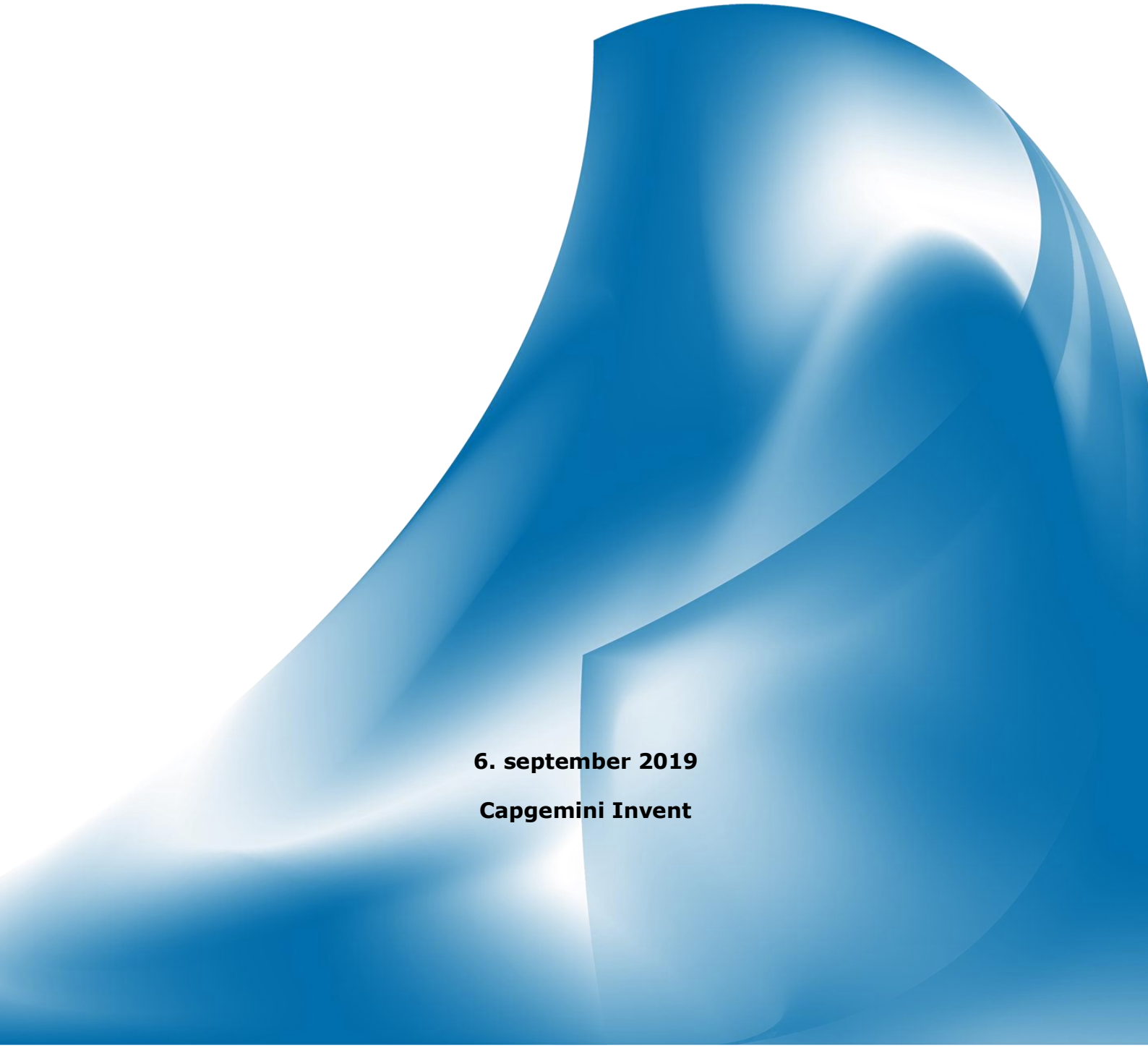
OMRÅDEGJENNOMGANG

ID-forvaltningen



6. september 2019

Capgemini Invent

Innholdsfortegnelse

Definisjonsliste

Leverandøren har under inkludert en liste med viktige definisjoner for ID-forvaltningen som benyttes i rapporten. Det påpekes at definisjonene kan variere med kontekst og at de her gjelder ID-forvaltningen om ikke annet er oppgitt.

** I tråd med OECDs offisielle definisjoner*

*** Definisjon hentet fra Nasjonalt ID-senter*

**** Definisjon hentet fra Datatilsynet*

Andrelinje og tredjelinje**
Andrelinje og tredjelinje beskriver på hvilket kompetansenivå identitetsdokumentene er blitt undersøkt. Andrelinje består av høyt kvalifiserte dokumentgranskere med avansert utstyr for ekthetsvurdering og tilgang på referanser. De arbeider ofte tett sammen med førstelinjen. Tredjelinje er et spesialistnivå med sakkyndige dokumentgranskere, avansert utstyr for ekthetsvurdering og rekonstruksjon av forfalskninger.

Autentisering*
Verifisering av en påstått identitet i elektronisk kommunikasjon mellom to ukjente parter.

Biometri**
Biometrisk personinformasjon, heretter kalt biometri, er målbare, fysiske kjennetegn eller personlige atferdsmessige karaktertrekk. Biometri kan brukes til å gjenkjenne identiteten, eller til å verifisere identiteten, til en person som allerede er registrert med biometri, for eksempel fingeravtrykk eller foto.

Bruker
Ethvert individ som har mulighet og behov for å anskaffe et norsk ID-bevis, eller har rettigheter eller krav på ytelser i Norge (norsk borger, EØS-borger eller tredjelandsborger).

Brukergebyr
Kostnad i kroner som påløper for bruker ved utstedelse eller fornyelse av ID-bevis.

Brukerreise
Referer her overordnet til de prosesser og treffpunkt som bruker må gjennom for å anskaffe og fornye ID-bevis gjennom et livsløp, samt brukerens opplevelse av nevnte prosesser og treffpunkt.

Brukertid
Antall minutter som påløper for bruker på ulike treffpunkt direkte tilknyttet utstedelse eller fornyelse av ID-bevis.

Brukervennlighet
Grad av effektivitet og tilfredshet sett fra et brukerperspektiv. Leverandøren legger til grunn at redusert brukertid og redusert brukergebyr gir forbedret brukervennlighet.

D-nummer
Et d-nummer er et midlertidig identitetsnummer som kan tildeles utenlandske personer som i utgangspunktet skal oppholde seg i Norge i mindre enn seks måneder. D-nummeret består av elleve tall hvor de seks første tallene viser fødselsdato, men det første tallet er økt med fire.

Dokumentert identitet
En identitet omtales som dokumentert om en person er identifisert med pass eller annet godkjent legitimasjonsdokument.

Elektronisk ID*
Et sett med attributter som kan benyttes til verifikasjon av påstått identitet i elektronisk kommunikasjon mellom to parter. Eksempel på eID kan være en datafil med biometrisk informasjon, et brukernavn med tilhørende passord, eller et PKI-sertifikat med tilhørende nøkkelpar for autentisering.

Falske dokumenter**
En samlebetegnelse for totalfalske og delvis forfalskede dokumenter, der forfalskede dokumenter er ekte dokumenter hvor det er foretatt endringer. Betegnelsen kan også benyttes for ekte in-blanco dokumenter som er urettmessig utstedt. Beskrivelsen totalfalske dokumenter brukes hvis dokumentet i sin helhet er falskt. Misbruk av identitetsdokumenter vil si bruk av falske identitetsdokumenter, bruk av andre personers ekte dokumenter, eller når ekte dokumenter er utstedt på grunnlag av falske underlagsdokumenter.

Fødselsnummer
Fødselsnummer tildeles alle som blir født i Norge, alle som bosetter seg i Norge (opphold over seks måneder) og norske statsborgere som er født eller bosatt i utlandet og trenger fødselsnummer for å få et norsk pass. Fødselsnummeret består av elleve siffer hvor de seks første tallene viser fødselsdato. De tre neste sifrene er individnummer hvor det tredje nummeret viser til kjønn. De to siste sifrene er kontrollsiffer.

Grunnidentitet
Den identiteten som samfunnet skal ha tillit til og bygge videre på, for eksempel for offentlig og privat tjenesteyting. En norsk grunnidentitet består av et identitetsnummer (fødselsnummer eller et d-nummer) i kombinasjon med et sterkt ID-bevis.

ID-bevis
Benyttes om både fysisk utstedt dokument og elektronisk utstedt identifikasjon som har til hensikt å verifisere at en person er den han/hun utgir seg for å være.

Identifikasjonsdokument**
Benyttes kun om fysisk utstedt identifikasjon (eks ID-kort i lommebokstørrelse, eller andre dokument som fødselsattest/statsborgerbrev). Identitetsdokumenter inneholder tilstrekkelige opplysninger til sikker verifisering av den identiteten en person oppgir ved fremvisning av dokumentet.

Identitet*
(Her) personidentitet, et dynamisk sett med attributter som til sammen definerer en unik referanse til en bestemt person. I noen land, f.eks. Norge, er det tilstrekkelig med ett attributt, som fødselsnummer, mens det i andre land er nødvendig å oppgi en rekke attributter for unik identifikasjon, f.eks. fornavn, etternavn, fødselsdato, fødested, mors og fars navn.

Identitetsforvaltning*
Et bredt administrativt område som dekker det å identifisere personer innenfor et system (som f.eks. kan være et land, et datanettverk eller en organisasjon) og knytte disse til rettigheter og begrensinger til bruk av ressurser i dette systemet.

ID-tyveri***
Identitetstyveri er når noen skaffer seg, besitter, overfører, benytter eller fremstår som rette innehaver av et identifikasjonsbevis eller personopplysningene til en person for å begå økonomisk svindel, bedrageri eller annen kriminalitet. Rent praktisk kan et identitetstyveri for eksempel være å motta offentlige tjenester og ytelser uberettiget eller kjøpe varer, åpne en bankkonto, registrere et telefonabonnement, eller søke om kredittkort eller lån ved å bruke en annens identitet enn sin egen.

Identitetskrenkelse**
Innebærer å uberettiget sette seg i besittelse av en annens identitetsbevis, eller opptre med en annens identitet eller med en identitet som er lett å forveksle med en annens identitet, med forsett om å oppnå en berettiget vinning eller påføre en annen tap eller ulempe.

Identitetsnummer (ID-nummer)
I Norge bruker vi identitetsnummer for å identifisere innbyggere. En rekke offentlige og private virksomheter krever at du har et norsk identitetsnummer for å få tilgang til deres tjenester. Det finnes to ulike typer identitetsnummer: d-nummer og fødselsnummer.

Legitimasjonsdokument
Utstedt dokument som bekrefter at en person er den vedkommende utgir seg for. Dokumentet må være verifisert av en myndig instans. Pass er et eksempel på et legitimasjonsdokument.

Livsløpsperspektiv
Anses som en tidslinje for en gitt bruker fra 0 til 80 år.

Nasjonal eID
Benyttes om eID tilknyttet nasjonalt ID-kort.

Notoritet**
Omhandler ID-bevis som utstedes på bakgrunn av betryggende rutiner og registrerte og etterprøvbare opplysninger. ID-bevis kan ha varierende grad av notoritet.

Rekvisisjon
En rekvisisjon er en bestilling eller forespørsel som sendes til en annen part. I dette tilfelle bestiller en virksomhet opprettelse av et d-nummer som skal tildeles en bruker.

Rekvisisjonsgrunnlag
Saksbehandler fyller ut en rekvisisjon på bakgrunn av opplysninger vedkommende har mottatt om brukeren. Denne dokumentasjonen utgjør rekvisisjonsgrunnlaget. Det kan eksempelvis være et pass eller en søknad verifisert av en myndighet.

Politiet
Politiet brukes som samlebetegnelse for organisasjonsenhetene i politiet som offentlig forvaltningsorgan: Politidirektoratet, politidistriktene, samt underliggende særorganer og andre enheter som Kripos, Politiets utlendingsenhet og Nasjonalt ID-senter.

Sikkerhet
Begrepet sikkerhet kan tolkes svært vidt og brukes på ulike måter. Med sikkerhet i ID-forvaltningen mener leverandøren blant annet sikkerhet i prosessenestegene fastsetting, registrering, utstedelse og kontroll. Spesielt innenfor registrering er informasjonssikkerhet et sentralt område. Informasjonssikkerhet omhandler å sikre at informasjon ikke blir kjent for uvedkommende (konfidensialitet), ikke blir endret utilsiktet eller av uvedkommende (integritet) og er tilgjengelig ved behov (tilgjengelighet).[1]

Status «kontrollert», «ikke-kontrollert» og «unik»
Gjelder kategorisering av identiteter i Folkeregistret. Identiteten er «unik» dersom det foreligger biometriske data i et nasjonalt biometriregister og disse er kontrollert for «unikhet» mot øvrige biometriregistreringer. Identiteten er «kontrollert» dersom identiteten er registrert på grunnlag av fødselsmelding eller kontrollert ved personlig fremmøte for Skatteetaten eller Utlendingsforvaltningen med fremvisning av pass eller lignende. I alle andre tilfeller registreres identiteten som «ikke-kontrollert».

Sterkt fysisk ID-bevis
Et fysisk identitetsbevis som er egnet for en sterk identitetskontroll og som dessuten gir knytning til en norsk identifikator (fødselsnummer eller d-nummer). I tillegg må identitetsbeviset være basert på en sikker utstedelsesprosess.

Sterk identitetskontroll
Innebærer effektiv kontroll av at: a) fysisk identitetsbeviset er ekte (i praksis forutsetter dette chip i kortet) og b) det er innehaveren, og ikke noen andre, som benytter identitetsbeviset (i praksis forutsetter dette sjekk av at brukerens biometri samsvarer med innehaverens biometri). Sterk identitetskontroll kan benyttes i forbindelse med tjenester fra forvaltning og privat sektor, inkludert til å utstede e-ID.

Treffpunkt
Enhver fysisk eller digital interaksjon mellom bruker og en aktør/utsteder i den norske ID-forvaltningen.

Tjenesteeier
Benyttes i rapporten til å omtale både private og offentlige virksomheter som leverer tjenester eller ytelser til ulike brukergrupper innenfor ID-forvaltningens omfang.

Verifisering (av identitet)
En prosess der påstått identitet sjekkes mot et identifikasjonsdokument fremlagt av personen som påberoper seg identiteten.

[1] Difi, «Informasjonssikkerhet», u.å.

Sammendrag

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, mer effektiv ressursbruk og økt brukervennlighet.

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

Overordnet beskrivelse av ID-forvaltningen

For å holde oversikt over personer som er bosatt i landet eller som har annen tilknytning til landet, eksempelvis skatteplikt eller rett til trygdeytelser, tildeler norske myndigheter et identitetsnummer – enten et permanent fødselsnummer eller et midlertidig d-nummer. Identitetsnummeret registreres i Folkeregisteret, som er det sentrale personregisteret i Norge.

Ved registrering i Folkeregisteret skal alle identiteter kategoriseres enten som «unik», «kontrollert» eller «ikke-kontrollert». En person er «unik» dersom biometri (fysiske kjennetegn som for eksempel ansiktsfoto eller fingeravtrykk) foreligger og er sjekket mot andre biometriregistreringer (en-til-mange søk). Personen er «kontrollert» dersom identiteten er registrert på grunnlag av en fødselsmelding eller kontrollert ved personlig fremmøte. For øvrig benyttes kategorien «ikke-kontrollert».

En norsk grunnidentitet består av et identitetsnummer i kombinasjon med et sterkt fysisk ID-bevis. Kartleggingen har identifisert 38 ulike fysiske og elektroniske ID-bevis (eID) i Norge, hvorav tolv av disse er vektlagt i områdegjennomgangen. De vanligste fysiske ID-bevisene er pass, førerkort og bankkort med bilde, mens MinID, BankID, og Buypass er de vanligste eID-ene. Både offentlige og private aktører er utstedere av ID-bevis. ID-bevisene har ulike formål. Eksempelvis gir pass reiserett, førerkort gir førerrett og MinID gir tilgang til offentlige digitale tjenester. Ingen ID-bevis er obligatoriske. Likevel er det i praksis vanskelig å klare seg uten ID-bevis, da dette kreves for å kunne delta i sentrale samfunnsaktiviteter. ID-bevis er nødvendig for eksempel for å åpne en bankkonto, delta i valg, starte en bedrift og kjøre bil.

I tillegg til aktiviteter som inngår i identitetsfastsettelse, registrering av identitet og utstedelse av både fysiske og elektroniske ID-bevis er ID-kontroll en del av ID-forvaltningen. En rekke ID-kontroller gjennomføres av en persons identitet i et livsløp, både av fysisk ID-bevis ved eksempelvis grensekontroller og ved autentisering gjennom bruk av eID for tilgang til tjenester og ytelser fra eksempelvis NAV og Lånekassen. ID-porten benyttes som løsning for å gi tilgang til offentlige digitale tjenester som krever innlogging og autentisering med eID.

Myndighetsansvaret for ID-forvaltningen er delt mellom flere departementer med underliggende etater og virksomheter, hvor elleve departementer med 18 tilhørende virksomheter har en rolle. Organiseringen er historisk betinget og bygger på at aktørene har komparative fortrinn ved utførelse av ulike funksjoner og oppgaver. De mest sentrale aktørene er Politidirektoratet (POD) med ansvar for blant annet utstedelse av pass og nasjonale ID-kort og grensekontroll, Utlendingsdirektoratet (UDI) med overordnet ansvar for utlendingssaker, Skattedirektoratet med ansvar for Folkeregistret og Direktoratet for forvaltning og IKT (Difi) med ansvar for regelverk for eID, formidling av eID-en MinID og ID-porten. Førerkortet godtas også som ID-bevis i

mange sammenhenger og gjør Statens vegvesen (SVV) til en sentral aktør. Banknæringen, med ansvar for bankkort med bilde og BankID, er også en sentral aktør.

POD har siden 2007 arbeidet med å utrede og tilrettelegge for utstedelse av nasjonalt ID-kort med eID i Norge. Arbeidet, som gjennomføres i PODs program «Nye pass og ID-kort» (NPID), har siden den gang vært gjenstand for betydelige forsinkelser. I henhold til nåværende plan vil utrulling av nasjonale ID-kort med eID være klart i løpet av 2020. Det legges til grunn utstedelse basert på frivillighetsprinsippet, tilsvarende dagens ordning for pass. Tjenesteeiere kan selv bestemme om de skal kreve nasjonalt ID-kort for tilgang til offentlige tjenester og ytelser. Et av formålene med et nasjonalt ID-kort med eID er å gjøre det enkelt for norske borgere å skaffe seg et identitetsbevis med høy tillit og bredt bruksområde. I første omgang vil det nasjonale ID-kortet være et tilbud til norske statsborgere, men intensjonen er å utvide tilbudet til også å omfatte utenlandske statsborgere.

Avgrensninger

Arbeidet er gjennomført under forutsetning om at nye pass og nasjonale ID-kort med eID er klart til utstedelse i valgt tjenestestruktur i løpet av 2020. En kvalitetssikring av pass og ID-programmet har ikke vært leverandørens mandat. De første delene av ID-prosessen (identitetsfastsettelse, registrering av identitet og utstedelse av ID-bevis) er i samråd med oppdragsgiver vektlagt høyere prioritet enn ID-kontroll i arbeidet.

Vurdering av nåsituasjonen for ID-forvaltningen

Sektorprinsippet ligger til grunn for fordeling av ansvar og oppgaver innenfor ID-forvaltningen. Mange aktører er involvert i ID-arbeidet, men få har ID som sin kjerneaktivitet. ID-arbeidet er i stor grad integrert i sektorenes ansvarsområde og saksbehandling. Det er imidlertid utstrakt behov for koordinering, da ID-relaterte problemstillinger ofte er tverrsektorielle. Leverandøren erfarer at bevisstheten rundt slike problemstillinger har økt, og det finnes eksempler på vellykket omstilling på tvers av departementsområder. Moderniseringen av Folkeregistret og ID-porten er slike eksempler. På tross av dette, kjennetegnes likevel deler av ID-forvaltningen av lav gjennomføringsevne. Prosjektet nye pass- og nasjonale ID-kort, et stort og viktig ID-relatert prosjekt som også påvirker mange andre deler og prosesser i ID-forvaltningen, har møtt gjentatte forsinkelser og utsettelser. Dette påvirker fremdriften og måloppnåelsen på ID-området isolert og som helhet. Dagens ID-forvaltningen har ikke én eier eller én aktør som arbeider som premissgiver. Konsekvensen av fragmentering og lav grad av **strategisk styring** er at ingen i tilstrekkelig grad har tatt ansvar for å gi helhetlige føringer eller ta helhetlige prinsipielle beslutninger. Helhetlige vurderinger med tanke på brukervennlighet, kvalitet og sikkerhet og ressursbruk blir i mindre grad ivaretatt i dagens styringsmodell. Videre er uklar oppgavefordeling og et stort antall register med begrensede delingsmuligheter, til hinder for effektiv saksbehandling og samarbeid.

Reguleringen av ID-forvaltningen er fragmentert. Det finnes ikke ett felles sektorovergripende **regelverk** som regulerer hele ID-området, og hva som skal anses som gyldig legitimasjon er ikke entydig definert. I stedet er det et relativt stort antall regelverk som hver for seg regulerer deler av, men som likevel samlet sett dekker hele ID-forvaltningen. Utover bestemmelser om deling av data mellom ulike aktører og på tvers av sektorer, er samhandling mellom de ulike aktørene i liten grad regulert.

Befolkningen har høy grad av tillit til arbeid utført av det offentlige, dette gjelder også ID-relatert arbeid. **Brukervennligheten** i ID-forvaltningen er likevel svakt dokumentert samlet sett. Flere ulike aktører utsteder ID-bevis som i dag oppfattes som gyldige, noe som medfører fleksibilitet for brukeren i situasjoner der det stilles krav om

fremvisning av fysisk legitimasjon. Denne fleksibiliteten bidrar imidlertid til svakere sikkerhet og økt ID-relatert misbruk. Utover pass har i dag brukere få gode alternativer til sikker fysisk legitimering. Dagens regelverk medfører for bruker i underkant av 30 oppmøter for utstedelse og fornyelse av pass, førerkort og bankkort med bilde i et livsløp. Avhengig av fremtidig gyldighet for pass vil nye regelverk for pass og nasjonalt ID-kort medføre 40 til 46 oppmøter. Leverandøren vurderer de samlede oppmøtekravene, spesielt for fysiske ID-bevis, som høye. Dagens private eID med autentisering gjennom ID-porten er i stor grad velfungerende og utbredt, samt bidrar til å redusere kostnader og tidsbruk sett fra et brukerperspektiv.

Økt fokus på ID-relaterte problemstillinger og oppbygning av kompetansemiljøer har hatt positiv effekt på **kvalitet og sikkerhet** i ID-forvaltningen. Likevel er det i kartleggingen identifisert flere sikkerhetsutfordringer som åpner for at borgere kan tilegne seg og operere med falske identiteter. Dette gjelder blant annet prosessen med rekvirering og tildeling av d-nummer som utføres av mange aktører med ulike rutiner. Videre er det i dag mulig for en borger å tilegne seg flere identitetsnummer i Folkeregistret og kunne operere med flere identiteter. Varierende kompetanse, innad og på tvers av virksomheter, tilknyttet utstedelse, fornyelse og tap av ID-bevis som betraktes som gyldige, samt svak ID-kontroll i forbindelse med utstedelse av eID gir også sikkerhetsutfordringer. Videre er det en risiko at ID-bevis betraktes som gyldige av tjenesteeiere uavhengig av formålet ID-beviset var utstedt til. Samfunnsmessige konsekvenser av feil og misbruk i ID-forvaltningen er i varierende grad dokumentert og kvantifisert. Leverandøren har anskueliggjort at konsekvensene er betydelig høyere enn reelt dokumenterte feil og misbruk. Pågående initiativ som modernisering av Folkeregisteret og utrulling av nye pass og nasjonalt ID-kort vil adressere enkelte av disse sikkerhetsutfordringene. Dagens planer for opptak, lagring og bruk av biometri for de ulike brukergruppene vil også kunne bidra til økt sikkerhet i ID-forvaltningen.

Samlet **ressursbruk** i ID-forvaltningen anslås til i underkant av 1,5 mrd. kroner og i underkant av 1 200 årsverk i 2018. Aktørenes bevissthet knyttet til ressursbruk for ID-relatert arbeid vurderes som lav. Det er videre krevende å vurdere ressurseffektiviteten samlet for ID-forvaltningen, når det ikke er definert entydige mål for verken brukervennlighet, sikkerhet eller ressursbruk. Motstridende indikasjoner på utvikling i ressurseffektivitet innen ulike saksområder og manglende enhetlig styring gjør det også utfordrende å vurdere utviklingen i ressurseffektivitet over tid.

Fragmentert styring, regulering og lite enhetlig dokumentasjon om målområdene sikkerhet, brukervennlighet og ressursbruk må ikke nødvendigvis isolert sett betraktes som en utfordring. Leverandøren vurderer at dagens styring er en rotårsak for den svake styringsinformasjonen innen målområdene. Selv om hver enkelt aktør kan oppleve at det gjøres tilstrekkelige tiltak for å nå egne mål, gir summen av tiltak og en manglende helhetlig tilnærming ikke tilstrekkelig gode resultater for sikkerhet, brukervennlighet og ressursbruk på overordnet nivå. Hver enkelt del av ID-forvaltningen vektlegger primært egne behov og har i mindre grad insentiver, ressurser eller prioriterer å ivareta helhetlige behov for ID-forvaltningen. Vurderingene av nåsituasjonen slik beskrevet over tydeliggjør behov for forbedring innen målområdene. Nåsituasjonsvurderingene viser videre at dagens system og planlagte tiltak ikke sikrer det grunnleggende behovet både forvaltningen og individet har for å etablere en sikker kobling mellom fysisk person og identitet i Norge.

Anbefalinger

Med utgangspunkt i oppdragets mandat, analyser og vurderinger har leverandøren utarbeidet et sett med anbefalinger med mål om økt sikkerhet, brukervennlighet og ressurseffektivitet. Gitt innretningen av områdegjennomgangen er anbefalingene på et nivå hvor det vil være behov for ytterligere detaljering og konsekvensutredning før de

kan implementeres. Flere av anbefalingene er videre av prinsipiell karakter og dels avhengig av hverandre. Enkelte av anbefalingene kan implementeres separat, men gir høyest effekt om de implementeres samlet.

Utarbeide strategi for ID-forvaltningen forankret i regjeringen

Leverandøren anbefaler at én statsråd får et overordnet ansvar for å etablere en felles strategi for ID-forvaltningen som forankres i regjeringen. Som del av strategiarbeidet bør det etableres et kunnskapsgrunnlag som omfatter samfunnsmessige kostnader og konsekvenser knyttet til ID-kriminalitet. Formålet med strategien vil være å prioritere og balansere de ulike hensynene for å realisere en mer brukervennlig, sikker og ressurseffektiv ID-forvaltning. Forankring i regjeringen bidrar til mer målrettet og samordnet ressursinnsats.

Strategien bør definere langsiktig retning, mål og styringsparametere for ID-forvaltningen, samt tiltak for å oppnå disse. Nedenfor følger leverandørens skisse til mål basert på visjon utarbeidet av den tverretatlige koordineringsgruppen for identitetsforvaltning (KoID):

> *Visjon: Én person, én identitet i Norge*
>
> *Hovedmål: Kostnadseffektiv ID-forvaltning som tilrettelegger for et enklere og tryggere samfunn*
>
> *Delmål:*
> - *Høy tillit til og trygghet i ID-relaterte aktiviteter*
> - *Enkel, brukervennlig og tidsbesparende utstedelse og bruk av fysiske og elektroniske ID-bevis for alle*
> - *Offentlige tjenester, ytelser og plikter gis til rett person*
> - *Effektiv rollefordeling og ressursbruk*

Øvrige anbefalinger bygger på skissen til mål over. Eksisterende tiltak og planer, anbefalinger fra områdegjennomgangen, samt eventuelle nye tiltak vil samlet være viktige delelementer i strategien. Strategien bør bidra til å prioritere og balansere de ulike hensyn for å realisere en mer brukervennlig, sikker og ressurseffektiv ID-forvaltning. Berørte departementer utarbeider strategien i fellesskap.

Tydeliggjøre at norsk pass og nasjonalt ID-kort er gyldige fysiske ID-bevis, samt stille krav til disse for tilgang til offentlige tjenester og ytelser

Leverandøren anbefaler at det tydeliggjøres i regelverket at norsk pass og nasjonalt ID-kort er de gyldige fysiske ID-bevisene i Norge. Det vil da bli allment kjent hvilke ID-bevis man kan ha tillit til og skal betrakte som gyldige. Dette innebærer blant annet at førerkort og bankkort med bilde ikke vil være ansett som gyldig legitimasjon annet enn for sine formål som henholdsvis førerrettsbevis og betalingsmiddel.

Leverandøren anbefaler at nasjonalt ID-kort utstedes til norske statsborgere, samt utenlandske borgere med tilknytning til Norge (herunder både EØS-borgere og tredjelandsborgere). Leverandøren anbefaler videre at det stilles krav til alle brukergrupper om fremvisning av enten norsk pass eller nasjonalt ID-kort for tilgang til sentrale tjenester og ytelser der det kreves fysisk legitimasjon. Anbefalingen medfører at hver enkelt tjenesteeier ikke gis anledning til å selv definere hva som skal være gyldig legitimasjon for tilgang til tjenester eller opprettelse av ulike rettighetsbevis. Som del av implementeringen bør det finnes løsninger for enkelte utsatte brukergrupper, brukere som har utfordringer med å godtgjøre sin identitet, samt borgere som har tilknytning til Norge men oppholder seg i utlandet. Hvilke

tjenester og ytelser med pålagt oppmøte eller fysisk legitimasjon som bør omfattes av et krav om norsk pass eller nasjonalt ID-kort anbefales også detaljert nærmere. Leverandøren understreker at anbefalingen ikke innebærer en generell legitimasjonsplikt i Norge. Digital tilgang til tjenester og ytelser vil fortsatt foretas med eID, men flere forhold ved eID må avklares slik beskrevet i anbefalingen under.

Styrke arbeidet med eID

Leverandøren anbefaler implementering av nasjonal eID tilknyttet det nasjonale ID-kortet som et supplement til eksisterende private eID-er i markedet, men med enkelte tilpasninger basert på nærmere utredninger. Leverandøren anbefaler videre at det utredes nærmere hvordan ID-kontrollen ved pass- og ID-kontor kan legges til grunn for utstedelse av norske private eID-er. I tillegg anbefales det å utrede ytterligere hvordan det ved bruk av norske private eID-er regelmessig kan sendes en spørring til og kontrolleres mot Folkeregisteret om brukeren av eID-en har status «unik». Dersom dette ikke lar seg implementere anbefales det at et krav om nasjonal eID vurderes for autentisering til offentlige digitale tjenester og ytelser. Det anbefales videre at det utredes nærmere hvorvidt vederlagsmodellen til nasjonalt ID-kort med eID bør endres fra å være gratis i bruk for alle tjenesteeiere til å innføre en transaksjonskostnad som belastes tjenesteeiere ved autentisering til digitale tjenester.

Registrere «unike» identiteter gjennom bedre opptak, lagring og søk i ansikts- og fingeravtrykksbiometri

For å kunne oppnå visjonen *en person, en identitet i Norge* er det avgjørende at et identitetsnummer kan kontrolleres for «unik». For å kunne gjennomføre denne kontrollen og sikre at en person *låses* til identitetsnummeret kreves det opptak, lagring og søk i minst en av biometriformene. Med mål om høyere sikkerhet og kvalitet i ID-forvaltningen, anbefaler leverandøren at alle brukere med tilknytning til Norge, både norske og utenlandske borgere, avlegger biometri i biometriregistrene. Leverandørens anbefaling støtter opp om arbeidet med knytning av biometri mellom Folkeregisteret, utlendingsregisteret og pass- og ID-kortregisteret og vurdering av de rettslige rammene for lagring av fingeravtrykk i pass- og ID-kortregistrene.

For å dekke gapet mellom dagens andel av befolkningen som har avlagt biometri og anbefalingen om at alle norske statsborgere og utenlandske borgere med tilknytning til Norge skal avlegge biometri, anbefales det at det stilles krav om pass eller nasjonalt ID-kort for å få tilgang til sentrale tjenester og ytelser der det kreves fysisk legitimasjon (jf. anbefalingen over). Biometrien opptas som en del av prosessen med utstedelse av pass og ID-kort.

Leverandøren anbefaler i tillegg at det også opptas fingeravtrykk for alle brukergrupper, og at det tillates lagring av begge biometriformer i biometriregistrene, slik at disse blir tilgjengelige for en-til-mange søk.

På sikt bør det vurderes hvorvidt bruker selv kan være med å styre hva biometrien kan benyttes til, utover det opprinnelige formålet biometrien ble tatt for. Brukerstyrt deling av biometri kan benyttes til å forenkle identifisering av personen for utvalgte tjenester i det offentlige. Dette kan bidra til å gjøre forvaltningen mer brukervennlig og effektiv.

Krav om «kontrollert» og på sikt «unik» identitet for å motta offentlige tjenester og ytelser

Leverandøren anbefaler at det skal ligge en kontrollert identitet til grunn for en større andel av Folkeregisterets identitetsnummer enn i dag. En viktig forutsetning for å oppnå dette er at det stilles krav om gjennomført ID-kontroll av identitetsnummer, som vil gi

identitetsnummeret status «kontrollert», for utbetaling av offentlige ytelser eller tilgang på bestemte tjenester. Dette vil være tilsvarende praksisen man i dag har for tilgang på skattekort og vil sikre mer enhetlig behandling av statens inntekter og viktigste kostnader. På lengre sikt anbefaler leverandøren at status «unik» kan erstatte krav om status «kontrollert», men dette vil først kunne innføres når anbefalingen om at norsk pass og nasjonalt ID-kort skal være eneste gyldige fysiske ID-bevis er implementert.

Leverandøren anbefaler at krav om «kontrollert» identitetsnummer i første omgang skal gjelde alle personer som oppholder seg i Norge. For personer som oppholder seg i utlandet anbefaler leverandøren at det gjøres en strukturert gjennomgang av eksisterende aktive d-nummer for å øke andelen «kontrollert» i Folkeregisteret.

I dag er det elleve rekvirenter med store forskjeller i antall rekvirerte d-nummer og rutiner for dette. Leverandøren anbefaler at antall rekvirenter reduseres betydelig fra dagens nivå.

Redusere brukers behov for fysiske oppmøter gjennom å tilrettelegge for økt deling av data og gjenbruk av ID-kontroll ved ett skrankepunkt

Leverandøren anbefaler at det legges til rette for at personopplysninger som opptas og ID-kontrollen som gjennomføres i forbindelse med utstedelse pass og nasjonale ID-kort kan benyttes ved utstedelse og fornyelse av andre ID-bevis og til andre definerte formål. Et viktig virkemiddel vil være at ID-kontroll og opptak av personopplysninger i større grad gjøres ved ett skrankepunkt.

Det anbefales at det tilrettelegges for økt deling av ansiktsfoto og signatur, noe som vil ha særlig stor innvirkning ved anvendelse for fornyelse av norsk førerkort. Statens vegvesen vil eksempelvis gis nødvendig tilgang til ansiktsfoto og signatur som opptas og lagres i forbindelse med utstedelse av norsk pass og nasjonalt ID-kort. En slik løsning vil i praksis muliggjøre at fornyelsen av førerkort i sin helhet kan foregå digitalt, uten behov for oppmøte. Det anbefales videre at det gjennomføres en separat vurdering av hvilke offentlige og private aktører som bør få tilgang til ansiktsfoto og signatur. Særlig anser leverandøren det som hensiktsmessig at banker som utsteder av bankkort med bilde får tilgang.

Leverandøren anbefaler at det utredes nærmere hvordan ID-kontrollen som gjennomføres ved et skrankepunkt for utstedelse og fornyelse av pass og nasjonalt ID-kort kan benyttes som grunnlag for at brukere kan få utstedt eID fra private tilbydere.

Det er også leverandørens anbefaling at oppmøtekrav som stilles til EØS-borgere i større grad samkjøres ved ett skrankepunkt. Leverandøren anbefaler spesielt at registreringen etter ankomst til Norge, etablering av identitetsnummer, etablering av skattekort, samt tilhørende ID-kontroll gjennomføres med ett oppmøte. Tilsvarende gjennomføres etablering av oppholdskort og etablering av identitetsnummer med ett oppmøte i samme skrankepunkt for søkere av oppholdstillatelse.

Det planlegges for at gyldighetstiden for nasjonalt ID-kort settes til fem år og nye pass settes til enten fem år eller at dagens gyldighetstid på ti år videreføres. Leverandøren mener at mange av sikkerhetsbehovene i pass og ID-kort potensielt kan ivaretas ved fornyelse uten behov for fysisk oppmøte, spesielt ved at fysisk oppmøte for å oppdatere ansiktsfoto og fingeravtrykk gjennomføres sjeldnere enn hvert femte år. Med sentrallagring av fingeravtrykk ser leverandøren et potensial for å kutte 13 fysiske oppmøter. Leverandøren anbefaler at det utredes nærmere i hvilken grad fornyelse av pass og nasjonalt ID-kort kan gjennomføres uten fysisk oppmøte.

Sikre helhetlig styring og tydeliggjøre ansvar for ID-forvaltningen gjennom å nærmere utrede eierskap og etablering av en ID-etat (eventuelt ID-direktorat)

Leverandøren anbefaler å gi én statsråd, ett departement og én etat (eventuelt direktorat) et helhetlig ansvar for ID-forvaltningen. ID-forvaltningen er et tverrsektorielt politikk- og saksområde og ansvaret kan ligge i flere departementer hvor vektlegging av sikkerhet, brukervennlighet og ressursbruk vil være ulik.

Leverandøren har i sin vurdering av ansvarlig departement vektlagt forutsetningene for å sikre en helhetlig styring, relevant oppgaveportefølje, gjennomføringsevne, førstelinje, samt grensesnitt til departementets øvrige politikkområder. Disse hensyn kan hver for seg trekke i retning av ulike departementer.

Leverandøren anbefaler å gi Justis- og innvandringsministeren et helhetlig ansvar for ID-forvaltningen. Det formelle forvaltningsansvaret for utvalgte ID-relaterte lover og regelverk legges til JD. JD får et tydelig mandat og konkrete virkemidler til å ta en premissgiver- og samordningsrolle for helheten i ID-forvaltningen, men hvor hvert departement fortsatt er ansvarlig for egen sektors arbeid. Rollen vil være knyttet til operasjonalisering av regjeringens politikk innen ID, samt oppfølging av fastsatte mål og resultatkrav.

Det er leverandørens forståelse at ingen av departementene i dagens ID-forvaltning vurderer det som hensiktsmessig at deres underliggende virksomheter tar et utvidet ansvar innen ID. Dette begrunnes med at ID ligger utenfor underliggende virksomheters kjerneområder.

Anbefalingen innebærer videre at det utredes å etablere en ny etat som vil være et landsdekkende myndighetsorgan underlagt JD. Myndighetsorganet kan potensielt organiseres som et direktorat avhengig av valgt tilnærming til førstelinje slik nærmere beskrevet under, men vil i denne anbefalingen omtales som en etat. En eventuell etat vil være premissgiver for ID-forvaltningen og ha en samordningsrolle på tvers av ID-prosessen, herunder ansvar for både fysisk ID og eID. Etaten vil ha ansvar for ID-relaterte oppgaver, prosesser og systemer i tilknytning til registering av personopplysninger og utstedelse av ID-bevis med tilhørende ID-kontroll, mens oppgaver som relaterer seg til fastsettelse av identitet og ID-kontroll i etterkant av utstedelse vil ligge hos andre aktører.

Anbefalingen innebærer å benytte allerede eksisterende infrastruktur i form av politiets førstelinje ved at den nye etaten for ID overtar eller leier lokaler og teknisk utstyr fra politiet. Ansatte i politiets førstelinje som arbeider med ID-relaterte oppgaver, samt ansatte som arbeider med ID-relaterte oppgaver på skattekontorene, overføres formelt til den nye etaten. Ny etat vil ha en andrelinje og tredjelinje på lik linje med andre etater, men det vil være behov for en separat gjennomgang av faglinjene for å sikre en felles forståelse av avhengigheter og hensiktsmessig arbeidsdeling.

En beslutning om å gi et departement et helhetlig ansvar og etablere en ny etat er strategisk viktig. Anbefalingen er et viktig virkemiddel for å sikre mer enhetlig styring og profesjonalisering av ID-relatert kompetanse i et spesialisert fagmiljø. Anbefalingen må utredes ytterligere med vekt på kost-/nytte-effekter. Leverandøren anbefaler at dette arbeidet ledes av FIN og gjennomføres i samråd med JD. Parallelt må ansvar og oppgaver relatert til ID tydeliggjøres i justissektoren med mål om forenkling og ressurseffektivisering. Dette er i tillegg nødvendige, forberedende aktiviteter i forkant av en eventuell etablering av et nytt myndighetsorgan.

Gjennomføringsplan

Leverandørens anbefalinger er delvis avhengige av hverandre, mens enkelte kan implementeres på separat basis. Det er spesielt anbefalingen om å *Tydeliggjøre at norsk pass og nasjonalt ID-kort er gyldige fysiske ID-bevis, samt stille krav til disse for tilgang til offentlige tjenester og ytelser* som er tett knyttet til gjennomføringen av de øvrige anbefalingene. I tillegg er nevnte anbefaling avhengig av at anbefalingen om å *Styrke arbeidet med eID* gjennomføres.

Leverandøren vurderer endringsbehovet i ID-forvaltningen som stort og anbefaler at momentet som er skapt utnyttes for å sikre handling. Som tidligere nevnt vil det for alle anbefalingene, med unntak av den første som omhandler strategiutvikling, være behov for ytterligere detaljering og konsekvensutredning før de kan implementeres.

Arbeidet med ytterligere detaljering og konsekvensutredning av utvalgte tema anbefales igangsatt umiddelbart. Strategiutviklingsarbeidet bør også starte opp innen starten av 2020. De øvrige anbefalingene vil i ulik grad være avhengig av arbeidet med ytterligere utredning og foreslås videre gjennomført når dette foreligger.

Gevinster

Samlet sett vil anbefalingene bidra til økt sikkerhet og økt brukervennlighet, samt legge grunnlag for økt ressurseffektivitet. Anbefalingen om å tydeliggjøre at pass og nasjonalt ID-kort er gyldige fysiske ID-bevis med tilhørende krav til om disse for tilgang til sentrale offentlige tjenester og ytelser, anbefalingen om bedre opptak, lagring og søk i biometri, samt anbefalingen om krav om «kontrollerte» og på sikt «unike» identitetsnummer vil alle være vesentlige for å styrke sikkerheten. Anbefalingen om å redusere behov for oppmøter gjennom å tilrettelegge for økt deling av data og gjenbruk av ID-kontroll har meget positive effekter på brukervennlighet og redusert ressursbruk.

Ettersom sikkerheten og brukervennligheten ved dagens ID-forvaltning er svakt dokumentert og siden det anbefales ytterligere detaljering og konsekvensutredning av anbefalingene er ikke alle gevinster kvantifisert. Et overordnet estimat på årlige effekter for brukere og forvaltningen som følge av leverandørens anbefalinger gir 580 – 670 mill. kroner i positiv nytte per år. Estimatet for gevinster bør videreutvikles. Estimatet omfatter ikke kostnadene ved implementering av anbefalingene.

Leseveiledning

Anbefalingene som presenteres i del 4 må leses i sammenheng med leverandørens helhetlige vurderinger og drøfting av alternativ i del 3. Innhold i del 3 bygger i stor grad på funn og vurderinger fra nåsituasjonsbeskrivelsen i del 2, samt definisjoner og avgrensninger i del 1.

Del 1: Bakgrunn

Del 1 beskriver bakgrunnen for områdegjennomgangen og inneholder introduksjon av mandat, struktur og fremgangsmåte (kapittel 1) og overordnet om ID-forvaltningen og avgrensninger (kapittel 2).

1 Introduksjon

I dette kapittelet beskrives prosjektets mandat (kapittel 1.1), struktur på nåsituasjon, vurderinger og anbefalinger (kapittel 1.2) og fremgangsmåte og datagrunnlag (kapittel 1.3).

1.1 Mandat

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. Områdegjennomgangen dekker det ID-relaterte arbeidet i de departementer med underliggende etater og virksomheter som har en rolle i forbindelse med fastsettelse av identitet, registrering av identitet, utstedelse av fysiske og elektroniske ID-bevis (eID) samt ID-kontroll.

Oppdraget er strukturert som én helhetlig leveranse og arbeidet er gjennomført i perioden fra april til september 2019. Leverandøren er Capgemini Invent med støtte fra advokatfirmaet BAHR AS. Med utgangspunkt i oppdragets mandat har leverandøren kartlagt og analysert dagens ID-forvaltning med både forvalters og brukers perspektiv, samt utarbeidet anbefalinger om eventuelle endringer innenfor ulike områder tilknyttet ID-forvaltningen. I tråd med oppdragets mandat er det redegjort for positive og negative virkninger av anbefalingene. Det er i tillegg konkretisert forslag til gjennomføringsplan. Gitt innretningen av områdegjennomgangen er anbefalingene på et nivå hvor det vil være behov for ytterligere detaljering og konsekvensutredning før de kan implementeres.

Områdegjennomgangen er gjennomført som et prosjekt i samarbeid mellom Finansdepartementet (FIN), Justis- og beredskapsdepartementet (JD), Samferdselsdepartementet (SD) og Kommunal- og moderniseringsdepartementet (KMD) med en prosjektgruppe og et prosjektstyre, begge bestående av representanter fra de fire departementene. I tillegg har en referansegruppe bestående av medlemmer fra Nærings- og fiskeridepartementet (NFD), Utenriksdepartementet (UD), Kunnskapsdepartementet (KD), Arbeids- og sosialdepartementet (ASD) og Helse- og omsorgsdepartementet (HOD) deltatt i prosjektet. Leverandøren har gjennomført ti møter med prosjektgruppen, samt deltatt i seks prosjektstyremøter og ett referansegruppemøte[2]. Medlemmene i prosjektet har deltatt i diskusjoner om vurderinger og anbefalinger, men rapporten inneholder leverandørens egne vurderinger og anbefalinger.

[2] Under arbeidet ble det kun avholdt ett oppstartsmøte med referansegruppen

1.2 Struktur på nåsituasjon, vurderinger og anbefalinger

Rapporten for områdegjennomgangen er strukturert i fire deler, som fremstilt i figuren nedenfor.

Med utgangspunkt i mandatet har leverandøren utarbeidet en kartlegging av nåsituasjonen med tilhørende vurdering av fem ulike tema i del 2.

- Kapittel 3 om styring og struktur i ID-forvaltningen dekker aktørbildet, saksgang, registre og saksbehandlingssystemer, samt styring og struktur hos utenlandske aktører

- Kapittel 4 om gjeldende lover og regelverk i ID-forvaltningen dekker ulike regelverk som har betydning for ID-forvaltningen, med særlig henblikk på regelverkenes formål og hvilke muligheter de gir for samhandling mellom ulike aktører

- Kapittel 5 om brukerreiser og brukervennlighet dekker brukertilfredshet, hvilke ID-bevis som kreves fremlagt av bruker for å få tilgang til sentrale offentlige tjenester og ytelser, hvilke ID-bevis som kreves for utstedelse av andre ID-bevis, samt overordnet tidsbruk, direkte kostnad og antall treffpunkt som påløper for bruker

- Kapittel 6 om kvalitet og sikkerhet i ID-forvaltningen dekker prosessene relatert til tildeling av fødselsnummer, rekvirering og tildeling av d-nummer og utstedelse/fornyelse/tap av fysiske og elektroniske ID-bevis. Videre kartlegges registrering av biometri og samfunnsmessige konsekvenser relatert til feil og misbruk

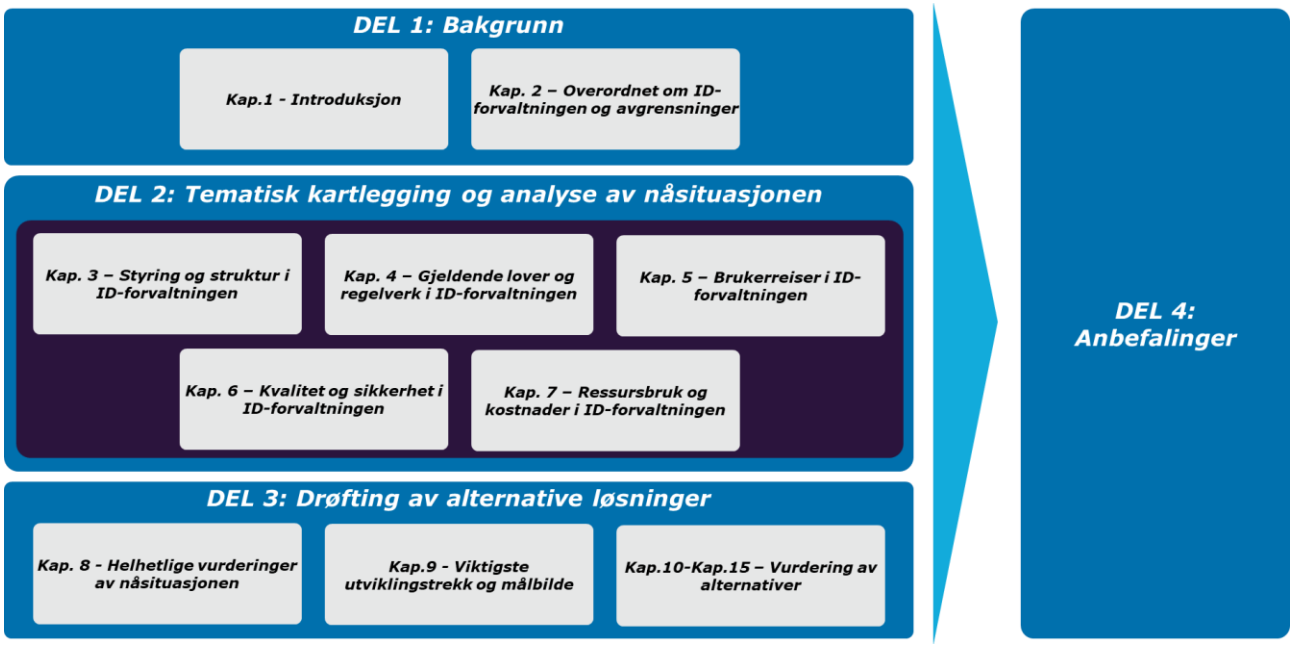
- Til slutt beskriver og vurderer kapittel 7, om ressursbruk og kostnader i ID-forvaltningen, ressursbruken i de ulike departement samlet sett og hos de ulike aktørene i ID-forvaltningen, utvikling over tid, samt analyser og vurderinger av kostnadseffektivitet på tvers av departementer og underliggende aktører i ID-forvaltningen

I del 3 drøftes alternative løsninger for ID-forvaltningen. I kapittel 8 oppsummeres helhetlige vurderinger av nåsituasjonen med utgangspunkt i nåsituasjonen og vurderingene dekket i kapittel 2-7.

- Kapittel 9 dekker viktigste utviklingstrekk i ID-forvaltningen, samt skisse til mål for ID-forvaltningen

- I kapittel 10-15 drøftes konkrete alternativ for ID-forvaltningen for seks ulike områder: fysiske ID-bevis og nasjonalt ID-kort, eID, identitetsnummer, biometri, behov for fysiske oppmøter og styring og struktur. Områdene som drøftes i disse kapitlene er valgt med bakgrunn i identifiserte utfordringer skissert under helhetlige vurderinger i kapittel 8, og hvor leverandøren har sett det nødvendig å dykke dypere ned i utfordringene og kartlegge alternativer til dagens praksis

Anbefalingene er gitt med utgangspunkt i leverandørens vurderinger, og dekkes i del 4.



Figur 1 Oppbygning av deler og kapitler i rapporten

1.3 Fremgangsmåte og datagrunnlag

I gjennomføringen av områdegjennomgangen har det blitt lagt til grunn en tre-stegs prosess med en tematisk kartlegging og analyse av nåsituasjonen, helhetlig vurdering av ID-forvaltningen og anbefalinger for forbedringer. Gitt kompleksiteten i problemstillingen, omfanget av interessenter og store mengder dokumentasjon har det vært viktig å benytte tilstrekkelig med tid og ressurser på første steg.

Leverandøren har definert fem analyseområder hvor det er gjennomført grundige analyser. Omfang og innretning av analysene er diskutert og gitt prioritet i prosjektgruppen, referansegruppen og prosjektstyret. Analyseområdene følger av kapitlene inkludert i del 2 som vist i figuren ovenfor.

Videre har det i gjennomføringen av både kvalitative og kvantitative analyser blitt benyttet et bredt spekter av datakilder. Et omfattende materiale av tidligere rapporter og andre dokumenter er benyttet som underlag. Leverandøren ønsker å påpeke at deler av dokumentasjonen som er mottatt og benyttet er unntatt offentlighet. Det vil ikke kildehenvises til disse direkte i rapporten. Det er videre gjennomført over 50 intervjuer og samtaler med relevante interessenter og aktører. Til sammen har leverandøren hatt dialog med omlag 110 personer fra prosjektgruppen, prosjektstyret, referansegruppen, relevante etater og virksomheter, private aktører, utenlandske aktører med flere. Dette er oppsummert i vedlegg 1, liste over intervjuobjekter).

Det ble i tillegg sendt ut to dataforespørsler til et utvalg aktører; én dataforespørsel om ressursbruk og brukerreise, samt en spørreundersøkelse knyttet til kvalitet, rutiner og retningslinjer for tre utvalgte prosesser i ID-forvaltningen (se vedlegg 2).

Helheten i ID-forvaltning er etter leverandørens vurdering i svært liten grad vurdert tidligere. For utvalgte aktører, saksområder eller ID-bevis finnes det et bredt spekter av rapporter og vurderinger, men disse tar som hovedregel utgangspunkt i den enkelte aktørs, saksområdes ellers ID-bevis sine behov. Videre er helheten av kvalitet og sikkerhet, ressursbruk og brukervennlighet i svært varierende grad dekket i tidligere gjennomført arbeid. For enkelte områder, som for ressursbruk og kostnader, eksisterer det ikke samlet datagrunnlag eller statistikk for ID-forvaltningen. I tillegg inngår ID-

relatert arbeid som del av andre arbeidsoppgaver hos de fleste aktører og data på ressursbruk og kostnader er dermed ikke direkte tilgjengelig i aktørenes rapportering.

For å svare ut oppdragets mandat har leverandøren derfor benyttet nevnte dataforespørsler for innhenting av data. Mottatt data er imidlertid delvis preget av å være estimater, da faktiske tall ikke er direkte tilgjengelig for de fleste aktørene. For enkelte analyser, slik som for ressursbruk i ID-forvaltningen, er tilnærming og datagrunnlag nærmere beskrevet i respektivt kapittel i del 2.

For utenlandske aktører er det hentet inn informasjon om ID-forvaltningen i Sverige, Danmark, Storbritannia og Latvia for ulike deler av de samme temaene som dekkes av del 2 (se vedlegg 3). Land ble valgt i samråd med prosjektgruppen, og med bakgrunn i relevans for ID-forvaltningen og grad av sammenligningsmuligheter med Norge. Informasjon om de ulike lands praksis er primært hentet fra offentlig tilgjengelig dokumentasjon og samtaler med utvalgte relevante fagpersoner i respektive land. Det har til dels vært utfordrende å innhente relevant informasjon grunnet manglende respons fra kontaktede personer og lite offentlig tilgjengelig dokumentasjon om relevante tema.

Som nevnt i kapittel 1.2 er det med bakgrunn i den tematiske kartleggingen i del 2 og den helhetlige vurderingen av ID-forvaltningen i del 3 beskrevet alternativer til dagens ID-forvaltning for seks ulike tema. Alternativene innenfor hvert tema er oppsummert og vurdert med «pluss-minusmetoden», en kvalitativ metode for å vurdere ikke-prissatte virkninger opp mot effektmål, der effektmålene er leverandørens forslag til alternativer og tiltak.[3] Hvert alternativ gis en konsekvens som er endringen sammenlignet med nåsituasjonen og vurderes ved hjelp av en skala basert på plusser og minuser. Skalaen strekker seg fra fire plusstegn som vil si at alternativet har meget stor positiv konsekvens, til fire minustegn som vil si at alternativet har meget stor negativ konsekvens. Betegnelsen «0» i midten av skalaen vil si at alternativet har ubetydelig/ingen konsekvens. Denne metoden er også brukt for å oppsummere gevinster av anbefalingene i kapittel 16.3.

Alternativene innenfor hvert tema er vurdert opp mot vurderingskriteriene som gjennomgående er benyttet i områdegjennomgangen, sikkerhet, ressursbruk og brukervennlighet. Vurderingene er gjort i et femårsperspektiv.

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

2 Overordnet om ID-forvaltningen og avgrensninger

I dette kapittelet gjennomgås overordnet informasjon om ID-forvaltningen i Norge og avgrensninger som ligger til grunn for del 2-4. Utover definisjoner gitt i innledningen i rapporten definerer kapittelet viktige begrep benyttet i rapporten. Det gis en beskrivelse av identitetsforvaltning (kapittel 2.1), Folkeregisteret og identitetsnummer (kapittel 2.2), ID-bevis og grunnidentitet (kapittel 2.3), prosess fra fastsetting av ID til ID-kontroll (kapittel 2.4), overordnet aktørbilde (kapittel 2.5), brukergrupper og brukerreiser (kapittel 2.6), relevant regelverk (kapittel 2.7), sakstyper og volum (kapittel 2.8), pågående arbeid tilknyttet ID-forvaltningen (kapittel 2.9), samt viktige avgrensninger (kapittel 2.10).

2.1 Identitetsforvaltning

Det eksisterer ingen enhetlig definisjon av begrepet identitetsforvaltning (ID-forvaltning), og det varierer derfor hva ulike aktører legger i begrepet. En vanlig definisjon, som benyttes hyppig internasjonalt, er at det er et bredt administrativt område som dekker det å identifisere personer innenfor et system (som for eksempel kan være et land, et datanettverk eller en organisasjon) og knytte disse til rettigheter og begrensinger til bruk av ressurser i systemet.[4] Leverandøren legger en tilsvarende definisjon til grunn og øvrige delkapitler redegjør nærmere hva dette betyr med tanke på et prosess-, aktør-, brukergruppe-, og regelverksperspektiv.

2.2 Folkeregisteret og identitetsnummer

Folkeregisteret er det sentrale personregisteret for Norge og danner grunnlaget for skattemanntallet, valgmanntallet og befolkningsstatistikken.[5] Folkeregisteret er en nasjonal felleskomponent[6] og er sådan en viktig del av den nasjonale infrastrukturen på personopplysningsområdet, da det inneholder og forvalter grunnleggende personopplysninger[7] om den enkelte person som er bosatt eller født i Norge eller har fått tildelt identitetsnummer[8]. For ID-forvaltningen danner registeret et robust fundament og både offentlige og private aktører benytter det i utstrakt grad som kilde til grunndata i ID-relatert arbeid.

I Norge brukes identitetsnummer i Folkeregisteret for å identifisere og holde oversikt over innbyggere.[9] En rekke offentlige og private virksomheter krever at man har et norsk identitetsnummer for å få tilgang til ulike tjenester. Det finnes to ulike typer identitetsnummer: fødselsnummer og d-nummer. Fødselsnummer tildeles alle som blir født i Norge, alle som bosetter seg i Norge (opphold over seks måneder) og norske statsborgere som er født eller bosatt i utlandet og trenger fødselsnummer for å få et norsk pass.

[4] Definisjonen er i samsvar med definisjoner brukt i OECD. Første gang brukt av JD i 2007
[5] Skatteetaten, «Dette er Folkeregisteret», u.å.
[6] KMD, «Hva er felleskomponenter?», 2014
[7] Her melder man også flytting, at man gifter seg eller dødsfall, endrer navn og bestiller attester
[8] Folkeregisterloven, § 2-1
[9] Skatteetaten, «Norsk identitetsnummer», u.å.

Hvis man ikke oppfyller vilkårene for å få tildelt et fødselsnummer, kan man få tildelt et d-nummer dersom man har begrunnet behov for det.[10] Det er d-nummerrekvirentene som definerer hva som regnes som begrunnet behov.[11]

2.3 ID-bevis og grunnidentitet

Det eksisterer ingen enhetlig definisjon på tvers av ID-forvaltningen som definerer et bevis som viser at en person har rett til en tjeneste eller som verifiserer at en person er den han/hun utgir seg for å være. Leverandøren viser til definisjonsliste tidligere i rapporten for valgt definisjon av ID-bevis og ID-dokument.

Som del av leverandørens kartlegging er det identifisert 38 ulike ID-bevis (ref. vedlegg 4). Det eksisterer ingen helhetlig oversikt som definerer hvilke norske ID-bevis som regnes som gyldige og dette varierer blant aktører og virksomheter. Tilsvarende er det verken helhetlig eller enhetlig definert på tvers av aktører hvilke utenlandske ID-bevis som anses som gyldige. På bakgrunn av dette, samt at ID-bevisene varierer i utbredelse og relevans, foretok leverandøren tidlig i prosessen en omfangsavgrensning av ID-bevis i samråd med prosjektgruppen. I tabellen nedenfor fremkommer de tolv ID-bevisene som danner grunnlaget for områdegjennomgangen. Leverandøren bemerker at oppholdskort i utgangspunktet ikke er et ID-bevis, men at det videre i rapporten vil inkluderes i oversikten over ID-bevis etter ønske fra JD, da det har mange av fellestrekkene til pass.

	ID-bevis	Utsteder
Fysiske ID-bevis		
1	Norsk pass	Politiet og utenriksstasjoner
2	Nasjonalt ID-kort[12]	Politiet[13]
3	Reisebevis for flyktninger	
4	Utlendingspass	
5	Oppholdskort (Schengen-standardisert)	
6	Norsk førerkort	Statens vegvesen
7	Norsk bankkort med bilde	Banker
8	Forsvarets ID-kort	Forsvaret
9	Norsk sjøfartsbok/Sjøfartskort	NAV (politiet fra 2020)
Elektroniske ID-bevis (eID)		
10	MinID	Difi
11	BankID	Banker
12	Buypass ID	Buypass AS

Tabell 1 Oversikt over ID-bevis

[10] Skatteetaten, «D-nummer», u.å.
[11] Man kan blant annet ha rett til et d-nummer dersom man er: a) skatte- eller avgiftspliktig til Norge; b) asylsøker eller person med gyldig oppholdstillatelse; c) omfattet av en ordning som forvaltes av NAV eller HELFO; d) rolleinnehaver i en juridisk enhet, for eksempel som styremedlem i et firma; eller e) rettighetshaver i grunnboken, for eksempel eier et hus
[12] Nasjonalt ID-kort vil etter nåværende plan utstedes fra 2020
[13] Utlendingsmyndighetene beslutter om utlendingspass og reisebevis for flyktninger skal utstedes

For eID ligger områdegjennomgangens fokus på eID-er som brukes i kontakt med det offentlige. Kapittel 2.8.2 beskriver bruken av eID i det offentlige, samt gjennomgår de ulike eID-ene som er tilgjengelige.

Felles for alle ID-bevisene er at de ikke er obligatoriske i seg selv, men at de kan kreves fra myndighetenes side dersom personen for eksempel ønsker å motta offentlige tjenester og ytelser eller gjennomføre borgeroppgaver som å stemme ved valg og betale skatt.

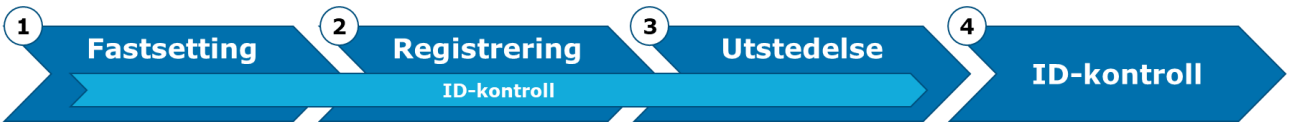
Norske myndigheters ID-forvaltning baserer seg på å registrere en grunnidentitet[14] for alle som har fått tildelt et norsk identitetsnummer i form av et fødselsnummer eller et d-nummer. En norsk grunnidentitet består av et identitetsnummer i kombinasjon med et sterkt fysisk ID-bevis, som fremstilt i figuren nedenfor.

Figur 2 Grunnidentitet

Hvilke ID-bevis som defineres som sterke er ikke regelverksforankret (nærmere beskrevet i kapittel 4.2.3). Kun pass og det kommende nasjonale ID-kortet oppfyller kravene som beskrevet i definisjonen av sterkt identitetsbevis og sterk identitetskontroll i definisjonslisten i begynnelsen av rapporten.[15] Dette har leverandøren valgt å ta utgangspunkt i.

2.4 Prosess fra fastsetting av ID til ID-kontroll

Leverandøren har valgt å beskrive prosessen i dagens ID-forvaltning med fire steg; identitetsfastsettelse, registrering av identitet, utstedelse av ID-bevis (både fysiske og elektroniske) og ID-kontroll som illustrert nedenfor. Stegene er ytterligere detaljert i tekst under.



Figur 3 Prosessen i dagens ID-forvaltning

Fastsetting: Førstegangsetablering av et individs identitet, ved fødsel av norske barn i Norge eller i utlandet og av tredjelandsborgere som ankommer Norge med ukjent identitet.

Registrering: Nedfellelse og lagring av individspesifikk informasjon (f.eks. biometri, identitetsnummer eller personopplysninger) i en database eller et register.

Utstedelse: Enhver handling fra utsteder som medfører produksjon av nytt ID-bevis. Dette kan gjelde førstegangsutstedelse av ID-bevis, fornyelse, utvidelse, duplikat, innbytte eller utskifting.

[14] SKD, «Forslag til visjon for nasjonal identitetsforvaltning», 2018
[15] Difi, «Sak 09-2017 Identitetsforvaltning», 2017

ID-kontroll: ID-kontroll er et vidt begrep som inngår i alle de fire fasene i prosessen. ID-kontroll som del av de tre første fasene defineres av leverandøren som manuell og/eller automatisk kontroll av om fremlagt ID-bevis er en autentisk representasjon av innehaver ved fastsettelse, registrering eller utstedelse av ID-bevis.

Etter de tre første stegene i prosessen, når fastsettelse, registrering og utstedelse er fullført, gjennomføres det videre en rekke ID-kontroller av en persons identitet i et livsløp, både av fysisk utstedte ID-bevis og ved hjelp av autentisering gjennom bruk av eID. Områdegjennomgangen har et helhetlig perspektiv på ID-forvaltning, men har i fjerde steg vektlagt følgende områder og kontrollaktiviteter:

- ID-kontroll for å bekjempe kriminalitet og ivareta sikkerhet
    - ID-kontroll i forbindelse med grensepasseringer og territorialkontroll
    - ID-kontroll i forbindelse med politiets øvrige oppgaveutførelse[16]
- ID-kontroll for å kunne motta tjenester og ytelser fra det offentlige
    - ID-kontroll i forbindelse med tjenester og ytelser fra NAV
    - ID-kontroll i forbindelse med tjenester utstedt av helsevesenet
    - ID-kontroll i forbindelse med tjenester fra det norske utdanningssystem (f.eks. fra Lånekassen)
- ID-kontroll for å få rettighet til og kunne gjennomføre borgeroppgaver
    - ID-kontroll i forbindelse med betaling av skatt
    - ID-kontroll i forbindelse med stemmegivning ved valg

I tillegg til kategoriene omtalt i de foregående punktene er ID-kontroll i forbindelse med tilgang til banktjenester vektlagt.

2.5 Overordnet aktørbilde

Myndighetsansvaret for ID-forvaltningen er delt mellom flere departementer med underliggende etater og virksomheter. Det er leverandørens forståelse at organiseringen er historisk betinget og har vært bygget på at de ulike aktørene har komparative fortrinn ved utførelse av ulike funksjoner og oppgaver. Som følge av dette er ID-relaterte aktiviteter en integrert del i berørte sektorers ansvarsområde og saksbehandling. Dette gjelder også for ID-bevis, ID-registre, lover og regelverk for ID og ID-kompetanse som hver for seg eller samlet bidrar til å ivareta sektorens behov eller dekke et bestemt formål. Som en konsekvens av dette foreligger ikke et definert formål eller målsetning for ID-forvaltningen.

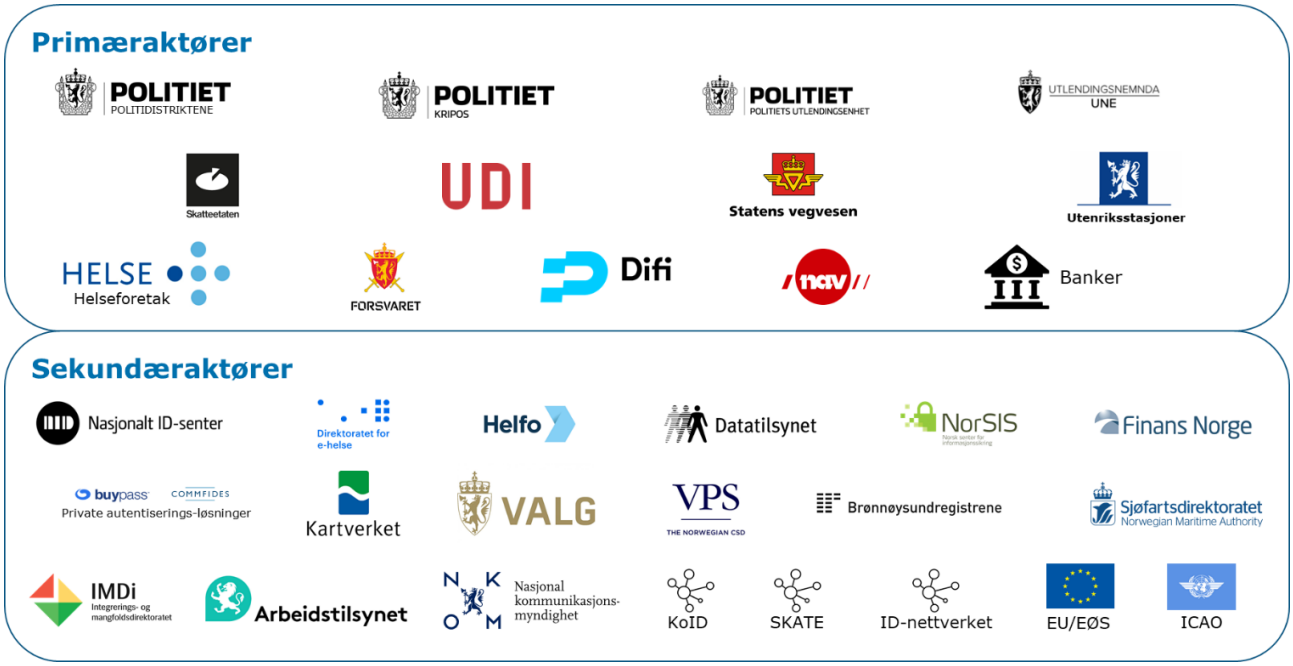
I totalbildet av aktører i ID-forvaltningen har leverandøren valgt å skille mellom primær- og sekundæraktører. Definisjonene er som følger:

[16] Politiets øvrige oppgaveutførelse innebærer blant annet å opprettholde alminnelig orden, forebygge og forhindre straffbare handlinger, beskytte borgere og deres lovlydige virksomhet, etterforske lovbrudd og trafikksikkerhetsarbeid

- Primæraktør: Aktøren arbeider med én eller flere av følgende aktiviteter: identitetsfastsettelse, registrering av identitet eller utstedelse av ID-bevis (ref. kapittel 2.4)

- Sekundæraktør: Aktøren arbeider ikke med overnevnte aktiviteter, men kun én eller flere av følgende aktiviteter: rekvirering d-nummer, tilrettelegging for ID-forvaltningen eller er en interessesammenslutning

Figuren nedenfor fremstiller aktører innen ID-forvaltningen fordelt på primær- og sekundæraktører. Aktørene er nærmere beskrevet i kapittel 3.1.1 relatert til deres arbeidsområder inn mot ID-forvaltningen.



Figur 4 Oversiktsbilde over primær- og sekundæraktører i ID-forvaltningen

Tabellen nedenfor oppsummerer primæraktørenes rolle opp mot de tre første fasene av prosessen i ID-forvaltningen. Alle aktørene vil i en eller annen form utøve ID-kontroll, enten i forbindelse med én eller flere av de tre første stegene i ID-prosessen eller i etterkant av at ID-bevis er utstedt.

Aktør	Fastsetting	Registrering	Utstedelse
Politidistrikter		X	X
Kripos	X	X	
Politiets utlendingsenhet	X	X	
Utlendingsnemnda	X	X	
Skatteetaten	(X)[17]	X	
Utlendingsdirektoratet	X	X	
Statens Vegvesen		X	X
Utenriksstasjoner		X	X
Helseforetak	X		
Difi			X
NAV		X	X
Banker		X	X
Forsvaret		X	X

Tabell 2 Primæraktørenes rolle opp mot de tre første fasene i prosessen i ID-forvaltningen

2.6 Brukergrupper og brukerreiser

Alle som oppholder seg eller ønsker å oppholde seg i Norge berøres av ID-forvaltningen. Utover norske statsborgere vil også en rekke utenlandske personer få innpass til Norge på bakgrunn av ulike formål, inkludert blant annet turistreiser, arbeidsinnvandring, asylsøkere, og flyktninger. I tillegg vil forvaltningen også omfatte alle med rettigheter til norske offentlige tjenester og ytelser, uavhengig om vedkommende befinner seg i Norge eller i utlandet. Behovet for, og kompleksiteten i å identifisere norske og utenlandske borgere vil være ulikt, og individenes forutsetninger for å identifisere seg vil også variere. Mange lover og regler reflekterer dette ved at det skilles på brukergrupper på bakgrunn av deres opprinnelsesland. Eksempelvis vil EØS-borgere omfattes av EU/EØS-lovgivning, mens saksgang og retningslinjer i UDI i visse tilfeller vil være ulikt avhengig av hvilket land brukeren kommer fra. Et tilsvarende skille gjøres også av mange tjenesteeiere i hvilke krav som stilles til fremvisning av legitimasjon. I lys av det foregående anser leverandøren det som hensiktsmessig å skille mellom enkelte brukergrupper i områdegjennomgangen. I samråd med prosjektgruppen har leverandøren lagt følgende brukergrupper til grunn:

1. **Norske statsborgere**: Barn med norsk mor eller far blir ved fødsel automatisk norske statsborgere. Barn som er under 18 år ved adopsjon av en norsk statsborger blir også automatisk norske statsborgere dersom vilkårene i adopsjonsloven er oppfylt. Personer over tolv år som har oppholdt seg til sammen syv år i landet de siste ti årene, og som fyller ulike krav og vilkår, har rett på statsborgerskap etter søknad. Kravene er noe annerledes for nordiske statsborgere og barn. Vilkårene for norsk statsborgerskap følger av kapittel 2-4 i Statsborgerloven.[18]

2. **EØS-borgere**: Statsborgere av land som omfattes av EØS-samarbeidet mellom EU og EFTA.

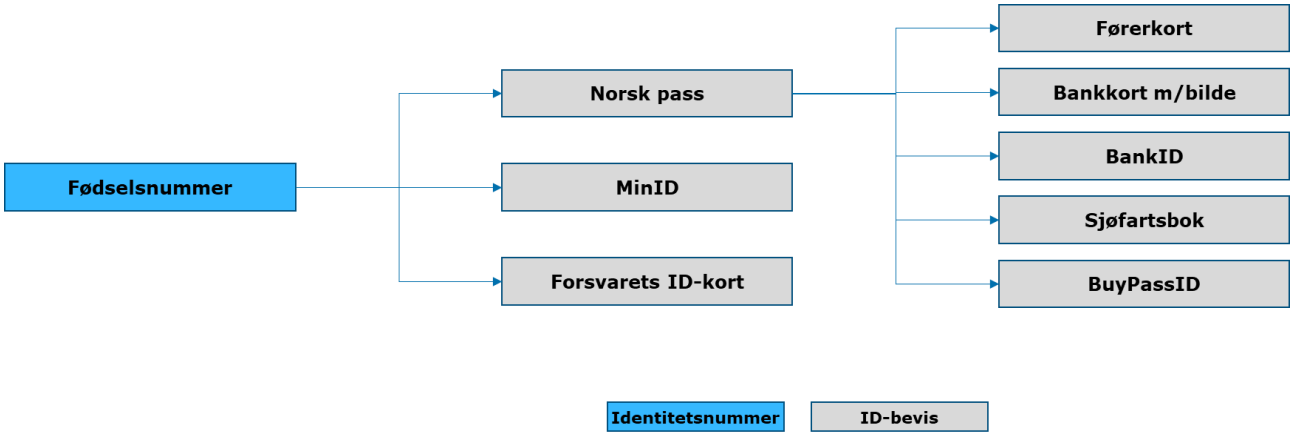
[17] Leverandøren opererer med at fastsettingen i praksis utføres av helseforetak eller utlendingsmyndighetene. Når folkeregistermyndigheten fatter vedtak om å tildele et identitetsnummer regner leverandøren dette som registrering i Folkeregisteret

[18] Lovdata, «Lov om norsk statsborgerskap (statsborgerloven) – Kapittel 2. Erverv av statsborgerskap ved fødsel og adopsjon», 2005

3. **Tredjelandsborgere**: Borgere i alle land, definert som enhver person som ikke er unionsborger i henhold til artikkel 20 nr. 1 i TEUV[19], og som ikke er borger av en stat som deltar i denne forordning i henhold til en avtale med Den europeiske union.[20]

De ulike brukergruppene vil i løpet av et livsløp anskaffe en rekke ID-bevis. Ulike utstedelseskrav fordrer at enkelte ID-bevis anskaffes før andre, noe som medfører at de ulike brukergruppene vil måtte anskaffe ID-bevis i en viss rekkefølge. Med bakgrunn i dette har leverandøren i det følgende skissert en forenklet oversikt for anskaffelse av ID-bevis for de ulike brukergruppene. Figurene som presenteres under er et forenklet hovedløp for anskaffelse av ID-bevis, en komplett oversikt over hvilke krav som stilles for utstedelse av ID-bevis presenteres i kapittel 5.1.3.

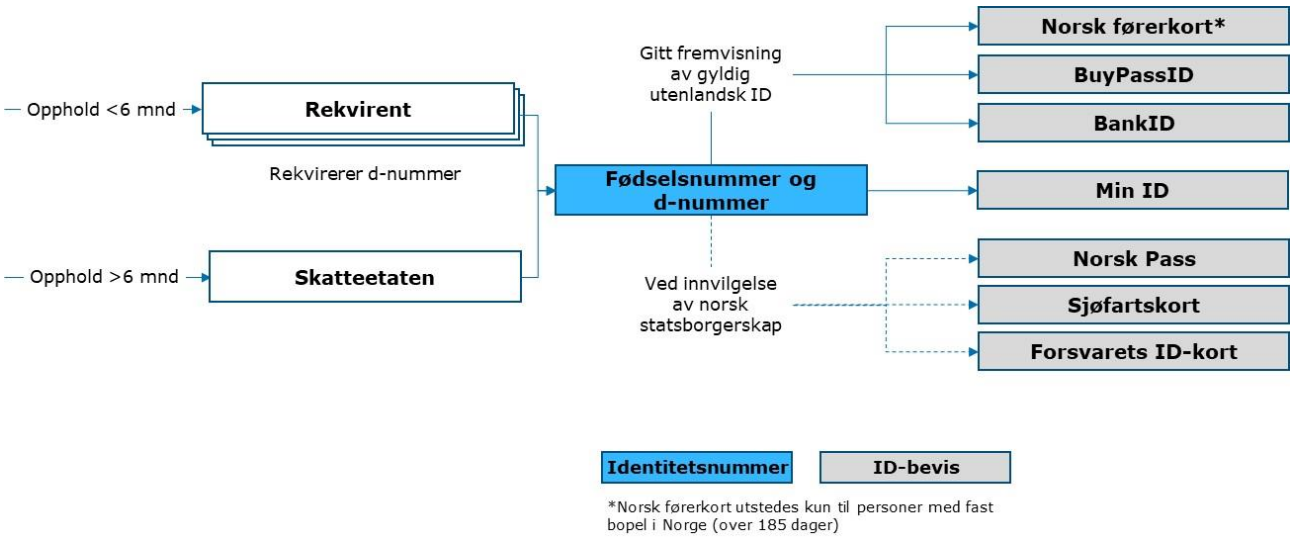
Figuren under viser en forenklet oversikt for anskaffelse av ID-bevis for norske borgere. Med utgangspunkt i tildelt fødselsnummer og gjeldende regelverk er det mulig for brukeren å få utstedt norsk pass, MinID og Forvarets ID-kort. Videre vil det norske passet muliggjøre anskaffelse av førerkort, bankkort med bilde, BankID, Sjøfartsbok eller BuyPass.



Figur 5 Forenklet oversikt for anskaffelse av ulike ID-bevis for norske borgere

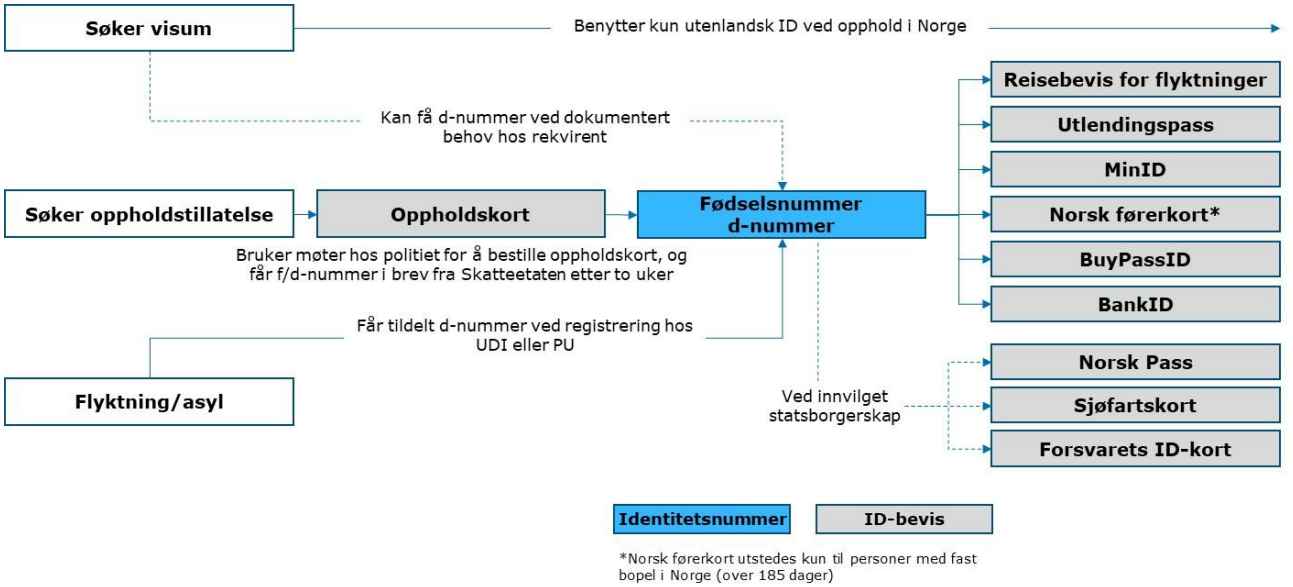
Under er en forenklet oversikt for anskaffelse av ID-bevis for EØS-borgere. Avhengig av om EØS-borgeren skal oppholde seg i Norge under eller over seks måneder, vil det bli tildelt henholdsvis et d-nummer eller fødselsnummer. D-nummeret og fødselsnummeret gir i utgangspunktet tilgang til de samme ID-bevisene, men dersom EØS-borgeren får innvilget statsborgerskap etter søknad åpner dette muligheter for anskaffelse av blant annet norsk pass slik vist i figuren under.

[19] Regjeringen.no, «Traktaten om den Europeiske Unions virkemåte (TEUV)», 1957
[20] Europaparlamentet og Rådet, «Dublin III-forordning, Kapittel I – Artikkel 2», 2013



Figur 6 Forenklet oversikt for anskaffelse av ID-bevis for EØS-borgere

Figuren under viser en forenklet oversikt for anskaffelse av ID-bevis for tredjelandsborgere. Etter å ha fått tildelt fødselsnummer eller d-nummer har tredjelandsborgere mulighet til å anskaffe flere ulike ID-bevis, avhengig av om de har fått innvilget opphold eller er i påvente av det. På samme måte som for EØS-borgere kan tredjelandsborgere gå til anskaffelse av norsk pass dersom søknad om statsborgerskap innvilges.



Figur 7 Forenklet oversikt for anskaffelse av ID-bevis for tredjelandsborgere

2.7 Relevant regelverk

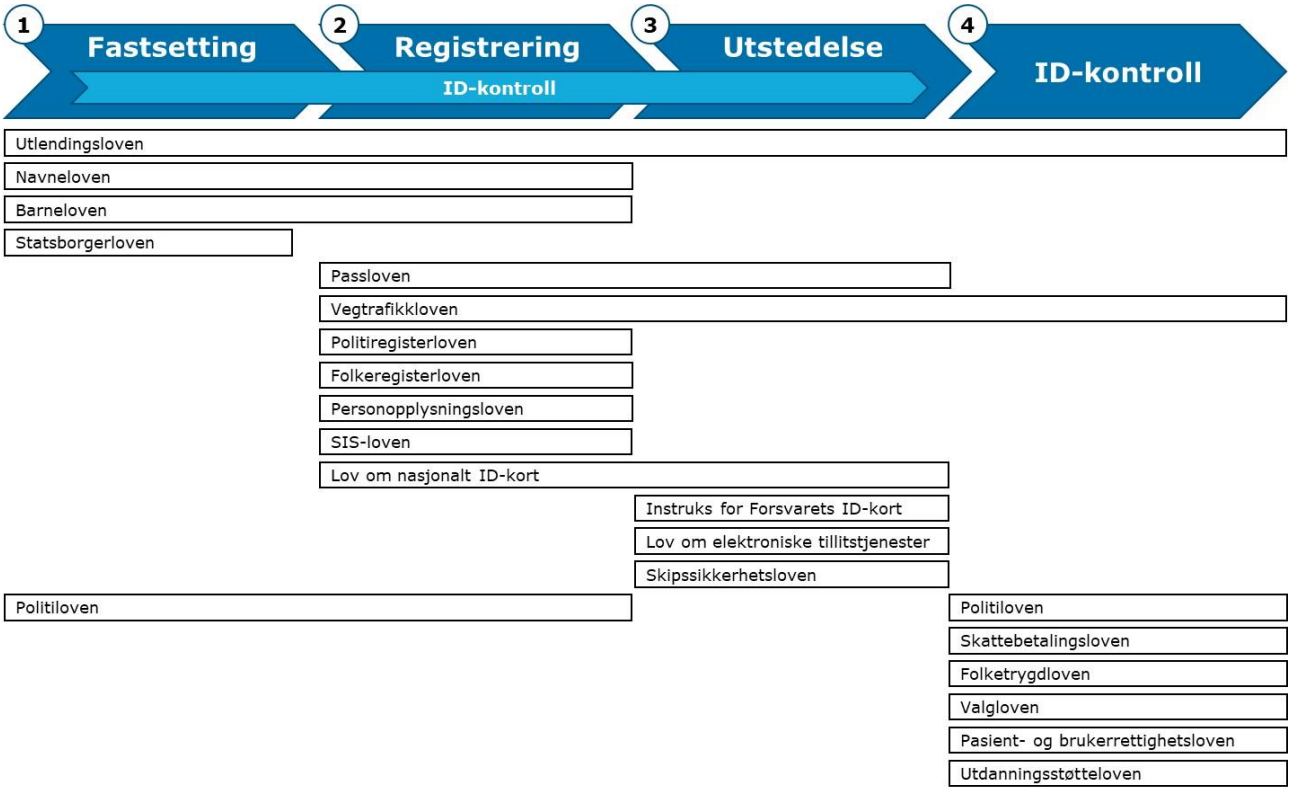
Begrepet regelverk benyttes i områdegjennomgangen som en samlebetegnelse på lover, forskrifter og andre regelverk slik som forordninger, rundskriv og instrukser.

