn til at gyldighetstiden for nasjonalt ID-kort, uten nasjonal eID, skal være annerledes enn for pass. Dette har imidlertid ikke vært en del av mandatet for tilleggsoppdraget og har dermed ikke vært gjenstand for en komplett vurdering. Leverandøren ser likevel det som hensiktsmessig at det bør vurderes om gyldighetstiden for nasjonalt ID-kort skal harmoniseres med valgt gyldighetstid for pass.

Leverandøren anbefaler videre at det snarlig gjennomføres en vurdering av om et offentlig-privat samarbeid for én felles kjerneinfrastruktur for private eID-er er en mer hensiktsmessig innretning for at det offentlige skal kunne ha en større rolle i befolkningens digitale autentisering ved bruk av eID.

Styrke sikkerheten ved utstedelse av private eID-er

Uavhengig av rollen til nasjonal eID og leverandørens anbefaling om avvikling, anbefaler leverandøren at sikkerheten ved utstedelse av private eID-er styrkes ved å innføre alternativ løsning 1 beskrevet i kapittel 3.5.1, alternativ løsning 2 beskrevet i kapittel 3.5.2 og alternativ løsning 4 beskrevet i kapittel 3.5.4. De alternative løsningene anbefales innført samlet for å sikre høyest mulig styrking av sikkerheten ved utstedelse av private eID-er. Leverandøren anbefaler følgelig at de tre løsningene under innføres:

- Sette krav til norsk pass eller nasjonalt ID-kort, og status «unik» i Folkeregisteret, for utstedelse av private eID-er
- Muliggjøre at ID-kontrollen som gjennomføres ved pass- og ID-kontor kan benyttes som grunnlag for utstedelse av private eID-er
- Tilrettelegge for at biometrisjekk ved hjelp av teknologiske løsninger for kontroll av bruker og fremvist ID-bevis ved utstedelse av private eID-er, med og uten fysisk oppmøte, kan gjennomføres

Anbefalingen vil sikre at brukere som får utstedt private eID-er har status «unik» i Folkeregisteret, ettersom den nødvendige biometriske informasjonen som behøves for å oppnå «unik» registreres og sjekkes ved utstedelse av norske pass og nasjonalt ID-kort. Videre vil anbefalingen utnytte den sterke ID-kontrollen, med tilhørende opptak av biometri, som gjøres ved pass- og ID-kontor, hvilket vil begrense feilutstedelse av eID-er. Innføring av biometrisjekk av bruker og fremvist ID-bevis vil kunne muliggjøre at bruker selv utfører ID-kontrollen for utstedelse av private eID-er, og behovet for oppmøtet for ID-kontroll og utstedelse av privat eID som i dag gjennomføres ved en bankfilial eller postkontor/post i butikk vil kunne falle bort.

Implementere teknologisk løsning for biometrisk kontroll av bruker og ID-bevis tilknyttet bruk av eID-er

Leverandøren anbefaler at det offentlige har én teknologisk løsning for å kunne gjennomføre biometrisk kontroll av bruker opp mot vedkommende sitt pass eller nasjonale ID-kort ved bruk av eID-er. Leverandøren anbefaler at biometrisjekk av bruker opp mot ID-bevis gjennomføres hyppig eller sjelden basert på en risikobasert vurdering av tjenesten som brukeren ønsker tilgang til. Løsningen skal kunne benyttes uavhengig av om bruker autentiserer seg med en norsk privat eID, nasjonal eID eller en utenlandsk eID gjennom ID-porten. Anbefalingen vil begrense misbruk der brukeren av eID-en ikke er den rettmessige eieren, som er den viktigste utfordringen ved dagens tilnærming til eID. Slik beskrevet i kapittel 3.1.5 er både TOVE alternativ 1 og IDmee eksempler på slike løsninger og det finnes andre løsninger i markedet. Leverandøren anbefaler videre at det offentlige har eierskap til en slik løsning for å sikre tilgang til sertifikatlister med høyest mulig kvalitet, hvilket bidrar til økt sikkerhet ved bruk av løsningen. Leverandøren anbefaler at en slik løsning anskaffes og eies av Difi i tett samarbeid med politiet, gitt dagens styringsstruktur i ID-forvaltningen.

De tre anbefalingene vil medføre at det offentlige har ulik prinsipiell tilnærming til ID-forvaltningen i det fysiske og det digitale rom tilknyttet knytningen mellom identitetsnummer og ID-bevis, ved at det offentlige kun utsteder fysiske ID-bevis og at det private utsteder elektroniske ID-bevis. Leverandøren vurderer at dette kan være en hensiktsmessig ansvarsfordeling, og anser at det offentlige gjennom arbeid med utstedelse av fysiske ID-bevis, tildeling av identitetsnummer og forvaltning av Folkeregisteret, regulering av markedet for eID-er, styring av tilgang til offentlige tjenester gjennom ID-porten med videre uansett vil ha en sentral og premissgivende rolle i ID-forvaltningen også i det digitale rom.