For å avgjøre hvilke regelverk som er særlig relevante for områdegjennomgangen har leverandøren tatt utgangspunkt i avgrensningene nevnt ovenfor i kapittel 2.2-2.5. Kartleggingen dekker også regelverk med særlig betydning for informasjonsdeling mellom myndigheter. Med dette som utgangspunkt har leverandøren kommet frem til at følgende regelverk er mest relevante for ID-forvaltningen og områdegjennomgangen, oppsummert i figuren nedenfor:

1. **Fastsettelse og registrering av ID:** Statsborgerloven, Folkeregisterloven, Barneloven, Navneloven, Utlendingsloven, Politiregisterloven, Politiloven, Passloven, Lov om nasjonalt ID-kort (ikke i kraft), Vegtrafikkloven, SIS-loven og Personopplysningsloven

2. **Utstedelse av ID-bevis:** Passloven, Vegtrafikkloven, Utlendingsloven, Lov om elektroniske tillitstjenester, Skipssikkerhetsloven (for sjøfartsbok), Instruks for Forsvarets ID-kort, Lov om nasjonalt ID-kort (ikke i kraft)

3. **ID-kontroll:** Politiloven, Utlendingsloven, Vegtrafikkloven, Folketrygdloven, Valgloven, Pasient- og brukerrettighetsloven, Utdanningsstøtteloven og Skattebetalingsloven



Figur 8 Relevante regelverk opp mot prosessen i ID-forvaltningen

2.8 Sakstyper og volum

Leverandøren vil i områdegjennomgangen analysere flere ulike sakstyper i ID-forvaltningen, og volumet av disse.

2.8.1 Tildeling av fødselsnummer, rekvirering og tildeling av d-nummer og utstedelse av ID-bevis

I 2018 tildelte Skatteetaten totalt 110 828 fødselsnummer der 55 941 var gjennom fødselsmeldinger fra helseforetak for barn født i Norge, mens 54 887 var for utenlandske borgere. 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».

Det utstedes et stort antall ID-bevis i Norge hvert år. Tabellen nedenfor viser antall ID-bevis utstedt og tapt per type i 2018, samt antall ID-bevis i omløp ved utgangen av 2018[21]. Samlet sett ble det i 2018 utstedt ca. 1,4 millioner ID-bevis i Norge, med norske pass, BankID og norske førerkort som de mest utstedte typene.

ID-bevis	Utstedt i 2018	Tapt i 2018	I omløp per 2018
Norsk pass[22]	701 272	32 197	4 993 116
Norsk førerkort[23]	289 284	83 455	2 446 742
BankID[24]	435 391	*Data ikke tilgjengelig*	4 000 000[25]
MinID[26]	121 410	*Data ikke tilgjengelig*	3 446 268
Buypass ID[27]	80 000	*Data ikke tilgjengelig*	2 900 000[28]
Reisebevis for flyktninger[29]	24 000	380	83 456
Utlendingspass[30]		29	4 992
Forsvarets ID-kort[31]	16 282	692	19 226
Norsk sjøfartsbok/Sjøfartskort[32]	3 404	*Data ikke tilgjengelig*	*Data ikke tilgjengelig*
Norsk bankkort med bilde[33]	*Data ikke tilgjengelig*	*Data ikke tilgjengelig*	*Data ikke tilgjengelig*
Oppholdskort (Schengen-standardisert)[34]	123 064	*Data ikke tilgjengelig*	*Data ikke tilgjengelig*
TOTALT	**1 794 107**	**118 244**	**-**

Tabell 3 Antall utstedte og tapte ID-bevis i 2018, samt ID-bevis i omløp ved utløpet av 2018 (sortert etter antall utstedte ID-bevis i 2018)

2.8.2 eID og ID-porten

En eID betegnes som *«et sett med attributter som kan benyttes til verifikasjon av påstått identitet i elektronisk kommunikasjon mellom to parter»*[35]. Løsninger for elektronisk autentisering har vært tilrettelagt i både offentlig og privat sektor over lengre tid i Norge. Siden 2010 har det i rundskriv fra KMD blitt stilt krav til å benytte

[21] Bankkort med bilde er ikke inkludert med tall i tabellen da bankene har mangelfull data på antall utstedte, antall tapte og totalt antall kort i omløp
[22] Data mottatt fra POD. Tall gjelder pass for voksne og barn, inkludert nødpass
[23] Data mottatt fra SVV. Tall gjelder førstegangsutstedelse og fornyelse av førerkort
[24] Utstedte BankID gjelder BankID utstedt det siste året fra 24.06.19. Dette tallet er ikke 1 til 1 med antall nye brukere da noen brukere har to sertifikater (kodebrikke + BankID på mobil). Det finnes ingen helhetlig statistikk på tap av BankID da det er hver enkelt utstederbank som håndterer dette
[25] Finans Norge, «BankID og kontroll av pass», 2019
[26] Data mottatt fra Difi
[27] Buypass oppgir at informasjon om tapte eID-er er konfidensiell, men at det er snakk om et lite antall.
[28] Buypass.no, 2019
[29] Data mottatt fra UDI og POD
[30] Data mottatt fra UDI og POD
[31] Data mottatt fra Forsvaret
[32] NAV oppgir at de ikke har noen oversikt over tap av sjøfartsbøker eller totalt antall i omløp
[33] Mangelfull data på utstedelser, tap og kort i omløp skyldes at bankene ikke usteder bankkort sentralt
[34] Data mottatt fra UDI
[35] JD, «Sluttrapport – Nasjonalt ID-kort», 2007

ID-porten som løsning for offentlige digitale tjenester som krever innlogging og autentisering med eID. Gjennom ID-porten kan brukere i dag benytte seg av en rekke eID-er for autentisering mot det offentlige: MinID (lansert 2008), Buypass (2010), Commfides (2011) og BankID (2012). Difi har ansvaret for ID-porten, samt utstedelse og drift av den offentlige eID-en MinID[36]. Difi har videre ansvaret for at ID-porten fungerer som den norske eIDAS-noden, det vil si at ID-porten skal akseptere autentiseringer ved bruk av andre europeiske eID-er som er godkjente i henhold til eIDAS-forordningen.[37]

eID-er som brukes for autentisering til offentlig digitale tjenester i Norge er klassifisert etter fire ulike sikkerhetsnivåer, der de ulike sikkerhetsnivåene gir tilgang til ulike offentlige digitale tjenester. Sikkerhetsnivå 4, kalt «høyeste sikkerhetsnivå», gis til eID-er med to-faktor autentisering som består av to elementer, noe personen vet (personlig passord eller kode) og noe personen har (kodegenerator eller SIM-kort for BankID på mobil).[38] Det kreves personlig oppmøte og ID-kontroll av bruker ved førstegangsutstedelse av kodegenerator, hvor hensikten er å sikre at kodegeneratoren blir utlevert til korrekt person. Sikkerhetsnivå 3, kalt «mellomhøyt sikkerhetsnivå», gis til eID-er med to-faktor autentisering, men det er derimot ikke krav om fysisk oppmøte og ID-kontroll av bruker ved utstedelse.[39] Sikkerhetsnivå 2 og 1 betegner at innlogging gjøres med henholdsvis engangskode eller kun med et passord som brukeren selv velger.[40]

MinID gir tilgang til offentlige digitale tjenester gjennom ID-porten opp til mellomhøyt sikkerhetsnivå (nivå 3), mens de tre private eID-ene; BankID, Buypass og Commfides alle gir tilgang til tjenester opp til og med høyeste sikkerhetsnivå (nivå 4). Leverandøren er blitt informert om at MinID kan benyttes for autentisering til majoriteten av offentlige digitale tjenester, men dog kun til tjenester som godkjenner sikkerhetsnivå 3. BankID, Buypass og Commfides gir derimot brukeren tilgang til alle offentlige digitale tjenester. Private brukere kan i tillegg benytte BankID og Buypass for autentisering ved en rekke private digitale tjenester. Med planene som foreligger for nasjonale ID-kort med eID vil også nasjonal eID med sikkerhetsnivå 4 inkluderes som autentiseringsalternativ i ID-porten på et fremtidig tidspunkt, og vil også kunne benyttes for autentisering ved en rekke private digitale tjenester.

EU vedtok 23. juli 2014 en forordning om et felles rammeverk for elektronisk identifikasjon og elektroniske tillitstjenester for elektroniske transaksjoner i det indre marked (eIDAS). Forordningen ble gjennomført i norsk rett i lov om elektroniske tillitstjenester, som trådte i kraft 15. juni 2018. eIDAS-forordningen klassifiserer eID-er i tre ulike sikkerhetsnivåer, «lav», «betydelig» og «høy».[41] MinID er jf. eIDAS klassifisert som sikkerhetsnivå «betydelig», mens BankID, Buypass og Commfides alle er klassifisert som sikkerhetsnivå «høy». Det pågående arbeidet med eIDAS beskrives i kapittel 2.9.2.

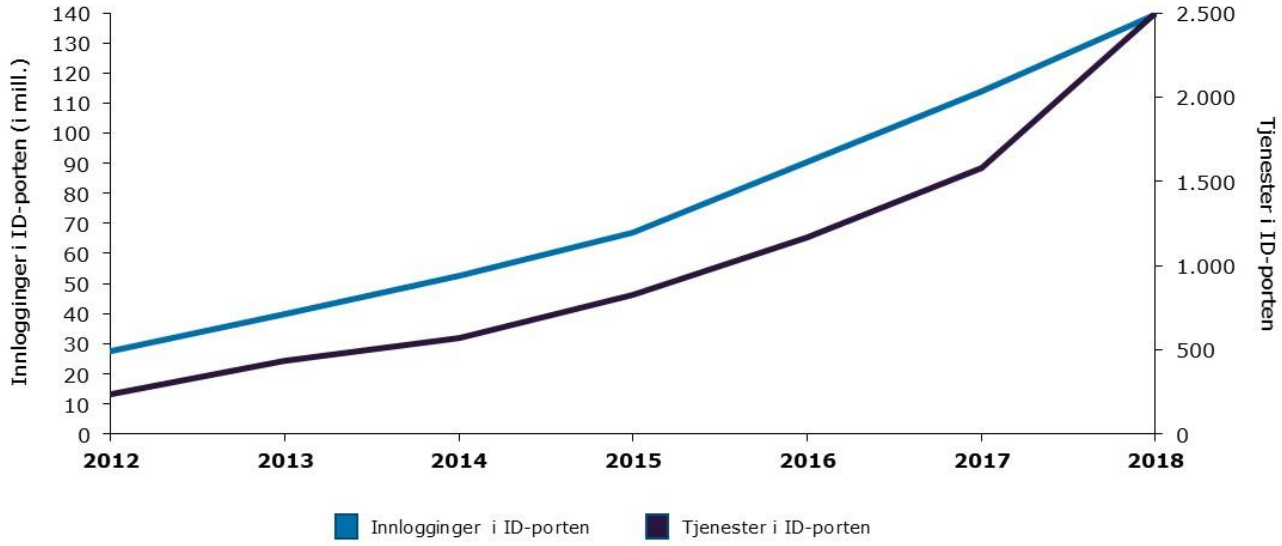
Det ble i 2018 gjennomført 139,4 mill. innlogginger gjennom ID-porten, hvorav ca. 82 prosent ble gjort med BankID.[42] For BankID totalt sett utgjør innloggingene gjennom ID-porten ca. 20 prosent av deres totale innlogginger per år[43]. MinID ble brukt i ca. 16 prosent av innloggingene, mens andelen innlogginger ved bruk av Buypass var ca. 2

[36] Basert på samtaler med representanter i Difi
[37] Basert på samtaler med representanter i Difi
[38] Difi, «Sikkerhet og informasjonskapsler – Ulike sikkerhetsnivå», 2019
[39] Difi, «Sikkerhet og informasjonskapsler – Ulike sikkerhetsnivå», 2019
[40] Altinn.no, «Innlogging – Diverse om innlogging – Sikkerhetsnivå», u.å.
[41] Se nærmere Prop. 71 LS (2017-2018), Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester 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
[42] Basert på informasjon forelagt leverandøren av Difi. Omfatter innlogginger ved bruk av BankID og BankID på mobil
[43] Basert på samtaler med Vipps AS

prosent. Commfides ble kun benyttet ved 0,01 prosent av innloggingene i ID-porten i 2018. Antallet innlogginger i ID-porten har doblet seg siden 2015, og har de siste seks årene vokst med omtrent 30 prosent i gjennomsnitt per år. Slik tabellen i kapittel 2.7.1 viser, var det ved utgangen av 2018 ca. 10,3 mill. eID-er i omløp i Norge, hvorav 6,9 mill. var av høyeste sikkerhetsnivå (nivå 4). Dette betyr trolig at de fleste norske borgere besitter to ulike eID-er. Leverandøren er imidlertid ikke kjent med at det eksisterer oversikt over hvordan antallet eID-er er fordelt på befolkningen.

Gjennom ID-porten ble det ved utgangen av 2018 tilbudt innlogging til 2 496 offentlige digitale tjenester, og siden 2015 har antallet tilgjengelige tjenester tredoblet seg. Av innloggingene i ID-porten i 2018 var 86 prosent til de ti mest brukte tjenestene, hvor Altinn var den mest brukte tjenesten.

Figuren under viser utviklingen i antall innlogginger og antall tilgjengelige tjenester i ID-porten fra 2012 til 2018.



Figur 9 Utvikling i antall innlogginger og antall tjenester i ID-porten

2.8.3 Saker tilknyttet EØS-borgere og tredjelandsborgere

Tabellen nedenfor oppsummerer et utvalg av ID-relaterte sakstyper knyttet til EØS-borgere og tredjelandsborgere. Utvalget gir et bilde av omfanget av, og utviklingen i tilstrømming av nevnte brukergrupper til landet.

ID-saker	2015	2018
Antall EØS-registreringer[44]	41 349	34 033
Innvilgede besøksvisum[45]	177 189	180 914
Innvilgede oppholdstillatelser for beskyttelse (asyl)[46]	8 796	3 577
Innvilgede oppholdstillatelser for arbeid	7 718	9 010
Innvilgede oppholdstillatelser for utdanning	6 319	5 638
Innvilgede oppholdstillatelser for familie	12 592	10 940

Tabell 4 Omfang av utvalgte ID-relaterte sakstyper (EØS- og tredjelandsborgere)

2.8.4 Fysiske ID-kontroller

Som beskrevet i kapittel 2.4 gjennomføres det ID-kontroller i alle stegene av dagens ID-forvaltning, både av fysisk utstedte ID-bevis og gjennom autentisering av elektroniske ID-bevis. I motsetning til for elektroniske ID-kontroller, er det mangelfull data på det totale antallet fysiske ID-kontroller som gjennomføres av offentlige aktører i ID-forvaltningen. Dette skyldes hovedsakelig at fysiske ID-kontroller gjennomføres av svært mange aktører i svært mange ulike prosesser, og at de ulike aktørene ikke loggfører antallet fysiske ID-kontroller som gjennomføres.

Leverandøren har likevel søkt å gi et bilde av antallet fysiske ID-kontroller tilknyttet steg 4 «ID-kontroll» (ref. kapittel 2.4) som ble gjennomført av offentlige aktører i 2018. Det vil si fysiske ID-kontroller som gjennomføres utenom stegene fastsettelse, registrering og utstedelse. Leverandøren har gjennom dataforespørsler til aktørene etterspurt antall gjennomførte fysiske ID-kontroller, men opplever at aktørene i svært varierende grad har data på dette.

POD har oversendt data for grense- og territorialkontroller i 2018, men har ikke mulighet til å gi estimater på antallet fysiske ID-kontroller som gjennomføres i politidistriktene som del av politiets øvrige oppgaveutførelse. SKD har oversendt data på antall gjennomførte fysiske ID-kontroller ved søknad om skattekort i de tilfeller bruker møter opp på skattekontorer, samt ved operative kontroller på arbeidsplasser. HOD, med underliggende helseforetak, gjennomfører ID-kontroll ved farskapsmeldinger ved fødsler der mor og far ikke er gift. NAV har ikke data eller estimater på antallet fysiske ID-kontroller som blir gjennomført i forbindelse med oppmøte på NAV-kontor for å få ytelser. Valgdirektoratet har ikke en rolle i fysiske ID-kontroller som gjennomføres i forbindelse med stemmegivning, da det er valgmedarbeidere ansatt av hver kommune, som kontrollerer velgernes ID ved stemmegivning. Tabellen under viser en oversikt over antall gjennomførte fysiske ID-kontroller i 2018, basert på data leverandøren har mottatt. Leverandøren er av den oppfatning at det samlede faktiske antall fysiske ID-kontroller som ble gjennomført i 2018 er betydelig høyere enn hva tabellen under viser, da datatilgjengeligheten hos flere aktører er begrenset.

[44] Antall EØS-borgere som har registrert seg for å arbeide, studere eller bo med familien sin i Norge, UDI, «EØS-registreringer etter statsborgerskap og formål», 2018 og 2015
[45] Antall personer som fikk besøksvisum i 2018 etter behandling av første søknad, UDI, «Besøksvisum innvilget i første instans etter statsborgerskap», 2018 og 2015
[46] Viser hvor mange personer som fikk oppholdstillatelser og er summen av konvensjonsflyktninger (asyl), annen flyktningstatus, opphold på humanitært grunnlag og overføringsflyktninger (fornyelse av oppholdstillatelser er ikke regnet med). UDI, «Innvilgede førstegangstillatelser etter statsborgerskap og type», 2018 og 2015

Fysiske ID-kontroller 2018	Aktør	Antall ID-kontroller
Grensepasseringer	POD	5 853 743
Territorialkontroll	POD	36 539
Søknad om skattekort ved oppmøte	SKD	143 763
Operativ kontroll arbeidsplasser	SKD	2 100
Farskapsmelding	Helseforetak	25 205
Stemmegivning ved valg (i 2017)[47]	Kommuner	2 945 345
Totalt antall fysiske ID-kontroller		**9 006 695**

Tabell 5 Utvalg av antall fysiske ID-kontroller i 2018

2.9 Pågående arbeid

Det pågår per september 2019 en rekke tiltak og arbeid relatert til ID-forvaltningen i Norge. Dette i tillegg til koordineringsgrupper og utvalg som jobber kontinuerlig med saker relatert til ID-forvaltningen. De neste delkapitlene gir en kort beskrivelse av et utvalg relevante tiltak og arbeid.

2.9.1 Pass og nasjonalt ID-kort

Pågående arbeid med oppdatering av regelverk og tjenestestruktur for pass og nasjonalt ID-kort

Det har siden utarbeidelsen av Handlingsplan for ID-området i 2011 pågått et omfattende arbeid med å bedre sikkerheten i utstedelse og kontroll av pass.[48] I løpet av det pågående arbeidet ble det i Riksrevisjonens rapport for budsjettåret 2014 også påpekt alvorlige mangler i prosessen med å utstede biometriske pass, herunder spesielt mangler ved informasjonssikkerheten, internkontroll og ID-kontroll samt mangelfull opplæring av politiets saksbehandlere.[49] Arbeidet med å lukke identifiserte avvik har pågått gjennom politiets program for «Nye Pass og ID-kort» (NPID – tidligere kjent som IDeALT programmet), og inkluderer blant annet nytt saksbehandlingssystem for pass og ID-kort, forbedret utstyr for ID-kontroll, tydeliggjøring av roller og oppgaver, opplæring av personell, forbedret sikkerhetsinfrastruktur, samt tilrettelegging for utstedelse av nasjonalt ID-kort med eID.

JD besluttet i november 2018 å innføre ny utstedelsesstruktur for pass og nasjonale ID-kort. Ny struktur legger til grunn at det skal etableres 77 pass- og ID-kontor på fastlandet, i tillegg til ett på Svalbard. Prosessen for å implementere ny struktur pågår, og skal etter planen være gjennomført i tide til lansering av nye pass og nasjonale ID-kort.[50]

[47] Antall stemmer ved stortingsvalget i 2017, Valgresultat.no, «Tall for hele Norge – Stortingsvalg 2017», 26.02.2018
[48] JD/POD, «Handlingsplan for ID-området», 2012
[49] Riksrevisjonen, «Dokument 1 (2015-2016) - Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2014», 2015
[50] JD, «Oppdragsbrev nr. 10/2018– Struktur for utstedelse av pass og nasjonale ID-kort», 26.11.2018

Forslag til ny forskrift om pass og nasjonale ID-kort ble i mars 2019 sendt ut på høring. Forslaget omhandler blant annet nye regler for fastsettelse av gebyr og behandling av opplysninger. I høringsforslaget er også passets gyldighetstid oppe til vurdering. Der fremsettes det to alternative forslag – ett som viderefører ti års gyldighetstid, og ett som reduserer gyldighetstiden til fem år.[51]

Planlagt utrulling av nasjonale ID-kort

Et forslag om å innføre nasjonalt ID-kort i Norge ble først fremlagt i 2007.[52] Arbeidet, som gjennomføres i PODs program «Nye pass og ID-kort» (NPID), har siden den gang vært gjenstand for betydelige forsinkelser. I løpet av perioden har flere sentrale aspekter om ID-kortets omfang og utrulling vært vurdert, herunder hvilke brukergrupper det nasjonale ID-kortet skal gjøres tilgjengelig for, hvorvidt det nasjonale ID-kortet skal være påkrevd eller frivillig, samt om nasjonalt ID-kort skal rulles ut med funksjonalitet for eID.

Nasjonalt ID-kort planlegges nå innført i 2020[53]. Det nasjonale ID-kortet vil gi norske borgere tilgang til et ID-bevis i kortformat utstedt med samme sikkerhet som for pass, og vil kunne erstatte passet som gyldig reisedokument innenfor Schengen-området. Biometriske opplysninger i form av ansiktsfoto og fingeravtrykk vil bli lagret i kortet. I ID-kortregisteret vil biometriske opplysninger i form av ansiktsfoto bli lagret.

I motsetning til pass, vil nasjonalt ID-kort også kunne utstedes uten reiserett**,** slik at personer som ikke har anledning til å reise ut av landet på grunn av kriminell handling, helseforhold eller annet, likevel kan legitimere seg. Lov 5. juni 2015 nr. 39 om nasjonalt ID-kort (ID-kortloven) gir rettslige rammer for planlagt ny ordning med nasjonalt ID-kort. Loven vil tre i kraft ved lanseringen av de nasjonale ID-kortene. Forslaget til ny forskrift om pass og nasjonalt ID-kort (sendt på høring mars 2019) bygger ut gjeldende regelverk for nasjonalt ID-kort med nye bestemmelser om blant annet gyldighetstid, gebyr og behandling av opplysninger. ID-kortets gyldighetstid foreslås her fastsatt til fem år.[54]

Det opprinnelige og primære formålet med et nasjonalt ID-kort er å gjøre det enkelt for norske borgere å skaffe seg et identitetsbevis med høy tillit og bredest mulig bruksområde. Ordningen skal medvirke til å erstatte mer usikre identitetsbevis og forhindre identitetstyveri og annen kriminalitet utført ved bruk av falsk, lånt eller stjålet identitet. I tillegg styrkes den enkeltes mulighet til å beskytte sin egen identitet og opplysninger om seg selv.[55]

Nåværende plan for utrulling legger til grunn at nasjonalt ID-kort utstedes basert på frivillighetsprinsippet, tilsvarende som dagens ordning for pass. For brukere vil nasjonalt ID-kort dermed være frivillig å anskaffe, og tjenesteeiere kan selv bestemme om det skal stilles krav til fremvisning av nasjonalt ID-kort for tilgang til offentlige tjenester og ytelser. [56]

I første omgang vil det nasjonale ID-kortet være et tilbud til norske statsborgere. Intensjonen er å utvide tilbudet til også å omfatte 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

[51] JD, «Høring – ny forskrift om pass og nasjonalt ID-kort», 2019
[52] JD, «Sluttrapport – Nasjonalt ID-kort», 2007
[53] JD, «Høring – ny forskrift om pass og nasjonalt ID-kort», 2019
[54] JD, «Høring – ny forskrift om pass og nasjonalt ID-kort», 2019
[55] JD, «Prop. 66 L, Lov om nasjonalt identitetskort (ID-kortloven)», 2014-2015
[56] JD, «Prop. 66 L, Lov om nasjonalt identitetskort (ID-kortloven)», 2014-2015

statsborgere vil bli sendt på egen høring når vilkår og fremdrift er nærmere avklart[57]. Situasjonen for utenlandske borgere er med dette uavklart på nåværende tidspunkt. Det er derimot klart at det EØS-rettslige ikke-diskrimineringsprinsippet vil bli etterlevd, noe som innebærer at EØS-borgere ikke kan behandles annerledes enn norske borgere. Krav som stilles til utenlandske EØS-borgere må følgelig også stilles til norske borgere.

2.9.2 eID

Status for nasjonal eID tilknyttet nasjonalt ID-kort

I sluttrapporten om Nasjonalt ID-kort fra 2007 ble det anbefalt at ID-kortet ble utstedt med funksjonalitet for eID.[58] Formålet med å etablere en nasjonal eID var å redusere risikoen for ID-misbruk, samt å tilby tjenesteeiere av digitale tjenester en elektronisk løsning med tilsvarende sikkerhet som pass.[59]

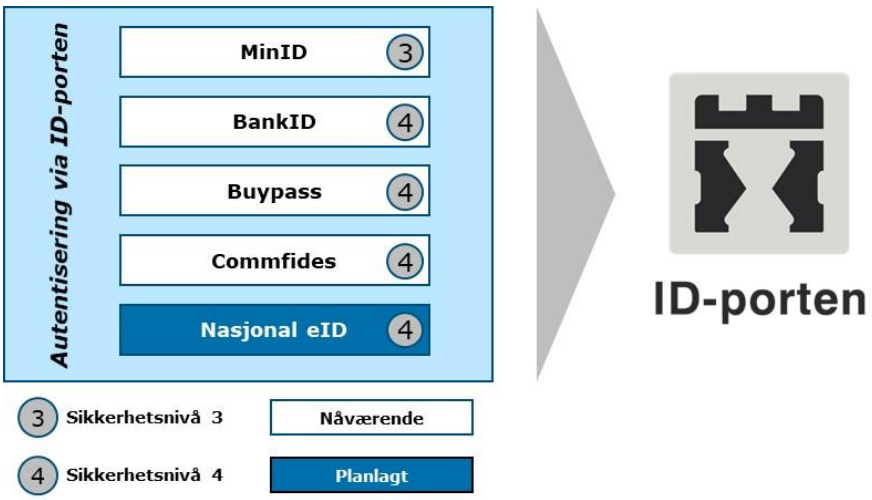
Leverandøren er informert om at det av hensyn til sikkerhet og kontroll i 2010 ble besluttet at nasjonalt ID-kort og tilknyttet eID måtte være underlagt samme styringssystem for informasjonssikkerhet for å kunne ha samme sikkerhetspolicy og oppfølging. Dette lar seg vanskelig gjennomføre dersom ikke både nasjonalt ID-kort og eID eies av samme virksomhet. Det ble derfor lagt til grunn for det videre arbeidet at sertifikatutsteder skulle være POD og ikke Difi.[60]

Nasjonal eID er avhengig av en sertifikatinfrastruktur. Leverandøren er gjort kjent med at infrastrukturen er anskaffet i markedet og er under implementering i politiets IKT-tjeneste (PIT), at installasjonen er nær ferdigstillelse og at den vil være en del av politiets øvrige sertifikatmiljø. Tilsvarende sentrale elementer som er nødvendig for utrulling av nasjonale ID-kort med eID er oppslagstjeneste for eID og produksjon av ID-kort. Disse er også anskaffet gjennom private aktører. Nytt saksbehandlingssystem er en forutsetning for sikkerhet og kvalitet i utrulling av nasjonal eID. Informasjon mottatt fra JD viser at arbeidet med nytt saksbehandlingssystem som utvikles av ekstern leverandør er forsinket, noe som har hatt innvirkning på tidslinjen for utrulling av nasjonal eID i sin helhet. Nasjonal eID må også ha et brukerstøtteapparat, og oppgaven skal løses av Difi etter avtale med POD.

Leverandøren er blitt gjort kjent med at det i 2016 endelig ble besluttet at nasjonalt ID-kort skulle etableres med elektronisk ID som et supplement til eksisterende eID-løsninger. I mars 2019 ble forslag til ny forskrift om pass og nasjonalt ID-kort sendt ut på høring, med blant annet forskriftsregler om tildeling og bruk av nasjonal eID.[61] Leverandøren er i etterkant av høringsforslaget gjort kjent med at det kan være aktuelt å lansere første versjon av nasjonale ID-kort uten aktivert nasjonal eID dersom dette reduserer risikoen for ytterligere utsettelser.

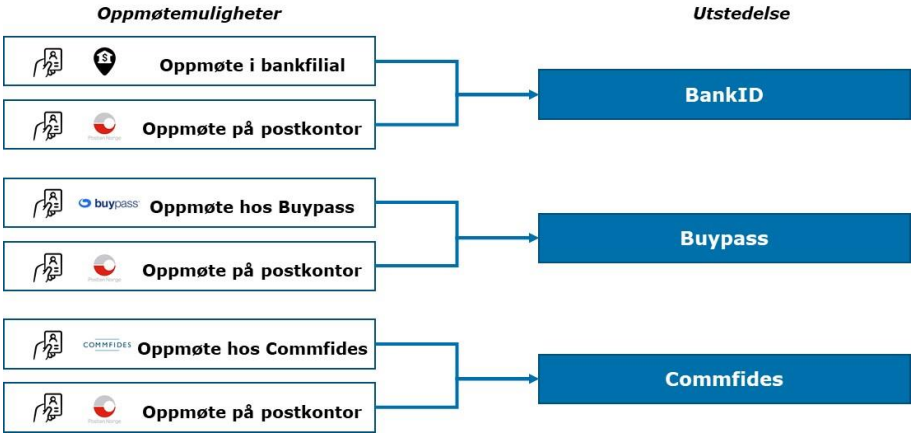
Figuren under viser de ulike eID-løsningene som i dag er tilgjengelige for autentisering til offentlige digitale tjenester gjennom ID-porten, samt den planlagte nasjonale eID tilknyttet nasjonalt ID-kort, med tilhørende sikkerhetsnivå.

[57] JD, «Høring – ny forskrift om pass og nasjonalt ID-kort», 2019
[58] JD, «Sluttrapport – Nasjonalt ID-kort», 2007
[59] JD, «Prop. 66 L, Lov om nasjonalt identitetskort (ID-kortloven)», 2014-2015
[60] JD, «Prop. 66 L, Lov om nasjonalt identitetskort (ID-kortloven)», 2014-2015
[61] JD, «Høring - ny forskrift om pass og nasjonalt ID-kort», 2019



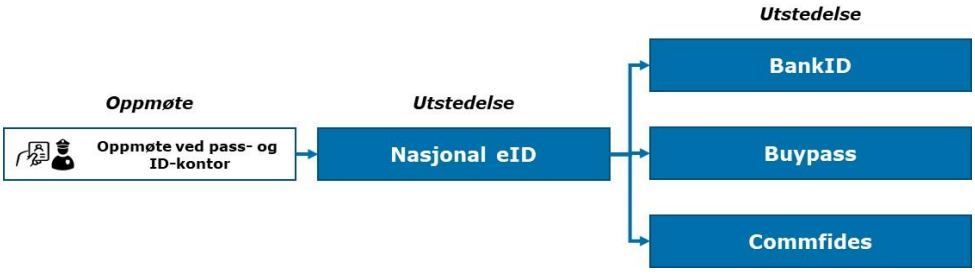
Figur 10 Nasjonal eID som supplement til eksisterende eID-løsninger

For å få utstedt private eID-er er det ulike krav til oppmøtested for obligatorisk ID-kontroll av bruker, avhengig av hvilken eID som utstedes. For BankID utstedt av banker med filialer må brukeren møte opp ved en filial for ID-kontroll, mens for BankID utstedt av banker uten filialer må brukeren møte opp ved postkontor eller post i butikk for ID-kontroll. Ved utstedelse av Buypass og Commfides kan brukeren velge mellom oppmøte hos utsteder eller ved postkontor/post i butikk for å gjennomføre ID-kontroll. Figuren under viser de ulike løsningene for ID-kontroll ved utstedelse av private eID-er.



Figur 11 Nåværende krav til oppmøte for etablering av privat eID

Som del av planene for nasjonal eID tilknyttet det nasjonale ID-kortet er det tiltenkt at den nasjonale eID-en skal kunne fungere som grunnidentitet som basis for utstedelse av private eID-er.[62] Figuren under illustrerer utstedelse av privat eID ved bruk av nasjonal eID.



Figur 12 Fremtidig krav til oppmøte ved etablering av privat eID gjennom nasjonalt eID

[62] POD, "Beslutningsgrunnlag for eID på nasjonalt ID-kort, delleveranse 3: Konseptbeskrivelse», 2016

Ansvar for forvaltning og regulering av eID

Ansvaret for forvaltning og regulering av eID er i dag fordelt på ulike departementer og dette gjelder også ansvaret for nasjonal eID. Oppgavene tilfaller KMD og JD og er beskrevet under.

- **KMD** er ansvarlig for regulering og implementering av bruk av eID og digital tilgang til offentlige tjenester.[63] KMD innehar forvaltningsansvar for lov om elektroniske tillitstjenester med tilhørende forskrifter.[64] KMD er også ansvarlig for kravspesifikasjon for PKI (Public Key Infrastructure)[65] i offentlig sektor og rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, som er under revisjon.[66] KMD har overtatt NFDs ansvar til å gi forskrift om å «*etablering av et felles tillitsmerke, om tillitslister, om akkreditering av samsvarsvurderingsorganer, om utforming av samsvarsvurderingsrapport og regler for gjennomføring av samsvarsrevisjoner, om krav til og sertifisering av kvalifiserte elektroniske signatur- og seglfremstillingssystemer, om kvalifiserte valideringstjenester for elektronisk signatur og elektronisk segl*».[67] Leverandøren er kjent med at overtagelsen av ansvaret ved rapportens utarbeidelse er en pågående prosess. Nasjonal kommunikasjonsmyndighet (Nkom), også underlagt KMD, er tilsynsmyndighet for tillitstjenester

- **JD** er ansvarlig for utstedelse og regulering av nasjonal eID tilknyttet nasjonalt ID-kort. JD innehar i tillegg samordningsansvaret for IKT-sikkerheten i sivil sektor[68]

Tilrettelegging mot eIDAS-forordningen

I lys av en utvikling mot økt integrasjon for eID på kontinentet pågår det nå et arbeid med å få på plass et mer helhetlig reguleringsregime for eID. 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. Dette skal oppnås blant annet gjennom en gjensidig plikt til å anerkjenne andre lands eID-løsninger, gitt at eID-løsningen er notifisert til og oppført på liste av Europakommisjonen.[69] For eksempel vil BankID kunne brukes til å benytte seg av offentlige tjenester i andre europeiske land, og EØS-borgere vil kunne benytte notifiserte eID-er fra sitt hjemland for autentisering til offentlige digitale tjenester i Norge. Etableringen av et rettslig rammeverk for diverse tillitstjenester, inkludert sertifikattjenester for nettstedsautentisering, skal også bidra til å oppnå formålet med forordningen.

Leverandøren er gjort kjent med at det i arbeidet med forordningen har vært diskusjoner tilknyttet kravene for hva som skal til for å tilfredsstille høyeste sikkerhetsnivå («high»). Det pågår et arbeid i den mellomstatlige organisasjonen FATF (Financial Action Task Force) for å heve sikkerhetskravene til eID (herunder stille krav til knytning mot biometri og utstedelse av offentlig myndighet). Norge er representert i dette arbeidet gjennom FIN og JD. JD informerer om at dette vil muliggjøre harmonisering av kravene til identifisering i fysiske tjenester (både offentlige og

[63] Nordic eID Survey, Final Report, 2015
[64] Lovdata, «Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester)», 2018
[65] JD, «Sluttrapport – Nasjonalt ID-kort», 2007: «*En teknologisk infrastruktur som muliggjør en stor skala bruk av elektronisk ID og e-signatur på Internett*»
[66] Lovdata, «Deleg. til NFD og KMD etter lov om elektroniske tillitstjenester», 2018
[67] Lovdata, «Deleg. til NFD og KMD etter lov om elektroniske tillitstjenester», 2018
[68] JD, «Høring - ny forskrift om pass og nasjonalt ID-kort», 2019
[69] JD, «Prop. 66 L, Lov om nasjonalt identitetskort (ID-kortloven)», 2014-2015

private), som i dag er regulert i Hvitvaskingsregelverket, og kravene til identifisering i digitale tjenester, som i dag kun er regulert for offentlige tjenester.

I forbindelse med eIDAS-forordningen har Europakommisjonen fastsatt åtte gjennomføringsrettsakter. Det pågår nå en prosess om å gjøre gjennomføringsrettsaktene til norsk rett gjennom forskrifter til lov om elektroniske tillitstjenester. KMD har nylig hatt forslag til implementering av nevnte gjennomføringsrettsakter på høring[70], og er i prosess med å implementere nytt rammeverk for identifikasjon og sporbarhet, samt ny selvdeklarasjonsforskrift.[71]

2.9.3 Modernisering av Folkeregisteret

«Skatteetaten jobber med en komplett modernisering av dagens register for at det skal speile dagens og fremtidens samfunn og behov».[72] I 2014 godkjente Stortinget igangsetting av prosjektet modernisering av Folkeregisteret innenfor en kostnadsramme på 536 mill. kroner. Satsingen i regi av Skattedirektoratet (SKD) som startet i 2016 pågår, med planlagt ferdigstilling i 2020. Arbeidet skal ivareta økte krav til identitetsforvaltning, økt datakvalitet og raskere ajourhold, i tillegg til å sikre et godt personvern og god tilgjengelighet til folkeregisteropplysninger.

Prosjekt modernisering av Folkeregisteret skal legge til rette for nytt saksbehandlingssystem, nye elektroniske grensesnitt, selvbetjeningsløsninger, videreutvikling av modernisert infrastruktur og driftsplattform, tilrettelegging for ny lov[73], samt innføring av nye løsninger.

Skatteetaten uttaler på sine nettsider at nytt folkeregister muliggjør store gevinster for samfunnet[74] med større grad av automatisert saksbehandling og tidsbesparelser på registreringer i registeret. Dette resulterer i et folkeregister av høyere kvalitet på opplysninger og raskere informasjonsutveksling. I tillegg oppgis det at det vil sikre en mer helhetlig identitetsforvaltning gjennom elektronisk tildeling av d-nummer og innføring av identitetsgrunnlag («kontrollert», «ikke kontrollert» og «unik»). For borgerne generelt betyr moderniseringen at de sjeldnere trenger å oppgi informasjon til hver enkelt av de offentlige virksomhetene de er i kontakt med, fordi de offentlige virksomhetene kan samhandle bedre om opplysningene om borgere.

2.9.4 Biometri

Knytning av biometri mellom Folkeregisteret, passregisteret og utlendingsregisteret

I 2016 ble det lagt frem en utredning om knytning mellom Folkeregisteret og biometriregistrene (Passregisteret, nasjonalt ID-kortregister og Utlendingsregisteret) i justissektoren der arbeidsgruppen anbefalte en knytning mellom registrene for å sikre «unike» identiteter i Folkeregisteret.[75] Ny kategorisering for grunnlag for *registrert*

[70] KMD, «Høring – Implementering av gjennomføringsrettsakter til eIDAS-forordningen, nytt rammeverk for identifikasjon og sporbarhet og ny selvdeklarasjonsforskrift», 2019
[71] JD, «Høring - ny forskrift om pass og nasjonalt ID-kort», 2019
[72] Skatteetaten, «Modernisering av Folkeregisteret», u.å.
[73] I 2017 fikk Norge ny lov om folkeregistrering
[74] Skatteetaten, «Gevinster for samfunnet med nytt Folkeregister», u.å.
[75] JD, FIN og KMD, «Utredning – knytning mellom Folkeregisteret og biometri i Passregisteret, Nasjonalt ID-kortregister og Utlendingsregisteret», 2016

identitet ble nedfelt i lov 9. desember 2016 nr. 88 om folkeregistrering (folkeregisterloven) § 3-2. Grunnlaget for registrert identitet introduserer kategoriene «unik», «kontrollert» og «ikke-kontrollert». Dersom personens identitet er kontrollert ved personlig fremmøte for Skatteetaten eller utlendingsmyndighetene med fremvisning av pass eller tilsvarende, registreres identiteten som «kontrollert». Dersom vilkårene for å registrere en persons identitet som «kontrollert» ikke er oppfylt, registreres identiteten som «ikke-kontrollert».[76]

Kategoriseringen er i praksis gjennomført fra 2017 for kategoriene «kontrollert» og «ikke-kontrollert», men ikke for status «unik». Skatteetaten er som folkeregistermyndighet avhengig av justissektoren for å kunne registrere i Folkeregisteret om en identitet er «unik», dvs. at det foreligger biometrisk data om en person og at disse er sjekket for unikhet. Dette vil i betydelig grad øke kvaliteten på registerets identitetsopplysninger. I justissektoren opptas bilder og fingeravtrykk til ulike formål. For å kunne gjøre en undersøkelse av om en person er «unik» i Norge, kreves det at de biometriske personopplysningene som innhentes av utlendingsmyndighetene og av politiet, lagres på en slik måte at det er mulig å gjøre søk på tvers i databasene hvor biometrien lagres.[77] For at dette skal fungere i praksis må det gjøres tilpasninger og legges til ny funksjonalitet i ABIS.[78] POD, utlendingsforvaltningen og SKD arbeider nå med å utvikle en modell for kobling mellom passregisteret, utlendingsregisteret og Folkeregisteret for å kunne markere om en registrert identitet i Folkeregisteret er «unik». JD arbeider med tilhørende regelverksendringer i utlendingsloven og pass- og ID-kortlovene, jf. blant annet høringsnotat 15. juli 2019 om endringer i utlendingsloven m.m. (utvidet bruk av biometri i utlendingssaker).

Vurdering om fremtidig lagring av fingeravtrykk i pass- og ID-kortregistrene

POD, Utlendingsdirektoratet (UDI) og SKD samarbeider for å styrke fundamentet for grunnidentitet gjennom innføring av kvalitetsindikatoren «unik» (ref. modernisering av Folkeregisteret over). Som ledd i dette arbeidet er det behov for å jobbe med de rettslige rammene, herunder vurdere personvernkonsekvenser, for å kunne ta stilling til om det skal åpnes for sentrallagring av fingeravtrykk i pass- og ID-kortloven. Dette kan ytterligere styrke kvalitetsindikatoren «unik». Spørsmålet om lagring av fingeravtrykk fra pass- og ID-kortutstedelse har også betydning for effekten av andre tiltak for i ID-forvaltningen.

Utvidet bruk av biometri i utlendingssaker

JD sendte i juli 2019 et forslag på høring om regelendringer som innebærer mer bruk av biometri i utlendingssaker.[79] Forslagene innebærer blant annet at det skal tas fingeravtrykk, i tillegg til ansiktsfoto i alle utlendingssaker utenom EØS-borgere omfattet av EØS-regelverket. Dette gjelder i dag kun for noen sakstyper. Det foreslås videre at politiet skal kunne søke i registrert biometri ved grensekontroll og innenlands utlendingskontroll slik at identiteten kan undersøkes «på stedet» i større grad enn i dag. Som en videre del av forslagene foreslås det at registrerte fingeravtrykk lagres vesentlig lengre enn etter gjeldende regelverk, og som hovedregel i 20 år.

[76] FIN, «Forskrift til folkeregisterloven (folkeregisterforskriften), § 3-2-1», 2017
[77] FIN, Prop. 164 L (2015-2016) «Lov om folkeregistrering (folkeregisterloven)»
[78] JD, FIN og KMD, «Utredning – knytning mellom Folkeregisteret og biometri i Passregisteret, Nasjonalt ID-kortregister og Utlendingsregisteret», 2016
[79] JD, «Mer bruk av biometri i utlendingssaker», 2019

De foreslåtte tiltakene er ment å bidra til å forebygge og avsløre ID-misbruk, motvirke ulovlig opphold og bidra til bekjempelse av ID- og arbeidskriminalitet. I tillegg legger endringsforslagene til rette for koordinering med parallelle prosesser om modernisering av Folkeregisteret og innføring av nasjonalt ID-kort. Høringsforslaget har frist for å sende inn høringssvar i oktober 2019.

Det pågående arbeidet med utvidet bruk av biometri utlendingssaker er en del av UDIs moderniseringsprogram[80].

Når det gjelder personvernutfordringen knyttet til disse regelendringene uttaler departementet i høringsnotatet at «utvidet bruk av fingeravtrykk og ansiktsfoto i utlendingskontrollen er nødvendig og forholdsmessig, og ligger innenfor det folkerettslige og lovmessige handlingsrommet.»[81]

2.9.5 Tverretatlig koordineringsgruppe for identitetsforvaltning (KoID) og forslag til visjon for nasjonal identitetsforvaltning

En koordineringsgruppe for identitetsforvaltning (KoID) ble i 2018 etablert av interessesammenslutningen *Styring og koordinering av tjenester i e-forvaltning* (Skate) på bakgrunn av behov for bedre koordinering innen identitetsforvaltning.[82] KoID består av ledere fra Difi, POD, UDI og SKD. Gruppen har ikke beslutnings- eller gjennomføringsmyndighet, men skal gi råd til de fire etatslederne. KoIDs hovedformål er å bidra til en styrket identitetsforvaltning i Norge og at de fire etatenes innsats på dette området blir mer målrettet og koordinert[83]. KoID har foreslått en visjon for identitetsforvaltningen:

1. *En person, en identitet i Norge*

2. *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*

3. *Alle med et norsk identitetsnummer skal oppleve trygghet for at ingen andre skal kunne overta identiteten. Ingen med norsk identitetsnummer skal utsettes for ID-tyveri*

4. *Ingen skal kunne operere med falske eller fiktive identiteter i Norge*

I mottatt presentasjon fra Skatteetaten fremstilles dette noe forenklet som fire ambisjoner «en person en identitet», «sterke ID-bevis til alle», «kunne kreve sterk ID-kontroll og tilgang til sterk ID-kontroll» samt «alle skal kunne få e-ID på nivå fire»[84]. De fire etatslederne i Difi, POD, UDI og SKD, samt NAV har gitt sin tilslutning til KoIDs anbefalte visjon, som også er behandlet i Skate.

[80] UDI, «Årsrapport 2018», 2019
[81] JD, «Høringsnotat 15. juli 2019 om forslag til endringer i utlendingsloven m.m. om opptak og lagring av biometri i utlendingssaker», 15. juli 2019
[82] Difi, «Mandat for koordineringsgruppe for ID-forvaltning (KoID)», 2017
[83] SKD, «Forslag til visjon for nasjonal identitetsforvaltning», 2018
[84] Difi, mottatt presentasjon: «KoID – hva vil vi oppnå», u.å.

2.9.6 Øvrige tiltak for sikrere identitet og identitetsforvaltning

Tiltak i sentrale nasjonale strategier

I to av regjeringens sentrale strategier, strategien mot arbeidskriminalitet og digitaliseringsstrategien fra 2019, listes det i opp noen tiltak relatert til ID.

Regjeringens strategi mot arbeidslivskriminalitet inkluderer følgende tiltak som alle er under implementering:

- Sikrere ID-dokumenter
- ID-kontroll ved utstedelse av d-nummer og helhetlig ansvar for EØS borgere
- Utrede knytning av biometri mellom Folkeregisteret, passregisteret og utlendingsregisteret (omtalt i kapittel 2.9.4)

I tillegg nevnes det i regjeringens digitaliseringsstrategi, under målet om «felles økosystem for nasjonal digital samhandling og tjenesteutvikling», at regjeringen vil:

- Vurdere hvordan en kan sikre e-ID og e-signatur til alle grupper som har behov for det, og retningslinjer for bruk av ansatt-ID

Det er ikke besluttet når overnevnte punkt i digitaliseringsstrategien skal gjennomføres eller hvem som skal gjennomføre det per september 2019.

Ny grenselov vedtatt

Lov 20. april 2018 nr. 8 om grensetilsyn og grensekontroll av personer (grenseloven) er vedtatt av Stortinget, men har ikke trådt i kraft. Det følger av pressemelding fra regjeringen at «gjeldende regler om grensetilsyn og grensekontroll følger for en stor del av folkerettslige avtaler som Norge er bundet av, særlig gjennom Schengen-samarbeidet og avtalene med nabolandene Sverige, Finland og Russland. Disse reglene videreføres i lovforslaget, som heller ikke innebærer endringer i ansvarsfordelingen og organiseringen av grensekontrollen.»[85]

Endringer i grensekontroll og internasjonalt samarbeid

Europaparlamentet og Rådet fremmet i 2018 forslag til to rettsakter om å etablere et rammeverk for interoperabilitet mellom EUs informasjonssystemer. Den ene rettsakten retter seg mot grensekontroll og visum, og den andre mot politi og rettslig samarbeid, asyl og migrasjon. Forslagene tar samlet sett sikte på å styrke forvaltningen av Schengen-yttergrenser og bidra til styrket indre sikkerhet. Formålet med forslagene er å sikre at sluttbrukere har rask, sømløs og kontrollert tilgang til den informasjon de trenger for å kunne løse sine oppgaver. Saken har blitt forhandlet i rådsarbeidsgruppen DAPIX og lagt videre til justisrådene mai 2018.[86]

Europaparlamentet og Rådet fremmet i 2019 forslag til rettsakt om endring av VIS-forordningen (se ytterligere beskrivelse i kapittel 3.1.4). Endringsforslaget omfatter fire hovedelementer[87]:

- Kopi av pass skal registreres i VIS sentralt (gjøres ikke i dag)

[85] JD, «Ny lov om grensetilsyn og grensekontroll (grenseloven), 11.08.2017
[86] JD, «Interoperabilitetspakken (grenser og visum)», 30.05.2018
[87] JD, «Endring av VIS-forordningen», 25.06.2019

- Fingeravtrykk skal tas av barn fra seks års alder (i dag fra tolv års alder)
- Formålet med VIS utvides til å inkludere registrering av oppholdstillatelser (i dag er det informasjonsmangel fordi opphold utover tre måneder ikke registreres i noen felles EU-base)
- Det blir en automatisert kryss-sjekk av relevante databaser og regler om screening. Dette henger sammen med interoperabilitetsarbeidet

Formålet med endringsforslaget er å forenkle visumsøknadsprosedyrene, forenkle og styrke kontroll på yttergrensen og inne på Schengen-territoriet. Per august 2019 har endringsforslaget vært behandlet i rådsarbeidsgruppen Visa Working Party, og det påtroppende finske formannskapet planlegger å starte triologforhandlinger med Europaparlamentet høsten 2019.[88]

Europaparlamentet og Rådet vedtok 30. november 2017 en forordning om etablering av et system for elektronisk registrering av tredjelandsborgeres passering av Schengen-samarbeidets yttergrenser ved korttidsopphold – Entry/Exit System (EES).[89] Systemet vil registrere tidspunkt og sted for inn- og utreise, samt biometriske kjennetegn (ansiktsbilde og fire fingeravtrykk) for de reisende. Dataene vil bli kontrollert ved senere inn- og utreiser. Systemet vil automatisk beregne hvor lenge tredjelandsborgeren kan oppholde seg på Schengen-territoriet, og vil varsle medlemslandene der reisende ikke forlater Schengen-territoriet innen utløpet av lovlig oppholdstid. Registrering og kontroll i EES erstatter dagens praksis med manuell stempling i reisedokumenter. Systemet skal effektivisere grensekontrollprosessen, samtidig som kvaliteten i prosessen styrkes. Beslutning om godtakelse av rettsakten er under arbeid i Regjeringen.

2.10 Viktige avgrensninger

Leverandøren understreker at det er gjennomført et antall detaljerte analyser som er avklart i samråd med prosjektgruppen. Det har videre ikke vært en del av leverandørens mandat å kvalitetssikre det pågående pass- og ID-programmet.

I samråd med prosjektgruppen ble det i tillegg besluttet at noe pågående arbeid i ID-forvaltningen ikke skulle tas opp til vurdering i forbindelse med områdegjennomgangens arbeid. Dette gjelder følgende:

- Struktur for nye pass- og ID-kontor
- Selve prosessen for utrulling av nye pass og nasjonale ID-kort med eID

[88] JD, «Endring av VIS-forordningen», 25.06.2019
[89] Europaparlaments- og rådsforordning (EU) 2017/2226 av 30. november 2017 om opprettelse av et inn- og utreisesystem til registrering av inn- og utreiseopplysninger om tredjelandsstatsborgere som passerer Den europeiske Unions medlemsstaters ytre grenser, samt avslag på innreise og fastsettelse av betingelsene for adgang til inn- og utreisesystemet med hensyn på rettslig håndhevelse og om endring av forordning (EF) nr. 767/2008 og forordning (EU) nr. 1077/2011

Del 2: Tematisk kartlegging og analyse av nåsituasjonen

Del 2 inneholder en tematisk kartlegging og analyse av nåsituasjonen inkludert beskrivelse av nåsituasjonen, samt funn og vurderinger av nåsituasjonen tilknyttet hvert tema. Delen dekker styring og struktur i ID-forvaltningen (kapittel 3), gjeldende lover og regelverk i ID-forvaltningen (kapittel 4), brukerreiser og brukervennlighet i ID-forvaltningen (kapittel 5), kvalitet og sikkerhet i ID-forvaltningen (kapittel 6) og ressursbruk og kostnader i ID-forvaltningen (kapittel 7).

3 Styring og struktur av ID-forvaltningen

I dette kapittelet gis en beskrivelse av nåsituasjonen (kapittel 3.1) og leverandørens funn og vurderinger tilknyttet nåsituasjonen (kapittel 3.2) for styring og struktur av ID-forvaltningen. Kapittelet dekker funn og vurderinger av aktørbildet, geografisk tjenestestruktur, saksgang, registre og saksbehandlingssystemer og styring og struktur hos utenlandske aktører.

3.1 Nåsituasjonen

3.1.1 Aktørbilde i ID-forvaltningen med administrativ styringslinje

I kapittel 2.5 ble det gitt et overblikk over involverte aktører i ID-forvaltningen fordelt på primær- og sekundæraktører. Figuren nedenfor fremstiller aktørbildet i dagens ID-forvaltning og den administrative styringslinjen. I tillegg til den formelle administrative styringslinjen har forvaltningen en faglig linje som omtalt i kapittel 4.1.21.

Stortinget er øverste myndighet og vedtar lover som ligger til grunn for Regjeringens utøvelse. I kartleggingen av nåsituasjonen for ID-forvaltningen anses elleve av 16 departementer for å være aktører i ID-forvaltningen da disse har underliggende etater eller virksomheter som anses som primær- eller sekundæraktører inn mot ID-forvaltningen, jf. kapittel 2.5. Departementenes oppgaver på et overordnet nivå innebærer blant annet gjennomføring av sektorpolitikk og styring og oppfølging av underliggende virksomheter.[90]

Videre er det totalt 18 underliggende etater og virksomheter som anses som aktører i ID-forvaltningen. Underliggende virksomheter har ulike betegnelser, men ofte brukes betegnelsen etater. Det er store forskjeller med hensyn til størrelse, organisering og hvilke fullmakter de har.[91] De underliggende etatene og virksomhetene instrueres av ansvarlige departementer gjennom individuelle tildelingsbrev hvor det er satt mål og styringsparametere.[92] Statlige virksomheter er underlagt økonomiregelverket som stiller krav til internkontroll og det er den enkelte etats- og virksomhetsledelse som har ansvaret for å påse at internkontrollen er tilpasset risiko og vesentlighet. [93]

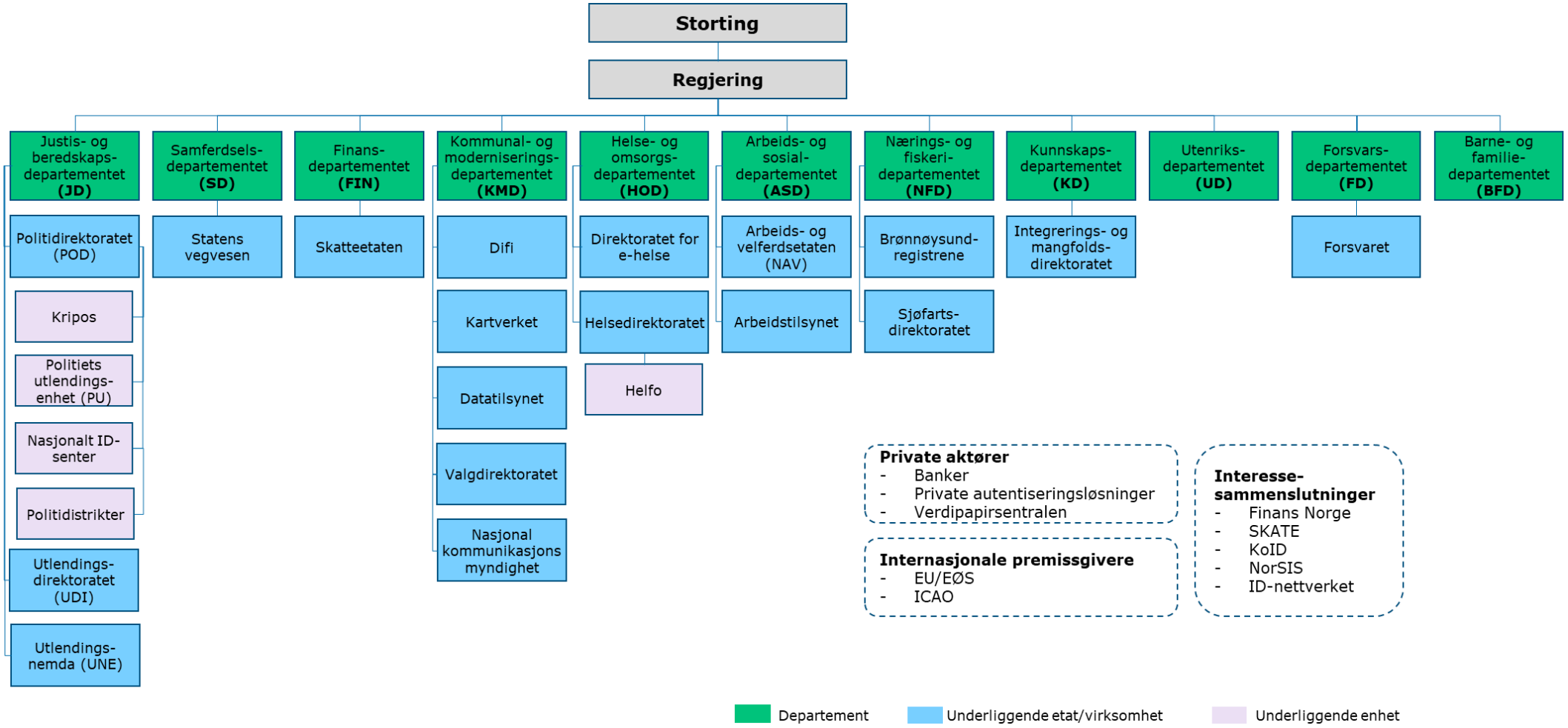
Enkelte etater og virksomheter i ID-forvaltningen har underliggende enheter som er en del av ID-forvaltningen. De kan bestå av flere distrikter, kontorer, resultatområder, regioner og/eller tjenestesteder og er ofte førstelinje. Disse er oppsummert i tabell 6 under.

[90] KMD, «Om forholdet mellom politisk ledelse og embetsverk», 2019
[91] KMD, «Om forholdet mellom politisk ledelse og embetsverk», 2019
[92] I tillegg gis det supplerende tildelingsbrev og diverse instrukser til enkelte virksomheter
[93] FIN, «Reglement for økonomistyring i staten. Bestemmelser om økonomistyring i staten», 2015

Videre har flere interessesammenslutninger og samarbeidsfora, eksempelvis Skate, KoID, ID-nettverket, norsk senter for informasjonssikring (NorSIS) og Finans Norge viktige funksjoner og roller i ID-forvaltningen.

Internasjonale premissgivere som EU/EØS og ICAO er også involvert ved at de er ansvarlig for regelverk som setter krav til og rammer for ID-forvaltningen i Norge.

Det er i tillegg private aktører som har viktige grensesnitt og samhandler med ID-forvaltningen. Dette gjelder aktører i bank- og finansnæringen, samt tilbydere av autentiseringsløsninger (Buypass og Commfides).



Figur 13 Den administrative styringslinjen i dagens ID-forvaltning

Dep.	Underliggende virksomhet	Distrikt/kontor/resultatområde/tjenestested	Antall[94]
JD	POD	Politidistrikter	12
		Passkontor[95]	141
		Politistasjoner og lensmannskontor	225
SD	SVV	Trafikkstasjoner[96]	72
FIN	Skatteetaten	Skattekontor (som kontrollerer ID)[97]	42
HOD		Regionale helseforetak (RHF)	4
		Helseforetak (HF)	20
		Fødeavdelinger og fødestuer	45
ASD	NAV	NAV Ytelseslinjen	4
		NAV-kontor	456
UD		Utenriksstasjoner	99

Tabell 6 Antall distrikter, kontorer, resultatområder eller tjenestesteder under utvalgte underliggende virksomheter

Nedenfor følger en kort beskrivelse av figuren og tabellen ovenfor med aktørene og deres rolle inn mot ID-forvaltningen i Norge. Både primæraktører og sekundæraktører er beskrevet (ref. kapittel 2.5). Det påpekes at aktørenes ansvar for lover og regelverk beskrives i kapittel 4.

Justis- og beredskapsdepartementet[98]

Politidirektoratet (POD): Har ansvaret for faglig ledelse, styring, oppfølging, og utvikling av politidistriktene og særorganene i politiet.[99] Det ble i 2018 opprettet en egen ID-seksjon i avdeling for politifag i POD som har prosesseieransvar for utstedelse av og sikkerhet for pass og ID-dokumenter, ansvar for å sette standarder for å kontrollere og verifisere ID i politiet, samt et overordnet ansvar for biometri og særskilt ansvar for fingeravtrykk og foto.[100]

- Kripos: Nasjonal enhet underlagt POD for bekjempelse av organisert og annen alvorlig kriminalitet.[101] Kripos bistår politiet med fastsettelse av ukjente identiteter via Interpol-samarbeidet og videre registrering av identiteter[102]. Som politiets nasjonale kompetansesenter innehar Kripos også viktig ekspertkompetanse for avdekking av ID-tyveri og falsk ID. De er videre ansvarlig for å sjekke fingeravtrykk i saker om beskyttelse (asyl) opp mot EUs fingeravtrykksdatabase (EURODAC) for asylsøkere og ulovlige grensepasseringer[103]

- Politiets utlendingsenhet (PU): Nasjonalt særorgan underlagt POD som bistår politiet i utlendingssaker. PU har det primære ansvaret for å klarlegge

[94] Tallene viser antall distrikter, kontorer, regioner og/eller tjenestesteder i underliggende etat eller enhet der dette er relevant. Tallene er basert på oppgitte tall på hjemmesider og/eller direkte kommunikasjon med aktører
[95] Per november 2018. JD besluttet i 2018 å redusere antall pass- og ID-kontor til 78, og dette arbeidet pågår
[96] Vegvesenet har levert forslag til ny struktur på trafikant- og kjøretøyområdet til SD 20. mai, der de foreslår å redusere antall trafikkstasjoner. Samferdselsministeren har med frist 1. november bedt SVV om ytterligere vurderinger av avbøtende tiltak der ny struktur gir lengre reisevei for publikum
[97] Skatteetaten, «Skattekontorer som utfører ID-kontroll», u.å.
[98] JD har det overordnede ansvaret for å utforme staten sin flyktning- og innvandringspolitikk og har et bredt samarbeid med andre departement om oppgaver på feltet
[99] JD, «Politidirektoratet», u.å.
[100] Norges Politilederlag, «Arne Isak Tveitan – ny ID-sjef i POD», 2018
[101] Politiet, «Kripos», u.å.
[102] Politiet, «Kripos – Hovedarbeidsområder», u.å.
[103] Kripos vil få et litt større ansvarsområde for utlendingsforvaltningen med utvidelse med foto og oppholdssaker, og vil stå for den manuelle kontrollen av treff

asylsøkeres identitet[104], herunder fastsettelse. De mottar og registrerer søknad (oppretter sak) fra asylsøkere og foretar undersøkelser om deres reiserute ved ankomst. I tillegg bistår PU politidistriktene med kontrollvirksomhet og identitetsundersøkelser i utlendingssaker hvor det er tvil om søkers identitet. PU har ansvar for å opprette sak i Datasystemet for utlendings- og flyktningsaker (DUF) og tildele asylsøkere et DUF-nummer[105]

- Nasjonalt ID-senter (NID): Et faglig selvstendig ekspertorgan som skal sikre høy kvalitet på ID-arbeidet som gjøres i politiet, utlendingsforvaltningen og hos andre offentlige virksomheter. NID har spisskompetanse på ID- og underlagsdokumenter, tilbyr opplæring og verktøy, samt gir bistand og råd til aktører innen utlendingsforvaltningen og andre norske offentlig organer[106]

- Politidistrikter: I utlendingsforvaltningen (heretter kalt utlendingsforvaltningens førstelinje) er det politidistriktene som mottar, forbereder og behandler søknader om midlertidig og permanent oppholdstillatelse, utlendingspass og reisebevis, samt statsborgerskap.[107] Utlendingsforvaltningens førstelinje har ansvaret for ID-kontroll i saker der de mottar og behandler søknader om visum og oppholdstillatelse. Utlendingsforvaltningens førstelinje utsteder utlendingspass, reisebevis og Schengen-standardiserte oppholdskort. I tillegg har de ansvaret for registreringen av EØS-borgere.[108] I politidistriktene ligger det både passkontor og øvrige politistasjoner og lensmannskontor. Passkontorene har overordnet ansvar for utstedelse av pass og fremtidens nasjonale ID-kort med eID

Utlendingsdirektoratet: UDI som faglig overordnet organ instruerer politiet og utenriksstasjonene i utlendingssaker.[109] UDI har delegert vedtaksmyndighet til politiet i en rekke sakstyper. UDI behandler de sakene som utenrikstjenesten og politiet ikke har myndighet til å avgjøre, og de sakene der det er usikkert om det bør gis oppholdstillatelse. Disse oppgavene inkluderer også fastsettelse og registrering av identitet. UDI behandler søknader om beskyttelse (asyl), besøksvisum, familieinnvandring, oppholdstillatelser for å arbeide og studere, statsborgerskap, permanent oppholdstillatelse og reisedokumenter. De fatter også vedtak om bortvising og utvising.[110]

Utlendingsnemnda (UNE): Klageinstans for utlendingssaker og statsborgersaker. Alle saker som behandles i UNE har først blitt behandlet av UDI.[111] I flere tilfeller innebærer behandlingen av saker å bekrefte og fastsette oppgitt identitet, samt registrere opplysninger. UNE foretar vurderinger av identitet etter samme regelverk som UDI.

Samferdselsdepartementet

Statens vegvesen (SVV): Har blant annet ansvar for gjennomføring av førerprøver.[112] Det er et pågående arbeid med å utrede organiseringen av SVV som forventes å påvirke både SVV og underliggende trafikkstasjoner.[113]

[104] Politiet, «Politiets utlendingsenhet», u.å.
[105] UDI, «UDI rundskriv – Behandling av ny søknad om beskyttelse etter midlertidig bestemmelse i utlendingsforskriften § 8-8 a», 2018
[106] NID, «Om Nasjonalt ID-senter», u.å.
[107] PwC, «Evaluering av Nasjonalt ID-senter», 2013
[108] UDI, «Registreringsbevis for EU/EØS-borgere», u.å.
[109] UDI, «Hvem gjør hva i utlendingsforvaltningen», u.å.
[110] UDI, "Hvem gjør hva i utlendingsforvaltningen», u.å.
[111] UNE, "Om UNE", u.å.
[112] SVV, «Våre oppgaver og roller», 2018
[113] SVV, «Fra regioner til divisjoner», 2019

- Trafikkstasjoner: Registrerer personopplysninger og har ansvar for utstedelse og fornyelse av førerkort, inkludert kontroll av foto/ID

Finansdepartementet

Skatteetaten: Etaten har ansvaret for et oppdatert folkeregister og at skatter og avgifter blir fastsatt og innkrevd på riktig måte.[114] SKD er sentral folkeregistermyndighet (se kapittel 2.2 for beskrivelse av Folkeregisteret).

- Skattekontor: Skattekontorene utsteder skattekort og utfører ID-kontroll i forbindelse med innrullering i Folkeregisteret, når en person flytter til Norge og fyller kravene til bosetting i Norge. Det tildeles i den forbindelse et fødselsnummer eller d-nummer fra Folkeregisteret og fattes vedtak om bosetting.[115] ID-kontroll skjer på 42 utvalgte skattekontor også for aktører som kan rekvirere d-nummer[116]

Kommunal- og moderniseringsdepartementet

Difi: Forvalter den nasjonale felleskomponenten ID-porten og er utsteder av MinID. De er også ansvarlige for felles infrastruktur for eID (ID-porten), samt formidling og forvaltning av og for eID.[117] Regjeringen har besluttet at Difi og Altinn skal samles i et nytt digitaliseringsdirektorat fra 1. januar 2020 som skal ligge under KMD.[118]

Kartverket: Kartverket er ansvarlig for å rekvirere d-nummer for utenlandske personer som trenger det i forbindelse med tinglysning i grunnboken.[119]

Datatilsynet: Datatilsynet fører kontroll med at personvernregelverket etterleves, og medvirker til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem.[120] Datatilsynet har sterk interesse i å sikre at samfunnet har gode byggeklosser for å bekjempe ID-tyveri og følgene av det. På dette området er Datatilsynet en rådgiver og pådriver. Som et tilsynsorgan har de et lovpålagt ansvar innen ID-området i henhold til personopplysningsloven.[121]

Valgdirektoratet: Har ansvar for den operative valggjennomføringen på landsbasis[122] hvor det gjennomføres ID-kontroll når det avgis stemme. Kommunene og fylkeskommunene har ansvar for den praktiske gjennomføringen av valget.

Nasjonal kommunikasjonsmyndighet (Nkom): Er oppnevnt som tilsynsorgan etter lov om elektroniske tillitstjenester.

[114] Skatteetaten, «Samfunnsoppdrag og strategi», u.å.
[115] Lovdata, «Lov om folkeregistrering (folkeregisterloven)», 2016, § 2-2 har regler om hvilke nasjonale identifikasjonsnumre som skal brukes i Folkeregisteret. Skatteetaten tildeler fødselsnumre til personer som er bosatt i Norge, eller norske statsborgere som er bosatt i utlandet. Andre personer kan tildeles d-nummer når det er behov for å registrere dem i det norske Folkeregisteret
[116] Når en virksomhet (f.eks. NAV) rekvirerer et d-nummer med hjemmel i folkeregisterforskriften, får d-nummeret automatisk status «ikke kontrollert» i Folkeregisteret. For at status skal settes til «kontrollert», må personen møte opp hos ett av 42 skattekontorene som har fått i oppgave å gjennomføre ID-kontroll
[117] Difi, «Om Difi», 2019
[118] KMD og FIN, «Samler digitaliseringsinnsatsen i ett direktorat», 2019
[119] Kartverket, «Søknad om d-nummer», 2018
[120] Datatilsynet, «Datatilsynets oppgaver», u.å.
[121] POD, Handlingsplan for ID-området, 2012
[122] Valgdirektoratet, «Mål og samfunnsoppdrag», 2018

Helse- og omsorgsdepartementet

Direktoratet for e-helse: Fag- og myndighetsorgan som skal forvalte og realisere digitale, nasjonale e-helseløsninger som bidrar til en effektiv helsetjeneste med høy kvalitet.[123]

Helsedirektoratet: Instruerer Helfo (rekvirent) som er Helsedirektoratets ytre etat.[124]

- Helfo: Rekvirerer d-nummer for asylsøkere og NATO-personell som skal ha fastlege[125]

Helseforetak: Landets regionale helseforetak har underliggende helseforetak som drifter fødeavdelinger og fødestuer i hele landet.[126]

- Fødeavdelinger og fødestuer: Jordmødre eller leger på fødeavdelinger og fødestuer er ansvarlige for å fastsette identitet ved å sende en fødselsmelding til Skatteetaten for å bekrefte at et barn er født[127]

Arbeids- og sosialdepartementet[128]

Arbeids- og velferdsdirektoratet (NAV): Tilbyr kommunale og statlige tjenester og ytelser[129] og er rekvirent av d-nummer. NAV skal bare rekvirere d-nummer når det er nødvendig for å behandle henvendelse eller sak, forutsatt at de ikke har d-nummer eller fødselsnummer fra før.[130]

- NAV-kontor og NAV Ytelseslinjen: NAV-kontorene registrerer personopplysninger og rekvirer d-nummer for arbeidssøkende EØS-borgere. Ytelseslinjen ved enhetene NAV Arbeid og ytelser, NAV Familie- og pensjonsytelser og NAV Kontroll har hjemmel til å rekvirere d-nummer for alle andre brukere som har rett til å få det.[131] 16 NAV-kontor har sjøfartsfaglige oppgaver og innehar per i dag oppgaven som utsteder og kontrollør av sjøfartsbøker på vegne av Sjøfartsdirektoratet[132]

Arbeidstilsynet: Arbeidstilsynet skal følge opp at virksomheter ivaretar sitt ansvar etter arbeidsmiljølovgivningen og øvrig relevant regelverk som er tillagt tilsynets myndighet. De utsteder HMS-kort.[133]

Nærings- og fiskeridepartementet

Brønnøysundregistrene: Utvikler og driver digitale tjenester som effektiviserer, samordner og forenkler dialogen med det offentlige for privatpersoner og virksomheter. De har forvaltningsansvaret for Altinn frem til 01.01.2020.[134] Digitaliseringsministeren har den faglige styringslinjen i Altinn fra 01.01.2020. Brønnøysundregistrene rekvirerer d-nummer for registrering i foretaksregisteret, enhetsregisteret eller

[123] Direktoratet for e-helse, «Om Direktoratet for e-helse», 2019
[124] Helfo, «Helfos organisasjon», 2019
[125] Skatteetaten, «D-nummer», u.å.
[126] HOD, «De regionale helseforetakene», 2014
[127] Skatteetaten, «Barn født i Norge», u.å.
[128] ASD har det overordnede ansvaret for arbeidsinnvandringspolitikken og saksfeltet som gjelder innreise og opphold i Norge for utlendinger som omfattes av EØS-avtalen eller EFTA-konvensjonen
[129] NAV, «Organisering av NAV-kontoret», 2019
[130] For eksempel ved registrering som arbeidssøker, registrering av opplysninger om medlemskap i folketrygden eller øvrige tjenester og ytelser i NAV
[131] NAV, «Rutine for rekvirering av d-nummer», Oppdatert 24. mai 2018
[132] NAV, «Sjøfartsoppgaver i NAV», 2019. Oppgaven med å utstede sjøfartsbøker vil overtas av politiet i 2020
[133] Arbeidstilsynet, «HMS-kort i bygg og anlegg», u.å.
[134] Brønnøysundregistrene, «Om oss», 2018

løsøreregisteret.[135] Regjeringen har besluttet at Difi og Altinn skal samles i et nytt digitaliseringsdirektorat fra 1. januar 2020. Det kan påvirke Brønnøysundregistrenes rolle i ID-forvaltningen.[136]

Sjøfartsdirektoratet: Direktoratet er eier av ID-beviset Sjøfartsbok og bestemmer form og innhold.[137]

Kunnskapsdepartementet[138]

Integrerings- og mangfoldsdirektoratet (IMDi): Fagorgan med ansvar for å iverksette integreringspolitikken på departementets ansvarsområder med vekt på å styrke kompetanse innen integrering og mangfold, samt bosetting av flyktninger.[139] De utsteder også ID-bevis til statsautoriserte tolker, men dette regnes ikke som godkjent ID.[140]

Utenriksdepartementet[141]

Utenriksstasjoner: Utenriksstasjonene er ansvarlige for utstedelse av pass, grenseboerbevis og diplomatkort i utlandet. Utenriksstasjonene registrerer identiteter, og har ansvaret for ID-kontroll i saker der de mottar og behandler søknader om visum og oppholdstillatelse. Norge hadde per mai 2017 99 utenriksstasjoner[142] fordelt på ambassader (81), faste delegasjoner i multilaterale organisasjoner (7), generalkonsulater (9) og andre representasjoner (2).

Forsvarsdepartementet

Forsvaret: Forsvaret registrerer personopplysninger og utsteder forsvarets ID-kort både for vernepliktige og ulike kategorier av ansatte.[143]

Barne- og familiedepartementet

Departementet har forvaltningsansvar for barneloven som påvirker deler av ID-prosessen.

Interessesammenslutninger

Finans Norge: Har en kontrollfunksjon og et ansvar for å verifisere rett identitet ved samhandling med kundene.[144] Under Finans Norge ligger Bankenes Standardiseringskontor (Bits AS) som har ansvar for å etablere, vedlikeholde og videreutvikle norske bankstandarder som brukes i den felles infrastrukturen.[145]

Styring og koordinering av tjenester i e-forvaltning (Skate): Strategisk samarbeidsråd og rådgivende organ som skal bidra til at digitaliseringen av offentlig sektor blir

[135] Skatteetaten, «D-nummer», u.å.
[136] KMD og FIN, «Samler digitaliseringsinnsatsen i ett direktorat», 2019
[137] Sjøfartsdirektoratet, «Sjøfartsbok», 2015. Sjøfartsbok er et identitetsbevis for norske arbeidstakere på fartøy, samt et dokument for registrering av fartstid fra NOR- eller NIS-registrert skip.
[138] KD har det overordnede ansvaret for integreringspolitikken. Departementet har ansvar for bosetting av flyktninger og forvaltning av statsborgerloven
[139] JD, ASD, KD og UD, «Aktører og ansvarsforhold i utlendingsforvaltningen», 2018
[140] Integrerings- og mangfoldsdirektoratet, «Dette gjør IMDi», 2019
[141] Det er i hovedsak to seksjoner under serviceavdelingen i UD som er involvert i ID-forvaltningen. Seksjon for konsulære saker driver bistand til norske borgere i utlandet og administrasjon av honorære konsulater. Seksjon for utlendingsfeltet har ansvar for den administrative oppfølgingen av utenriksstasjonenes arbeid på utlendingsfeltet, herunder visum og opphold
[142] UD, «Ansvarsområder og oppgaver i Utenriksdepartementet», 2017
[143] JD, «Nasjonalt ID-kort», 2007
[144] POD, «Handlingsplan for ID-området», 2012
[145] Bits AS, «Dette gjør Bits», u.å.

samordnet og gir gevinster for innbygger, næringsliv og forvaltningen. Difi er sekretariat for dette strategiske samarbeidsrådet.[146]

Koordineringsgruppe for ID-forvaltning (KoID): Rådgivende koordineringsgruppe på direktoratsnivå som skal bidra til at identitetsforvaltningen i Norge blir samordnet og gir gevinster for offentlig sektor, innbyggerne og næringslivet. Arbeidet med KoID ble ytterligere detaljert i kapittel 2.9.5.

Norsk senter for informasjonssikring (NorSIS): Er en del av regjeringens helhetlige satsing på informasjonssikkerhet i Norge og er en uavhengig og nøytral aktør. NorSIS gir informasjon om trusler, råd om forebygging og hjelp ved kriminalitet og krenkelse på nettet.[147] De har vist en interesse til å medvirke i ulike temaer innenfor ID-området, blant annet biometri og tiltak for bekjempelse av ID-tyveri.

ID-nettverket: Arbeider for en mer helhetlig ID-forvaltning i Norge og er ett av fire satsningsområder hos NID. Nettverket ble etablert i september 2013, og NID er sekretariat for nettverket som møtes en gang hvert halvår. Nettverket omfatter 18 etater og organisasjoner og er en møteplass for erfaringsutvekslinger, dialog og samarbeid, og skal sørge for nyttig kunnskapsoverføring om utfordringer, strategier og tiltak innen ID.[148]

Internasjonale premissgivere

EU/EØS: Premissgiver og kravstiller til en lang rekke prosessområder og systemer innenfor ID-området. Blant annet utformer EU krav til bruk av standardiserte oppholdskort, krav til bruk av fingeravtrykk i maskinlesbare pass og oppholdskort, og krav til sikkerheten i hvordan medlemsland gis tilgang til fingeravtrykk (EAC). I tillegg utformer EU krav til grense- og ID-kontroll gjennom Schengen regelverket, hvor Schengen Borders Code gir de viktigste føringene. Alle krav som til nå har vært fastsatt av EU innen ID-området er obligatoriske for Norge gjennom Schengen regelverk og EØS avtalen.[149]

International Civil Aviation Organization (ICAO): Utformer krav, spesifikasjoner og beste praksis til pass og reisedokumenter, inkludert bruk av biometri og sertifikater i grensekontroll. De viktigste kravene er samlet i standarden Doc 9303, hvor Norge er pliktig å følge alle minstekrav.[150]

Private aktører

Banker: Registrerer personopplysninger og utsteder bankkort med bilde og BankID.

Private autentiseringsløsninger: Buypass og Commfides utsteder elektroniske ID som benyttes for digital autentisering.

Verdipapirsentralen (VPS): Har rekvirentstatus for d-nummer ved opprettelse av VPS-konto.[151]

[146] Difi, «Skate – styring og koordinering av tenester i e-forvaltning», 2019
[147] NorSIS, «Om NorSIS», u.å.
[148] NID, «Hva er ID-nettverket?», u.å.
[149] POD, Handlingsplan for ID-området, 2012
[150] POD, Handlingsplan for ID-området, 2012
[151] Skatteetaten, «D-nummer», u.å. Verdipapirsentralen oppgir i mailutvekslinger at de ikke rekvirerer d-nummer i praksis.

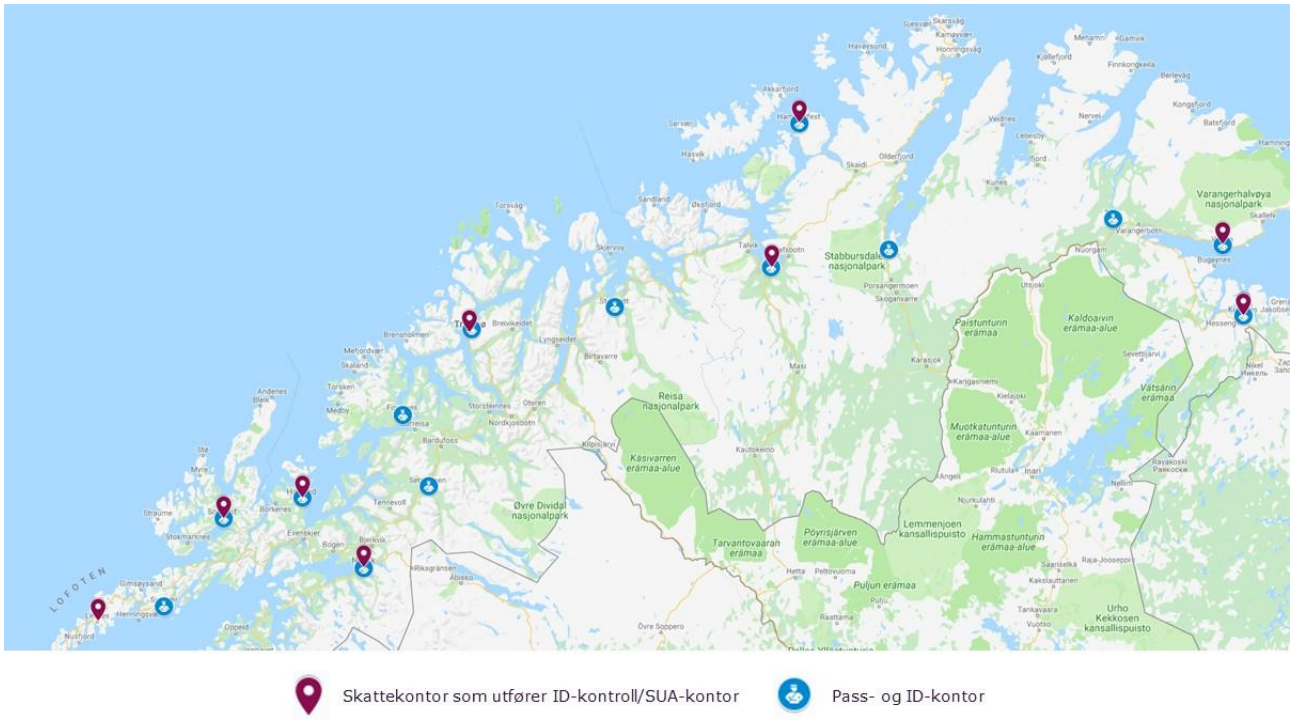
3.1.2 Geografisk tjenestestedstruktur

Det er i dagens struktur en rekke tjenestesteder i førstelinjen hvor brukere kan møte opp for å få utstedt ID-bevis, få veiledning og behandlet saker relatert til ID, slik vist i kapittel 3.1.1 tabell 6. For å gi en oversikt over den geografiske tjenestestedstrukturen til de mest sentrale tjenestestedene i ID-forvaltningen, har leverandøren undersøkt og sammenlignet lokasjonen til de vedtatte pass- og ID-kontorene, skattekontorene som utfører ID-kontroll og Servicesenter for utenlandske arbeidstakere (SUA).

JD har gjennom arbeidet med ny struktur for pass- og ID-kontorer besluttet at dagens 141 passkontor skal reduseres til 78, inkludert pass- og ID-kontor på Svalbard, med grunnlag i kjøretidsberegninger til de ulike lokasjonene. Det er i dag 42 skattekontor som utfører ID-kontroll av brukere, inkludert Svalbard, samt fem SUA-kontorer som utfører ID-kontroller og tilbyr andre tjenester til utenlandske arbeidstakere i Norge. Leverandøren har i analysene av lokasjonene til de nevnte tjenestestedene ekskludert skattekontoret og pass- og ID-kontoret på Svalbard.

Leverandøren har undersøkt luftlinjeavstanden mellom tjenestestedene nevnt over. Funnene viser at 91 prosent av de 46 skattekontorene/SUA-kontorene har et pass- og ID-kontor innen 15 km radius, og at 59 prosent har et pass- og ID-kontor innen 1 km radius. Dette betyr at det er stor grad av geografisk nærhet mellom skattekontorene/SUA-kontorene og de vedtatte pass- og ID-kontorene.

Kartutsnittet i figuren under illustrerer geografisk nærhet mellom pass- og ID-kontorene og skattekontorene/SUA-kontorene.



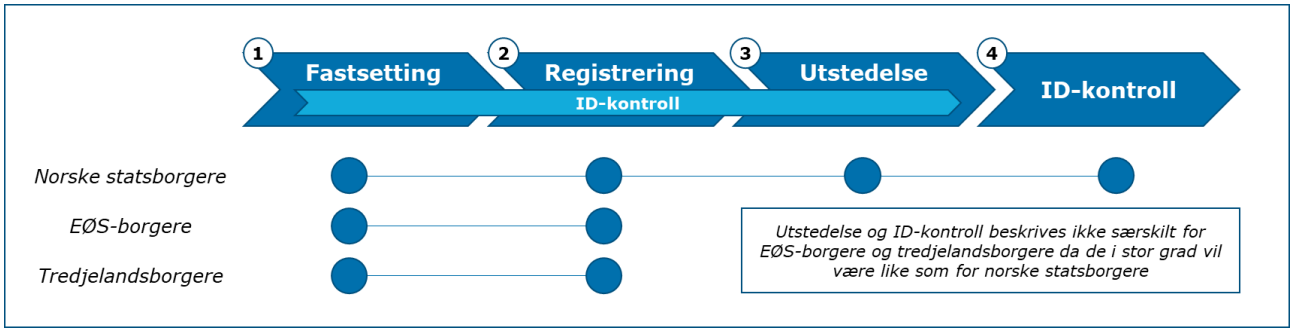
Figur 14 Geografisk nærhet mellom pass- og ID-kontor og skattekontor/SUA-kontor

3.1.3 ID-forvaltningens saksgang fra et aktørperspektiv

I det påfølgende kapittelet vil leverandøren beskrive dagens saksgang relatert til ID fra et aktørperspektiv for de tre brukergruppene i ID-forvaltningen. Det tas utgangspunkt i prosessen i ID-forvaltningen beskrevet i kapittel 2.4 og de overordnede brukerreisene i kapittel 2.6.

Saksgangen frem til en person blir tildelt identitetsnummer i Folkeregisteret vil være svært ulik avhengig av om personen er norsk statsborger, EØS-borger eller tredjelandsborger. Når personen *har* fått et identitetsnummer tildelt i Folkeregisteret vil derimot saksgangen være forholdsvis lik for utstedelse og ID-kontroll for de tre brukergruppene.[152]

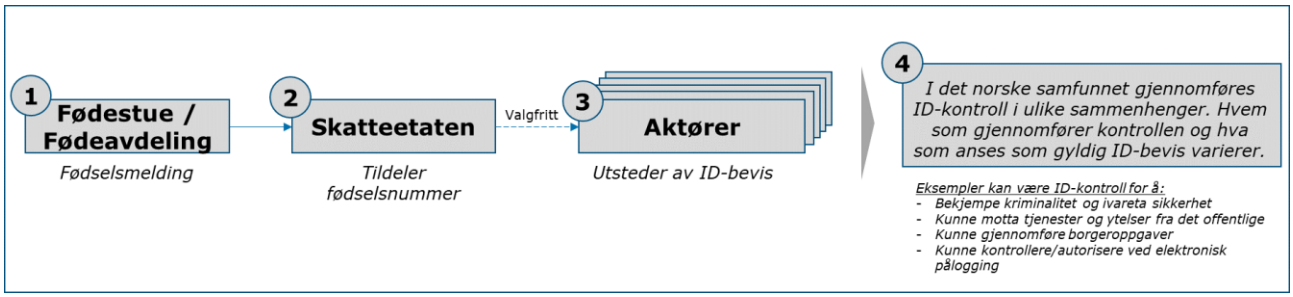
I dette kapittelet vil leverandøren beskrive saksgangen i de fire stegene for norske statsborgere (ved fødsel). For EØS-borgere og tredjelandsborgere har leverandøren fokusert på prosessen frem til tildeling av identitetsnummer i Folkeregisteret. I fastsettingssteget er det viktig å skille utlendingsforvaltningens formål og oppgave med å fastsette identitet på grunnlag av opprinnelig identitet, og Folkeregisterets behov for å "låse" en person til en identitet i Norge.



Figur 15 ID-forvaltningens saksgang i et aktørperspektiv

For tredjelandsborgere er i tillegg prosessen knyttet til visum, statsborgerskap og tilbakekall av statsborgerskap og oppholdstillatelse beskrevet.

Norske statsborgere (ved fødsel)



Figur 16 Saksgang for norske statsborgere (ved fødsel)

Denne prosessen vil gjelde for personer som er norske statsborgere ved fødsel (enten født i Norge eller i utlandet). Prosessen for EØS-borgere eller tredjelandsborgere som søker norsk statsborgerskap beskrives noen avsnitt lengre ned.

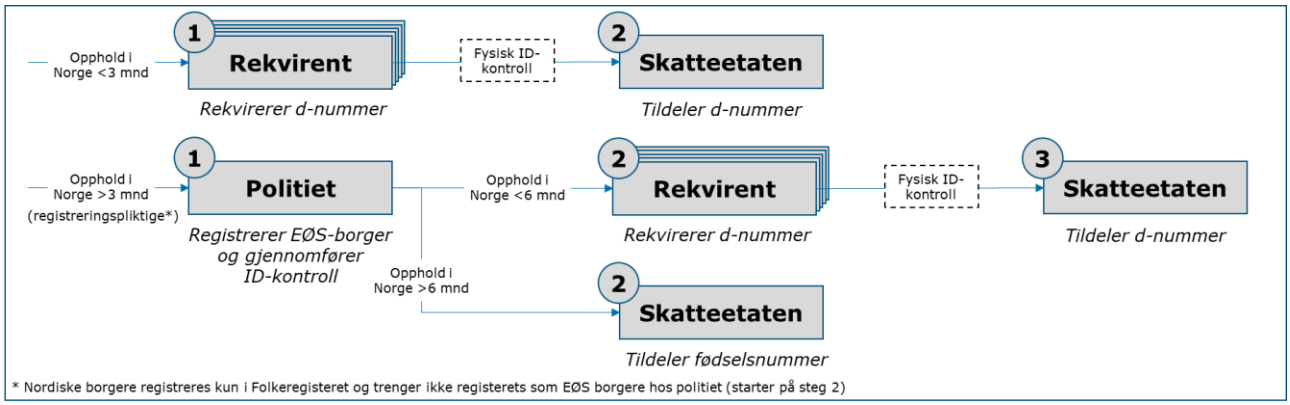
Ved fødsel i Norge fyller fødeavdeling/-stue ut en fødselsmelding (steg 1)[153], hvor melding sendes elektronisk til Skatteetaten. Denne forsendelsen foretas hver 12. time og det etableres et hjelpenummer av helsepersonellet i påvente av tilbakemelding fra Skatteetaten. Hos Skatteetaten opprettes det deretter automatisk et fødselsnummer i

[152] Saksgangen for utstedelse vil være forholdsvis lik, men det påpekes at brukergruppene har krav på ulike dokumenter. Det er for eksempel bare norske borgere som får norske pass, bare personer med flyktningstatus som får reisebevis for flyktninger og bare noen tredjelandsborgere som har rett på utlendingspass

[153] Når barn er født uten at lege/jordmor er til stede må mor selv melde fødsel til Skatteetaten. Om registermyndigheten har kommet til at fremlagte opplysninger ikke gir grunnlag for med rimelig sikkerhet å fastslå familierelasjon, kan mor og barn DNA-testes (Folkeregisterforskriften § 8-4-1)

Folkeregisteret (steg 2).[154] Som norsk statsborger registrert i Folkeregisteret har en person videre mulighet til å søke en rekke ID-bevis (steg 3). Fødes barnet i utlandet, er norsk statsborger ved fødsel og skal bli registrert bosatt i Norge, må foreldrene møte opp med barnet på skattekontor med barnets pass og utfylt flyttemelding (eventuelt også fødselsattest og DNA-test for noen land).[155] Hvis barnet med foreldre skal fortsette å bo i utlandet kan barnet få fødselsnummer i forbindelse med søknad om norsk pass.

EØS-borgere



Figur 17 Saksgang for EØS-borgere

Registreringen av EØS-borgere i Norge avhenger av hvor lenge borgeren skal oppholde seg i landet.

Om borgeren skal være i Norge i **mindre enn tre måneder** kan personen få tildelt et d-nummer om rekvirenten vurderer at det er et begrunnet behov for det.[156] Det er flere aktører som kan rekvirere d-nummer (ref. kapittel 6.1.2) og det er rekvirenten som beslutter hvorvidt det skal gjennomføres kontroll av personen eller ikke (steg 1). En eventuell kontroll gjennomføres på ett av 42 skattekontor. Skatteetaten er som folkeregistermyndighet ansvarlig for å tildele d-nummeret (steg 2).

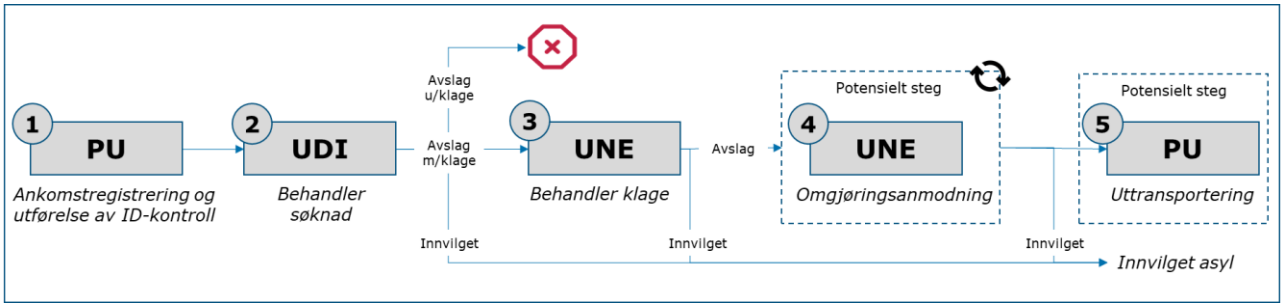
Om borgeren skal være i Norge i **mer enn tre måneder** er det obligatorisk å registrere seg hos politiet (steg 1) for å få et registreringsbevis som bekrefter at du har oppholdsrett i Norge.[157] Dette gjelder kun for ikke-nordiske EØS-borgere. Ved oppmøte hos politiet vil det gjennomføres ID-kontroll. Videre er det igjen to alternativer for tildeling av identitetsnummer i Folkeregisteret. Om personen skal være i Norge i **mindre enn seks måneder**, og rekvirenten vurderer det til å være et begrunnet behov, kan d-nummer rekvireres. Her vil Skatteetaten tildele og registrere d-nummeret i Folkeregisteret på samme måte som i avsnittet over med en potensiell ID-kontroll. Om personen skal være i Norge i **mer enn seks måneder** og ellers fyller vilkårene for bosetting i Norge, tildeles et fødselsnummer og personen registreres i Folkeregisteret som bosatt.

Tredjelandsborgere

I det påfølgende vil leverandøren beskrive saksgangen for søkere av asyl, opphold, visum, og statsborgerskap. Videre vil også saksgangen i tilbakekallssaker av statsborgerskap og oppholdstillatelse beskrives.

[154] Helsenorge, «Farskapserklæring og fødselsmelding», u.å.
[155] Folkeregisterforskriften § 8-4-3 til § 8-4-9
[156] Dette kan eksempelvis være tilfellet om borgeren skal jobbe eller studere i Norge i mindre enn tre måneder
[157] Utlendingsforskriften § 196b

Asylsøkere



Figur 18 Saksgang for asylsøkere

Når en person kommer til Norge og søker asyl har PU ansvaret for ankomstregistrering[158]. Dette innebærer opptak av fingeravtrykk[159] og ansiktsfoto, registrering av opplyste personalia og opprettelsen av et DUF-nummer (steg 1). PU fastsetter ikke identitet i ankomstfasen, men skal ved registrering bidra til å utrede dette så langt det er mulig. Alle asylsøkere får tildelt d-nummer etter rekvirering fra utlendingsforvaltningen.

Da 90-95 prosent[160] av asylsøkere ikke fremlegger reisedokumenter (pass) eller tilsvarende ID-bevis er det først og fremst søkerens egne opplysninger utlendingsforvaltningen tar utgangspunkt i. Det stilles spørsmål og eventuelt kontrollspørsmål til søkeren. Søkeren blir orientert om plikten til medvirkning for klarlegging av identitet og bedt om å legge frem all dokumentasjon som kan ha betydning for ID-fastsetting. Ved behov kan eventuelle tvangsmidler benyttes for å belyse saken (ransaking, gjennomgang av mobile enheter, eller lignende). Når UDI mottar saken for behandling gjennomfører de asylintervju (steg 2). UDI vil også følge opp med spørsmål knyttet til søkerens identitet og bakgrunn. Som dokumentasjon på at søkeren har lov til å oppholde seg i Norge mens søknaden er til behandling, får vedkomne utstedt et asylsøkerbevis[161].

Om det er momenter ved saken som tilsier at søknaden skal avslås, ut ifra opplysninger fra søkerens side og landinformasjon, tar ikke UDI eller UNE stilling til om utlendingens identitet er sannsynliggjort.[162] Dette gjelder derimot ikke om identiteten er sannsynlig og dokumentert med reisedokument eller tilsvarende ID-dokument, eller om det foreligger opplysninger som tilsier at det er meget sannsynlig at utlendingens opplysninger om identitet er korrekte.

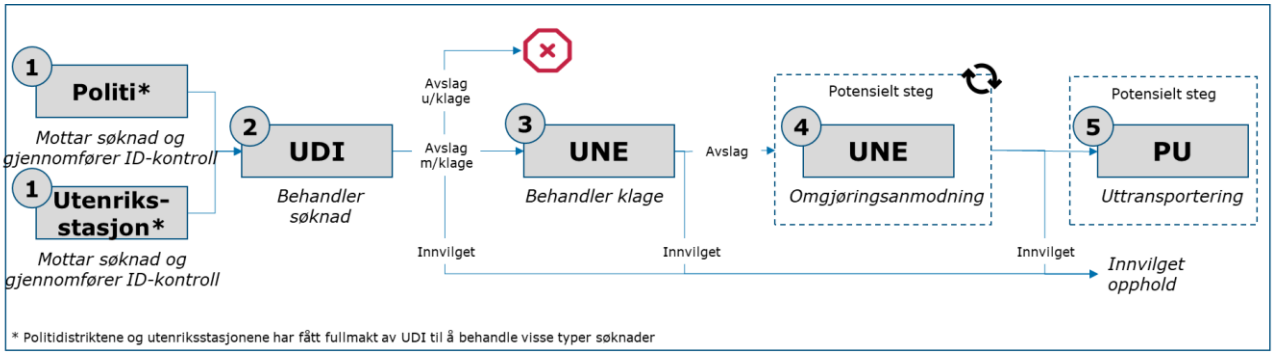
Dersom søknaden innvilges må UDI eller UNE alltid ta stilling til spørsmålet om identitet, og foreta en bevisvurdering av alle opplysninger i saken som har betydning for ID-fastsettelse.

Dersom søker får avslag og velger å påklage denne avgjørelsen behandles saken av UNE (steg 3). Dersom UNE fastholder avslaget kan søkeren kreve omgjøringsanmodning[163] (steg 4). UNE tar også stilling til identiteten ved klage eller omgjøringsanmodning. Dersom avslagsvedtaket opprettholdes må personen reise ut

[158] UDI, «UDI rundskriv», 2018
[159] PU oppgir at fingerbiometri tas to ganger for asylsøkere ved ankomst. Første gang på en maskin som søker opp mot VIS (kontrollsøk mot straffesaksregisteret og lagring av biometri i utlendingsdatabasen). Andre gang på en annen maskin som søker opp mot Eurodac (søk for å kontrollere om personen har søkt asyl tidligere). Denne prosessen beskrives som svært arbeidskrevende og kan ta opp mot 20 minutter per asylsøker, og enda lenger tid i de tilfeller hvor asylsøker har mange treff i Eurodac og VIS
[160] Informasjon mottatt direkte fra UNE
[161] Kortene er basert på søkers egne opplysninger og inneholder ellers få sikkerhetselementer
[162] Oppgitt i samtale med UNE
[163] Personer som har fått sin søknad avslått kan be UNE om å se på saken på nytt. Dette er kjent som omgjøringsanmodning

av landet, skjer ikke dette frivillig kan PU bistå med eventuell uttransportering (steg 5). I forbindelse med effektuering av avslagsvedtak vil PU gjennomgå saken og identitetsopplysningene. Om det er nødvendig å gjennomføre retur er det sentralt at identiteten er fastsatt og akseptert av hjemlandet.

Søkere av oppholdstillatelse



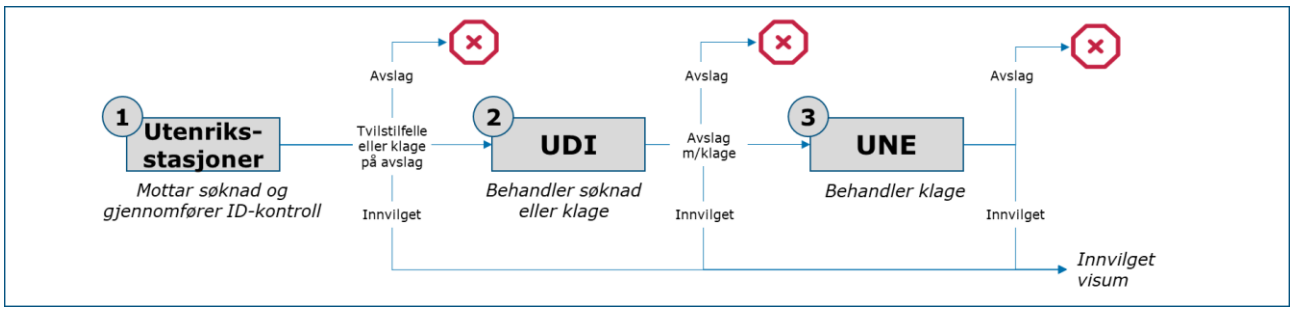
Figur 19 Saksgang for søkere av oppholdstillatelse

Søkere av oppholdstillatelse kan være arbeidsinnvandrere, studenter, familieinnvandrere med flere. Oppholdssøknad mottas både i og utenfor Norge (steg 1). Søknader i Norge mottas av lokalt politi, mens søknader utenfor Norge mottas av utenriksstasjonene. Politidistriktene og utenriksstasjonene har fått delegert vedtaksmyndighet av UDI til å behandle visse typer saker.[164]

Dersom politidistrikter eller utenriksstasjon ikke har vedtaksmyndighet sendes søknaden til UDI for behandling (steg 2). Dersom søknaden får avslag av UDI og søker velger å påklage denne avgjørelsen havner saken hos UNE som behandler klagen (steg 3). Ved avslag kan søker be om omgjøringsanmodning (steg 4). Dersom avslagsvedtaket opprettholdes må personen reise ut av landet. Om dette ikke skjer frivillig kan PU bistå med eventuell uttransportering (steg 5).

For alle søkere som får oppholdstillatelse (med noen få unntak), sendes det automatisk melding om innvilget opphold fra UDI til Folkeregisteret. Deretter får disse tildelt identitetsnummer. Ved innvilget opphold blir det også utstedt oppholdskort (ved å møte opp hos politiet og bestille dette) som beviser at personen har fått oppholdstillatelse i Norge.

Visumsøkere



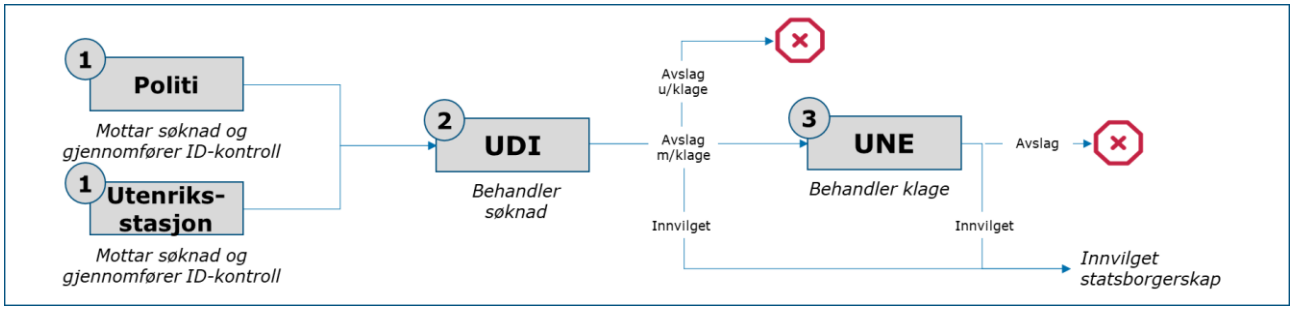
Figur 20 Saksgang for visumsøkere

Visumsøknad mottas av utenriksstasjonene som for enklere søknader har vedtakskompetanse (steg 1). Dette gjelder de aller fleste søknader. Mottak av søknader

[164] Informasjon mottatt fra UDI

er ved nesten alle utenriksstasjoner satt ut til eksterne tjenesteytere. Visum er delt inn i ulike kategorier etter hva som er formålet med tillatelsen.[165] I tvilstilfeller eller ved klage på avslag fra utenriksstasjonene sendes saken videre til UDI for behandling (steg 2). Dersom visumsøknaden får avslag hos UDI kan søkeren klage på vedtaket. Klagen behandles siden av UNE (steg 3). Ved innvilget visum får personen rett til å oppholde seg i Norge så lenge visumet tilsier. I noen tilfeller mottar politiet søknad om forlengelse av visum eller om ekstra innreise.[166] I tilfellene politiet er delegert vedtaksmyndighet behandler de søknaden og effektuerer vedtaket. Det samme gjelder for UDI der de har vedtaksmyndighet.

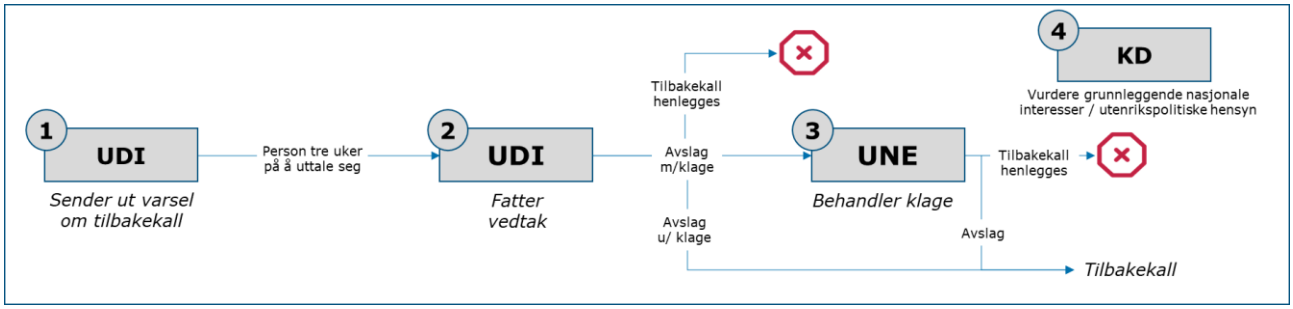
Søkere om statsborgerskap



Figur 21 Saksgang for søkere om statsborgerskap

Søknader og meldinger om norsk statsborgerskap innleveres til norsk politi eller norsk utenriksstasjon (steg 1).[167] Søknaden om statsborgerskap behandles siden av UDI (steg 2). Det er visse vilkår som må oppfylles for å få statsborgerskap og disse følger av statsborgerloven og -forskriften. Dersom søknaden får avslag og vedkommende klager på vedtaket, blir klagen behandlet av UNE (steg 3). Om søknad blir innvilget er personen norsk statsborger med alle rettigheter dette innebærer.

Tilbakekallssaker



Figur 22 Saksgang ved tilbakekallssaker

Tilbakekall kan forekomme i saker hvor en person har fått innvilget oppholdstillatelse[168] og i saker hvor statsborgerskap har blitt innvilget[169] på grunnlag av uriktige opplysninger[170]. Status som flyktning kan også tilbakekalles i visse tilfeller.[171] Det meste av tilbakekallssaker oppdages i politidistriktene eller av PU. UDI ber politiet

[165] UDI, «Generelt praksisnotat for visum», 2010
[166] UDI, «RS 2010-168», 2014
[167] KD, «Statsborgerskap og statsborgerloven», 2018
[168] Lovdata, «Lov om utlendingers adgang til riket og deres opphold her (utlendingsloven), § 63», 2008
[169] UDI, «Tilbakekall av statsborgerskap», 15.01.2017
[170] I noen tilfeller kan tillatelser tilbakekalles selv om det ikke er gitt uriktige opplysninger og vedtaket i utgangspunktet var riktig – f.eks. hvis man forlater Norge og oppholder seg i hjemlandet eller annet land i mer enn 6 måneder av en tillatelsesperiode på ett år
[171] Etter betingelser i utlendingsloven § 37

foreta intervju av personen slik at vedkomne får forklart seg om forholdet. Deretter sender UDI ut et varsel om tilbakekall (steg 1). Personen har da tre uker på å komme med en uttalelse i saken. UDI tar deretter en endelig avgjørelse (steg 2), som igjen kan påklages til UNE (steg 3).

Tilbakekall av statsborgerskapssaker er per september 2019 berostilt ved instruks fra departementet.[172] Dette skyldes at det per i dag ligger en sak på høring som gjelder domstolsbehandling av saker om tilbakekall av statsborgerskap der det forslås alternativer for endringer i statsborgerloven som fastsetter at saker for tilbakekall av statsborgerskap skal behandles av domstolen i førsteinstans.[173] Det er over 800 tilbakekallssaker som avventer dette lovforslaget.[174]

I juli 2019 sendte KD ny instruks til UDI og UNE som fastsetter at statsborgerskap kan tilbakekalles dersom hensyn til grunnleggende nasjonale interesser eller utenrikspolitiske hensyn skulle tilsi det. Dette er et unntak av den ovennevnte berostillingen av tilbakekall av statsborgerskapssaker. Saker som angår grunnleggende nasjonale interesser eller utenrikspolitiske hensyn skal fra nå sendes fra UDI til KD for vurdering. KD kan i disse tilfellene instruere UDI i hva de skal gjøre med saken (steg 4).[175]

Generelt om domstolsbehandling i utlendingsforvaltningen

Alle negative vedtak UNE fatter kan bringes inn for domstolene dersom utlendingen tar dette skrittet.[176] Hvis UDI er klageinstans kan også UDIs vedtak bli brakt inn for domstolene.

Domstolene kan bare vurdere om vedtaket er gyldig eller ikke gyldig (korrekte faktum, rettsregler og god nok saksbehandling). Domstolene kan ikke gi tillatelser eller rettigheter etter utlendingsloven. Mener domstolen et vedtak er ugyldig, må UNE/UDI behandle saken på nytt. Hvis det f.eks. er feil i saksbehandlingen, kan UNE/UDI rette dette og saken kan etter omstendighetene få samme resultat.

3.1.4 Registre og saksbehandlingssystem i ID-forvaltningen

Det finnes ikke en enhetlig definisjon av begrepet ID-register eller tilsvarende. I henhold til politiregisterloven er et register en samling av opplysninger som er lagret systematisk på en slik måte at opplysninger om den enkelte kan finnes igjen.[177] Denne definisjonen er tilnærmet identisk med definisjonen SSB benytter.[178]

Det eksisterer heller ikke noen samlet registeroversikt over registre og saksbehandlingssystemer som er involvert i ID-forvaltningen i Norge. Formålet med det enkelte register er lovregulert. Regelverkene omfatter gjerne hvilke opplysninger som kan lagres, hva de kan benyttes til og i hvilken utstrekning de kan deles med andre. Det eksisterer en rekke register og saksbehandlingssystemer som er en del av ID-forvaltningen.

[172] KD, «Rundskriv - Instruks om berostillelse av saker om tilbakekall av statsborgerskap etter statsborgerloven § 26 annet ledd», 2019
[173] KD, «Høringsnotat – Forslag til endringer i statsborgerloven (domstolsbehandling av saker om tilbakekall av statsborgerskap)», 2018. Svarfristen gikk ut i november 2018, men prosessen er tidkrevende og lovforslag er ikke lagt frem for Stortinget pt.
[174] Informasjon oppgitt i samtaler med UDI
[175] Regjeringen, «UDI har fått ny instruks om tilbakekall av statsborgerskap», 2019
[176] Informasjon oppgitt i samtaler med UNE
[177] Lovdata, «Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven), § 2», 2010
[178] SSB, «Noen sentrale begreper knyttet til metadata – til bruk i SSBs felles metadatasystemer», u.å.

Leverandøren har i områdegjennomgangen fokusert på registre med personopplysninger. Omfanget i kartleggingen av registre avgrenses mot virksomhetsregistre og landsregistre som illustrert under.

Figur 23 Ulike registertyper

Videre er det mange registre som er avhengige av en god helhetlig ID-forvaltning, men anses utenfor omfanget i denne områdegjennomgangen. Eksempler på dette er Førerkortregisteret, Brønnøysundregisteret, Elvirksomhetsregisteret, Enhetsregisteret, Konkursregisteret, Kontakt- og reservasjonsregisteret, Løsøreregisteret, MVA-registeret, Aa-registeret (arbeidsgiver- og arbeidstakerregisteret), og øvrig registerforvaltning i NAV.

I det påfølgende har leverandøren benyttet følgende kategorisering av registre:

- Forvaltningsregister: Registre for forvaltningens behandling av opplysninger med nærmere bestemte forvaltningsmessige formål
- Politiregister: Register for politiets behandling av opplysninger til politimessige formål. Reguleres av politiregisterloven og politiregisterforskriften
- Internasjonale registre: Sentrale registre hvor databehandlingsansvarlig er en internasjonal organisasjon/konstellasjon og det eksisterer en samhandling med norske registre
- Nasjonale og internasjonale etterlysningsregistre: Sentrale registre hvor databehandlingsansvarlig er en internasjonal organisasjon/konstellasjon og det eksisterer en samhandling med politiets registre eller saksbehandlingssystem
- Saksbehandlingssystem: Systemer for elektronisk saksbehandling

Leverandøren har valgt å ikke vektlegge registre som benyttes som støtte i saksbehandlingen eller registre som fortsatt er under planlegging. Med registre som benyttes som støtte i saksbehandlingen mener leverandøren registre som benyttes som oppslagsverk for saksbehandlere i deres arbeid med ID-kontroll. Eksempler på dette er blant annet ID-databasen drevet av NID[179] og ICAO PKD[180]. Eksempler på registre som fortsatt er under planlegging er Nasjonalt ID-kortregister, Registered Traveller Programme (RTP) og Entry/Exit System (EES).

Nedenfor følger en overordnet beskrivelse av alle relevante registre og hvem som er behandlingsansvarlig.[181] I figur 24 har leverandøren inkludert en overordnet fremstilling av hvilke registre og saksbehandlingssystemer som samhandler, og satt dette i sammenheng med prosessen for dagens ID-forvaltning.

[179] ID-databasen bistår med informasjon til saksbehandlere som kontrollerer ID, både ved passkontorer og utenriksstasjoner
[180] ICAO PKD Internasjonalt register som inneholder statusinformasjon om alle medlemslandenes (65) sertifikater som bekrefter ekthet på reise-, rettighets- og identifikasjonsdokumenter
[181] Lovdata, «Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven), § 2» , 2010, *«Behandlingsansvarlig er den som etter lov og forskrift alene eller sammen med andre bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes»*

Oversikt over direktetilgang/utlevering i de ulike registrene er hjemlet i lov og beskrives i kapittel 4.1.

Forvaltningsregistre

- Folkeregisteret (Freg): Inneholder blant annet administrative identifikasjonsnummer (fødselsnummer eller d-nummer) for personer som er bosatt i Norge eller som har en tilknytning til Norge som gir et behov for dette. Folkeregisteret mottar sine data fra blant annet helseforetak, utlendingsdatabasen eller fra d-nummerrekvirenter. Registeret danner grunnlaget for blant annet skattemanntallet, valgmanntallet og befolkningsstatistikken og er forutsetning for at alle borgere skal motta informasjon fra offentlige myndigheter, og at deres rettigheter og plikter blir ivaretatt.[182] SKD er sentral registermyndighet og behandlingsansvarlig for Folkeregisteret[183]

- Passregisteret: Inneholder personopplysninger, biometri i form av ansiktsfoto[184] og signatur på alle som har fått utstedt norsk pass. I registeret inntas opplysninger som er nødvendig for forvaltning av registeret og utstedelse av pass.[185] Politiet og grensekontrollmyndighetene kan hente ut opplysninger fra passregisteret på grunnlag av bestemmelsene som er satt i passloven. POD er behandlingsansvarlig for passregisteret

- Utlendingsdatabasen (UDB): Det sentrale registeret i utlendingsforvaltningen hvor alle saker som er behandlet etter statsborgerskap- eller utlendingsloven, som for eksempel søknad om visum, opphold, statsborgerskap og beskyttelse i Norge. Dataene som lagres er hovedsakelig hentet fra søknadsskjemaet, søknadsdokumentene, vedtaksdata, samt informasjon som søker oppgir under et eventuelt intervju. Det lagres også et ansiktsfoto av alle søkere. Ansiktsfotoene skal imidlertid overføres til ABIS (ref. punkt om biometrisystem nedenfor). Videre inneholder databasen informasjon om utlendinger som oppholder seg i asylmottak.[186] For oppholds-søkere blir personopplysningene automatisk overført fra UDB til Folkeregisteret nå når utlendingsmyndighetene innvilger oppholdstillatelse[187], for asylsøkere skjer dette allerede når søknad registreres av politiet første gang[188]. De viktigste saksbehandlingssystemene som er tilknyttet utlendingsdatabasen er DUF, NORVIS og SESAM (omtalt lenger ned).[189] *UDI er «behandlingsansvarlig for UDB, men Justis- og beredskapsdepartementet, UNE, utenriksstasjonene og politiet har tilgang til opplysninger i denne databasen både for å ivareta egne behandlingsformål og for å bistå UDI i saksbehandlingen. UNE har selvstendig behandlingsansvar for egne behandlingsformål. Eksempelvis er det politiet som foretar ankomstregistrering av en asylsøker og som legger disse opplysningene inn i Utlendingsdatabasen som databehandler for UDI. UNE har tilgang til opplysningene i Utlendingsdatabasen for å avgjøre klager på vedtak som er fattet av UDI»*[190]

[182] Skatteetaten.no, «Dette er Folkeregisteret», u.å.
[183] Lovdata, «Lov om folkeregistrering (folkeregisterloven), § 1-3», 2016
[184] Et bilde av fingeravtrykkene lagres i passets elektroniske brikke og blir deretter slettet fra saksbehandlingssystemet og opptaksutstyret for biometri (omtales nærmere i kapittel 6.1.5)
[185] Lovdata, «Lov om pass (passloven), § 8», 1997
[186] NID, «Biometri og identitet – Utfordringer og nye muligheter for utlendingsforvaltningen», 2013
[187] UDI rundskriv, 2019
[188] Basert på epostkorrespondanse med PU
[189] Simonsen Vogt Wiig, «Samtykke som rettslig grunnlag for utlendingsforvaltningens adgang til å registrere og behandle personopplysning», 2015
[190] Simonsen Vogt Wiig, «Samtykke som rettslig grunnlag for utlendingsforvaltningens adgang til å registrere og behandle personopplysning», 2015

- Utlendingsregisteret: Register for fingeravtrykk som opptas av utlendinger som søker om beskyttelse i Norge, når personen ikke kan dokumentere sin identitet eller når det er grunn til å mistenke at søker oppgir falsk identitet. Videre vil det tas fingeravtrykk av utlendinger som blir utvist eller bortvist fra Norge. Registeret er en avgrenset del av politiets fingeravtrykksdatabase. Når det opptas nye fingeravtrykk søkes det mot allerede lagrede fingeravtrykk. Fra november 2019 utvides utlendingsregisteret med et fotoregister, og automatisk ansiktssammenligning blir innført som ny metode. UDI er behandlingsansvarlig for utlendingsregisteret, mens Kripos er databehandler

Politiregistre

Det eksisterer totalt 19 ulike politiregistre som benyttes ved straffesaksbehandling eller til forebygging og bekjempelse av straffbare handlinger.[191] Kripos har behandlingsansvar for 17 av de 19 politiregistrene (se vedlegg 5 for oversikt). I tillegg har Økokrim ansvar for Hvitvaskingsregisteret og Politiets IKT-tjenester har ansvar for Utlendingssystemet (se under).

Saksbehandlingssystem

- Datasystem for utlendings- og flyktningsaker (DUF): Ett av utlendingdatabasens tilhørende saksbehandlingssystem. DUF brukes blant annet for behandling av søknader om beskyttelse eller oppholdstillatelse.[192] Hva som registreres av informasjon varierer basert på sakstype. Felles for alle saker i DUF er at utlendingen tildeles en unik personidentifikator (DUF-nummer). Løsningen brukes også til klagebehandling av UNE. UDI er behandlingsansvarlig for DUF

- Basis Løsning (BL): Saksbehandlingssystem for politiet. I BL opprettes, lagres og registreres alle dokumenter og opplysninger i hele straffesakskjeden. BL har kobling mot fødselsnummer i Folkeregisteret, men ikke DUF-nummer fra UDB, som må legges inn manuelt. Politidistriktene er behandlingsansvarlig

- Norsk Visumsystem (NORVIS): Saksbehandlingssystem for alle visumsaker som utlendingsforvaltningen mottar. NORVIS er den nasjonale enheten tilknyttet VIS (ref. internasjonale etterlysningsregistre) hvor formålet er å legge til rette for utveksling av opplysninger i forbindelse med behandling av visumsøknader og for identifisering blant annet ved innreise ved Schengens yttergrense.[193] Løsningen brukes også til registrering av oppholdssøknader. UDI er behandlingsansvarlig

- Utlendingssystemet (UTSYS): Politiets saksbehandlingssystem som benyttes til ID-fastsettelse, internering og uttransportering. UTSYS henter informasjon fra UDB og politiets sentrale systemer og suppleres med informasjon fra PU. PU er behandlingsansvarlig

- Grense- og territorialkontrollsystemet (GTK): Teknisk hjelpemiddel som brukes til å gjennomføre inn- og utreisekontroll ved å verifisere om utlendinger fyller vilkårene for å reise inn i eller ta opphold i riket.[194] Formålet med GTK er blant annet å bidra til effektiv oppgaveløsning og notoritet ved inn- og utreisekontroll og utlendingskontroll på territoriet. GTK har i hovedsak karakter av å være en

[191] Datatilsynet, «Om politiregisterloven», u.å.
[192] JD, «Høringsnotat – politiets tilgang til opplysninger fra utlendingsmyndighetenes registre», 2016
[193] SVW, «Samtykke som rettslig grunnlag for utlendingsforvaltningens adgang til å registrere og behandle personopplysning», 2015
[194] JD, «Prop. 161 L (2016-2017) – Lov om grensetilsyn og grensekontroll av personer (grenseloven)», 2017

portal for kontroll av opplysninger mot andre systemer, men visse opplysninger registreres og lagre for å gi grunnlag for den nødvendige kontrollen. GTK er derfor også et register. Kripos er behandlingsansvarlig for GTK

- PassWeb: Et saksbehandlingssystem der data for passøknader sendes til produksjon av pass og for lagring i passregisteret[195]

Tabellen nedenfor oppsummerer saksbehandlingssystemene beskrevet overfor, samt hvem som er brukere av dem.

Saksbehandlingssystem	Brukere
DUF	Politidistriktene, PU UDI, UNE, Skatteetaten[196]
BL	Politidistriktene, PU
NORVIS	UDI, UD v/utenriksstasjoner, Politidistriktene, PU
SESAM	UDI og asylmottakene
UTSYS	PU og politidistriktene
GTK	Politidistriktene

Tabell 7 Brukere av saksbehandlingssystem i ID-forvaltningen[197]

Biometrisystem

- Automated Biometric Identification System (ABIS): Et system med underliggende kilder (registre med biometrisk personinformasjon). Forenklet kan man si at formålet med systemet er søk og sammenligning av biometrisk personinformasjon og analyse av treff. Når det er hjemmel for søk mellom register, kan det legges inn funksjonalitet for det i ABIS. Løsningen er både en database med ulike registre og en saksbehandlingsløsning som benyttes av Kripos

- Biometric data transmission (Biometra): Programvare for opptak/lesing av biometrisk personinformasjon. Dette benyttes blant annet i passleseren som benyttes på lufthavner. Løsningen brukes i tillegg av PU og hos politidistriktene for opptak av biometri til ABIS av både de som søker om beskyttelse og de som etterforskes for lovbrudd

Internasjonale registre

- European Asylum Dactyloscopy Database (Eurodac): Et sentralt elektronisk fingeravtrykkregister over utlendinger (hovedsakelig asylsøkere) som er registrert i land som deltar i Dublin-samarbeidet.[198] Formålet med registeret er å finne ut om en asylsøker tidligere har søkt beskyttelse i et annet land som er tilknyttet Eurodac. Fingeravtrykkene i Eurodac blir slettet etter 10 år, eller når det kommer melding om at personen har fått statsborgerskap i et av landene

[195] NID, «Biometri og identitet – Utfordringer og nye muligheter for utlendingsforvaltningen», 2013
[196] Flere saksbehandlere i Skatteetaten hadde inntil 2018 lesetilgang til DUF. Det er nå erstattet med systemet OHS som henter informasjonen fra DUF
[197] NID, «Biometri og identitet – utfordringer og nye muligheter for utlendingsforvaltningen», 2013 og epostkorrespondanse med PU
[198] UDI, «Dublin-samarbeidet», u.å.

som deltar i samarbeidet. Det er UDI som er behandlingsansvarlig for opplysningene som registreres i Eurodac, mens det er politiet som sender og mottar fingeravtrykkopplysninger[199]

- Visa Information System (VIS): Schengens visuminformasjonssystem som lagrer personopplysninger og biometri av visumsøkere. Består av et sentralt internasjonalt system og medlemstatenes nasjonale systemer.[200] Som nevnt tidligere er det UDI som er behandlingsansvarlig for den norske delen av VIS (NORVIS)

Internasjonale etterlysningsregistre

- Schengens informasjonssystem (SIS II): Et elektronisk informasjonssystem hvor etterlyste personer, personer med innreiseforbud og stjålne gjenstander registreres, som et hjelpemiddel i forbindelse med utlendingskontroll og pågripelse av etterlyste personer. Kan registrere biometri. Kripos er behandlingsansvarlig for den nasjonale delen av SIS-systemet. Utlendingsmyndighetene har på bestemte vilkår tilgang til opplysninger som er lagret i SIS

- Interpol: Administrerer 17 registre som kan benyttes av Interpols medlemsland. Eksempler på registre er DNA-profiles, Facial Recognition System og Stolen and Lost travel Documents (SLTD)[201]

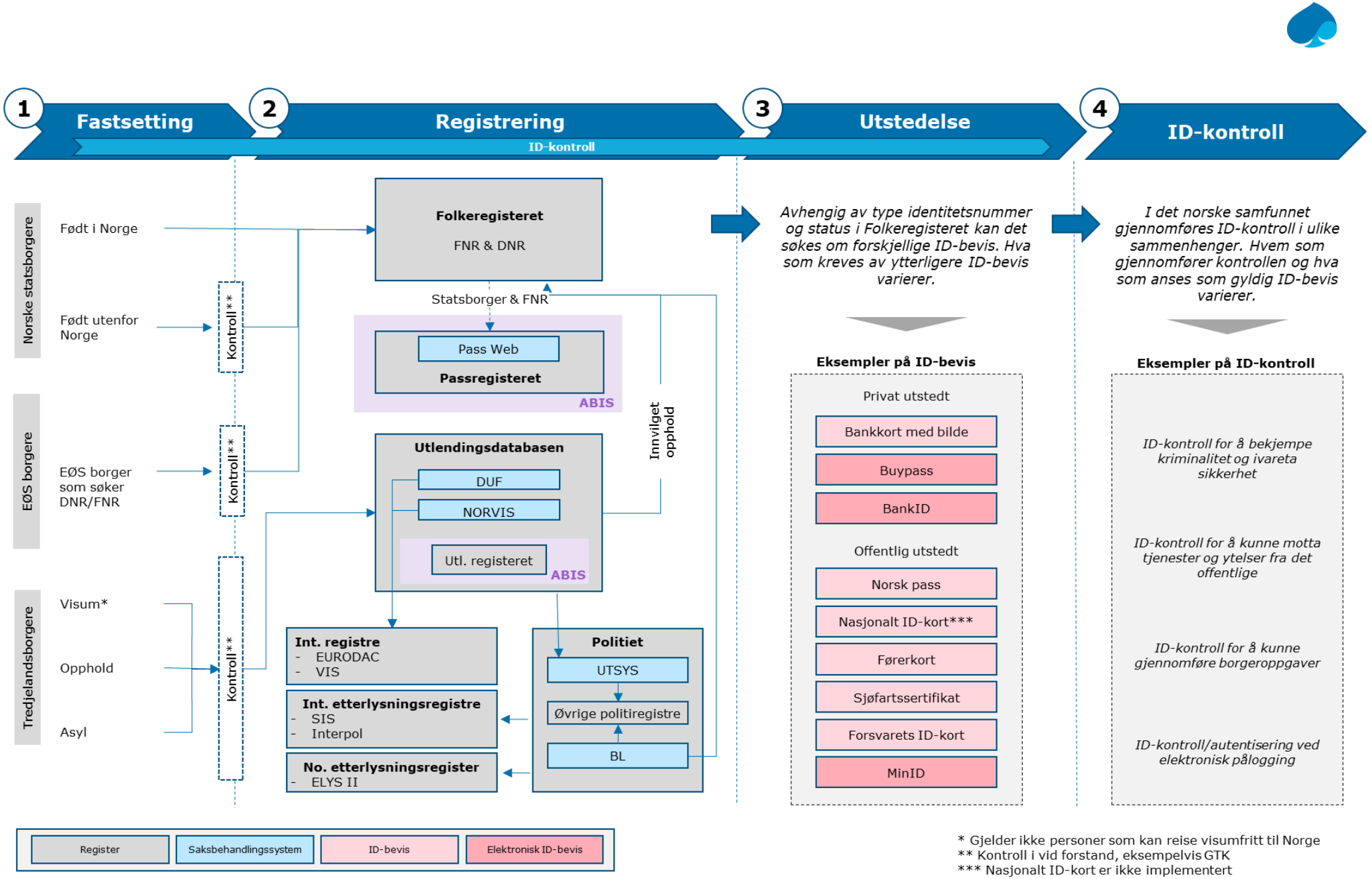
Nasjonale etterlysningsregistre

- ELYS II: Politiets sentrale etterlysningsregister som blant annet omfatter etterlyste personer, kjøretøy, kjennetegn, våpen pass, båter og båtmotorer[202]

Det er flere pågående forbedringsinitiativ knyttet til ulike deler av registrene i ID-forvaltningen. Herunder modernisering av UDB, utvidet bruk av biometri i utlendingsforvaltningen og modernisering av Folkeregisteret. For øvrige pågående tiltak se kapittel 2.9.6.

Figuren på neste side gir en overordnet fremstilling av leverandørens forståelse av registre og saksbehandlingssystemer og hvordan de samhandler med hverandre og deler data.[203] Oversikten er verifisert med sentrale aktører i ID-forvaltningen.

[199] UDI, «Informasjon om Eurodac til den som registreres i Eurodac (RS 2010-019V)», 2010
[200] NID, «Biometri og identitet – Utfordringer og nye muligheter for utlendingsforvaltningen», 2013
[201] Interpol, "Our 17 databases", u.å.
[202] NID, «Biometri og identitet – Utfordringer og nye muligheter for utlendingsforvaltningen», 2013
[203] EØS-borgere skal registrere seg hos politiet om oppholdet i Norge overstiger tre måneder. Politiet vil da registrere EØS-borgeren i utlendingsdatabasen. Dette er ikke lagt inn i illustrasjonen «Overordnet fremstilling av samhandling mellom registre og saksbehandlingssystemer i ID-forvaltningen» da prosessen for registrering i utlendingsdatabasen er svært ulik for EØS-borgere og tredjelandsborgere. For EØS-borgere vil det ikke opptas biometri og ID-kontrollen vil være mye mindre omfattende. EØS-borgere får heller ikke får innvilget opphold på samme måte som tredjelandsborgere da de har en rett til å oppholde seg i Norge utfra sin status som EØS-borger i henhold til EØS-avtalen.



Figur 24 Overordnet fremstilling av samhandling mellom registre og saksbehandlingssystemer i ID-forvaltningen

3.1.5 Styring og struktur hos utenlandske aktører

Dette kapittelet beskriver kort ID-forvaltningen i Sverige, Danmark, Storbritannia og Latvia med tanke på om det eksisterer en aktør med helhetlig ansvar for ID-forvaltningen, samt om landet har et sentralt register, tilsvarende Folkeregisteret. Hensikten er å synliggjøre enkelte sentrale elementer tilknyttet styring og struktur for sammenlignbare land. Datagrunnlaget for informasjon om utenlandske aktører ble beskrevet i kapittel 1.3.

Ved gjennomgang av dokumentasjon fremstår forvaltningen i Sverige, Danmark og Storbritannia som fragmentert, da ingen av landene har en aktør som har det helhetlige ansvaret for ID-forvaltningen. I Latvia er derimot forvaltningen samlet i et organ- The Office of Citizenship and Migration Affairs (OCMA) er underlagt Innenriksdepartementet.

Sverige, Danmark og Latvia har et sentralt register, tilsvarende det norske Folkeregisteret. Storbritannia har ikke et slikt sentralt register, men heller sektorvise registre som tjener ulike formål. Eksempelvis har the Department for Work and Pension-Welfare (DWP) et register som benyttes for å administrere velferdsstatens oppgaver, Her Majesty's Revenue and Customs (HMRC) et register for skatteformål og National Health Sector (NHS) et register over helsejournaler. DWP og HMRC bruker et National Insurance Number (NI) som den primære identifikatoren, mens NHS benytter et NHS nummer. DWP og HMRC deler noe informasjon og ansvaret overlapper i enkelte tilfeller, men det er ingen link mellom NHS og CIS/HMRC.

	Sverige	Danmark	Storbritannia	Lativa
En aktør med helhetlig ansvar for ID-forvaltningen	Nei	Nei	Nei	Ja
Et sentralt register, tilsvarende Folkeregisteret	Ja	Ja	Nei	Ja

Tabell 8 Styring og struktur i utvalgte land (se vedlegg 3 for mer utfyllende beskrivelse av hvert enkelt land)

3.2 Funn og vurderinger

Under følger leverandørens vurderinger av nåsituasjonen innen styring og struktur av ID-forvaltningen. Helhetlige vurderinger foretas av leverandøren i del 3 av rapporten.

3.2.1 Det er mange gode intensjoner, men likevel lav endringstakt og gjennomføringsevne i dagens ID-forvaltning

Det har over tid vært en økende forståelse for ID-relaterte problemstillinger i Norge og flere virksomheter i privat og offentlig sektor har gjennomført både individuelle og tverrsektorielle tiltak for å møte disse. Som omtalt i kapittel 2.9 er det etter leverandørens vurdering mange viktige pågående initiativer innen ID-forvaltningen. Dette gjelder både innad og mellom ulike involverte sektorer. Det finnes flere gode eksempler på vellykket omstilling på tvers av departementsområder, for eksempel ID-porten og modernisering av Folkeregisteret. På en annen side har prosjektet nye pass- og nasjonale ID-kort, et stort og viktig ID-relatert prosjekt som også påvirker mange andre deler og prosesser i ID-forvaltningen, møtt gjentatte forsinkelser og utsettelser. Dette påvirker fremdriften og måloppnåelsen på ID-området isolert og som helhet. Flere andre beslutningsprosesser for eksempel relatert til biometri, hvor flere av aktørene har ulike synspunkter, har også vist seg å være tidkrevende.

3.2.2 Ingen aktør har ID som kjerneoppgave, men et stort antall offentlige og private virksomheter har det som deloppgave eller er involvert i deler av ID-prosessen

Som fremstilt i figur 13 og beskrevet i kapittel 3.1.1 er et stort antall aktører involvert i deler av dagens ID-forvaltning, men utover NID er det ingen aktører som har ID som sin kjerneoppgave. Flere av aktørene oppgir i samtaler at ID-oppgaver historisk sett har manglet prioritering opp mot andre områder, men at fokuset på ID-relaterte problemstillinger har blitt forsterket de siste årene, noe som oppleves som positivt. Flere ytrer også at koordinering og samhandling på tvers er i stor grad basert på behov og interesse. Leverandøren deler denne oppfatningen.

3.2.3 Lav grad av strategisk og overordnet styring på ID-området gir en sektoriell og fragmentert tilnærming til ID-forvaltning

Det er ikke en ansvarlig eier eller en aktør som er samordner og har en premissgiverrolle og/eller instruksjonsmyndighet i ID-forvaltningen. Leverandøren vurderer at det er relativt lav vektlegging og tidsbruk (prioritering) i departementsembetsverket med ansvar for deler av ID-forvaltningen, med begrenset kompetanse og perspektiv på helheten. Leverandøren oppfatter at ansvar og roller ikke er tilstrekkelig avklart og det er en manglende tydelighet i prioritering for etater med ansvar for en bred portefølje.

I dag ivaretar hver sektor sine formål, ansvarsområder og oppgaver, men en mer helhetlig ivaretagelse av området og tydeligere prioriteringer er etterlyst blant de fleste involverte aktører som leverandøren har vært i dialog med. Flere aktører oppgir å savne en mer helhetlig og forankret plan eller strategi for ID-forvaltningen. Leverandøren vurderer det som positivt at det eksisterer en visjon for KoID og at flere aktører støtter denne, men samlet sett dekker ikke dette behovet for strategisk og overordnet styring for ID-forvaltningen. Visjonen er heller ikke forankret i politisk styrende organer, verker regjeringen eller Stortinget. Den fragmenterte styringen gjør at ansvars- og

oppgavefordelingen fremstår som ressursmessig ineffektiv og gir grobunn for målkonflikter.

3.2.4 Ansvar og oppgavefordelingen i ID-forvaltningen er til dels uklar og det bygges flere parallelle kompetansemiljøer, spesielt innen justissektoren

Leverandøren vurderer at ansvar- og oppgavedelingen ikke fremstår som tilstrekkelig gjennomtenkt, men har blitt slik over tid. Dette gjelder spesielt for justissektoren som har mange involverte aktører i ID-forvaltningen. Her er det blant annet etablert to kompetansemiljøer gjennom NID og Kripos med delvis overlappende roller og ansvar. Dublert kompetanse på smale fagområder kombinert med ulik historie, kultur og stolthet gir mindre robuste fagmiljøer, kan være konfliktskapende og gir ikke den fleksibilitet og skalerbarhet som et større fagmiljø gir. Det er en reell risiko for at dette medfører ineffektiv ressursbruk innad i justissektoren og mellom sektorer. Denne betraktningen deles av NOU 2017:11[204] som oppgir at manglende ressurseffektivitet viser seg på flere områder i politiets oppgaveløsning og kompetansebygging, herunder identitetsarbeidet hvor det er flere uklare avgrensninger mellom NID, Kripos og andre ID-miljøer i etaten.

3.2.5 Departementene gir ingen føringer gjennom tildelingsbrevene som underbygger enhetlig tilnærming til ID-forvaltning på tvers av virksomhetene

Mål og styringsparametere relatert til ID og ID-arbeid fremstår ikke tilstrekkelig samkjørt i den enkelte sektor eller på tvers av sektorer.

Ingen av de 18 virksomhetene leverandøren har identifisert til å ha en rolle i ID-forvaltningen har samsvarende mål som gjelder identitetsforvaltning, utenom UNE og UDI i utlendingsforvaltningen. For 13 av 18 virksomheter er identitet som begrep ikke nevnt i tildelingsbrevene.

Leverandøren er ikke blitt gjort oppmerksom på styringsparametere tilknyttet bruker og samfunnseffekter relatert til ID.

3.2.6 Fragmentert ansvarliggjøring av eID gir ulike syn og usikker retning for eID i fremtiden

Ansvaret for forvaltning og regulering av eID er i dag fordelt på ulike departementer som beskrevet i kapittel 2.8.2. Leverandøren bemerker at forvaltningsansvar for ulike aspekter tilknyttet eID fordelt mellom ulike departementer gjør seg gjeldende i delvis sprikende tilnærminger og synspunkter tilknyttet fremtidig retning for eID. Dette fremkommer eksempelvis tilknyttet argumentasjon for og mot eID i de planlagte nasjonale ID-kortene, noe leverandøren er gjort kjent med.

[204] NOU, «Bedre bistand. Bedre beredskap – fremtidig organisering av politiets særorganer», 2017

3.2.7 Det er mange ulike aktører involvert i ID-forvaltningens saksgang med delvis uklar rollefordeling og suboptimal informasjonsflyt mellom partene, spesielt i utlendingsforvaltningen

Som fremstilt i diverse figurer i kapittel 3.1.3 er det delvis komplekse saksganger og mange involverte aktører i ID-prosessene for EØS-borgere og tredjelandsborgere. I samtaler med aktører involvert i utlendingsforvaltningen har det blitt påpekt at det til dels er uklare skiller mellom hvilke arbeidsoppgaver og roller som tilfaller hver aktør. Det har også blitt påpekt at informasjonsflyten mellom aktørene er suboptimal og at aktørene mangler tilgang til hverandres saksinformasjon. Dette fører til dobbeltarbeid og gir grobunn for konflikter mellom aktørene.

3.2.8 Folkeregisteret danner et robust fundament for ID-forvaltningen og tilrettelegger godt for gjenbruk av personopplysninger

Det fremkommer av figur 24 i kapittel 3.1.4 og i samtaler at Folkeregisteret er en sentral felleskomponent i ID-forvaltningen som gir virksomheter mulighet til å innhente mye relevant informasjon. Mange aktører i ID-forvaltningen benytter Folkeregisteret i utstrakt grad som kilde til grunndata. Strukturen på selve Folkeregisteret vurderes av leverandøren som god og det tilrettelegger for gjenbruk av personopplysninger. I tillegg legger registeret til rette for dataminimalitet. Videre vurderes den pågående moderniseringen av Folkeregisteret detaljert i kapittel 2.9.3 som et positivt tiltak med fokus på effektivisering, sikkerhet og personvern som vil komme ID-forvaltningen til gode.

3.2.9 Komplekst registerlandskap med begrensede delingsmuligheter vanskeliggjør effektivt samarbeid mellom de ulike aktørene i ID-forvaltningen

Leverandøren er som nevnt i kapittel 3.1.4 ikke kjent med at det finnes en oversikt over registre og saksbehandlingssystemer i ID-forvaltningen og hvordan de samhandler med hverandre i dag og hva som er målbilde i fremtiden. Antall registre og saksbehandlingssystemer i ID-forvaltningen er stort og komplekst, og det påvirker samarbeidet mellom aktørene i ID-forvaltningen. Hvert register og system tjener sitt formål og bidrar til datadublering innad i det enkelte register og mellom registre. Leverandørens inntrykk er at prinsippet om ett register til ett formål skaper høyere terskler for datadeling og vanskeliggjør effektiv saksbehandling og samhandling. Dette gjelder både mellom etater og innad i den enkelte etat. Eksempelvis er det i samtaler påpekt utfordringer i samhandlingen mellom blant annet utlendingsmyndigheter og politi ved deling av data. Det er også blitt påpekt utfordringer med datadeling innad i politietaten, blant annet fordi det går et klart skille mellom straffesaker og forvaltningssaker. Videre trekker enkelte aktører frem at forvaltningsansvar for masterdata må avklares og tydeliggjøres. Det gjelder både hvem som skal eie sentrale data og hvem som skal ha tilgang for å sikre goddatakvalitet og redusert duplisering av data.

Videre er det leverandørens oppfatning at det med dagens registerlandskap er svært krevende å oppdatere og sikre konsistens på tvers av alle relevante registre og sektorer, spesielt i tilfeller hvor det avdekkes at en person har operert med falsk ID og denne informasjonen må deles og rettes opp i flere steder på tvers av ID-forvaltningen.

3.2.10 Norge er ikke alene om å ha en fragmentert ID-forvaltning med mange involverte aktører

Som fremlagt i kapittel 3.1.5 har både Danmark, Sverige og Storbritannia en fragmentert ID-forvaltning og mangler en felles premissgiver for forvaltningen. Ved gjennomgang av dokumentasjon fremgår det at nevnte lands forvaltninger har et stort antall involverte aktører og at det dem imellom er begrenset informasjonsdeling og kommunikasjon. Videre ser leverandøren en tendens til mangel på definert og tydelig styring og struktur. Ingen eksperter leverandøren har hatt kontakt med har evnet å gi en overordnet beskrivelse av landets ID-forvaltning, noe som styrker oppfatningen av en fragmentert forvaltning. Latvia har, i motsetning til Danmark, Sverige og Storbritannia, samlet ID-forvaltningen i et organ. Aktøren er ansvarlig for registrering og vedlikehold av landets sentrale register, fastsetting av juridisk status til enkeltindivider, utstedelse av pass og nasjonale ID-kort, og gjennomførelsen av statlig migrasjon- og asylpolitikk. Implikasjon av en slik organisering er klare og definerte ansvarsområder, redusert ressursbruk, større sikkerhet og økt brukervennlighet.

4 Gjeldende lover og regelverk i ID-forvaltningen

I dette kapittelet gis en beskrivelse av nåsituasjonen (kapittel 4.1) i form av en oversikt over regelverk som har betydning for ID-forvaltningen. Videre gis en beskrivelse av leverandørens funn og vurderinger knyttet til nåsituasjonen (kapittel 4.2) med særlig henblikk på regelverkenes formål og hvilke muligheter regelverkene gir for samhandling mellom ulike aktører innen ID-forvaltningen, herunder datadeling.

4.1 Nåsituasjonen

Leverandøren har identifisert 38 gjeldende lover, forskrifter, forordninger og rundskriv som relevante for ID-forvaltningen. I tillegg kommer 2 lover som ikke har trådt i kraft enda: lov om nasjonalt ID-kort og grenseloven. Av de 40 regelverkene er det for områdegjennomgangens formål lovene som fremgår av figur 8 i kapittel 2.7 som er særlig relevante.

I det følgende gjennomgås de mest sentrale lovene med hensyn til relevans for ID-forvaltningen, formålet med regelverket, regelverkets virkeområde, hvilke departementer og etater som forvalter regelverket, og hjemler for innhenting, lagring, deling og behandling av informasjon som er relevant for ID-forvaltningen.

4.1.1 Barneloven

Lov 8. april 1981 nr. 7 om barn og foreldre (barnelova) er relevant for fastsetting og registrering av identitet. Loven bestemmer at det skal gis fødselsmelding til folkeregistermyndigheten og hvem som skal anses som barnets foreldre. I fødselsmeldingen skal også barnets navn angis dersom det er bestemt.

Formålet med barneloven er å regulere rettsforholdet mellom barn og foreldre. Loven gjelder som utgangspunkt for alle barn i Norge, uavhengig av statsborgerskap.

Utover at det skal sendes fødselsmelding til folkeregistermyndigheten, regulerer ikke barneloven behandling av ID-relevant informasjon.

Barneloven forvaltes av BLD.

4.1.2 Navneloven

Lov 7. juni 2002 nr. 19 om personnavn (navneloven) er relevant for fastsetting og registrering av personnavn. Loven bestemmer at alle plikter å ha et navn og at foreldre plikter å navngi sine barn.

Formålet med navneloven er å regulere navn for navngivning av personer. Loven gjelder for «alle som er registrert som bosatt her i riket og har til hensikt å bli boende her varig», jf. navneloven § 14. Loven kan således gjelde for alle tre brukergrupper i ID-forvaltningen.

Navneloven regulerer ikke ID-relevant informasjon, utover at navn skal registreres i Folkeregisteret.

Navneloven forvaltes av JD.

4.1.3 Statsborgerloven

Lov 10. juni 2005 nr. 51 om norsk statsborgerskap (statsborgerloven) er relevant for fastsetting av identitet, ved at den regulerer hvem som skal anses som norske statsborgere. Statsborgerloven bestemmer at barn blir norske statsborgere ved fødselen dersom faren eller moren er norsk statsborger og foreldreskapet følger av barneloven. Barn som adopteres av en norsk statsborger blir norsk statsborger ved adopsjonen dersom barnet er under 18 år på adopsjonstidspunktet. Statsborgerskap kan også erverves etter søknad.

Formålet med statsborgerloven er å regulere statsborgerskapet, som er en formalisering av den uuttalte samfunnskontrakten mellom stat og borger.[205]

Statsborgerloven hjemler ingen egne registre, men henviser til Folkeregisteret. Statsborgerloven § 29 bestemmer at organer som behandler saker etter statsborgerloven kan, uten hinder av taushetsplikt, pålegge politiet, Lånekassen, NAV, skattemyndighetene, kommunene og folkeregistermyndigheten å utlevere opplysninger.[206] Det følger av statsborgerforskriften at det er UDI og UNE som kan innhente opplysninger fra de nevnte organene i saker om erverv og tap av norsk statsborgerskap.[207]

KD har forvaltningsansvar for statsborgerloven.

4.1.4 Utlendingsloven

Lov 15. mai 2008 nr. 35 om utlendingers adgang til riket og deres opphold her (utlendingsloven) er relevant for fastsetting av ID, registrering av ID, utstedelse av ID-bevis og kontroll av ID.

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. Loven skal også legge til rette for at utlendinger tar arbeid eller etablerer næringsvirksomhet i Norge.[208]

Formålet med de særlige reglene i kapittel 13 om utlendinger som omfattes av EØS-avtalen og EFTA-avtalen dekkes av lovens formålsparagraf § 1.[209] Det kan likevel nevnes at hovedformålet med disse særlige reglene er å ivareta disse borgernes rett til å ferdes og oppholde seg fritt på medlemsstatenes territorium. Oppholdsretten omfatter retten til å ta opphold og til å ta arbeid eller drive ervervsvirksomhet. Formålet er videre å forenkle de administrative formalitetene som er knyttet til innreise og opphold for disse personene.[210]

Utlendingsloven regulerer ulike grunnlag for opphold i Norge. I den forbindelse registreres alle utlendinger i en egen utlendingsdatabase (UDB).

---

[205] Ot.prp. nr. 41 (2005-2006) Om lov om norsk statsborgerskap (statsborgerloven), punkt 3.1
[206] Både skattemyndighetene og folkeregistermyndigheten sorterer under Skatteetaten
[207] Forskrift 30. juni 2006 om erverv og tap av norsk statsborgerskap (statsborgerforskriften)
[208] Se Ot.prp. nr. 75 (2006–2007) Om lov om utlendingers adgang til riket og deres opphold her (utlendingsloven), blant annet kapittel 8.5
[209] Se Ot.prp. nr. 72 (2007-2008) Om lov om endringar i utlendingslovgivinga (reglar for EØS- og EFTA-borgarar o.a.), se punkt 7.2 og særmerknad til § 109
[210] Ibid, punkt 8.2

Fingeravtrykk tatt med hjemmel i utlendingsloven lagres i et eget utlendingsregister. UDI er behandlingsansvarlig for registeret. Kripos er databehandler.

Med hjemmel i utlendingsloven utstedes det ulike ID-bevis til utlendinger, som skal gi tilgang til enkelte tjenester og ytelser, og realisere enkelte rettigheter, de ellers ikke ville fått fordi de av ulike årsaker ikke kan få ID-bevis som norske statsborgere har tilgang til. Dette inkluderer reisebevis for flyktninger og utlendingspass. Utlendingsloven hjemler også utstedelse av Schengen-standardisert oppholdskort.[211]

Per i dag regulerer utlendingsloven dessuten grenseovervåkning og inn- og utreisekontroll, herunder ID-kontroll i denne sammenheng. Grenseforordningen er gjennomført i norsk rett gjennom utlendingsforskriften § 4-1, jf. utlendingsloven § 14.[212] [213]

Utlendingsloven § 15 fastsetter hovedprinsippene om gjennomføringen av inn- og utreisekontroll. Det primære ved inn- og utreisekontroll er identitets- og dokumentkontroll.[214]

Utlendingsloven § 101 bestemmer at Eurodac-forordningen gjelder som norsk lov.[215] Se nærmere beskrivelse av Eurodac i kapittel 3.1.4.

VIS-forordningen gjennomføres i utlendingsloven § 102 og de følgende bestemmelser.[216] Se nærmere beskrivelse av VIS i kapittel 3.1.4.

Utlendingsloven med tilhørende forskrifter forvaltes av JD. De særlige reglene om EØS- og EFTA-borgere har ASD forvaltningsansvaret for.

4.1.5 Folkeregisterloven

Lov 9. desember 2016 nr. 88 om folkeregistrering (folkeregisterloven) er sentral for registrering av identiteten til personer med tilknytning til Norge.

Formålet med folkeregisterloven er å legge til rette for sikker, korrekt og effektiv registrering av grunnleggende 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.[217]

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.

---

[211] Se nærmere kapittel 2.2
[212] Europaparlaments- og rådsforordning (EU) 2016/399 om bevegelsen av personer over grenser (grenseforordningen)
[213] Forskrift 15. oktober 2009 nr. 1286 om utlendingers adgang til riket og deres opphold her (utlendingsforskriften)
[214] Lov 20. april 2018 nr. 8 om grensetilsyn og grensekontroll av personer (grenseloven) er vedtatt, men har ikke trådt i kraft. Grenseloven skal blant annet regulere inn- og utreisekontroll
[215] Europaparlaments- og rådsforordning (EU) nr. 603/2013 (Eurodac-forordningen 2013)
[216] Europaparlaments- og rådsforordning (EF) nr. 767/2008 om visuminformasjonssystemet (VIS) og utveksling om opplysninger mellom medlemsstatene om visum for kortvarig forhold. [VIS-forordningen]
[217] Lovdata, «Lov om folkeregistrering (folkeregisterloven) - § 1», 2016

4.1.6 Passloven

Lov 19. juni 1997 nr. 82 om pass (passloven) er relevant for utstedelse av norsk pass. Loven hjemler opprettelsen av passregisteret.

Formålet med passloven er å regulere utstedelse av norske pass. 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.

Det følger av passloven § 3 at det er et vilkår for å få pass at søkeren godtgjør sin identitet og sitt norske statsborgerskap. I henhold til passforskriften § 7 må den som vil anskaffe pass godtgjøre sin identitet med «gyldig norsk førerkort eller med annet minst like sikkert identitetskort påført bilde og fødselsnummer.»[218]

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.

I høringsnotat om forslag til forskrift om pass og nasjonalt ID-kort er det foreslått å fastsette i forskrift at UD er behandlingsansvarlig for behandling av opplysninger om diplomatpass, tjenestepass og spesialpass i passregisteret, og at UDI er behandlingsansvarlig for behandling av opplysninger om utlendingspass og reisebevis for flyktninger i passregisteret, se forskriftsutkastet § 6-1.

Passloven forvaltes av JD.

4.1.7 Lov om nasjonalt ID-kort

Lov 5. juni 2015 nr. 39 om nasjonalt identitetskort (ID-kortloven) er relevant for ID-forvaltningen fordi den hjemler utstedelse av et nasjonalt ID-kort og opprettelsen av et nasjonalt ID-kortregister. Loven ventes å tre i kraft i 2020.

Formålet med loven er å regulere ID-kort. Formålet med ID-kortet er nærmere beskrevet i kapittel 2.9.1.

Slik loven nå er utformet gjelder den kun for norske statsborgere. Utstedelse av nasjonalt ID-kort til EØS-borgere og tredjelandsborgere er under utredning. Se nærmere kapittel 2.9.1 og del 3 kapittel 10.

Det følger av loven § 3 at søker «plikter å godtgjøre sin identitet og statsborgerskap, blant annet ved å avgi opplysninger og fremlegge dokumenter som ID-kortmyndigheten anser nødvendige.» Det fremgår av høringsnotatet om forslag til forskrift om pass og nasjonalt ID-kort, forskriftsforslaget § 2-4 at «[p]ass- og ID-kortmyndigheten kan kreve at søkeren godtgjør sin identitet ved å gi de opplysninger, herunder navn, statsborgerskap, fødselsdato, fødselsnummer, fødested og familieforhold, og legge frem de dokumenter som er nødvendige for å verifisere

[218] Forskrift 9. desember 1999 nr. 1263 om pass (passforskriften)

identiteten.» Kravet til godtgjøring av identitet tilsvarer materialet sett i all hovedsak gjeldende passforskrift § 7 selv om ikke førerkort nå nevnes eksplisitt i forskriftsteksten.

ID-kortregisteret kan kobles mot passregisteret, jf. § 9. Det følger av forarbeidene at «[k]oblingen til passregisteret muliggjør automatiserte søk mellom opplysningene i registrene».

Det følger av § 10 Tilgang (rett til direkte søk) at «ID-kortmyndigheten, Politidirektoratet, Kripos og ansatte i politiet som utfører grensekontroll kan gis tilgang til opplysninger i nasjonalt ID-kortregister, eller opplysningene kan på annen måte gjøres tilgjengelig for dem når det er tjenestemessig behov for opplysningene til utstedelse av nasjonalt ID-kort eller utførelse av grensekontroll.»

Det følger av § 11 Utlevering av opplysninger at «[o]pplysninger fra nasjonalt ID-kortregister kan utleveres når det er nødvendig for å kontrollere identiteten til innehavere av nasjonalt ID-kort eller kortets ekthet» og at «[u]tlevering av opplysninger etter første ledd kan skje ved direkte søk som går ut på treff eller ikke-treff.»

I høringsnotat om forslag til forskrift om pass og nasjonalt ID-kort er det foreslått i utkastet til forskriften § 6-1 at POD skal være behandlingsansvarlig for ID-kortregisteret.

JD forvalter ID-kortloven.

4.1.8 Vegtrafikkloven

Lov 18. juni 1965 nr. 4 om vegtrafikk (vegtrafikkloven) er relevant for registrering av identitetsopplysninger, herunder ansiktsfoto, utstedelse av førerkort og for kontroll av førerkort i forbindelse med trafikkontroll.

Formålet med vegtrafikkloven er å ivareta hensyn til trafikksikkerhet, fremkommelighet og miljø innenfor virkeområdet i loven § 1. Videre regulerer loven forholdet mellom veg, kjøretøy og trafikant. Loven gjelder for enhver. Norske statsborgere, EØS-borgere og tredjelandsborgere kan få utstedt norsk førerkort, så fremt de har lovlig opphold og fast bopel i Norge, og er registrert i Folkeregisteret.

Det følger av førerkortforskriften § 5-2 at for å få utstedt førerkort må det fremvises «akseptabel legitimasjon med navn, fødselsnummer (elleve siffer), eller d-nummer for de som ikke har norsk fødselsnummer, og bilde.»[219]

Vegtrafikkloven hjemler et førerkortregister og et motorvognregister. Politiets tilgang til opplysninger i de to registrene følger av vegtrafikkloven § 43b.

SD har forvaltningsansvar for vegtrafikkloven.

4.1.9 Skipssikkerhetsloven

Lov 16. februar 2007 nr. 9 om skipssikkerhet (skipssikkerhetsloven) er relevant for ID-forvaltningen fordi den hjemler Forskrift 25. november 1988 nr. 940 om kontroll av maritim tjeneste, som regulerer utstedelse av sjøfartsbok.

[219] Forskrift 19. januar 2004 nr. 298 om førerkort m.m. (førerkortforskriften)

Lovens formål er i henhold til § 1 å trygge liv og helse, miljø og materielle verdier ved å legge til rette for god skipssikkerhet og sikkerhetsstyring, herunder hindre forurensning fra skip, sikre et fullt forsvarlig arbeidsmiljø og trygge arbeidsforhold om bord på skipet, samt et godt og tidsmessig tilsyn.

Det er kun norske statsborgere som kan få utstedt sjøfartsbok, jf. forskriften § 5. Videre stilles det blant annet krav om fremvisning av gyldig norsk pass.

Loven forvaltes av NFD.

4.1.10 Forsvarets ID-kort

Utstedelse av forsvarets identitetskort er ikke regulert i lov eller forskrift. Det følger av instruks for FD-ID fastsatt av Forsvarets personell og vernepliktssenter at som hovedregel kreves enten førerkort eller pass som legitimasjon for å få utstedt forsvarets identitetskort. Ved fornyelse er det normalt tilstrekkelig å fremvise identitetskortet som skal fornyes.

4.1.11 Personopplysningsloven

Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven) er relevant for ID-forvaltningen fordi den bestemmer at personvernforordningen (GDPR) skal gjelde som norsk lov.[220] Loven fastsetter regler om vern av fysiske personer i forbindelse med behandling av personopplysninger, jf. forordningen art. 1(1).

Formålet med personopplysningsregelverket er å sikre vern av fysiske personers grunnleggende rettigheter og friheter, og særlig deres rett til vern av personopplysninger, jf. forordningen art. 1(2).

Personopplysningsloven gjelder ikke for alle deler av ID-forvaltningen. Det følger av forordningen art. 2(2)(d) at den ikke gjelder ved behandling av personopplysninger som utføres «av vedkommende myndigheter med henblikk på å forebygge, etterforske, avsløre eller straffeforfølge straffbare forhold eller iverksette strafferettslige sanksjoner, herunder vern mot og forebygging av trusler mot den offentlige sikkerhet.» I slike tilfeller gjelder politiregisterloven, se neste kapittel.

Personopplysninger skal behandles i tråd med følgende prinsipper:[221]

- Lovlighet, rettferdighet og åpenhet
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet og konfidensialitet

JD har forvaltningsansvaret for Personopplysningsloven.

[220] EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [PVF, GDPR]
[221] Personvernforordningen art. 5(1)

4.1.12 Politiregisterloven

Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) er relevant for registrering og politiets bruk av personopplysninger.

Formålet med loven er å bidra til effektiv løsning av politiets og påtalemyndighetens oppgaver, beskyttelse av personvernet og forutberegnelighet for den enkelte ved behandlingen av opplysninger.

Politiregisterloven gjelder for politiets og påtalemyndighetens behandling av opplysninger, med unntak av opplysninger som reguleres av lov om Schengen informasjonssystem (se kapittel 4.1.13) eller som er del av politiets forvaltningsvirksomhet eller sivile gjøremål. Politiregisterloven gjelder for norske statsborgere, EØS-borgere og tredjelandsborgere.

På områdene hvor politiregisterloven ikke gjelder, så gjelder personopplysningsloven. Dette betyr at politiet ved behandling av personopplysninger må forholde seg til to ulike regelverk.

Politiregisterloven hjemler til sammen 19 ulike registre (beskrevet i vedlegg 5). Det følger av loven § 4 at opplysninger som utgangspunkt «kan behandles til det formålet de er innhentet for eller til andre politimessige formål». Videre er formålet med hvert enkelt register nærmere beskrevet i politiregisterforskriften. Det følger av forskriften § 2-1 at det er ulike myndigheter som har behandlingsansvaret for ulike registre; Riksadvokaten, embetsledere, politimestre, Sysselmannen på Svalbard, sjef PST og sjefene for særorganene.

Tilsvarende gir loven generelle regler om tilgang til (mulighet for direkte søk) og utlevering av opplysninger i registrene, mens forskriftene gir konkrete regler for hver enkelt forskrift. I hovedsak er det regler om taushetsplikt og personvernhensyn i form av nødvendighets-, formåls- og forholdsmessighetskrav som regulerer muligheter og begrensninger for informasjonsdeling.

Politiregisterloven forvaltes av JD.

4.1.13 Lov om Schengen informasjonssystem

Lov 16. juni 1999 nr. 66 om Schengen informasjonssystem (SIS-loven) er relevant for ID-forvaltningen fordi den hjemler den norske delen av SIS, se nærmere kapittel 3.1.4.

Formålet med loven er i henhold til § 1 «å regulere behandlingen i Norge av opplysninger innenfor Schengen informasjonssystem (SIS), herunder å ivareta hensynet til personvern.»

Loven gjelder for norske statsborgere, EØS-borgere og tredjelandsborgere.

Kripos er registeransvarlig. Politimyndighet, påtalemyndighet, utlendingsmyndighet og myndighet med ansvar for registrering av motorkjøretøyer tilgang til SIS i henhold til loven § 12.

I henhold til loven § 13 kan det utleveres opplysninger fra SIS til politi- og tollmyndighet, Kystvakten, påtalemyndighet, utlendingsmyndighet, veimyndighet, JD og POD.

SIS-loven forvaltes av JD.

4.1.14 Lov om elektroniske tillitstjenester

Lov 15. juni 2018 nr. 44 om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester) er relevant for ID-forvaltningen fordi den setter opp noen felleseuropeiske rammer for bruken av elektroniske tillitstjenester på tvers av landegrensene.[222] Loven er også relevant for ordninger for elektronisk identifikasjon.[223]

Formålet med loven er å gjennomføre eIDAS-forordningen i norsk rett. Loven gjelder for norske statsborgere, EØS-borgere og tredjelandsborgere.

eID reguleres ikke direkte i loven, men det stilles krav til utstedelse av sertifikater som kan brukes til nettstedsautentisering. Gjeldende norske ordning med frivillig selvdeklarering, som både BankID, Buypass og Commfides har benyttet seg av består også etter innføringen av den nye loven, jf. § 10, jf. forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere. eID er i forordningen som sådan ikke definert som en tillitstjeneste.

Det er kun ved tilgang til offentlige tjenester at forordningen stiller krav om anerkjennelse av andre lands eID-løsninger. Videre gjelder anerkjennelsesplikten kun i de tilfeller det stilles krav om eID som er på sikkerhetsnivå som tilsvarer *betydelig* eller *høy*. Det følger av forarbeidene at «[d]ersom medlemsstaten mener at det ikke finnes et tilsvarende nivå (eksempelvis at det nasjonale nivået er strengere enn eIDAS *høy*), vil det etter departementets syn ikke være noen anerkjennelsesplikt for tjenester som krever dette nivået.»[224] Det er også lagt til grunn av departementet at forordningen ikke krever endring av dagens regelverk for tildeling av identitetsnumre i Folkeregisteret.

Videre er det kun anerkjennelse av autentiseringen som reguleres direkte av forordningen. Hvilke krav som skal stilles for å få tilgang til en tjeneste beror på nasjonal lovgivning. Eventuell knytning til nasjonalt identitetsnummer reguleres ikke i forordningen.

Loven forvaltes av KMD.

4.1.15 Folketrygdloven

Lov 28. februar 1997 nr. 19 om folketrygd (folketrygdloven) er relevant for ID-forvaltningen fordi den fastsetter hvilke krav som skal stilles til identifikasjon for mottakere av de stønader som følger av loven.

«Folketrygden er et nasjonalt, sosialt forsikringssystem som ble innført 1. januar 1967. Mesteparten av folketrygden administreres av arbeids- og velferdsetaten (NAV). Alle personer som er bosatt i Norge er pliktig medlem av folketrygden.»[225] Loven regulerer en rekke ulike ytelser, slik som for eksempel stønad ved arbeidsløshet, sykdom og alderspensjon.

[222] Europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked(eIDAS-forordningen)
[223] eID reguleres ikke direkte i loven, men det stilles krav til utstedelse av sertifikater som kan brukes til nettstedsautentisering. Gjeldende norske ordning med frivillig selvdeklarering, som både BankID, Buypass og Commfides har benyttet seg av består også etter innføringen av den nye loven, jf. § 10, jf. forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere. eID er i forordningen som sådan ikke definert som en tillitstjeneste
[224] 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
[225] Lovdata, «Lov om folketrygd (folketrygdloven)», 1997

Folketrygdens formål er å gi økonomisk trygghet ved å sikre inntekt og kompensere for særlige utgifter ved arbeidsløshet, svangerskap og fødsel, aleneomsorg for barn, sykdom og skade, uførhet, alderdom og dødsfall. Folketrygden skal bidra til utjevning av inntekt og levekår over den enkeltes livsløp og mellom grupper av personer. Folketrygden skal bidra til hjelp til selvhjelp med sikte på at den enkelte skal kunne forsørge seg selv og klare seg selv best mulig til daglig.

Loven gjelder for norske statsborgere, EØS-borgere og tredjelandsborgere.

Det følger av folketrygdloven § 21-3 at «[e]n 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.»

Ifølge Rundskriv til ftrl kap. 21 - Saksbehandlingsrundskriv godtas også førerkort «og annen minst like sikkert identitetskort med bilde og fødselsnummer, for eksempel bankkort.»

Folketrygdloven § 21-4 bestemmer at Arbeids- og velferdsetaten og Helsedirektoratet har rett til å innhente de opplysninger som er nødvendige for å kontrollere om vilkårene for en ytelse er oppfylt. Det kan innhentes opplysninger fra «helsepersonell, andre som yter tjenester forutsatt at de gjør det for trygdens regning, arbeidsgiver, tidligere arbeidsgiver, tilbyder av posttjenester, utdanningsinstitusjon, barnetilsynsordning, offentlig virksomhet, Folkeregisteret, pensjonsinnretning, forsikringsselskap og annen finansinstitusjon og regnskapsfører.»

Folketrygdloven forvaltes av ASD.

4.1.16 Pasient- og brukerrettighetsloven

Lov 2. juli 1999 nr. 63 om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven) er relevant for ID-forvaltningen fordi den regulerer retten til å få helsetjenester og fordi en persons identitet har betydning for omfanget av rett til helsehjelp.

Lovens formål er i henhold til § 1-1 å bidra til å sikre befolkningen lik tilgang på tjenester av god kvalitet ved å gi pasienter og brukere rettigheter overfor helse- og omsorgstjenesten. Loven skal også bidra til å fremme tillitsforholdet mellom pasient og bruker og helse- og omsorgstjenesten, fremme sosial trygghet og ivareta respekten for den enkelte pasients og brukers liv, integritet og menneskeverd.

Loven gjelder for alle som oppholder seg i riket, og er dermed relevant for norske statsborgere, EØS-borgere og tredjelandsborgere.

Loven stiller ikke krav om at man må legitimere seg for å få den helsehjelpen man har krav på etter loven. Identitet har likevel betydning for hvilke rettigheter man har. Det følger av forskrift om tjenester til personer uten fast opphold § 2 at ikke alle personer som oppholder seg i Norge har samme rett til helsehjelp.[226] Alle har rett til øyeblikkelig hjelp, men ikke alle har fulle rettigheter til helsehjelp.

Loven regulerer ikke deling av data mellom myndigheter.

[226] Forskrift 16. desember 2011 nr. 1255 om rett til helse- og omsorgstjenester til personer uten fast opphold i riket

Loven forvaltes av HOD.

4.1.17 Skattebetalingsloven

Lov 17. juni 2005 nr. 67 om betaling og innkreving av skatte- og avgiftskrav (skattebetalingsloven) er relevant for ID-forvaltningen fordi den fastsetter regler for utstedelse av skattekort.

Formålet med loven er å regulere innkreving og betaling av skatt. Loven gjelder for norske statsborgere, EØS-borgere og tredjelandsborgere.

Verken skattebetalingsloven eller skattebetalingsforskriften stiller krav til identifikasjon ved utstedelse av skattekort. Det fremgår imidlertid av skjemaet RF-1209 Søknad om skattekort/forskuddsskatt for utenlandske borgere at man må ha med pass eller annen legitimasjon ved søknad om skattekort. Det fremgår ikke av skjemaet hvilke identifikasjonsdokumenter som godtas. Ifølge nyinorge.no er det ulike krav til hva som er gyldig ID-bevis for ulike brukergrupper.[227]

Det følger av skattebetalingsloven § 3-4 at «Innkrevingsmyndighetene kan kreve at folkeregistermyndigheten uten hinder av taushetsplikt som de ellers har, skal gi de opplysningene som er nødvendige for innkrevingsmyndighetenes arbeid etter denne loven.»

FIN har forvaltningsansvaret for skattebetalingsloven.

4.1.18 Utdanningsstøtteloven

Lov 3. juni 2005 nr. 31 om utdanningsstøtte (utdanningsstøtteloven) er relevant for ID-forvaltningen fordi den regulerer tilgang til utdanningsstøtte.

Utdanningsstøtteordningens formål er i henhold til loven § 1 å bidra til like muligheter til utdanning uavhengig av geografiske forhold, alder, kjønn, funksjonsdyktighet, økonomiske og sosiale forhold, å sikre samfunnet og arbeidslivet tilgang på kompetanse og at utdanningen skjer under tilfredsstillende arbeidsforhold, slik at studiearbeidet kan bli effektivt.

Loven gjelder som hovedregel for norske statsborgere. Loven gjelder også for EØS-borgere og tredjelandsborgere på nærmere fastsatte vilkår.

Loven stiller ikke krav om legitimasjon for å få utdanningsstøtte. Forskriftene til loven stiller heller ikke krav om legitimasjon. Identitet har imidlertid betydning for rett til utdanningsstøtte. For eksempel har norske statsborgere og utlendinger ulike rettigheter.

Etter § 23 kan Lånekassen innhente opplysninger fra blant andre Skatteetaten, NAV, barneverntjenesten, Folkeregisteret, Vernepliktsverket og UDI, dersom opplysningene har betydning for søkerens eller låntakerens rettigheter eller plikter fastsatt i eller i medhold av utdanningsstøtteloven. Lånekassens adgang til å innhente opplysninger fra andre myndigheter er regulert nærmere i forskrift 28. august 2014 nr. 1123 om Lånekassens adgang til innhenting av opplysninger.

Utdanningsstøtteloven forvaltes av KD.