For ytterligere beskrivelse og vurderinger som er lagt til grunn for anbefalingene tilknyttet eID se kapittel 3.

5.1.3 Anbefalinger styring og struktur – et felles skrankepunkt

Etablere et felles skrankepunkt med politiets, Skatteetatens og UDIs førstelinje for å styrke sikkerheten og redusere antall oppmøter i ID-forvaltningen

Leverandøren anbefaler å etablere et felles skrankepunkt (førstelinje) for ID-relaterte kjerneoppgaver knyttet til identitetsregistrering og ID-kontroll (som beskrevet i alternativ 2 i kapittel 4.4.4) i Norge for å:

- Sikre at viktige ID-oppgaver blir utført enhetlig, sikkert, effektivt og brukervennlig
- Sikrer at både norske og utenlandske borgere kun trenger å oppgi informasjon én gang, får tilstrekkelig veiledning og oppnår rask søknadsbehandling samtidig som antall fysiske oppmøter begrenses til et minimum
- Sikre enhetlig registrering av grunndata i riktige registre og utøve ID-kontroll både av norske og utenlandske borgere ved hjelp av like rutiner, retningslinjer og ansatte med spisskompetanse

Skrankepunktet inkluderer kun prosesser for ID-relaterte oppmøter som gjennomføres i Norge. Dette medfører at aktiviteter som finner sted i utlandet, på utenriksstasjonene, er holdt utenfor og er ikke en del av anbefalingen. Det samme gjelder asylsøkerprosessen som i hovedsak gjennomføres i PUs førstelinje som beskrevet i kapittel 4.2.1.

Hva er et felles skrankepunkt

Leverandøren anbefaler at følgende prosesser fra politiet, Skatteetaten og UDI inngår i et felles skrankepunkt (som beskrevet i kapittel 4.4.4 om alternativ 2):

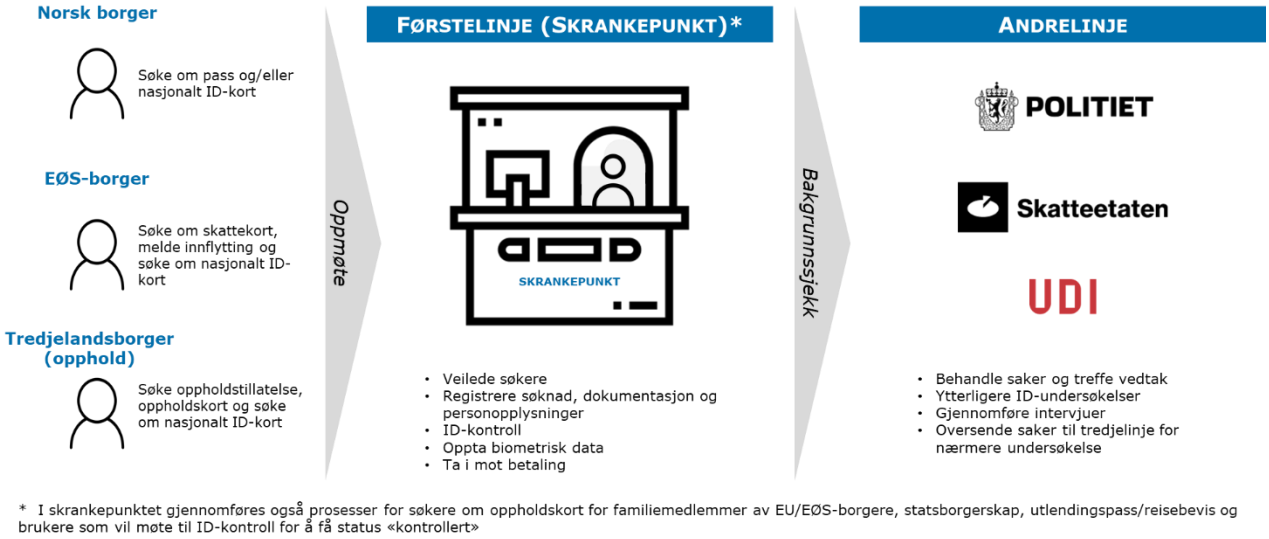
- *Søknad om pass og/eller nasjonalt ID-kort (fra pass- og ID-kontor)*
- *Søknad om skattekort for personer som ikke har fødselsnummer eller «kontrollert» d-nummer (fra skattekontor)*
- *Melde innflytting til Norge fra utlandet (fra skattekontor)*
- *ID-kontroll gjennomført på vegne av andre rekvirenter i tilfeller der det kreves status «kontrollert» eller bruker ønsker å bli «kontrollert» (fra skattekontor)*
- *Søknad om oppholdstillatelse og utstedelse av oppholdskort (fra utlendingskontor)*
- *Søknad om oppholdskort for familiemedlemmer av EU/EØS-borgere (fra utlendingskontor)*
- *Søknad om statsborgerskap (fra utlendingskontor)*
- *Søknad om utlendingspass og reisebevis (fra utlendingskontor)*

Skrankepunktet legges til politiet og de 78 planlagte pass- og ID-kontorene. Politiets førstelinje er et naturlig valg som felles skrankepunkt, da de har identitetsregistrering og ID-kontroll som en av sine kjerneoppgaver, og innehar nødvendig kompetanse og infrastruktur i form av oppmøtesteder og teknisk utstyr. POD, underlagt JD, har ansvaret for administrativ og faglig ledelse, styring, oppfølging og utvikling av politidistriktene, herunder de felles skrankepunktene.

Pass- og ID-kontorene representerer her et grensesnitt mot alle brukergrupper. Et felles skrankepunkt innebærer at alle norske borgere, EØS-borgere og tredjelandsborgere møter opp på samme sted og får løst alle sine behov som krever oppmøter i prosessene over, i mange tilfeller kun ved ett oppmøte. I de felles skrankepunktene vil alle ansatte kunne motta alle typer saker og det vil følgelig være et felles køsystem hvor de fleste timene må bestilles på forhånd.

Leverandøren har i figuren under skissert hvordan et felles skrankepunkt vil fungere i praksis for norske borgere, EØS-borgere og tredjelandsborgere som søker opphold.[223] I tillegg vil øvrige tredjelandsborgere som søker statsborgerskap, oppholdskort for familiemedlemmer av EU/EØS-borgere, utlendingspass/reisebevis eller borgere som ønsker å møte til ID-kontroll for å få status «kontrollert», kunne møte i de felles skrankepunktene for å gjennomføre disse prosessene.

[223] For tredjelandsborgere med søkere om opphold som eksempel da dette er den største gruppen tredjelandsborgere



Figur 42 Illustrasjon av et felles skrankepunkt

Ved etablering av et felles skrankepunkt må ansvars- og oppgavefordelingen mellom første- og andrelinje endres og tydeliggjøres som beskrevet i kapittel 4.4.2. Det etableres todelt saksbehandling hvor førstelinjen veileder, mottar søknader, registrerer dokumentasjon og personopplysninger for alle typer saker. Videre gjennomfører førstelinjen ID-kontroll, opptar biometrisk data og tar imot betaling der dette er påkrevd. Det gjøres ingen form for ytterligere saksbehandling i førstelinjen. Når aktivitetene er gjennomført oversendes saken fortrinnsvis digitalt til andrelinjen i enten politiet, UDI eller Skatteetaten avhengig av sakstype. Det er kun andrelinjen som har vedtaksmyndighet i alle saker. Andrelinjen og vedtaksmyndigheten vil som i dag ligge i respektive eksisterende etater.

Anbefalingen medfører at politiet ved politidistriktene gis myndighet til å rekvirere identitetsnummer, både d-nummer og fødselsnummer.[224] Dette kan gjøres på samme måte som for utlendingsmyndighetene per i dag.[225] Grunnlaget for rekvireringen vil fra politiets side være å utøve myndighetsoppgaver på vegne av andre aktører i skrankepunktene, og på sikt for å utstede nasjonale ID-kort til personer som får dette tilbudet. Skatteetaten er fortsatt tildelingsmyndighet av identitetsnummer.

Behov for systemstøtte og regelverksendringer

Anbefalingen omfatter ikke endring av myndighetsansvar mellom POD, SKD og UDI eller etablering av en ny myndighet på direktoratsnivå, men vil påvirke myndigheten som ligger til skattekontorene i første instans, jf. § 1-3 i folkeregisterloven. I praksis vil endringen fungere på samme måte som myndigheten som er delegert til utlendingskontorene i dag, blant annet gjennom utlendingsloven, forskrift, rundskriv og databehandleravtaler.[226]

Et felles skrankepunkt krever endringer i relevante regelverk med tilhørende forskrifter, herunder harmonisering av regelverk, etablering av nødvendige hjemler, samt felles begrepsbruk og semantikk for å legge til rette for «kun én gang» og sammenhengende tjenester med brukeren i sentrum. Det er nødvendig å etablere hjemler for sikker deling av data mellom myndighetene slik at opplysningene som innhentes, registreres. kontrolleres og utleveres, kan benyttes til flere formål hos de respektive myndighetene på tvers av instanser og sektorer. Personvernhensyn har stor betydning for utformingen