[227] Nyinorge.no, «Skattekort», u.å.

4.1.19 Valgloven

Lov 28. juni 2002 nr. 57 om valg til Stortinget, fylkesting og kommunestyrer (valgloven) er relevant for ID-forvaltningen fordi den stiller krav om legitimasjon ved stemming ved valg.

Formålet med loven er i henhold til § 1-1 å legge forholdene til rette slik at borgerne ved frie, direkte og hemmelige valg skal kunne velge sine representanter til Stortinget, fylkesting og kommunestyrer. Loven er relevant kun for norske statsborgere.

Dersom stemmemottakeren ikke kjenner velgeren, skal velgeren legitimere seg, jf. loven § 8-4 sjette ledd. Verken loven eller valgforskriften regulerer nærmere hva som anses som «legitimasjon».

Valgloven pålegger folkeregistermyndigheten å stille til disposisjon for valgmyndighetene et foreløpig manntall og hvem som skal innføres i manntallet.

Valgloven forvaltes av KMD.

4.1.20 Politiloven

Lov 4. august 1995 nr. 53 om politiet (politiloven) er relevant for ID-forvaltningen fordi den hjemler fastsettelse av fiktiv identitet, registrering av personopplysninger og kontroll av ID-bevis.

Formålet med politiloven er enkelt forklart å regulere politiets arbeid og myndighet. Det følger av politiloven § 1 Ansvar og mål at staten skal sørge for den polititjeneste som samfunnet har behov for. Politiet skal gjennom forebyggende, håndhevende og hjelpende virksomhet være et ledd i samfunnets samlede innsats for å fremme og befeste borgernes rettssikkerhet, trygghet og alminnelige velferd for øvrig.

Politiloven er relevant for norske statsborgere, EØS-borgere og tredjelandsborgere.

Politiloven kapittel IIa regulerer fiktiv identitet, inkludert registrering av personopplysninger i denne forbindelse. Politiloven § 7 hjemler politiets adgang til å gi pålegg om å oppgi personalia.[228]

I medhold av politiloven § 29 a kan politiet, uten hinder av taushetsplikt innhente fra folkeregistermyndigheten, de opplysninger som er nødvendige for utførelsen av oppgaver etter politiloven.

JD forvalter politiloven.

4.1.21 Faglige styringslinjer

Tabellen under viser hvilke departementer som har forvaltningsansvar for eller har særlig tilknytning til de mest ID-relevante lovene. Mørk grønn indikerer forvaltningsansvar, mens lys grønn indikerer tilknytning til lov.

[228] Politiloven må leses i sammenheng med politiloven § 5 og straffeloven. § 162. Politiets hjemmel til å pålegge personer å oppgi personalia diskuteres nærmere av Steinar Fredriksen i LoR 2013 s. 21 til 37

Lov/DEPARTEMENT	JD	FIN	KMD	ASD	KD	HOD	SD	BFD	NFD
Passloven									
ID-kortloven									
Politiloven									
Politiregisterloven									
SIS-loven									
Utlendingsloven				EØS/ EFTA					
Navneloven									
Personopplysningsloven									
Folkeregisterloven									
Skattebetalingsloven									
Valgloven									
Lov om elektroniske tillitstjenester									
Folketrygdloven									
Statsborgerloven									
Utdanningsstøtteloven									
Pasient- og brukerrettighetsloven									
Barneloven									
Vegtrafikkloven									
Skipssikkerhetsloven									

Tabell 9 Faglige styringslinjer

4.2 Funn og vurderinger

4.2.1 Regelverkenes formål dekker samlet sett de ulike formålene med ID-forvaltning

Reguleringen av ID er fragmentert. Det finnes ikke ett regelverk som behandler alle aspektene ved ID i Norge. Folkeregisterloven og lov om nasjonalt ID-kort er særlig sentrale lover, som direkte regulerer deler av ID-forvaltningen. I andre regelverk inngår ID som en del av den øvrige reguleringen av et forvaltningsområde.

Kartleggingen viser at regelverkene som har betydning for ID-forvaltningen skal ivareta et bredt spekter av og tidvis motstridende formål. At identitet er et helt sentralt element i et menneskes liv gjenspeiles i det gjeldende regelverket. Betydningen av identitet vises ved at det relevante regelverket både er omfangsriktig og at det spenner over mange sentrale samfunnsområder. Kontroll med hvem som får adgang til å komme til landet (innreise/innvandring) er også et viktig formål med ID-forvaltningen. Som en del av oppdraget skulle leverandøren vurdere om formålet med de ulike regelverkene er dekkende for det overordnede formålet med ID-forvaltningen.

Det foreligger imidlertid ingen offisiell helhetlig beskrivelse av hva som er det overordnede formålet med ID-forvaltningen i Norge. Flere tverrfaglige prosjekter og initiativ, slik som NID og Koordineringsgruppen for ID-forvaltning, trekker frem overordnede målsettinger og utfordringer. Ingen av disse initiativene dekker etter leverandørens syn i tilstrekkelig grad det brede spekteret av ulike hensyn som ID-forvaltningen omfatter.

Formålet med ID-forvaltning er sammensatt. Slik leverandøren vurderer det er det overordnede formålet med ID-forvaltning å ivareta grunnleggende individuelle rettigheter og å yte tjenester til befolkningen på den ene siden og på den andre siden å ivareta myndighetenes ansvar for å sørge for den enkeltes sikkerhet og å bidra til rettferdig fordeling av goder.

En persons identitet har betydning for muligheten til å delta i valg, ta arbeid, starte næringsvirksomhet, åpne en bankkonto, og motta ytelser fra NAV. Deltakelse i det norske samfunnslivet kan være en viktig forutsetning for vellykket integrering. Landets behov for utenlandsk arbeidskraft spiller også en viktig rolle for ID-forvaltningen.

For myndighetene er ID-forvaltning avgjørende ved ivaretakelsen av en rekke grunnleggende tjenester, slik som kriminalitetsforebygging og kriminalitetsbekjempelse, rettferdig innkreving av skatt og rettferdig tildeling av helse- og velferdstjenester. Dette er forhold som trekker i retning av en noe strengere ID-forvaltning.

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. Leverandørens har utarbeidet en skisse til mål for ID-forvaltningen i kapittel 9.2.

De relevante regelverkene synes samlet sett å dekke alle de ulike formålene som inngår i det overordnede formålsbildet for ID-forvaltningen. Det er imidlertid klart at ingen av regelverkene alene dekker det totale bildet, men at de hver for seg dekker kun deler. Gjennomgangen av formålene etterlater således ingen særlige utfordringer. På regelverksnivå ligger nok heller utfordringene i at det ved utarbeidelse av det enkelte regelverk ikke er foretatt tilstrekkelige avveininger opp mot formål og hensyn som ligger utenfor det aktuelle regelverket, men som likevel blir berørt. Dette kan gi utfordringer ved praktisering av regelverket.

4.2.2 Justissektoren har en betydelig regelverksportefølje innenfor ID-forvaltningen

Gjennomgangen av regelverk viser at justissektoren samlet sett har ansvar for sentrale og omfattende deler av ID-forvaltningen, slik som passloven, utlendingsloven, politiregisterloven og personopplysningsloven, se tabell 9 i kapittel 4.1.21.

Hvilke departementer og etater som forvalter de ulike regelverkene er primært et organisatorisk og i liten grad et rettslig anliggende. Et naturlig utgangspunkt er at et departement har forvaltningsansvaret for det regelverket en underliggende etat er satt til å forvalte. Ett eksempel på dette er JD har ansvar for både politiloven og politietaten.

Et annet eksempel er at JD har ansvar for utlendingsloven og utlendingsforvaltningen. Innad i JD er ansvaret for ulike deler av utlendingsloven fordelt mellom Politiavdelingen og Innvandringsavdelingen. Forvaltning av utlendingsloven representerer videre et unntak fra hovedregelen ved at det er ASD som har hovedansvaret for loven kapittel 13 om EØS-borgere.

Et neste unntak er at JD har forvaltningsansvar for personopplysningsloven, mens Datatilsynet sorterer under KMD.

4.2.3 Dagens regulering inneholder ingen enhetlig definisjon av hva som skal anses som gyldig legitimasjon

Hva som skal anses som gyldig eller akseptabel legitimasjon er ikke klart definert i dagens regelverk.[229]

Folketrygdloven, førerkortforskriften, passforskriften, utkast til forskrift om pass og nasjonalt ID-kort og skipssikkerhetsloven har bestemmelser om hva som er gyldig legitimasjon. Alle regelverkene har forskjellig tilnærming til hva som er gyldig legitimasjon og bestemmelsene gjelder kun innenfor virkeområdet til det enkelte regelverket, og dermed innenfor avgrensede deler av samfunnet.

I folketrygdloven er kravet «pass eller annen gyldig legitimasjon». I førerkortforskriften er kravet «akseptabel legitimasjon med navn, fødselsnummer (elleve siffer), eller d-nummer for de som ikke har norsk fødselsnummer, og bilde.» For å få pass er det krav om å godtgjøre sin identitet med «gyldig norsk førerkort eller med annet minst like sikkert identitetskort påført bilde og fødselsnummer.» For utstedelse av sjøfartsbok er det krav om gyldig norsk pass.

På de øvrige områdene som leverandøren har sett på finnes det ingen bestemmelser i lov eller forskrift om hva som er gyldig legitimasjon.[230] Som det fremgår av kapittel 5.1.2 og 5.1.3 er det varierende praksis for hva som godtas som legitimasjon.

At det stilles ulike krav til legitimasjon i de ulike sektorene er ikke nødvendigvis i seg selv en utfordring. I utlendingsforvaltningen er det for eksempel vanskelig å operere med en felles standard da man der står overfor et stort antall ulike scenarioer. Videre følger det av høringsnotat med forslag til forskrift om pass og nasjonalt ID-kort at myndighetene har en bevisst holdning til hva som skal til for å anse noen for å ha godtgjort sin identitet. Økonomiregelverkets krav om internkontroll er relevante i denne sammenheng.

4.2.4 Regelverkene inneholder en rekke bestemmelser om deling av data mellom myndigheter, men andre former for samhandling er i liten grad regulert

Med samhandling mener leverandøren her ulike former for samarbeid og koordinering mellom myndigheter. Deling av opplysninger mellom myndigheter er én form for samhandling.

Samarbeid og koordinering

Et eksempel på at samarbeid og koordinering mellom myndigheter er regulert på lovsnivå finner vi på området nasjonal sikkerhet, et område som i likhet med ID-forvaltningen involverer mange departementer og etater. Sikkerhetsloven er en sektorovergripende lov. Den fastslår at det enkelte departementet sammen med respektive underliggende etater har ansvar innenfor sin sektor. JD og FD og deres felles underliggende etat Nasjonal sikkerhetsmyndighet er gitt et overordnet og sektorovergripende ansvar. Sikkerhetsloven § 3-2 fastsetter en uttrykkelig plikt for Nasjonal sikkerhetsmyndighet og andre myndigheter med tilsynsansvar om å samarbeide.

[229] Se nærmere kapittel 2.2
[230] Et unntak er imidlertid vedlegg 4 til utlendingsforskriften som lister opp legitimasjonsdokumenter utstedt av EØS eller EFTA-land som godkjennes som reisedokument

Leverandørens kartlegging av regelverk viser som nevnt at det innenfor ID-forvaltningen ikke finnes tilsvarende sektorovergripende regelverk. Flere relevante regelverk, slik som for eksempel utlendingsloven, forutsetter langt på vei samarbeid og koordinering mellom myndigheter, men regulerer ikke dette direkte.

Det er ikke en forutsetning for et vellykket samarbeid at dette er regulert i lov. Lovregulering kan dessuten føre til liten fleksibilitet når det gjelder muligheten for omorganisering. På den annen side så vil prosessen frem mot en lovregulering kunne lede til nyttige drøftinger og avklaringer om oppgave- og ansvarsfordeling mellom aktørene. Den endelige løsningen vil kunne fremstå med mer legitimitet og som mer forutsigbar enn om den ikke var fremkommet ved lov. Stortinget vil dessuten i større grad kunne føre kontroll med nettopp samarbeidet mellom etatene.

Deling av data

Deling av data reguleres i en rekke av de relevante regelverkene. Når datadeling omhandles benyttes gjerne begrepene tilgang (også kalt rett til direkte søk), utlevering og innhenting. Det kan handle om tilgang til ulike registre hos andre myndigheter eller det kan handle om å innhente opplysninger fra saksarkiv. Regler om taushetsplikt og personvern setter opp viktige rammer for mulighetene til å dele informasjon.

Datadeling handler i all hovedsak om at den enkelte myndighet trenger informasjon fra andre for å ivareta sine oppgaver, typisk å komme til riktig resultat i en sak. Eksempelvis kan NAV innhente opplysninger fra helsemyndighetene for å fatte vedtak som har å gjøre med stønad i forbindelse med helsehjelp. Det ligger altså et konkret formål til grunn for hver hjemmel til å dele opplysninger.

Kartleggingen viser at det i dagens regelverk er en rekke hjemler for at data kan deles mellom myndigheter. For eksempel har mange aktører tilgang til Folkeregisteret, og for Lånekassen er det som nevnt i kapittel 4.1.15 utarbeidet en egen forskrift som utelukkende handler om informasjonsinnhenting fra andre myndigheter. Leverandøren har ikke foretatt en systematisk gjennomgang av alle de ulike hjemlene for å dele data. Det er imidlertid klart at ikke all deling av informasjon mellom myndigheter er relevant for ID-forvaltningen. Noe nærmere om datadeling som er særlig relevant for ID-forvaltningen omhandles blant annet i kapittel 14.2.1.

En særlig interessant hjemmel til å dele informasjon mellom ulike myndigheter kom inn i personopplysningsloven i 2018, som et ledd i oppfølgingen av Arbeidslivskriminalitetsstrategien. Personopplysningsloven § 12 a fastslår at «offentlige myndigheter kan utlevere personopplysninger til hverandre når det er nødvendig for å forebygge, avdekke, forhindre eller sanksjonere arbeidslivskriminalitet.» Dette gjelder ikke for særlige kategorier (sensitive) eller taushetspliktige personopplysninger.

Begrepet «arbeidslivskriminalitet» innebærer i første rekke «handlinger som bryter med norske lover om lønns- og arbeidsforhold, trygder, skatter og avgifter, gjerne utført organisert, som utnytter arbeidstakere eller virker konkurransevridende og undergraver samfunnsstrukturen.» Det følger imidlertid av forarbeidene til loven at begrepet også kan omfatte konkurskriminalitet, korrupsjon og hvitvasking, samt arbeidet som gjøres av offentlige organer som deltar i samarbeid mot arbeidslivskriminalitet i et a-krimsenter eller ved et nasjonalt tverretatlig etterretnings- og analysesenter.

Er det for eksempel snakk om en trygdesvindelsak så hjemler altså bestemmelsen at ulike myndigheter i anledning trygdesvindelsaken kan dele personopplysninger med hverandre. I den grad trygdesvindel og annen arbeidslivskriminalitet kan ses på som ID-kriminalitet kan bestemmelsen også sies å legge til rette for informasjonsdeling

innenfor ID-forvaltningen. Hvorvidt aktørene i ID-forvaltningen har benyttet denne hjemmelen for å dele informasjon i ID-sammenheng har leverandøren ikke undersøkt.

Bestemmelsen viser videre at det innenfor personvernet er rom for å gi hjemmel til informasjonsdeling med en relativt vid formålsangivelse uten helt klare grenser. En tilsvarende hjemmel finnes ikke for bekjempelse av ID-relatert kriminalitet. Etter leverandørens oppfatning er det imidlertid prinsipielt sett ikke noe i veien for å opprette en tilsvarende bestemmelse der formålet er å bekjempe ID-relatert kriminalitet.

Flere intervjuobjekter har påpekt utfordringer knyttet til datadeling mellom og innad i etater. Det er blant annet blitt nevnt utfordringer knyttet til deling av data mellom utlendingsmyndigheter og politi. Det er også blitt påpekt utfordringer med datadeling innad i politietaten, og det er henvist til at det går et klart skille mellom straffesaker og forvaltningssaker.

Det kan være flere grunner til at det påpekes manglende muligheter for datadeling. Det kan for det første være at ønsket datadeling ikke er mulig i henhold til personopplysningsloven. For det andre kan det være at selv om personopplysningsloven åpner for den ønskede datadelingen, så er det ikke politisk vilje til å gi nødvendig hjemmel i norsk lov. En tredje mulighet kan være at det ikke er blitt gjort forsøk på å skaffe til veie tilstrekkelig hjemmel.

Deling av data er en relativt omfattende problemstilling. Gitt oppdragsbeskrivelsen og rammene for områdegjennomgangen har leverandøren ikke undersøkt deling av data i ID-forvaltningen nærmere fra et regelverksperspektiv. Rettslige aspekter ved informasjonsdeling i forvaltningen ble drøftet av forvaltningslovutvalget i NOU 2019: 5 Ny forvaltningslov. I Riksrevisjonens undersøkelse av digitalisering i statlige virksomheter var gjenbruk av informasjon ett av flere temaer som ble berørt.[231] Det ble konkludert med at statlige virksomheter gjenbruker informasjon bare delvis. Rapporten peker blant annet på taushetsplikt og personvern som faktorer som begrenser muligheten for å gjøre informasjon tilgjengelig for gjenbruk.[232]

I Difis konseptvalgutredning beskrives dagens situasjon og fremtidige ambisjoner for deling av offentlige data.[233] Når det gjelder regelverk oppsummeres behovsanalysen som følger: «*Det er behov for et mer harmonisert og digitaliseringsvennlig regelverk med ensartede begreper, som legger til rette for automatisering av prosesser gjennom deling og gjenbruk av data. Regelverket må sikre forsvarlig databehandling, slik at data deles når de kan og skjermes når de må.*»

[231] Riksrevisjonens administrative rapport nr. 1 2018, Riksrevisjonens undersøkelse av digitalisering av statlige virksomheter
[232] Se nærmere Riksrevisjonens rapport punkt 5.1
[233] Difi, Deling av data, Konseptvalgutredning, versjon 1.0 – Sladdet, 5. november 2018, Difi-rapport 2018:7

5 Brukerreiser og brukervennlighet i ID-forvaltningen

I dette kapittelet gis en beskrivelse av nåsituasjonen (kapittel 5.1) og leverandørens nåsituasjonsvurdering (kapittel 5.2) for ulike brukergruppers møte med den norske ID-forvaltningen. Kapittelet tar blant annet for seg brukertilfredshet, hvilke ID-bevis (jf. definisjon i begrepsliste) som kreves fremlagt av bruker for å få tilgang til sentrale offentlige tjenester og ytelser, hvilke ID-bevis som kreves for utstedelse av andre ID-bevis, samt overordnet tidsbruk, direkte kostnad og antall treffpunkt (jf. definisjoner i begrepsliste) som påløper for bruker med tilhørende vurderinger. Forenklede brukerreiser er illustrert i kapittel 2.6.

5.1 Nåsituasjonen

5.1.1 Brukertilfredshet i den norske ID-forvaltningen

Det er ikke identifisert samlede undersøkelser som viser innbyggernes tilfredshet med ID-forvaltningen som helhet eller tilfredshet fordelt på brukergrupper (norske borgere, EØS-borgere og tredjelandsborgere). Det er heller ikke per aktør i ID-forvaltningen eller per ID-bevis identifisert sammenlignbare data om tilfredshet ved ID-relaterte aktiviteter. Likevel foreligger det en rekke rapporter og undersøkelser som gir et innblikk i brukernes inntrykk av, og erfaringer med, ulike offentlige aktører og tjenester, herunder flere av aktørene i den norske ID-forvaltningen.

Overordnet brukertilfredshet og omdømme for utvalgte aktører i ID-forvaltningen

Difis innbyggerundersøkelse viser at brukere generelt er fornøyd med tjenestene som leveres av ID-relaterte aktører. Målt på total tilfredshet skårer relevante aktører følgende: Fastlege (86/100), sykehus (80/100), Lånekassen (77/100), SVV (71/100), Skatteetaten (71/100), politi (69/100) og NAV (60/100).[234] Myndighetsorganene, spesielt Lånekassen og Skatteetaten, er blant aktørene som har vist størst positiv utvikling siden tilsvarende undersøkelse ble gjennomført i 2015. Målt på tillit skårer også nesten alle nevnte aktører over 70[235]. Unntaket er NAV, som kun får 59/100 poeng. En brukerundersøkelse ble også gjennomført for utlendingsforvaltningen i 2017. Resultatene viste en positiv utvikling i brukertilfredsheten både for politiet, utenriksstasjonene og UDI.[236] Det bør påpekes at rapportene måler brukernes generelle tilfredshet og tillit til aktørene, og ikke er direkte knyttet opp mot virksomhetenes ID-relaterte aktiviteter.

Kantar sin omdømmemåling av offentlig sektor (2018) nyanserer dette bildet. Selv om Lånekassen også her anses til å ha et sterkt omdømme, har omdømmet til Skatteetaten, politiet og Difi blitt klassifisert som «sårbart». SVV, UDI og NAV anses etter rapporten klassifiseringsmetodikk til å ha «svakt omdømme».[237]

Brukervennlighet og tilfredshet med offentlige digitale løsninger

En økende andel av brukerens møte med det offentlige foregår på digitale flater. Dette får konsekvenser for ID-forvaltningen i form av økt grad av elektroniske autentiseringer

[234] Difi, «Innbyggerundersøkelsen 2017 – hva mener brukerne», 2017
[235] Målinger >70 kategoriseres som «fornøyd» i henhold til metodikken benyttet i rapporten
[236] UDI, UD og POD, «Brukerundersøkelse for utlendingsforvaltningen», 2017
[237] Kantar TNS, «Offentlig Omdømme», 2018. *Merk: «Omdømme» klassifiseres i rapporten som særdeles sterkt, sterkt, sårbart eller svakt*

for tilgang til offentlige digitale tjenester. Samtidig vil også prosesser for utstedelser av ID-bevis i større grad foregå elektronisk eller ved hjelp av selvbetjeningsløsninger.

I en rapport gjennomført på vegne av KMD har brukere svart på deres opplevelse av brukervennligheten til offentlige digitale tjenester og nettsider. 37 prosent av respondentene opplever det som enten enkelt eller svært enkelt å orientere seg i offentlige digitale tjenester.[238]

Innbyggerne har også generelt et godt inntrykk av sentrale statlige publikumstjenester på nett: Altinn.no (75), Skatteetaten.no (74), Lånekassen.no (72), Vegvesen.no (70) og Nav.no (60).[239] Andelen som benytter selvbetjeningsløsninger varierer til dels mellom aktørene: Lånekassen (61 prosent), Skatteetaten (31 prosent) NAV (28 prosent), politi (13 prosent) og SVV (11 prosent).[240]

Kraftig vekst i antall innlogginger i ID-porten de siste årene (fra under 20 millioner i 2010 til over 140 millioner i 2018 – se kapittel 2.7.2 for grafisk fremstilling)[241] anses av Difi som å være en sterk tillitserklæring fra brukerne. Tall fra SSB viser også at Norge ligger i Europatoppen i bruk av offentlige nettjenester[242], mens Europakommisjonen[243] rangerer Norge svært høyt i grad av digitalisering i offentlig sektor sammenlignet med andre land. Analyser gjennomført av OECD underbygger dette bildet, men peker samtidig på at Norge har en fragmentert tilnærming til digitalisering av offentlig sektor.[244]

Bruketilfredshet med Folkeregisteret

Folkeregisteret er Norges «grunnregister» av personopplysninger og mer enn 20 000 offentlige og private aktører er brukere av opplysninger som Folkeregisteret tilbyr.[245] Registerets funksjon og rolle i ID-forvaltningen har tidligere blitt beskrevet i kapittel 2.2 og 3.1.1-3.1.4. Moderniseringen av Folkeregisteret er omtalt i kapittel 2.9.3.

I intervjuer gjennomført av leverandøren med sentrale aktører blir Folkeregisteret hyppig trukket frem som en styrke ved den norske ID-forvaltningen. Leverandøren vurderer videre at befolkningen generelt har tillit til opplysningene som er registrert i Folkeregisteret og at dette videre gir økt tillit til den norske stat. En brukerundersøkelse for Folkeregisteret gjennomført i 2018 underbygger en slik vurdering, og viser en gjennomgående tilfredshet med registeret og kvaliteten på innholdet.[246] Høy tillit og tilfredshet blant befolkningen er karakteristikker som også gjelder for Skatteetaten, som har det overordnede ansvaret for Folkeregisteret. Ifølge etatens årlige brukerundersøkelse hadde 80 prosent av respondentene i 2018 et ganske eller svært godt inntrykk av Skatteetaten.[247]

Ventetid for fornyelse av pass

Lange passkøer er en sak som tidvis har vært svært synlig i nyhetsbildet, og har i løpet av våren 2019 blant annet blitt omtalt i media som en «passkrise».[248] Særlig utgjør dette et problem på Østlandet og perioden frem mot sommerferieavvikling. Lange

[238] KMD (gjennomført av Sentio Research), «Et brukerperspektiv på digitaliseringen av offentlige tjenester», 2018
[239] Difi, «Hva mener innbyggerne», 2017
[240] Difi, «Innbyggerundersøkelsen 2017 – hva mener brukerne», 2017 (s. 44)
[241] Difi, «Innlogginger i ID-porten», 2019
[242] SSB, «Norge i europatoppen i bruk av offentlige nettjenester», 2019
[243] Europakommisjonen, «eGovernment Benchmark», 2018
[244] OECD, «Digital Government Review of Norway», 2017
[245] Skatteetaten, «Om prosjektet: Slik foregår moderniseringen av Folkeregisteret», u.å.
[246] Skatteetaten, «Årsrapport for Skatteetaten, 2018
[247] Skatteetaten/Opinion, «Befolkningsundersøkelse», 2018
[248] VG, «Passkrise på Østlandet: – Folk står i kø fra klokken syv og tidligere», 19.01.2019

ventetider for pass er følgelig blant de mer synlige eksemplene på negative brukeropplevelser i ID-forvaltningen.

5.1.2 Krav til legitimasjon for tilgang til offentlige tjenester og ytelser

Hvilke legitimasjonskrav som ligger til grunn for tilgang til utvalgte sentrale offentlige tjenester og ytelser varierer. Som tidligere poengtert i kapittel 4.2.3 eksisterer det heller ingen helhetlig oversikt eller lovfestet definisjon av hvilke norske ID-bevis som regnes som gyldige. For aktørene inkludert i tabellen under har leverandøren i følgende kapittel kartlagt hvilke krav til legitimasjon som fremkommer for utvalgte tjenester og ytelser.

Aktør	Tjenester og ytelser
Skatteetaten	Tilgang til skattekort for muligheten til å arbeide og betale skatt i Norge
Lånekassen	Støtte til utdanning
NAV	Stønader i forbindelse med arbeid (eksempelvis arbeidsavklaringspenger, dagpenger og sykepenger) Familierelaterte stønader (eksempelvis foreldrepenger, barnetrygd, kontantstøtte og barnebidrag) Pensjonsutbetalinger (eksempelvis alderspensjon og uføretrygd)
Det norske helsevesenet	Behandling i primær- og/eller spesialisthelsetjenesten
Altinn/ Brønnøysundregistrene	Stifte og registrere aksjeselskap

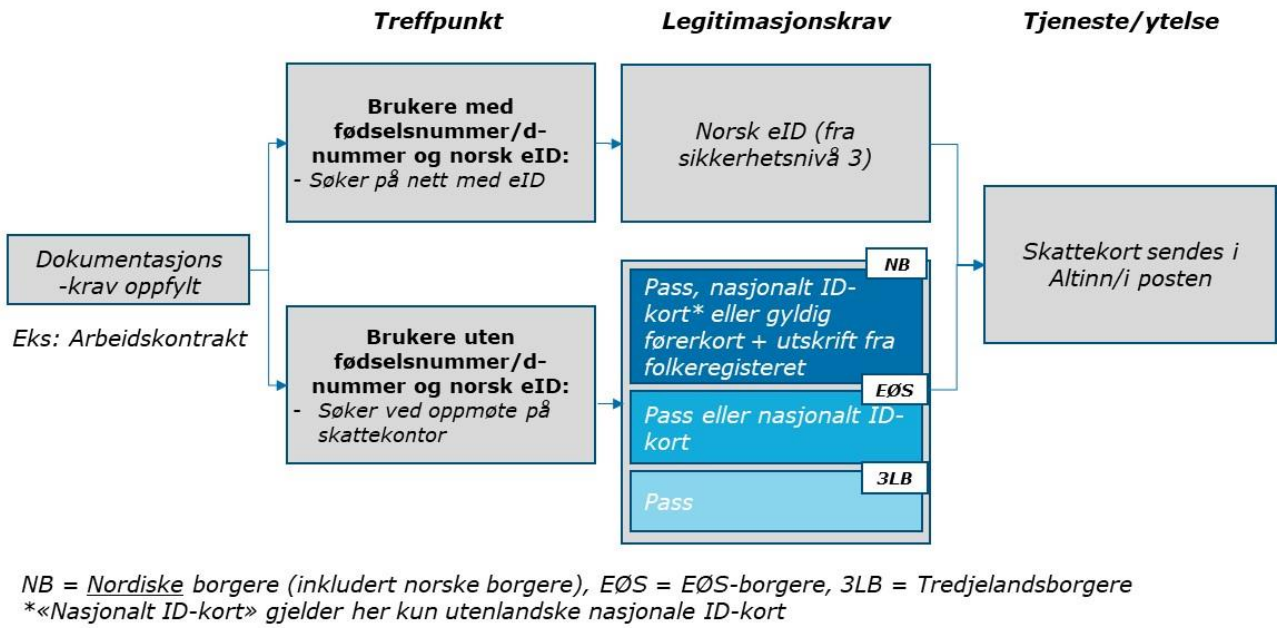
Tabell 10 Utvalgte offentlige tjenester og ytelser hvor legitimasjonskrav er kartlagt

Et sammendrag av leverandørens kartlegging knyttet til legitimasjonskrav for ulike tjenester og ytelser er illustrert i figur 25-29 under. For tilgang til offentlige tjenester og ytelser i utvalget kan ID-kontroll i all hovedsak gjennomføres med eID og behovet for oppmøte er særdeles begrenset. Krav til type ID-bevis, både for digital og fysisk ID-kontroll, varierer. En mer detaljert oversikt med kildehenvisning er beskrevet i vedlegg 6.

Skattekort

Figuren under viser gjeldende treffpunkt og legitimasjonskrav som ligger til grunn for anskaffelse av norsk skattekort. Dersom bruker innehar fødselsnummer eller d-nummer samt en norsk eID, er det tilstrekkelig å søke om skattekortet på nett. Norsk eID med sikkerhetsnivå 3 benyttes dermed til å kontrollere søkerens identitet. Søkere som ikke har norsk fødselsnummer eller d-nummer må søke om skattekort ved oppmøte på skattekontoret, og fremvise legitimasjon i henhold til statsborgerskap. Utover legitimasjonskravene som fremgår av figuren gjør Skatteetaten også unntak for enkelte grupper (eksempelvis asylsøkere og flyktninger).[249]

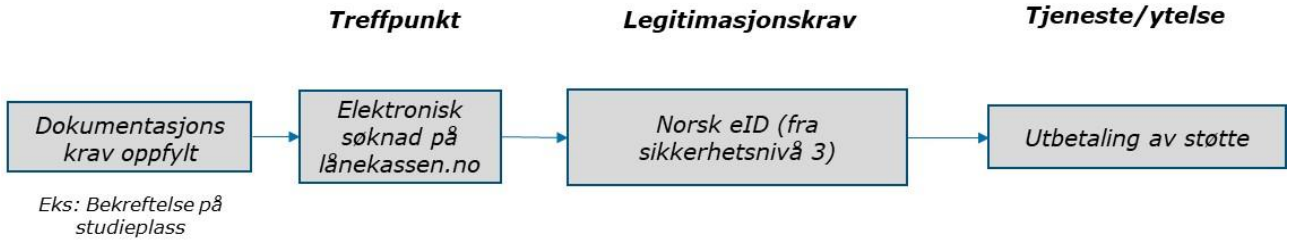
[249] Skatteetaten.no, «ID-kontroll», u.å.



Figur 25 Legitimasjonskrav for utstedelse av skattekort fra Skatteetaten[250]

Utdanningsstøtte

Som vist i figuren under stilles det krav om innlogging på lånekassens nettsider for å kunne søke om utdanningsstøtte. Det er ikke mulig å søke utelukkende på papir eller ved fysisk oppmøte. Både norske og utenlandske borgere må dermed inneha en norsk eID med minst sikkerhetsnivå 3 for å kunne søke om støtte. Dersom bruker kvalifiserer til støtte fra Lånekassen kan beløpet i utgangspunktet kun utbetales til en norsk bankkonto, som også fordrer at brukeren har et fødselsnummer eller et d-nummer for å kunne opprette.[251] Krav til innsending av dokumentasjon vil variere avhengig av hva slags støtte det søkes om, samt søkerens statsborgerskap og lovlige tilknytning til Norge. Likevel opplyses det ikke spesifikt om ytterligere krav til identifikasjon på Lånekassens nettsider utover behovet for innlogging med norsk eID.



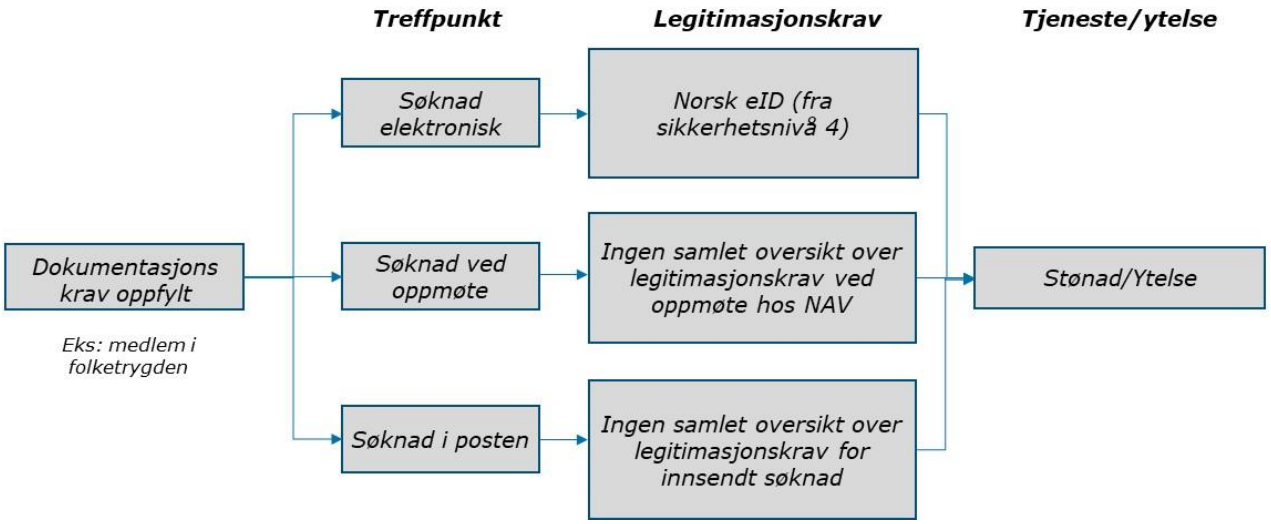
Figur 26 Legitimasjonskrav for støtte fra Lånekassen

Stønad/Ytelse

NAV tilbyr en rekke stønader og ytelser, der enkelte kan søkes om elektronisk mens andre kan, eller må, søkes om ved innsending av søknadsdokumenter i posten. Legitimasjonskravene beskrives nærmere under i figur 27. Innlogging på nav.no kan gjøres med norsk eID fra sikkerhetsnivå 3, men det stilles krav til sikkerhetsnivå 4 for å kunne søke om ytelser elektronisk. For søknad om stønad/ytelse ved innsending i posten eller ved oppmøte fremkommer det ingen samlet oversikt på NAV sine sider over hvilke ID-bevis NAV anser som gyldig legitimasjonsgrunnlag.

[250] Se kapittel 2.8.2 for nærmere beskrivelse av ulike sikkerhetsnivåer for eID
[251] Lånekassen.no, «Kan dere overføre pengene til min utenlandske konto?», u.å.

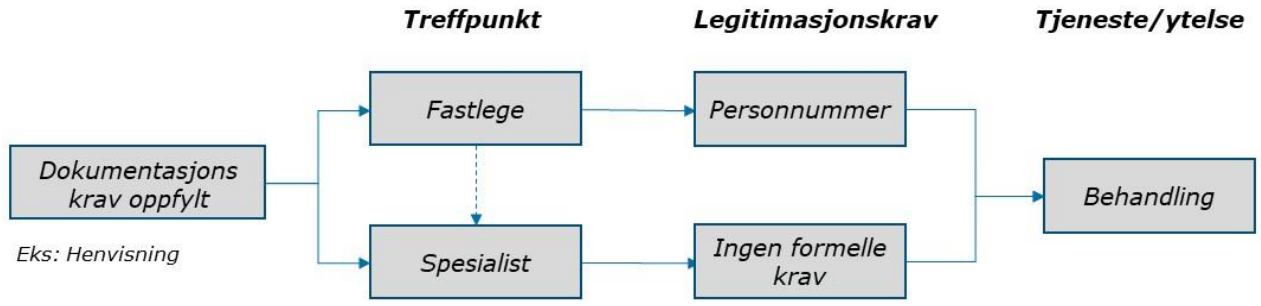
I folketrygdloven fremkommer det at «*en person som krever eller mottar en ytelse, plikter å legitimere seg ved å framvise pass eller annen gyldig legitimasjon når arbeids- og velferdsetaten krever det. Han eller hun plikter også å legitimere seg ved kontakt med helsepersonell eller andre med sikte på erklæringer eller uttalelser mv. til etaten som grunnlag for tilståelse eller fortsatt utbetaling av ytelser».*[252] Jf. § 21-4 er legitimeringen hos helsepersonell dog ikke nødvendig dersom stønadstaker er kjent for den som skal avgi erklæring eller uttalelse. Hva som ligger i begrepet «annen gyldig legitimasjon» spesifiseres ikke nærmere i lovteksten eller i forespurt materiale.



Figur 27 Legitimasjonskrav for stønad/ytelse fra NAV

Fastlege/spesialisthelsetjeneste

Figuren under illustrerer legitimasjonskrav som legges til grunn for behandling hos fastlege eller spesialisthelsetjenesten. For behandling hos fastlege vil det være tilstrekkelig å kunne oppgi sitt identitetsnummer, enten muntlig eller skriftlig. Etter samtaler med HOD, erfarer leverandøren videre at det per dags dato ikke foreligger formelle krav til fremleggelse av legitimasjon for behandling i primær- eller spesialisthelsetjenesten.



Figur 28 Legitimasjonskrav for behandling i primær- og spesialisthelsetjenesten

Stifte og registrere selskap

Figuren nedenfor gir en oversikt over hvilke legitimasjonskrav en bruker står overfor ved de ulike stegene som medgår i stiftelse og registrering av et aksjeselskap. Selve stiftelsen gjennomføres ved innsending av søknad på altinn.no. Bruker har her en rekke innloggingsalternativer til rådighet, blant annet norsk eID (fra sikkerhetsnivå 3),

[252] ASD, «Folketrygdloven, § 21-3», 01.05.1997

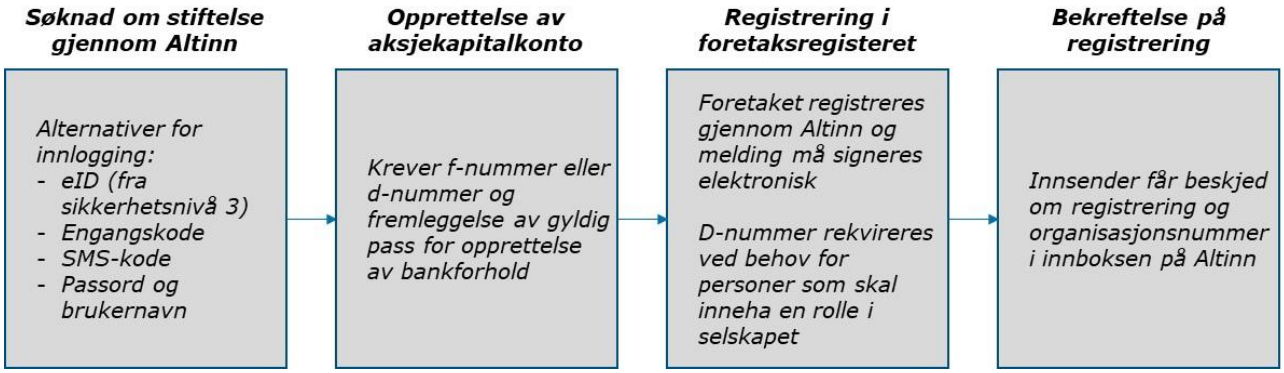
engangskodebrev, SMS-kode og passord/brukernavn.[253] Innloggingsmulighetene som er nevnt i det foregående som ikke benytter norsk eID er lagt til rette for i egen innloggingsløsning i Altinn. Disse benytter dermed ikke ID-porten som innloggingsportal. Det fremkommer at innlogging med brukernavn og passord kun gir tilgang til et *fåtall tjenester*, men det blir ikke nærmere spesifisert om dette inkluderer tilgang til portal for selskapsopprettelse.

Stifter må videre opprette en aksjekapitalkonto og be om bekreftelse på innbetalt aksjekapital fra banken. Dersom stifter ikke innehar en norsk bankkonto vil vedkommende måtte opprette dette hos banken ved fremleggelse av fødselsnummer eller d-nummer, samt gyldig pass.

Det vil deretter måtte innsendes melding om registrering i foretaksregisteret. Denne tjenesten er helelektronisk, og gjennomføres også på Altinn sine hjemmesider.[254] Ved registrering vil søker få tilsendt en melding i innboksen på Altinn som vil måtte signeres *elektronisk* av både stifter, styret, banken og revisor.

Det er nødvendig med fødsels- eller d-nummer dersom en person skal inneha en rolle i det opprettede selskapet (eksempelvis daglig leder eller styremedlem).[255] Dersom en person uten d-nummer skal inneha en rolle i det nyopprettede selskapet vil Brønnøysundregistrene rekvirere d-nummer for den det gjelder basert på innsendt søknad. Denne søknaden må sendes på papir, og med bekreftet kopi av et legitimasjonsdokument. Brønnøysundregistrene oppgir legitimasjonskravet til å «normalt være pass og nasjonalt ID-kort».[256] ID-kontrollen som gjennomføres er kun basert på innsendt kopi av ID-bevis, og er ikke tilstrekkelig for å få status «kontrollert» i Folkeregisteret før søker møter til ID-kontroll hos Skatteetaten.

Når registermelding er signert elektronisk av styret og banken vil innsender få beskjed i sin innboks på Altinn om at selskapet har blitt registrert.



Figur 29 Legitimasjonskrav for å stifte og registrere et AS

5.1.3 Krav til oppmøte og legitimasjon ved førstegangsutstedelse og fornyelse av ID-bevis

Hvilke ID-bevis som anses som gyldig legitimasjon ved utstedelse og fornyelse av andre ID-bevis varierer sterkt mellom de ulike ID-bevisene, og ID-kontroll ved førstegangsutstedelse og fornyelse gjennomføres stort sett ved personlig oppmøte. Leverandørens kartlegging av legitimasjons- og oppmøtekrav for førstegangsutstedelse

[253] Altinn.no, «Starte og registrere aksjeselskap», 2019
[254] Brønnøysundregisteret, «Samordnet registermelding», 2019
[255] Altinn.no, «Starte og registrere aksjeselskap», 2019
[256] Brønnøysundregisteret, «D-nummer», 2019

og fornyelse av ID-bevis er nærmere beskrevet i vedlegg 7. Et sammendrag av kartleggingen er illustrert i det påfølgende i tabell 11 og 12. Som illustrasjonen viser er det for alle ID-bevis (med unntak av MinID) krav om personlig oppmøte ved førstegangsutstedelse.

ID-bevis	Krav ved førstegangsutstedelse	Krav ved fornyelse
Norsk pass	Personlig oppmøte	Personlig oppmøte
Norsk førerkort	Personlig oppmøte	Personlig oppmøte[257]
Norsk bankkort med bilde[258]	Personlig oppmøte	Automatisk[259]
Oppholdskort[260]	Personlig oppmøte	Personlig oppmøte
Reisebevis for flyktninger	Personlig oppmøte	Personlig oppmøte
Utlendingspass	Personlig oppmøte	Personlig oppmøte
Norsk sjøfartsbok	Personlig oppmøte	Personlig oppmøte
MinID	Bestilles på nett	Ingen krav til fornyelse
BankID[261]	Personlig oppmøte	Automatisk
Buypass ID	Personlig oppmøte	Fornyes elektronisk[262]
Forsvarets ID-kort	Personlig oppmøte	Gjelder ut tjenesteperioden[263]
Nasjonalt ID-kort[264]	Personlig oppmøte	Personlig oppmøte

Tabell 11 Oppmøtekrav ved utstedelse

[257] Det kreves personlig oppmøte for fornyelse av førerkort dersom bildet skal fornyes
[258] Krav om fremvisning av pass og personlig oppmøte kan fravikes ved visse vilkår, Kilde: BITS, «Regler om utstedelse av legitimasjonsbevis/bankkort med bilde», 2018
[259] Bildet på bankkortet vil etter reglement fra BITS måtte oppdateres senest hvert 10. år. Kilde: BITS, «Regler om utstedelse av legitimasjonsbevis/bankkort med bilde», 2018
[260] Jf. beskrivelse i kapittel 2.3 regnes ikke oppholdskort som ID-bevis, men er inkludert i oversikten etter ønske fra JD
[261] Krav om fremvisning av pass og personlig oppmøte kan fravikes ved visse vilkår, Kilde: BITS, «Regler om utstedelse av legitimasjonsbevis/bankkort med bilde», 2018. For enkelte banker uten filialer vil ID-kontrollen gjennomføres ved postkontor (med fortsatt krav om fremleggelse av pass). Leverandøren viser til Sbanken som et eksempel
[262] BuyPass ID kan fornyes ved bruk av eksisterende eID dersom den ikke allerede er utløpt, Kilde: Svar fra BuyPass på forespørsel om kvalitet og sikkerhet
[263] Forsvarets ID-kort mottatt ved førstegangstjeneste gjelder ut tjenesteperioden
[264] Det legges til grunn at norsk nasjonalt ID-kort vil utstedes i henhold til forelagt plan for NPID-prosjektet

		Legitimasjon som kan benyttes ved førstegangsutstedelse av ID-bevis															
		Norsk pass	Utenlandsk pass	Norsk førerkort utstedt etter 1.januar 1998	Norsk bankkort med bilde	Forsvarets ID-kort	Postens ID-kort	Utenlandsk nasjonalt ID-kort (EØS-land)	Utenlandsk Nasjonalt ID med eID	Reisebevis for flyktninger	Utlendingspass	Norsk sjøfartsbok /Sjøfartskort	Oppholdskort	Fødselsattest*	Statsborgerbrev*	F-nummer*	D-nummer*
ID-bevis	Norsk pass																
	Norsk førerkort																
	Norsk bankkort med bilde																
	Oppholdskort*																
	Reisebevis for flyktninger												**				
	Utlendingspass												**				
	Norsk sjøfartsbok																
	MinID																
	BankID																
	BuyPass ID																
	Forsvarets ID-kort																
	Nasjonalt ID-kort																

Tabell 12 Legitimasjonskrav ved førstegangsutstedelse av ID-bevis

Figuren over gir en oversikt over hva som anses som gyldig legitimasjon ved førstegangsutstedelse av ID-bevis, gitt at alle andre dokumentasjonskrav for utstedelse er oppfylt. Celler markert i grønn viser til legitimasjon (markert i blått i øverste rad) som er oppført av utstedende myndighet som tilstrekkelig for å utstede ID-bevis (markert i grått i kolonne til venstre). Gule celler viser til underbyggende ID-bevis eller ID-dokumenter som ikke alene er tilstrekkelig for utstedelse, men som i visse tilfeller må framvises sammen med annen legitimasjon. Eksempelvis for utstedelse av norsk pass oppgir politiet norsk førerkort og bankkort med bilde som gyldig legitimasjon (markert med grønn), men vil ved førstegangsutstedelse også kunne kreve fremleggelse av fødselsattest eller statsborgerbrev (markert med gul) for å stadfeste statsborgerskap. Norsk bankkort med bilde kan benyttes som et annet eksempel, der det ifølge regelverket fra BITS stilles krav om fremleggelse av gyldig norsk eller utenlandsk pass (markert grønn). Utover dette kravet vil bruker måtte inneha et norsk f-nummer eller d-nummer (markert gul).

*Fødselsattest, statsborgerbrev, fødselsnummer og d-nummer regnes ikke som legitimasjon. De er likevel inkludert i matrisen da de i mange tilfeller er med på å underbygge fremvist legitimasjon, og i visse tilfeller kan alene utgjøre grunnlag for utstedelse av ID-bevis (eksempelvis er fødselsnummer tilstrekkelig for å få tilsendt MinID). Jf. beskrivelse i kapittel 2.3 regnes oppholdskort heller ikke som et ID-bevis, men er inkludert i oversikten etter ønske fra JD.

**Det fremgår av UDIs rundskriv RS 2012-009 at utstedelse av reisebevis og utlendingspass hviler på identitetsfastsettelsen gjennomført ved innvilgelse av opphold. Det fremgår videre av Utlendingsforskriften paragraf 12-11 at «*pass eller annet reisedokument søkeren er i besittelse av, må innleveres*» ved søknad om reisebevis eller utlendingspass, samt at «*politiet skal om nødvendig forlange fremlagt de legitimasjonspapirene søkeren har eller kan skaffe, og eventuell dokumentasjon av søkerens status som flyktning*».[265] Hvilke legitimasjonspapirer dette gjelder fremgår ikke av forskriftene (utover eventuelt eksisterende eller utgått pass/reisebevis), og spesifiseres heller ikke nærmere på politiets eller UDI sine nettsider.[266]

5.1.4 Bruksmønstre for digitale og fysiske ID-bevis

Antall ganger en bruker reelt benytter ID-bevis som legitimasjonsgrunnlag gjennom et livsløp vil variere for ulike ID-bevis. Leverandøren er ikke kjent med om det foreligger statistikk eller annen form for helhetlig oversikt over totalt antall årlige fremvisninger av ulike ID-bevis i Norge.

Bruksmønster - fysiske ID-bevis

Mange brukere må benytte pass til førstegangsutstedelse av enkelte ID-bevis, blant annet ved anskaffelse av bankkort med bilde/BankID, sjøfartskort, fornyelse av pass samt fremtidig utstedelse av nasjonalt ID-kort slik vist i tabell 12 over. Utover utstedelsen av nevnte ID-bevis er passets funksjon sannsynligvis i hovedsak tilknyttet brukerens reisevirksomhet. Dette vil være delvis begrenset som følge av Norges deltagelse i Schengenområdet, som gir grunnlag for å reise innen områdets 26 medlemsland uten å gjennomgå kontroll av pass.[267] Det er nærliggende å tro at dette vil gjelde for en ikke-ubetydelig andel av nordmenns reisevirksomhet, og vil i den forstand innebære en betydelig tidsbesparelse for både bruker og kontrollerende

[265] JD, «Utlendingsforskriften §12-11», 15.10.2009
[266] UDI, «Sjekkliste for utlendingspass», u.å.
[267] UDI, «Schengen / Schengenområdet», 2019

myndighet. Likevel vil pass ofte også måtte medbringes som følge av legitimasjonskrav fra ulike virksomheter i utlandet.

Videre vil en bruker gjennom et livsløp stå overfor en rekke situasjoner som krever fremleggelse av et fysisk ID-bevis. Noen eksempler inkluderer kontroll av ID ved skattekontor, henting av rekommandert sending på postkontor, ulike kontrollaktiviteter gjennomført av politiet, adgang til lokaler av et visst sikkerhetsnivå eller ved behov for å kontrollere alder. Behovet for fremvisning av fysiske ID-bevis for ID-kontroll for tilgang til offentlige ytelser eller tjenester, som vist i kapittel 5.1.2, er begrenset. Behovet for fremvisning av fysiske ID-bevis til det offentlige er vesentlig lavere enn øvrige eksempler nevnt over.

Statistikk over fremvisningen av ulike ID-bevis i Norge er som nevnt innledningsvis begrenset. Leverandøren er likevel forelagt materiale som gir et overordnet bilde på hvilke ID-bevis som benyttes til utleveringer av sendinger (brev, pakker og gods) hos Posten Norge. Av totalt 1,64 millioner sendinger i perioden 2017 til 2018 ble 44 prosent hentet ved fremvisning av bankkort med bilde, 41 prosent med førerkort, 9 prosent med pass eller reisebevis, 5 prosent med Europeisk ID-kort og 1 prosent med postens ID-kort.

Bruksmønster – elektroniske ID-bevis

Overordnet vil antall ganger en bruker benytter eID til autentisering overfor det offentlige gjennom et livsløp overstige bruken av fysisk ID-bevis som legitimasjonsgrunnlag. Utstedelse av eID forutsetter et fysisk ID-bevis for å verifisere identiteten. Figurer 25-29 viser at en bruker som har anskaffet gyldig norsk eID i stor grad kan benytte dette til sin digitale interaksjon med offentlig sektor. Som tidligere omtalt i kapittel 2.8.2, var det om lag 139 millioner innlogginger gjennom ID-porten i løpet av 2018, noe som tilsvarer i underkant av 30 innlogginger i gjennomsnitt per borger per år. Utover dette benytter borgerne eID til autentisering mot private aktører i utstrakt grad.

5.1.5 Overordnet beskrivelse av brukerreise for anskaffelse av utvalgte ID-bevis, med tilhørende brukertid og brukergebyr (for norske borgere)

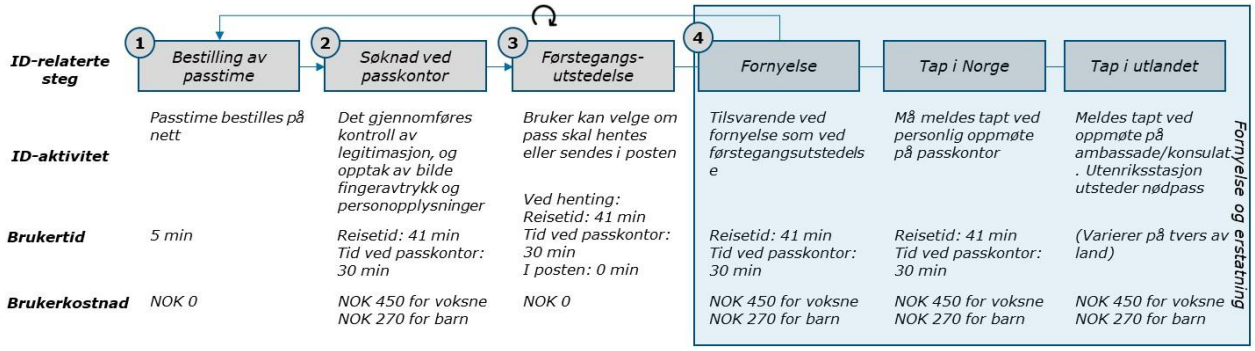
Beskrivelse av brukerreise for anskaffelse av ID-bevis

Leverandøren har kartlagt hvilke steg en norsk borger må gjennom for å anskaffe ID-bevis, samt deres tilhørende brukertid og brukergebyr. I figurene under er dette illustrert for noen av de mest brukte ID-bevisene for norske borgere. Brukergebyr gjelder her kun gebyr for utstedelse av ID-kortet, og vil ikke omfatte eventuelle transportkostnader til og fra utstedelsespunkt. Brukertid inkluderer tid benyttet til transport, samt total oppholdelsestid ved utstedelsespunkt (herunder tid benyttet til venting, registrering av personinformasjon, bildetaging og kontroll av ID). Definisjonene som ligger til grunn for brukertid og brukergebyr er nærmere beskrevet innledningsvis i leverandørens definisjonsoversikt, og utbredelsen av nevnte ID-bevis er nærmere beskrevet i kapittel 2.8.

Figuren under forklarer hvilke steg en bruker må gjennom for henholdsvis førstegangsutstedelse og fornyelse/erstatning av tapt pass (markert i blå boks i figuren), samt estimert brukertid og brukergebyr som påløper ved hvert steg. Som det fremkommer av figuren må passtime bestilles av bruker på forhånd, før bruker må møte fysisk på passkontor til avtalt tid. Bruker kan i dag gjøre dette på 141 passkontorer i Norge (ref. tabell 6 i kapittel 3.1.1). Ved utstedelse kan bruker velge om passet skal hentes personlig, eller om det skal sendes i posten. For fornyelse av pass

ved utløpsdato, samt erstatning av tapt pass, gjelder tilsvarende prosess som ved førstegangsutstedelse.

Politiet sender pass (førstegangsutstedelse og fornyelse) i vanlig postgang, og passet skal være tilgjengelig for brukeren innen 10 dager.[268]

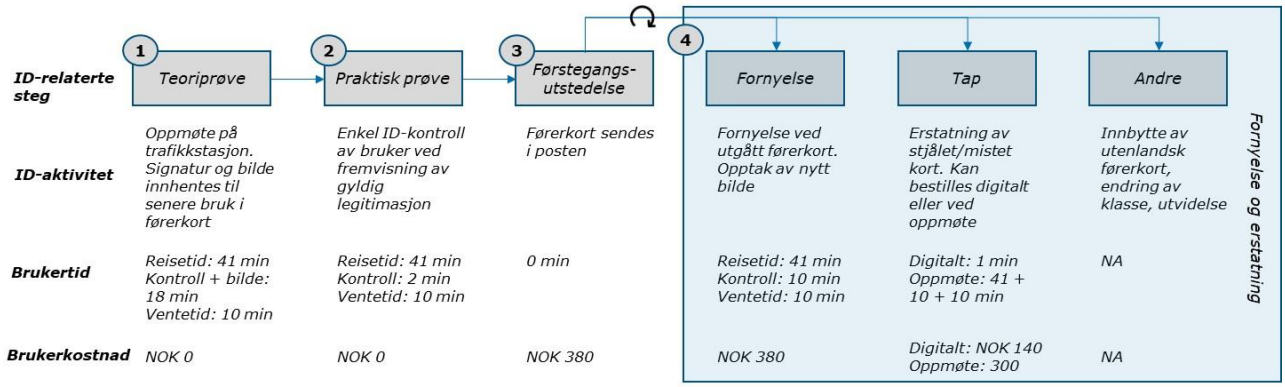


Figur 30 Brukerreise for anskaffelse av norsk pass (norske borgere)[269]

Som vist i figuren under er brukerens første ID-relaterte steg ved førstegangsutstedelse av norsk førerkort å møte ved trafikkstasjon for å gjennomføre teoriprøve. Det er ved dette oppmøtet at signatur og ansiktsfoto innhentes for senere bruk i førerkortet. Bruker må møte ved trafikkstasjon igjen ved praktisk prøve, der det gjennomføres en enkel kontroll av brukers legitimasjon. Dersom bruker består den praktiske prøven vil førerkortet sendes hjem til vedkommende i posten. Ved førerkortets utløp vil bruker måtte møte igjen ved trafikkstasjonen for å fornye kortet, i all hovedsak fordi bruker må ta nytt bilde til førerkortet. Førstegangsutstedelse og fornyelse av førerkort ved oppmøte kan gjennomføres ved en av statens 72 trafikkstasjoner (ref. tabell 6 i kapittel 3.1.1). Dette skiller seg fra prosessen for å erstatte tapt førerkort, der bruker får mulighet til å bestille et duplikat digitalt uten å måtte møte opp fysisk.

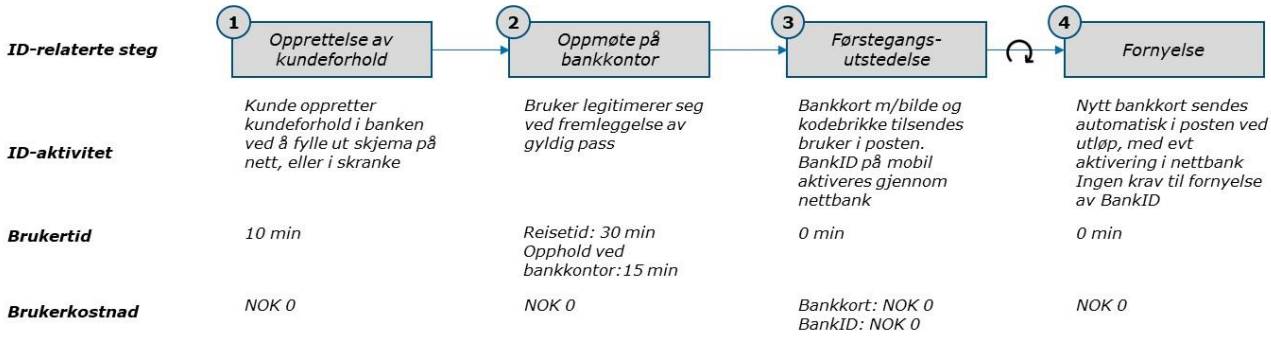
Ved forsendelse av førerkort i posten (førstegangsutstedelse og fornyelse) er normal leveringstid syv virkedager. Ved tapt førerkort må bruker vente minst fire uker før nytt førerkort kan bestilles.[270]

[268] Politiet.no, «Pass og timebestilling», u.å.
[269] Gebyr og informasjon om steg 1-4 hentet fra politiets hjemmesider. Brukertid basert på forutsetninger fra Menon, «Samfunnsøkonomisk analyse av redusert gyldighetstid på pass», 2018 og leverandørens egne vurderinger:
Tid ved passkontor: «Enhver person som besøker passkontoret, uavhengig om vedkommende er samsøker eller ikke, bruker 30 minutter»
Kjøretid: Gjennomsnittlig kjøretid på 20,27 min én vei, basert på scenario om 102 passkontorer (scenario valgt pga. nærmest dagens antall passkontorer)
Bestilling av passtime: Leverandøren benytter en antagelse om brukertid på 5 minutter for bestilling av passtime på nett
[270] Vegvesen.no, «Bestill førerkort», 2019



Figur 31 Brukerreise for anskaffelse av norsk førerkort (norske borgere)[271]

Figur 32 under tar for seg brukerreisen for bankkort med bilde og BankID. For å anskaffe et bankkort med bilde, BankID eller BankID på mobil, må bruker først opprette et kundeforhold i banken. Opprettelse av kundeforholdet kan gjøres både på nett eller i skranken, men det stilles krav om fysisk oppmøte og fremleggelse av gyldig pass for å kunne utstede bankkort med bilde, BankID og BankID på mobil. Kravet til fremvisning av legitimasjon gjelder kun ved første opprettelse av kundeforholdet, men bruker vil etter reglementet også måtte fornye bilde på bankkortet ved oppmøte hvert tiende år. Ifølge tall fra Finans Norge eksisterer det om lag 940 ekspedisjonssteder (hovedkontorer og bankfilialer) som vil kunne behandle brukerhenvendelse ved fysisk oppmøte.[272]



Figur 32 Brukerreise for anskaffelse av bankkort med bilde, BankID og BankID på mobil[273]

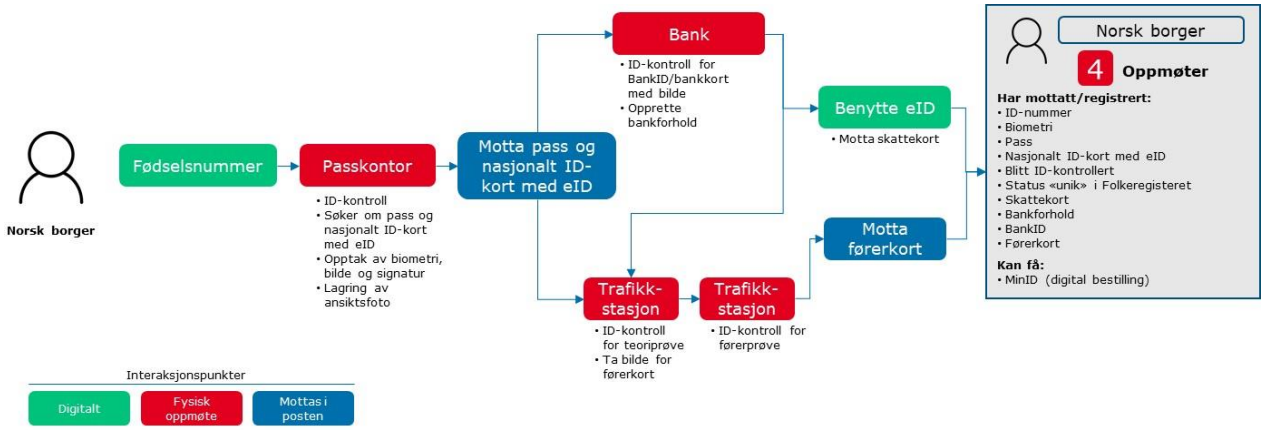
[271] Tall for tidsbruk for ID-kontroll og gjennomsnittlig kjøretid til trafikkstasjon er oppgitt av SVV (41 minutter tur/retur basert på dagens struktur i 2020). Leverandøren legger til grunn en antagelse om gjennomsnittlig ventetid ved utstedelsespunkt på 10 minutter per utstedelse

[272] Finansnorge.no, «Antall ekspedisjonssteder», 2017

[273] Om bankkort: Førstegangsutstedelse eller fornyelse av bankkort er ikke i seg selv gebyrbelagt. Det vil derimot som regel påløpe en fast kostnad for bankkortets innehaver, uavhengig av fornyelse eller antall transaksjoner, samt uavhengig av om bankkortet er utstedt med eller uten bilde. Årsgebyret varierer noe mellom banker og kundesegmenter hos bankene. Etter leverandørens vurdering er årsgebyret en kostnad som primært knytter seg til bankkortets funksjon som betalingskort, og ikke en direkte ID-kostnad. Brukergebyret tilknyttet bankkort med bilde er derfor satt til 0 kroner. Enkelte banker uten filialer vil benytte seg av legitimering ved postkontor (Personlig utlevering mottakingsbevis PUM). Dersom bruker allerede har opprettet et bankforhold, vil ikke opprettelse av et nytt bankforhold nødvendigvis stille krav til oppmøte. Leverandøren legger til grunn en antatt gjennomsnittlig reisetid til utstedelsespunkt på 30 minutter tur/retur, 10 minutter for opprettelse av kundeforhold samt 15 minutter opphold hos bankkontor ved oppmøte

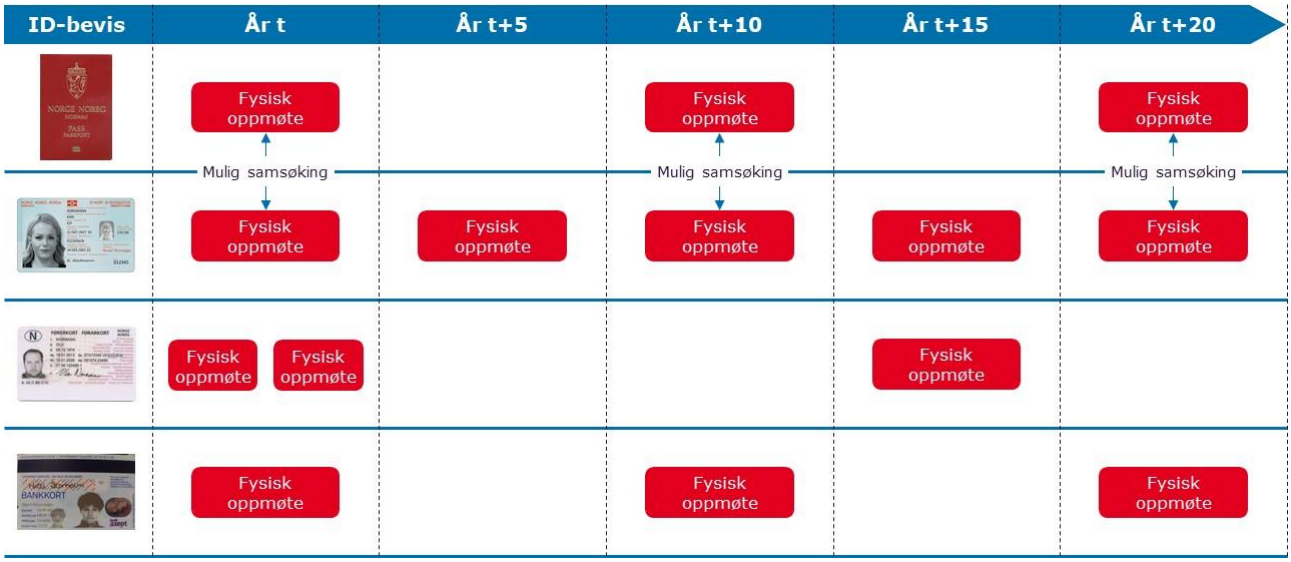
Eksempel på brukerreise for førstegangsutstedelse av identitetsnummer og ID-bevis for norske borgere med dagens løsning og vedtatte planer for nasjonalt ID-kort med eID

Figuren under illustrerer et eksempel på en norsk borgers brukerreise for førstegangsutstedelse av identitetsnummer og utvalgte ID-bevis. Figuren legger til grunn dagens prosess for utstedelse av ulike ID-bevis, samt vedtatte planer for nasjonalt ID-kort med eID. Brukerreisen viser at en norsk borger må gjennom fire oppmøter for å få utstedt pass, nasjonalt ID-kort med eID, førerkort, bankkort med bilde og BankID.



Figur 33 Eksempel på brukerreise for norsk borger for førstangsutstedelse av ID-bevis

Figuren under illustrerer overordnet hvilke fysiske oppmøter en bruker må gjennom for førstegangsutstedelse og fornyelse av utvalgte ID-bevis over tid, gitt gjeldende krav til fornyelse og gyldighetstid, samt vedtatte planer for nasjonalt ID-kort.



Figur 34 Oppmøter ved utstedelse og fornyelse av ID-bevis med dagens løsning og vedtatte planer for nasjonalt ID-kort med eID

5.1.6 Overordnet beskrivelse av brukerreise for anskaffelse av ID-bevis og identitetsnummer, med tilhørende brukertid og brukergebyr (for EØS-borgere og tredjelandsborgere)

Leverandøren har i det følgende kartlagt hvilke steg EØS-borgere og tredjelandsborgere må gjennom for å tilegne seg et d-nummer, samt overordnet

beskrevet prosessen for å anskaffe sentrale ID-bevis. Kartleggingen har i hovedsak fokusert på brukerreisen tilknyttet de største rekvirentene (Skatteetaten og NAV), samt brukerreisen for utvalgte ID-bevis (norsk førerkort og bankkort med bilde).

Tildeling av d-nummer

Som beskrevet i kapittel 6.1.2 har en rekke aktører myndighet til å rekvirere et d-nummer, dersom bruker ikke har et norsk identitetsnummer fra før og det foreligger et begrunnet behov. Aktører som har myndighet til å rekvirere d-nummer er Skatteetaten, NAV, Brønnøysundregisteret, banker, Kartverket, utenriksstasjoner, VPS, Helfo, UDI, PU og UNE. Majoriteten av d-nummer tildelt i 2018 ble rekvirert av Skatteetaten (56 prosent) og NAV (36 prosent). Leverandøren vil i det følgende beskrive de steg som inngår for bruker i å få tildelt d-nummer hos de to største rekvirentene (NAV og Skatteetaten), samt hvilken brukertid og brukergebyr som påløper.

Tildeling av d-nummer gjennom NAV

NAV kan bestille d-nummer på vegne av EØS-arbeidssøkere og for mottakere av ytelser.[274] Om lag 96 prosent av rekvisisjoner fra NAV er knyttet til EØS-borgere.[275]

En bruker søker ikke om d-nummer direkte, men d-nummer rekvireres av NAV når det er nødvendig for å behandle henvendelse eller sak. Det er kun NAV-kontorene og ytelseslinjen som har fullmakt til å rekvirere d-nummer. NAV-kontorene kan kun rekvirere d-nummer for EØS-borgere som skal registrere seg som arbeidssøkende i Norge, mens ytelseslinjen rekvirerer for alle andre saker. Dersom en EØS-borger uten norsk identitetsnummer skal registrere seg som arbeidssøker hos NAV, vil vedkommende måtte møte fysisk på et NAV-kontor (elektronisk registrering er forbeholdt brukere med norsk eID fra sikkerhetsnivå 4[276]). Dette kan gjennomføres ved et av NAV sine 456 kontorer (ref. tabell 6 i kapittel 3.1.1). Enheter i ytelseslinjen rekvirerer derimot d-nummer kun på grunnlag av dokumenter som er sendt inn eller innhentet i en søknadsprosess, ikke ved personlig oppmøte.[277]

I et eksempel der en EØS-borger har rett på ytelser fra NAV, men ikke har et norsk identitetsnummer, vil en søknad om ytelse resultere i at d-nummer blir rekvirert for brukeren uten krav til oppmøte.[278] En slik prosess er beskrevet i tabell 13 under.

[274] Skatteetaten.no, «D-nummer», 2019
[275] Basert på data mottatt fra representanter i NAV
[276] Nav.no, «Arbeidssøkerregistrering», u.å.
[277] NAV, «Rutine for rekvirering av d-nummer», 2019
[278] Jf. «Rutine for rekvirering av d-nummer», 2019 kan ytelseslinjen i NAV rekvirere d-nummer for følgende grupper av personer: *1) Barn og/eller ektefelle av et medlem i folketrygden, når bruker søker om ytelse fra NAV, 2) Part og/eller barn i bidragssak som skal behandles etter norske regler om underholdsbidrag, eller 3) Personer som har behov for at NAV registrerer opplysninger om medlemskap i norsk eller utenlandsk trygdeordning*

	Steg 1	Steg 2	Steg 3
Beskrivelse	Bruker sender inn dokumentasjon i forbindelse med søknad om ytelse	Saksbehandler i NAV benytter informasjon i dokumentene til å automatisk rekvirere d-nummer fra Skatteetaten. D-nummeret returneres normalt i løpet av få minutter	Bruker får brev om tildelt d-nummer i posten.
Brukertid	Tid til innsamling og innsending av nødvendige dokumenter	0 min	0 min
Brukergebyr	0 kroner	0 kroner	0 kroner

Tabell 13 Brukerreise for rekvirering av d-nummer uten oppmøte (eks ved NAV Ytelse)

Brukerreise for tildeling av d-nummer gjennom Skatteetaten

Skatteetaten, ved skattekontoret, rekvirerer d-nummer til skatte- og avgiftspliktige personer.[279] Som beskrevet i kapittel 6.1.2 krever skattekontoret personlig oppmøte og ID-kontroll ved søknad om skattekort, med enkelte unntak. Leverandøren tar ikke her stilling til unntakene i kartleggingen av brukerreiser. Brukerreisen for anskaffelse av skattekort (og tilhørende d-nummer) for EØS-borgere og tredjelandsborgere er beskrevet på Skatteetaten sine nettsider[280]. De overordnede stegene er gjengitt i det følgende, og oppsummert i tabellen under.

Steg 1 – Timebestilling: Bruker må bestille time på Skatteetaten.no. Det påløper i praksis ingen brukergebyr eller brukertid ved bestillingen.

Steg 2 - Transport til skattekontor: Bruker må reise til skattekontor i henhold til innkalling/timebestilling. Gjennomsnittlig reisetid tur/retur estimeres til 50 minutter.[281]

Steg 3 - Opphold på skattekontor: Bruker leverer ferdig utfylt papirsøknad om skattekort for utenlandske borgere (RF-1209)[282]. Bruker må kunne dokumentere behov for skattekort og gjennomgår ID-kontroll ved oppmøte på et av Skatteetatens 42 utvalgte kontor (ref. kapittel 3.1.1). Krav til legitimasjon er forskjellig for EØS-borgere og tredjelandsborgere.[283] Estimert tid som bruker oppholder seg på skattekontoret i forbindelse med ID-kontroll er estimert til 25 minutter.[284] Anskaffelsen av skattekortet er gebyrfritt. Bruker får bekreftelse på tildelt d-nummert i skranken etter at vedkommende har gjennomført ID-kontroll.[285]

Skattekortet blir normalt klart innen fem virkedager. Skattetrekksmeldingen mottas elektronisk i Altinn, og arbeidsgiver får muligheten til å laste ned skattekortet elektronisk. Det er ikke behov for bruker å levere skattekortet til arbeidsgiver.[286]

[279] Skatteetaten.no, «D-nummer», 2019
[280] Skatteetaten.no, «Søknad om skattekort for utenlandsk borger», u.å.
[281] Ingen dokumentasjon forelagt leverandør. Estimert basert på tjenestestruktur for passkontor og trafikkstasjoner som sammenligningsgrunnlag
[282] Skatteetaten.no, «Søknad om skattekort for utenlandske borgere», 2019
[283] Skatteetaten.no, «ID-kontroll», 2019
[284] Skatteetaten oppgir på sine nettsider at det settes av 15 minutter for hver avtale ved oppmøte på skattekontor. Leverandøren er imidlertid forelagt informasjon fra FIN om at ID-kontrollen ved skattekontoret i realiteten tar ca. 25 minutter i gjennomsnitt
[285] Skatteetaten.no, «D-nummer», 2019
[286] Skatteetaten.no, «Søknad om skattekort for utenlandske borgere», 2019

	Steg 1	Steg 2	Steg 3
Beskrivelse	Bruker bestiller time hos skattekontor på skatteetaten.no	Bruker reiser til skattekontor i henhold til innkalling/ timebestilling	Opphold ved skattekontor (ventetid, behandling i skranke og ID-kontroll)
Brukertid	Tilnærmet 0 min	Estimert til 50 min	25 min
Brukergebyr	0 kroner	0 kroner	0 kroner

Tabell 14 Brukerreise for rekvirering av d-nummer ved skattekontor

Brukerreise for anskaffelse av norsk førerkort (EØS- og tredjelandsborgere)

Både EØS-borgere og tredjelandsborgere må være registrert i Folkeregisteret med f-nummer eller d-nummer for å få utstedt norsk førerkort,[287] og vil derfor forut for eventuell anskaffelse måtte gjennomgå prosess for rekvirering av d-nummer eller fødselsnummer.

Dersom bruker ikke innehar et førerkort fra eget hjemland fra før, vil vedkommende måtte gjennomgå prosesstegene som beskrevet i figur 31 (*Brukerreise for anskaffelse av norsk førerkort*). Dette vil i hovedsak foregå på lik linje som for norske borgere, med unntak av enkelte ulike krav til fremleggelse av utenlandsk legitimasjon.[288]

Brukere med førerkort fra EU/EØS-land kan velge å kjøre med kortet i Norge, eller bytte det direkte inn til norsk førerkort i tilsvarende klasse uten å måtte ta nye prøver. Utfylt søknad (inkludert fødselsnummer eller d-nummer) leveres på trafikkstasjon eller per post sammen med originalt førerkort og bostedsattest.[289]

SVV godkjenner innbytte av førerkort for tolv land utenfor EU/EØS.[290] Dersom brukerens førerkort er fra et land utenfor oppgitt liste vil vedkommende måtte søke norsk førerkort på lik linje med norske førstegangssøkere (se figur 31).

Brukerreise for anskaffelse av norsk bankkort med bilde (EØS- og tredjelandsborgere)

Det er krav til at brukerens fødselsnummer eller d-nummer skal fremkomme på bankkortet.[291] Bruker vil således måtte tilegne seg et f- eller d-nummer forut for utstedelse av bankkort med bilde.[292] For EØS-borger og tredjelandsborger som allerede innehar f- eller d-nummer vil anskaffelsesprosessen foregå tilsvarende som for norske borgere (se figur 32).

EØS-borgere og tredjelandsborgere vil ved førstegangsutstedelse måtte legitimere seg med gyldig utenlandsk pass, eller «andre dokumenter som etter en konkret risikobasert vurdering anses som gyldig legitimasjon med samme sikkerhetsnivå som pass». Den enkelte bank kan fravike kravet om fremlagt pass under visse vilkår, men vil da måtte

[287] Lovdata, «Førerkortforskriften», 2019
[288] Av utenlandsk legitimasjon godtar SVV utenlandsk pass (ikke nødpass) og ID-kort fra andre EU/EØS-land, dersom bruker i tillegg til å vise ID kan oppgi sitt fødselsnummer eller d-nummer enten muntlig eller skriftlig. Kilde: Vegvesen.no, «Gyldig legitimasjon», 2019
[289] SVV, «Innbytte av førerkort fra land innenfor EU/EØS», 2019
[290] SVV, «Innbytte av førerkort fra land utenfor EU/EØS», 2019
[291] BITS, «Regler om utstedelse av legitimasjonsbevis (Bankkort med bilde)», 2018
[292] Banker og finansinstitusjoner har også myndighet til å rekvirere d-nummer for personer som innehar et «forretningsforhold med et norsk finansforetak». Rekvirerte d-nummer fra banker utgjør imidlertid en svært lav andel av totalt antall rekvirerte d-nummer, og leverandøren har ikke avklart nærmere hva som ligger til grunn for bankenes rekvirering

kreve fremleggelse av annen form for legitimasjon i henhold til krav fremsatt i hvitvaskingsloven.

Det fremkommer ikke tydelig fra BITS sitt reglement hvilke ID-bevis som anses som gyldige under de vilkår der pass ikke kan fremlegges, samt hva som i praksis skal ligge til grunn for den fysiske ID-kontrollen. Administrasjonen i BITS stiller seg til disposisjon for nærmere veiledning om «hva som menes med dokumenter likestilt med utenlandsk pass samt hvilken grad banken skal kreve tilleggsdokumentasjon for stadfesting av utenlandske personers identitet».[293]

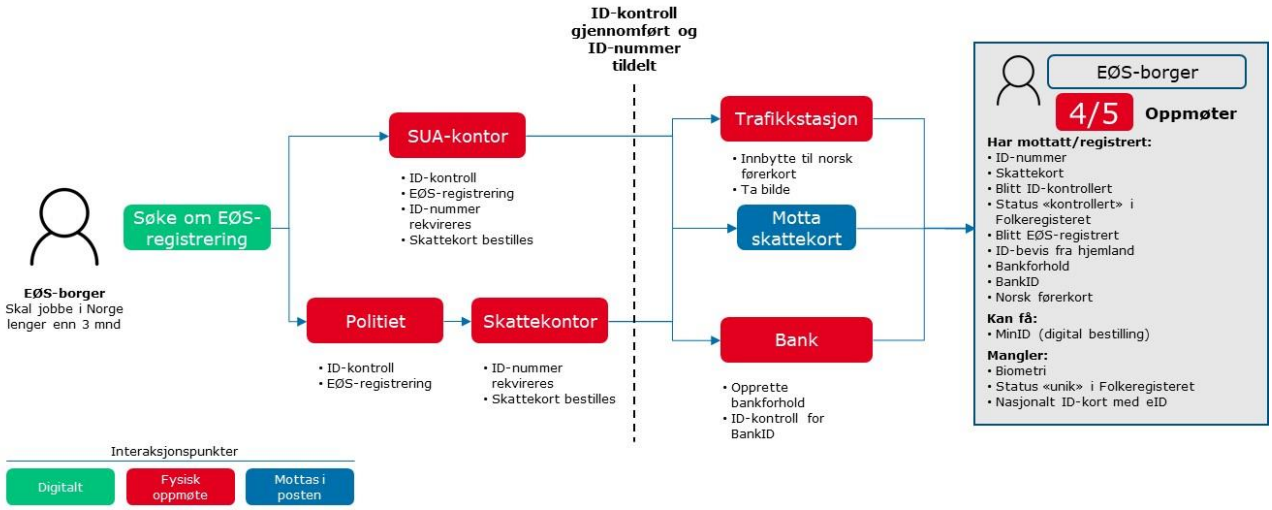
Nærmere om brukerreise for asylsøkere ved ankomst til Norge

Leverandøren er forelagt informasjon fra PU om at fingeravtrykk opptas to ganger for asylsøkere ved ankomst til Norge.[294] Prosessen beskrives som svært arbeidskrevende og kan ta opp mot 20 minutter per asylsøker. Ytterligere tidsbruk anslås i de tilfeller hvor asylsøker har mange treff i Eurodac og VIS.

Eksempel på dagens brukerreiser for førstegangsutstedelse av identitetsnummer og ID-bevis for EØS-borgere og tredjelandsborgere

Figurene under viser eksempler på brukerreiser for førstegangsutstedelse av identitetsnummer og ID-bevis for henholdsvis EØS-borgere og tredjelandsborgere som skal arbeide i Norge. Figurene legger til grunn dagens prosess for utstedelse.

Brukereisen for EØS-borgere viser at det kreves fire til fem oppmøter for at en EØS-borger skal få tildelt identitetsnummer og utstedt førerkort, skattekort og BankID. EØS-borgeren kan spare ett oppmøte ved å bestille time og møte opp ved et SUA-kontor, der Arbeidstilsynet, politiet, Skatteetaten og UDI samarbeider på én lokasjon. Figuren under viser en brukereise der EØS-borgeren først møter hos politiet for EØS-registrering, for deretter å møte opp hos skattekontoret for å søke om skattekort. Det er også en mulighet for EØS-borgeren å først møte opp hos skattekontoret og deretter hos politiet for EØS-registrering.



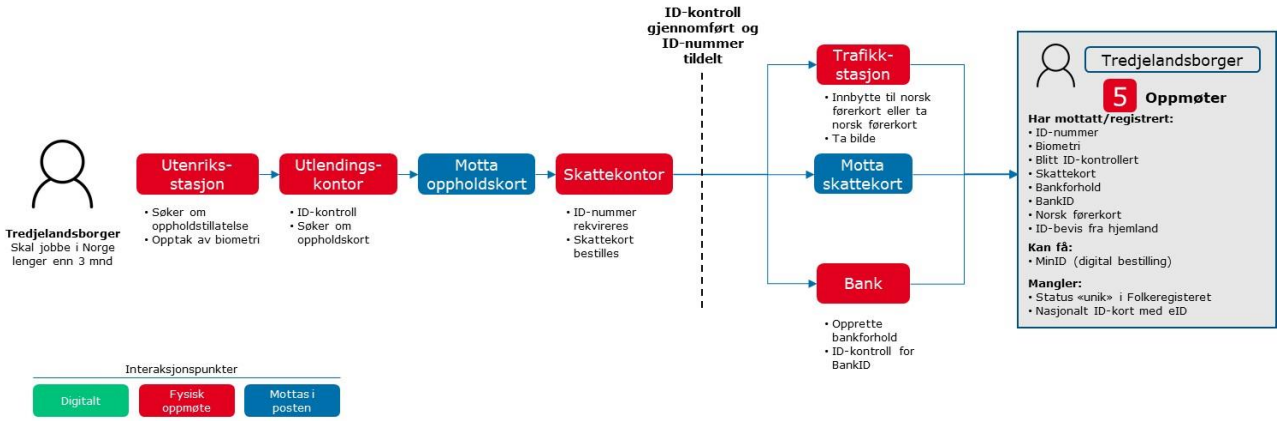
Figur 35 Brukerreise for EØS-borger for utstedelse av identitetsnummer og ID-bevis

Under vises et eksempel på brukerreisen for førstegangsutstedelse av identitetsnummer og ID-bevis til en tredjelandsborger som skal arbeide i Norge. Slik

[293] BITS, «Regler om utstedelse av legitimasjonsbevis (Bankkort med bilde)», 2018

[294] Prosessen referer til henholdsvis 1) Opptak av fingeravtrykk ved Norvis maskin for kontrollsøk mot straffesaksregisteret og lagring av biometri i utlendingsdatabasen og 2) Opptak av biometri med Eurodac maskin for å kontrollere om personen har søkt asyl tidligere

det fremkommer av figuren kreves det fem oppmøter for at tredjelandsborgeren skal få tildelt identitetsnummer og utstedt førerkort, skattekort og BankID.



Figur 36 Brukerreise for tredjelandsborger for utstedelse av identitetsnummer og ID-bevis

5.1.7 Kartlegging av antall treffpunkt, brukertid og brukergebyr i et livsløpsperspektiv (for norske borgere)

Beskrivelse av antall treffpunkt i et livsløpsperspektiv

Bruker vil i løpet av et livsløp anskaffe en rekke ID-bevis, og med varierende hyppighet fornye nevnte ID-bevis. Førstegangsutstedelse og fornyelse av ID-bevisene kan gjennomføres enten ved fysisk oppmøte eller digitalt. For å beskrive antall fysiske og digitale treffpunkt for en bruker ved anskaffelse av ulike ID-bevis har leverandøren tatt utgangspunkt i tre ulike scenarioer.

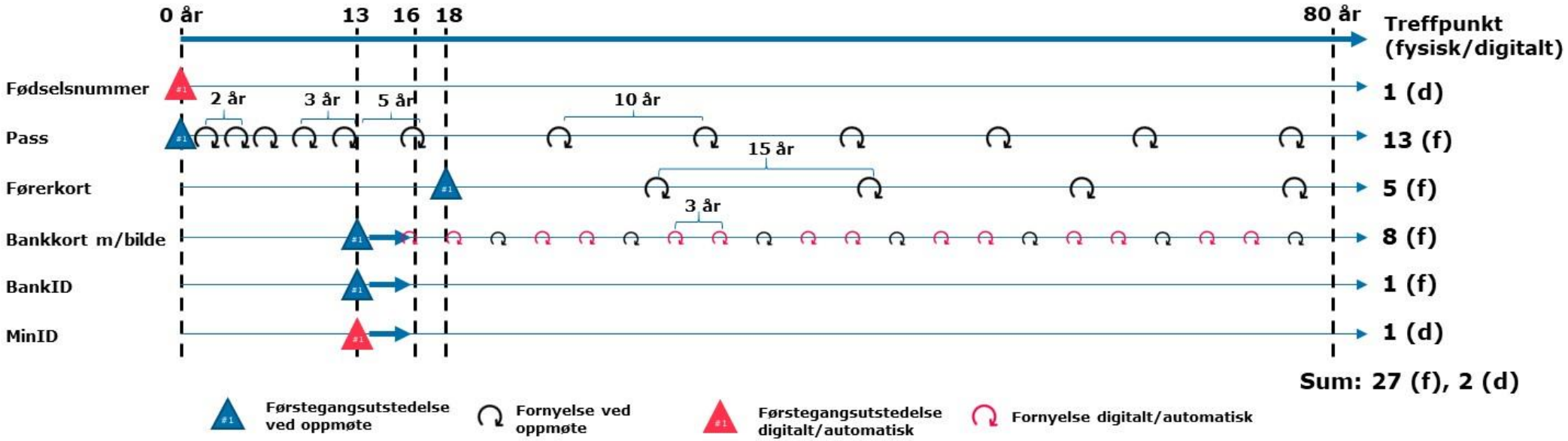
> *Scenario 1:* Dagens situasjon med 10-års gyldighetstid for pass og ingen utstedelse av nasjonalt ID-kort
>
> *Scenario 2:* 5-års gyldighetstid for både pass og nasjonale ID-kort
>
> *Scenario 3:* 10-års gyldighetstid for pass og 5-års gyldighetstid for nasjonale ID-kort

De ulike scenarioene beskrives nærmere i det følgende.

Scenario 1

Figuren under gir en illustrativ oversikt over ID-bevis som er blant de vanligste å anskaffe for norske borgere (jf. kapittel 2.8.1) med en overordnet oversikt over hvor ofte disse ID-bevisene skal fornyes i løpet av livet. Figuren benytter en tidslinje som løper fra fødsel (0 år) til en alder av 80 år. Særskilt for pass er gyldighetstiden for voksne per dags dato satt til 10 år jf. passloven § 6[295]. Antall fysiske (f) og digitale (d) treffpunkt for bruker per ID-bevis er summert til høyre i figuren. Som illustrasjonen viser vil en borger totalt ha omtrent 27 fysiske treffpunkt og to digitale treffpunkt med dagens regelverk. Dette vil selvsagt variere noe avhengig den enkeltes behov for ID-bevis, levetid, samt også eventuelle fremtidige endringer i regelverk. Leverandøren legger dermed i det videre til grunn at dagens regelverk medfører i underkant av 30 treffpunkt i ID-forvaltningen i løpet av et livsløp for norske borgere.

[295] Lovdata, «Lov om pass (passloven)», 1997



Forutsetninger: *Oversikt gjelder for norsk borger født i Norge. Pass fornyes hvert 10 år for voksne. Nasjonale ID-kort ikke utstedt. Bruker anskaffer ID-bevis så fort alder tillater og fornyer ID-bevis ved utløp. Ikke medregnet tap av ID-bevis. Forsvarets ID-kort, Sjøfartsbok og BuyPassID ikke inkludert. Gjelder for en norsk borger født i 2019 gitt at vilkår og regler for utstedelser holdes konstant i løpet av et livsløp på 80 år.*

Førerkort: *Kun inkludert førstegangsutstedelse og fornyelse (ikke inkludert: tap av førerkort, duplikat, innbytte, spesialendring etc)*

Bankkort/BankID: *Det legges til grunn at bilde på bankkort må oppdateres ved oppmøte hvert 10. år. Kun krav til oppmøte dersom kundeforhold opprettes etter 2007. Krav om oppmøte og fremleggelse av pass kan fravikes i visse tilfeller (Kilde: BITS, Regler om utstedelse av legitimasjonsbevis (Bankkort med bilde), 2018)*

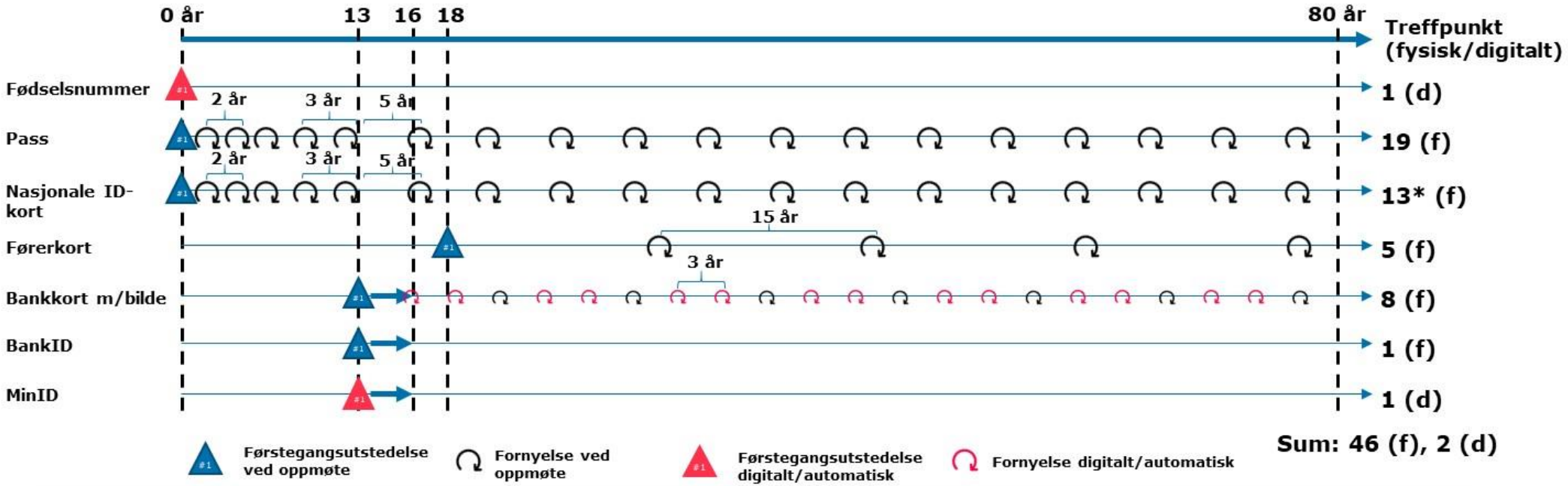
Figur 37 Anskaffelser og fornyelser av ID-bevis i et livsløpsperspektiv for en gjennomsnittlig norsk borger

Scenario 2

Foreslåtte endringer for nye pass og nasjonale ID-kort er beskrevet og drøftet i JD sitt forskriftsforslag om pass og nasjonale ID-kort.[296] Status for dette arbeidet har tidligere bitt omtalt i rapporten under kapittel 2.9.1. Dokumentet inneholder blant annet forslag om at gyldighetstid for nasjonalt ID-kort settes til fem år, samt en vurdering av om gyldighetstid for pass skal reduseres fra ti til fem år.

Figuren under gir en illustrativ oversikt over antall treffpunkt og krav til antall fornyelser av ID-bevis i et livsløpsperspektiv dersom forslag om fem års gyldighetstid for pass legges til grunn, samt at nasjonalt ID-kort utstedes etter tilsvarende vilkår. Leverandøren antar at det i et slikt scenario i praksis vil forekomme en viss grad av samsøknad (tilfeller der bruker fornyer pass og nasjonalt ID-kort samtidig). I figuren er en samsøknadsgrad på 30 prosent lagt til grunn (basert på antagelser benyttet i politiets gebyrmodell). Øvrige antagelser forutsetninger er forklart nærmere i tekst under figuren. Leverandøren legger til grunn at fem års gyldighetstid for pass og nasjonale ID-kort med en samsøkingsgrad på 30 prosent vil resultere i 46 fysiske treffpunkt i ID-forvaltningen i løpet av et livsløp for norske borgere.

[296] JD, «Høring – ny forskrift om pass og nasjonalt ID-kort», 2019



Forutsetninger: *Oversikt gjelder for norsk borger født i Norge. Pass fornyes hvert 5. år for voksne. Nasjonale ID-kort utstedt på like vilkår med pass. Antatt samsøknadsgrad på 30 prosent. Bruker anskaffer ID-bevis så fort alder tillater og fornyer ID-bevis ved utløp. Ikke medregnet tap av ID-bevis. Forsvarets ID-kort, Sjøfartsbok og BuyPassID ikke inkludert. Gjelder for en norsk borger født i 2019 gitt at vilkår og regler for utstedelser holdes konstant i løpet av livsløp.*

Førerkort: *Kun inkludert førstegangsutstedelse og fornyelse (ikke inkludert: tap av førerkort, duplikat, innbytte, spesialendring etc)*

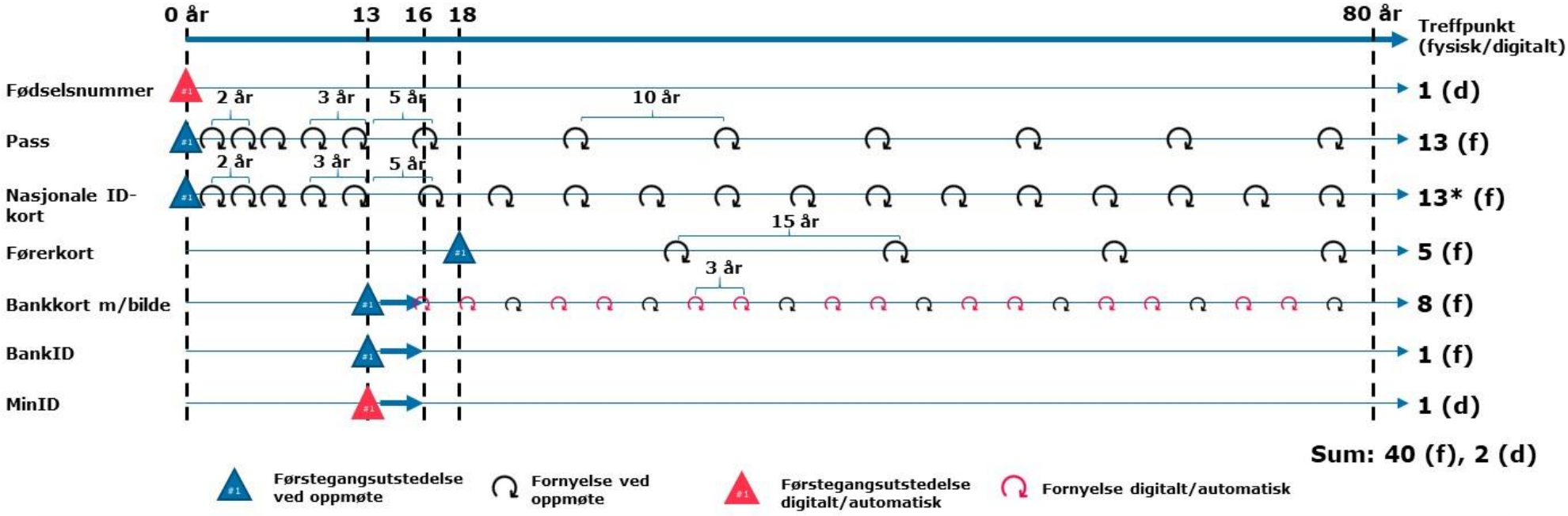
Bankkort/BankID: *Det legges til grunn at bilde på bankkort må oppdateres ved oppmøte hvert 10. år. Kun krav til oppmøte dersom kundeforhold opprettes etter 2007. Krav om oppmøte og fremleggelse av pass kan fravikes i visse tilfeller (Kilde: BITS, Regler om utstedelse av legitimasjonsbevis (Bankkort med bilde), 2018)*

**Leverandøren legger til grunn en samsøknadsgrad på 30 prosent. Antall fysiske treffpunkt for nasjonalt ID-kort reduseres derfor fra 19 til 13 treffpunkt*

Figur 38 Anskaffelser og fornyelser av ID-bevis i et livsløpsperspektiv, fem års gyldighet for pass og nasjonale ID-kort for en gjennomsnittlig norsk borger

Scenario 3

Figuren under illustrerer antall treffpunkt i et livsløp for en gjennomsnittlig norsk borger dersom gyldighetstid for pass og nasjonalt ID-kort settes til henholdsvis ti og fem år, samt en antatt samsøkingsandel på 30 prosent legges til grunn. Basert på illustrasjonen under legger leverandøren til grunn at nevnte forutsetninger for gyldighetstid for pass og nasjonalt ID-kort vil medføre 40 treffpunkt i ID-forvaltningen for norske borgere i løpet av et livsløp.



Forutsetninger: *Oversikt gjelder for norsk borger født i Norge. Pass fornyes hvert 10. år for voksne. Nasjonale ID-kort fornyes hvert 5. år. Antatt samsøknadsandel på 30 prosent. Bruker anskaffer ID-bevis så fort alder tillater og fornyer ID-bevis ved utløp. Ikke medregnet tap av ID-bevis. Forsvarets ID-kort, Sjøfartsbok og BuyPassID ikke inkludert. Gjelder for en norsk borger født i 2019 gitt at vilkår og regler for utstedelser holdes konstant i løpet av livsløp.*

Førerkort: *Kun inkludert førstegangsutstedelse og fornyelse (ikke inkludert: tap av førerkort, duplikat, innbytte, spesialendring etc)*

Bankkort/BankID: *Det legges til grunn at bilde på bankkort må oppdateres ved oppmøte hvert 10. år. Kun krav til oppmøte dersom kundeforhold opprettes etter 2007. Krav om oppmøte og fremleggelse av pass kan fravikes i visse tilfeller (Kilde: BITS, Regler om utstedelse av legitimasjonsbevis (Bankkort med bilde), 2018)*

**Leverandøren legger til grunn en samøknadsandel på 30 prosent. Antall fysiske treffpunkt for nasjonalt ID-kort reduseres derfor fra 19 til 13 treffpunkt*

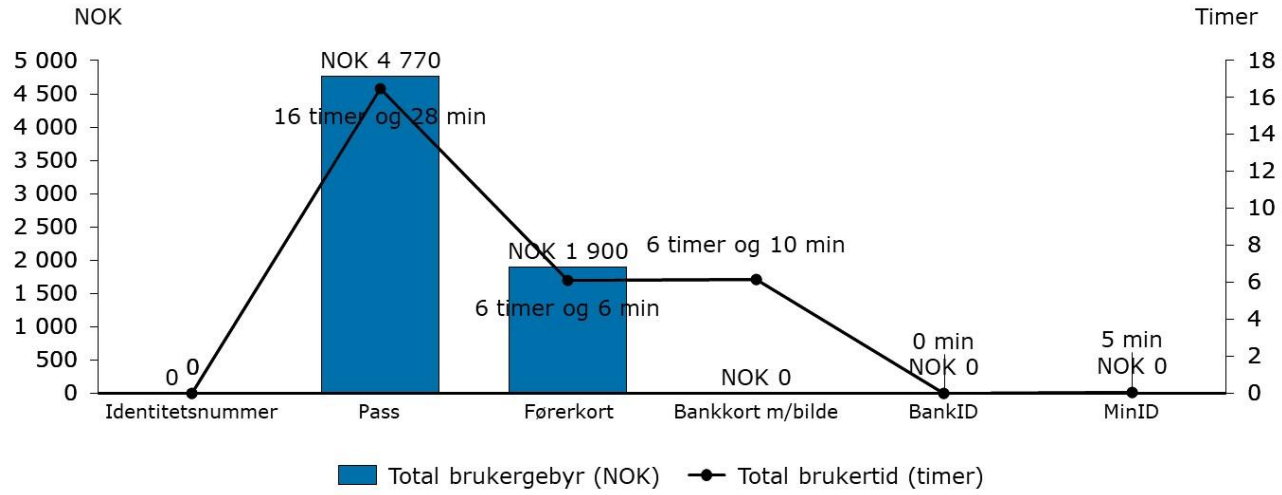
Figur 39 Anskaffelser og fornyelser av ID-bevis i et livsløpsperspektiv, ti års gyldighet for pass og fem års gyldighet nasjonale ID-kort for en gjennomsnittlig norsk borger

Kartlegging av brukergebyr og brukertid per bruker for anskaffelse og fornyelse av ID-bevis i et livsløpsperspektiv for norske borgere

I utregningene av brukergebyr og brukertid per bruker i et livsløp har leverandøren lagt til grunn brukertid og brukergebyr som spesifisert i figurer 30-32 i kapittel 5.1.5, samt antall treffpunkt som spesifisert i figur 37-39. Utregningene er visualisert etter de tre scenarioene beskrevet innledningsvis i kapittelet. Framgangsmåte og beskrivelse av utregninger er nærmere forklart i vedlegg 8.

Scenario 1

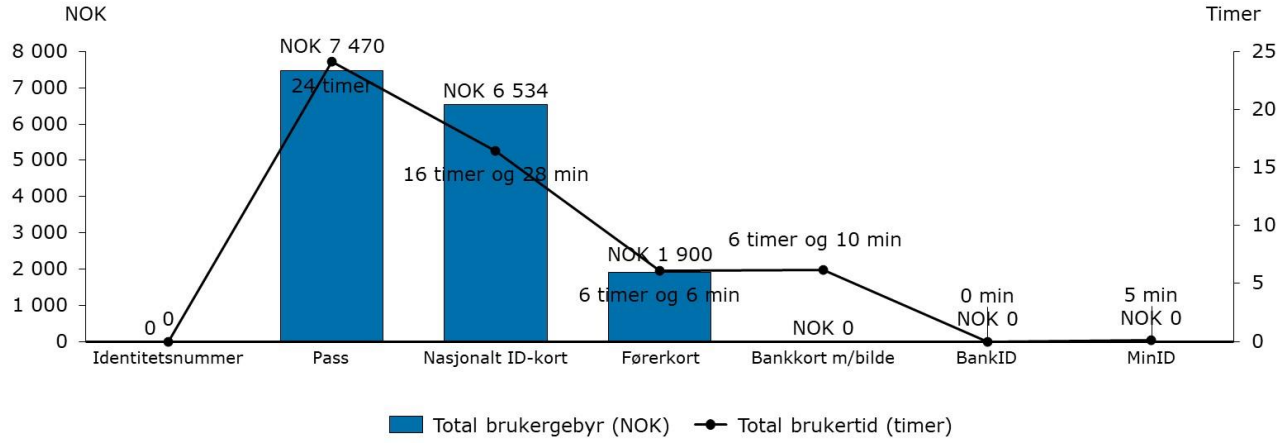
Gitt dagens situasjon med 10-års gyldighetstid for pass og ingen utstedelse av nasjonale ID-kort vil total tid og totalt brukergebyr som påløper til anskaffelse og fornyelse av ID-bevis per bruker i et livsløp utgjøre henholdsvis om lag 29 timer og 6 670 kroner. En oversikt over tidsbruk og brukergebyr per ID-bevis for norske borgere er illustrert i figur 40 under.



Figur 40 Estimert samlet brukergebyr og brukertid for anskaffelse og fornyelse av ID-bevis per bruker i et livsløpsperspektiv (10-års gyldighetstid for pass, ingen utstedelse av nasjonale ID-kort)

Scenario 2

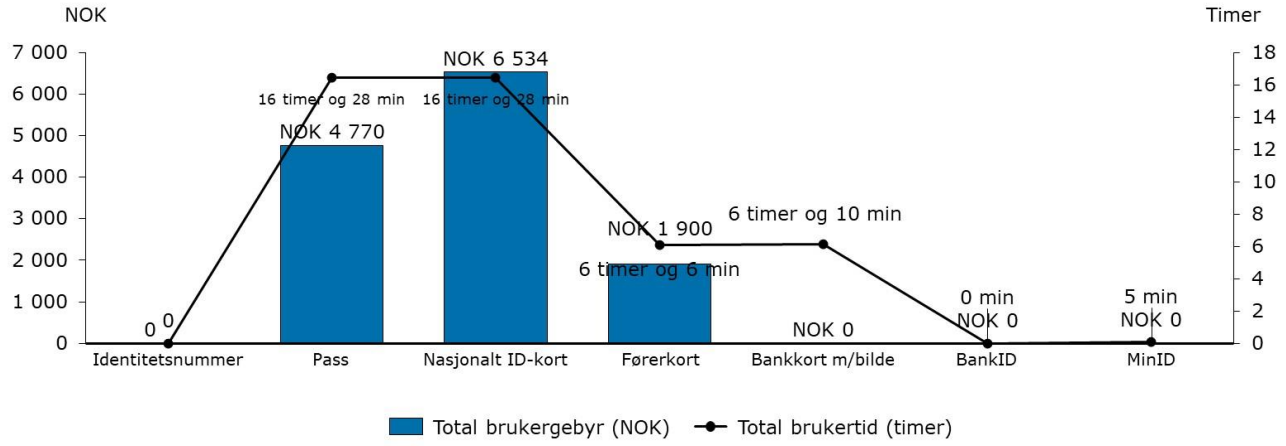
Gitt 5-års gyldighetstid for pass og 5-års gyldighetstid på nasjonale ID-kort vil total tid og totalt brukergebyr som påløper til anskaffelse og fornyelse av ID-bevis per bruker i et livsløp utgjøre henholdsvis om lag 53 timer og 14 500 kroner. Utregningene legger til grunn en samsøknadsgrad mellom pass og nasjonale ID-kort på 30 prosent, samt en samsøknadsrabatt på 40 prosent. Brukertid og brukergebyr for nasjonale ID-kort er ellers forutsatt å være likt som for pass. En oversikt over tidsbruk og brukergebyr per ID-bevis for norske borgere er illustrert i figur 41 under.



Figur 41 Estimert samlet brukergebyr og brukertid for anskaffelse og fornyelse av ID-bevis per bruker i et livsløpsperspektiv (5-års gyldighetstid for pass, 5-års gyldighetstid for nasjonalt ID-kort)

Scenario 3

Gitt 10-års gyldighetstid for pass og 5-års gyldighetstid på nasjonale ID-kort vil total tid og totalt brukergebyr som påløper til anskaffelse og fornyelse av ID-bevis per bruker i et livsløp utgjøre henholdsvis om lag 45 timer og 11 800 kroner. Utregningene legger til grunn en samsøknadsgrad mellom pass og nasjonale ID-kort på 30 prosent, samt en samsøknadsrabatt på 40 prosent. Brukertid og brukergebyr for nasjonale ID-kort er ellers forutsatt å være likt som for pass. En oversikt over tidsbruk og brukergebyr per ID-bevis for norske borgere er illustrert i figur 42 under.



Figur 42 Estimert samlet brukergebyr og brukertid for anskaffelse og fornyelse av ID-bevis per bruker i et livsløpsperspektiv (10-års gyldighetstid for pass, 5-års gyldighetstid for nasjonalt ID-kort)

5.1.8 Verdiberegning av brukers tidsbruk

For å kunne kvantifisere gevinster av tidsbesparelser for bruker er det hensiktsmessig å kunne sette en kroneverdi på brukers tidsbruk. Det fremgår av FINs rundskriv R-109/2014 at alternativkostnadsprinsippet skal legges til grunn ved verdsetting av tidsbesparelser, samt at nasjonale gjennomsnitt skal benyttes som tidsverdier for berørte personer. Vesentlig for kostnadsberegningen er om tidsanvendelsen foregår i arbeidstiden eller fritiden. Dersom det legges til grunn at tidsanvendelsen foregår i arbeidstiden anbefales det i rundskrivet at arbeidsgivers tapte verdiskapning målt ved brutto-reallønnsskostnader legges til grunn.[297] Selvsagt vil det variere hvorvidt bruker

[297] FIN, «R-109/14 - Prinsipper og krav ved utarbeidelse av samfunnsøkonomiske analyser mv», 30.04.2014

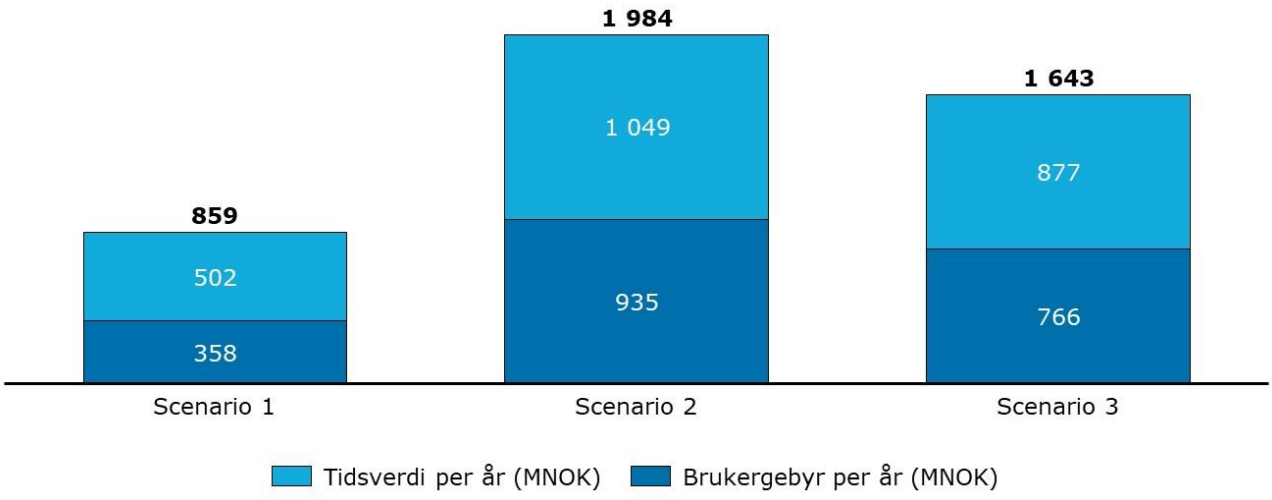
benytter arbeidstid eller fritid til anskaffelse av ID-bevis, men siden åpningstiden til aktørene som utsteder ID-bevis i all hovedsak ligger innenfor normal arbeidstid har leverandøren valgt å legge arbeidstid til grunn. I Direktoratet for økonomistyring (DFØ) sin veiledning for samfunnsøkonomiske analyser anbefales det videre at bruttolønnskostnadene justeres for å reflektere arbeidsgiveravgift og andre sosiale ansattkostnader (herunder pensjonskostnader). I det videre legges det til grunn en antagelse om at arbeidsgiveravgift og sosiale kostnader til sammen i gjennomsnitt utgjør et påslag på 30 prosent av bruttolønnskostnader.[298]

Den gjennomsnittlige bruttomånedslønnen i Norge i 2018 var 45 610 kroner (gjennomsnitt for alle sektorer, før skatt og ekskludert overtid).[299] Justert for arbeidsgiveravgift og sosialkostnader utgjør dette en bruttlønnskostnad for arbeidsgiver på 59 293 kroner i måneden og 711 516 kroner i året. Dersom et gjennomsnittlig antall timer per årsverk på 1950 timer (inkludert ferie)[300] legges til grunn tilsvarer dette en tidsverdi på 365 kroner per time.

Kartlegging av samfunnsmessige kostnader av brukertid og brukerbetaling

I kartleggingen over fremkommer det at en norsk borgers gjennomsnittlige tidsbruk for anskaffelse og fornyelse av ID-bevis (identitetsnummer, pass, nasjonalt ID-kort, førerkort, bankkort med bilde, BankID og MinID) i scenario 1-3 i løpet av et livsløp summerer seg til henholdsvis ca. 29 timer, 53 timer og 45 timer. Tilhørende brukergebyr er henholdsvis 6 670 kroner, 15 904 kroner og 13 204 kroner.

Basert på brukertiden og brukerbetalingen i det foregående, samt enkelte antagelser knyttet til antall ID-bevis i omløp, gjennomsnittlig tidsverdi per time og antall år i et gjennomsnittlig livsløp har leverandøren overordnet estimert den årlige samfunnsmessige kostnaden som medgår til tid og brukerbetaling per år.[301] Estimatene tar ikke hensyn til at det tar noen år å fullt ut implementere de ulike scenariene. Effekten er illustrert i figuren under for scenario 1-3.



Figur 43 Estimert samlet verdi av tidsbruk og brukergebyr per år for anskaffelse og fornyelse av ID-bevis under ulike scenarier for gyldighetstid for pass og nasjonalt ID-kort

[298] DFØ, «Veileder i samfunnsøkonomiske analyser», 2018
[299] SSB, «Lønn», 04.02.2019
[300] SSB, «Utførte årsverk», u.å.
[301] Utregningene har benyttet følgende antagelser: Antall pass i omløp: 5 millioner (antatt likt for nasjonale ID-kort over tid), antall førerkort i omløp: 2,5 millioner, antall bankkort med bilde i omløp: 2 millioner, antall år i et livsløp: 80, tidsverdi kroner/time: 365

Verdiene over er kun ment som et høynivå estimat på samlet kostnad for brukers tidsbruk og brukerbetaling for alle ID-bevis. En fullstendig samfunnsøkonomisk beregning forutsetter at antagelser ettergås nærmere, herunder justeringer for forventet vekst i realbruttolønn, forventet vekst i antall ID-bevis i omløp, tidsverdien av penger samt differensiering basert på lønnsnivå/betalingsvillighet mellom ulike brukergrupper.

5.1.9 Internasjonal sammenligning av brukergebyr for anskaffelse av ulike ID-bevis

Tabellen under viser gjeldende gebyr for voksenpass, nasjonalt ID-kort og førerkort i Norge, Sverige, Danmark, Storbritannia og Lativa. Leverandøren bemerker at det ikke er kompensert for forskjeller i kjøpekraft mellom landene i tabellen, og at en eventuell justering av kjøpekraft vil kunne endre forskjellene i gebyrer noe.

Gebyr ved førstegangsutstedelse av ID-bevis (norske kroner[302])	Pass, voksne	Nasjonalt ID-kort	Førerkort
Norge	450 kroner	-	380 kroner
Sverige	320 kroner[303]	366 kroner[304]	229 kroner[305]
Danmark	818 kroner[306]	196 kroner[307]	365 kroner[308]
Storbritannia	802 kroner[309]	-	361 kroner[310]
Latvia	277 kroner[311]	139 kroner[312]	215 kroner[313]

Tabell 15 Gebyrer for bruker i norske kroner ved førstegangsutstedelse av ID-bevis

5.2 Funn og vurderinger

Under følger leverandørens vurderinger av nåsituasjonen innen brukerreiser og brukervennlighet i ID-forvaltningen. Helhetlige vurderinger foretas av leverandøren i del 3 av rapporten.

5.2.1 Folkeregisteret oppfattes som svært brukervennlig for norske borgere og oppleves som en styrke i ID-forvaltningen

Svært mange respondenter fra leverandørens kartlegging trekker frem Folkeregisteret som en styrke i den norske ID-forvaltningen. Slik redegjort for i kapittel 5.1.1 er det ikke forelagt utfyllende dokumentasjon om brukers opplevelse av Folkeregisterets funksjonalitet, men leverandøren vurderer det som svært brukervennlig at borgere kun trenger å forholde seg til ett identitetsnummer som kan benyttes til et bredt spekter

[302] Valutakurser benyttet for omregning av gebyrer er hentet fra Norges Bank 30.07.2019 16:00
[303] Polisen, «Pass och nationelt id-kort», 11.02.2019
[304] Polisen, «Pass och nationelt id-kort», 11.02.2019
[305] Transportstyrelsen, «Förnya kökortet», u.å.
[306] Borger.dk, «Ansøg om eller forny dansk pas», u.å.
[307] Borger.dk, «Legitimationskort – Ansøg om legitimationskort», u.å.
[308] Borger.dk, «Fornyelse af kørekort», u.å.
[309] GOV.UK, «Passport fees», u.å.
[310] GOV.UK, «Driving licence fees», u.å.
[311] PMLP.gov.lv, «State fees for issuance of passport and identity card», 01.04.2012
[312] PMLP.gov.lv, «State fees for issuance of passport and identity card», 01.04.2012
[313] Integratin.lv, «Transport - Driving licence», u.å.

av formål. Utover brukere har også utstedere av ID-bevis og tjenestetilbydere stor nytte av tilgang til personinformasjon som er lagret i Folkeregisteret.

I utenlandsk kontekst eksisterer det eksempler på land som ikke opererer med et sentralt folkeregister. Sammenlignet med eksempelvis Storbritannia, som praktiserer fragmenterte register med ulike formål, er det etter leverandørens vurdering langt mer formålstjenlig både fra et brukerperspektiv og et aktørperspektiv med et sentralt folkeregister.

5.2.2 Det er stor variasjon og fleksibilitet for bruker i hva som regnes som gyldige ID-bevis

Slik vist i figur 25-29 i kapittel 5.1.2 varerier kravene til gyldig legitimasjon for å få tilgang til ulike offentlige tjenester og ytelser mellom aktørene. Selv om pass kan anses som det sikreste ID-beviset i omløp på nåværende tidspunkt, godtas også en rekke andre ID-bevis ved personlig fremmøte. Dette er etter leverandørens vurdering isolert sett brukervennlig for brukeren. At ulike eID-er og ID-porten gir bred tilgang til offentlige tjenester og ytelser ansees også som særdeles brukervennlig.

Videre viser tabell 12 i kapittel 5.1.3 at kravene til hva som regnes som gyldig legitimasjon for å få utstedt nye ID-bevis varierer betydelig mellom aktørene. Dette kan oppfattes som brukervennlig for innbyggeren, men også forvirrende da det ikke er klare retningslinjer på hva som regnes som gyldig legitimasjon på tvers av aktører. Det vil si at det anses uklart hva innbyggeren trenger av gyldig legitimasjon for å få tilgang til ulike ID-bevis. Det kan videre fremstå som lite intuitivt at private aktører har blant de strengeste kravene til legitimasjon i den norske ID-forvaltningen. For innbyggeren er det brukervennlig at ID-bevis med en lav notoritet kan gi tilgang til ID-bevis med en høyere notoritet.

Sikkerheten ved dagens fleksible tilnærming er dekket i kapittel 6.

5.2.3 Det er høy grad av krav til oppmøte for førstegangsutstedelse og fornyelse av offentlige ID-bevis, samt lite gjenbruk av informasjon

Som vist i kapittel 5.1.3 tabell 11 er det (med unntak av for MinID) krav om personlig oppmøte for førstegangsutstedelse av samtlige ID-bevis. Tilsvarende er det høy grad av krav til oppmøte for å fornye nevnte ID-bevis, spesielt for fysiske ID-bevis utstedt av det offentlige. Sett i sammenheng med legitimasjonskravene som er kartlagt for ulike offentlige tjenester og ytelser i figurer 25-29 i kapittel 5.1.2 er det påfallende høy grad av oppmøteplikt ved utstedelse og fornyelse av ID-bevis. Leverandøren er kjent med enkelte unntak, men det er i hovedsak liten grad av gjenbruk av personlige identifikatorer eller bilder mellom aktører som utsteder ID-bevis. Isolert sett er det leverandørens vurdering at høy grad av personlig oppmøte ved fornyelse og førstegangsutstedelse med lav gjenbruk av informasjon (dersom samtykke til dette er gitt) bidrar til å redusere brukeropplevelsen, da dette medfører et betydelig tidsforbruk i et livsløpsperspektiv.

5.2.4 Velfungerende og utbredt norsk eID bidrar sterkt til å redusere kostnader og tidsbruk fra et brukerperspektiv

Sammenlignet med fysiske ID-bevis stiller eID færre krav til kontinuerlige fornyelser gjennom et livsløp (se tabell 11 kapittel 5.1.3 og figur 37 kapittel 5.1.7). Kartleggingen

illustrert ved figurer 25-29 i kapittel 5.1.2 viser også at det i hovedsak er lagt godt til rette for at brukere skal kunne benytte eID til ID-kontroll for å tilegne seg offentlige tjenester og ytelser. Bruker betaler heller ingen direkte kostnader for verken utstedelse eller bruk av BankID og MinID i løpet av livet. I den grad legitimering med eID kan benyttes framfor krav om legitimering ved personlig oppmøte vil dette også innebære redusert brukertid (i form av reisetid, ventetid og behandlingstid i skranke) og ofte redusert brukergebyr (i form av lavere gebyrer ved bruk av selvbetjeningstjenester). I den sammenheng er det leverandørens vurdering at eID er en sterk bidragsyter til å redusere kostnader og brukertid i de treffpunkt der eID tilbys som et alternativ til oppmøte, og står i den forstand sentralt i en forbedret brukeropplevelse.

5.2.5 Det er lav bevissthet om samlet brukertid og kostnad i en brukers livsløp for fysiske ID-bevis

I leverandørens kartlegging av antall treffpunkt i et livsløpsperspektiv fremkommer det at majoriteten av oppmøtekravene en bruker står overfor stilles i forbindelse med fornyelse av norsk pass. Figur 38 og figur 39 illustrerer videre at antall treffpunkt vil øke betydelig som følge av en eventuell redusert gyldighetstid på pass og utstedelse av nasjonalt ID-kort. Graden av samsøknad (tilfeller der bruker fornyer pass og nasjonalt ID-kort samtidig) vil i stor grad påvirke hvor betydelig denne endringen blir. I Menon sin samfunnsøkonomiske analyse av redusert gyldighet for pass, blir konsekvenser for bruker blant annet drøftet.[314] Problemstillinger relatert til oppmøtekrav relatert til utstedelse av førerkort er også drøftet av SVV i sin pågående endring av tjenestestrukturen for trafikantområdet[315]. I vurderingen for pass er det i hovedsak de samfunnsøkonomiske konsekvensene som vektlegges, og ikke nødvendigvis brukerens oppfatninger og synspunkter. Det er leverandørens vurdering at den samlede brukertiden og brukergebyret som påløper for ulike ID-bevis i et livsløpsperspektiv i mindre grad har blitt drøftet i dokumentasjonen som har blitt forelagt. Tilsvarende er det i liten grad utredet hvilken påvirkning de planlagte endringene vil medføre fra et brukerperspektiv.

5.2.6 Med unntak av pass er brukers direktekostnad for anskaffelse av ID-bevis marginalt høyere enn sammenlignbare land

Som det fremkommer i kapittel 5.1.8 er brukergebyret for anskaffelse av førerkort og nasjonalt ID-kort (gitt planlagt fremtidig gebyr for nasjonalt ID-kort i Norge) noe høyere enn sammenlignbare land. Leverandøren anser denne differansen å være relativt liten. Samtidig fremkommer det at gebyret for utstedelse av pass i Norge ligger betydelig lavere enn tilsvarende gebyr i Danmark og Storbritannia.

5.2.7 Det er få gode alternativer til pass for en sikker legitimering ved krav om fysisk oppmøte

Brukere uten norsk førerkort og bankkort med bilde står i praksis igjen med norsk pass som gyldig legitimasjonsgrunnlag. Samtidig er leverandøren kjent med at bankkort med bilde utgjør en stadig lavere andel av totale bankkort som utstedes hvert år. I lys av få reelle alternativ anser leverandøren det som svært lite brukervennlig dersom en bruker i praksis påkreves å måtte benytte pass til enhver legitimering. Det anses videre

[314] Menon, «Samfunnsøkonomisk analyse av redusert gyldighetstid for pass», 2018
[315] SVV, «Forslag til ny tjenesteleveransemodell og tjenestestruktur på TK-området», 2019

som problematisk at staten ikke tilbyr noe reelt alternativ til dette utover at bruker må kunne kjøre bil eller inneha et bankkort med bilde. Nasjonale ID-kort forventes å adressere problematikken nevnt i det foregående.

5.2.8 Brukerreisen for EØS-borgere er betydelig enklere enn brukerreisen for tredjelandsborgere

Som følge av Norges medlemskap i EØS medfører på flere områder at brukerreisen for EØS-borgere i Norge forenkles betydelig. Eksempelvis vil EØS-borgere for mange offentlige tjenester, og for utstedelsen av enkelte ID-bevis, kunne benytte sine respektive nasjonale ID-kort som legitimasjonsgrunnlag. Videre vil EØS-borgere, til forskjell fra majoriteten av tredjelandsborgere, eksempelvis ha anledning til å benytte et førerkort utstedt i et annet EØS-land til bruk i Norge inntil førerkortet utløper. EØS-borgeren vil også kunne bytte inn sitt utenlandske førerkort mot et norsk førerkort uten å måtte ta ny førerprøve. EØS-regelverket tilrettelegger også for at brukergruppen slipper å søke om oppholdstillatelse og visum.

På den andre siden er det viktig å poengtere at EØS-borgere forut for et opphold i Norge også vil stå overfor flere fysiske oppmøtekrav. Blant annet vil vedkommende måtte registrere seg hos politiet ved opphold over tre måneder, samt gjennomgå et ytterligere fysisk oppmøte for å anskaffe et identitetsnummer.

6 Kvalitet og sikkerhet i ID-forvaltningen

I dette kapittelet gis en beskrivelse av nåsituasjonen (kapittel 6.1) og leverandørens nåsituasjonsvurderinger (kapittel 6.2) knyttet til kvalitet og sikkerhet i ID-forvaltningen. Kapittelet tar blant annet for seg prosessene relatert til tildeling av fødselsnummer, rekvirering og tildeling av d-nummer og utstedelse/fornyelse/tap av fysiske og elektroniske ID-bevis. Videre kartlegges samfunnsmessige konsekvenser relatert til feil og misbruk og biometri.

6.1 Nåsituasjonen

Leverandøren er ikke gjort kjent med at det eksisterer en helhetlig strukturert kartlegging som tar for seg kvalitet og sikkerhet i ID-forvaltningen. Den eksisterende dokumentasjonen forelagt leverandøren, tar for seg separate deler av ID-forvaltningen og baserer seg på den enkelte aktørs rolle/perspektiv i ID-forvaltningen. Det er opp til den enkelte aktør i å definere hva som er tilstrekkelig kvalitet og sikkerhet relatert til ID i henhold til økonomireglementet.[316]

Basert på totaliteten av tilgjengelig informasjon har leverandøren valgt å fokusere på de delene av ID-prosessen som er rotårsak til kvalitet og sikkerhetsutfordringer i ID-forvaltningen i stort (herunder ID-kontrollen som gjøres på det enkelte området):

- tildeling av fødselsnummer
- rekvirering og tildeling av d-nummer
- utstedelse/fornyelse/tap av fysiske ID-bevis
- utstedelse/fornyelse/tap av elektroniske ID-bevis (eID)

Fødselsnummer og d-nummer tildeles i høyt volum hvert år og brukes i Norge for å identifisere innbyggerne.[317] Når en person har en identitet i Folkeregisteret vil den, sammen med ulike ID-bevis, kunne gi rett til nye og sterkere ID-bevis, og benyttes som dokumentasjon for ulike offentlige tjenester og ytelser, som beskrevet i kapittel 5.1.2 og 5.1.3. Kvalitet og sikkerhet i disse prosessene er dermed meget vesentlig for ID-forvaltningen.

Denne tilnærmingen er valgt i samråd med prosjektgruppen. De fire overnevnte delene av ID-prosessen er beskrevet i kapittel 6.1.1 til 6.1.4. Nåsituasjonsbeskrivelsen er basert på den enkelte aktørs egne rutiner/retningslinjer, spørreundersøkelse (vedlegg 2), intervjuer og rapporter.

Kapittel 6.1.5 ser på de samfunnsmessige konsekvensene av feil og misbruk av ID. Leverandøren er ikke gjort kjent med at det eksisterer en helhetlig kartlegging over de samfunnsmessige konsekvensene. I dokumentasjonen leverandøren har mottatt er ID-relaterte samfunnsmessige konsekvenser i liten grad tydeliggjort og andelen ID-misbruk kommer ikke frem. Leverandøren har forsøkt å kartlegge de samfunnsmessige konsekvensene i kategoriene økonomisk kriminalitet (herunder arbeidslivskriminalitet og trygdesvindel) og samfunnssikkerhet, og med dette gi et anslag på andelen relatert til ID.

[316] Også omtalt som «Regelverket for økonomistyring i staten». En felles instruks for departementene og de underliggende virksomhetene i statsforvaltningen
[317] Skatteetaten, «Norsk identitetsnummer», u.å.

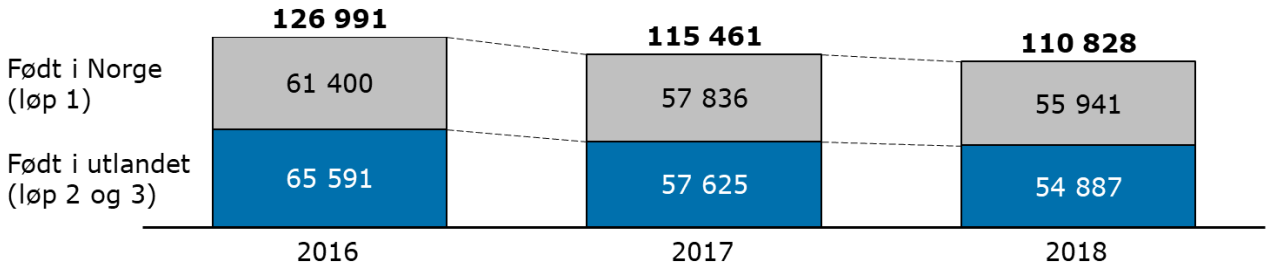
Kapittel 6.1.6 ser på biometri og beskriver hva det er, hvordan det benyttes i Norge i dag og hvordan det kan bidra til å øke kvalitet og sikkerhet i ID-forvaltningen. Nåsituasjonsbeskrivelsen er basert på en rekke intervjuer og rapporter.

6.1.1 Kvalitet og sikkerhet i forbindelse med tildeling av fødselsnummer

Det er kun Skatteetaten som tildeler fødselsnummer i Folkeregisteret. Dette gjøres gjennom tre ulike løp:

1. Melding om fødsel fra helseforetak (nyfødte)
2. Melding fra utlendingsmyndighetene (tredjelandsborgere)
3. Melding om innflytting ved personlig oppmøte på et skattekontor (EØS-borgere/nordiske borgere/gjeninnvandrere/norske barn født i utlandet)

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 (kategori 1), mens 54 887 var for utenlandske borgere (kategori 2 og 3). 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 44 Tildelte fødselsnummer siste tre år[318]

Rutiner, retningslinjer og kvalitet

For barn født i Norge sendes en fødselsmelding automatisk til Skatteetaten eller mor melder fødselen til Skatteetaten dersom barnet fødes uten lege eller jordmor til stede.[319] Deretter registreres opplysninger om barnet i Folkeregisteret og tildeles et fødselsnummer. Det gjennomføres vanligvis ingen ID-kontroll av mor når barn fødes på norske sykehus. Det stilles derfor heller ingen kompetansekrav utover stillingen som lege eller jordmor. For barn født i utlandet må foreldre møte opp på skattekontoret sammen med barnet når de kommer tilbake til Norge for at barnet skal bli registrert bosatt i Norge.[320] Det kreves da pass (ofte tildelt av norsk utenriksstasjon) og utfylt flyttemelding for barnet, samt fra utvalgte land original kopi av fødselsattest og i noen tilfeller DNA-test. Om familien skal bo i utlandet får barnet fødselsnummer tildelt av Skatteetaten i forbindelse med søknad om norsk pass gjennom en norsk utenriksstasjon.

[318] Skatteetaten, mottatt dokumentasjon på fødselsnummer
[319] Skatteetaten, «Barn født i Norge», u.å.
[320] Skatteetaten, «Barn født i utlandet», u.å.

Når det kommer til rutiner for tildeling av fødselsnummer til utlendinger har utlendingsmyndighetene gjennom vinteren 2019 endret sine systemer og rutiner som følge av arbeidet med å modernisere Folkeregisteret.[321] Til nå har det vært slik at en utlending som kommer til Norge etter tredjelandsregelverket først har vært i kontakt med politiet som har foretatt kontroll av deres identitet og vurdert grunnlaget deres for å bli i Norge. De som har fått oppholdstillatelse for mer enn seks måneder har måttet henvende seg til et skattekontor for å melde fra om at de skal flytte til Norge. Dette resulterer i en innflyttingsmelding og et fødselsnummer sendt til utlendingen. I den nye rutinen sendes det en innflyttingsmelding til Skatteetaten *samtidig* som personen får effektuert sin tillatelse hos politiet og personen får et brev med fødselsnummer i posten. Dermed slipper utlendingen å kontakte flere etater i Norge og avgi samme informasjon.[322]

Det gjennomføres årlige kompetanseløft i Skatteetaten når det kommer til ID-kontroll i forbindelse med tildeling av fødselsnummer for utlendinger og tildeling av d-nummer (adresseres senere). Medarbeidere som utfører ID-kontroll gjennomgår «Grunnkurs ID-kontroll» og et obligatorisk videregående kurs i ID-kontroll.[323] Hvert skattekontor som foretar ID-kontroller har i tillegg en superbruker som har et spesielt ansvar for å holde seg selv, gruppeleder og kollegaer oppdaterte på ID-relaterte spørsmål, nye dokumenter og problemstillinger. Det avholdes månedlige møter for alle superbrukere for erfaringsutveksling og løfting av felles problemstillinger. Skatteetaten har i tillegg to ID-spesialister som har et landsdekkende ansvar for opplæring og oppfølging av alle saksbehandlere som utfører ID-kontroll.

Skatteetaten opplever at rutinene for tildeling av fødselsnummer generelt er gode, at de er allment kjent blant ansatte og at de følges. Det er ikke meldt om avvik på området, og Skatteetaten vurderer kompetansekravene i forbindelse med tildeling av fødselsnummer som tilstrekkelige.

Potensielle feilkilder ved tildeling av fødselsnummer

Det kan være ulike feilkilder ved tildeling av fødselsnummer. Under følger de viktigste potensielle feilkildene slik forelagt leverandøren.

Skatteetaten og ulike rapporter påpeker en svakhet i at tilretteleggingen for status «unik» i regelverket ikke utnyttes i praksis grunnet manglende knytning mot biometri i tildelingen av fødselsnummer. I utgangspunktet tildeles hver person kun ett identitetsnummer, men slik systemet er i dag kan det ikke garanteres at en person ikke får flere identitetsnummer.[324] Samme feilkilde gjelder også i prosessen for rekvirering av d-nummer (kapittel 6.1.2).

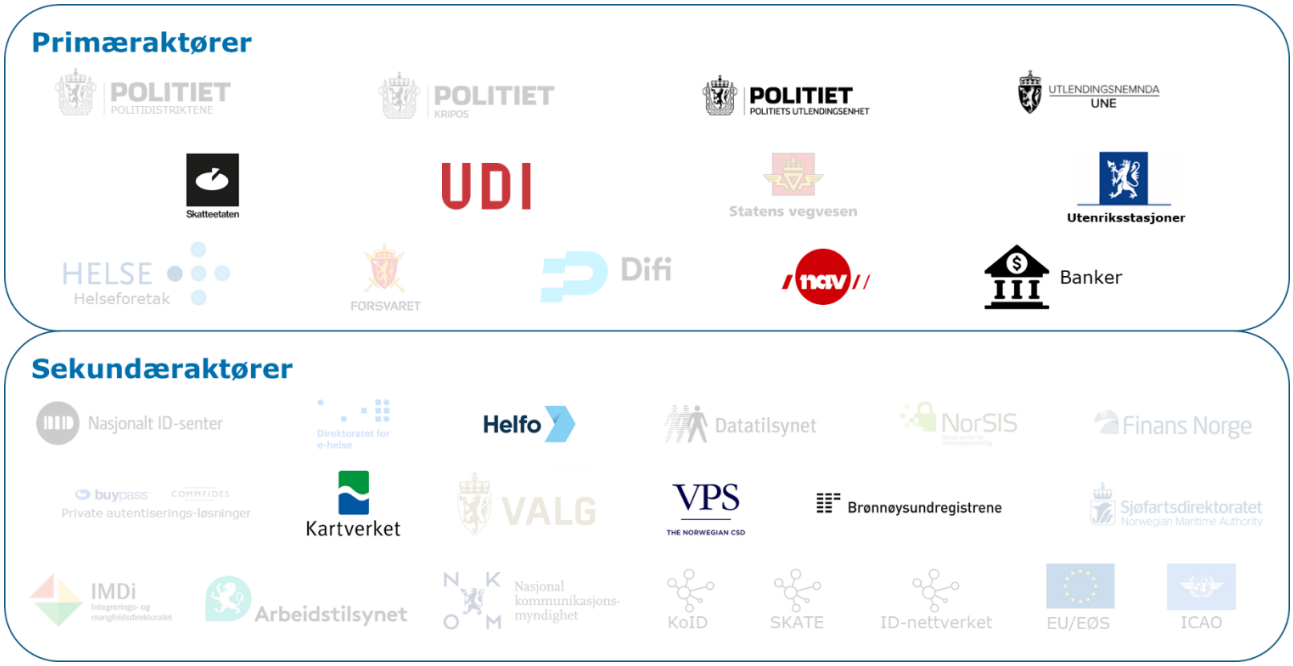
Helseforetakene foretar ved fødsel svært sjelden ID-kontroll av mor i forbindelse med utfylling og innsending av fødselsmelding. Dette gjør det mulig at en kvinne føder i en annen kvinnes navn eller gjennomføre ulovlig surrogati. Dette medfører blant annet risiko for at barnet blir registrert med et annet statsborgerskap enn det som følger av loven. Slike tilfeller er eksemplifisert med enkeltsaker kommunisert i møter med HOD, men det finnes ikke noen statistikk på dette.

[321] UDI, «Nye rutiner for tildeling av fødselsnummer», 2018
[322] Folkeregistermyndigheten vil alltid være tildelingsmyndighet uavhengig av om de gjenbruker prosesser fra andre aktører
[323] Alle ansatte som jobber på kontorer hvor det utføres få ID-kontroller per ansatt per år (færre enn 300 per ansatt i året) deltar på en hospiteringsordning på kontoret i Oslo, for å sikre nok mengdetrening
[324] JD, FIN og KMD, «Utredning om knytning mellom Folkeregisteret og biometriregistrene i justissektoren», 2016

6.1.2 Kvalitet og sikkerhet i forbindelse med rekvirering og tildeling av d-nummer

Et d-nummer rekvireres når rekvirerende myndighet har behov for et d-nummer for å kunne samhandle med en person. Eksempelvis rekvirerer skattemyndighetene d-nummer for å samhandle med en skatte- og avgiftspliktig person og det er folkeregistermyndigheten (skattekontorene) som tildeler d-nummeret. Det er rekvirentene som vurderer personens begrunnede behov for d-nummer, og dette er noe Skatteetaten ikke etterprøver.

Figuren nedenfor gir et oversiktsbilde over aktører involvert i ID-forvaltningen, hvor de elleve rekvirentene oppgitt på Skatteetatens hjemmesider er fremhevet.[325]



Figur 45 Oversiktsbilde over primær- og sekundæraktører der rekvirenter er fremhevet[326]

UNE oppgir at de ikke rekvirerer d-nummer i praksis. Videre oppgir VPS at de heller ikke rekvirerer d-nummer ettersom dette utføres av deres kontoførere på vegne av investor. Kontoførere kan være fondsforvaltere, verdipapirforetak og banker. I UD, på utenriksstasjonene, er praksisen litt annerledes enn for de øvrige rekvirentene, da d-nummer kun rekvireres for personell ved utenlandske representasjoner i Norge og deres medfølgende familiemedlemmer som er tilmeldt til og akseptert av departementet.

Som presentert i tabellen nedenfor står Skatteetaten og NAV for det store flertallet av rekvirerte d-nummer i 2018, med totalt 92 prosent. Blant de øvrige rekvirentene var Brønnøysundregistrene størst med 4 160 rekvisisjoner og Helfo minst med seks rekvisisjoner.[327] Antallet rekvirerte d-nummer økte fra 2016 til 2017 og videre til 2018. Videre viser tall fra Skatteetaten at over 50 prosent av tildelte d-nummer i 2018 var til personer som oppholder seg i utlandet.[328]

[325] Skatteetaten, «D-nummer», u.å.
[326] Regjeringen har besluttet at Difi og Altinn skal samles i et nytt digitaliseringsdirektorat fra 1. januar 2020. Det kan påvirke Brønnøysundregistrenes rolle som rekvirent
[327] Når det gjelder antall rekvirerte d-nummer påpeker Skatteetaten at dette antallet vil variere fra dag til dag på grunn av tidsforskyvninger og kontinuerlige endringer i identitetsgrunnlag
[328] Utenlandsk postadresse registreres på tidspunktet tildelingen ble foretatt. Den kan være endret/fjernet etter tildeling

Rekvirent	Antall 2016	Antall 2017	Antall 2018	Pst. 2018
Skatteetaten	57 140	59 704	60 318	**56 pst.**
NAV	18 818	31 644	38 838	**36 pst.**
Brønnøysundregistrene	4 264	3 714	4 160	
Utlendingsmyndighetene (PU, UNE, UDI)	2 127	2 837	2 277	
Bank/finans	2 190	1 385	1 096	
Kartverket	417	356	437	**8 pst.**
Utenriksstasjoner	0	0	388	
Diverse[329]	0	0	26	
Helfo	10 085	529	6	
Total	**95 042**	**100 169**	**107 546**	**100 pst.**
Andel med norsk postadresse	52 pst.	45 pst.	43 pst.	
Andel med utenlandsk postadresse	17 pst.	18 pst.	52 pst.	
Andel uten postadresse	31 pst.	36 pst.	4 pst.	

Tabell 16 Antall rekvirerte d-nummer fordelt på aktører (2016-2018)[330]

Folkeregisteret hadde ved utgangen av 2018 hele 847 721 aktive d-nummer der 351 585 av disse hadde status «kontrollert».[331] Dette tilsvarer 41 prosent. Status «kontrollert» innebærer som nevnt i rapportens definisjonsliste at personens identitet er kontrollert ved personlig fremmøte på ett av 42 skattekontor eller via utlendingsmyndighetene.[332] Det er den offentlige etaten eller private virksomheten som tilbyr en tjeneste som avgjør om en identitet må være «kontrollert» for å få tilgang på deres tjenester. Skatteetaten skriver i sin årsrapport for 2018 at «*Den enkelte aktør må selv vurdere behovet for ID-kontroll og risikovurdere egne tjenester opp mot det regelverk de forvalter. Tilgangen til å se statuskodene «kontrollert» og «ikke-kontrollert» fra Folkeregisteret ble tilgjengeliggjort for brukerne i eksisterende grensesnitt fra våren 2018*».[333]

Skatteetaten krever at det foretas en ID-kontroll før det tildeles skattekort. I 2018 ble ca. 55 000 av Skatteetatens ca. 60 000 rekvirerte d-nummer (ref. tabell over) kontrollert. Differansen gjelder i de tilfeller det ikke er foretatt kontroll da visse grupper av mennesker er fritatt dette.[334]

Mange av de øvrige rekvirentene krever ikke status «kontrollert» for bruk av deres tjenester, og har heller ikke hjemler for å kunne gjøre det. Per i dag eksisterer det

[329] Samling av rekvirenter med lavt antall rekvisisjoner som ikke lenger har egen kode i oversikt mottatt fra Skatteetaten
[330] Basert på data mottatt fra Skatteetaten 27.06.2019
[331] Skatteetaten, mottatt dokumentasjon på d-nummer. Gjelder d-nummer tildelt før 01.01.2019
[332] Folkeregisterforskriften § 3-2-1
[333] Skatteetaten, «ID-kontroll», 2019
[334] Skatteetaten oppgir på sine hjemmesider at følgende personer er unntatt oppmøteplikt til ID-kontroll: 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, 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, de som er i en situasjon der det vil være svært byrdefullt å møte opp på skattekontoret og legitimere seg. Sistnevnte kan søke fritak. For å få fritak må det sendes skriftlig søknad

ingen god statistikk på hvor mange (utover Skatteetatens egne rekvireringer) som blir sendt til ID-kontroll på skattekontorene og/eller faktisk gjennomfører denne ID-kontrollen. Skatteetaten anslår selv at ca. 1-2 prosent av d-nummer rekvireringene møter til ID-kontroll, og at 98-99 prosent av d-nummer rekvirert av andre enn Skatteetaten blir stående som «ikke-kontrollert» i Folkeregisteret.[335]

Når NAV rekvirerer et d-nummer med hjemmel i folkeregisterforskriften, får d-nummeret automatisk status «ikke kontrollert» i Folkeregisteret. For at status skal settes til «kontrollert», må personen møte opp hos ett av skattekontorene som har fått i oppgave å gjennomføre ID-kontroll. Norsk trygdelovgivning sier ikke noe om hvilke konsekvenser det har at en bestemt person har fått sin ID kontrollert. En søknad kan derfor verken innvilges eller avslås med hjemmel i ID-kontrollen i seg selv. Derimot inngår ID-kontrollen som et vurderingskriterium når saksbehandler skal vurdere om krav til lovlig opphold i Norge er oppfylt.

NAV oppgir at de oppfordrer brukere å bli «kontrollert» på skattekontor og skriver i informasjonsskriv til sine brukere at *«D-nummeret har et begrenset bruksområde fram til dine ID-dokumenter har blitt kontrollert. For å gjøre dette, må du personlig møte opp på skattekontoret og vise gyldig legitimasjon.»* NAV rekvirerte om lag 38 000 d-nummer i 2018, men kun i underkant av 1 000 d-nummer gjaldt personer som oppholdt seg i Norge på tildelingstidspunktet. Leverandøren er ikke kjent med at det gjennomføres ID-kontroll av personer i utlandet utover mottak av dokumentasjon fra bruker som har opparbeidet rettigheter og offisielle dokumenter mottatt fra andre lands trygdemyndigheter i tråd med trygdeavtaler som Norge har inngått med andre land.

Leverandøren er ikke kjent med at det er rutiner for å følge opp i etterkant hvis en bruker ikke møter til kontroll ved et av skattekontorene for eksempel om det sendes en tilbakemelding for videre oppfølging av brukeren og om dette potensielt kan få konsekvenser for hvilke tjenester eller ytelser brukeren mottar inntil d-nummeret er kontrollert.

Alle d-nummer blir satt som «inaktive» i Folkeregisteret fem år etter tildeling.[336] Inaktive d-nummer tildelt ved utgangen av 2018 var 939 484 hvor 1 169 av dem hadde status «kontrollert». Offentlige og private virksomheter som har myndighet til å rekvirere et d-nummer har også mulighet til å reaktivere d-nummeret. En person med inaktivt d-nummer kan også selv reaktivere det, men da ved å møte til ID-kontroll på et av Skatteetatens 42 skattekontor.

Rutiner, retningslinjer og kvalitet

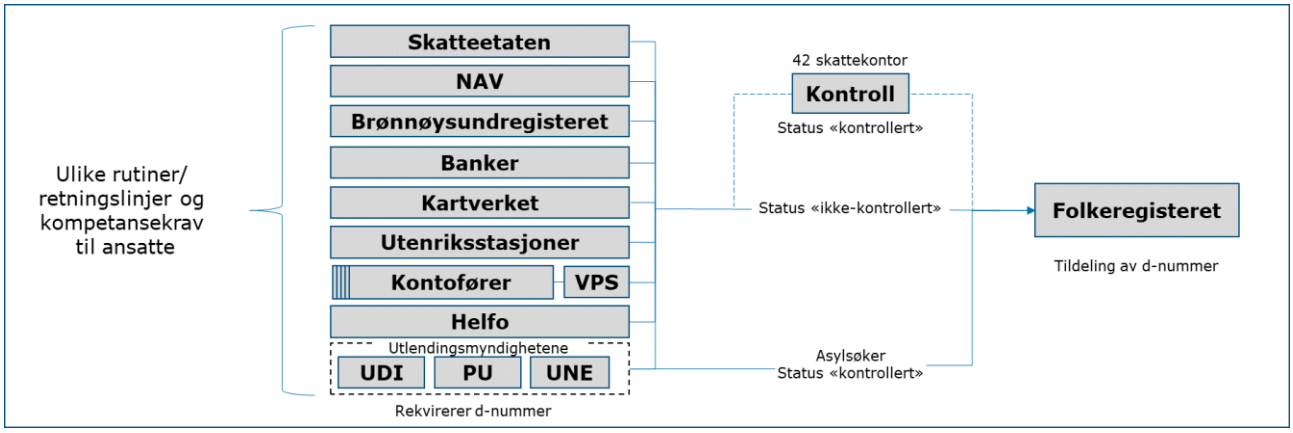
Tildeling av d-nummer skjer i stor grad automatisk via en digitalisert løsning, hvilket i praksis betyr at tildelingen skjer umiddelbart. Generelt stilles det kun krav til innsending av bekreftet kopi av ID-dokumenter ved rekvisisjon av d-nummer. Rekvirentene er ansvarlige for å fylle ut obligatoriske opplysninger om vedkommende og innhente dokumentasjon dersom det mangler.[337]

Feil i opplysninger kan føre til vanskeligheter rundt identifisering av brukeren og i noen tilfeller kan samme person få tildelt flere d-nummer uten at dette blir oppdaget.[338] Dette kan skje både med og uten overlegg fra brukerens side og fører til d-nummer dublering. Når rekvisisjonen sendes fra en av rekvirentene vil Skatteetaten automatisk gjennomføre en kontroll som forsøker å fange opp personer som allerede har et identitetsnummer. Oppstår det tvil om en dublering går saken til manuell behandling

[335] Informasjon mottatt i samtale med Skatteetaten
[336] Skatteetaten, «D-nummer», u.å.
[337] NAV, «Brukerveiledning DREK – Elektronisk rekvirering av d-nummer», 2019
[338] NAV, «Brukerveiledning DREK – Elektronisk rekvirering av d-nummer», 2019

hos saksbehandler i Skatteetaten. Som eksempel på en dublering kan en EØS-borger som har et aktivt d-nummer fra et tidligere arbeidsopphold, få et nytt d-nummer dersom han/hun kommer tilbake til Norge med endret navn som følge av giftemål og dette ikke oppdages.

Praksis for krav til ID-kontroll hos Skatteetaten ved rekvirering av d-nummer varierer som tidligere nevnt mellom rekvirentene. Skatteetaten krever personlig oppmøte og ID-kontroll ved søknad om skattekort med noen unntak, mens det for øvrige rekvirenter er opp til rekvirenten om den vil kreve at en person er ID-kontrollert for å få tilgang til deres tjenester/ytelser. På utlendingsfeltet er praksisen for asylsøkere noe annerledes. Tredjelandsborgere som søker asyl får her tildelt d-nummer parallelt med DUF-nummer, men det er først etter at UDI har ferdigbehandlet søkeren og innvilget opphold at Folkeregisteret gjenbruker ID-kontrollen og setter status på d-nummeret til «kontrollert»[339] (se eksempel på saksgang i kapittel 3.1.3). Figuren nedenfor gir en overordnet prosessbeskrivelse av hvordan d-nummer rekvireres og tildeles.



Figur 46 Overordnet prosess for rekvirering av d-nummer

Som nevnt innledningsvis i kapittelet er ikke leverandøren gjort oppmerksom på at det eksisterer felles overordnede rutiner/retningslinjer som gjelder for alle rekvirentene. Leverandøren har i spørreundersøkelsen blitt opplyst av samtlige rekvirenter, utenom UNE og VPS som i praksis ikke rekvirer d-nummer, at de har egne rutiner eller retningslinjer for rekvireringsprosessen i sin etat eller virksomhet.[340] Leverandøren har fått tilsendt rutinene fra de fleste aktørene. Rutinene og/eller retningslinjene er i stor grad etter leverandørens oppfatning ulikt utformet og inneholder ulik grad av informasjon og detaljering. Rutinene/retningslinjene ligger på alt fra én til elleve sider. Én av bankene som deltok i spørreundersøkelsen oppgir at de ikke har utarbeidede sentrale retningslinjer for rekvirering av d-nummer.

Ingen av rekvirentene har formelle kompetansekrav til ID-relatert utdanning eller sertifisering, utover generelle stillingskrav for ansatte som er involvert i rekvireringsprosessen. For samtlige aktører blir nødvendig kompetanse gitt til medarbeiderne som er involvert, og det oppgis at det gjennomføres intern kursing og opplæring av nye ansatte. Behov for ID-relatert kompetanse og behov for intern kursing og opplæring bestemmes av den enkelte aktør.

Samtlige av rekvirentene vurderer kvaliteten på *egne* rutiner eller retningslinjer i forbindelse med rekvisisjon av d-nummer som gode. På den annen side poengteres det

[339] Forskrift til folkeregisterloven (folkeregisterforskriften) (§ 3-2-1)
[340] UD opplyser at de ikke har laget egne rutiner/retningslinjer for rekvirering av d-nummer, men oversender i e-post til leverandøren en god rutinebeskrivelse av hvordan rekvireringen gjøres. Det er kun tre ansatte som har denne oppgaven

av enkelte at det todelte behandlingssystemet mellom søker, rekvirent og skattekontor er tungvint og tidkrevende.

Det er en felles enighet blant rekvirentene om at *egne* rutiner og retningslinjer er godt kjent blant ansatte og at de etterfølges.

Samtlige aktører oppgir at den overordnede kompetansen for å gjennomføre deres *egne* oppgaver i forbindelse med rekvirering av d-nummer er tilstrekkelig. Det påpekes likevel av noen at kontrollen som gjøres av rekvirentene er langt mer begrenset enn den som gjøres av skattekontorene og at det derfor krever mindre særskilt kompetanse. Én av rekvirentene vurderer at de innehar kompetanse i tråd med deres rutiner tilknyttet rekvirering av d-nummer, men at kompetansen for å sjekke om ID-dokumenter er forfalsket eller liknende er mindre god.

Potensielle feilkilder ved rekvirering og tildeling av d-nummer

Det kan være ulike feilkilder ved rekvirering og tildeling av d-nummer. Under følger de viktigste potensielle feilkildene slik forelagt leverandøren.

Rekvirentene sender i liten grad personer til Skatteetatens kontorer for ID-kontroll. Hovedgrunnen til dette oppgis å være manglende insentiver og hjemler for å kreve ID-kontroll. Videre trekkes det frem at det er spesielt krevende å få kontrollert personer som oppholder seg i utlandet og at dette særlig for NAV representerer et høyt antall rekvisisjoner.[341] Samlet betyr dette at et høyt antall d-nummer bli stående som «ikke-kontrollert» i Folkeregisteret og at disse kan brukes til tjenester hvor det ikke er noen krav til «kontrollert». Skatteetaten påpeker i sin årsrapport for 2018 at manglende identitetskontroll for d-nummer (og fødselsnummer) fortsatt er et problem og at det trolig vil ta noe tid for rekvirentene å få på plass regelverksendringer og retningslinjer for hvem som skal til ID-kontroll.[342]

Det er manglende dublettkontroll og risiko for d-nummer dublering ved tildeling som beskrevet tidligere.[343] Utfordringen er reell for alle tjenesteeiere som baserer seg på digital eller fysisk legitimasjon. Dette problemet nevnes også i flere rapporter leverandøren har fått innsyn i og NAV oppgir selv at det ble funnet 519 dubletter blant deres tildelte d-nummer i 2018. Som del av arbeidet med moderniseringen av Folkeregisteret ble det i 2016 oppgitt å være iverksatt tiltak for å avdekke dubletter[344], men det oppgis fortsatt som en stor feilkilde blant rekvirentene. Dubletter kan skape merkostnader for virksomhetene og problemer for de registrerte, samt gjøre at utveksling av informasjon mellom virksomheter er vanskeligere og informasjonen får dårligere kvalitet.[345] Det åpner også opp for misbruk av for eksempel trygdeytelser.

Skatteetaten og ulike rapporter påpeker en svakhet i at tilretteleggingen for status «unik» i regelverket ikke utnyttes i praksis grunnet manglende knytning mot biometri i tildelingen av d-nummer. I utgangspunktet tildeles hver person kun ett identitetsnummer, men slik systemet er i dag kan det ikke garanteres at en person ikke får flere identitetsnummer. Samme feilkilde gjelder også i prosessen for tildeling av fødselsnummer (kapittel 6.1.1).

[341] Gjelder ofte personer som har en svært løs tilknytning til Norge og som potensielt aldri vil oppholde seg i landet. Grupper av personer kan være: a) Barn og/eller ektefelle av et medlem i folketrygden, når bruker søker om ytelse fra NAV; b) Part og/eller barn i bidragssak som skal behandles etter norske regler om underholdsbidrag; c) Personer som har behov for at NAV registrerer opplysninger om medlemskap i norsk eller utenlandsk trygdeordning (oppgitt i e-post fra NAV)
[342] Skatteetaten, «Årsrapport 2018 for Skatteetaten», 2019
[343] Denne feilkilden er kan også være relevant for tildeling av fødselsnummer, men trekkes spesielt frem i forbindelse med rekvirering av d-nummer
[344] Difi, «Folkeregisteret – Endringer», 2016
[345] Skatteetaten, «Konseptvalgutredning – Ny personidentifikator i Folkeregisteret», 2015

De overnevnte feilkildene støttes også opp av tidligere vurderinger som er blitt gjort i dokumentasjon leverandøren har fått innsyn i. I tillegg trekkes det fram at rutiner for ID-kontroll varierer mellom rekvirentene og at service til publikum og effektivitet i flere tilfeller vektlegges mer enn sikkerhet.

6.1.3 Kvalitet og sikkerhet i forbindelse med utstedelse, fornyelse og tap av fysiske ID-bevis

I kapittel 2.3 ble en oversikt over tolv ID-bevis områdegjennomgangen har fokusert spesielt på presentert. Denne listen er utgangspunkt for vurderingen av kvalitet og sikkerhet i forbindelse med utstedelse, fornyelse og tap av ID-bevis.[346]

I kapittel 2.8.1 ble en tabell som oppsummerte antall ID-bevis utstedt (inkludert fornyelser av fysiske ID-bevis) og tapt per type i 2018 fremvist. Den viste at det totale antall ID-bevis utstedt i Norge i 2018 var ca. 1,8 millioner der norske pass, BankID og norske førerkort var mest utstedt.

Har en person kommet i besittelse av et ID-bevis kan det i flere tilfeller brukes til å få tilgang til nye og sterkere ID-bevis. Dette kan igjen fungere som en døråpner til å motta offentlige tjenester og ytelser (dette presenteres også i kapittel 5.1.2 og 5.1.3). Det er derfor svært viktig at prosessene tilknyttet utstedelse, fornyelse og tap av ID-bevis holder god kvalitet og et høyt sikkerhetsnivå.

Rutiner, retningslinjer og kvalitet for eID-løsningene (BankID, MinID og Buypass) diskuteres separat i kapittel 6.1.4.

Rutiner, retningslinjer og kvalitet

Det eksisterer ingen felles eller overordnede rutiner gjeldende for aktører som utsteder fysiske ID-bevis. Samtlige aktører har egne rutiner eller retningslinjer for utstedelse, fornyelse og/eller tap av ID-bevis.[347] Som forklart i kapittel 5.1.3 setter aktørene egne standarder og krav for hva som er gyldig legitimasjon ved utstedelse og fornyelse av ID-bevis.

De fleste aktørene oppgir at rutiner for utstedelse, fornyelse og tap av ID-bevis følger av samme rutiner/retningslinjer. Videre oppgir samtlige aktører at de følger samme rutine for utstedelse og fornyelse av ID-bevis. De ansatte i SVV følger det interne dokumentet «Rutinehåndbok for førerkortarbeid» samt prosessverktøy i arbeidet med utstedelse og tap av førerkort. I politiet følger rutiner for utstedelse og tap av pass av rundskriv 2015/002[348] og brukerhåndbok. Disse er tilgjengelige på KO:DE som er politiets intranett for deling av kompetanse, samt sendt på mail til saksbehandlere og formidlet og diskutert i paroler[349]. Det samme rundskrivet gjelder for utenriksstasjonene ved utstedelse av pass. Politiets rutiner for utstedelse, fornyelse og tap av reisebevis og utlendingspass følger av UDIs rundskriv 2019-001[350] og andre rundskriv UDI har utarbeidet, samt utlendingsloven og utlendingsforskriften. Bits (under Finans Norge) setter regler som gjelder for bankers utstedelse av bankkort med

[346] Med unntak av nasjonalt ID-kort da dette fortsatt ikke er lansert
[347] Bortsett fra politiet og utenriksstasjoner som har et felles rundskriv som gjelder for utstedelse av pass
[348] Politiet, «Rundskriv 2015/002 – Retningslinjer for passmyndighetenes behandling av saker ihht passloven m/forskrifter», 2015
[349] En parole er et orienterings- og introduksjonsmøte ved en politiavdeling
[350] UDI, «UDI rundskriv – Forberedelse, behandling og utstedelse av reisebevis for flyktninger og utlendingspass», 2019

bilde som legitimasjonsbevis der vilkår, legitimasjonskontroll med mer oppgis[351], men bankene har også i noen tilfeller øvrige egne retningslinjer som følges sentralt.

I politiets årsrapport i 2018 oppgis det at «*ombygging og sikring av pass- og ID-kontorer er frikoblet fra innføringen av nye systemløsninger og lanseringstidspunktene for nye pass og nasjonale ID-kort. På denne måten oppfylles nasjonale og internasjonale krav tidligere enn ved å vente på nye IKT-systemer*». Dette for å lukke merknader fra Riksrevisjonen og oppfylle fastsatte kvalitets- og sikkerhetsmessige krav for pass og ID-kontor.[352]

Når det gjelder kompetansekrav har POD utarbeidet minimumskompetansekrav for alle saksbehandlere innen pass og ID i kontrollinjen, vedtakslinjen og jurist vedtakslinje.[353] Dette inkluderer også krav til bestått avsluttende prøve etter fullført opplæring. For ansatte i utenriksstasjonene som jobber med forvaltningsmessige oppgaver som pass, kreves det gjennomført kurs organisert av UD og/eller tidligere erfaring med feltet. I politidistriktene har mange ansatte deltatt på første- og/eller andrelinjekurs i regi av NID. Det arrangeres også fagsamlinger der enkelte av dem har fokus på ID. SVV oppgir at alle ansatte skal delta på førerkortrelatert kurs arrangert av SVV med instruktører fra NID, men at de ikke har noen sentral opplæring av vikarer. I NAV er det ved utstedelse av Sjøfartsbøker kun et kompetansekrav at saksbehandler har spesialkompetanse på sjøfartsfaglige oppgaver.

Det varierer i hvilken grad utstederne vurderer kvaliteten på rutiner og retningslinjer i forbindelse med utstedelse og tap av ID-bevis som god. SVV påpeker at rutinebeskrivelsene i håndbøker er omfattende, men at de ikke har noen rutinebeskrivelse for hvordan de skal handle dersom det oppdages at kunden benytter falsk, manipulert eller et imposterdokument[354]. Det er generelt en uenighet blant politidistriktene om hvordan retningslinjer for utstedelse av pass, reisebevis og utlendingspass oppleves. Noen påpeker for reisebevis og utlendingspass at enkelte rundskriv oppleves som omstendelige med tungt språk. For pass påpekes det at brukerhåndboken ikke gir tilstrekkelige svar i vanskelige spørsmål og at brukerhåndbok og rundskriv i noen tilfelles oppleves som motstridende. På en annen side opplever noen politidistrikter retningslinjene som gode. POD ytrer at de er kjent med varierende kvalitet på rutinene ved utstedelse av pass i politiet, og påpeker videre at det gjøres en stor innsats for å styrke passutstedelsen gjennom en rekke tiltak. I dokumentasjon leverandøren har fått innsyn i fremkommer det at *banknæringen og Statens vegvesen ønsker å unngå risikoen ved at deres kort benyttes som ID-dokument da de erkjenner mangelfull kontroll i utstedelsesprosessen*.

Noen politidistrikter oppgir at de har hatt behov for å utarbeide egen rutine eller egen liste med spørsmål som bør stilles i forbindelse med tap av ID-bevis. Andre politidistrikter nevner at de ønsker seg en klarere punktliste knyttet til tap av ID-bevis.

Alle utstederne oppgir at egne rutiner og retningslinjer oppleves å være allment godt kjent og følges blant alle medarbeidere som er involvert i prosessene med utstedelse, fornyelse eller tap av ID-bevis.

De fleste aktørene oppgir at ID-kompetansen i sin etat eller virksomhet anses som tilstrekkelig da alle ansatte gjennomfører ulike former for kurs og opplæring innen ID-området. Det påpekes av noen at grunnet økt fokus på ID og midler til ID-arbeid har

[351] Bits, «Regler om utstedelse av legitimasjonsbevis (bankkort med bilde)», 2018
[352] Politiet, «Politiets årsrapport», 2018
[353] POD, «Kompetansekrav – Saksbehandlere pass og nasjonalt ID-kort», 2018
[354] NID, «Ekte pass, men feil person», 07.07.2017: «*Imposter er en person som benytter et ekte og korrekt utstedt dokument som tilhører en annen. Et identitetsdokument brukt på denne måten betegnes som imposterdokument. Slike dokumenter reiser i utgangspunktet ikke dokumenttekniske problemstillinger, og en dokumentteknisk undersøkelse vil ikke kunne avsløre en imposter*»

kompetansen på feltet vært økende blant alle ansatte. Andre mener likevel at det er områder der det er behov for å øke kompetansen og holde ansatte kontinuerlig oppdaterte på trender innen ID-feltet. Noen mener også at det er behov for økt fokus på personkontroll i skranken. POD påpeker at kompetansen til de ansatte som utsteder pass varierer, men at det gjøres en stor innsats og en rekke tiltak for å styrke de ansattes kompetanse.

Potensielle feilkilder

Det kan være ulike feilkilder ved utstedelse, fornyelse og tap av ID-bevis. Under følger de viktigste potensielle feilkildene slik forelagt leverandøren. Noen feilkilder gjelder kun for noen brukergrupper, og dette er i så fall spesifisert.

Det påpekes mangel på kompetanse og mangelfull opplæring av ansatte som utsteder ID-bevis. ID-kontroll blir mer og mer krevende grunnet mer sofistikerte forfalskningsmetoder og volum av personer hvor det kreves grundigere undersøkelse, noe som gir økt behov for god ID-kompetanse.[355] Feilkilden trekkes spesielt frem når det kommer til opplæring av og kompetansekrav til vikarer. For passforvaltning trekkes det også frem at ID-kompetanse er ulikt fordelt og ikke når frem til alle som jobber med dette. JD trekker frem at pass- og ID-forvaltningen er i ferd med å moderniseres og at et sentralt element i moderniseringen er å sikre tilstrekkelig opplæring til alle som arbeider med utstedelse av pass og ID-kort. Leverandøren erfarer at manglende kompetanse i ID-forvaltningen også understøttes i mange rapporter.[356] I NOU 2017:11 «Bedre bistand. Bedre beredskap.» oppga tre av tolv politimestre at etterforskningskompetanse og erfaring på ID-området «i mindre grad» er tilstrekkelig i politidistriktene.

Ved fornyelse av ID-bevis kan saksbehandler ta ID-kontrollen «for lett» og baserer den på at personen som ønsker fornyelse er rett person ifølge eksisterende ID-bevis. Dersom en person har fått et ID-bevis på bakgrunn av feil informasjon kan dette være vanskeligere å oppdage når ID-beviset skal fornyes.

I forbindelse med utstedelse av ID-bevis er bruk av imposterdokumenter et problem. Det er her snakk om misbruk av ekte dokumenter, hvor personen som fremviser dokumentet utgir seg for å være innehaveren. En kontroll av selve ID-dokumentet vil ikke alene indikere at noe er galt.[357] Ifølge NID er dette problemet økende.[358]

Pass, bankkort og førerkort sendes i vanlig post og på den måten kan de potensielt ende opp hos feil mottaker som kan føre til at dokumentet misbrukes. Som nevnt i kapittel 5.1.5 er det ofte valgfritt om mottaker vil hente ID-beviset hos utsteder eller motta det i posten. Det har vært flere tilfeller av at ID-bevis har kommet på avveie og ikke havnet hos riktig mottaker, og risikoen forbundet med det har vært mye omtalt i media.

Ved utstedelse av reisedokumenter til utenlandske borgere som har fått innvilget reisedokument etter å ha søkt asyl vil en feilkilde være informasjonen utlendingen selv har oppgitt. Dette kan være både med og uten overlegg. Dette gjelder informasjon som fødselsdato, navn fødested o.l. Det vil alltid være utlendinger som oppgir uriktige opplysninger om sin bakgrunn for at disse skal passe med forklaringer de gir når de kommer til Norge.

[355] SVV, «Samordning av ID-forvaltning – videre arbeid», 2018
[356] Blant annet i NID, «ID-kontroll i utlendingsforvaltningen», 2015
[357] NID, «Ekte pass, men feil person», 2017
[358] NID, «Misbruk av ID-dokumenter 2017», 2018

For lav bemanning kombinert med svake forutsetninger for å holde ventetiden nede trekkes frem som et problem. Dette gjelder spesielt i politiet for tredjelandsborgere og EØS-borgere. Dette fører til at medarbeidere bruker for lite tid på den enkelte utlending i skranken og at man ikke har nødvendig ro i situasjonen til å skjerpe fokus ved person- og dokumentkontrollen man gjør. Dårlig tid og stress i situasjonen resulterer i at man ikke er mistenksomme og grundige nok.

6.1.4 Kvalitet og sikkerhet i forbindelse med utstedelse, fornyelse og tap av elektroniske ID-bevis (eID)

Som beskrevet i kapittel 2.8.2 er det i dag flere ulike eID-løsninger for autentisering til offentlige digitale tjenester gjennom ID-porten. Brukere kan i dag benytte seg av den offentlige eID-en MinID, samt de private eID-ene BankID, Buypass og Commfides.[359]

Rutiner, retningslinjer og kvalitet

Bits (eget aksjeselskap eid av Finans Norge) setter, på samme måte som for bankkort med bilde, regler som gjelder for utstedelse og behandling av BankID. I tillegg gjelder lov om elektroniske tillitstjenester for sertifikatutstedere der det settes krav til kontroll av undertegners identitet. Ved utstedelse av BankID for banker som har fysiske filialer gjøres dette av ansatte ved bankfilialene der bruker må fremvise pass eller eventuelt andre ID-bevis banken definerer som gyldige. For banker som ikke har fysiske filialer foretas ID-kontrollen ved utstedelse gjennom Posten PUM (personlig utlevering av mottakingsbevis) enten på postkontor eller post i butikk. Ved utlevering av en PUM-sending må adressaten forevise godkjent legitimasjon.[360] Hva som er godkjent legitimasjon framgår av hentemeldingen for PUM. Adressaten må også kvittere for å hente sendingen personlig og legitimasjonsdokumentet blir kopiert.

Én av bankene oppgir at deres ressurser på antihvitvask og kundeopprettelse anbefaler at bankene er restriktive med å utstede BankID på grunnlag av d-nummer da det er svært vanskelig å vurdere enkelte utenlandske ID-dokumenter.

Buypass oppgir at de følger nasjonale og internasjonale retningslinjer/krav, men at rutiner/retningslinjer i forbindelse med utstedelse og fornyelse i stor grad ikke er relevant grunnet at prosessene her er tilnærmet 100 prosent automatisert. Buypass har egne rutiner for tap/sperring av Buypass. ID-kontroll ved utstedelse gjøres på samme måte som for BankID.