[224] PU er per i dag eneste enhet innen politiet som har myndighet til å rekvirere d-nummer
[225] Utlendingsmyndighetene sender melding til Skatteetaten når en person får innvilget oppholdstillatelse og Skatteetaten tildeler identitetsnummer på bakgrunn av meldingen
[226] Informasjon mottatt på e-post fra UDI, andre halvår 2019

av regelverket. Dette må som nevnt tidligere understøttes av tilstrekkelig systemstøtte slik at vedtakslinjer i neste instans har tilgang til nødvendige saksopplysninger.

En viktig forutsetning for realiseringen av et felles skrankepunkt er at utførelsen av arbeidsoppgavene understøttes av nødvendig systemstøtte. Det er avgjørende med et godt integrasjonsgrunnlag som kan understøtte formålet med et felles skrankepunkt slik at opplysninger og data kan overføres på tvers av systemene på en sikker og enkel måte. Leverandøren anbefaler at det undersøkes nærmere ulike løsninger for dette.

Større kompleksitet i fag- og styringslinjer

Styrings- og ansvarsforholdene mellom politiet og Skatteetaten endres ved å etablere et felles skrankepunkt. Det gir større kompleksitet i fag- og styringslinjene og trolig økt behov for koordinering mellom de to etatene. Det er færre endringer relatert til samhandlingen mellom POD og UDI utover at grensesnittet mellom pass- og ID-kontorene og utlendingskontorene internt i politiet påvirkes.

SKD vil fortsatt være folkeregistermyndighet og behandlingsansvarlig for Folkeregisteret. Myndigheten som er delegert til skattekontorene i første instans påvirkes ved at ansvar, oppgaver, medarbeidere og ressurser for definerte prosesser på skattekontorene overføres til pass- og ID-kontorene. Anbefalingen innebærer at oppgaveporteføljen på skattekontorene reduseres. Grensesnittet mellom utlendingskontorene og pass- og ID-kontorene endres ved at førstelinjen samles i et skrankepunkt.

Færre oppmøter for EØS-borge og tredjelandsborgere

Anbefalingen påvirker ikke antall oppmøter for norske borgere, som fortsatt vil ha ett oppmøte i forbindelse med søknad om pass og/eller nasjonalt ID-kort. For EØS-borgere blir brukervennligheten markant bedre. Avvikling av EØS-registreringsordningen og muligheten til å gjennomføre flere aktiviteter i et felles skrankepunkt, reduserer antall oppmøter fra fire til ett. Anbefalingen vil også ha betydelig effekt på brukervennligheten for tredjelandsborgere. Muligheten for å gjennomføre flere aktiviteter i et felles skrankepunkt vil redusere antall oppmøter fra tre til to for søkere om statsborgerskap eller to til ett for søkere om opphold eller oppholdskort for familiemedlemmer av EU/EØS-borgere.

Endret organisering gir gevinster i et samfunnsperspektiv

Politiet og de 78 planlagte pass- og ID-kontorene er et naturlig valg som felles skrankepunkt, da de har identitetsregistrering og ID-kontroll som en av sine kjerneoppgaver, og innehar nødvendig kompetanse og infrastruktur i form av oppmøtesteder og teknisk utstyr. Alle ledere og medarbeidere ved skrankepunktene vil være ansatt i politiet.

Det er ikke behov for å endre utformingen av pass- og ID-kontorene, etter utrulling av biometrikiosker og annet teknisk utstyr for ID-kontroll og dokumentgransking, for å kunne utføre aktivitetene knyttet til skatte- og utlendingsrelaterte prosesser på samme sted. Derimot vil det være nødvendig å vurdere dimensjoneringen og utvidelse av kapasitet nærmere ved hvert enkelt kontorsted for å sikre at det er tilstrekkelig med bemanning og skranker for å håndtere nye oppgaver og prosesser fra både skattekontorene og utlendingskontorene. Det gjelder også utstedelse av nasjonalt ID-kort for utlendinger.

I tråd med styrt utvikling og pågående arbeid med å digitalisere og automatisere Skatteetatens tjenester har leverandøren grunn til å tro at behovet for fysiske oppmøter på de 42 skattekontorene vil reduseres til et minimum eller opphøre på mellomlang

sikt. Formålet til SUA-kontorene vil i sin helhet bortfalle da alle prosesser som i dag utføres på disse kontorene vil legges til de felles skrankepunktene. Når det gjelder utlendingskontorene vil det være et redusert behov for skranker eller direkte kontakt med bruker på de i dag 41 eksisterende utlendingskontorene. Dette gir muligheter for å digitalisere og effektivisere gjenstående oppgaver i andrelinjen.

Endret skrankepunktorganisering vil gi størst gevinster knyttet til økt sikkerhet og brukervennlighet. Skrankepunktet bidrar til noe redusert ressursbruk for forvaltningen, men potensialet er størst sett fra et samfunnsperspektiv. Det vil være vesentlige sikkerhetsgevinster som følge av enhetlig registrering av grunndata i riktige registre og utøvelse av ID-kontroll vil det være hensiktsmessig å gjenbruke ID-kontroll og annen relevant informasjon innhentet i skrankepunktet (ansiktsfoto, signatur etc.) for andre aktører, eksempelvis for utstedere av private eID-er og Statens vegvesen for utstedelse av førerkort. Det vil gi positive ringvirkninger i forvaltningen. Det vil også være betydelig gevinster i form av spart tidsbruk ved færre oppmøter for EØS-borgere og tredjelandsborgere.

Robuste fagmiljø for økt kompetanse og kvalitet i ID-aktiviteter

Anbefalingen medfører at det etableres et robust fagmiljø for utførelse av viktige sammenfallende ID-aktiviteter som per i dag finner sted i førstelinjen på henholdsvis pass- og ID-kontorene, skattekontorene og utlendingskontorene. Det gis faglige og tekniske forutsetninger for bedre ID-kontroll ved alle prosesser. En forutsetning for enhetlige, sikre, effektive og brukervennlige felles skrankepunkt er at POD gir felles overordnede føringer til politidistriktene om hvordan og etter hvilke rutiner og retningslinjer aktivitetene skal gjennomføres og hvilken kompetanse de ansatte skal inneha. Det bør videre være fokus på å bygge kompetanse spesifikt tilknyttet disse aktivitetene. Totalt gir dette økt kvalitet og økt sikkerhet i prosessene.

Anbefalingen legger grunnlag for å kunne følge opp tiltak 27 i regjeringens strategi mot arbeidslivskriminalitet ved at EØS-borgere i Norge behandles enhetlig i en samlet førstelinje ved rekvirering av d-nummer og ID-kontroll, noe som gir en sikrere og mer effektiv identitetsforvaltning for EØS-borgerne.

Trinnvis implementering av felles skrankepunkt

I kapittel 4.4.3 og 4.4.4 har leverandøren beskrevet to alternative tilnærminger til et felles skrankepunkt. Leverandøren anbefaler en trinnvis implementering av et felles skrankepunkt ved å innføre et felles skrankepunkt for prosessen ved pass- og ID-kontor og prosessene i skattekontorene først, ved å pilotere på utvalgte lokasjoner, for å lære og innhente erfaringer for så å gradvis innfase på alle lokasjoner. På et senere tidspunkt innfase prosessene ved utlendingskontorene i samme skrankepunkt.

Sammenhenger med øvrige anbefalinger

Leverandørens anbefalinger er delvis avhengige av hverandre. Spesielt gjelder dette anbefalingen tilknyttet felles skrankepunkt som legger til rette for et oppmøtested for ID-relaterte oppgaver for alle brukergrupper på tvers av forvaltningen, og derigjennom stimulere til én person, én identitet i Norge ved at flere får tilgang på gyldige ID-bevis og en større andel blir «kontrollert» og/eller «unik» i Folkeregistret. Et felles skrankepunkt muliggjør høyere utbredelse av nasjonalt ID-kort for EØS-borgere og tredjelandsborgere.

Gjennom arbeidet med et felles skrankepunkt opprettholder leverandøren hovedrapportens anbefaling «Sikre helhetlig styring og tydeliggjøre ansvar for ID-forvaltningen gjennom å nærmere utrede eierskap og etablering av en ID-etat (eventuelt ID-direktorat)». Anbefalingen om et felles skrankepunkt kan implementeres

uavhengig av om en ID-etat velges utredet. Et felles skrankepunkt er et steg i riktig retning for å sikre helhetlig styring og ansvar for ID-forvaltningen i Norge. Det er et av flere virkemiddel for å oppnå visjonen for ID-forvaltningen, men etter leverandørens syn vil det være nødvendig å ta i bruk sterkere grep langs styring- og strukturdimensjonen over tid.

For ytterligere beskrivelse og vurderinger som er lagt til grunn for anbefalingen se kapittel 4.