Utstedelse av MinID skjer ved at sluttbruker bestiller MinID på internett og får tilsendt pinkoder som post til folkeregistret adresse. Det er en integrert tilleggssikring ved at bruker mottar velkomstbrev som post til folkeregistret adresse etter at brukeren er blitt aktivert. Løsningen for utstedelse er selvbetjent, brev trykkes i «lukket løsning» og ansatte i MinID er ikke involvert i utstedelsen. Følgelig gjennomføres det ingen fysisk ID-kontroll ved utstedelsen av MinID. I tillegg til den vanlige løsningen for MinID har Difi et samarbeid med Skatteetaten for å utstede MinID til personer med kortere arbeidsopphold i Norge. Prosjektet omtales som MinID-on-the-fly, og her skjer utstedelse når personen møter til ID-kontroll hos Skatteetaten.

Dagens eID-er har evig gyldighetstid, noe som betyr at eventuelle feil i en tidligere ID-kontroll ikke vil bli plukket opp på et senere tidspunkt. Det er ingen krav til fremvisning av ID-bevis ved fornyelse av eID da denne skjer automatisk. Ved tap av eID sperres denne av bruker selv eller gjennom utsteder.

[359] Commfides er ikke en del av ID-bevis prioritert i områdegjennomgangen (ref. kapittel 2.3)
[360] Posten, «Legitimasjon og fullmakter», u.å.

Ved utstedelse av BankID og Buypass gjennom Posten PUM er det som regel ingen kompetansekrav til ansatte hos posten eller dagligvareansatte i post i butikk.

Potensielle feilkilder

Under følger de viktigste potensielle feilkildene slik de er forelagt leverandøren.

Det kan legges falske fysiske identitetsbevis til grunn for opprettelse og utstedelse av eID, noe som videre gir bred tilgang til en rekke tjenester.

Det gjøres ingen fysisk kontroll ved utstedelse av MinID og noen hevder at det er fare for at det mangler etterlevelse av rutiner for kontrollen som gjøres ved utlevering med Posten PUM som banker og Buypass benytter for utstedelse av eID. Bankene og Buypass stoler på at Posten er gode nok til å sjekke og kreve ID-bevis, men har ingen god måte å sjekke og kontrollere at disse rutinene etterfølges. Manglende ID-kontroll ved bestilling av MinID gjør også at det er enkelt å bestille, aktivere og misbruke en annens person MinID dersom personens fødselsnummer og folkeregistrerte adresse er kjent for andre. Totalt sett fører dette til at det generelt foreligger potensielle sikkerhetshull ved utstedelse av eID.

Bankene, som utstedere av BankID, har ikke forutsetning for å kunne sjekke doble identiteter ved ID-kontrollen som gjennomføres ved utstedelse. Videre kan ikke bankene sjekke om andre aktører i ID-forvaltningen har gjort «feil» ved respektive aktørers ID-kontroller, for eksempel ved at de ikke har tilgang til å se hvorvidt brukere som søker om eID har status «kontrollert» i Folkeregisteret eller ikke. Det er videre ingen begrensning på hvor mange BankID-er som kan utstedes på det enkelte identitetsnummer. Dette er mulig ettersom bankene ikke sjekker seg imellom om et identitetsnummer tidligere har fått utstedt BankID. Sistnevnte setning gjelder ikke for Buypass og Commfides.

Om en person på urettmessig grunnlag har fått utstedt en eID kan denne i praksis brukes videre til evig tid da fornyelsen gjøres automatisk uten ID-kontroll. Dette gjelder uavhengig om identitetsnummeret knyttet til eID-en er «kontrollert» eller «ikke-kontrollert». Det gjøres heller ingen kontroll på om personen som bruker eID-en faktisk er rettmessig eier.

Det nevnes for øvrig i flere samtaler leverandøren har gjennomført at feil og misbruk i eID ikke oppfattes som et stort problem. Tilfellene som blir rapportert av misbruk er som regel i forbindelse med at personer har gitt fra seg eID-passord til noen de har tiltro til. Det nevnes likevel i Finanstilsynets risiko- og sårbarhetsanalyse 2018[361] at svindel foretatt av familiemedlemmer, eksempelvis ved bruk av BankID vurderes som en av de viktigste truslene. Verken Finanstilsynets ROS-analyse eller samtaler med banker gir et samlet estimat på konsekvensene av feil eller misbruk av eID for finansnæringen.

6.1.5 Samfunnsmessige konsekvenser av feil og misbruk av ID

I områdegjennomgangen definerer leverandøren samfunnsmessige konsekvenser ved feil og misbruk av ID i vid forstand. Det kan være konsekvenser i form av direkte verditap for samfunn og individ, men også andre indirekte belastninger og skadevirkninger. Tidligere forskning og undersøkelser viser at det er utfordrende å beregne samfunnets kostnader ved kriminalitet.[362]

[361] Finanstilsynet, «Risiko- og sårbarhetsanalyse (ROS) 2018», 2019
[362] JD, «Kriminalitetens samfunnsmessige kostnader», 2006

Samfunnsmessige konsekvenser ved feil og misbruk av andres identiteter og ID-bevis kan være betydelige. Konsekvenser er knyttet til bevisste og ubevisste feil gjennomført av enkeltpersoner, private og/eller offentlige virksomheter. Det er gjort ulike evalueringer, kartlegginger og undersøkelser på enkeltområder med varierende grad av faktaorientering relatert til samfunnsmessige konsekvenser av feil og misbruk. Leverandøren har ikke blitt opplyst om eller gjort oppmerksom på at det eksisterer statistikk, nøkkeltall[363] eller rapporter som dokumenterer samlede samfunnsmessige kostnader av feil og misbruk for ID-forvaltningen.

Nye pass og nasjonale ID-kort med eID er en av de store pågående satsingene i ID-forvaltningen. I programmets gevinstoversikt har leverandøren ikke identifisert kvantifiserbare samfunns- og brukereffekter eller en kvantifiserbar nullpunktsmåling av feil og misbruk av ID. Hovedfokus i oversikten er gevinster for politiet, men samfunnsmessige gevinster trekkes fram i den grad det er kjent. POD skriver at *«fordi det ikke har vært mulig å tallfeste de samfunnsmessige gevinstene knyttet til redusert ID-misbruk og opprettholdelse av norske ID-dokumenters anseelse er beregnet netto nåverdi negativ. Sett i lys av tiltakets kvalitative effekter vurderes nytteverdien likevel å overstige investeringskostnadene».* [364]

Siden datagrunnlaget er mangelfullt og det ikke finnes noen helhetlig klassifisering av samfunnsmessige konsekvenser har leverandøren valgt tilnærmingen i tabell 17. Samfunnsmessige konsekvenser kan være kategorisert som fremstilt i tabellen nedenfor.

Direkte og indirekte konsekvenser på samfunnsnivå	Direkte og indirekte konsekvenser på individnivå
• Økonomisk kriminalitet 1. *Arbeidslivskriminalitet* 2. *Trygdesvindel* 3. *Annet* • Øvrig kriminalitet og samfunnssikkerhet	• Fysiske, psykiske og økonomiske belastninger

Tabell 17 Klassifisering av samfunnsmessige konsekvenser

Basert på risiko og vesentlighet har leverandøren i kartleggingen av samfunnsmessige konsekvenser av feil og misbruk vektlagt konsekvenser for samfunnet: økonomisk kriminalitet, herunder arbeidslivskriminalitet og trygdesvindel, samt øvrig kriminalitet og samfunnssikkerhet. I dette kapittelet beskriver leverandøren først implikasjonene av feil og misbruk for samfunnet. For å vurdere kostnader har leverandøren i tabell 18 oppsummert kvantifiserbare eksempler med henvisninger til relevante rapporter. Samfunnsmessige kostnader ved feil og misbruk i ID-forvaltningen som ikke avdekkes defineres i områdegjennomgangen som mørketall.

Konsekvenser for samfunnet

I tildelingsbrevet for 2019 fikk politiet fem hovedmål, hvorav ett er: «*Alle som oppholder seg i Norge har avklart identitet og lovlig opphold».* Videre skriver JD at *«politiet registrerer riktig identitet sikrer korrekte vedtak i forvaltningen, og kan bl.a. redusere misbruk av offentlige ordninger. Utlendinger med ukjent identitet som oppholder seg i landet, kan utgjøre en risiko for samfunnssikkerheten og økt kriminalitet. Gode ID-vurderinger er et viktig samfunnsansvar for politiet».*[365]

[363] I tildelingsbrev til POD 16.01.2019, vedlegg 3, skal det for 2019 under ID-avklaring fremkomme statistikk over saker der det er avdekket falsk ID eller imposter, både i Norge og ved innreise til Norge
[364] POD, «Gevinstoversikt for Nye pass og nasjonale ID-kort med eID (versjon 2.2)», 2019
[365] JD, «Tildelingsbrev til POD», 2019

Økonomisk kriminalitet
Politiets STRASAK-rapport gir en oversikt over anmeldt kriminalitet totalt, og i 2018 ble det anmeldt 318 566 lovbrudd. Økonomisk kriminalitet utgjorde 9 prosent av totalt anmeldte lovbrudd i 2018, men hvor stor del som er relatert helt eller delvis til ID-misbruk fremkommer ikke av statistikken. [366]

Ifølge POD er misbruk av ID-dokumenter ofte en del av en mer omfattende sak i politiets register. Saker blir registrert på ulike typer kriminalitet uten at det framgår at ID er et element i saken. POD skriver at «*dette vanskeliggjør uthenting av statistikk og per i dag har man ikke lykkes med å fremskaffe en pålitelig oversikt over antall saker der ID-forfalskning eller misbruk inngår*».[367]

POD understreker at misbruk av eID er et betydelig problem som får store konsekvenser særlig for finansnæringen og for den enkelte som rammes.

1. *Arbeidslivskriminalitet*

Regjeringens strategi mot arbeidslivskriminalitet (2019–) er et viktig tiltak i bekjempelsen av økonomisk kriminalitet.[368] Arbeidslivskriminalitet kjennetegnes ved at det spenner over organisatoriske grenser, myndighetenes forvaltningsområder og hierarkiske nivåer i staten.[369] Som beskrevet i kapittel 4.2.4 innebærer begrepet arbeidslivskriminalitet: *«Handlinger som bryter med norske lover om lønns- og arbeidsforhold, trygder, skatter og avgifter, gjerne utført organisert, som utnytter arbeidstakere eller virker konkurransevridende og undergraver samfunnsstrukturen.*[370]

Samfunnsøkonomisk analyse har tidligere anslått at arbeidslivskriminalitetsomfanget i 2015, målt med skjult verdiskaping, var om lag 28 mrd. kroner. Det finnes ulike former for arbeidslivskriminalitet og de skriver at *«unndragelse av skatter- og avgifter i hovedsak gjennomføres av næringsliv, mens arbeidslivsrelatert trygdesvindel*[371] *i større grad er et samarbeid mellom arbeidstaker og arbeidsgiver»*.[372]

Ett av flere kjennetegn ved arbeidslivskriminalitet som regjeringens strategi peker på er bruk av uriktige eller falske opplysninger og dokumentasjon til offentlig myndighet. Det kan eksempelvis være bruk av falsk identitet og registrering av uriktig informasjon i ulike offentlige registre. En del av lovbruddene innenfor arbeidslivskriminalitet er avhengige av uriktig status i ett eller flere registre for å kunne gjennomføres.[373] Økokrims trusselvurdering fra 2018 peker på at «*Norge har over tid vært en attraktiv destinasjon for arbeidssøkende, med mulighet for økt inntekt og et bedre liv. Utenlandske personer uten lovlig opphold, er særlig utsatt for utnyttelse av kriminelle aktører. I de mest alvorlige sakene rapporteres det om menneskehandel tilknyttet organisert kriminalitet. ID- og dokumentmisbruket ser også ut til å øke*».

Som beskrevet i kapittel 6.1.2 kan et feiltildelt d-nummer få alvorlige konsekvenser. Som et eksempel kan en person med to eller flere d-numre fordele inntekten sin på disse, og dette vil gi tapte skatteinntekter for staten. NID oppgir at misbruk av identitet og legalisering av denne kan bidra til utnyttelse av arbeidskraft. Det er registrert flere eksempler på at borgere av EU-land låner bort identiteten sin til tredjelandsborgere

[366] Økonomisk kriminalitet defineres gjerne som «profittmotiverte, lovstridige handlinger som ofte begås innenfor eller med utspring i en økonomisk virksomhet som i seg selv er – eller gir seg ut for å være – lovlig». Hvitvasking, skatte-, avgifts- og tollunndragelser, regnskapskriminalitet og verdipapirkriminalitet faller inn under denne definisjonen
[367] Politiet, «Gevinstoversikt for nye pass og nasjonale ID-kort med eID» (versjon 2.2, behandlet 8.2.2019)
[368] Regjeringen, «Strategi mot arbeidskriminalitet (2019-)», 2019
[369] Fimreite m.fl. (2011) "Organisering, samfunnssikkerhet og krisehåndtering", Difi (2014) "Mot alle odds? Veier til samordning i norsk forvaltning"
[370] Prop. 115 L (2017-2018) Endringer i personopplysningsloven (bekjempelse av arbeidslivskriminalitet).
[371] Alle former for trygdesvindel defineres ikke som arbeidslivskriminalitet
[372] Samfunnsøkonomisk analyse, «Analyse av former, omfang og utvikling av akrim», 2017
[373] SKD, Direktoratet for arbeidstilsynet, Arbeids- og velferdsetaten, POD, «mål- og resultatstyring for det tverretatlige a-krimsamarbeidet», 2017

som utfører arbeid i Norge. Skatteetaten oppgir også at de ser eksempler på at flere personer bruker den samme identiteten. Videre, dersom eksterne aktører, som finansbedrifter, fastleger eller NAV, legger til grunn fødsels- eller d-nummer uten annen dokumentasjon eller kontroll kan dette få store følgefeil.

2. Trygdesvindel

I tildelingsbrev for 2019 står det at *«NAV skal forebygge og avdekke trygdesvindel. Det skal gjennomføres risikoanalyser for å identifisere områder som er særlig utsatt for trygdesvindel, der også behovet for nye eller supplerende virkemidler og om fordelingen av ressurser mellom forebyggende tiltak og etterfølgende kontroll gir best mulig effekt blir vurdert».*[374]

NAV definerer trygdesvindel som at en bruker bevisst gir feil opplysninger og dermed får for mye utbetalt.[375] I årsrapporten for 2018 skriver NAV: *«Muligheten for at feilutbetalings- og svindelsaker ikke blir forebygget, avdekket og håndtert på en tilfredsstillende måte, har NAV i flere år identifisert som en risiko»*.

I 2018 ble det utbetalt totalt 513,9 mrd. kroner fra NAV.[376] Det ble anmeldt 166 mill. kroner for trygdesvindel, hvorav andelen relatert til ID er ukjent. De fleste av sakene var knyttet til svindel av dagpenger for eksempel ved at brukere har arbeidet og mottatt lønn som er uforenlig med ytelsen. Det ble anmeldt trygdesvindel i sammenheng med arbeidslivskriminalitet for til sammen 27,5 mill. kroner i 2018.[377]

NAV understreker imidlertid at det er store mørketall, og ukjent hvor stor andel av de totale utbetalingene som er feilutbetalt eller svindelsaker. NAV peker i dialog med leverandøren på at det er flere mulige kilder til trygdesvindel som følge av feil og misbruk av ID. To av de mistenkte feilkildene er rekvirering av d-nummer for personer i utlandet og svakheter ved ID-kontroll av brukere for enkelte ytelser.

Når det gjelder utenlandske saker legger NAV i hovedsak til grunn offisiell dokumentasjon de mottar fra trygdemyndigheter i land som Norge har trygdeavtaler med i sin saksbehandling uten å gjennomføre ytterligere ID-kontroller.[378]

Videre vurderer NAV at mangel på deling av informasjon mellom sektorer og virksomheter er utfordrende for å avdekke feil og misbruk av ID. Det er ikke gode nok rutiner i dag på at NAV får beskjed om falske identiteter. NAV samarbeider med primæraktørene i ID-forvaltningen, og er kjent med andres porteføljer av saker som er til behandling knyttet til feil og misbruk av ID uten at de nødvendigvis får tilgang til informasjonen og kan bruke det i egen saksbehandling. Samarbeidsaktørene viser ofte til at de ikke har hjemmel til å utlevere opplysninger til NAV.

Ifølge NAV er det betydelige usikkerheter knyttet til beregning av kostnaden relatert til falsk ID eller misbruk av ID. Tidligere beregninger viser at en fiktiv identitet i norske registre gjennom et «livsløp» kan utgjøre 13-14 mill. kroner i stønader per identitet.[379]

---

[374] ASD, tildelingsbrev for NAV, 2019
[375] NAV, «Trygdesvindel», 2019
[376] NAV, «Årsrapport», 2018
[377] NAV, «NAV i tall og fakta», 2019
[378] Frem til nå har dokumentasjon på trygdeopplysninger vært sendt på papir per post mellom land med begrenset systemstøtte. EUs EESSI-prosjekt utvikler en sentral løsning for utveksling av trygdeopplysninger på tvers av land som er planlagt implementert i 2019. Trygdeavtalene har regler om hvilket lands trygdeordning du skal være tilknyttet. Personer fra avtaleland skal behandles likt uavhengig av statsborgerskap. Den mest omfattende avtalen som Norge har er med EØS-landene. EØS-avtalens trygdebestemmelser går foran både norsk lov og andre trygdeavtaler som Norge har inngått
[379] Utredning «Knytning mellom Folkeregisteret og biometri i Passregisteret, Nasjonalt ID-kortregister og Utlendingsdatabasen», 2016

NAV antar at denne typen saker vil være svært sjeldne, og at beløpet i avdekte saker erfaringsmessig er vesentlig lavere med et gjennomsnitt på om lag 0,5 mill. kroner. NAV har ikke oppgitt antall saker, men illustrerer i eksemplene nedenfor hvordan stønader er utbetalt til personer som har vist seg å operere med falsk identitet. Her har NAV avdekket falsk identitet og avverget ytterligere feilutbetalinger. NAV gjør oppmerksom på at det er stor usikkerhet knyttet til beregning av kostnader.[380] Vedlegg 9 fremstiller en oversikt over antall anmeldte saker av trygdemisbruk i perioden 2010-2019 mottatt fra NAV basert på bruk av uriktig identitet i Folkeregisteret. Beløp per år varierer anslagsvis fra 0 mill. kroner til 7 mill. kroner.

Det er grunn til å tro at det er betydelige mørketall for ID-relaterte saker, uten at dette kan dokumenteres med statistikk eller styringsinformasjon.

Eksempel 1: En falsk identitet mottok til sammen ca. 1,7 mill. kroner i ulike stønader, frem til den falske identiteten ble avdekket. I løpet av en 11-års periode ble det utbetalt følgende stønader: Barnetrygd, kontantstøtte, sykepenger, foreldrepenger, dagpenger og arbeidsavklaringspenger.

Under forutsetning av at den falske identiteten ikke hadde blitt avdekket og at personen hadde gått over på uføretrygd og senere alderspensjon estimeres den totale stønaden å beløpe seg til ca. 11 mill. kroner.

Fordeling:
- ca. 0,5 mill. kroner i barnetrygd frem til barna fyller 18 år
- ca. 7,5 mill. kroner i uføretrygd fram til 67 år (vurderes som et konservativt estimat)
- ca. 3 mill. kroner i alderspensjon fra fylte 67 til 80 år (vurderes som et konservativt estimat)

Eksempel 2: En falsk identitet mottok til sammen ca. 1,2 mill. kroner i ulike stønader, frem til den falske identiteten ble avdekket. I løpet av en 11-års periode ble det utbetalt følgende stønader: Overgangsstønad, barnetrygd, bidragsforskudd og dagpenger.

Under forutsetning om at den falske identiteten ikke hadde blitt avdekket, og at vedkomne hadde gått over på alderspensjon estimeres den totale stønaden å beløpe seg til ca. 4,1 mill. kroner.

Fordeling:
- ca. 0,5 mill. kroner i barnetrygd frem til barna fyller 18 år
- ca. 0,6 mill. kroner i bidragsforskudd frem til barna fyller 18 (beregnet bidrag forskuddet etter ordinær forskudd)
- ca. 3 mill. kroner i alderspensjon fra fylte 67 til 80 år (vurderes som et konservativt estimat)

Det er ikke beregnet fremtidig uføretrygd i denne saken i og med at det ikke har vært utbetalt sykestønader på denne falske identiteten.

[380] Epost fra NAV 29. mai 2019

Øvrig kriminalitet og samfunnssikkerhet
Samfunnet er i endring og kriminaliteten blir mer digital og grenseløs, ifølge politiets årsrapport for 2018.[381] Politiet beskriver i sin vurdering en dreining fra fysisk til digital kriminalitet, og at denne forventes å fortsette. [382]

Norge er en liten og åpen økonomi. EØS-avtalen skal sikre fri flyt av varer, personer, tjenester og kapital. Den gir norsk næringsliv adgang til et marked med 500 millioner mennesker. Dette gir vesentlige effektiviseringsgevinster for enkeltpersoner, private bedrifter og den norske økonomien. Rundt tre fjerdedeler av norsk eksport går til EØS-området ifølge arbeids- og sosialministeren.[383]

EØS-avtalen og Schengen-samarbeidet gjør det også lettere for personer å bevege seg på tvers av våre landegrenser uten identitets- og personkontroll.[384] For politiet er avklaring av identitet og kontroll over hvem som til enhver tid befinner seg i landet avgjørende i arbeidet med forebygging av kriminalitet, kriminalitetsbekjempelse og beredskap i samfunnet.[385] JD trekker frem at svakheter i ID-forvaltningen i Norge kan få implikasjoner for vårt medlemskap i Schengen på sikt.

Justis- og innvandringsministeren uttalte i 2019 at *«misbruk av falsk identitet er et omfattende problem i dag. Vi har et sted mellom 10 000 og 30 000 personer i Norge som er her ulovlig, og vi har ikke noen identitet på dem».*

I et samfunnssikkerhetsperspektiv bør norske myndigheter ha oversikt over hvem som befinner seg i landet. I den nasjonale risikovurderingen understrekes det at uten bruk av biometrisøk hvor man kontrollerer om ansiktsfoto eller fingeravtrykk er registrert på en annen identitet, vil det være en risiko for at en person har flere identiteter, med tilhørende samfunnsmessige konsekvenser.[386] Feil og misbruk av ID kan svekke tilliten til velferdsstaten og skape samfunnssikkerhetsmessige utfordringer ved at det kombineres med andre former for kriminalitet som cyber, terrorisme, menneskesmugling, menneskehandel og illegal innvandring.[387]

Det har vært en betydelig innvandring til Europa de siste årene, og de sikkerhetsmessige og sosioøkonomiske forholdene tilsier at det vil fortsette. I JDs nasjonale risikovurdering trekkes det frem at økt tilstrømning av utenlandske borgere erfaringsmessig medfører en økning i benyttelsen av falske ID-dokumenter og identitetsmisbruk. JD peker på at misbruk av ID er en viktig driver for menneskesmugling. [388] Ifølge Kripos bruker bakmenn blant annet falske ID- og reisedokumenter eller falske underlagsdokumenter for å registrere ofre for menneskehandel i EØS for å utnytte smutthull i regelverket.[389] JDs risikovurdering viser til at menneskehandel og menneskesmugling er blitt mer utbredt blant organiserte kriminelle i EU. Aktører som tilbyr falske dokumenter med ulovlig innreise som hensikt, vil utgjøre en betydelig trussel for samfunnssikkerheten, også fordi dokumentene kan gjenbrukes innen andre former for kriminalitet. Dette gjelder eksempelvis ved at kriminelle grupper kontrollerer hele menneskehandelskjeden, fra rekruttering av ofre til hvitvasking av profitten og potensiell terrorfinansiering.[390] Europol påpeker at

[381] Politiet, «Politiets årsrapport», 2018
[382] Politiet, «Trender i kriminalitet 2018 – 2021», 2018
[383] Regjeringen, «EØS-avtalen 25 år - arbeidsliv i endring», 2019
[384] Regjeringen, «Ofte stilte spørsmål», 2017
[385] Politiet, «Politiets årsrapport», 2018
[386] Regjeringen, «Nasjonal risikovurdering - Hvitvasking og terrorfinansiering i Norge», 2018
[387] NID, «Misbruk av ID-dokumenter», 2017
[388] Regjeringen, «Nasjonal risikovurdering - Hvitvasking og terrorfinansiering i Norge», 2018
[389] Politiet, «Menneskehandel i Norge – kriminelle aktører», 2017
[390] Regjeringen, «Nasjonal risikovurdering - Hvitvasking og terrorfinansiering i Norge», 2018

terrorister har brukt menneskesmuglingsnettverk til å komme til Europa, og menneskesmugling utnyttes av terroristorganisasjoner for å skaffe finansiering.[391]

I STRASAK-rapporten 2018 beskriver politiet at det lenge har vært kjent at kriminelle misbruker andres identiteter og bruker fiktive identiteter til å begå ulike former for kriminalitet digitalt og fysisk.[392] De forsøker å utnytte svakheter i fastsettelse, registrerings- og utstedelsesprosessen til ID-bevis. Dette er utfordrende for både private og offentlige aktører med behov for å verifisere identitet til enkeltpersoner og deres tilknytning til Norge.[393] JD oppgir at *«svakheter i identifisering er en direkte årsak til omfattende kriminalitet. Mangelfull identifisering og utstedelse av ID-bevis kan legge til rette for menneskehandel og utnytting av svake personer, ofte gjennom en såkalt ID-karusell - hvor oppholdskort og asylssøkerbevis "går i arv". I enkelte bransjer er dette et så alvorlig problem at det i beste fall er konkurransevridende og i verste fall innebærer at lovlig drevne selskaper går konkurs»*.

Det er en betydelig, ikke kvantifisert, samfunnsøkonomisk kostnad ikke å avklare identitet fra første kontakt med offentlig sektor i Norge. Det kan gi økte oppfølgingskostnader av denne personen senere i andre deler av samfunnet, både privat og offentlig. Politiet har ansvaret for viktige oppgaver og for at ID-forvaltningen samlet skal kunne levere på dette*: grensekontroll og utlendingskontroll på territoriet, førstelinjen i utlendingsforvaltningen, registrering av asylsøkere, samt uttransportering av personer uten lovlig opphold.*[394]

I gevinstoversikten for nye pass og nasjonale ID-kort med eID skriver POD at *«de er kjent med at det har vært en endring i modus for misbruk av identiteter i løpet av de siste årene. Det har endret seg fra etablering og bruk av falske identiteter til misbruk av ekte identiteter satt i system. Dette gjelder særlig identiteter fra EØS-land.»*[395] Frontex og Europol peker på at det økende sikkerhetsnivået i moderne reisedokumenter og strengere migrasjonspolitikk blant landene i Schengen gjør at misbruk av autentiske reisedokumenter trolig vil bli mer utbredt.[396] Norske borgere har i dag visumfrihet til 186 land og politiet understreker at *«opprettholdelse av norske reisedokumenters status internasjonalt forutsetter at internasjonale forpliktelser og regler overholdes, at ID-dokumentene holder høyt sikkerhetsnivå, og at utstedelsesprosesser og systemer er tilfredsstillende».*[397] Det finnes eksempler på produksjonsutstyr av pass på avveie i enkelte land, men dette gjelder ikke Norge. Derimot finnes det et marked for kjøp og salg av ID-bevis på det mørke internettet.[398] Et raskt søk på internett viser at norske pass ansees som verdifulle internasjonalt. NID sin rapport om «Misbruk av nordiske pass ved reiser» (2019) viser at omfanget av misbruk av norske pass i utlandet var høyere enn hva man tidligere har vært kjent med.

En av de viktigste prosessene i et demokratisk samfunn som Norge er gjennomføring av valg. Som beskrevet i kapittel 4.1.19 skal velgeren legitimere seg dersom stemmemottakeren ikke kjenner velgeren, men verken loven eller valgforskriften regulerer nærmere hva som anses som «legitimasjon». På valgkortene som sendes ut til alle stemmeberettigede personer i Norge oppgis det at minstekravet for legitimasjon er at det må inneholde navn, fødselsdato og bilde. Videre oppgir Valgdirektoratet at *«stemmemottaker skal imidlertid utvise skjønn ved vurdering av velgers legitimasjon.*

[391] Europol, «Serious and Organised Crime Threat Assessment (SOCTA)», 2017
[392] Politiet, «STRASAK-rapporten», 2018
[393] Politiet, «STRASAK-rapporten», 2018
[394] Politiet, «Politiets årsrapport», 2018
[395] Politiet, «Gevinstoversikt for nye pass og nasjonale ID-kort med eID» (versjon 2.2, behandlet 8.2.2019)
[396] NID, «Misbruk av ID-dokumenter», 2017
[397] Politiet, «Gevinstoversikt for nye pass og nasjonale ID-kort med eID» (versjon 2.2, behandlet 8.2.2019)
[398] NorSIS, «Hvor mye koster din digitale identitet?», u.å.

Så lenge legitimasjonen viser at velgeren er den vedkommende utgir seg for å være, anses det som godt nok. Dette gjelder også selv om legitimasjon eventuelt har gått ut på dato».[399] Det viser en manglende bevisst holdning til hvilken legitimasjon som er sikker nok i det enkelte tilfellet. Uklare krav til ID-kontrollen i valglokalene og begrenset opplæring av de som skal gjennomføre den er en potensiell feilkilde og samfunnssikkerhetsrisiko. Eksempelvis bør det ved vurdering av hva som er gyldig legitimasjon ved valg sees hen til brukervennlighet og valgdeltakelse, men like viktig er tilliten til en viktig demokratisk prosess og sikkerhetsnivået for å redusere muligheten for å avgi flere stemmer og kunne påvirke valgresultatet.

Oppsummering
For å vurdere samfunnsmessige kostnader ved feil og misbruk relatert til ID-forvaltningen har vi i tabellen under oppsummert kvantifiserbare eksempler med henvisninger til relevante rapporter.

[399] Valgdirektoratet, «Legitimasjon», 2019

Områder	Samfunnsmessig kostnader	Kostnader relatert til ID	Kilde
Arbeidslivskriminalitet Analyse av former, omfang og utvikling av arbeidslivs-kriminalitet.	For 2015 ble det anslått at arbeidslivskriminalitetsomfanget, målt med skjult verdiskaping, var 1,2 prosent av fastlands-BNP, eller om lag **28 mrd. kroner.** Dersom man kun ser på arbeidslivskriminalitet som det anslåtte unndratte beløpet og trygdesvindel er andelen 0,5 prosent, eller om lag 12 mrd. kroner.	Kostnader relatert til ID er ikke spesifisert. Feil og misbruk omtales som en av flere årsaker.	Samfunnsøkonomisk analyse (rapport 69-2017)
Trygdesvindel En kartlegging av fem stønadsordninger (2011) Misbruk av sykepengeordningen i folketrygden (2013)	I Norge ble mørketallene (både avdekket og ikke avdekket) for trygdesvindel estimert av Proba samfunnsanalyse i to rapporter fra 2011 og 2013. Rapportene omfattet de 6 ytelsene som ble vurdert til de med høyest risiko for trygdesvindel. Anslagene oppgis å være svært usikre, men gir likevel indikasjoner på at det er betydelige beløp som ikke avdekkes sett i forhold til det som avdekkes. For sykepenger ble svindelen anslått til å være minst 6 prosent av utbetalingene. For de øvrige ytelsene var svindelen anslått til ca. 5 prosent, med stor variasjon mellom de ulike ytelsene. **I 2011-kroner tilsvarer det om lag 8 mrd. kr**.	Kostnader relatert til ID er ikke spesifisert. Feil og misbruk omtales som en av flere årsaker. NAV gjør oppmerksom på at det har skjedd regelverksendringer siden kartleggingen ble gjennomført som reduserer risikoen for svindel og som må tas i betraktning.	PROBA samfunnsanalyse (2011) og (2013)
Trygdesvindel Totalt anmeldt trygdesvindel	I 2018 ble det anmeldt trygdesvindel for **166 mill. kroner**. Det var 1020 saker. Av totalt antall anmeldelser gjelder 89 prosent av sakene svindel av dagpenger og AAP.	Kostnader relatert til ID er ikke spesifisert.	NAVs årsrapport (2018)
Trygdesvindel Feilutbetalinger på sykepengeområdet	I 2018 anslo Oslo Economics at omfanget av feilutbetalinger knyttet til sykepenger, som innebærer både bevisste handlinger (trygdesvindel) og ubevisste handlinger (bruker- eller prosessfeil), utgjør inkludert **mørketall mellom 150 og 550 mill. kroner årlig**.	Kostnader relatert til ID er ikke spesifisert, men en årsak til feilutbetaling av sykepenger er identitetsmisbruk, der identiteten til brukeren som mottar sykepenger ikke stemmer overens med oppgitt identitet ved sykmelding og søknad om sykepenger.	Oslo Economics (2018)
Trygdesvindel Analyse av omfanget av feilutbetalinger av dagpenger	I 2019 anslo Oslo Economics at det totale omfanget av feilutbetalinger av dagpenger er **mellom 0,8 og 1,9 mrd. kroner årlig**. Dette tilsvarer mellom 6 og 14 prosent av utbetalingene.	Kostnader relatert til ID er ikke spesifisert.	Oslo Economics (2019)
Annet Misbruk av ID-dokumenter 2018	Årlig rapport over misbruk av identitets- og underlagsdokumenter avdekket i 2012-2018. **Totalt ble det rapportert om 1 167 misbrukte dokumenter i 2018**. Antallet er det høyeste som noen gang er registrert, og utgjør en økning på over 50 prosent fra 2017. NID ser også en økning i antall imposter. Det var flest misbrukte dokumenter fra Irak, Hellas og Italia. Andelen av dokumenter fra land i EU/Schengen var 63 prosent, og det utgjør en betydelig økning fra 2017 hvor andelen lå på 40 prosent. Tyrkere utgjør den største nasjonaliteten som er rapportert å ha misbrukt ID-dokumenter i 2018, etterfulgt av irakere og syrere.	Kostnader relatert til ID er ikke spesifisert. NID gjør oppmerksom på at datagrunnlaget kan være mangelfullt. Det er ikke mulig å hente entydig statistikk fra STRASAK om saker som gjelder falsk identitet og misbruk av ID-dokumenter. Misbruk av ID-dokumenter kan være registrert med ulike koder, f.eks. uriktig forklaring, dokumentfalsk eller brudd på utlendingsloven.	NID (2019)

Tabell 18 Oppsummering av samfunnsmessige kostnader

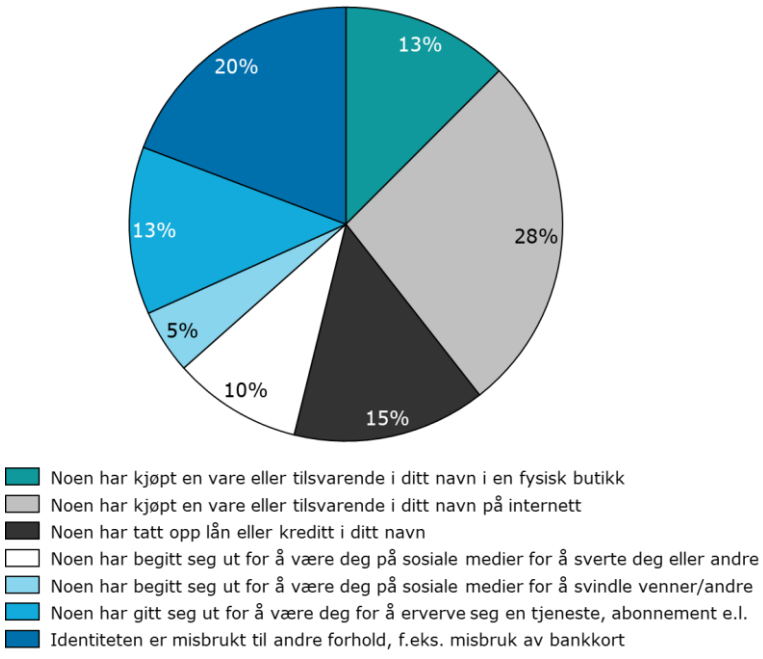
Konsekvenser for individet

Ifølge NorSIS har mer enn 150 000 nordmenn over 18 år opplevd misbruk av egen identitet de to siste årene.

Omfanget over identitetstyveri har vært stabilt mellom 3 og 4 prosent over tid. NorSIS har gjennomført undersøkelsen om identitetstyveri og sikring av identitet til befolkningen 18 år og eldre i Norge seks år rad: [400]

- *I 2018 oppgir 3,9 prosent at de har blitt utsatt for at noen andre har brukt deres identitet til å begå straffbare handlinger i løpet av de siste to årene*
- *Flere kvinner (4,7 prosent) enn menn (3,2 prosent) oppgir at de er blitt utsatt for det, men denne forskjellen er fortsatt liten*
- *Aldersgruppene som ser ut til å være mest utsatt er gruppen under 30 år (4,5 prosent) og mellom 30-44 år (5,6 prosent)*
- *Det er kun 38 prosent som oppgir at de har anmeldt forholdet. De som ikke anmelder oppgir ulike årsaker til det for eksempel at banken eller stedet hvor det inntraff fanget det opp, at man ikke tenkte på å anmelde det, led ikke økonomisk tap eller ble stoppet før det fikk andre konsekvenser*

Identitetstyveri kan være å få tilgang til offentlige tjenester og ytelser uberettiget eller kjøpe varer, åpne en bankkonto, registrere et abonnement, eller søke om lån ved å bruke en annens identitet.[401] Et ID-tyveri kan for eksempel skje ved at svindlere stjeler pass eller bankkort i posten, men den vanligste formen for misbruk er kjøp av varer på internett. På hvilken måte identiteter har blitt misbrukt fordeler seg som fremstilt i figuren nedenfor.



Figur 47 Ulike former for identitetsmisbruk (NorSIS, 2018)

[400] NorSIS, «ID-tyveri og sikkerhet for egen identitet», 2018
[401] Datatilsynet, «ID-tyveri», u.å.

Omfanget av ID-tyveri i en eller annen form er stort, og ifølge Datatilsynet synes det å ramme stadig flere. NorSIS skriver at det kan være kriminelle som ikke har noen relasjon til offeret, men også personer med nære relasjoner. Saker kan være svært belastende for enkeltpersoner og opprydding er ofte ressurskrevende. NorSIS peker på at økonomiske tap oftere går utover virksomheter som svindles gjennom ID-tyveri enn enkeltpersoner som utsettes for ID-tyveri. Flere opplever sosiale og psykiske utfordringer fordi de ikke lenger har kontroll over egen identitet.[402]

Ifølge Finans Norge er det en økende trend at ID-tyverier blir utført av personer i nære relasjoner ved at de får tilgang til ID-bevis og benytter disse til å tilegne seg økonomisk gevinst for eksempel ta opp lån. [403] Dette understøttes av Finanstilsynets ROS-analyse for 2018 hvor de skriver «*Misbruk av avtaleinngåelse gjennom digital signering (BankID) er ifølge foretakene økende, og skjer i særlig grad i nære relasjoner. Personer med nære relasjoner kan ha tilgang til hverandres BankID, og personer som ikke er datakyndige, blir hjulpet til å signere. Dette er utfordrende for foretakene å håndtere*».

Videre peker Finanstilsynet på at «*Den økte digitaliseringen har medført at foretakenes kunder har måttet ta i bruk digitale identifiserings- og autoriseringsløsninger. Dette gjør kunden sårbar og utgjør en betydelig risiko for misbruk, med i verste fall store økonomiske konsekvenser for den skadelidende.*»

BankID har et svært bredt bruksområde. Det er derfor knyttet en konsentrasjonsrisiko til misbruk av BankID, ved at misbruket kan oppstå innen mange områder, slik som inngåelse av kjøpekontrakter, tegning av forsikring, skatteopplysninger, låneavtaler m.m. Det 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. [404]

I tillegg til misbruk i nære relasjoner, trekker politiet frem at BankID brukes til svindel av personer med midlertidig opphold som for eksempel overlater BankID og annen personlig informasjon til andre, og i organisert arbeidsmarkedskriminalitet ved at for eksempel arbeidsgiver tar kontroll over ansattes BankID.

Leverandøren har vært i dialog med Finans Norge og utvalgte banker om data og statistikk på antall saker og økonomiske konsekvenser av misbruk av ID i nære relasjoner, men har ikke mottatt dokumentasjon på dette.

Politiet opplyser at ID kan være et sentralt moment i både enkle mengdesaker og som en del av kompleks kriminalitet. Et eksempel fra POD på en typisk mengdesak kan være bruk av falsk identitet ved salg av mobiltelefon på finn.no der selger mottar beløp, men ikke sender varen til mottaker. Eksempler på mer kompleks ID-kriminalitet kan være såkalt CEO-bedrageri hvor en person benytter falsk ID og sender et falskt fakturakrav og krever betalt for ikke utførte tjenester/salg av varer. Et annet eksempel er menneskehandelsaker der fornærmede har uavklart ID og oppholdsstatus i utlandet.

Politiet oppgir selv at de ikke har god statistikk på ID-kriminalitet da bruk av falsk ID ofte blir registrert som bedrageri og ikke identitetskrenkelse. Totalt ble det registrert 21 724 saker tilknyttet bedrageri og 3 610 saker tilknyttet identitetskrenkelse i 2018. Totalt antall anmeldte lovbrudd i 2018 var 318 566.[405]

[402] NorSIS, «Trusler og trender 2018-19», 2018
[403] Finans Norge, «ID-tyveri kan være ødeleggende», 2017. Dette fremheves også i intervjuer med nøkkelpersoner
[404] Finanstilsynet, «Risiko- og sårbarhetsanalyse (ROS) 2018», 2019
[405] Politiet, «STRASAK-rapporten 2018», 2018

6.1.6 Bruk av biometri i ID-forvaltningen

Biometriske kjennetegn kan beskrives som kjennetegn som utgår fra kroppen, som er unike for deg som enkeltperson og samtidig permanente eller stabile over tid.[406] Biometrisk teknologi kan bidra til å verifisere og identifisere personer og benyttes bredt av både av private og offentlige aktører.[407] Eksempler på dette kan være ansikts- og fingeravtrykksgjenkjenning brukt til å verifisere/autentisere eieren av en smarttelefonen, eller ansiktsfoto og fingeravtrykk avlagt i forbindelse med passutstedelse. I en undersøkelse gjennomført av NorSIS svarte 72 prosent at de var positive til å benytte biometri som for eksempel fingeravtrykk til å bekrefte identitet som norsk innbygger. NorSIS oppgir at dette er noe lavere enn tidligere år og at det særlig er kvinnene som har bidratt til denne nedgangen. [408]

Biometri er et viktig virkemiddel i arbeidet med å avklare en persons identitet og er et tiltak som har blitt tatt i bruk på migrasjonsområdet og til kriminalitetsbekjempelse i flere land. I Norge brukes biometri av det offentlige i forholdsvis begrenset grad og spørsmål knyttet til personvern står sentralt. Av gjennomførte intervjuer og samtaler oppgis det av flere å være rom for å utnytte biometri i større grad, blant annet med bedre utnyttelse av eksisterende databaser, større grad av sentrallagring av biometri og bedre opplæring i opptak, lagring og søk i biometriske registre. I et fremtidig perspektiv kan man tenke seg brukerstyrt deling av biometri for mer effektiv og brukervennlig tjenesteytelse. Brukere kan selv styre om og hvilke offentlige aktører som får tilgang til egen biometri.

Opptak og anvendelse av biometri er et sentralt element i ID-forvaltningen og er helt avgjørende for grad av kvalitet og sikkerhet i verifiserings- og identifiseringsarbeidet.

Biometri og grunnidentitet

Det finnes to hovedkategorier biometriske teknologier. Den første kategorien er basert på anatomiske eller fysiologiske karakteristikker, eksempelvis gjenkjenning av fingeravtrykk, ansikt, iris og håndgeometri. Den andre kategorien er adferdsbasert, hvor teknologien måler adferd som inkluderer gjenkjenning av for eksempel håndskrift, tastedynamikk og ganglag.[409] Hva gjelder biometri og grunnidentitet er det i hovedsak anatomiske og fysiologiske karakteristikker som benyttes i ID-forvaltningen i Norge og i mindre grad adferdsbasert karakteristikker.

Leverandøren er kjent med at det i Norge ikke er etablert en sikker grunnidentitet da registrering i Folkeregisteret ikke innebærer registrering av biometri for å sikre enhetlig identifikasjon. Dermed er det mulig for en person å ha flere identiteter oppført i Folkeregisteret[410] og det er mulig for personen å utgi seg for å være ulike personer ved utstedelse av pass, førerkort, opprettelse av bankkonto eller urettmessig motta offentlige tjenester og ytelser. Leverandøren er videre kjent med at Skatteetaten mener det er sannsynlig at det er oppført et stort antall uriktige identiteter i Folkeregisteret.

Automated Biometric Identification System (ABIS) har som beskrevet i kapittel 3.1.4 funksjonalitet for søk på tvers av registre. Dette benyttes ikke i dag, da det ikke er

[406] Datatilsynet, «Biometri», u.å.
[407] NID, «Biometri og identitet – Utfordringer og nye muligheter for utlendingsforvaltningen», 2013
[408] NorSIS, «ID-tyveri og sikkerhet for egen identitet», 2018. Spørsmål: *Passord, pinkoder og biometri er eksempler på bekreftelse av identitet. Dette sikrer at kun du som rettmessig innehaver får tilgang til de tjenester og fordeler som følger av din rolle som norsk innbygger. Eks. Innlogging minibank, Altinn og andre tjenester som inneholder personinformasjon samt opprettelse av kundeforhold. Er du positiv eller negativ til å benytte biometri som for eksempel fingeravtrykk for å bekrefte din identitet*? (alternativer: Positiv / Negativ / Verken positiv eller negativ / Ikke sikker)
[409] NID, «Biometri og identitet – Utfordringer og nye muligheter for utlendingsforvaltningen», 2013
[410] POD, «UNIK-utredning», 2017

teknisk mulig å gjennomføre søk på tvers før nye pass og ID-kort lanseres med tilhørende nødvendig hjemmelsgrunnlag.

Flere faktorer kan påvirke kvaliteten på søk med biometri. Type biometri som opptas, og kvaliteten på denne, er avgjørende for hvor sikkert og godt søkeresultatet blir. Om to fingeravtrykk med god kvalitet sammenlignes er dette nært optimalt og gir et resultat som ikke kan trekkes i tvil. Et ansiktsfoto av god kvalitet kan være bedre egnet til å gjennomføre søk sammenlignet med et fingeravtrykk av dårlig kvalitet, men generelt er fingeravtrykk mer egnet til å gi presise treff enn ansiktsfoto. Det optimale er å ha kombinasjon av både fingeravtrykk og ansiktsfoto.[411] Historisk har ansiktsfoto opptatt i sammenheng med passutstedelse kun vært et foto, og ikke et foto med biometrisk personinformasjon. Som en del av utrullingen av nye biometrikiosker vil passfoto fremover inkludere denne teknologien. For passbilder tatt før denne utrullingen vil det være mulig å konvertere eksisterende foto og tillegge disse biometrisk personinformasjon som grunnlag for søk i biometriske algoritmer.

Biometri knyttet til kvalitetsindikatoren «unik»

Som beskrevet i del 1 foreligger en rekke endringer og tilpasninger knyttet til opptak, lagring og bruk av biometri. Forslag og vedtak til endringer innebærer utvidet bruk av biometri i utlendingsforvaltningen, gjennomføring av biometriske en-til-mange sammenligningssøk ved utstedelse av pass og nasjonale ID-kort og lovforslag om lagring av fingeravtrykk i pass- og ID-kortregistrene som tilrettelegger for status «unik» i Folkeregisteret.

Biometri er nøkkel i modernisering av Folkeregisteret med tanke på etablering av kvalitetsindikatoren «unik». Det er en forutsetning for status «unik» at alle personer som er registrert med identitetsnummer i Folkeregisteret (fødselsnummer eller d-nummer) også er registrert i ett av biometriregistrene. Å tilrettelegge for status «unik» i Folkeregisteret er et oppdrag POD, UDI og SKD har blitt gitt av JD. Aktørene har utredet hva som må til for å oppnå målsetningen om å overføre «unik» identitet fra biometriregistrene i justissektoren til Folkeregisteret. Det er identifisert flere tiltak som må gjennomføres for at UDI og POD skal overlevere melding om «unik» til Folkeregisteret.

- Tekniske tilpasninger i ABIS og nytt hjemmelsgrunnlag for å muliggjøre en-til-mange søk på tvers av utlendingsregisteret og pass- og ID-kortregisteret
- Øke kvaliteten på søkene med å ta i bruk en algoritme for søk på tvers i ansiktsfoto, samt åpne for lagring og søk med fingeravtrykk ved søknad om pass og nasjonalt ID-kort, tilsvarende som for tredjelandsborgere, for å ytterligere styrke og effektivisere kontrollen
- Styrke fagmiljøet i Kripos som håndterer tvilstilfeller ved biometriske søk og større kapasitet på manuell saksbehandling
- Sette kvalitetskrav til søk på tvers

Opptak av biometri og søk mellom biometriregistre vil gjøre det mulig å merke identiteten i Folkeregisteret som «unik». Dette vil i betydelig grad øke kvaliteten og sikkerheten på identitetsopplysningene i Folkeregisteret.

[411] POD, «UNIK-utredning», 2017

Biometri og personvern

Personvernhensyn står sentralt når det kommer til opptak, lagring og anvendelse av biometri. I motsetning til tidligere er biometriske opplysninger etter den nye personopplysningsloven nå en særlig kategori personopplysninger.[412] Når det gjelder personopplysningsloven og prinsippene som ligger bak den, er det særlig kravene om nødvendighet, formålsbestemthet, forholdsmessighet og dataminimalitet som er relevante å vurdere.[413]

- **Nødvendighet:** Behandlingen av personopplysninger må være nødvendig for å oppnå et mål. Det er bare nødvendig hvis man ikke kan oppnå det samme målet på annet vis

- **Formålsbestemthet**: Personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene

- **Forholdsmessighet**: I den grad det skal gjennomføres tiltak som innebærer inngrep i personvernet skal tiltaket ikke være mer inngripende enn det som er nødvendig for å oppnå formålet med tiltaket

- **Dataminimalitet**: Opplysningene skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for

Disse prinsippene vurderes relevante for all opptak, lagring og anvendelse av biometri innenfor ID-forvaltningen.

Forskjellige innganger til biometriregistrering i Norge

Avhengig av hvilken brukergruppe en person tilhører varierer det i hvilken grad det registreres biometri av vedkommende:

- For **norske statsborgere** opptas biometri i form av ansiktsfoto og fingeravtrykk for de som søker og får innvilget pass. Ansiktsfoto lagres i et sentralt passregister, mens fingeravtrykk blir lagret i inntil 30 dager før sletting.[414] Et bilde av fingeravtrykkene lagres i passets elektroniske brikke og blir deretter slettet fra saksbehandlingssystemet og opptaksutstyret for biometri.[415] Lagring av biometri er regulert i passloven med forskrift

- For **tredjelandsborgere** opptas det ansiktsfoto i alle oppholds-, visum[416]- og asylsaker. Her lagres ansiktsfoto i utlendingsdatabasen og tilgjengeliggjøres utlendingsforvaltningen gjennom blant annet saksbehandlingssystemene DUF, UTSYS og Norvis. Fingeravtrykk tas i alle asyl- og visumsaker. I asylsaker lagres fingeravtrykket i politiets utlendingsregister[417], mens det i visumsaker lagres i sentral VIS database. For oppholdssaker tas det kun fingeravtrykk til politiets utlendingsregister i de tilfeller hvor det søkes oppholdstillatelse som familiemedlem til utlending som har søkt asyl i utlendingsregisteret. [418] Likevel

[412] Det kreves et særskilt behandlingsgrunnlag for å kunne behandle særlige kategorier personopplysninger, se nærmere personvernforordningen art. 9
[413] Utredning knytning mellom Folkeregisteret og biometri i passregisteret, nasjonalt ID-kort register og utlendingsregisteret, 2016
[414] POD, «Rundskriv – Retningslinjer for passmyndighetenes behandling av saker ihht passloven m/forskrifter», 2015
[415] POD, «UNIK-utredning», 2017
[416] Enkelte land utenfor EU/EØS har avtale med Norge og kan reise til landet visumfritt. UDI spesifiserer hvilke land dette gjelder for på sine hjemmesider
[417] Basert på epostkorrespondanse med PU
[418] JD, «Høring om forslag til endringer i utlendingsloven m.m. om opptak og lagring av biometri i utlendingssaker», 2019

er det et poeng at alle som får innvilget oppholdstillatelse skal ha et oppholdskort. Her tas fingerbiometrien på samme måte som for norske pass og lagres dermed kun i oppholdskortets elektroniske brikke. Lagring av biometri er regulert av utlendingsloven §100 og utlendingsforskriften §18-1. Det pågår et arbeid med å opprette et eget fotoregister for utlendingsregisteret i ABIS hvor asyl, opphold og visumsaker vil samles (ref. kap 2.8.2)

- For **EØS-borgere** opptas det per i dag ikke biometri i norske biometriregistre (verken ansiktsfoto eller fingeravtrykk)

	Norske statsborgere	EØS-borgere	Tredjelandsborgere (asyl, opphold, visum)
Opptak av biometri	Ansiktsfoto og fingeravtrykk opptas ved passutstedelse	Biometri avlegges ikke i norske biometriregistre	Ansiktsfoto og fingeravtrykk registreres av PU, politiet, og Utenriksstasjonene avhengig av sakstype
Lagring av biometri	Ansiktsfoto lagres passregisteret (ABIS) Fingeravtrykk lagres kun i passet	Biometri avlegges ikke i norske biometriregistre	Ansiktsfoto lagres i UDB. Lagring av fingeravtrykk avhenger av sakstype.
Hvor lenge lagres biometri	Ansiktsbiometri slettes ikke Fingeravtrykk varer like lenge som passet	Biometri avlegges ikke i norske biometriregistre	Ansiktsbiometri slettes ikke Ulike sletterutiner for fingeravtrykk. Avhenger av oppholdsstatusen til tredjelandsborgeren.

Tabell 19 Opptak og lagring av biometrisk personinformasjon per brukergruppe (obs: for tredjelandsborgere vil ansiktsfoto lagres i utlendingsregisteret fra november 2019)[419]

6.2 Funn og vurderinger

Under følger leverandørens vurderinger av nåsituasjonen innen kvalitet og sikkerhet i ID-forvaltningen. Helhetlige vurderinger foretas av leverandøren i del 3 av rapporten.

Leverandøren har valgt å klassifisere enkelte av funnene og vurderingene knyttet til kvalitet og sikkerhet som «sikkerhetshull». Der dette gjelder fremkommer det tydelig av overskriften. De øvrige funn og vurderingene knyttet til kvalitet og sikkerhet er av mer generell art.

6.2.1 Sikkerhetshull: Et høyt antall rekvirenter med manglende felles rutiner, delt ansvarliggjøring og varierende grad av ID-kontroll kan føre til uriktig tildeling av d-nummer som kan gi store følgefeil i ID-forvaltningen

Som påpekt av leverandøren i kapittel 6.1.2 er det mange virksomheter som har myndighet til å rekvirere d-nummer. Per i dag eksisterer det ingen helhetlig rutine for rekvirering som gjelder for alle aktører selv om oppgaven i utgangspunktet er lik.

[419] Basert på Skatteetaten, «Utredning - Knytning mellom Folkeregistret og biometri i passregisteret, Nasjonalt ID-kortregister og Utlendingsregisteret», 2016 og JD,» Høring om forslag til endringer i utlendingsloven m.m. om opptak og lagring av biometri i utlendingssaker», 2019 og epostkorrespondanse med PU

Leverandøren vurderer at kvaliteten og sikkerheten i rekvireringsprosessen varierer basert på hvilken aktør som gjennomfører rekvireringen og i hvilken grad det begrunnende behovet for d-nummer vurderes av rekvirenten og den enkelte ansatte før det tildeles et d-nummer. Det er leverandørens oppfatning at samtlige aktører opplever at de selv gjør en god jobb med tanke på d-nummerrekvirering, men at forskjellene i rutinene sier noe annet.

Leverandøren vurderer videre at det er uklarheter mellom folkeregistermyndigheten og d-nummerrekvirentene når det gjelder samhandling og rolleforståelse. Ytterligere uklarheter oppstår da Skatteetaten tilrår «kontrollert», men hver etat gjør en risikovurdering på om det skal kreves for deres respektive tjenester. Dette fører til dårligere kvalitet og sikkerhet i rekvireringsprosessen som helhet.

Videre er det leverandørens vurdering at det er manglende insentiver og hjemler hos rekvirentene til å *kreve* status «kontrollert» på d-nummer for å få tilgang til deres tjenester. Dette fører til at det rekvireres et unødvendig høyt antall d-nummer som blir stående med status «ikke-kontrollert» i Folkeregisteret. Dette d-nummeret kan personen bruke videre til andre tjenester.

Dette støttes også i dokumentasjon leverandøren har fått innsyn i.

6.2.2 Sikkerhetshull: Dublerte identitetsnummer i Folkeregisteret gjør det mulig å operere med mer enn en identitet i Norge

Leverandøren vurderer dublerte identitetsnummer (både fødselsnummer og d-nummer) i Folkeregisteret å være en sentral sikkerhetsrisiko i ID-forvaltningen. Folkeregisteret er på mange måter navet i ID-forvaltningen og opplysningene her legges til grunn i nærmest all personrelatert forvaltning og medfører dermed følgefeil for den øvrige ID-forvaltningen ved feil.

Rekvirentene er ikke tilstrekkelig klare over de store konsekvensene det kan ha om identitetsnummer rekvireres unødvendig og til personer med falske identiteter eller identitetsdokumenter. Rekvirentene mangler også en bevisst tilnærming til å stille krav om «kontrollert» versus «ikke-kontrollert» identitet ved tilgang til offentlige tjenester. Leverandøren vurderer at effektivitet og service til brukerne tillegges større vekt enn risikoen for at en person med falske ID-dokumenter får tildelt identitetsnummer. Det overnevnte understøttes av dokumentasjon leverandøren har fått innsyn i.

Utfordringen er sentral for alle tjenesteeiere som baserer seg på digitale eller fysiske ID-bevis. Det kan spesielt trekkes frem at dupliserte d-nummer kan utgjøre en ekstra risiko i forbindelse med å få tilgang på eID som utelukkende legger d-nummer til grunn for utstedelse slik MinID gjør.

6.2.3 Sikkerhetshull: Kompetansen tilknyttet utstedelse, fornyelse og tap av ID-bevis varierer både mellom virksomhetene og innad i den enkelte virksomhet

Det er forskjell på krav til kompetanse mellom virksomhetene som utsteder ID-bevis, og det eksisterer ingen felles standarder for krav til kvalitet og kompetanse på tvers av sektorer. Enkelte ID-kontroller gjennomføres med lavere kvalitet og dersom denne ID-kontrollen ligger til grunn ved neste ID-kontroll utgjør dette en risiko for følgefeil.

Det er leverandørens vurdering at det er ulikt kompetansenivå også innad i den enkelte virksomhet, og et eksempel her er politidistriktene, som beskrevet i kapittel 6.1.3.

Dette kan være en naturlig konsekvens av varierende saksvolum og -kompleksitet, men utgjør likefult en sikkerhetsrisiko.

Dette poenget understøttes ved at flere aktører leverandøren har gjennomført samtaler med påpeker at det mangler kompetanse på ID innad i virksomhetene, spesielt når det kommer til håndtering av falske fysiske ID-bevis. Leverandøren vurderer det som positivt at politiet oppgir at det jobbes med kompetanseheving, og at flere aktører påpeker at kompetansen har blitt bedre grunnet økt fokus på ID-relaterte problemstillinger.

6.2.4 Sikkerhetshull: Manglende eller svak ID-kontroll i forbindelse med utstedelse av eID gir potensial for misbruk i stor skala

Leverandøren vurderer at omfanget av misbruk kan være større om en person har fått utstedt et eID-bevis på grunnlag av svak/ingen ID-kontroll, sammenlignet med fysiske ID-bevis. Elektroniske ID-bevis er lett å bruke mot mange tjenesteytere på nett på kort tid og er samtidig upersonlig i form av at misbrukeren kan sitte bak en skjerm uten å være i kontakt med en fysisk kontrollør. Det vurderes at terskelen for å utnytte elektroniske ID-bevis er lavere enn for fysiske ID-bevis.

6.2.5 Sikkerhetshull: ID-bevis kan brukes som en døråpner til nye og sterkere ID-bevis og for å motta offentlige tjenester og ytelser, noe som utgjør et betydelig sikkerhetshull i ID-forvaltningen

I kapittel 5.1.3 ble det illustrert figurer som viste at kravene til gyldig legitimasjon for å få utstedt nye ID-bevis og for å få tilgang til offentlige tjenester og ytelser varierer. Flere ID-bevis utstedt på bakgrunn av en mindre sterk ID-kontroll fungerer som gyldig ID-bevis for å få utstedt andre og sterkere ID-bevis. Eksempelvis kan både bankkort og førerkort brukes for å få utstedt pass når statsborgerskap og identitet er godtgjort. Disse ID-bevisene kan igjen brukes videre for å få tilgang til og motta offentlige tjenester og ytelser, og også i disse tilfellene stilles det ulike krav til hva som anses å være gyldig ID-bevis.

6.2.6 Sikkerhetshull: Aktører som mangler kunnskap og hjemler til å identifisere og beslaglegge falsk ID forventes å opptre som «kontrollinstitusjoner»

Kontrollinstitusjoner innen justissektoren, spesielt politiet, er forventet å gjennomføre kontroll av ID-bevis med høy kompetanse og har i tillegg hjemler til å beslaglegge falske ID-bevis.

Mange virksomheter som ikke er en del av justissektoren forventes også å gjennomføre kontroll av ID-bevis ved fysisk oppmøte som en del av sitt virksomhetsområde. Eksempler på dette kan være at SVV gjennomfører kontroll ved utstedelse av førerkort eller at banker gjennomfører kontroll ved opprettelsen av et kundeforhold. Krav eller forventning om fremleggelse av en eller annen form for legitimasjon er også vanlig tilknyttet ulike offentlige tjenester og ytelser. Ansatte i virksomhetene er her forventet å gjennomføre kontroll av ID-bevis med tilstrekkelig kvalitet uten at de nødvendigvis

har opplæring på området eller hjemmel[420] til å beslaglegge falske ID-bevis om det avdekkes.

Med lav kompetanse på kontroll av ID-bevis og begrenset mulighet til å agere dersom kontrollen avdekker falsk ID utgjør dette betydelig sikkerhetshull og en risiko for at falske ID-bevis fortsetter å sirkulere i samfunnet, selv etter oppdagelse. Leverandøren er gjort oppmerksom på frustrasjon hos flere aktører i ID-forvaltningen som opplever at personer får ta med seg falsk ID og prøve på nytt andre steder ettersom det er begrenset mulighet for beslaglegning.

6.2.7 Generelt har kvaliteten og sikkerheten i ID-forvaltningen bedret seg de siste årene med økt fokus på ID-relaterte problemstillinger og oppbygging av kompetansemiljøer

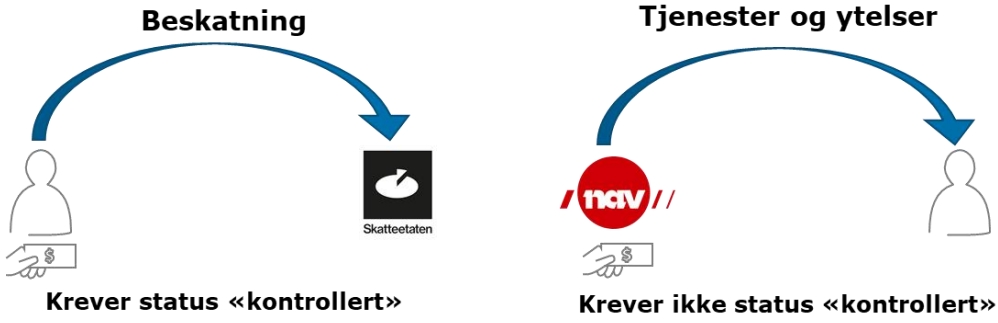
Leverandøren vurderer at økt fokus og kompetanse på ID og områder tilknyttet ID over tid har hevet kvaliteten og sikkerheten i ID-forvaltningen. ID-forvaltningen har økt i kompleksitet, og det har derfor vært behov for kompetanseheving som følger utviklingen og trender på området. Sterke kompetansemiljøer i form av blant annet NID og Kripos har bidratt og bidrar med generelle kompetanseløft i ID-forvaltningen. Leverandøren vurderer også at arbeid med ID-relaterte oppgaver har fått økt anerkjennelse sammenlignet med tidligere. Foreslåtte tiltak fra rapporter og dokumentasjon[421] som har blitt igangsatt, samt løpende igangsettelser, har bidratt og bidrar til at sikkerhetsavvik tilknyttet ID-området lukkes helt eller delvis. Eksempler på dette er jobben som er gjort med å lukke merknader i Riksrevisjonens rapport for budsjettåret 2014[422], sentralisering av ID-kontroll hos Skatteetaten, regelverksendringer og igangsetting av moderniseringsprogrammer.

6.2.8 ID-forvaltningen har strengere kontrollkrav til personer som skal innbetale skatt, enn personer som skal motta tjenester og ytelser fra det offentlige

Både Skatteetaten og NAV rekvirerer d-nummer, men kun Skatteetaten setter krav til «kontrollert» for bruk av deres tjenester (ref. kapittel 6.1.2). NAV og øvrige rekvirenter oppfordrer til status «kontrollert», men setter ikke selv noen krav til det i sin saksbehandling.

På bakgrunn av denne praksisen kan det hevdes at staten krever en høyere grad av sikkerhet i form av å kontrollere riktig identitet forbundet med å sikre statens inntektsgrunnlag (skatt) sammenlignet med deler av statens utgifter (tjenester og ytelser). Fra et finansperspektiv kan det hevdes at det er mer fokus på å sikre topplinjen enn bunnlinjen. Dette er fremstilt i figuren nedenfor.

[420] Ansatte i virksomhetene har mulighet til å gjennomføre sivilt beslag etter straffeprosessloven § 206 første ledd andre punktum: «beslag kan tas enhver når den mistenkte treffes eller forfølges på fersk gjerning eller ferske spor.» [420], men i hvor stor grad dette brukes er usikkert
[421] Eksempelvis «Handlingsplan for ID-området» 2012 av POD
[422] Politiet oppdaterer med status på dette arbeidet i sin årsrapport



Figur 48 Forenklet illustrasjon av dagens praksis ved ID-kontroll av rekvirerte d-nummer

Leverandøren er gjort kjent med det store flertallet av NAVs d-nummer rekvireres på vegne av personer som oppholder seg i utlandet (estimert til 97 prosent)[423] og at det er særlig utfordrende å gjennomføre ID-kontroll på denne gruppen. Denne problemstillingen er relevant også for flere av rekvirentene.

Det er etter leverandørens syn likevel ikke et tilstrekkelig rasjonale for kun å kreve «kontrollert» d-nummer av skattehensyn, og ikke for mottak av tjenester og ytelser. Basert på det er det leverandørens vurdering at det burde være en mer ensartet praksis og likebehandling.

6.2.9 Moderniseringen av Folkeregisteret innebærer flere forbedringstiltak som forventes å gagne ID-forvaltningen i stort

Moderniseringen av Folkeregisteret innebærer flere forbedringstiltak, og spesielt muligheten til å markere personer som har møtt opp til fysisk kontroll (status «kontrollert» og status «ikke-kontrollert») og personer som har fått kontrollert identiteten med søk på tvers av biometriregistrene (status «unik»). Dette tiltaket legger godt til rette for knytning av biometri og gir sikkerhetsgevinster ved gjennomføring, samt potensielle effektiviserings- og brukergevinster.

Videre oppleves det som en hensiktsmessig arbeidsdeling på tvers av sektorgrensene at Skatteetaten gjenbruker ID-kontrollen gjennomført av politidistriktenes utlendingsforvaltning for status «kontrollert» på tredjelandsborgere.

6.2.10 Fastsatt identitet er nødvendig for å delta i det norske samfunnet, og graden av ID-kontroll som gjøres i denne forbindelse varierer sterkt mellom brukergruppene

For å delta i et samfunn kreves det at et individs identitet er fastsatt. Prosessen for å fastsette identiteten varierer i stor grad avhengig av hvilken brukergruppe man tilhører. For norske statsborgere gjennomføres det i praksis ikke noen form for ID-kontroll i forbindelse med fastsettelse. Det samme gjelder til en viss grad for EØS-borgere da de kan reise fritt i Schengen og ID-kontrollen gjennomført i Norge baserer seg på ID-bevis utstedt i hjemlandet. For tredjelandsborgere, og da spesielt asylsøkere, er situasjonen annerledes. Kontrollen her er i større grad knyttet til å fastsette identitet, ettersom det store flertallet asylsøkere kommer til landet uten ID-bevis. Utlendingsmyndighetene opererer her med sannsynlighetsovervekt for identitet og denne vurderingen kan være svært krevende.

[423] NAV har i møter med leverandøren oppgitt at ca. 970 av totalt 38 838 d-nummer rekvireringer fra kom fra personer som oppholdt seg utenfor Norge

Fra et kvalitet- og sikkerhetsperspektiv vurdere leverandøren at det er en utfordring at det ikke eksisterer en harmonisert tilnærming til hvilke ID-bevis som skal ligge til grunn for kontroll i ID-forvaltningen. Personer i utlendingsforvaltningen oppgir som et eksempel at UDI kan godkjenne ett underlagsdokument, mens Skatteetaten ikke godkjenner samme dokument. Selv i UDI er det ulik praksis for godkjente dokumenter avhengig av hvilken avdeling du jobber i. I disse tilfellene ender man opp med at enkelte ambassaders praksis eller enkeltuttalelser blir lagt til grunn. Med en slik inngang blir det utfordrende for andre aktører å gjenbruke ID-kontrollen.

Det er leverandørens vurdering at aktørene på utlendingsfeltet har et bevisst forhold til identitetsfastsettelsen på utlendingsfeltet, men i noe mindre grad er klar over følgene av en feil fastsatt ID, samt hvor komplekst det er å rette opp i dette på tvers av systemene i ID-forvaltningen.

6.2.11 Det er ikke i tilstrekkelig grad lagt til rette for bruk av biometri på tvers av brukergrupper i ID-forvaltningen

Biometri opptas av norske statsborgere i forbindelse med utstedelse av pass og av asylsøkere i forbindelse med ankomstregistrering. Dagens praksis er at det kun tas ansiktsfoto av oppholds- og visumsøkere, mens det for EØS-borgere ikke tas noen form for biometri. Dette til tross for at flere tjenesteytere mener EØS-borgere er den største brukergruppen og kilden til misbruk av offentlige tjenester og ytelser (se kapittel 6.1.5). Det foreligger ikke noen tall på hvor mange EØS-borgere som urettmessig mottar tjenester og ytelser fra det offentlige, men flere tjenesteytere påpeker at de antar det er store mørketall.

For å sikre *en person, en identitet* i Norge og dermed redusere handlingsrommet for de som urettmessig mottar tjenester og ytelser oppgir flere aktører biometri som et viktig virkemiddel. Leverandøren er positiv til at UDI i løpet av oktober 2019 vil få på plass opptak av fingeravtrykk i tillegg til ansiktsfoto for alle tredjelandsborgere (som omtalt i kapittel 2.9.4).

6.2.12 Biometri er et komplekst fagfelt der personvernutfordringene vektlegges mer enn personverngevinstene

Det er mange uavklarte forhold relatert til biometri og disse strekker seg fra overordnede føringer til detaljerte forhold knyttet hvem det skal opptas biometri for, type biometri og til hvilket formål biometrien skal brukes. I tillegg er det en rekke kompliserende faktorer knyttet til både norske og utenlandske regelverk som ID-forvaltningen må forholde seg til.[424] Dette, sammen med personvern gjør biometri til et område som er komplekst å navigere.

Det er leverandørens inntrykk at personvern i stor grad brukes som et argument mot bruk av biometri og at personvernutfordringer vektlegges tyngre enn personverngevinstene. Opptak av biometri styrker ID-sikkerheten og legger til rette for *en person, en identitet i Norge*. For borgeren vil en sikrere identitet styrke personvernet og gjøre det vanskeligere for andre å utgi seg for å være borgeren. Personvern er et sentralt drøftingstema når det kommer til ID-forvaltning og det er viktig at både styrkene og svakhetene relatert til biometri fremkommer i denne diskusjonen.

[424] Som eksempel nevnes Utlendingsloven og EØS-regelverket

6.2.13 Samfunnsmessige kostnader og konsekvenser vurderes å være betydelig høyere enn reelt dokumentert feil og misbruk av ID

Som påpekt i kapittel 6.1.5 viser kartleggingen leverandøren har gjort i forbindelse med feil og misbruk av ID at det finnes svært lite dokumentert informasjon på området. Leverandøren vurderer det som utfordrende å kvantifisere de samfunnsmessige konsekvensene ved feil og misbruk basert på tilgjengelig datagrunnlag. Det eksisterer begrenset dokumentasjonen, men etter leverandørens syn er det store avvik mellom avdekte saker og mørketall dokumentert i ulike rapporter.

Videre kan det til dels ikke dokumenteres om forebyggende tiltak som gjennomføres, er tilstrekkelig målrettet og, gir nødvendig effekt når det mangler statistikk på området. Det er utfordrende for ID-forvaltningen at det i liten grad eksisterer statistikk over ID-kriminalitet. ID som kriminalitetsform har en gjenstridighet i seg: den spenner over organisatoriske grenser, myndighetenes forvaltningsområder og hierarkiske nivåer i staten.[425]

6.2.14 Manglende kostnadsbilde tilknyttet feil og misbruk av ID kan føre til at andre politikkområder blir prioritert foran ID-området

Leverandøren vurderer at begrenset kostnadsdokumentasjon tilknyttet feil og misbruk av ID fører til at ID-forvaltningen i visse tilfeller nedprioriteres foran andre områder der det foreligger bedre dokumentasjon. Det kan i større grad sås tvil om ringvirkningene av kriminalitetsutfordringene tilknyttet feil og misbruk av identiteter og ID-bevis når dette ikke kan tallfestes og man møter andre politikkområders interesser.

Leverandøren vurderer videre at ID-forvaltningen historisk sett har manglet prioritering opp mot andre områder og at området er grenseoverskridende og «faller mellom flere stoler». Dette kan være medvirkende årsaker til manglende statistikk på området.

[425] Fimreite m.fl., "Organisering, samfunnssikkerhet og krisehåndtering", 2011. Difi, 2014. "Mot alle odds? Veier til samordning i norsk forvaltning"

7 Ressursbruk og kostnader i ID-forvaltningen

I dette kapittelet gis en beskrivelse av nåsituasjonen (kapittel 7.1) og leverandørens nåsituasjonsvurdering (kapittel 7.2) for ressursbruken i ID-forvaltningen. Kapittelet gir en oversikt over ressursbruken i de ulike departement samlet sett og hos de ulike aktørene i ID-forvaltningen, utvikling over tid, samt analyser og vurderinger av kostnadseffektivitet på tvers av departementer og underliggende aktører i ID-forvaltningen.

7.1 Nåsituasjonen

Leverandøren har ikke blitt opplyst om eller blitt gjort oppmerksom på at det eksisterer statistikk, nøkkeltall eller rapporter som helhetlig dokumenter ressursbruk og kostnader ved ID-forvaltningen samlet sett. Ressursbruk på ID-relaterte aktiviteter er også relativt lite belyst i tidligere rapporter og analyser slik leverandøren har fått dette forelagt. Kostnader ved ID-forvaltningen er i liten grad direkte tilgjengelig for de fleste aktørene i ID-forvaltningen, med noen få unntak. Dette kan forklares av at ID-relatert arbeid hos de fleste aktører inngår som en integrert del av andre arbeidsoppgaver, og kostnaden eller tiden knyttet til ID-relatert arbeid benyttes i liten grad i styringen. Dette er også nærmere beskrevet i kapittel 3.2.2 og 3.2.3. Derfor er ikke informasjon om kostnader ved ID-forvaltningen direkte tilgjengelig i for eksempel aktørenes regnskapsførings- eller timeregistreringssystemer.

For å kartlegge ressursbruken i ID-forvaltningen ble det distribuert en standardisert dataforespørsel om ressursbruk til 14 aktører. Dette samsvarer med de 13 primæraktørene beskrevet i kapittel 2.5, med unntak av banker, samt Brønnøysundregistrene og NID. Leverandøren har vært i samtaler med et utvalg store norske banker i forbindelse med datainnhentingen, og samtalene indikerer en betydelig ressursbruk relatert til bankkort med bilde og eID. Grunnet vektlegging i områdegjennomgangen og datatilgjengelighet fokuserer kapittelet på ressursbruken i offentlige virksomheter og ressursbruk tilknyttet ID-relaterte aktiviteter i bankene er dermed ikke inkludert kapittelets figurer.

I dataforespørselen ble aktørene bedt om å spesifisere ressursbruken for tre ulike tidspunkt; historisk ressursbruk 2015, nåværende ressursbruk 2018 og fremtidig ressursbruk 2021, fordelt på antall årsverk og løpende kostnader tilknyttet ID-forvaltning. Dette ble gjort for å kunne sammenligne utviklingen i ressursbruk over tid. Leverandøren forankret datainnsamlingstilnærming med de antatt største aktørene i ID-forvaltningen i forkant av utsendelse av dataforespørselen, og aktørene ble bedt om å spesifisere egne kostnader tilknyttet ID-forvaltning for å sikre at dataforespørselen dekket de viktigste kostnadselementene. Aktørene ble også bedt om å fordele ressursbruk på ulike ID-relaterte aktiviteter, i samsvar med prosess fra fastsetting til ID-kontroll beskrevet i kapittel 2.4. I tillegg ble aktørene spurt om å spesifisere andel utstedte av ID-bevis og andel behandlede ID-saker for de tre brukergruppene spesifisert i kapittel 2.6. Alle aktørene ble forespurt om løpende ID-relaterte kostnader, det vil si kostnader til personell, drift og forvaltning inklusive lokalkostnader, eventuelle produksjons- og distribusjonskostnader tilknyttet ID-bevis, samt eventuelle investeringskostnader. I vedlegg 10 er det nærmere beskrevet hvilke kostnader som er inkludert per aktør. Samtlige aktører ble stilt en rekke oppfølgingsspørsmål for kvalitetssikring av datagrunnlaget. Leverandøren har imidlertid prioritert oppfølging av de største aktørene innen ID-forvaltningen da datagrunnlaget for disse aktørene er mer komplekst enn for de mindre aktørene. Figurene i kapittelet viser samlede kostnader om ikke annet er spesifisert.

Leverandøren har ikke mottatt data fra POD på ressursbruken tilknyttet ID-relatert arbeid i politidistriktenes førstelinje i forbindelse med utlendingsforvaltningen eller ressursbruken tilknyttet ID-kontroller som er en del av politiets øvrige oppgaveutførelse. POD begrunner dette med at det er stor variasjon i oppgavene som utføres i førstelinjen i utlendingsforvaltningen, slik at det ikke er mulig å gi kvalitetssikrede estimater på den totale ressursbruken tilknyttet arbeidet som utføres. ID-kontrollene i politiets øvrige oppgaveutførelse er ifølge POD så tett knyttet sammen med andre oppgaver at det ikke er mulig å utarbeide et estimat på ressursbruken tilknyttet ID-kontrollene som gjennomføres. Følgelig vil de totale estimatene på ressursbruken i POD, og dermed for hele ID-forvaltningen, gjennomgående være lavere enn hva ressursbruken i realiteten er.

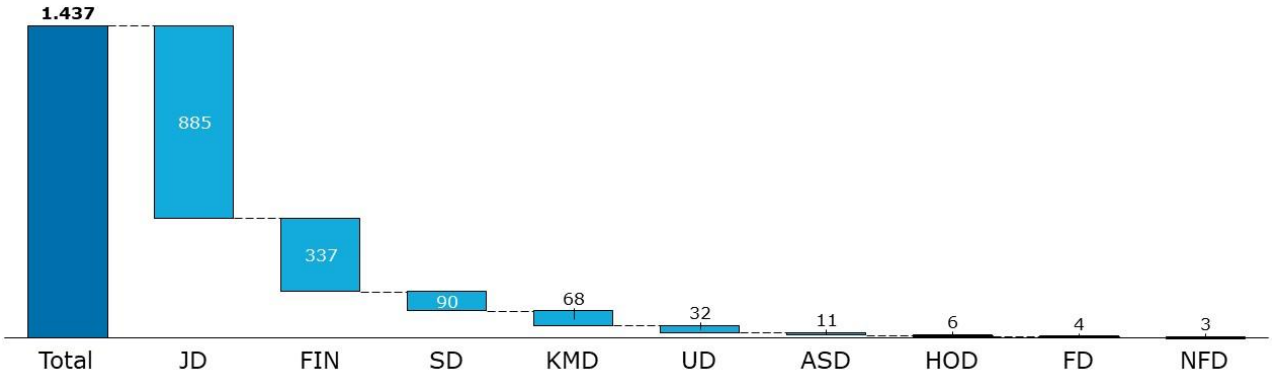
Leverandøren gjør oppmerksom på at kostnadsestimatene er oppgitt i bruttotall og at eventuelle inntekter for aktørene i form av brukergebyr eller tilsvarende ikke er medregnet. Da tilgjengeligheten på ressursbruk knyttet til ID-forvaltning varierer mellom de ulike aktørene har aktørene i varierende grad basert oversendt data på estimater. Basert på dette anser leverandøren de totale estimatene som noe usikre, men er imidlertid av den oppfatning at de totale estimatene gir et representativt bilde av den totale ressursbruken i dagens ID-forvaltning og at de dermed er egnet som grunnlag for å gjøre vurderinger og gi anbefalinger.

7.1.1 Ressursbruk på departementsnivå med underliggende etater og virksomheter

Innhentet data fra de 14 forespurte aktørene i ID-forvaltningen har blitt sammensatt for å kartlegge den totale ressursbruken i dagens ID-forvaltning i 2018, slik presentert i de to figurene under. Figurene under viser elleve aktører, da data for Politidistriktene, Kripos, PU og NID er samlet under POD som aktør.

Dagens ressursbruk på departementsnivå og per aktør

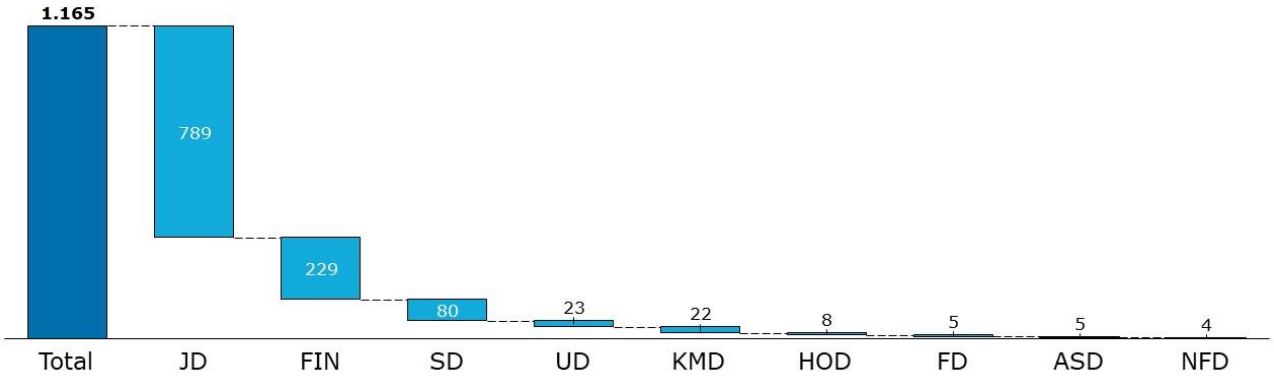
Som figuren under viser, ligger de største kostnadene tilknyttet ID-forvaltningen i JD og underliggende virksomheter med omtrent 890 mill. kroner, etterfulgt av FIN og underliggende virksomheter med omtrent 340 mill. kroner. Samlet ressursbruk for ID-forvaltningen var på omtrent 1,44 mrd. kroner i 2018.



Figur 49 Totale kostnader tilknyttet ID-forvaltningen i 2018 per departement i mill. kroner

Figuren under viser antall årsverk tilknyttet ID-forvaltningen per departement og underliggende virksomheter i 2018. JD med underliggende virksomheter har størst ressursbruk målt i antall årsverk med 789 i 2018, mens FIN og SD med underliggende virksomheter benyttet henholdsvis 229 og 80 årsverk til ID-relatert arbeid i 2018. KMD med underliggende virksomheter hadde kun 22 årsverk knyttet til ID-forvaltning i 2018, et relativt lavt antall årsverk sammenlignet med ressursbruken på 68 mill.

kroner. Dette kan i hovedsak forklares av at KMD har ansvaret for driften av ID-porten og eIDAS i Norge.



Figur 50 Totale årsverk tilknyttet ID-forvaltningen i 2018 per departement

I JD står POD med underliggende virksomheter for 76,5 prosent av totale kostnader relatert til ID-forvaltningen, mens UDI og UNE står for hhv. 21 prosent og 2,5 prosent av totale kostnader. Størsteparten av dagens kostnader i POD kommer fra arbeid relatert til registrering, utstedelse og fornyelse av pass ved passkontorene. For UDI er det saksbehandlingen i utlendingsforvaltningen som driver kostnadene. I tillegg utgjør investeringer i forbindelse med nye pass og nasjonale ID-kort en betydelig del av kostnadene for JDs underliggende virksomheter. Innad i POD stammer 47 prosent av kostnadene fra registrering, utstedelse og fornyelse av pass ved passkontorene, 26 prosent fra PU sitt ID-relaterte arbeid med utlendingsforvaltningen, 13 prosent fra grense- og territorialkontroll utført av politidistriktene, 8 prosent fra Kripos sitt ID-relaterte arbeid og 6 prosent fra NID sin rolle med å styrke ID-arbeidet i utlendingsforvaltningen, politiet og andre offentlige virksomheter. Som nevnt i kapittel 7.1 har ikke leverandøren mottatt data på ressursbruken tilknyttet ID-relatert arbeid i politidistriktenes førstelinje i forbindelse med utlendingsforvaltningen eller ressursbruken tilknyttet ID-kontroller som er en del av politiets øvrige oppgaveutførelse. Dette medfører at ressursbruken for POD er lavere i estimatene som presenteres i rapporten enn hva den er i realiteten.

FINs totale kostnader på omtrent 340 mill. kroner skyldes at SKD og Skatteetaten primært har en vesentlig rolle i ID-forvaltningen, blant annet grunnet ansvaret for Folkeregisteret, samt utøving av ID-kontroll ved skattekontorene. Prosjektet med modernisering av Folkeregisteret som går fra 2016 til 2020 gjør at kostnadene for FD også omfatter betydelige investeringskostnader. Helheten av prosjektet modernisering av Folkeregisteret var ved rapportens utarbeidelse ca. 577 mill. kroner, hvorav 155 mill. kroner er henførbart 2018. [426]

SDs totale kostnader knyttet til ID-forvaltningen på 90 mill. kroner kan i sin helhet tilegnes SVV. Det er SVVs ansvar for utstedelse og fornyelse av førerkort, samt ID-kontroll og opptak av foto ved teoriprøve, som driver aktørens kostnader relatert til ID-forvaltningen.

KMDs ID-relaterte kostnader på omtrent 70 mill. kroner kommer fra Difi og driftsansvaret for ID-porten og utstedelse av MinID, samt ansvaret for eIDAS i Norge.

UD hadde i 2018 en total kostnad knyttet til ID-forvaltningen på 32 mill. kroner. Dette stammer fra Serviceavdelingen i departementet og er knyttet til ID-relatert arbeid både

[426] Basert på intervjuer med representanter i Skatteetaten

i departementet og ved utenriksstasjonene, som for eksempel utstedelse av norske pass i andre land.