5.1.4 Konsekvenser for anbefalinger i hovedrapporten

Som del av arbeidet med tilleggsrapporten har leverandøren arbeidet direkte videre spesielt med to av anbefalingene fra hovedrapporten:

- *Anbefaling 2: Tydeliggjøre at norsk pass og nasjonalt ID-kort er gyldige fysiske ID-bevis, samt stille krav til disse for tilgang for offentlige tjenester og ytelser*
- *Anbefaling 3: Styrke arbeidet med eID*

Anbefalingene i tilleggsoppdraget tilknyttet tema 1 om fysiske ID-bevis og nasjonalt ID-kort, spesielt knyttet til hvordan krav til norsk pass og nasjonalt ID-kort kan stilles, nyanserer og endrer deler av anbefaling 2 fra hovedrapporten. For øvrig gjør leverandøren ingen endring i sin anbefaling 2 fra hovedrapporten. Anbefalingene i tilleggsoppdraget tilknyttet tema 2 om eID erstatter i sin helhet anbefaling 3 fra hovedrapporten.

Arbeidet med et felles skrankepunkt berører flere av anbefalingene fra hovedrapporten og spesielt to av anbefalingene:

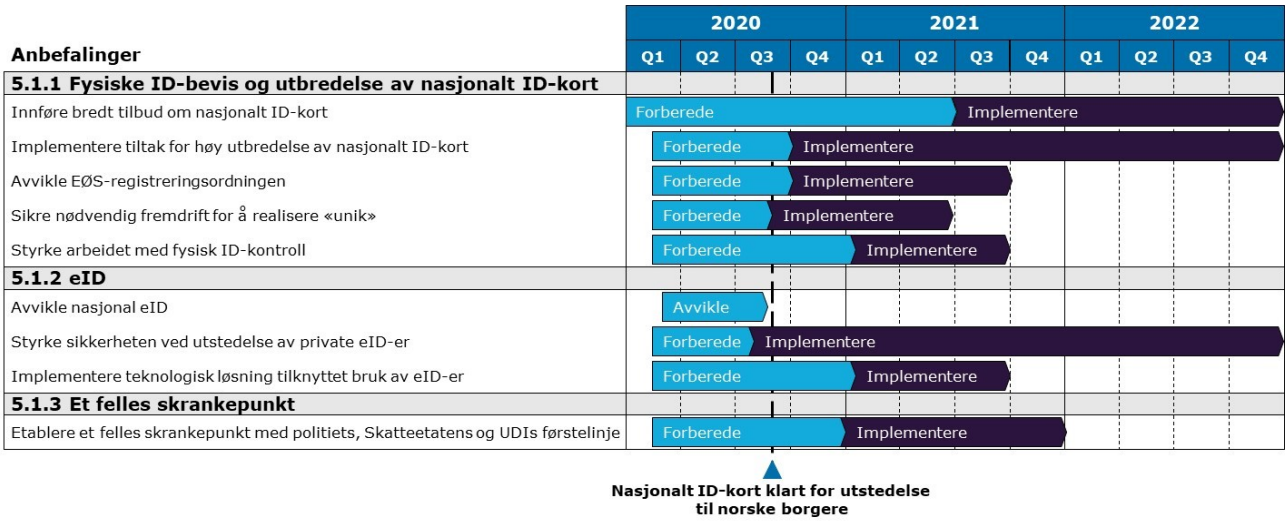
- *Anbefaling 6: Redusere brukers behov for fysiske oppmøter gjennom å tilrettelegge for økt deling av data og gjenbruk av ID-kontrollen ved ett skrankepunkt*
- *Anbefaling 7: Sikre helhetlig styring og tydeliggjøre ansvar for ID-forvaltningen gjennom å nærmere utrede eierskap og etablering av en ID-etat (eventuelt ID-direktorat)*

Arbeidet med et felles skrankepunkt gir ingen endringer i anbefaling 6 og 7 i hovedrapporten.

Arbeidet med tilleggsrapporten gir heller ingen endring på øvrige anbefalinger.

5.2 Plan for gjennomføring

Figuren under illustrerer en overordnet gjennomføringsplan for leverandørens anbefalinger, med foreslått tidspunkt for forberedelse og implementering av de ulike anbefalingene.



Figur 43 Overordnet gjennomføringsplan for anbefalinger

5.3 Gevinster og utvalgte implementeringskostnader

Slik beskrevet i kapittel 16.3 og kapittel 8 i hovedrapporten er den reelle og enhetlige dokumentasjonen av dagens sikkerhet, brukervennlighet og ressurseffektivitet begrenset. Dette vanskeliggjør gode vurderinger av hvilken samfunnsmessig gevinst anbefalinger med økt ressursbruk medfører av økt sikkerhet og derav reduserte samfunnskostnader. Samlet nytte av anbefalingene er derav krevende å estimere.