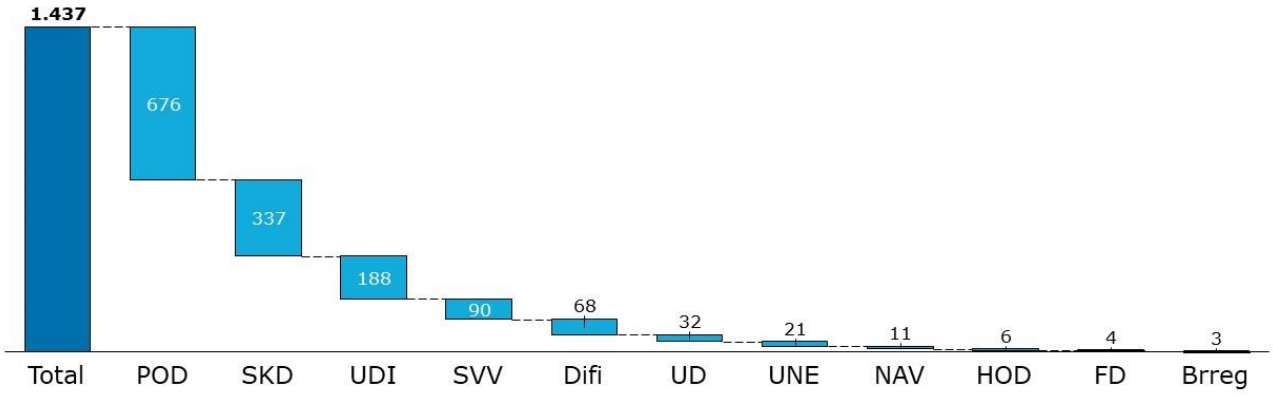
ASD, med NAV som underliggende virksomhet, hadde gjennom rekvirering av d-nummer og investering i ny rekvireringsløsning for d-nummer i 2018 en total kostnad på 11 mill. kroner knyttet til ID-forvaltning.

HOD har i underliggende helseforetak kostnader knyttet til innsendelse av dokumentasjon og registrering av nyfødte i Folkeregisteret, samt ID-kontroll av farskapsmelding ved fødsler[427], som i 2018 summerte seg til 6 mill. kroner.

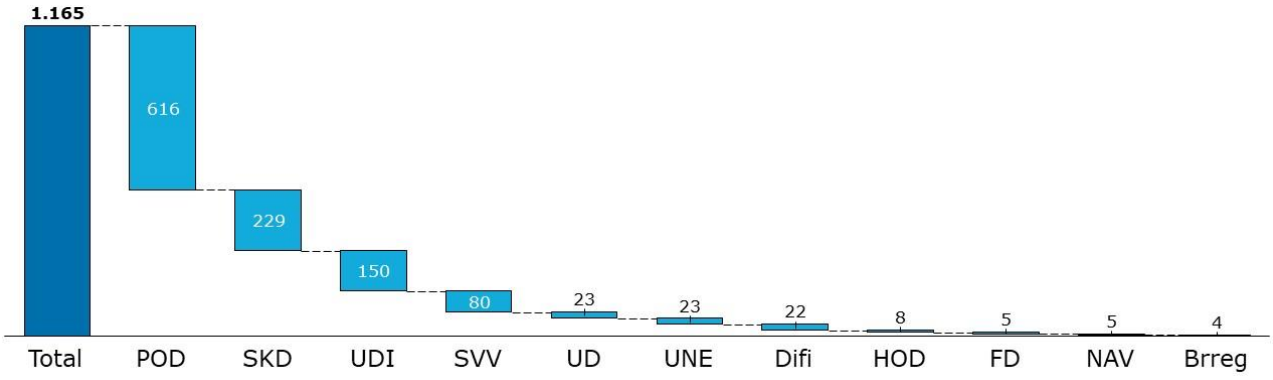
Forsvarsdepartementet utsteder Forsvarets ID-kort til sine ansatte, hvilket i 2018 medførte totale kostnader på 4 mill. kroner.

For NFD kan kostnaden knyttet til ID-forvaltning i sin helhet tilegnes Brønnøysundregistrene, som i 2018 hadde en kostnad på 3 mill. kroner som følge av arbeid med rekvisisjon av d-nummer.

Figurene under viser totale kostnader og årsverk for de sentrale aktørene i ID-forvaltningen i 2018. En mer detaljert oversikt totale kostnader og årsverk for de ulike aktørene finnes i vedlegg 10.



Figur 51 Totale kostnader tilknyttet ID-forvaltningen i 2018 per aktør i mill. kroner



Figur 52 Totale årsverk tilknyttet ID-forvaltningen i 2018 per aktør

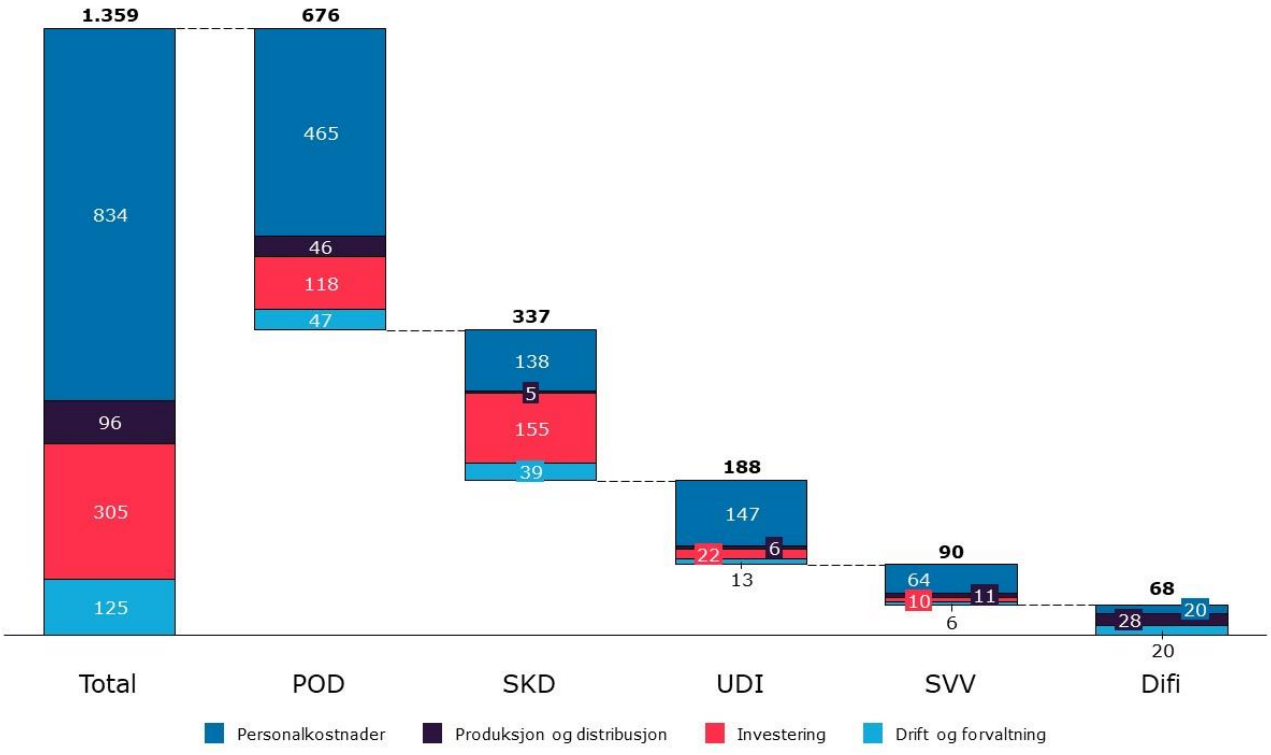
Kostnadsfordeling ved de fem største aktørene

Figuren under viser fordelingen av kostnadene for de fem største aktørene i ID-forvaltningen i 2018 (POD, SKD, UDI, SVV og Difi), som omfatter 95 prosent av de totale kostnadene. Slik figuren viser utgjør personalkostnader den største kostnaden

[427] Basert på intervjuer med representanter i HOD og Direktoratet for e-helse

samlet sett for de fem aktørene, mens det for de ulike aktørene er enkelte forskjeller i hva som er det største kostnadselementet. For POD, UDI og SVV er personalkostnader det største kostnadselementet, hvilket kan forklares av at de tre aktørene utfører mye ID-relatert arbeid med fysisk interaksjon med brukere i form av henholdsvis passutstedelse og grense- og territorialkontroll, utlendingsforvaltning og utstedelse av førerkort. SKD og Difi har i mindre grad fysisk interaksjon med brukere, og personalkostnaden utgjør dermed en lavere andel av totalkostnaden sammenlignet med POD, UDI og SVV. Samlede identifiserte investeringskostnader var 305 mill. kroner, hovedsakelig fordelt på SKD og POD. SKD har betydelige investeringskostnader i 2018, grunnet prosjektet med modernisering av Folkeregisteret. For Difi er produksjons- og distribusjonskostnader det største kostnadselementet, hvilket skyldes autentiseringer ved bruk av eID gjennom ID-porten og utstedelse av MinID til brukere. Øvrige direkte produksjons- og distribusjonskostnader hos de ulike aktørene relatert til ulike fysiske ID-bevis er samlet sett relativt begrenset med omtrent 70 mill. kroner. De samlede kostnadene for drift og forvaltning hos de fem aktørene er på 125 mill. kroner. For POD stammer drifts- og forvaltningskostnadene hovedsakelig fra utstyr og husleie ved passkontor og utgifter til tolk i PU, for SKD skyldes kostnadene systemforvaltning av dagens Folkeregister og husleie, for UDI stammer kostnadene fra lisenser tilknyttet EU-systemene VIS, SIS og Eurodac, og for Difi er systemforvaltning av ID-porten og ansvar for den norske eIDAS-noden kostnadsdriverne.

Leverandøren har, som nevnt i kapittel 7.1, ikke mottatt data fra POD på ressursbruk for politidistriktenes ID-relaterte arbeid i utlendingsforvaltningen eller ressursbruken tilknyttet ID-kontroller som er en del av politiets øvrige oppgaveutførelse. Leverandøren har heller ikke mottatt detaljerte kostnader for grense- og territorialkontroll utover personalkostnader. Følgelig har ikke leverandøren grunnlag for å si noe om årsverk og kostnader ved politidistriktenes utlendingsforvaltning eller ID-kontroller som del av politiets øvrige oppgaveutførelse, og heller ikke beskrive kostnader ved grense- og territorialkontroll utover personalkostnader.

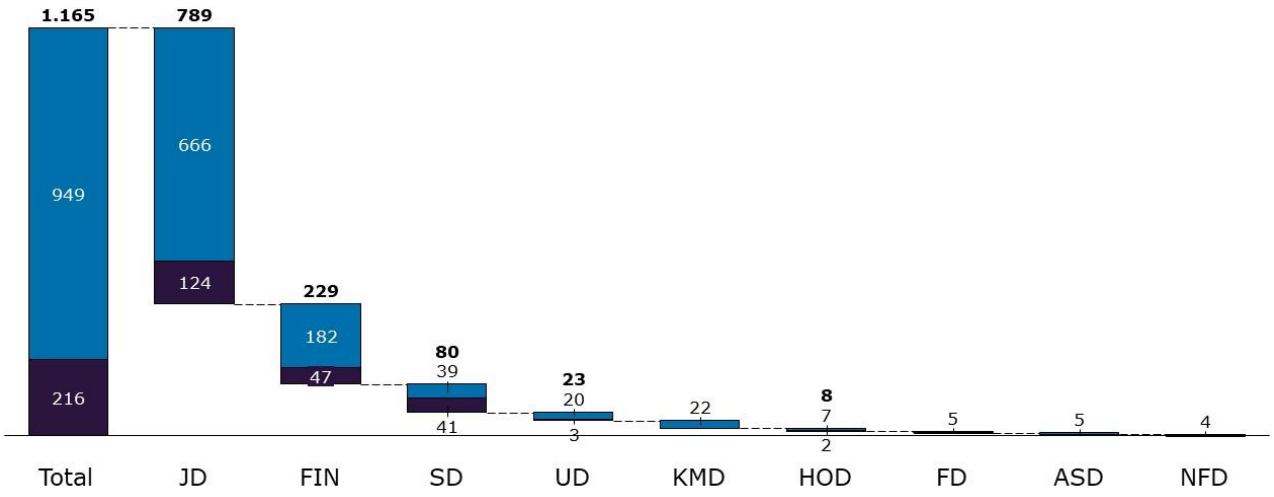


Figur 53 Fordeling av kostnader i 2018, i mill. kroner, for de fem største aktørene

7.1.2 Ressursbruk tilknyttet ID-prosessen

Aktørenes ressursbruk tilknyttet de tre første stegene (fastsetting, registrering og utstedelse) i ID-prosessen er beskrevet i kapittel 2.4. Ressursbruken i disse stegene er ofte svært integrert og det har vært utfordrende for aktørene i datainnsamlingen å skille ressursbruken fra hverandre. Aktørene ble i tillegg bedt om å spesifisere ressursbruk tilknyttet ID-kontroller som ikke er en del av de tre første stegene i prosesskjeden, men etter utstedelse av ID-bevis. Det har for enkelte aktører vært utfordrende å spesifisere ressursbruk for disse ID-kontrollene og tallene for årsverk tilknyttet ID-kontroll i figurene under er derfor i stor grad estimater mottatt fra aktørene. Det er i figurene under benyttet årsverk som grunnlag for fordeling av ressursbruk mellom prosesstegene, da det for flere aktører er svært krevende å dele inn kostnader etter prosesstegene.

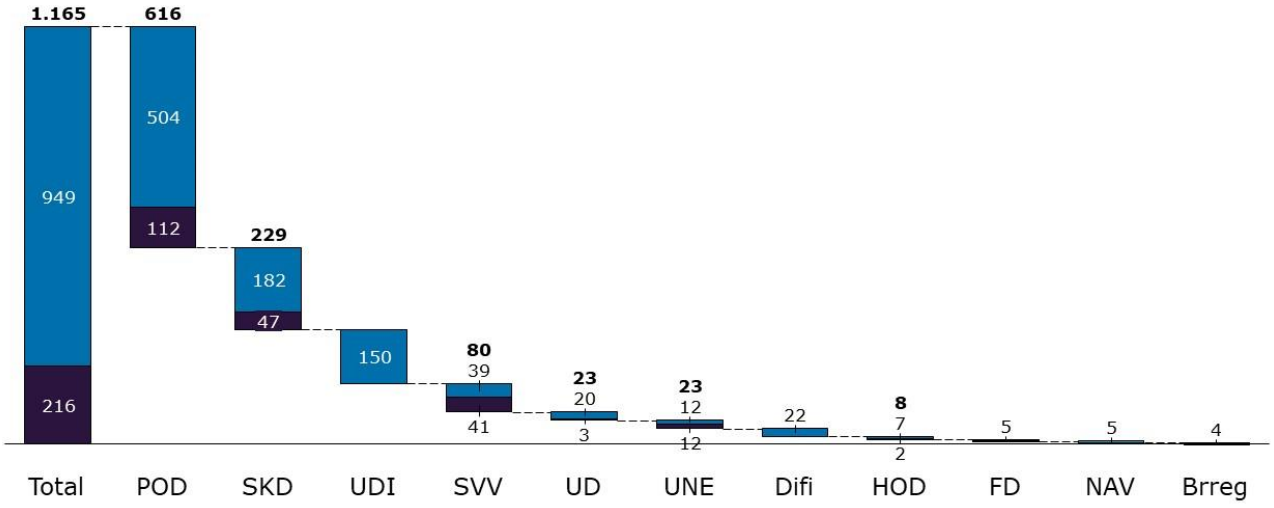
Figuren under viser antall årsverk fordelt på departementene i ID-forvaltningen fordelt på henholdsvis fastsettelse, registrering og utstedelse, samt ID-kontroll. Basert på data er totalt sett 81 prosent av årsverkene knyttet til arbeid med fastsettelse, registrering og utstedelse, mens 19 prosent går med til ID-kontroll. Det er store forskjeller mellom departementene og de underliggende virksomheter ved fordeling av ressursbruk. JD med underliggende virksomheter benytter kun 16 prosent av årsverkene tilknyttet ID-forvaltningen på ID-kontroll. SD og underliggende virksomhet ved SVV benytter i motsetning 51 prosent av årsverkene sine på ID-kontroll, grunnet obligatorisk ID-kontroll ved gjennomføring av teoriprøve og praktisk prøve ved trafikkstasjoner.



Figur 54 Antall årsverk per departement fordelt på steg i prosessen for ID-forvaltningen

Videre viser figuren under at enkelte aktører kun har ressursbruk knyttet til ett av de to prosesstegene, som for eksempel UDI og Difi. ID-kontrollen som gjennomføres i forbindelse med UDI sitt arbeid utføres av politidistriktenes førstelinje eller ved utenriksstasjonene, ettersom UDI selv ikke har førstelinje som utfører ID-kontroll.[428] Basert på mottatte data fra PU og UDI er de totale kostnadene for ID-relatert arbeid tilknyttet utlendingsforvaltningen estimert til 366 mill. kroner og 357 årsverk i 2018. Den totale ressursbruken er imidlertid høyere i realiteten, ettersom leverandøren ikke har mottatt data på politidistriktenes ressursbruk tilknyttet utlendingsforvaltningen. Difi gjennomfører ingen ID-kontroller i forbindelse med deres driftsansvar for ID-porten og utstedelse av MinID, samt ansvaret for eIDAS i Norge, og helheten av årsverkene knyttet til ID-forvaltning i virksomheten tilfaller derfor steget fastsettelse, registrering og utstedelse. Selv om Difis årsverk knyttet til ID-forvaltningen ikke gjennomfører ID-kontroller, er det viktig å presisere at en stor andel av Difis totale kostnader skyldes nettopp ID-kontroller i form av elektroniske autentiseringer gjennom ID-porten. Se kapittel 7.1.3 for antall innlogginger gjennom ID-porten fordelt på ulike aktører.

[428] Basert på intervjuer med representanter i UDI



Figur 55 Antall årsverk per aktør fordelt på steg i prosessen for ID-forvaltning

7.1.3 Ressursbruk for ID-porten og dagens eID

Difi sine kostnader og årsverk knyttet til ID-forvaltningen presentert i kapittel 7.1.1 stammer fra ansvaret for ID-porten, ansvaret for den norske eIDAS-noden, distribusjonskostnader knyttet til MinID og transaksjonskostnader gjennom ID-porten.[429]

Difi sine totale kostnader tilknyttet ID-forvaltning var i 2018 68 mill. kroner og direktoratet benyttet 22 årsverk. Det betyr at den totale kostnaden for den norske stat, gjennom Difi, ved å tilby felles innlogging til offentlige digitale tjenester var på 68 mill. kroner i 2018. De 68 mill. kronene går med til å dekke samtlige aktørers transaksjonskostnader ved innlogging via ID-porten, drift og forvaltning av ID-porten og den offentlige eID-en MinID, samt ansvaret for den norske eIDAS-noden. Finansieringsmodellen til ID-porten er delt mellom sentralfinansiering og transaksjonsfinansiering fra kundene. Med kunde menes virksomheter som benytter ID-porten som pålogging til sine tjenester, dvs. i stor grad primæraktører dekket i områdegjennomgangen. I 2018 utgjorde sentralfinansering 51 prosent av driftskostnadene for ID-porten, mens 49 prosent av driftskostnadene finansieres av kundene. For kunder med mindre enn 200 000 innlogginger per år er bruk av ID-porten gratis for kunden og dekkes i sin helhet av Difi. Kunder med over 200 000 innlogginger per år betaler en fast transaksjonspris uavhengig av volum, og bidrar dermed med finansiering på alle sine innlogginger. Utvikling av løsningene i ID-porten, samt drift av MinID og eIDAS, er også sentralfinansiert.[430]

Transaksjonsprisen kundene betaler per autentisering varierer fra år til år, men har i perioden 2015 til 2018 sunket med ca. 2 prosent (ikke prisjustert). Transaksjonsprisen er et gjennomsnitt av prisene for de ulike eID-ene som er tilgjengelig i ID-porten, da Difi ikke belaster kundene basert på hvilken autentiseringsløsning brukerne velger å benytte seg av. Transaksjonskostnader som Difi tar på seg generert av kunder med under 200 000 autentiseringer beløp i 2018 seg til 5 mill. kroner. Utsendelse av PIN-brev for MinID kostet i 2018 Difi 1,7 mill. kroner, fordelt på 121 410 utstedte MinID. Om en sammenligner den totale kostnaden for det offentlige ved å tilby digital autentisering gjennom ID-porten og MinID på 68 mill. kroner mot totalt 139,4 millioner autentiseringer i 2018, gir det en kostnad per autentisering på ca. 0,5 kroner.

[429] Basert på samtaler med representanter i Difi
[430] Data mottatt fra representanter i Difi

Tabellen under viser antall innlogginger for de ti mest brukte tjeneste i ID-porten. Transaksjonskostnaden for innlogging til tjenestene belastes til slutt aktøren selv og kan anses som aktørens kostnad ved elektronisk ID-kontroll. I kapittel 7 er imidlertid samtlige transaksjonskostnader tilknyttet autentisering gjennom ID-porten ført under Difi for å vise et totalbilde av det offentliges kostnader ved å tilby felles innlogging til offentlige digitale tjenester.

Topp ti brukte tjenester 2018	Antall innlogginger
Altinn	39,2 mill.
NAV	37,8 mill.
Helsenorge	12,3 mill.
Digipost	12,3 mill.
Lånekassen	5,7 mill.
SVV	4,3 mill.
Skatteetaten	3,0 mill.
Autopass	1,9 mill.
Mine resepter	1,8 mill.
Samordna opptak	1,8 mill.
Totalt topp 10	**120,1 mill.**

Tabell 20 De ti mest brukte tjenestene i ID-porten i 2018[431]

7.1.4 Utvikling i ressursbruk over tid (2015, 2018 og estimat for 2021)

Basert på innsamlet data om ressursbruk fra aktørene har leverandøren gjort en overordnet sammenligning av utviklingen i den totale ressursbruken tilknyttet ID-forvaltningen, uttrykt ved antall årsverk og totale kostnader. Figurene under viser at antallet årsverk har sunket fra 2015 til 2018, men antas å øke mot 2021, mens de totale kostnadene tilknyttet ID-forvaltningen har steget fra 2015 til 2018 og antas å øke videre frem mot 2021. Leverandøren påpeker at tall for 2021 er beste estimat mottatt fra aktørene, basert på dagens situasjon og vedtatte planer frem mot 2021.

En av forklaringene for reduksjonen i det totale antall årsverk fra 2015 til 2018 er at det i 2015 var en masseankomst av flyktninger til Norge, hvilket bidro til økt antall årsverk i PU og UDI for utlendingsforvaltningen i 2015. I 2018 er antall årsverk i PU og UDI betydelig redusert, grunnet færre ankomne flyktninger til Norge. Antall årsverk tilknyttet NPID-prosjektet økte fra 2015 til 2018 og bidrar til at nettoreduksjonen i antall årsverk fra 2015 til 2018 begrenses. Videre reduserte SKD sine årsverk relatert til ID med 13 prosent fra 2015 til 2018 som bidrar til at totalt antall årsverk i ID-forvaltningen ble redusert.

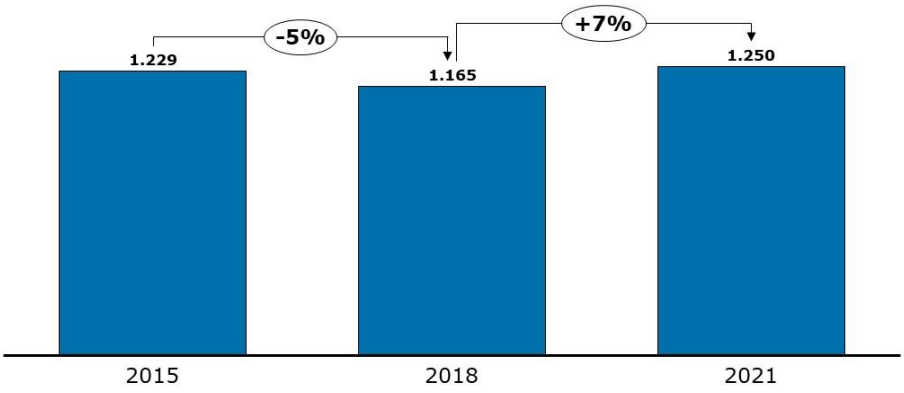
Økningen i de totale kostnadene fra 2015 til 2018 skyldes dels at POD har erstattet manuelle prosesser og kontorer i perioden, på bekostning av økte drift og forvaltningskostnader. Investeringskostnadene tilknyttet NPID-prosjektet er i tillegg så betydelige at de mer enn veier opp for den reduserte personalkostnaden i utlendingsforvaltningen fra 2015 til 2018. NPID-prosjektet slik nærmere beskrevet i kapittel 2.9.1 vil videre bidra til økt sikkerhet i utstedelse og bruk av ID-bevisene pass og nasjonalt ID-kort, og høyere sikkerhet gir økte drifts- og forvaltningskostnader. Som beskrevet i kapittel 7.1.1 investeres det ca. 577 mill. kroner i prosjektet modernisering

[431] Basert på data om ID-porten mottatt fra Difi

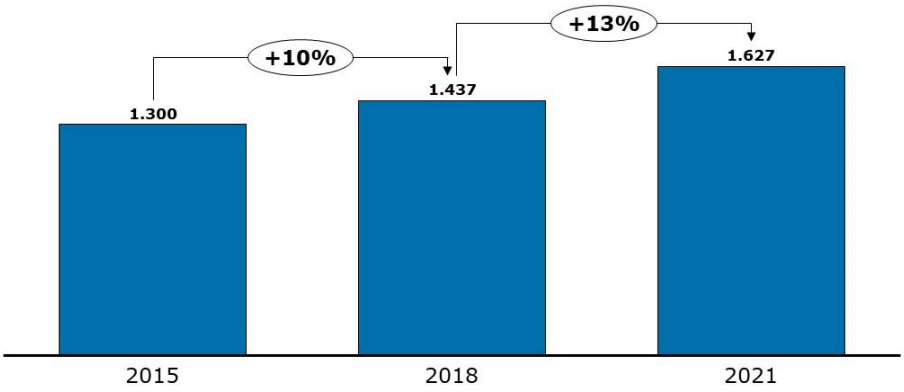
av Folkeregisteret fra 2016 til 2020, som også forklarer deler av økningen i de totale kostnadene fra 2015 til 2018.

Den estimerte økningen i totalt antall årsverk fra 2018 til 2021 skyldes i hovedsak at det etableres en ny andrelinje ved utstedelse av pass og nasjonalt ID-kort i politiet som del av NPID-prosjektet, hvilket øker det totale antall årsverk som er tilknyttet utstedelse av pass og i fremtiden nasjonale ID-kort. PU har en pågående nedbemanningsprosess som ventes å resultere i en ti prosent reduksjon i antall årsverk for aktøren fra 2018 til 2021. Videre forventer SVV en elleve prosent reduksjon i antall årsverk tilknyttet utstedelse av førerkort fra 2018 til 2021, grunnet økt bruk av selvbetjeningsløsningen for fornying av førerkort på nett. Det er ikke identifisert vesentlig planlagt reduksjon i antall årsverk relatert til ID-relatert arbeid hos andre aktører. Totalt sett viser estimatene mottatt fra aktørene at det forventes en økning i antall årsverk relatert til ID-arbeid frem mot 2021.

De totale kostnadene er antatt å øke fra 2018 til 2021, i hovedsak drevet av økte kostnader som følge av det planlagt fullførte NPID-prosjektet. Videre viser estimatene fra UDI at det forventes økte kostnader tilknyttet investeringer i EU-systemene VIS, SIS og Eurodac i 2021. Prosjektet modernisering av Folkeregisteret fullføres i 2020 og tilhørende tidligere investeringskostnader reduseres, men økte drifts- og forvaltningskostnader tilknyttet det moderniserte Folkeregisteret begrenser nettoreduksjonen i SKDs totale kostnader i 2021.



Figur 56 Utvikling i totale antall årsverk tilknyttet ID-forvaltningen



Figur 57 Utvikling i totale kostnader tilknyttet ID-forvaltningen

7.1.5 Kostnadsdekkende ID-bevis

Leverandøren har blitt forelagt gebyrmodeller fra POD og SVV for deres respektive ID-bevis. Gebyrmodellene gir en oversikt over direkte kostnader som påløper ved registrering og utstedelse av et ID-bevis, og benyttes av aktørene til å beregne kostnadsdekkene gebyrer for ID-bevisene som utstedes. Tabellen under gir en oversikt over påløpte kostnader, tilhørende gebyrer for bruker og differansen mellom de to.

Slik tabellen viser er det for utstedelse av pass ikke fullt kostnadsdekkende gebyrsatser, og gebyrsatsene har stått uendret siden 2008. Ved å justere for prisstigning med utgangspunkt i konsumprisindeksen, er imidlertid gebyrsatsene reelt sett redusert fra 2008 til 2018.[432] Slik det fremgår av tabellen er kostnadene ved utstedelse av pass for barn høyere enn for voksne, hovedsakelig grunnet høyere tidsbruk ved passkontorets skranker. Samtidig er gebyrsatsen for et barnepass lavere enn for et voksenpass, da gyldigheten på et barnepass er kortere enn for et voksenpass slik at den totale gebyrkostnaden for å inneha et gyldig barnepass er høyere enn for et voksenpass. I forbindelse med utrulling av nye pass og nasjonale ID-kort er det utarbeidet en oppdatert gebyrmodell som i tråd med FINs bestemmelser om statlig gebyr- og avgiftsfinansiering[433] vil gjøre at gebyrene for de ulike passtypene kan settes til å fullt ut dekke kostnaden ved å produsere og levere passene.[434] JD foreslår i tillegg å videreføre dagens ordning med lavere gebyrsats for barnepass, og at kostnadene i stedet subsidieres eksempelvis ved et høyere gebyr for voksenpass.[435]

Tabellen under viser at førerkort duplikat utstedt som følge av bestilling ved fysisk oppmøte ikke er fullt ut kostnadsdekkede, men at gebyrene for førstegangsutstedelse og utstedelse av duplikat i sum er relativt kostnadsdekkende. I 2018 ble 52 prosent av bestillingene for duplikat av førerkort gjort via SVV selvbetjeningsløsning på nett, som ble lansert i midten av februar 2018.[436] I tillegg til at gebyret for brukeren er lavere ved bestilling på nett, er den økende andelen digitale bestillinger av duplikat førerkort fordelaktig for SVV da prosessen er mindre ressurskrevende og kostnadsdekkende slik tabellen viser.

ID-bevis	Kostnad ved å utstede ID-bevis (2019)	Gebyr for bruker (2019)	Differanse *(gebyr – kostnad)*
Pass, voksne[437]	477 kroner	450 kroner	-27 kroner
Pass, barn	645 kroner	270 kroner	-375 kroner
Førerkort, førstegangsutstedelse og fornyelse (fysisk oppmøte) [438]	370 kroner	380 kroner	10 kroner
Førerkort, bestilling av duplikat (fysisk oppmøte)	336 kroner	300 kroner	-36 kroner
Førerkort, bestilling duplikat (på nett)	133 kroner	140 kroner	7 kroner

Tabell 21 Gebyrer og kostnader for pass og førerkort

[432] Ssb.no, «Priser og prisindekser – Konsumprisindeksen», 10.07.2019
[433] FIN, «Rundskriv R-112/15 Bestemmelser om statlig gebyr- og avgiftsfinansiering», 2015
[434] JD, «Høring - ny forskrift om pass og nasjonalt ID-kort», 2019
[435] JD, «Høring - ny forskrift om pass og nasjonalt ID-kort», 2019
[436] Data mottatt av representanter i SVV
[437] Gebyrer for pass er hentet fra Politiet.no, «Pass og timebestilling», u.å.
[438] Gebyrer for førerkort er hentet fra Vegvesen.no, «Priser på teoriprøve, oppkjøring, utstedelse og foto», 26.04.2019

I kapittel 5.1.9 ble gebyrene for pass, nasjonalt ID-kort og førerkort i Sverige, Danmark, Storbritannia og Latvia presentert. Leverandøren har i liten grad identifisert dokumentert informasjon på de reelle kostnadene ved å utstede de ulike ID-bevisene i de nevnte landene, men Sverige opererer etter leverandørens forståelse med kostnadsdekkende gebyr for pass og nasjonalt ID-kort.[439] Leverandøren er ikke kjent med at det eksisterer komplett sammenligningsgrunnlag for om det praktiseres kostnadsdekkende gebyr for de ulike ID-bevisene på tvers av landene. Det fremgår av tabellen i kapittel 5.1.9 at gebyrene for pass i Danmark og Storbritannia er vesentlig høyere enn i Norge Sverige og Latvia, og at gebyret for nasjonalt ID-kort i Sverige fremstår som høyt sammenlignet med gebyret i Danmark og Latvia.

Gebyrene for førerkort er relativt like på tvers av landene, men gebyret for førerkort i Sverige er lavt sammenlignet med gebyret i Norge til tross for at gebyret for pass er relativt likt i de to landene.

Forskjeller i gebyrer mellom landene kan potensielt forklares av effektivitetsforskjeller i utstedelsen av ID-bevisene, der lavere gebyr indikerer høyere effektivitet gitt at gebyrene er kostnadsdekkende. Forskjellene kan også i høy grad skyldes kvalitetsforskjeller mellom landene per ID-bevis. Ettersom leverandøren ikke fullt ut er kjent med om det praktiseres kostnadsdekkende gebyrer eller om det er kvalitetsforskjeller for ID-bevisene i de nevnte landene kan det ikke sies med sikkerhet at effektiviteten varierer mellom landene.

7.2 Funn og vurderinger

Under følger leverandørens vurderinger av nåsituasjonen for ressursbruk i ID-forvaltningen. Helhetlige vurderinger foretas av leverandøren i del 3 av rapporten.

7.2.1 Det er liten bevissthet på ressursbruk tilknyttet ID-relatert arbeid

Mottatt data på ressursbruk var for enkelte av aktørene av varierende kvalitet, men er gjennom oppfølgingsspørsmål i stor grad blitt kvalitetssikret med aktørene. Leverandøren oppfatter det slik at få aktører har direkte tilgjengelig data på egen ressursbruk knyttet til ID-forvaltning, og at enkelte aktører til en viss grad mangler oversikt over sitt ID-relaterte arbeid. Det er derfor flere aktører som har basert oversendt data på estimater. Aktørene har spesielt utfordringer med å gi en oversikt over påløpte kostnader på noe annet enn et overordnet nivå, og har ikke tilgjengelig data på ressursbruk knyttet til henholdsvis fastsettelse, registrering og utstedelse og ID-kontroll. Det er for flere av aktørene varierende datakvalitet på ressursbruk for andre år enn 2018, hvilket gjør at analysene over tid i stor grad baserer seg på aktørenes estimater.

Mangelen på tilgjengelig data skyldes blant annet lite enhetlig styring av ID-området, lite enhetlig tilnærming til føring av tid i aktørenes timeregistreringssystemer, forskjeller i regnskapsføring hos de ulike aktørene og varierende oversikt over egne oppgaver tilknyttet ID-forvaltningen. Eksempelvis opplever leverandøren at det er utfordrende for aktørene å svare ut ressursbruken knyttet til ID-kontroll som ikke er direkte tilknyttet registrering og utstedelse/fornyelse av ID-bevis. Dette gjelder spesielt for POD, som ikke har estimater på ressursbruk tilknyttet ID-kontroller utført av politiets førstelinje i utlendingsforvaltningen og ID-kontroller som del av politiets øvrige oppgaveutførelse. I dette tilfellet vurderes det som lite hensiktsmessig at verken UDI

[439] SOU 2019:14, «Ett säkert statligt ID-kort – med e-legitimation», 2019

som eier av regelverket eller POD som utførende aktør har styringsinformasjon om hvilken ressursbruk regelverket medfører. UDI eller POD har dermed ingen styringsinformasjon om oppgavene utføres på en ressurseffektiv måte.

7.2.2 Kostnadsnivået på ulike ID-bevis lar seg til dels logisk forklare

Dagens struktur og innretning for registrering, utstedelse og fornyelse av pass medfører vesentlige kostnader, både per pass og samlet sett. Passets begrensede gyldighetsperiode og krav til fysisk oppmøte ved fornyelse bidrar til et høyt kostnadsnivå. Videre er dagens innretning med saksbehandlere i skranke på et stort antall passkontorer kostnadsintensivt med tanke på ressursbruk. Kostnadsnivået øker ytterligere ved at passet som fysisk «bok» må produseres og distribueres til mottaker. Den pågående innføringen av økte sikkerhetsmekanismer slik som eksempelvis andre linje kontroll øker sikkerhetsnivået, men øker også kostnadene. De overnevnte punkter gjør at det høye kostnadsnivået for pass som ID-bevis lar seg til dels logisk forklare. En del av de samme betraktningene gjelder for førerkort.

Strukturer for ID-bevis som ikke inneholder fornyelse eller med automatisk / digital fornyelse gir vesentlig lavere kostnader. Ved å ikke ha krav til fysisk oppmøte hos saksbehandler reduseres kostnaden til ressursbruk betraktelig, og digital fornyelse og ID-kontroll gjør at prosessen blir langt mer kostnadseffektiv. Eksempelvis er kostnaden knyttet til eID lav sammenlignet med fysiske ID-bevis, da kostnader ved fysisk oppmøte, fornyelse, produksjon og distribusjon er fraværende. Det samme gjelder digital fornyelse av førerkort, jf. tabell 21.

7.2.3 Statens kostnader for etablering av fysiske ID-bevis er høye sammenlignet med bruk av elektroniske ID-bevis

Politiets og SVVs totale kostnader knyttet til pass og førerkort var i 2018 henholdsvis 320 mill. kroner og 90 mill. kroner ifølge mottatt data fra de to aktørene. Dette omfatter alle kostnader som påløper ved å tilby de fysiske ID-bevisene til befolkningen. For øvrige fysiske ID-bevis slik nevnt i kapittel 2.3 påløper også betydelige kostnader. Samtidig viser analysene at ressursbruken knyttet til fysiske ID-kontroller, og dermed antall kontroller, er relativt lav og at kostnaden for å benytte et pass eller førerkort ved en fysisk ID-kontroll dermed blir høy fordelt på antall kontroller. Til sammenligning var Difis totale kostnad ved å tilby tjenestene i ID-porten 68 mill. kroner i 2018, hvilket med 139,4 mill. innlogginger gir en kostnad per autentisering på omtrent 0,5 kroner.

Leverandøren er videre kjent med at bankene har betydelige kostnader med å etablere og drifte BankID som ikke nødvendigvis belastes staten/Difi gjennom transaksjonsgebyret per autentisering. Disse kostnadene stammer i hovedsak fra brukerservice som bankene yter sine kunder, samt kostnader ved å utstede BankID brikker til kunder.

I 2018 ble det gjennomført omtrent 139 mill. innlogginger gjennom ID-porten, dvs. elektroniske ID-kontroller, hvilket tilsvarer omtrent 30 innlogginger per innbygger i Norge. Prisen for både gjennomføring av en slik elektronisk ID-kontroll og saksbehandlings-, produksjons- og distribusjonskostnaden knyttet til eID er vesentlig lavere enn for en fysisk ID-kontroll. Dagens kommunikasjon mellom det offentlige og en norsk borger gjøres hovedsakelig digitalt, og behovet for å legitimere seg med fysisk ID-bevis er lavt sammenlignet med bruken av eID. Det offentliges kostnader til ID-kontroll ville derfor vært vesentlig høyere ved høyere bruk av fysiske ID-bevis.

7.2.4 Det er krevende å vurdere samlet ressurseffektivitet i ID-forvaltningen og per ID-bevis

Som vist i kapittel 7.1 er statens samlede kostnader relatert til ID-forvaltningen omtrent 1,44 mrd. kroner. Dagens ressursbruk er en funksjon av dagens praksis, omfang av fysiske ID-bevis med høye krav til fornyelser, lite gjenbruk av informasjon på tvers av aktører og vedtatte investeringer og oppgraderinger av dagens løsninger og systemer. Ressursbruken er videre en funksjon av valgt brukervennlighet og sikkerhet.

Når det ikke eksisterer enhetlige mål eller styringsparametere for verken sikkerhet, brukervennlighet eller ressursbruk/produktivitet er det krevende å entydig konkludere hva nivået på ressurseffektiviteten i realiteten er. Leverandøren mener at det er enkelte motstridende indikasjoner på utvikling i ressurseffektivitet i ID-forvaltningen:

- Ingen av aktørene har på selvstendig grunnlag fremlagt dataunderlag som tilsier vesentlig økning i ressurseffektivitet i nyere tid
- Estimerte kostnader stiger fra 2015-2021 relativt raskt, men kan blant annet i POD forklares med antatte økninger i sikkerhetsnivå
- Passgebyr for bruker har stått uendret siden 2008, hvilket kan tyde på positiv utvikling av kostnader til produksjon eller at området i liten grad er fulgt opp historisk med oppdatering av passgebyr
- Store forskjeller i passgebyrer sammenlignet med naboland. Passgebyret er vesentlig høyere i Storbritannia og Danmark og noe lavere i Sverige, sammenlignet med Norge. Gebyret for førerkort er imidlertid høyere i Norge enn i Sverige. Gitt Norges demografi og høye kostnadsnivå forventet leverandøren til dels at Norge ville ligge i «den høye enden», men effektivitets- og kvalitetsforskjeller i utstedelsesprosessen i de ulike landene kan imidlertid ha en innvirkning på gebyrforskjellene.

Basert på funnene presentert i kapittel 7.2.4 og det faktum at det er manglende enhetlig styring av området, slik beskrevet i kapittel 3, vurderer leverandøren at det sannsynligvis er noe å hente for å øke ressurseffektiviteten på tvers av ID-forvaltningen.

Del 3: Drøfting av alternative løsninger

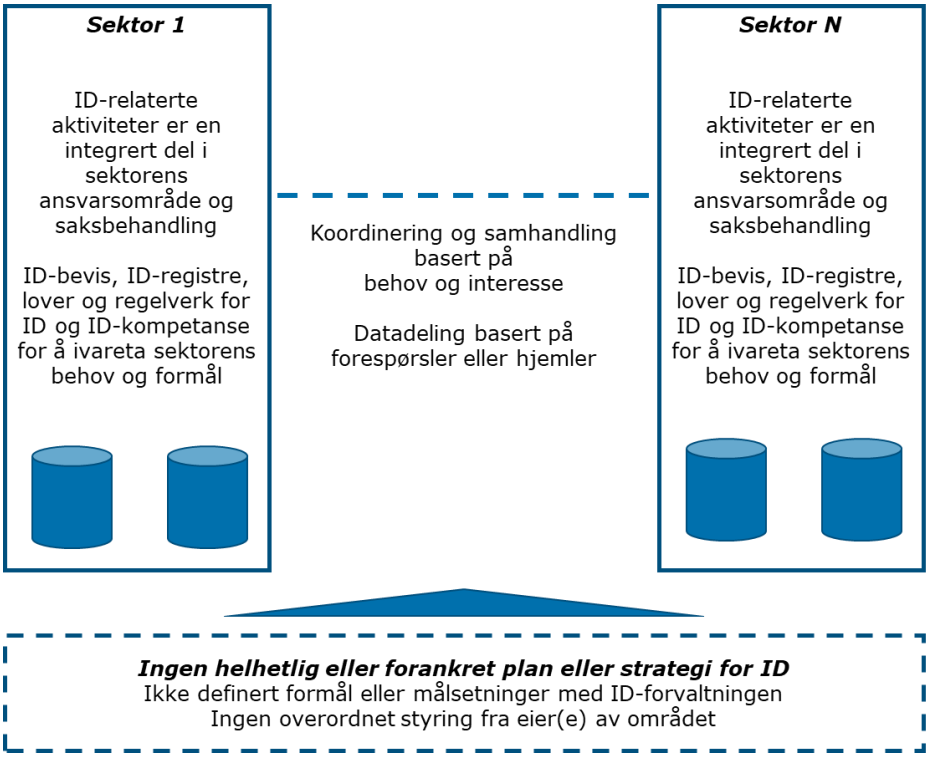
Del 3 drøfter alternative løsninger for ID-forvaltningen. Delen inneholder helhetlige vurderinger av nåsituasjonen (kapittel 8) og viktigste utviklingstrekk og skisse til mål for ID-forvaltningen (kapittel 9). Med dette som utgangspunkt har leverandøren valgt å drøfte utfordringene og kartlegge alternativer til dagens praksis for seks tema. Temaene er fysiske ID-bevis og utbredelse av nasjonalt ID-kort (kapittel 10), eID (kapittel 11), identitetsnummer i Folkeregisteret (kapittel 12), biometri (kapittel 13), fysiske oppmøter (kapittel 14) og styring og struktur (kapittel 15). Alternativene innenfor hvert tema er vurdert metodisk, slik beskrevet i kapittel 1.3, opp mot sikkerhet, brukervennlighet og ressursbruk.

8 Helhetlige vurderinger av nåsituasjonen

Nåsituasjonen for ID-forvaltningen er i del 2 beskrevet gjennom fem definerte analyseområder med tilhørende funn og vurderinger per analyseområde. I det følgende gir leverandøren sin helhetlige vurdering av nåsituasjonen for ID-forvaltningen.

8.1 Forståelse av dagens tilnærming til ID-forvaltningen

Som utgangspunkt for den helhetlige vurderingen har leverandøren i figuren under beskrevet sin forståelse av dagens tilnærming til ID-forvaltning.



Figur 58 Leverandørens fortolkning av dagens tilnærming til ID-forvaltning

Sektorprinsippet står sterkt i Norge og legges til grunn for oppgave- og ansvarsfordelingen i staten. Dette gjelder også aktivitetene som naturlig faller inn under dagens ID-forvaltning, hvor oppgavene i stor grad er integrert i sektorenes ansvarsområde og saksbehandling. Elleve departementer, med tilhørende virksomheter, har en rolle i dagens ID-forvaltning. Dette innebærer at ID-bevis, ID-

registre, regelverk og ID-kompetanse i stor grad er utviklet for å ivareta sektorens behov og formål. Helheten av ID-forvaltningen er av natur tverrsektoriell og krever koordinering og samhandling for å kunne løses hensiktsmessig i dagens struktur. Koordinering og samhandling er i stor grad basert på hvilke behov og interesser de ulike aktørene har til enhver tid. ID-forvaltningen, slik den fremstår i dag, har ikke en eier eller en aktør som arbeider som premissgiver. ID er i liten grad en kjerneaktivitet for aktørene, men et stort antall aktører har ID som en sideaktivitet eller er involvert i deler av ID-prosessen.

8.2 Viktigste styrker ved dagens ID-forvaltning

Fokuset på ID-relaterte problemstillinger har blitt forsterket de seneste årene og er nå gjenstand for vesentlig større oppmerksomhet enn tidligere. Befolkningen har i stort høy grad av tillit til arbeid utført av det offentlige, dette gjelder også ID-arbeid.

Ansvars- og rollefordelingen for ID-området har utviklet seg over tid og er fragmentert. Tilnærmingen gir stor frihet innad i hver sektor til å definere hvordan ID-arbeidet skal uføres. Hver sektor har høy grad av kontroll på egne og relevant data, relativt god brukervennlighet i ID-prosessen og i tillegg er det høy grad av nærhet mellom sektorens tjenester/leveranser og ID-relatert arbeid i hver sektor. Flere gode fagmiljøer med spisskompetanse innenfor eget ID-område for alle sektorer har bidratt til bedre kvalitet og økt sikkerhet i ID-forvaltningen de siste årene.

Folkeregistret, med nøkkelopplysninger om alle personer som er eller har vært bosatt i Norge, danner et robust fundament for ID-forvaltningen. Pågående arbeid med modernisering av Folkeregisteret legger grunnlag for å kunne registrere borgere med «unik» identitet, i tillegg til «kontrollert» og «ikke-kontrollert». Både offentlige og private aktører benytter Folkeregistret i utstrakt grad som kilde til grunndata i ID-relatert arbeid, noe som gir betydelige gevinster. Det vurderes også som positivt at et sentralt folkeregister gir brukerne ett identitetsnummer å forholde seg til.

Et bevisst fokus på offentlige digitaliseringstiltak har gitt de fleste brukere muligheten til å nyttiggjøre seg offentlige digitale tjenester gjennom autentisering i ID-porten. Dagens private eID-er med autentisering gjennom ID-porten er i stor grad velfungerende og utbredt, samt bidrar til å redusere kostnader og tidsbruk sett fra et brukerperspektiv. Dagens tilnærming vurderes videre som ressurseffektiv.

Samarbeid på tvers av offentlig sektor er styrket og endringsvilligheten i form av at majoriteten av aktørene ønsker en mer helhetlig tilnærming til ID-forvaltningen er tydelig. Utvalgte etater og virksomheter har, gjennom arbeidet i KoID, en omforent visjon for fremtidens ID-forvaltning. Kombinert med nært forestående ferdigstilling av betydelige moderniseringsprosjekter (modernisering av norske pass og lansering av nasjonale ID-kort med eID samt modernisering av Folkeregisteret) er det momentum for å forbedre ID-forvaltningen i Norge.

8.3 Viktigste utfordringer ved dagens ID-forvaltning

Under følger en vurdering av utfordringer eller svakheter ved dagens ID-forvaltning. De identifiserte områdene er sett opp mot hvilke konsekvenser de har for sikkerhet, brukervennlighet og ressursbruk.

Dagens styring gir en sektoriell og fragmentert tilnærming til ID-forvaltningen, hvor hver sektor ivaretar sitt formål, ansvarsområde og aktivitetene de skal løse. Mange aktører er involvert i ID-arbeidet, men få har ID som sin kjerneaktivitet. Konsekvensen

av fragmentering og lav grad av **strategisk styring** er at ingen har ansvar for å gjøre helhetlige vurderinger, gi helhetlige føringer eller ta helhetlige prinsipielle beslutninger. Det er ikke tilrettelagt for å kunne styre ID-forvaltningen helhetlig basert på kostnader, brukertilfredshet eller sikkerhet. Det finnes en stor mengde utredninger og dokumentasjon på ID-området med til dels forskjellige konklusjoner og anbefalinger. Samlet sett er helheten av tidligere dokumentasjon på kostnader, brukertilfredshet og sikkerhet svak, hvor mål, måltall og faktiske resultater i varierende grad er dokumentert.

Med mange involverte aktører er det krevende å oppnå konsensus om veivalg og sikre gjennomføringskraft. Det er mange gode intensjoner, men endringstakten og gjennomføringsevnen i dagens ID-forvaltning er lav. Prosjektet nye pass- og nasjonale ID-kort, et stort og viktig ID-relatert prosjekt som også påvirker mange andre deler og prosesser i ID-forvaltningen, har møtt gjentatte forsinkelser og utsettelser. Dette påvirker fremdriften og måloppnåelsen på ID-området isolert og som helhet. Utvikling innenfor blant annet digitalisering, data og personvern, biometri og sikkerhet skjer raskt og kan ha stor betydning for området. Det er derfor en risiko for at lav gjennomføringsevne ikke sikrer implementering av fremtidsrettede løsninger, da ID-forvaltningen i dag hovedsakelig implementerer beslutninger som er foretatt mange år tilbake. Lav grad av strategisk styring medfører negative konsekvenser for bruker, ressursbruk og sikkerhet.

Reguleringen av ID-forvaltningen er fragmentert. Det finnes ikke ett felles sektorovergripende **regelverk** som regulerer hele ID-området, og hva som skal anses som gyldig legitimasjon er ikke entydig definert. I stedet er det et relativt stort antall lover og andre regelverk som regulerer deler av, og som samlet sett dekker de ulike formålene med ID-forvaltningen. Regelverkene inneholder en rekke hjemler for deling av data mellom ulike aktører og på tvers av sektorer. Andre former for samhandling er i liten grad regulert.

Det er lav bevissthet tilknyttet samlet **brukervennlighet** og liten grad av helhetlig tilnærming på tvers av de ulike brukergruppene. Bruker har, med dagens løsninger, stor fleksibilitet i hvilke krav som stilles til fremvisning av fysisk legitimasjon, men har samtidig få gode alternativer til pass for en sikker fysisk legitimering. Norske borgere har nærmere 30 treffpunkt med ID-forvaltningen for etablering og fornyelse av pass, førerkort og bankkort med bilde i et livsløpsperspektiv. Treffpunktene er i all hovedsak knyttet til oppmøtekrav for etablering og fornyelse av fysiske ID-bevis. Avhengig av fremtidig gyldighet for pass vil nytt regelverk medføre 40 til 46 oppmøter etter innføring av nasjonalt ID-kort. Leverandøren vurderer at nåværende og planlagt antall oppmøter er høyt, spesielt i et stadig mer digitalisert samfunn. I tillegg legges det i liten grad til rette for gjenbruk og deling av relevant data mellom aktørene i ID-forvaltningen for å etterkomme prinsippet om «kun en gang». Det må i noen utstrekning tilskrives personopplysningsregelverket, som setter rammer for deling av personopplysninger. Nettopp dette er en særlig utfordring innenfor ID-forvaltningen, ettersom svært mye informasjon av praktiske hensyn burde vært delt i stor utstrekning, og at ID-forvaltningen grunnleggende sett handler om å behandle personopplysninger. Her fremstår ofte regelverksutfordringer begrensende. Dagens manglende fokus på brukervennlighet har negative konsekvenser både for brukervennlighet og ressursbruk.

Krav til **kvalitet og sikkerhet** varierer blant aktørene i ID-forvaltningen og er ikke enhetlig på tvers av ID-forvaltningen. Det eksisterer begrenset med statistikk og nøkkeltall som dokumenterer samlede samfunnsmessige kostnader av feil og misbruk av ID. Samtidig er det en omforent forståelse av at det er store mørketall. Leverandøren har gjennom kartleggingen anskueliggjort at de reelle samfunnsmessige kostnadene er betydelig høyere enn i faktisk avdekt misbruk relatert til ID. Svakheter i ulike deler av ID-prosessen er en direkte årsak til sikkerhetsutfordringene, hvor spesielt tildelingen

av identitetsnummer, omfanget av fysiske ID-bevis, eksisterende tilnærming til eID og biometri er viktige problemstillinger.

Et stort antall virksomheter har myndighet til å rekvirere **d-nummer,** noe som er en betydelig kilde til feil og misbruk. Rekvirenter har individuelle rutiner og retningslinjer for en aktivitet av lik karakter, hvilket fører til varierende kvalitet og sikkerhet i prosessen. Sikkerhetsutfordringer gir seg blant annet utslag i muligheter for at personer kan registreres med flere identitetsnummer i Folkeregistret. Ansvars- og rollefordelingen mellom Skatteetaten som folkeregistermyndighet og rekvirenter oppleves også som uklar og fører til at det rekvireres et unødvendig høyt antall identitetsnummer som blir stående med status «ikke-kontrollert» i Folkeregisteret. Mange rekvirenter gir positive utslag for brukervennligheten, mens sikkerheten ikke blir ivaretatt tilstrekkelig. Ressursbruk vurderes å være relativ høy med dagens løsning og understøttes av mangel på standardisering i oppgaveløsning fordelt på mange aktører.

Det er lav bevissthet rundt hvilke **fysiske ID-bevis** som er gyldige både for brukere og hos tjenesteytere. En rekke aktører utsteder ulike ID-bevis som oppfattes som gyldige, hvor det i regelverket ikke er entydig definert hva som utgjør gyldig legitimasjon. Det er i tillegg manglende samsvar mellom krav til kvalitet og/eller sikkerhet for opprettelse av ID-bevis og de tjenester og/eller ytelser ID-beviset gir tilgang til. Det finnes ingen bruk av felles standarder eller retningslinjer for kvalitets- eller kompetansekrav for kontroll av ID-bevis på tvers av sektorer. Dette blir spesielt en utfordring når ett ID-bevis med lav notoritet og svak ID-kontroll kan benyttes til å tilegne seg nye ID-bevis med høy notoritet. Videre er det en utfordring at flere aktører som gjennomfører ID-kontroll mangler kunnskap og hjemler til å identifisere og beslaglegge falske ID-bevis og således begrense sirkulering av disse i samfunnet. Muligheten for å tilegne seg ulike ID-bevis kan isolert gi en positiv effekt på brukeropplevelsen, men blir trukket ned på bakgrunn av usikkerheten rundt hvilke ID-bevis som faktisk er gyldige. Ressursbruk og sikkerhet vurderes som negativt påvirket av et stort antall utstedere og utydelige krav til gyldig legitimasjon.

Til tross for at dagens løsninger for digital autentisering med eID gjennom ID-porten fungerer svært godt og blir godt mottatt i samfunnet for øvrig er det enkelte utfordringer. Eksisterende **eID-løsninger** med høyeste sikkerhetsnivå er private og det offentlige vil først kunne tilby en eID på høyeste sikkerhetsnivå ved innføring av nasjonalt ID-kort med eID. Dagens løsning gjør at utstedelsen av eID på høyeste sikkerhetsnivå, og dermed senere autentiseringer ved bruk, utelukkende belager seg på ID-kontrollen gjennomført av private tilbydere av eID. Regelverket for utstedelse og ID-kontroll ved fysisk oppmøte følges, men forutsetningene til å sjekke eksempelvis doble identiteter og til å inneha høy kompetanse på ID-kontroll er begrenset. I tillegg ligger det en risiko i at BankID er såpass dominerende i markedet, slik at et potensielt eierskifte av BankID eller problemer med tilgjengeligheten til tjenesten kan være utfordrende. Videre vil enkelte brukergrupper falle utenfor med dagens system for eID. Dagens tilnærming til eID har i all hovedsak sikkerhetsmessige utfordringer.

Manglende opptak, lagring og bruk av **biometri** (ansikt og fingeravtrykk) på tvers av de ulike brukergruppene påvirker videre kvaliteten i ID-forvaltningen negativt. Spesielt er opptaket av biometri for EØS-borgere fraværende. Kontroll av biometri vil kunne gi betydelige fordeler og tette sikkerhetshull gjennom blant annet å redusere handlingsrommet for de som opptrer med flere identiteter i Folkeregistret og urettmessig mottar tjenester og ytelser. Bruk av biometri er likevel omstridt da hensynet til personvern står sterkt. Personvernutfordringene synes å bli vektlagt mer enn personverngevinstene og kan være til hinder for en effektiv ID-forvaltning. I et brukerperspektiv kan manglende bruk av biometri ses på som både positivt og negativt,

avhengig av ståsted i personvernspørsmålet. Hva gjelder sikkerhet og ressursbruk er konsekvensen negativ.

Samlet **ressursbruk** var i underkant av 1,5 mrd. kroner og i underkant av 1 200 årsverk i 2018. Aktørenes bevissthet knyttet til ressursbruk for ID-relatert arbeid vurderes som lav. De fleste aktører har utfordringer med å gi en oversikt over påløpte kostnader for ID på noe annet enn svært overordnet nivå for et gitt år. Dette er riktignok ikke overraskende da ID-området i liten grad er styrt helhetlig eller av hver aktør. Dette medfører videre at analyser av kostnadsfordeling på henholdsvis fastsettelse, registrering, utstedelse og ID-kontroll er krevende, det samme er tilfelle for kostnadsutviklingen. Det er utfordrende å entydig konkludere hva nivået i ressurseffektiviteten i ID-forvaltningen er når det ikke eksisterer enhetlige mål eller måltall for området. Motstridende indikasjoner på utvikling i ressurseffektivitet innen ulike saksområder og manglende enhetlig styring vanskeliggjør konklusjon om utviklingen i ressurseffektivitet.

8.4 Oppsummerende vurderinger tilknyttet sikkerhet, brukervennlighet og ressursbruk

Det er flere styrker ved dagens ID-forvaltning, men også betydelige utfordringer som allerede skissert ovenfor. Svak styringsinformasjon innen både sikkerhet, brukervennlighet og ressursbruk i ID-forvaltningen tydeliggjør behov for forbedring. Nåsituasjonsvurderingene viser at dagens system og planlagte tiltak ikke sikrer det grunnleggende behovet både forvaltningen og individet har for å etablere en kobling mellom fysisk person og identitet i Norge. En identitet, uavhengig av om identitetsnummeret er et fødselsnummer eller et d-nummer, vil først kunne låses ved knytning til sentralt lagret biometri.

Under oppsummerer leverandøren de mest sentrale styrkene og utfordringene opp mot vurderingskriteriene som er lagt til grunn for områdegjennomgangen.

Sikkerhet er svært sentralt i ID-forvaltningen. Dokumentasjonen på området er til dels svak, men nåsituasjonsanalysen peker i retning av flere utfordringer, herunder lav grad av strategisk styring og gjennomføringsevne, stort omfang av fysiske ID-bevis, ingen enhetlig prosess for tildeling av identitetsnummer, manglende opptak, lagring og bruk av biometri samt dagens tilnærming til eID. Leverandøren vurderer med dette sikkerheten i dagens ID-forvaltning som svak, men at pågående, ikke ferdigstilte initiativ vil styrke denne betydelig.

På lik linje som for sikkerhet er lav grad av strategisk styring og gjennomføringsevne en utfordring for **brukervennlighet** i ID-forvaltningen. Utover dette er det flere områder som oppleves å ha positive fortegn ut fra et brukerperspektiv. Dette gjelder særlig dagens eID-løsninger. Brukervennligheten i dagens ID-forvaltning vurderes av leverandøren som tilfredsstillende til god, men at pågående, ikke ferdigstilte initiativ vil svekke brukervennligheten. Betydelig økning i krav til fysiske oppmøter i et livsperspektiv er avgjørende for denne vurderingen.

Det er krevende å vurdere ressurseffektiviteten samlet for ID-forvaltningen, når det ikke er definert entydige mål for verken brukervennlighet, sikkerhet eller ressursbruk. Mottatt data for **ressursbruk** er av varierende kvalitet og bevisstheten knyttet til ID-relatert arbeid er lav, utfordringer knyttet til svak strategisk styring og gjennomføringsevne kan være medvirkende årsaker til dette. Stort omfang av fysiske ID-bevis, mange rekvirenter av d-nummer samt manglende opptak, lagring og bruk av biometri er andre utfordringer som bidrar til et relativt høyt ressursbruk. Folkeregistret som kilde til grunndata i ID-relatert arbeid utgjør videre et robust fundament og

vurderes å være ressurseffektivt. Leverandøren vurderer at det sannsynligvis er noe å hente ved å øke ressurseffektiviteten på tvers av ID-forvaltningen. Samtidig vil pågående, ikke ferdigstilte initiativ medføre økt ressursbruk noe som trolig er nødvendig for å styrke sikkerheten.

Det er en utfordring at ID-forvaltningen nærmest per definisjon handler om å behandle personopplysninger. Personopplysningsregelverket gir rom for å behandle og dele personopplysninger. Samtidig er det klart at noe av poenget med regelverket er at det ikke skal være fri flyt av personopplysninger. Aktørenes mulighet til å innhente, behandle og dele personopplysninger seg imellom er dermed begrenset. Dette får i noen grad negative konsekvenser for både effektiviteten, brukervennligheten og sikkerheten i ID-forvaltningen.

8.5 Behov for forbedring og alternative løsninger

Spesielt vurderer leverandøren at dagens styring er en rotårsak til mange av de viktigste utfordringene som er identifisert. Vesentlige forbedringer av en svakt dokumentert sikkerhet, brukervennlighet og til dels ressursbruk er særdeles krevende uten å forbedre styringen. På bakgrunn av dette har leverandøren vurdert trender og utarbeidet en skisse til mål for ID-forvaltningen. I tillegg er seks tema som adresserer utfordringene skissert ovenfor drøftet med ulike alternativ i de resterende kapitlene i del 3:

- Fysiske ID-bevis og utbredelse av nasjonalt ID-kort
- eID
- Identitetsnummer i Folkeregisteret
- Biometri
- Fysiske oppmøter
- Styring og struktur

9 Viktigste utviklingstrekk og målbilde

9.1 Trender med konsekvenser for ID-forvaltningen

ID-relaterte aktiviteter og ID-forvaltningen har vært i utvikling de siste ti årene. Eksempelvis har eID fått omfattende utbredelse, det er vedtatt implementering av nasjonale ID-kort og omfanget av asylsøkere med behov for ID-fastsettelse har variert sterkt. En rekke trender og utviklingstrekk kan ha påvirkning på ID-forvaltningen i et tiårs perspektiv. For å vurdere alternativer for økt sikkerhet, økt brukervennlighet og redusert ressursbruk er konsekvensene av trender for ID-forvaltningen viktig.

Leverandøren har gjennomført en kartlegging basert på et utvalg av nasjonale og internasjonale kilder med formål om å utarbeide en oversikt over viktige trender med direkte konsekvenser for ID-forvaltningen.[440] I kartleggingsarbeidet har leverandøren benyttet tre overordnede kategorier: Teknologisk utvikling, politisk utvikling og samfunnsutvikling. Totalt ni trender har blitt identifisert og fordelt på nevnte kategorier. Videre har leverandøren kort beskrevet de viktigste konsekvensene av trendene for ID-forvaltningen. Leverandørens vurdering av usikkerhet i utfallsrommet for trenden og vurdering av viktighetsgrad for ID-forvaltningen er spesifisert i lav, medium og høy. Omfang av flyktninger er et eksempel på en trend med høy usikkerhet i utfallsrommet.

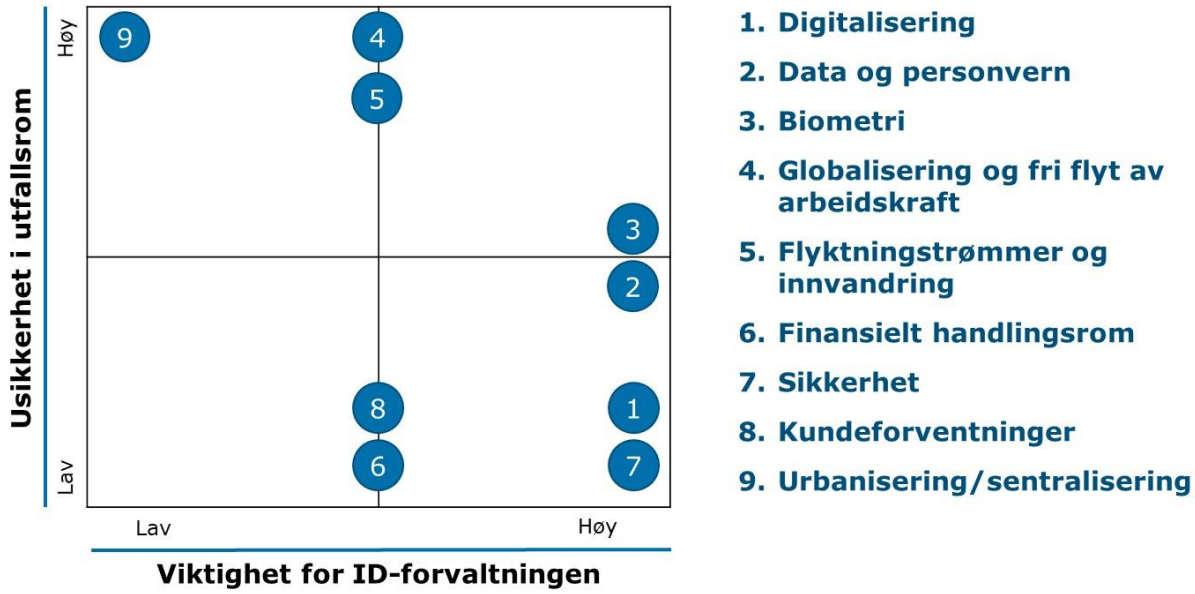
I tabellen under følger de trender leverandøren vurderer at har konsekvenser for fremtidig ID-forvaltning i et tiårs perspektiv. Leverandøren erkjenner at enkelte trender til dels kan høre hjemme i flere trendkategorier, samt at visse trender vil kunne motvirke hverandre. Trender og samfunnsutvikling eksempelvis relatert til det grønne skiftet/klimaendringer, økt populisme, aldrende befolkning, nye framvoksende marked og ressursbegrensninger er vurdert som indirekte for ID-forvaltningen og er ikke nærmere beskrevet under. Felles for mange av trendene er bakenforliggende drivere tilknyttet befolkningsvekst, klimaendringer, økonomisk vekst og teknologisk utvikling.

[440] *Kildegrunnlag: NAV, «Omverdenanalyse», 2019; FIN, «Perspektivmeldingen», 2017; MIT Sloan Review, «The World in 2030: Nine megatrends to watch», 2019 ; Politiet, «Omverdenanalyse», 2015; OECD, «Embracing Innovation in Government – Global Trends», 2018; KMD, «Digitaliseringsstrategi for Offentlig Sektor», 2019; Politiet, «Årsrapport», 2018; Verdensbanken, «World Development Indicators», 2019; PST, «Trusselvurdering», 2019; SSB, «Landbakgrunn for innvandrere i Norge, 2019; UDI, «Statistikk om innvandring», 2019; SSB, «Visualisering av innvandringsbakgrunner», 2019; SSB, «Innvandrere og norskfødte med innvandrerforeldre», 2019, KMD, «Scenarioer for offentlig sektor i 2040», 2019*

Trendkategori	Trend	Konsekvenser og relasjon til ID-forvaltningen	Usikkerhet utfallsrom	Viktighet ID-forvaltningen
Teknologisk utvikling	**Digitalisering** Økt grad av automatisering og selvbetjeningsløsninger Økt grad av mobile og integrerte løsninger	Økt andel digitale tjenester/selvbetjeningsløsninger med eID/ autentiseringer gjennom ID-porten Reduksjon i antall brukersteder/tjenestesteder med færre steder å benytte fysiske ID-bevis. Forventet fortsatt reduksjon i antall filialer i bankene som utsteder ID-bevis og antall trafikkstasjoner som utsteder førerkort Endrede kundeforventninger med reduksjon i behov for fysiske ID-bevis	Lav	Høy
Teknologisk utvikling	**Data og personvern** Økende bruk av data Styrket vektlegging av at forbrukeren / borgeren eier sine data	Innsamlet data på personer, produkter og organisasjoner vil vokse eksponentielt ID-data kan kun deles mellom aktører mot samtykke og mer krevende å dele data mellom ulike registre	Medium	Høy
Teknologisk utvikling	**Biometri** Bedre teknologiske forutsetninger for å oppta og lagre biometrisk data Økt bruk av biometri i ID-kontroll av bruker (både i privat og offentlig sektor)	Gir i større grad mulighet til å koble en person til en unik identitet Muliggjør raskere og mer presise ID-kontroller for private og offentlige aktører. Redusert sannsynlighet for misbruk og svindel Gir mer sømløse brukeropplevelser digitalt og for fysisk handel eller tjenester, og en større aksept for bruk av dette (spesielt tilknyttet smarttelefoner) Regulatoriske utfordringer knyttet til opptak og lagring av biometri, samt deling av biometrisk data på tvers av registre	Medium	Høy
Politisk utvikling	**Globalisering og fri flyt av arbeidskraft** Økt proteksjonisme nasjonalt og internasjonalt Reduksjon av mobilitet mellom nasjoner, særlig ift. flyt av arbeidskraft til Norge	Volumet av EØS- og tredjelandsborgere som krever fastlagt identitet reduseres Reduksjon i internasjonalt samarbeid som reduserer mulighetsrommet til grenseoverskridende løsninger (eks. eIDAS-forordningen)	Høy	Medium
Politisk utvikling	**Flyktningstrømmer og innvandring** Redusert ankomst av flyktninger/asylsøkere	Redusert omfang for fastsettelse av ID («hvem du var») Behov for å avdekke falske opphold	Høy	Medium

	Økt andel innvandrerbefolkning og mer heterogen befolkning	Nye former for migrasjon og sakstyper som følge av økt innvandrerbefolkning i Norge		
Samfunnsutvikling	**Finansielt handlingsrom** Eldrebølge og reduserte oljeinntekter gir redusert finansielt handlingsrom Styrket vektlegging av økt produktivitet og effektivitet blant offentlige aktører	Aktørene i ID-forvaltningen må oppnå mer med mindre. Produktivitet fordrer økt grad av digitalisering/ selvbetjeningsløsninger, innovasjon eller offentlig-privat samarbeid Stiller krav til effektiv organisering av ID-forvaltningen; hindre dobbeltarbeid, minimere unødvendige ID-kontroller, effektiv koordinering mellom departement og etater	Lav	Medium
Samfunnsutvikling	**Sikkerhet** Økt vektlegging av et sikkert og trygt samfunn Økt kompleksitet i kriminalitet	Styrket viktighet av sikre ID-bevis Kriminaliteten blir mer kompleks og foregår oftere med bruk av digitale verktøy og på digitale arenaer. Gir et sterkere behov for sikker eID Økt grad av elektroniske grensesnitt og elektronisk lagret informasjon muliggjør andre former, større skala og mer grenseoverskridende kriminell aktivitet enn tidligere. Gir et sterkere behov for sikker eID	Lav	Høy
Samfunnsutvikling	**Kundeforventninger** Raskere endring i kundeforventninger Økt vektlegging av brukeropplevelse fra offentlige aktører (brukervennlighet, digitale grensesnitt)	Krav til ID-aktører for å optimalisere brukeropplevelsen (brukers anskaffelse og benyttelse av ID-bevis), herunder større grad av selvbetjeningsløsninger, lavere brukertid og lavere brukergebyr i et livsløpsperspektiv Gode løsninger fra privat sektor og andre aktører i offentlig sektor setter standarden for brukeropplevelse for ID Forventning om at data avgis en gang og at staten kan benytte denne informasjonen Kunden godtar å gjøre arbeid med registrering og fornyelse av identitetsopplysninger selv i elektroniske grensesnitt om total tidsbruk reduseres	Lav	Medium
Samfunnsutvikling	**Urbanisering/sentralisering** Forflytning av befolkning fra distrikt til byer	Reduksjon i behov for brukersteder/tjenestesteder for utstedelse av fysiske og elektroniske ID-bevis Krevende å opprettholde robuste fagmiljø for aktiviteter tilknyttet utstedelse av ID og ID-kontroll i mindre byer og tettsteder	Høy	Lav

Tabell 22 Leverandørens kartlegging av trender relevante for ID-forvaltningen



Figur 59 Trender i ID-forvaltningen vurdert etter grad av viktighet og usikkerhet

Figuren ovenfor gir et overblikk over identifiserte trender kategorisert etter leverandørens vurdering av viktighet for ID-forvaltningen og grad av usikkerhet i utfallsrommet for trenden. Leverandøren vurderer spesielt at trendene tilknyttet digitalisering, data og personvern, bruk av biometri og sikkerhet vil ha en betydelig påvirkning på ID-forvaltningen i årene som kommer.

For enkelte av trendene skissert over vil innflytelsen på ID-forvaltningen være tilknyttet ulik grad av usikkerhet. Leverandøren vurderer at fortsatt digitalisering, endrede kundeforventninger, redusert finansielt handlingsrom og vektlegging av sikkerhetshensyn med en høy grad av sannsynlighet å ha en betydelig innvirkning på ID-forvaltningen i årene som kommer, dvs. at usikkerheten i utfallsrommet er lav. For digitalisering legger leverandøren til grunn at det vil det være ulik fremvekst og vektlegging av ulike teknologier med tilhørende usikkerhet, mens trenden om fortsatt digitalisering vil bestå.

For andre trender er usikkerheten i utfallsrommet større. Eksempelvis forventes framskritt og adopsjon av løsninger relatert til biometri å ha vesentlig påvirkning. Derimot vil styrken i denne trenden etter leverandørens syn i stor grad være politisk betinget, da biometriens rolle i ID-forvaltningen blant annet vil avhenge av hvilke føringer som legges for opptak, benyttelse og deling av biometrisk informasjon. Videre vil trendene tilknyttet globalisering og fri flyt av arbeidskraft kunne ha betydning for ID-forvaltningen i form av endrede volumer for ankomst av EØS- og tredjelandsborgere til Norge. Det samme gjelder omfang av flyktningestrømmer og innvandring. Spesielt innen fri flyt av arbeidskraft til Norge har den langsiktige trenden historisk vært tiltakende, mens det de siste par årene har vært en reduksjon. Leverandøren vurderer det per dags dato som uklart hvilken retning disse trendene vil ta, og likeledes hvilken effekt det vil ha på identitetsforvaltningen. Viktigheten er vurdert til medium, da det uansett vil være et omfang av arbeidsinnvandrere, flyktninger og innvandrere. Systemer og prosesser uansett må være tilstede for å håndtere dette.

9.2 Skisse til mål for ID-forvaltningen

Med utgangspunkt i leverandørens kartlegging og vurdering av nåsituasjonen i del 2, helhetlige vurderinger av nåsituasjonen i kapittel 8 og relevante trender har leverandøren utarbeidet en skisse til mål for ID-forvaltningen. Først redegjør leverandøren for sin vurdering av forslag til visjon for nasjonal identitetsforvaltning fra tverretatlig koordineringsgruppe for identitetsforvaltning (KoID), før det presenteres en skisse til mål for ID-forvaltningen. Arbeidet med forslag til visjon for nasjonal identitetsforvaltning er redegjort for i kapittel 2.9.5.

9.2.1 Vurdering av forslag til visjon for nasjonal identitetsforvaltning fra KoID

Leverandøren vurderer overordnet at forslaget til visjon for nasjonal ID-forvaltningen innehar mange gode kvaliteter. Det er en god vektlegging av sikkerhet, til dels brukervennlighet, samt at enkelte formuleringer er enkle å forholde seg til. Videre stiller leverandøren seg bak majoriteten av formuleringene og intensjonene lagt til grunn i visjonen. Leverandørens vurdering av forslaget til visjon er i stor grad avhengig av hva visjonen skal benyttes til. Leverandøren ser utfordringer ved forslaget til visjon, spesielt om det skal vurderes opp mot målsetningene i områdegjennomgangen (økt sikkerhet, redusert ressursbruk og økt brukervennlighet) eller behandles politisk. Visjonen for ID-forvaltningen ved KoID er etter leverandørens oppfatning for snevert definert for å styre ID-forvaltningen i Norge. Dette er nærmere redegjort for under.

Begreper og terminologi

Formål, hovedmål og delmål etableres av ansvarlig departement for underliggende virksomheter[441]. Et formål benyttes for å gi et bilde av hvorfor en virksomhet er til og hoved- og delmål sier noe om hva som skal oppnås innen ulike områder av en virksomhet. En visjon benyttes av enkelte virksomheter for å vise retning for hvordan en virksomhet skal realisere sitt formål. Det rapporteres på hovedmål og evt. delmål gjennom Prop. 1 S spesielt for virksomheter, men også for tverrgående politikkområder i offentlig forvaltning. Leverandøren erfarer at begrepsbruk tilknyttet hoved- og delmål er vanligst i offentlig sektor, mens begrepsbruk med visjoner og ambisjoner er mindre vanlig. Leverandøren vurderer derfor det som mest hensiktsmessig å benytte hovedmål og delmål for ID-forvaltningen.

Hva som ønskes oppnådd og helhetlig vektlegging

I henhold til Direktoratet for økonomistyring (DFØ) skal et godt mål beskrive en ønsket tilstand, ønsket effekt eller resultat. Det henvises ofte til at mål skal vise til samfunns- eller brukereffekter som ønskes oppnådd. Videre skal et mål ikke gi en beskrivelse av aktiviteter eller oppgaver. Et mål skal sagt på en annen måte vise til hva man ønsker å *oppnå* innen et politikkområde eller for en virksomhet[442].

Visjonen til KoID viser i varierende grad til hva som ønskes oppnådd av samfunns- og brukereffekter. For enkelte formuleringer, slik som for «*alle med norsk identitetsnummer skal oppleve trygghet for at ingen andre skal kunne overta identiteten*» vises det godt til ønsket brukereffekt. Samfunnseffekter er relativt lite dekket i visjonen etter leverandørens oppfatning. Det vises i liten grad til

[441] Direktoratet for økonomistyring, «Veileder i mål og resultatstyring i staten», 2010 og Direktoratet for økonomistyring, «Veileder i etatsstyring», 2011
[442] Direktoratet for økonomistyring, «Veileder i mål og resultatstyring i staten», 2010 og Direktoratet for økonomistyring, «Veileder i etatsstyring», 2011

samfunnseffekten av god identitetsforvaltningsforvaltning, eksempelvis for kriminalitetsbekjempelse som helhet, betydning for samfunnssikkerheten som helhet med videre.

Områdegjennomgangens målsetninger er som nevnt knyttet til økt sikkerhet, redusert ressursbruk og økt brukervennlighet. Leverandøren vurderer at forslaget til visjon for KoID ikke dekker kostnadseffektivitet og kun i begrenset grad dekker brukervennlighet utover perspektiv relatert til misbruk og trygghet. Sagt på en annen måte kan visjonen for KoID adresseres med betydelig økt ressursbruk og redusert brukervennlighet. Leverandøren vurderer at det er lite hensiktsmessig at kun hovedsakelig sikkerhet, i et relativ snevert perspektiv, er vektlagt.

Enkelhet i formuleringer

Flere av formuleringene i visjonen for KoID er enkle å forholde seg til og forstå. Dette gjelder spesielt «*En person, en identitet i Norge*». Enkelte deler av visjonen er riktignok særdeles kompleks og utydelig formulert, dette gjelder spesielt «*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*». Leverandøren vurderer at slike komplekse formuleringer er krevende å kommunisere, spesielt om formuleringene skal behandles politisk.

9.2.2 Leverandørens skisse til mål for ID-forvaltningen

Med utgangspunkt i leverandørens helhetlige vurderinger av nåsituasjonen, relevante trender og vurdering av forslag til visjon fra KoID har leverandøren utarbeidet en skisse til mål for ID-forvaltningen. Skissen til mål benyttes som underlag for vurdering av alternativ for økt sikkerhet, redusert ressursbruk og økt brukervennlighet for ID-forvaltningen i del 3 av områdegjennomgangen. Skissen bygger på struktur og tilnærming for mål og resultatstyring i staten, samt bygger videre på forslag til visjon for nasjonal identitetsforvaltning fra KoID.

Visjon: Én person, én identitet i Norge

Hovedmål: Kostnadseffektiv ID-forvaltning som tilrettelegger for et enklere og tryggere samfunn

Delmål:

- *Høy tillit til og trygghet i ID-relaterte aktiviteter*
- *Enkel, brukervennlig og tidsbesparende utstedelse og bruk av fysiske og elektroniske ID-bevis for alle*
- *Offentlige tjenester, ytelser og plikter gis til rett person*
- *Effektiv rollefordeling og ressursbruk*

Under følger en beskrivelse av hva hovedmålet og delmålene betyr.

Kostnadseffektiv ID-forvaltning som tilrettelegger for et enklere og tryggere samfunn
Målsetningen innebærer at ID-forvaltning er en viktig samfunnsoppgave, hvor staten gjennom ID-forvaltningen, skal bidra til et enklere og tryggere samfunn for alle borgere. ID-forvaltningen skal sikre tilgang til grunnleggende individuelle rettigheter og deltakelse i samfunnet og bidra til riktig tildeling av tjenester, ytelser og plikter. ID-forvaltningen skal utøves kostnadseffektivt i et samfunnsmessig perspektiv. Måloppnåelse fra delmålene er med å sannsynliggjøre måloppnåelse på hovedmålet.

Høy tillit til og trygghet i ID-relaterte aktiviteter
Målsetningen innebærer at alle med norsk identitetsnummer skal oppleve trygghet for at ingen andre skal kunne overta identiteten. Målsetningen medfører videre at ingen med norsk identitetsnummer skal utsettes for ID-tyveri og at ingen skal operere med falske eller fiktive identiteter i Norge. Tilliten til offentlig utstedte «sterke ID-bevis» skal være høy. Delmålet nås hvis borgere med norsk identitetsnummer opplever høy tillit til og trygghet til ID-bevis, ID-kontrollaktiviteter og det offentliges forvaltning av personopplysninger.

Enkel, brukervennlig og tidsbesparende utstedelse og bruk av fysiske og elektroniske ID-bevis for alle
Målsetningen innebærer at utstedelse og fornyelse av ID-bevis skal være enkel og brukervennlig for alle. Det skal være enkelt å dokumentere sin identitet for å kunne delta i samfunnet og få tilgang til grunnleggende tjenester og ytelser. Dette medfører at utstedelse og fornyelse av fysiske og elektroniske ID-bevis har et begrenset krav til oppmøte med tilhørende effektiv saksbehandling. Antall ID-bevis som gir tilgang til plikter, tjenester og ytelser er begrenset, og det er tydelig hva det offentlige aksepterer av ID-bevis. Målsetningen innebærer videre at digital pålogging for offentlige tjenester og ytelser er pålitelig, enkel, brukervennlig og tidseffektiv. Delmålet nås hvis borgere har høy tilfredshet ved ID-bevis og samlet krav til oppmøte er begrenset.

Offentlige tjenester, ytelser og plikter gis til rett person
Målsetningen innebærer at grunnleggende individuelle rettigheter og deltakelse i samfunnet med tilhørende plikter, tjenester og ytelser gis til rett person. Dette betyr at enhver som er tildelt et norsk identitetsnummer skal gis mulighet til å dokumentere eierskapet til identitetsnummeret fysisk og digitalt. Delmålet nås om omfanget av feil og misbruk relatert til identitetsforvaltningen reduseres.

Effektiv rollefordeling og ressursbruk
Målsetningen innebærer at staten styrer og organiserer ID-forvaltningen med klare roller og ansvar mellom aktørene i ID-forvaltningen, samt at øvrige mål nås på en kostnadseffektiv måte. Delmålet nås ved økt kostnadseffektivitet i ID-forvaltningen.

10 Vurdering av alternativer knyttet til fysiske ID-bevis og utbredelse av nasjonalt ID-kort

10.1 Oppsummering vurdering nåsituasjonen

Følgende kapittel vurderer alternativer knyttet til fysiske ID-bevis samt utrulling av nasjonalt ID-kort. For leverandørens vurderinger knyttet til nasjonal eID vises det til kapittel 11.

Det ble utstedt ca. 1,2 millioner fysiske ID-bevis i Norge i 2018 (se kapittel 2.8.1). Som beskrevet i kapittel 5 kan brukere i dag legitimere seg med en rekke ulike ID-bevis, både for å få tilgang til andre ID-bevis samt for å få tilgang til ulike tjenester og ytelser. Fra kapittel 4 fremkommer det at dokumentasjons- og legitimasjonskrav for ulike ID-bevis og ulike tjenester og ytelser reguleres av flere forskjellige lover og forskrifter. Følgelig vil det variere etter det enkelte regelverk hva som regnes og benyttes som gyldig legitimasjon. Dagens regulering inneholder ikke en entydig definisjon av gyldig legitimasjon.

Et viktig funn fra kapittel 3 om struktur og organisering er at ID-forvaltningen fremstår som fragmentert, og at det på området ikke er et departement eller underliggende virksomhet som beslutter hvilke ID-bevis som skal anses gyldige på tvers. Kapittelet om kvalitet og sikkerhet belyser videre at sikkerheten tilknyttet utstedelsen av ulike ID-bevis er svært varierende. Det trekkes frem som et potensielt sikkerhetshull at fysiske ID-bevis utstedt på bakgrunn av en mindre sterk ID-kontroll i mange tilfeller fungerer som gyldig ID-bevis for å få utstedt andre og sterkere ID-bevis. Det fremkommer videre at kompetansen rundt håndtering av falske fysiske ID-bevis er mangelfull blant enkelte aktører leverandøren har vært i samtaler med.