Effekt på sikkerhet, brukervennlighet og ressursbruk

Tema 1: Fysiske ID-bevis og utbredelse nasjonalt ID-kort

Delanbefaling 1 om et tilbud om nasjonalt ID-kort til alle med rett på fødselsnummer og d-nummer vil isolert sett tilrettelegge for økt sikkerhet i forvaltningen. Ressursbruken for utstedelse av nasjonale ID-kort antas å øke fra dagens situasjon, da et bredere tilbud antas å medføre høyere utstedelsesvolum. Brukervennligheten vil øke med et bredt tilbud, spesielt for brukergrupper som tidligere ikke har hatt tilgang til sterke ID-bevis.

Delanbefaling 2 vil gi økt sikkerhet sammenlignet med dagens situasjon. Anbefalingen vil kunne ha betydelig sikkerhetsmessig effekt når relevante aktører gjennomfører en kollektiv innsats for å stimulere til høyest mulig utbredelse og krav om norsk pass og nasjonalt ID-kort. Anbefalingen anses likevel å gi mindre sikkerhetsmessige gevinster enn leverandørens anbefaling 2 fra hovedrapporten. Til gjengjeld vil en mer fleksibel tilnærming til krav kunne oppfattes som mer brukervennlig, spesielt for brukere som vil ha utfordringer med å anskaffe et norsk pass eller nasjonalt ID-kort. Effekt på ressursbruk er ikke vurdert kvantitativt, men vil i stort avhenge av i hvilken grad tjenesteeiere velger å stilles krav.

Delanbefaling 3 om å avvikle EØS-registreringsordningen, vil gi en håndfast besparelse for forvaltningen. Redusert tidsbruk som følge av et redusert oppmøte for bruker anses

brukervennlig for de brukerne som berøres av tiltaket. Leverandøren ser ingen vesentlige sikkerhetsmessige implikasjoner av å avvikle EØS-registreringsordningen.

Delanbefaling 4 om at «unik» baseres på pass-, ID-kort og utlendingsregisteret og det må sikres nødvendig fremdrift for juridisk og teknisk tilrettelegging har isolert sett begrensede gevinster. Implementering av «unik» stor positiv konsekvens for sikkerheten.

Delanbefaling 5 om styrking av fysisk ID-kontroll, vil ha stor positiv konsekvens for sikkerheten i ID-forvaltningen gjennom redusert risiko for imposter-misbruk. Økt ressursbruk må påregnes for å tilgjengeliggjøre nødvendig utstyr for sterk fysisk ID-kontroll hos tjenesteeiere. Effekten på ressursbruk anses derfor middels negativ.

Tema 2: Elektronisk ID (eID)

Delanbefaling 1 om å avvikle nasjonal eID vil gi middels positiv konsekvens for det offentliges ressursbruk. Selv om det offentlige vil kunne unngå 28 mill. kroner i investeringskostnader som POD enda ikke har forpliktet seg til, samt spare 12 mill. kroner i estimerte årlige forvaltningskostnader til nasjonal eID, vil det økonomiske regnestykket isolert for forvaltningen gå i null ettersom nasjonal eID i sin helhet er gebyrfinansiert. Det totale antall brukere som anskaffer nasjonalt ID-kort vil derimot spare tilsvarende beløp som nevnt over ved at utstedelsesgebyret for nasjonalt ID-kort kan reduseres som følge av at nasjonal eID avvikles, med tilhørende samfunnsøkonomisk samlet gevinst. Leverandøren vurderer imidlertid at avvikling av nasjonal eID vil spare forvaltningen for kostnader til videreutvikling av løsningen, som ikke inngår i gebyrmodellen og dermed ikke er planlagt gebyrfinansiert. Dersom en harmonisering av gyldighetstiden for pass og nasjonalt ID-kort medfører økt gyldighetstid for nasjonalt ID-kort, vil dette ha betydelige samfunnsmessige effekter i form av redusert antall oppmøter for brukere, reduserte gebyrkostnader og redusert ressursbruk for forvaltningen.

Delanbefaling 2 om å styrke sikkerheten ved utstedelse av private eID-er, anses å ha stor positiv konsekvens for sikkerheten i ID-forvaltningen, da den vil sikre at status «unik» vil ligge til grunn for utstedelsen av alle nye private eID-er, samt begrense feilutstedelser av private eID-er. Fra et brukervennlighetsperspektiv vil anbefalingen om tilrettelegging for biometrisjekk uten oppmøte ved utstedelse av private eID-er ha stor positiv konsekvens. Tiltaket vil tilsvarende potensielt ha en stor samfunnsøkonomisk effekt på ressursbruk i bankfilial og postkontor/post i butikk dersom det tillater at det fysiske oppmøtet og ID-kontroll i bankfilial og postkontor/post i butikk faller bort.

Delanbefaling 3 om å implementere teknologisk løsning for biometrisk kontroll av bruker og ID-bevis tilknyttet bruk av eID-er, vil ha meget stor positiv konsekvens for sikkerheten ved at misbruk der brukeren av eID ikke er rettmessig eier reduseres. Anbefalingen vil ha liten negativ konsekvens for det offentliges ressursbruk, da det er overordnet estimert at kostnader til implementering bør være begrenset.

Tema 3: Styring og struktur – et felles skrankepunkt

Anbefalingen under tema 3 vil ha meget stor positiv innvirkning på sikkerheten i ID-forvaltningen gjennom etablering av robuste fagmiljøer, todelt saksbehandling og sikrere prosesser for registrering av identitet og utstedelse av ID-bevis. Anbefalingen anses å ha stor positiv konsekvens for brukervennligheten som følge av færre oppmøter for EØS-borgere og tredjelandsborger og flere mulige oppmøtelokasjoner. Tiltaket vil også ha positiv effekt på ressursbruk, men i noe mindre grad enn for sikkerhet og brukervennlighet, i form av bedre kapasitetsutnyttelse ved gjenbruk av ID-kontroll og økt deling av data. Det er krevende å estimere prissatt nytte ved deling av data, siden

det ikke er dataene eller delingen i seg selv, men anvendelsen av dataene som skaper verdi. DNV GL og Menon Economics (2015) peker på et potensial på flere mrd. kroner ved felles metoder og standarder for beskrivelser og informasjonsforvaltning i offentlig sektor.

Overordnede estimat på økonomiske gevinster for brukere og forvaltning

Tema 1: Fysiske ID-bevis og utbredelse nasjonalt ID-kort

For tema 1, fysiske ID-bevis og utbredelse av nasjonalt ID-kort, medfører anbefalingene isolert sett begrensede økonomiske gevinster. Gevinsten av å avvikle EØS-registreringsordningen er hensyntatt i vurderingene tilknyttet et skrankepunkt. Et bredt tilbud om nasjonalt ID-kort vil medføre økt ressursbruk for forvaltningen isolert sett, men vil være dekket av gebyr fra brukerne. Den økte ressursbruken av et bredt tilbud sammenlignet med et smalere tilbud er ikke kostnadsberegnet, men anses som nødvendig for å realisere visjonen for ID-forvaltningen.

Tema 2: Elektronisk ID (eID)

Gjennomføring av anbefalingene for tema 2, eID, vil medføre moderate til lave implementeringskostnader. Det er ikke beregnet direkte økonomiske gevinster av anbefalingene.

Tema 3: Styring og struktur – et felles skrankepunkt

Gjennomføring av anbefalingen for tema 3, et felles skrankepunkt, medfører gevinster for bruker og forvaltning som beskrevet gjennomgående i kapittel 4.4.4. Leverandøren understreker at de største gevinstene ved gjennomføring av etablering av et felles skrankepunkt vil knytte seg til økt sikkerhet og brukervennlighet.

Gevinster for brukere i form av tidsbesparelse er estimert til en tidsverdi på ca. 135 mill. kroner for EØS-borgere og tredjelandsborgere per år. For forvaltningen er gevinster i form av reduserte årsverk estimert til å omtrent være netto 30 årsverk. Disse fordeler seg på reduserte årsverk ved skattekontorene og utlendingskontorene, samt et behov for flere årsverk ved de felles skrankepunktene grunnet en økning i avsatt tid i skrankepunktet per bruker fra 20 til 25 minutter. Reduksjon i årsverk tilsvarer en total kostnadsbesparelse på ca. 17 mill. kroner. Mer effektiv saksbehandling som følge av standardiserte og hvor mulig digitaliserte prosesser samt økt deling av data vil videre kunne bidra til å redusere ressursbruk ytterligere både i første- og andrelinje. En potensiell reduksjon i antall SUA-kontor, skattekontor og utlendingskontor som muliggjøres ved å etablere et felles skrankepunkt for ID-forvaltningen kunne spare staten for leiekostnader og øvrige driftskostnader.

Implementeringskostnader vil på en annen side redusere de økonomiske gevinstene. Grunnet mangel på tallgrunnlag og ressursbruk tilknyttet dette er kostnadene kategorisert som ikke-kvantifiserbare effekter. Dette gjelder kostnader knyttet til ombygging/utvidelse av lokaler, IKT-utstyr og systemstøtte, kompetanseutvikling, med mer. For disse effektene må det gjøres ytterligere analyser for å kunne estimere kvantitative kostnader.

Leverandørens vurdering er at samlet nytte vil overstige kostnader til implementering.

© 2019 Capgemini. All rights reserved.