Førerkort og bankkort med bilde aksepteres som gyldige ID-bevis

Det fremkommer av nåsituasjonsanalysen at det i tillegg til pass er mulig å fremvise førerkort eller bankkort med bilde som gyldig legitimasjon i en rekke tilfeller. Selv om det på nåværende tidspunkt ikke eksisterer noe lovfestet krav om hva som utgjør gyldig ID-bevis i Norge er det tydelig at førerkort og bankkort med bilde til en viss grad fyller en slik rolle. Både banknæringen ved Finans Norge og SVV har uttalt seg positivt til et fremtidig scenario der bankkortets og førerkortets status som gyldig ID-bevis begrenses, da både førerkort og bankkort med bilde utstedes på bakgrunn av andre formål. Flere norske banker velger i dag å kun utstede bankkort uten bilde. Eksempelvis er leverandøren kjent med at Eika Gruppen har oppfordret sine banker til å avslutte bruken av bankkort med bilde, og anslår omløpet av bankkort med bilde til å være en svært lav andel av gruppens totale utstedte kort (< 5 prosent).[443] Økt digitalisering, slik overordnet dekket i kapittel 9, med mer mobile og integrerte løsninger vil trolig også på sikt redusere omfanget av bankkort generelt sett.

Erfaringer fra andre land med nasjonale ID-kort

Norge er ett av kun fire EU-/EØS-land som ikke utsteder nasjonale ID-kort. Mange nasjonale ID-kort utstedt i Europa er også vedtatt obligatorisk for personer med statsborgerskap i utstederlandet. I enkelte tilfeller er også nasjonalt ID-kort gjort obligatorisk for utenlandske borgere med en viss tilknytning til utstederlandet (eksempelvis Estland). De fleste land globalt utsteder også nasjonalt ID-kort, hvor flere har lovfestet krav til obligatorisk anskaffelse.[444]

[443] Informasjon forelagt leverandøren fra Eika Gruppen, 30.05.2019
[444] Lovdata, «Forskrift om utlendingers adgang til riket og deres opphold her (utlendingsforskriften)», vedlegg 4, 15.10.2009

Sverige er blant landene som utsteder nasjonale ID-kort, men det er ikke obligatorisk for svenske borgere å anskaffe kortet. Andre ID-kort som i stor grad aksepteres som gyldig legitimasjon er førerkort, SIS-merket ID-kort og ID-kort utstedt av Skatteverket (*folkbokförda*). I en nylig publisert utredning om nasjonale ID-kort foreslås det å etablere et prinsipp om at det nye nasjonale ID-kortet, sammen med pass, skal utgjøre eneste gyldige fysisk statlig utstedte ID-bevis i Sverige.[445] Fra 2007 har borgertjenesten i Danmark utstedt et nasjonalt ID-kort kjent som «legitimasjonskort». Utover dette benyttes dansk førerkort og pass som gyldige ID-bevis. Storbritannia utsteder ikke et nasjonalt ID-kort, men baserer seg på pass, førerkort og «Proof of Age Standards Scheme» (forkortes *PASS)* som allment akseptert gyldig legitimasjon.

Leverandøren er gjort kjent med at EU arbeider med en ny forordning for nasjonale ID-kort og oppholdsdokumenter om felles krav på tvers av EU-land[446]. Europaparlamentet og Europarådet ble i februar 2019 enige om å øke sikkerhetskravene til nasjonale ID-kort.[447]

Leverandørens vurdering av viktigste utfordringer ved dagens situasjon

Det er en vedvarende utfordring at utstedelse av nasjonalt ID-kort har vært gjenstand for kontinuerlige forsinkelser over lang tid. Flere forbedringsprosesser som pågår i parallell (jf. kapittel 2.9 om «pågående arbeid»), herunder arbeidet med «unik» og modernisering av Folkeregisteret, innehar vesentlige avhengigheter mot arbeidet i politiets NPID prosjekt. Det anses videre som utfordrende at det ikke foreligger en fullstendig og detaljert utbredelsesstrategi for nasjonalt ID-kort, selv etter lang tids forberedelser og utredninger. Utfordringen må ses i sammenheng med at mange av ID-kortets samfunnsmessige gevinster er nært knyttet opp mot utbredelse i befolkningen.

Slik beskrevet i kapittel 5.1.2, 5.1.3 og 6.2.5 er det en sikkerhetsmessig utfordring at krav til fremlagt legitimasjon varierer, både for tilgang til tjenester og ytelser samt for utstedelse av ulike ID-bevis. Herunder er det en utfordring at flere fysiske ID-bevis utstedt på bakgrunn av en mindre sterk ID-kontroll i mange tilfeller fungerer som gyldig ID-bevis for å få utstedt andre og sterkere ID-bevis. Det anses også som problematisk at det ikke foreligger noen tydelige retningslinjer på tvers for hvilke ID-bevis som blir ansett som gyldig legitimasjon.

Utover leverandørens liste over ID-bevis (jf. kapittel 2.3) eksisterer det svært mange ID-bevis i Norge i dag, med varierende grad av formål, utbredelse og sikkerhet i utstedelse. Antallet ulike ID-bevis i omløp bidrar til å komplisere bildet for både utstedere og brukere om hvilke ID-bevis som blir regnet, eller bør regnes som gyldige.

Leverandøren registrerer at det for enkelte av de mest benyttede ID-bevisene blir uttalt av utstederne selv at bevisenes rolle som allment anerkjente legitimasjonsdokumenter bør innskrenkes. Dette gjelder spesielt for banknæringen ved Finans Norge (utstedere av bankkort med bilde), og for SVV (utsteder av norsk førerkort). Dette er ikke en utfordring i seg selv, men det anses som problematisk at det er per i dag ikke eksisterer et ID-bevis i Norge hvis hovedformål er identifikasjon. Det er en utfordring at de fysiske ID-bevisene som er mest utbredt i dag og som benyttes hyppigst ved legitimering har andre primærformål.

[445] SOU 2019:14, «Ett säkert statligt ID-kort – med e-legitimation», 2019
[446] Europalov, «Fri bevegelse av personer: styrket sikkerhet av ID-kort og oppholdsdokumenter», 2019
[447] Europarådet, «Better security for ID documents: Council Presidency and European Parliament reach provisional agreement», 2019

Vurdering av planlagt innføring av nasjonalt ID-kort

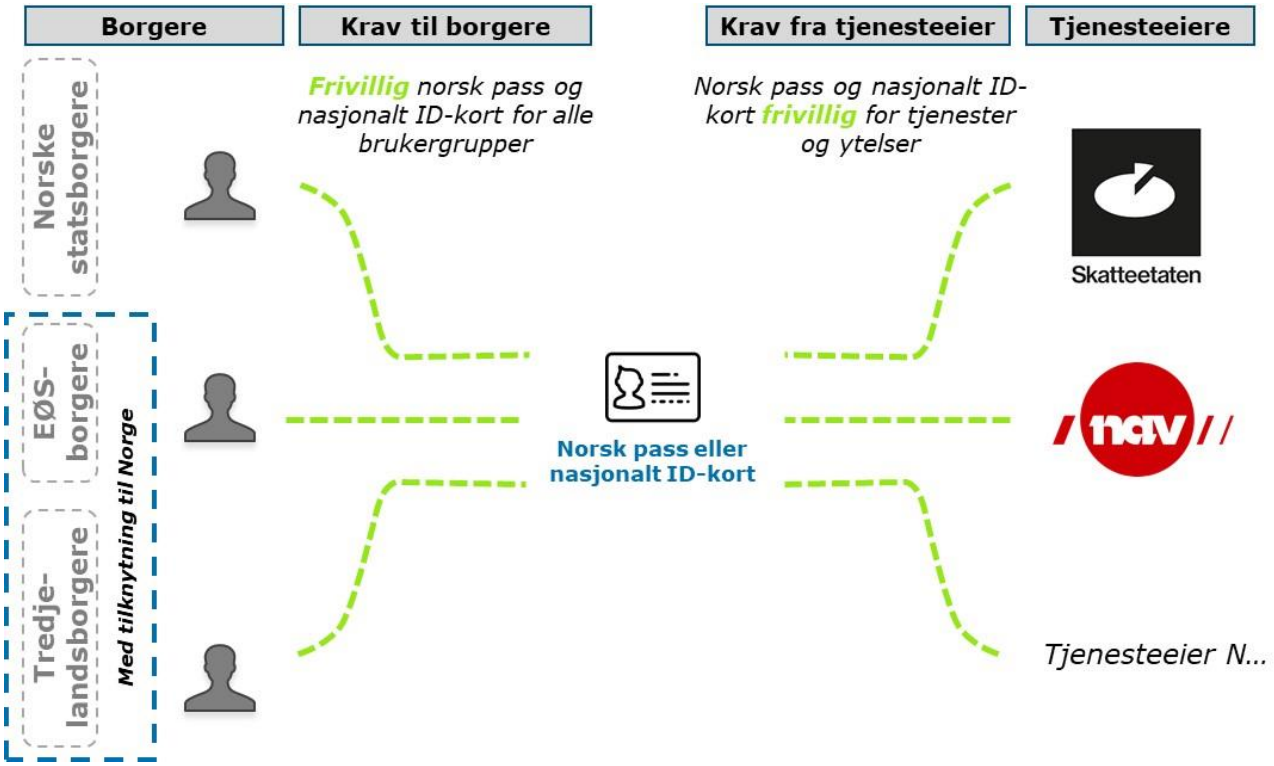
Status for planlagt innføring av nasjonalt ID-kort er tidligere blitt omtalt i kapittel 2.9.1. Leverandørens overordnede vurdering av utrullingen slik planene foreligger fremkommer i det følgende.

En styrke i utstedelsen av det nasjonale ID-kortet ligger i at både norske og på sikt utenlandske borgere gis muligheten til å få et sterkt ID-bevis i et praktisk «lommebok-format». Selv ved frivillig utrulling vil nasjonalt ID-kort ha verdi for brukergrupper som ikke kvalifiserer til norsk pass, men som nå gis muligheten til å anskaffe et sikkert ID-bevis. Generelt anses det som en styrke at nasjonalt ID-kort bidrar til å øke andelen av sikre ID-bevis i omløp, og vil kunne ha svært positiv innvirkning for blant annet bekjempelse av arbeidslivskriminalitet og økt sikkerhet i utstedelse av tjenester og ytelser. Videre vil utstedelse av nasjonalt ID-kort bidra til å bygge opp under status «unik» i Folkeregisteret. Det anses også som en styrke ved nåværende plan at utstedelsen ikke bryter med frivillighetsprinsippet for noen brukergrupper.

Flere av styrkene nevnt over vil likevel være nært knyttet opp mot ID-kortets grad av utbredelse. Det anses derfor som en svakhet ved dagens plan, basert på frivillighetsprinsippet, at det vil være en vedvarende risiko for lav utbredelse av nasjonalt ID-kort i befolkningen. Usikkerheten ligger i om bruker vil anse behovet for et nytt ID-bevis som stort nok til at vedkommende er villig til å betale et betydelig gebyr for å anskaffe det, all den tid majoriteten av brukerne har andre ID-bevis som gjennomgående aksepteres som gyldige. Undersøkelser gjennomført av POD og Difi i 2016 indikerer dog at etterspørselen etter nasjonalt ID-kort vil være tilstrekkelig til å sikre en nødvendig utbredelse.[448] Leverandøren anser det likevel som mulig at utbredelsen av nasjonalt ID-kort blir lavere enn forespeilet av politiet, dersom det ikke stilles krav til anskaffelse. Dette har også blitt påpekt i flere rapporter som leverandøren har blitt forelagt (herunder *«Oppfølging av oppdrag 053»* samt *«Helhetlig ansvar for EØS-borgere»*). Lav utbredelse vil følgelig redusere grunnlaget for å realisere flere av de samfunnsmessige gevinstene nevnt over, herunder ID-kortets bidrag til bekjempelse av arbeidslivskriminalitet samt effekten av biometriopptak som gir status «unik» i Folkeregisteret. Videre foreligger det en sannsynlighet for at lav utbredelse vil kunne medføre enkelte negative konsekvenser for NPID prosjektet som helhet, deriblant lav avkastning på allerede investerte midler.

Figuren under gir en overordnet visualisering av nåværende plan for utrulling av nasjonalt ID-kort, der ID-kortet vil være frivillig å erverve samt at det vil være frivillig for bruker om ID-kortet skal fremvises for tilegnelse av sentrale tjenester og ytelser.

[448] POD, «Beslutningsgrunnlag for eID på nasjonalt ID-kort, delleveranse 4: Insentiver for utbredelse og bruk», 2016



Figur 60 Nåværende plan: Frivillig å anskaffe norsk pass og nasjonalt ID-kort, og frivillig å fremvise for tilgang til tjenester og ytelser

10.2 Drøftinger av alternativer for fysiske ID-bevis og utbredelse av nasjonalt ID-kort

På grunnlag av nåsituasjonen og de største utfordringene dekket over er det i det følgende skissert ulike alternativer for den fremtidige utbredelsen for nasjonalt ID-kort og andre fysiske ID-bevis. Etter leverandørens oppfatning er det risikoen som forbindes med utbredelse av nasjonalt ID-kort som utgjør den sentrale utfordringen ved nåværende planer. Dersom det nasjonale ID-kortet skal utfylle deler av sitt formål om å kunne erstatte mindre sikre ID-bevis vil en høy utbredelse i befolkningen være viktig. Det er leverandørens vurdering at høy utbredelse vanskelig vil kunne sikres uten at det stilles enten krav til fremvisning av norsk pass eller nasjonalt ID-kort for sentrale tjenester og ytelser eller et obligatorisk krav til anskaffelse. Leverandøren drøfter disse mulighetene under som henholdsvis alternativ 1 og 2.

Et øvrig alternativ er også å legge til rette for å styrke kontroll og sikkerhet i utstedelsen av førerkort og bankkort med bilde. Leverandøren anser en slik løsning som lite hensiktsmessig, og har lagt til grunn at implementering av enten alternativ 1 eller alternativ 2 under vil forutsette at førerkort og bankkort med bilde i det videre ikke skal aksepteres som gyldig legitimasjon annet enn til sine formål.

Nasjonalt ID-kort for ulike brukergrupper

Obligatorisk nasjonalt ID-kort, eller et eventuelt krav om legitimering med nasjonalt ID-kort, fordrer at alle borgere som har behov for å legitimere seg overfor norske myndigheter også gis rett til å erverve nasjonalt ID-kort. Spørsmålet om hvilke brukergrupper som vil ha rett til å anskaffe nasjonalt ID-kort står derfor sentralt i begge leverandørens forslag til alternativer. Leverandøren har blitt forelagt betydelig dokumentasjon knyttet til problemstillingen nevnt over. Et sammendrag av sentrale momenter i oversendt materiale gjengis i det følgende.

Hvilke brukergrupper som skal ha rett til nasjonalt ID-kort ble inngående drøftet i forslag til lov om nasjonalt identitetskort.[449] Som utgangspunkt blir det lagt til grunn at alle norske statsborgere vil kunne tilegne seg et nasjonalt ID-kort. Hvilke utenlandske borgere som også vil kunne ha tilgang er gjenstand for nærmere vurdering i forslaget. Der ble det blant annet poengtert at «*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 om det ikke fullt ut kan dokumenteres at denne grunnidentiteten er den korrekte*». Departementet presenterte på daværende tidspunkt en konklusjon om at det kunne være hensiktsmessig å avvente erfaringer med utrulling av ordningen for norske borgere før det det ble åpnet for utenlandske borgere, samt at det ble avsatt mer tid til en mer inngående drøftelse av «*vilkår for blant annet godtgjøring av identitet, statsborgerskap og tilknytning til Norge som må stilles for å sikre at ordningen fungerer etter hensikten*». I utgangspunktet er nasjonalt ID-kort til utlendinger tiltenkt utstedt uten reiserett.

I POD sin oppfølging av oppdrag 053[450] (Nasjonalt ID-kort til utenlandske borgere) anbefales det en politisk vurdering av spørsmålet om offentlige tjenesteeiere kan stille krav om sikker verifisering av identitet med nasjonalt ID-kort med eID for å gi sine ytelser. Det foreslås videre at det legges til grunn i forskriftsbestemmelse at nasjonalt ID-kort kan utstedes til utenlandske borgere som utover å ha lovlig opphold har *tilknytning* til Norge og godtgjør sin identitet. Med tilknytning til Norge menes utenlandsk statsborger som er folkeregistrert som bosatt i Norge, har arbeid av minst seks måneders varighet med daglig arbeidssted i Norge, fast eiendom i Norge, eller på annen måte har tilknytning til Norge og kan sannsynliggjøre et særskilt behov for å legitimere seg med nasjonalt ID-kort. EØS-borgere som er registrert i Norge med hjemmel i utlendingsloven foreslås også å ha rett på nasjonalt ID-kort. POD foreslår videre at utenlandske statsborgere som anses å ha godtgjort sin identitet i tilstrekkelig grad til å få varig opphold, også skal kunne få utstedt nasjonalt ID-kort. Det foreslås at det på et fremtidig tidspunkt utredes videre hvilke løsninger som skal gjelde for utenlandske statsborgere med usikker identitet.

I sin rapport «Helhetlig ansvar for EØS-borgere» fra desember 2018 anbefaler en arbeidsgruppe bestående av POD, SKD og UDI at nasjonalt ID-kort utstedes også til EØS-borgere og tredjelandsborgere. Anbefalingen ble gitt med forbehold om at det nasjonale ID-kortet blir tilbudt *alle* med fødselsnummer og d-nummer som har «lovlig opphold» og «tilknytning til riket», samt at tjenesteeiere har hjemmel til å *kreve* nasjonalt ID-kort som legitimering.

Leverandøren er kjent med at enkelte tjenesteeiere har spørsmålsstilt hensiktsmessigheten i å stille tidsmessig opphold i Norge som forutsetning for å få utstedt nasjonalt ID-kort, blant annet på grunnlag av at unntak i seg selv vil kunne skape nye risikomomenter. Flere tjenesteeiere har videre kommunisert at et eventuelt krav til nasjonalt ID-kort vil måtte gjelde hele befolkningen, samt at det bør kunne stilles krav til nasjonalt ID-kort til EØS-borgere uavhengig av arbeidets varighet.

I PODs plan for innføring av nasjonalt ID-kort fra februar 2019[451] blir det foreslått en egen korttype for utenlandske borgere med usikker identitet. Det blir videre foreslått en gradvis innføring av nasjonalt ID-kort til utlendinger, der nordiske borgere og land med stor arbeidsinnvandring til Norge gis tilgang først, etterfulgt av EØS-borgere og tredjelandsborgere i en senere fase.

[449] JD, «Prop. 66 L (2014-2015), Lov om nasjonalt identitetskort (ID-kortloven)», 2014-2015
[450] POD, «Oppfølging av oppdrag 053 gitt i 2017 – Nasjonalt ID-kort til utenlandske borge», 19.10.2018
[451] POD, «Plan for innføring av nasjonalt ID-kort for utenlandske borgere», 2019

I høringsnotatet om ny pass og ID-kort forskrift fra 2019 fremkommer det at 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.[452]

Uavklarte utfordringer knyttet til utstedelse av nasjonalt ID-kort til EØS- og tredjelandsborgere

Basert på materiale forelagt leverandøren (nærmere beskrevet over) er det generell aksept for at utstedelse av nasjonalt ID-kort til brukere med «lovlig opphold» og «tilknytning til riket» vil være sentralt for å oppfylle ID-kortets formål. Leverandøren vurderer dog at et slikt grunnlag for utstedelse, slik det er skissert p.t., vil forutsette at en rekke uavklarte spørsmål må utredes nærmere. Noen vesentlige eksempler på slike prinsipielle utfordringer gjengis i det følgende (listen anses ikke som uttømmende):

Brukere bosatt i utlandet: En rekke personer vil kunne ha en klar tilknytning til Norge, samt et behov for å legitimere seg overfor norske myndigheter, men vil aldri fysisk oppholde seg i landet. Dette vil blant annet inkludere EØS-borgere i utlandet med krav på ytelser fra NAV, eiere av fast eiendom i Norge som er bosatt i utlandet samt en rekke tilfeller der utenlandske borgere med opphold i utlandet tildeles d-nummer til ulike formål. Som poengtert i kapittel 6.1.2 ble over 50 prosent av d-nummer rekvirert i 2018 tildelt personer som oppholder seg i utlandet.

Brukere med kortere opphold i Norge: Personer med arbeidsopphold i Norge kortere enn 3 til 6 måneder i Norge vil også ha et behov for å legitimere seg overfor norske myndigheter, blant annet i forbindelse med søknad om skattekort.

Utenlandske borgere uten mulighet til å tilstrekkelig «godtgjøre sin identitet»: Tilfellet gjelder blant annet for utenlandske borgere uten varig opphold, og med uavklart eller usikker identitet (herunder asylsøkere og flyktninger). Leverandøren er kjent med at dette utgjør per dags dato utgjør ca. 2.200 utenlandske borgere.

10.2.1 Alternativ 1: Krav om norsk pass eller nasjonalt ID-kort som eneste gyldige fysiske ID-bevis for tilgang til offentlige tjenester og ytelser

Alternativ 1 legger til grunn at det tydeliggjøres i regelverket at enten norsk pass eller norsk nasjonalt ID-kort må fremvises for å få tilgang til sentrale offentlige tjenester og ytelser der det kreves fysisk legitimasjon. Anbefalingen medfører videre at hver enkelt tjenesteeier ikke gis anledning til å selv definere gyldig legitimasjon for tilgang til tjenester eller opprettelse av ulike former for rettighetsbevis. Øvrige ID-bevis, herunder førerkort og bankkort med bilde, samt utenlandske ID-bevis aksepteres dermed ikke lenger som gyldig legitimasjon.

For å kunne kreve fremvisning av norsk pass eller nasjonalt ID-kort for sentrale norske tjenester og ytelser er det en forutsetning at alle brukere med behov for å legitimere seg overfor relevante tjenesteytere gis rett til å anskaffe minst ett av ID-bevisene. Et premiss for alternativet er følgelig at retten til å søke om nasjonalt ID-kort vil måtte omfatte både norske borgere, EØS-borgere og tredjelandsborgere. For norske borgere er denne retten ivaretatt uten videre ved at brukergruppen vil ha rett til anskaffelse av både et norsk pass eller et nasjonalt ID-kort. For utenlandske borgere legges det til grunn for alternativet at nasjonalt ID-kort vil kunne utstedes til alle borgere med lovlig opphold eller tilknytning til Norge (jf. forslag fra POD om forskriftsbestemmelse om

[452] JD, «Høring – ny forskrift om pass og nasjonalt ID-kort», 2019

nasjonalt ID-kort til utenlandske borgere, nærmere beskrevet i det foregående). Leverandøren anerkjenner at det forut for en implementering av alternativ 1 vil måtte utredes nærmere hvilke brukergrupper som vil tilfredsstille et krav om «tilknytning», samt at det må finnes løsninger for borgere som har utfordringer med å godtgjøre sin identitet, borgere på korte opphold i Norge, samt borgere som er bosatt i utlandet og ikke vil ha mulighet til å møte opp fysisk.

Tjenesteeiere hvor det skal stilles krav til fysisk legitimering med norsk pass eller nasjonalt ID-kort er fortrinnsvis SKD og NAV. Virksomhetenes brukere utgjør en svært stor andel av befolkningen, og vil ha spesielt stor effekt i å sikre høy utbredelse av nasjonalt ID-kort. Leverandøren er også kjent med at flere tjenesteeiere som POD har vært i dialog med gjennomgående stiller seg positive til å kunne stille krav om legitimering med nasjonalt ID-kort, såfremt ID-kortet gjøres tilgjengelig for alle tjenesteeiernes brukere. Leverandøren understreker at hvilke tjenester og ytelser med pålagt oppmøte eller fysisk legitimasjon som kan, eller bør, omfattes av legitimasjonskravet ikke har vært gjenstand for nærmere vurdering som del av områdegjennomgangen, og vil måtte inngå i en utredning av alternativet på et senere tidspunkt.

Det må også utredes nærmere hvilke lovendringer som skal gjennomføres for at dette alternativet skal få best mulig virkning. Leverandøren vil her begrense seg til å peke på enkelte mulige løsninger. Som nevnt tidligere varierer det mellom de aktuelle regelverkene hvilke ID-bevis som anses som gyldige. Antakelig vil imidlertid alternativet medføre behov for å endre alle regelverkene som per i dag stiller krav om legitimasjon for å få tilgang til tjenester, ytelser eller ID-bevis. For det første er det ingen regelverk som per i dag tillater nasjonalt ID-kort som legitimasjon. For det andre er det flere regelverk som ikke uttømmende angir hvilken type legitimasjon som kreves.

Det er særlig to alternative løsninger som for leverandøren fremstår som mest nærliggende. Et første alternativ er at det i det enkelte regelverk som gir tilgang til en tjeneste, ytelse eller ID-bevis uttrykkelig stilles krav om at det fremvises norsk pass eller nasjonalt ID-kort. Et andre alternativ er at det i passloven og ID-kortloven fastsettes at henholdsvis norsk pass og nasjonalt ID-kort skal anses for å være gyldig legitimasjon i Norge. Regelverkene som regulerer tilgang til tjenester, ytelser eller ID-bevis kan da stille krav om at det fremvises «gyldig legitimasjon». Endring av passloven og ID-kortloven utelukker ikke gjennomføring av det første alternativet.

Endring av passloven og ID-kortloven i henhold til alternativ to kan få noen flere positive effekter. Å slå fast i lovs form hva som skal anses for å være gyldig legitimasjon i Norge kan ha en virkningsfull symboleffekt. Det blir da allment kjent hvilke ID-bevis man kan ha stor grad av tillit til. Dette kan bidra til å løse opp i dagens uklarheter omkring hva som er gyldig legitimasjon og hvor «sikre» de mange ID-bevisene er. Videre blir det allment kjent at man ikke uten videre kan ha tillit til andre typer ID-bevis.

Leverandørens vurdering av de overordnede styrkene og svakhetene ved alternativ 1 som skissert over er oppsummeres punktvis i det følgende.

Styrker:

- Sikrer økt oppføring som «unik» i Folkeregistret for norske borgere og utenlandske borgere (inkludert EØS-borgere) med tilknytning til Norge

- Bidrar til å øke andelen sikre fysiske ID-bevis i omløp, og på den måten forebygge og bekjempe kriminalitet som involverer falsk eller stjålet identitet

- Fysiske ID-bevis med lavere sikkerhet i utstedelse og bruk vil få en mindre fremtredende rolle som legitimasjonsgrunnlag. Reduserer usikkerheten blant brukere og tjenesteeiere rundt hvilke fysiske ID-bevis som anses som gyldige

- Legger til rette for at tjenesteytere og kontrollorganer i langt større grad vil ha mulighet for å gjennomføre sterk ID-kontroll, inkludert kontroll av biometri og teknisk kontroll av sertifikater

- Svarer ut et uttalt ønske fra tjenesteeiere om å kunne stille sterkere krav til identifikasjon for sine brukere

- Fraviker ikke frivillighetsprinsippet direkte

- Lik praksis for alle med rett til offentlige tjenester og ytelser

- Medfører at både norske statsborgere og utenlandske borgere med tilknytning til Norge gis rett til et identitetsbevis med samme sikkerhetsnivå som pass. Gir den enkelte rett til å kunne dokumentere sin identitet for å kunne delta i samfunnet og få tilgang til grunnleggende tjenester og ytelser

- Styrker den enkeltes personvern gjennom å redusere risiko for ID-tyveri

- Samsvarer i stor grad med konklusjonene fra utredning om nasjonale ID-kort i Sverige, der det anbefales at pass og nasjonale ID-kort utgjør eneste gyldige offentlige utstedte ID-bevis

Svakheter:

- Flytter ansvar for utbredelse til tjenesteeiere

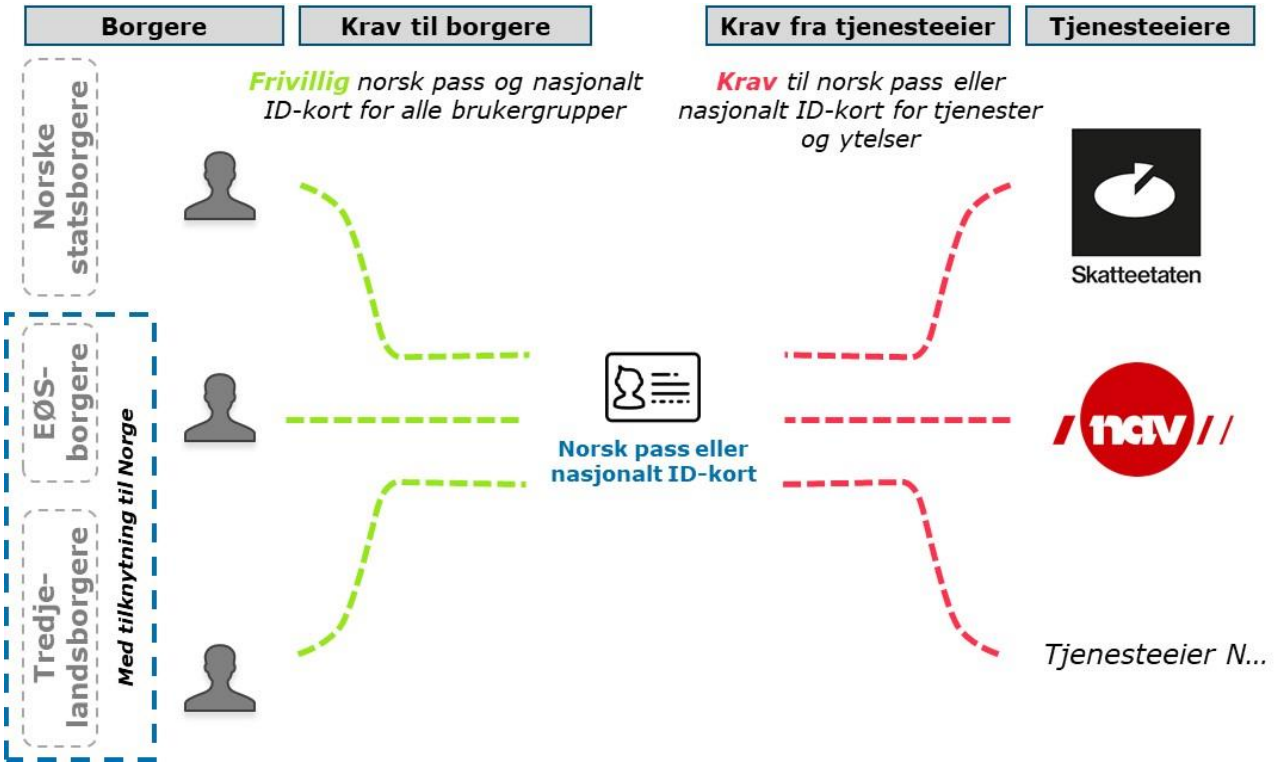
- Potensiell økning i reise- og oppmøtetid for utenlandske borgere samt økt ressursbruk for utstedelse av nasjonalt ID-kort hvert 5 år

- Fordrer nærmere utredning av løsninger for borgere som oppholder seg i utlandet og har tilknytning til Norge, EØS-borgere med korte opphold i Norge samt borgere med redusert mulighet til å tilstrekkelig godtgjøre sin identitet

- Noe mindre utbredelse av nasjonalt ID-kort enn ved å innføre obligatorisk nasjonalt ID-kort. Sikkerhetsmessige gevinster og effekten for status «unik» reduseres derfor også tilsvarende.

- Personvernutfordringer knyttet til opptak og lagring av biometriske opplysninger vil måtte adresseres

Figuren under gir en overordnet visualisering av alternativ 1. Forslaget innebærer at nasjonalt ID-kort og norsk pass vil være frivillig å erverve, men at det reguleres i regelverket at enten norsk pass eller nasjonalt ID-kort må fremvises for tilegnelse av sentrale tjenester og ytelser der det kreves fysisk legitimasjon.



Figur 61 Alternativ 1: Krav til norsk pass eller nasjonalt ID-kort for tilgang til offentlige tjenester og ytelser

10.2.2 Alternativ 2: Obligatorisk pass eller nasjonalt ID-kort for norske og utenlandske borgere

Alternativ 2 innebærer at norske myndigheter fraviker frivillighetsprinsippet og innfører obligatorisk anskaffelse enten av norsk pass eller nasjonalt ID-kort for norske statsborgere og utenlandske borgere[453] med tilknytning til Norge. I likhet med alternativ 1 vil et krav om obligatorisk anskaffelse av norsk pass eller nasjonalt ID-kort bidra til å sikre høy utbredelse av sikre ID-bevis og støtte opp om status «unik» i Folkeregisteret. I alternativet vil tjenesteeiere fortsatt stå fritt til å kreve fremvisning av legitimasjon henhold til sine sikkerhetsbehov. Problemstillingen tilknyttet hvilke utenlandske brukergrupper som vil ha rett til nasjonalt ID-kort vil gjelde begge alternativ. Leverandøren viser her til tilhørende drøfting og vurdering av problemstillingen under alternativ 1. Behov for endringer i regelverket er ikke nærmere drøftet utover beskrivelsen i alternativ 1. I tillegg vil alternativ 2 nødvendiggjøre en nærmere utredning av hvilke konsekvenser et krav til obligatorisk ID-kort vil ha for finansiering av ID-kortet, samt hvilke sanksjoner som vil foreligge dersom kravet ikke overholdes av bruker.

Finansieringsmodell for nasjonalt ID-kort

Det kan oppfattes som uheldig å brukerfinansiere et ID-bevis som vil være obligatorisk for bruker. Dagens finansiering av nasjonalt ID-kort er beskrevet i politiets gebyrmodell, og er i sin helhet basert på at bruker betaler et gebyr ved førstegangsutstedelse og ved fornyelse. Leverandøren vurderer at alternativ 2 potensielt vil nødvendiggjøre en overgang fra gebyrfinansiert ID-kort til bevilgningsfinansiert løsning. Leverandøren er på nåværende tidspunkt ikke kjent med om det foreligger dokumentasjon eller er gjennomført analyser tilknyttet en slik problemstilling.

[453] POD, «Nasjonalt ID-kort til utenlandske borgere», 2017

Sanksjoner for håndheving av krav om nasjonalt ID-kort

Dersom det skal stilles krav til anskaffelse av nasjonalt ID-kort vil det måtte utredes hvilke sanksjoner som skal gjelde for individer som ikke overholder kravet.

Leverandørens vurdering av de overordnede styrkene og svakhetene ved alternativ 2 presenteres under.

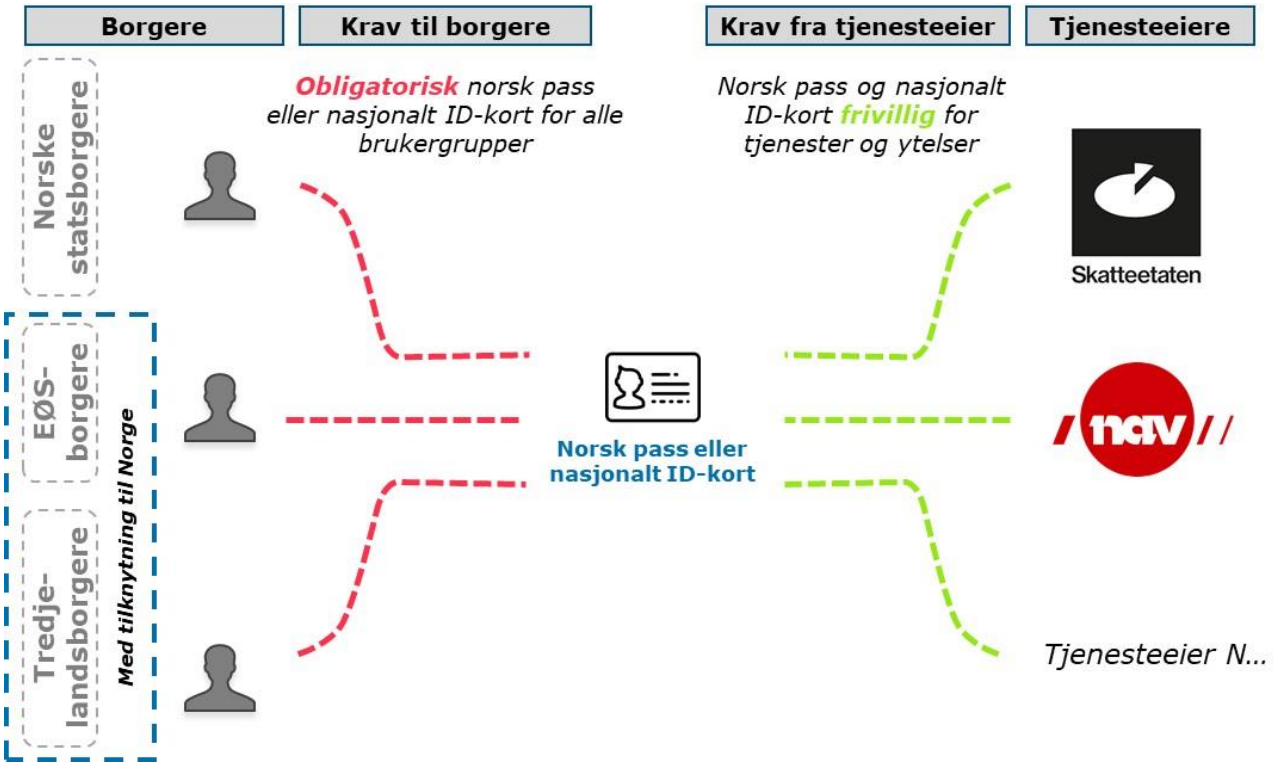
Styrker:

- Sikrer full utbredelse av oppføring som «unik» i Folkeregistret for norske borgere og utenlandske borgere (inkludert EØS-borgere) med tilknytning til Norge
- Alle borgere vil inneha et sikkert ID-bevis, som bidrar til å forebygge og bekjempe kriminalitet hvor falsk eller stjålet identitet er involverer
- ID-bevis med lavere sikkerhet i utstedelse og bruk vil få en mindre fremtredende rolle som legitimasjonsgrunnlag
- Tilrettelegger for at tjenesteytere kan stille krav om fremvisning av sterke ID-bevis dersom dette anses som hensiktsmessig i henhold til sine sikkerhetsbehov
- Legger til rette for at tjenesteytere og kontrollorganer i langt større grad vil ha mulighet for å gjennomføre sterk ID-kontroll, inkludert kontroll av biometri og teknisk kontroll av sertifikater
- Lik praksis for alle med rett til offentlige tjenester og ytelser
- Gir enkelte mulighet til å kunne dokumentere sin identitet for å kunne delta i samfunnet og få tilgang til grunnleggende tjenester og ytelser
- Styrker den enkeltes personvern gjennom å redusere risiko for ID-tyveri

Svakheter:

- Politiske, samt potensielt rettslige utfordringer ved å fravike frivillighetsprinsippet
- Eventuelle sanksjoner mot brukere som ikke anskaffer pass eller nasjonalt ID-kort vil måtte utredes nærmere
- Forutsetter en nærmere vurdering av om nasjonalt ID-kort og pass kan bevilgningsfinansieres og ikke gebyrfinansieres
- Potensiell økning i reise- og oppmøtetid for utenlandske borgere samt økt ressursbruk for utstedelse av nasjonalt ID-kort hvert 5 år
- Fordrer nærmere utredning av løsninger for borgere som oppholder seg i utlandet og har tilknytning til Norge, EØS-borgere med korte opphold i Norge samt borgere med redusert mulighet til å tilstrekkelig godtgjøre sin identitet
- Personvernutfordringer knyttet til opptak og lagring av biometriske opplysninger vil måtte adresseres

Figuren under gir en overordnet visualisering av alternativ 2. Forslaget innebærer at nasjonalt ID-kort og norsk pass vil være obligatorisk å anskaffe, men at det ikke legges videre føringer for hvilke legitimasjonskrav som tjenesteeiere skal stille.



Figur 62 Alternativ 2: Obligatorisk Nasjonalt ID-kort eller pass for alle norske og utenlandske borgere

10.3 Oppsummering av alternativer opp mot sikkerhet, brukervennlighet og ressursbruk

Under har leverandøren overordnet oppsummert drøftingen med tanke på sikkerhet, brukervennlighet og ressursbruk. Tabellen under oppsummerer drøftingen basert på rammeverket for pluss-minusmetoden beskrevet i kapittel 1.3.

Alternativ 1, *krav om norsk pass eller nasjonalt ID-kort som eneste gyldige fysiske ID-bevis for tilgang til offentlige tjenester og ytelser,* vurderes å ha en meget stor positiv konsekvens for sikkerheten gjennom å bidra til å sikre høy utbredelse av det nasjonale ID-kortet. Utbredelse er nøkkelen til den største samfunnsnytten, da økt bruk av sterke identitetsbevis vil sikre den enkeltes vern mot identitetstyveri og bidra til å forebygge og bekjempe annen kriminalitet som involverer falsk eller stjålet identitet. Videre er høy utbredelse for alle med tilknytning til Norge sentralt i å kunne støtte opp om en høy andel med status «unik» i Folkeregisteret. I tillegg vil anbefalingen redusere generell bruk og etablering av mindre sikre fysiske ID-bevis i samfunnet. Sett opp mot brukervennlighet vil brukerne få mindre valgfrihet enn i dag i valg av legitimasjon. EØS-borgere og tredjelandsborgere avkreves også et nytt ID-bevis, men en større andel av befolkningen vil få tilgang til ett sikkert ID-bevis. Det vil være enklere for den enkelte å dokumentere sin identitet for å kunne delta i samfunnet og få tilgang til grunnleggende tjenester og ytelser. Videre bidrar alternativet til å redusere usikkerheten blant brukere og tjenesteeiere rundt hvilke ID-bevis som anses som gyldige. I sum er brukervennligheten overordnet vurdert lik som dagens planer for utstedelse av nasjonalt ID-kort. Alternativet vurderes å ha stor negativ konsekvens for ressursbruk som følge av høy utbredelse og dermed økte kostnader til utstedelse av nasjonalt ID-kort. Utover konsekvensene for sikkerhet, brukervennlighet og

ressursbruk fordrer alternativet en nærmere utredning av løsninger for borgere som oppholder seg i utlandet og har tilknytning til Norge, EØS-borgere med korte opphold i Norge samt borgere med redusert mulighet til å tilstrekkelig godtgjøre sin identitet.

Alternativ 2, *obligatorisk pass eller nasjonalt ID-kort for norske og utenlandske borgere* vurderes tilsvarende som alternativ 1 å ha meget stor positiv konsekvens for sikkerheten i ID-forvaltningen. Obligatorisk norsk pass eller nasjonalt ID-kort vil sikre enda høyere utbredelse av sterke ID-bevis, og vil relativt til alternativ 1 ha tilsvarende større effekt i å støtte opp om status «unik» i Folkeregisteret. Fra et brukervennlighetsperspektiv vil alternativet medføre at tredjelandsborgere og EØS-borgere plikter å anskaffe et nytt ID-bevis. Det vil være enkelt for den enkelte å dokumentere sin identitet for å kunne delta i samfunnet og få tilgang til grunnleggende tjenester og ytelser. Samlet er effekten av alternativet derfor vurdert som lik som dagens planer for utstedelse av nasjonalt ID-kort. Obligatorisk pass eller nasjonalt ID-kort er antatt å medføre stor pågang for utstedelse av nasjonalt ID-kort, spesielt fra utenlandske brukergrupper. Den negative effekten på ressursbruk anses følgelig å være meget stor. Utover konsekvensene for sikkerhet, brukervennlighet og ressursbruk fordrer alternativet en nærmere utredning av de politiske og rettslige utfordringene ved å fravike frivillighetsprinsippet, finansiering av ID-kortet samt eventuelle sanksjoner knyttet til brukere som ikke overholder kravet.

	Sikkerhet	Brukervennlighet	Ressursbruk
Alternativ 1: Krav om norsk pass eller nasjonalt ID-kort som eneste gyldige fysiske ID-bevis for tilgang til offentlige tjenester og ytelser	++++	0	---
Alternativ 2: Obligatorisk norsk pass eller nasjonalt ID-kort for norske og utenlandske borgere	++++	0	----

Tabell 23 Oppsummering av drøfting knyttet til fysiske ID-bevis og utbredelse av nasjonalt ID-kort

11 Vurdering av alternativer knyttet til eID

11.1 Oppsummering vurdering nåsituasjonen

Begrepet eID, funksjon og formål med ID-porten, samt utbredelsen og bruken av ulike eID-er i Norge per dags dato er overordnet beskrevet i kapittel 2.8.2. Pågående arbeid med nasjonal eID er beskrevet i kapittel 2.9.2. I del 2 av rapporten vurderes ulike aspekter ved eID, tilknyttet de fem temaene struktur og styring (kapittel 3), regelverk (kapittel 4), brukertilfredshet (kapittel 5), kvalitet og sikkerhet (kapittel 6) og ressursbruk (kapittel 7). Hovedtrekkene av leverandørens vurderinger tilknyttet eID er gjengitt under.

I kapittel 5 fremkommer det at et bevisst fokus på offentlige digitaliseringstiltak har gitt de fleste brukere muligheten til å nyttiggjøre seg offentlige digitale tjenester gjennom autentisering i ID-porten. Brukerundersøkelser viser videre at innbyggerne i stor grad er fornøyd med dette tilbudet. I kombinasjon med høy utbredelse av velfungerende private eID-er, der BankID innehar en dominerende posisjon, kan norske borgere i dag benytte eID-løsninger i verdenstoppen for innlogging til digitale tjenester både i offentlig og privat sektor.

I kartleggingen av nåsituasjonen for kvalitet og sikkerhet beskrevet i kapittel 6 fremkommer det at det eksisterer en viss grad av dublerte d-nummer i Folkeregisteret (se kapittel 6.1.2). Fra et sikkerhetsperspektiv kan dupliserte d-nummer blant annet utgjøre en sikkerhetsrisiko for opprettelse av eID som utelukkende legger d-nummer til grunn, slik MinID gjør. I kapittel 6.1.4 beskrives mangelen på fysisk ID-kontroll ved bestilling av MinID som en sikkerhetsrisiko som kan utnyttes av kriminelle. I tillegg er det ikke krav til ID-kontroll ved fornyelse av eID-er, da fornyelsen skjer automatisk. Videre kan manglende kunnskap og erfaring om ID-kontroll hos ansatte i bank, postkontor og post i butikk utgjøre en sikkerhetsrisiko ved utstedelse av BankID og Buypass. Det eksisterer per i dag ingen grense for hvor mange BankID-er som kan utstedes til et spesifikt identitetsnummer i ulike banker. Faktisk avdekket misbruk av eID for det offentlige spesielt, men også generelt i samfunnet, er relativt svakt dokumentert. Intervjuer tilsier at de største konsekvensene er tilknyttet misbruk av eID i nære relasjoner.

Fra kartleggingen i kapittel 7 fremkommer det at de samlede kostnadene for drift og forvaltning av ID-porten og MinID, inklusive statens autentiseringskostnader ved bruk av BankID, Buypass og Commfides, kan anses som relativt lave sammenlignet med ressursbruken i ID-forvaltningen for øvrig. Kartleggingen i kapittel 7 viser at statens samlede kostnader til autentisering for ulike eID-løsninger gjennom ID-porten er relativt lave sammenlignet med gevinsten disse løsningene gir, og prisen per transaksjon i ID-porten er redusert over tid.

Leverandørens vurdering av viktigste utfordringer ved dagens situasjon

Som beskrevet i kapittel 5 er det mange aspekter ved dagens løsninger for eID som fungerer svært godt og som blir godt mottatt i samfunnet for øvrig. Likevel er det leverandørens vurdering at det eksisterer enkelte utfordringer per dags dato.

Deler av prosessen ved utstedelse av private eID-er har sikkerhetsrisiko i form av at ID-kontrollen som ligger til grunn for utstedelsen utføres enten av en bankansatt eller av en ansatt ved postkontor eller post i butikk. Videre har dagens eID-er evig gyldighetstid, noe som betyr at eventuelle feil i en tidligere ID-kontroll ikke blir plukket opp på et senere tidspunkt. Private utstedere av eID følger kravene[454] for utstedelse

[454] KMD, «Kravspesifikasjon for PKI i offentlig sektor. Versjon 2.0», 2010

ved å gjennomføre en ID-kontroll av søkerne, og leverandøren er derfor av den oppfatning av at regelverkets utforming begrenser hvilket sikkerhetsnivå som kan oppnås ved utstedelse av private eID-er. Bankene, som utstedere av BankID, har ikke forutsetning for å kunne sjekke doble identiteter ved ID-kontrollen, hvilket leverandøren heller ikke anser at burde være bankenes rolle. Videre kan ikke bankene sjekke om andre aktører i ID-forvaltningen har gjort «feil» ved respektive aktørers ID-kontroller, for eksempel ved at de ikke har tilgang til å se hvorvidt brukere som søker om eID har status «kontrollert» i Folkeregisteret eller ikke. Videre eksisterer det per i dag ingen begrensning på hvor mange BankID-er som kan utstedes til et spesifikt identitetsnummer, da en bruker kan få utstedt BankID i alle banker brukeren har et bankforhold i. Dette utgjør en utfordring ved at en uvedkommende potensielt kan tilegne seg en BankID for et annet identitetsnummer, samtidig som identitetsnummeret allerede har en aktiv BankID og dermed benytter denne som normalt uten å oppdage at det er utstedt ytterligere BankID-er på samme identitetsnummer.

Sett i lys av beskrevne trender med en økende grad av elektroniske grensesnitt mot det offentlige, er det i større grad enn tidligere viktig at alle som oppholder seg i landet gis tilgang til en sikker måte å kommunisere digitalt med det offentlige på. En utfordring med dagens system for eID er at enkelte brukergrupper vil falle utenfor. Basert på dagens regelverk vil det eksempelvis være problematisk for brukere å anskaffe BankID eller Bypass dersom vedkommende ikke kan fremvise et gyldig pass eller om brukeren ikke kvalifiserer for et bankforhold.[455] Eksempelvis finnes det mangelfulle løsninger for tredjelandsborgere uten pass eller personer uten verger per dags dato.

Slik beskrevet i kapittel 2 og kapittel 7 har ID-porten oppnådd god vekst i antall autentiseringer, og kostnaden per autentisering har blitt redusert over tid. Leverandøren vurderer riktignok at BankID, eid av Vipps AS, sin meget høye andel av antall autentiseringer gjennom ID-porten isolert sett utgjør en utfordring. Dette skyldes at det er risiko for at et foretak som dominerer et marked, kan ha både insentiver og muligheter til å gjøre det vanskelig for konkurrenter å konkurrere effektivt. Konkurransetilsynet § 11 «*forbyr derfor et dominerende foretak utilbørlig å utnytte sin dominerende stilling».*[456] Konkurransetilsynet vurderer at en høy markedsandel normalt er en viktig indikator på at et foretak er dominerende, og indikerer at en markedsandel på mellom 70-80 prosent i seg selv er en klar indikasjon på at det foreligger en dominerende stilling.[457] Videre vil også Vipps AS måtte forholde seg til de vilkår som lå til grunn for sammenslåingen med BankID og BankAxept, blant annet en *forpliktelse om å tilby BankID til konkurrerende betalingsløsninger på ikke-diskriminerende vilkår*.[458] Utfordringen med BankIDs høye andel av transaksjonsvolum gis på generelt grunnlag, da leverandøren ikke har foretatt en avgrensning av markedet BankID opererer i eller har indikasjoner på at Vipps AS misbruker sin stilling. Vipps AS, som nåværende eier av tjenesten BankID, har av natur en vesentlig mer kommersiell innretning enn det tidligere eierskapet i Finans Norge. For tjenesten BankAxept, også eid av Vipps AS, er leverandøren kjent med at flere aktører har fått betydelige prisøkninger etter utskillelsen fra Finans Norge. Selv om BankID ikke er en lik tjeneste som BankAxept kan problemstillingen om prisøkninger inntreffe også for BankID.

Videre vil det være av samfunnsmessig interesse å unngå at en privat aktør får inneha en svært dominerende posisjon på autentiseringer av innlogging til offentlige tjenester. Det vil videre kunne være problematisk dersom en slik dominerende privat aktør i fremtiden havner i utenlandske eierskap. Denne problemstillingen er vesentlig mer reell med BankID som en del av Vipps AS enn når BankID AS var en integrert del av Finans

[455] BITS, «Regler om BankID», 2018
[456] Konkurransetilsynet, «Utilbørlig utnyttelse av dominerende stilling – § 11 i konkurranseloven», 2019
[457] Konkurransetilsynet, «Forbud mot utilbørlig utnyttelse av dominerende stilling», 2018
[458] Konkurransetilsynet, «Fusjonen mellom Vipps, BankID og BankAxept tillates på vilkår», 2018

Norge eller direkte eid av bankene. Samtidig bør det påpekes at dagens eierstruktur i Vipps, der de største aksjonærene også er blant selskapets størst kunder, til en viss grad reduserer risikoen for en profittmaksimerende tilnærming. Et slikt scenario vil det også etter leverandørens vurdering være mulig å sikre seg mot gjennom gode avtaler mellom det offentlige og Vipps AS, som vil begrense et mulig salg til utenlandske aktører og dermed redusere risikoen et slikt salg kan medføre.

11.2 Drøftinger av alternativ for eID

I dette kapittelet beskrives planen for nasjonalt ID-kort med eID slik den foreligger i dag og leverandørens forståelse av styrker og utfordringer ved nåværende plan. Slik beskrevet i kapittel 2.10 er det lagt til grunn at nasjonalt ID-kort med eID vil rulles ut og har vært en forutsetning for leverandørens vurderinger. Derfor er ikke utstedelse av nasjonalt ID-kort uten eID vurdert som et alternativ. Videre skisseres leverandørens synspunkter på potensielle forbedringer og løsninger til utfordringene ved nåværende utrullingsplan og struktur for nasjonal eID.

11.2.1 Nåværende plan for Nasjonalt ID-kort med eID

Nasjonale ID-kort planlegges utstedt med klargjort funksjonalitet for tilknyttet eID. Brukere som av ulike grunner ikke ønsker å få tildelt klargjort tilknyttet eID vil ha mulighet til å reservere seg mot tildelingen. Nasjonal eID knyttes opp mot det nasjonale ID-kortet i form av en mikrobrikke som kan kommunisere med alle typer mobiltelefoner, PCer og annet utstyr med trådløs kommunikasjon av typen NFC (Near Field Communication). Nasjonal eID vil ikke kunne brukes uavhengig av det nasjonale ID-kortet. Nasjonal eID utstedes som et supplement til nåværende private utstedte eID-er, og vil utvikles og reguleres i tråd med det nasjonale regimet for bruk av eID i offentlig sektor samt eIDAS-forordningen.[459]

Nasjonal eID utstedes sammen med nasjonalt ID-kort, og vil derfor utstedes av politiet på samme vilkår og ved samme prosedyre. Dette oppfyller krav til sikkerhetsnivå 4 i Norge (definisjon i kapittel 2.8.2) samt sikkerhetsnivå «høy» jf. eIDAS-forordningen. Nasjonal eID vil kunne benyttes i både offentlig og privat sammenheng.[460] Staten tar rollen som sertifikatutsteder og registreringsautoritet[461] ved siden av eksisterende private løsninger.

Nasjonal eID foreslås finansiert gjennom et tilleggsgebyr til nasjonalt ID-kort. Brukere som velger å reservere seg mot eID tilknyttet det nasjonale ID-kortet vil ikke få fratrekk i gebyret. Bruk av nasjonal eID vil være gratis både for bruker og tjenesteeier. Fra politiets gebyrmodell fra mars 2019 er investeringskostnaden for eID estimert til 71 mill. kroner, med årlige drifts- og vedlikeholdskostnader på 10,9 mill. kroner. Politiet anser majoriteten av etableringskostnadene for nasjonal eID som irreversible. Enhetskostnaden for nasjonal ID-kort med eID beregnes i PODs gebyrmodell som 49 kroner høyere enn enhetskostnaden for nasjonalt ID-kort uten eID.

Under følger leverandørens vurderinger av styrker og svakheter tilknyttet nåværende plan for nasjonal eID. Enkelte av styrkene som beskrives under har også tilhørende

[459] Menon Economics, «Samfunnsøkonomisk analyse av redusert gyldighetstid på pass», 2018
[460] JD, «Høring - ny forskrift om pass og nasjonalt ID-kort», 2019
[461] Nasjonal Kommunikasjonsmyndighet, «Kvalifiserte tilbydere av tillitstjenester under tilsyn etter eIDAS-forordning», 2019

svakheter, men er behandlet separat for å tydeliggjøre både styrker og svakheter ved nåværende plan.

Styrker ved nåværende plan for nasjonal eID

Utstedelse av nasjonal eID i forbindelse med nasjonalt ID-kort samsvarer med de fleste europeiske lands løsninger. Sverige har hatt en annen modell med bruk av private eID-er i flere år, men har nylig gjennomført en statlig offentlig utredning av ID-området i Sverige, der det anbefales at staten tar ansvar for utstedelse av både fysisk og elektronisk ID-bevis.[462] Dette er tilsvarende nåværende plan for utstedelse av nasjonalt ID-kort med eID i Norge.

En statlig utstedt nasjonal eID vil sikre høy sikkerhet i utstedelsesprosessen. ID-kontrollen som gjennomføres ved utstedelse av nasjonal eID vil være tilsvarende som for pass, inkludert tilknytning til biometri. Sikkerheten som ligger til grunn for utstedelsen av nasjonal eID vil derfor være høyere enn for nåværende privat utstedte eID, som ikke har tilknytning til biometri og kun belager seg på manuell kontroll av et ID-bevis.

Videre vil mindre avstand, tydeligere definerte styringslinjer og mindre avvik i styring mellom sertifikatutsteder (POD) og kontroll i førstelinje (passkontor) sammenlignet med eID i markedet (eksempelvis BankID som sertifikatutsteder, bankene som førstelinje) øke sikkerheten i utstedelsesprosessen ytterligere. I tillegg vil sikkerhetsgrunnlaget for utstedelse av nasjonal eID være høyere enn for private utstedte eID, da ansatte ved pass- og ID-kontor besitter mer ID-kompetanse og utstyr enn ansatte i en bankfilial, postkontor eller ved post i butikk. Leverandøren anser det også som en styrke at nasjonal eID er tiltenkt benyttet for å opprette kundeforhold og få utstedt eID fra private tilbydere.

Nåværende plan for utstedelse legger til grunn at integrering og bruk av nasjonal eID til digitale tjenester vil være gratis for tjenesteeiere. Utover gebyret for anskaffelse vil det heller ikke være noen kostnad knyttet til antall transaksjoner/autentiseringer for bruker. Statlig utstedelse av eID vil i større grad kunne påse at kostnadene holdes lave for bruker også i fremtiden.

Utstedelse av nasjonal eID innfører et supplement til BankID på autentisering til både private og offentlige tjenester, hvilket reduserer samfunnsrisikoen ved et potensielt eierskifte av dominerende privat aktør. Videre vil utstedelse av nasjonal eID, med forbehold om bred utbredelse av nasjonalt ID-kort med eID, kunne gi staten et bedre utgangspunkt i forhandlinger om fornyelse av kontrakt med BankID for bruk ved autentisering gjennom ID-porten. En nasjonal eID tar også hensyn til argumentet om at staten fra et nasjonalt sikkerhetsperspektiv skal kunne tilby en nasjonal eID ved en nasjonal krise eller i annet scenario der privat eID blir satt ut av spill. Styrken i argumentet fordrer høy utbredelse av nasjonalt ID-kort med eID.

Store deler av kostnadene tilknyttet nåværende plan for utstedelse av nasjonal eID er allerede påløpt og anses som irreversible. POD fremholder at det foreligger betydelige synergier mellom nødvendig infrastruktur for nasjonal eID og eksisterende infrastruktur for pass. Videre er marginalkostnaden for utstedelse av nasjonal eID i tillegg til nasjonalt ID-kort av POD forespeilet til å være svært lav, uavhengig av utbredelse.

Innføring av en nasjonal eID muliggjør en potensiell utfasing av MinID på sikt, hvilket vil gjøre at samtlige tilgjengelige eID-er for autentisering gjennom ID-porten vil ha

[462] SOU 2019:14, «Ett säkert statligt ID-kort – med e-legitimation», 2019

sikkerhetsnivå 4. Som beskrevet i kapittel 6.1.4 er det flere svakheter ved utstedelse og bruk av MinID som vil kunne unngås ved at nasjonal eID innføres. Det forutsettes meget høy utbredelse av nasjonalt ID-kort med eID før MinID kan fases ut, gitt utbredelsen av MinID presentert i kapittel 2.8.1.

Utfordringer ved nåværende plan for nasjonal eID

Offentlig sektor og tjenesteeiernes behov dekkes i dag i stor grad av eksisterende løsninger.[463] BankID leverer i dag en autentiseringsløsning med høy utbredelse og som oppfattes som svært brukervennlig.

Selv om sikkerheten i utstedelsesprosessen av en nasjonal eID vil være høyere enn for de eksisterende private eID-ene, vil ikke sikkerheten ved bruk av nasjonal eID skille seg fra de private eID-ene. Bruken av både nasjonal og private eID-er baserer seg på to-faktor autentisering, og vil oppnå sikkerhetsnivå 4. Planlagt løsning for nasjonal eID benytter ikke biometrien som blir registrert ved utstedelse ved senere bruk av nasjonal eID, og det er dermed ingen økt sikkerhet i bruken av nasjonal eID sammenlignet med eksisterende private eID-er.

Det kan argumenteres for at enkelte av styrkene og suksesskriteriene for nasjonal eID vil være avhengig av høy grad av utbredelse i befolkningen. Blant annet fordrer argumentet om at innføring av en nasjonal eID vil redusere samfunnsrisikoen ved et potensielt eierskifte eller systemsvikt av dominerende privat aktør være avhengig av en høy utbredelse, det samme er gjeldende for utfasing av MinID som offentlig eID.

Den samfunnsmessige nytten av en nasjonal eID er i stor grad avhengig av en høy utbredelse av det nasjonale ID-kortet. Det er en risiko for utbredelsen og bruken av nasjonal eID om brukervennligheten ikke er god sammenlignet med eksisterende private eID-løsninger i markedet. Leverandøren har forespurt beskrivelser av brukerreiser for bruk av løsningene, men er blitt gjort kjent med at dette ikke eksisterer i ferdigstilte versjoner. Basert på overordnede beskrivelser i beslutningsgrunnlaget for eID på nasjonalt ID-kort utarbeidet av POD[464], fremstår løsningen for nasjonal eID som lite brukervennlig sammenlignet med eksisterende løsning fra BankID, da det kreves at brukeren må ha det nasjonale ID-kortet for hånden for å benytte autentisering ved nasjonal eID. I tillegg kreves det at brukeren har en smarttelefon med støtte for NFC for å autentisere seg med nasjonal eID. Leverandøren stiller spørsmål ved om brukervennligheten til nasjonal eID slik den er beskrevet i nåværende plan vil være tilstrekkelig til å sikre høy utbredelse i befolkningen, uten at det stilles krav til brukere om pass eller nasjonalt ID-kort for tilgang til offentlige tjenester og ytelser eller ved at pass eller nasjonalt ID-kort blir obligatorisk, slik beskrevet som alternativ i kapittel 10.2.

Leverandøren er gjort kjent med sluttbrukerundersøkelsen om eID som ble gjennomført i 2018 på oppdrag fra JD og KMD. I undersøkelsen svarer omtrent en tredjedel av respondentene at deres interesse for nasjonalt ID-kort øker dersom det inneholder en nasjonal eID. Samtidig svarer flest respondenter at det er det er egenskapene som erstatning for pass for reiser innenfor EØS og som fysisk legitimasjonskort som er mest attraktivt ved det nasjonale ID-kortet, og ikke den tilknyttede nasjonale eID-en.[465]

[463] POD, «Beslutningsgrunnlag for eID på nasjonalt ID-kort: Kartlegging – offentlige tjenesteeiere, delleveranse 8», 2016
[464] POD, «Beslutningsgrunnlag for eID på nasjonalt ID-kort, delleveranse 3: Konseptbeskrivelse», 2016
[465] POD, «Beslutningsgrunnlag for eID på nasjonalt ID-kort: Kartlegging – sluttbrukere, delleveranse 11», 2016

POD har synliggjort kostnadene ved nasjonal eID i gebyrmodellen for pass og nasjonale ID-kort. Drift- og forvaltningskostnadene omfatter blant annet brukerstøtte og systemdrift for nasjonal eID, som skal utøves av Difi innenfor Difis brukerstøttes allerede etablerte åpningstider. Basert på data mottatt fra banker med erfaring fra brukerstøtte for BankID, fremstår PODs estimater for kostnader til brukerstøtte for nasjonal eID som betydelig lavere enn hva bankene selv opplever med BankID, justert for volum. Videre er Difis allerede etablerte åpningstider langt kortere enn hva bankenes brukerstøtte opererer med, hvilket kan bety at tilgjengeligheten for brukerstøtte tilknyttet nasjonal eID blir lavere enn for eksempelvis BankID. Leverandøren er av den oppfatning at PODs kostnader til brukerstøtte kan bli vesentlig større enn estimert dersom nasjonal eID får betydelig utbredelse og bruk i samfunnet. Lave kostnader tilskrives fra POD/JD sin side synergieffekter med eksisterende systemer tilknyttet pass og nasjonale ID-kort. Dagens kostnadsanslag tar ikke hensyn til eventuelle videreutviklingskostnader av nasjonal eID. Slik beskrevet i kapittel 2.10 har det ikke vært en del av leverandørens mandat å kvalitetssikre det pågående pass- og ID-programmet.

Nasjonal eID skal utstedes som et supplement til privat utstedte eID-er i markedet med sikkerhetsnivå 4.[466] Ved nåværende plan for nasjonal eID vil brukeren bli belastet gebyr ved utstedelse, mens bruk av nasjonal eID vil være gratis for både bruker og offentlige og private tjenesteeiere. Modell med gratis anvendelse av nasjonal eID for private og offentlige tjenesteeiere kan anses konkurransevridende overfor eksisterende private tilbydere av eID. Private tjenesteeiere kan velge å benytte nasjonal eID som autentiseringsløsning uten at det påløper tjenesteeier noen kostnader, og dermed unngå kostnader som bruk av for eksempel BankID medfører i dag. Kostnaden for nasjonal eID vil derimot i sin helhet bæres av brukere av nasjonal eID. Staten tar også på seg en risiko dersom utbredelsen og bruken av nasjonal eID blir høy, med tanke på drifts- og forvaltningskostnader som resultat av høy bruk av nasjonal eID. Statens kostnader ved dagens bruk av private eID-er er derimot begrenset til transaksjonskostnader per autentisering gjennom ID-porten, og ytterligere drifts- og forvaltningskostnader tilfaller de private tilbyderne.

11.2.2 Potensielle forbedringer og løsninger til utfordringer ved eksisterende private eID-er og nåværende plan for nasjonal eID

Etter leverandørens oppfatning står man ovenfor alternativ om å styrke krav til sikkerhet tilknyttet utstedelse og bruk for private eID-er og/eller styrke utbredelsen og krav til bruk av nasjonal eID. Under presenteres leverandørens mulige forbedringer og løsninger til de utfordringer som er beskrevet for nåværende plan for nasjonal eID, samt utstedelse og bruk av eksisterende private eID-er.

I kapittel 10 drøfter leverandøren krav til pass og nasjonalt ID-kort for tilgang til offentlige tjenester og ytelser, samt om pass eller nasjonalt ID-kort gjøres obligatorisk. Av tidshensyn har leverandøren ikke drøftet hvorvidt det kan stilles krav om nasjonal eID for utvalgte tjenester og ytelser eller om nasjonal eID gjøres obligatorisk. Leverandøren vurderer at nærmere vurderinger av dette kan være hensiktsmessig. Av samme grunn er det heller ikke drøftet krav til økt krav til digital fornyelse av eID-er.

ID-kontroll ved pass- og ID-kontor legges til grunn for utstedelse av norske private eID-er

[466] JD, «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

En potensiell forbedring av den nåværende planen er å styrke utstedelsen av norske private eID-er ved at ID-kontrollen som gjennomføres ved søknad om pass og nasjonalt ID-kort også legges til grunn for utstedelse av norske private eID-er. Forslaget vil erstatte dagens løsning der ID-kontroll ved utstedelse av norske private eID-er gjennomføres av ansatte i en bankfilial, ved et postkontor eller ved post i butikk.

Ved oppmøte for søknad om pass og/eller nasjonalt ID-kort opptas det biometri i form av ansiktsfoto og fingeravtrykk av bruker, som muliggjør at brukeren kan få status «unik» i Folkeregisteret. Forbedringen innebærer videre at på pass- og ID-kontoret vil brukeren bli spurt om den ønsker at norske private eID-tilbydere kan ta kontakt via post til folkeregistrert adresse for å tilby utstedelse av norsk privat eID. Brukeren vil selv kunne velge hvilken norsk privat eID den ønsker å få utstedt, og mottar kodebrikke i posten etter at kundeforholdet er opprettet, slik som i dag. Norske private eID-tilbydere vil få tilgang til å sjekke om brukeren har status «unik» i Folkeregisteret basert på identitetsnummeret til brukeren, og tilbyderen vet dermed om brukeren er ID-kontrollert og har avgitt biometri. Denne løsningen vil gjøre at brukere som ikke anskaffer seg nasjonalt ID-kort, eller av ulike grunner reserverer seg mot nasjonal eID i tilknytning til det nasjonale ID-kortet, vil kunne få utstedt norsk privat eID med grunnlag i samme ID-kontroll som den nasjonale eID-en.

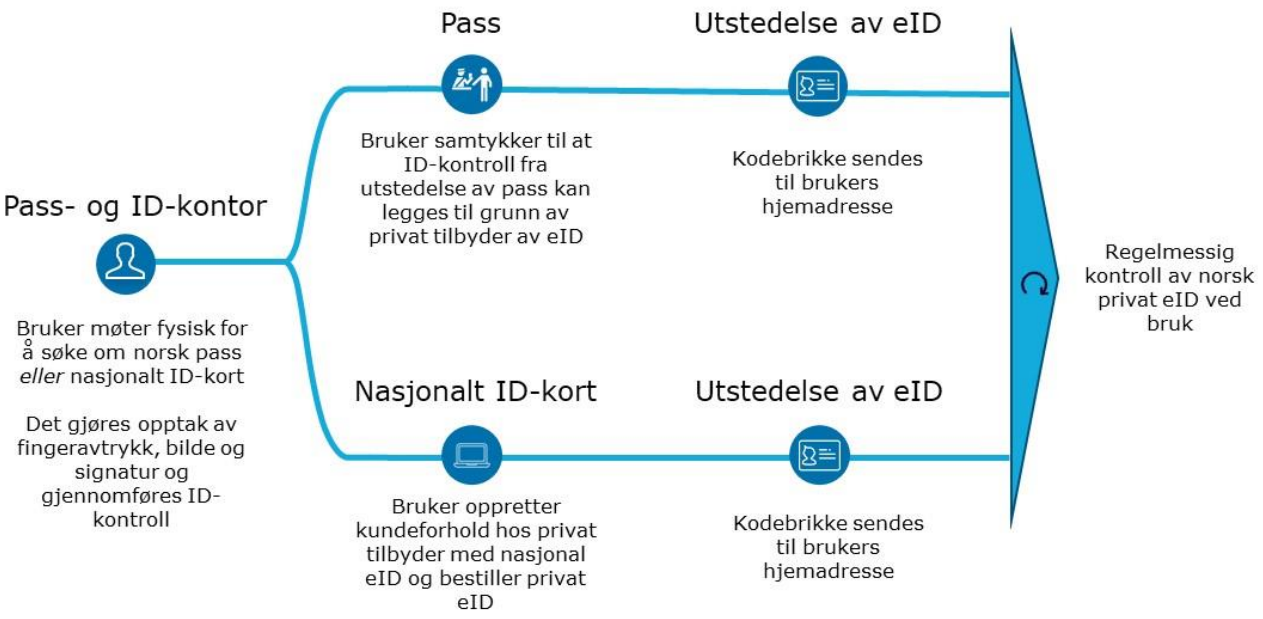
Etter utstedelse av nye norske private eID-er er gjennomført etter beskrivelsen over, vil det ved bruk av den norske private eID-en regelmessig sendes en spørring til Folkeregisteret som undersøker om brukeren er ID-kontrollert og har status «unik» i Folkeregisteret. Den samme spørringen vil også kunne gjøres for allerede aktive norske private eID-er. Dette medfører at brukere av norske private eID-er blir elektronisk ID-kontrollert også etter utstedelse, hvilket skiller seg fra dagens løsning der den eneste ID-kontrollen av eID-brukere gjøres ved utstedelsen. Gitt fem års gyldighet for nasjonale ID-kort og ti års gyldighet for pass, betyr det at en den foreslåtte elektroniske ID-kontrollen vil gjøres mot informasjon i Folkeregisteret som oppdateres minst hvert tiende år, forutsatt at brukeren av den norske private eID-en har et gyldig pass eller nasjonalt ID-kort. Dersom den elektroniske ID-kontrollen viser at brukeren ikke har vært til ID-kontroll ved et pass- og ID-kontor de siste ti år, vil den norske private eID-en bli sperret for autentisering til offentlige digitale tjenester gjennom ID-porten, inntil brukeren har møtt opp ved et pass- og ID-kontor for ID-kontroll og opptak av biometri.

Forbedringen er kun overordnet skissert fra leverandøren og vil innebære praktiske, juridiske og økonomiske konsekvenser som vil måtte utredes nærmere. Forbedringen samsvarer godt med uttalte mål om økt offentlig-privat samarbeid i regjeringens digitaliseringsstrategi.

Anvendelse av nasjonal eID for etablering av privat eID

I tillegg til å benytte ID-kontrollen som gjennomføres ved pass- og ID-kontorene som grunnlag for utstedelse av private eID-er, anser leverandøren det som hensiktsmessig at nasjonal eID kan benyttes for å opprette kundeforhold og få utstedt eID fra private tilbydere. Brukeren vil, etter å ha mottatt sitt nasjonale ID-kort med eID, kunne opprette kundeforhold og bestille eID fra private tilbydere ved å autentisere seg med nasjonal eID på nettet. Private eID-er utstedt på denne måten vil på samme måte som over kontrolleres elektronisk mot Folkeregisteret ved bruk, for å sikre regelmessig kontroll av brukeren.

Figuren under illustrerer et eksempel på hvordan de to løsningene beskrevet over kan se ut.



Figur 63 Gjenbruk av ID-kontroll ved pass og ID-kontor i utstedelse av privat eID

Endring av vederlagsmodell for nasjonal eID

Som en løsning til utfordring om konkurransevridning ser leverandøren det som en mulighet å endre vederlagsmodellen for nasjonal eID. Ved å innføre en transaksjonskostnad som belastes tjenesteeiere ved autentisering til digitale tjenester gjennom nasjonal eID vil konkurransen i markedet i større grad opprettholdes etter leverandørens oppfatning. Ved at de private og offentlige eID-konkurrerer på like vilkår vil en kunne redusere samfunnsrisikoen ved et potensielt eierskifte eller systemsvikt av dominerende privat aktør, gitt at utbredelsen for nasjonal eID er høy. Videre vil utfordringen om potensielt økte kostnader ved offentlig eID bli mer dynamisk, da staten vil få transaksjonsinntekter som kan bidra til å dekke kostnader for forvaltning av offentlig eID. Innføring av transaksjonskostnader vil gjøre det mulig å fjerne andelen av gebyret for det nasjonale ID-kortet som tilegnes nasjonal eID ved utstedelse. Leverandøren er riktignok gjort oppmerksom på at dagens vederlagsmodell er fordelaktig sett opp mot eIDAS, da dette regelverket legger til grunn at bruk av eID-er fra andre land skal kunne benyttes kostnadsfritt.

Etter leverandørens vurdering er en endring av vederlagsmodellen for nasjonal eID primært relevant med høy utbredelse av nasjonale ID-kort med eID hvor brukerne benytter eID-en til autentisering på en regelmessig basis.

12 Vurdering av alternativer knyttet til rekvirering og tildeling av identitetsnummer i Folkeregisteret

12.1 Oppsummering vurdering nåsituasjonen

Som påpekt i kapittel 5 og 6 brukes identitetsnummer i form av d-nummer eller fødselsnummer bredt i både offentlig og privat sektor, og ligger til grunn for både fysiske og elektroniske ID-bevis.

D-nummer og fødselsnummer er brukervennlig for norske borgere, EØS-borgere og tredjelandsborgere. Videre anerkjenner de fleste aktørene Folkeregisteret som en meget positiv del av ID-forvaltningen. De to typene identitetsnumre gir på mange måter de samme mulighetene, men prosessene for tildeling er ulike. Det er leverandørens vurdering at delt ansvarliggjøring og manglende felles rutiner gir varierende kvalitet og sikkerhetsutfordringer tilknyttet rekvireringsprosessen for d-nummer med potensielt store følgefeil. Videre er det leverandørens vurdering at antallet rekvirenter er høyt og at det blant de ulike er en varierende forståelse for hvilke muligheter et d-nummer *faktisk* gir og at krav til ID-kontroll og status «kontrollert» prioriteres deretter. Leverandøren har vurdert at statens inntekter og utgifter behandles ulikt ved at det er strengere kontroll for inntekter i form av beskatning.

Prosessen for å få tildelt fødselsnummer vurderes av leverandøren som en mer standardisert prosess med færre involverte aktører og strengere krav til ID-kontroll.

12.2 Drøfting av alternativer for rekvirering og tildeling av identitetsnummer i Folkeregisteret

Basert på nåsituasjonen har leverandøren skissert fire ulike alternativer som kan bidra til å forbedre prosessen med å tildele identitetsnummer i Folkeregisteret. Videre finner leverandøren det mest hensiktsmessig å drøfte alternativer for hvordan EØS-borgere og tredjelandsborgere får tildelt identitetsnummer i Folkeregisteret basert på vurderingene i del 2. Leverandøren vil i alternativ 1 vektlegge tiltak relatert til både fødselsnummer og d-nummer, mens de resterende alternativene vektlegger rekvirering og tildeling av d-nummer.

Under følger fire alternativer for hvordan tildeling av identitetsnummer kan være med å påvirke og øke sikkerheten, samt bedre kvaliteten i ID-forvaltningen. Alternativene kan implementeres samlet eller som enkeltstående initiativ.

12.2.1 Alternativ 1: Felles rutinebeskrivelse for alle d-nummerrekvirenter og aktører som gjennomfører ID-kontroll som legges til grunn for tildeling av fødselsnummer

Under vil leverandøren gjennomgå to underalternativer for å heve kvaliteten på identitetsnummer i Folkeregisteret. Tiltakene kan iverksettes samlet eller hver for seg.

Alternativ 1a: Felles rutinebeskrivelse for d-nummerrekvirenter

Som påpekt under funn i kapittel 6.2 er det leverandørens vurdering at rekvirentene benytter individuelle rutiner for en prosess av lik karakter, og at dette potensielt utgjør en sikkerhetsrisiko.

Alternativ 1a innebærer å utarbeide en felles rutine for d-nummerrekvirering for å sikre at samtlige rekvirenter utfører prosessen på lik måte og har en god og felles forståelse for prosessen og ID-relaterte utfordringer.

Styrker:

- Enhetlige rutiner bidrar til økt sikkerhet på tvers av aktører
- Alle rekvirenter gjøres i større grad oppmerksomme på viktigheten av «kontrollerte» d-nummer og potensiell risiko ved svak kontroll
- Bevarer høy grad av brukervennlighet ved å beholde nærhet til sektorenes saksbehandling og tjenesteproduksjon

Svakheter:

- Skatteetaten og NAV står for 92 pst av d-nummer rekvisisjoner og har utarbeidet egne rutiner hvor kvaliteten vurderes som god. En felles rutine som skal omfatte alle rekvirenter og deres behov kan bli svært omfattende og vanskelig å benytte i praksis
- Usikkert om en felles rutine alene vil styrke «ID-kontrollen» i rekvisisjonsprosessen hvilket oppleves som en av de reelle svakhetene i dagens prosess. Basert på dette vil alternativet i begrenset grad øke kvaliteten på d-nummer i Folkeregisteret

Alternativ 1b: Felles rutinebeskrivelse for hvilke ID-bevis som er gyldig for ID-kontrollen som ligger til grunn for tildelingen av fødselsnummer

Som påpekt i kapittel 6.2.5 eksisterer det ingen harmonisert tilnærming til hvilke ID-bevis som anses som godkjente og dette oppleves som en utfordring for flere aktører i ID-forvaltningen. Når det varierer mellom aktørene, og noen tilfeller internt hos den enkelte aktør, hvilke ID-bevis som er godkjente er det vanskelig for andre aktører og bygge på denne kontrollen.

Alternativ 1b innebærer å utarbeide et dokument/retningslinjer som detaljerer hvilke ID-bevis/ID-dokumenter som skal eller kan ligge til grunn for ID-kontroll ved tildeling av fødselsnummer. Som nevnt innledningsvis er dette ikke relevant for fødsler i Norge med tilhørende fødselsmelding.

Styrker:

- Forholdsvis enkelt å utarbeide og implementere på tvers av Skatteetaten og utlendingsforvaltningen
- Enhetlig beskrivelse bidrar til økt sikkerhet på tvers av aktører
- Bedre forståelse for hva som ligger til grunn for tidligere ID-kontroller vil øke tilliten til, og gjenbruket av, tidligere kontroller

Svakheter:

- Utlendingsforvaltningen er svært kompleks og det kan være praktisk utfordrende å sette krav til hvilke dokumenter som må foreligge i kontrollen

12.2.2 Alternativ 2: Gjøre folkeregistermyndigheten ansvarlig for rekvirering og tildeling av d-nummer

Alternativet innebærer at én aktør, for eksempel Skatteetaten som er folkeregistermyndighet i dag, er den eneste ansvarlige for å både rekvirere og tildele d-nummer i Folkeregisteret. Folkeregistermyndigheten vil således få et mer helhetlig ansvar for identitetsnummer, både permanente i form av fødselsnummer og midlertidige i form av d-nummer.

Som fremlagt i kapittel 6.1.2 rekvirerer Skatteetaten over halvparten av alle d-nummer. Alternativet innebærer økt ansvar for Skatteetaten isolert sett. De øvrige rekvirentene har et relativt lavt saksvolum med unntak av NAV, og til dels Brønnøysundregisteret og utlendingsmyndighetene. Leverandøren har ikke undersøkt hvilke prosess- og systemmessige konsekvenser det får for den enkelte rekvirent som mister sin rekvirentstatus, men det antas at dette er begrenset.

Per i dag er det den enkelte rekvirents ansvar å vurdere om behovet for d-nummer er begrunnet. Skatteetaten som folkeregistermyndighet overprøver ikke dette. Som et eksempel på begrunnet behov vil Brønnøysundregistret kun rekvirere d-nummer i de tilfeller det er behov for d-nummer i forbindelse med registrering i deres registre eller det skal rapporteres i Altinn på vegne av allerede registrerte rolleinnehavere.[467]

I dette alternativet vil folkeregistermyndigheten være ansvarlig for å foreta vurderingen av begrunnet behov. Behovsvurderingen er imidlertid nært tilknyttet det enkelte saksfelt og det er etter leverandørens syn den enkelte fagmyndighet som har best forutsetninger for å foreta denne vurderingen. Eksempelvis er det NAV som er nærmest til å vurdere om en person potensielt er omfattet av en bestemt stønadsordning[468] og dermed om det er behov for å rekvirere d-nummer i den enkelte sak. Etter leverandørens oppfatning vil det være svært krevende for den ene d-nummer-rekvirenten å vurdere behovet for d-nummer på alle de ulike områdene hvor d-nummer brukes per i dag.

Som nevnt i nåsituasjonen finnes det eksempler på at det rekvireres d-nummer uten at det strengt tatt er behov for et midlertidig identitetsnummer i Folkeregisteret, og at et internt løpenummer ville dekket behovet. I kartleggingen har enkelte aktører gitt uttrykk for at et løpenummer i hovedsak kunne dekket deres interne saksbehandlingsbehov. Det er leverandørens vurdering at løpenummer har en større sannsynlighet for å bli tatt i bruk om en aktør mister muligheten til å rekvirere d-nummer.

Styrker:

- Enklere å sikre at rekvisisjonsprosessen gjennomføres med tilstrekkelig høy kvalitet og sikkerhet ved at folkeregistermyndigheten får et mer helhetlig ansvar
- Tilrettelegger for at en større andel må gjennom identitetskontroll på Skattekontor og at andel «kontrollert» øker fra dagens nivå
- Enkelte aktører har oppgitt at et registreringsnummer i form av et løpenummer kan erstatte deres bruk av d-nummer som per i dag i all hovedsak benyttes til intern saksbehandling. Det kan således forventes at antall rekvirerte d-nummer reduseres fra dagens nivå

[467] Brønnøysundregisteret, «d-nummer», u.å.
[468] Folkeregisterforskriften § 2-2-3 første ledd bokstav g

Svakheter:

- Det vil være svært utfordrende for folkeregistermyndigheten å vurdere begrunnet behov på saksfelt de ikke har fagmyndighet
- Enkelte brukere vil bli henvist videre til Skatteetaten for å få rekvirert d-nummer, noe som vil føre til ytterligere et kontaktpunkt med ID-forvaltningen og redusert brukervennlighet
- Dagens rekvireringsprosess vurderes som tidseffektiv og det er en risiko for at saksbehandlingen vil trekke ut i tid dersom Skatteetaten får eneansvar for tildelingen av d-nummer. Dette kan gi redusert brukervennlighet

12.2.3 Alternativ 3: Kreve status «kontrollert» på d-nummer for å kunne motta tjenester og ytelser fra det offentlige (for å bidra til at statens inntekter og utgifter behandles likt)

Alternativ 3 innebærer å kreve status «kontrollert» for alle d-nummer som ligger til grunn for beskatning og mottak av tjenester og ytelser fra det offentlige. Det betyr at status «kontrollert» innføres som krav for alle personer med d-nummer som oppholder seg i Norge og skal motta tjenester og ytelser fra det offentlige, tilsvarende som Skatteetaten praktiserer for skattekort i dag.

Alternativet innebærer videre at for å få status «kontrollert» i Folkeregisteret må personen som oppholder seg i Norge møte til fysisk ID-kontroll ved et skattekontor for rekvirering av d-nummer uavhengig om det er en EØS-borger eller tredjelandsborger.

Leverandøren vurderer at å kreve status «kontrollert» for d-nummer som rekvireres til utenlandske personer i Norge, ikke skal være til hinder for at NAV vil kunne gi økonomisk og sosial sikkerhet til de brukerne som har krav på det og oppfyller vilkårene for tjenesten og/eller ytelsen.

På lengre sikt kan krav om status «unik» erstatte krav om status «kontrollert».

Styrker:

- Ved å kreve status «kontrollert» for å motta tjenester og ytelser fra det offentlige vil andel kontrollerte d-nummer øke vesentlig
- D-nummer tildelt i forbindelse med både beskatning og mottak av tjenester og ytelser fra det offentlige får en høyere grad av sikkerhet
- Økt tillit til velferdssystemet ved at det etableres tilsvarende krav til status «kontrollert» for mottakere av tjenester og ytelser som for beskatning
- Høyere terskel og vanskelighetsgrad for å utnytte det norske velferdssystemet

Svakheter:

- Fortsatt risiko for at personer som har korte opphold i Norge ikke vil møte til ID-kontroll. Dette er utfordrende å følge opp
- Utfordrende å kommunisere/implementere krav om status «kontrollert» for utenlandske personer med dårlige språkferdigheter, begrenset kjennskap til det offentlige systemet og kort oppholdstid

- En ID-kontroll utført for å få status «kontrollert» vil ikke ha samme sikkerhetsnivå som en ID-kontroll for status «unik». Om en person selv kan velge en av de to kontrollene, og etatenes ansvar og oppgaver ikke endres fra dagens situasjon, vil dette medføre et potensielt sikkerhetshull

12.2.4 Alternativ 4: Kreve status «kontrollert» for å kunne motta skattekort og/eller tjenester og ytelser fra det offentlige, uavhengig om personen befinner seg i Norge eller utlandet

Alternativ 4 innebærer å kreve status «kontrollert» for alle d-nummer som ligger til grunn for beskatning og mottak av tjenester og ytelser fra det offentlige for utenlandske personer, uavhengig om de befinner seg i Norge eller utlandet. Norske statsborgere har fødselsnummer og er ikke relevante i denne sammenheng.

Dagens praksis rundt fysisk kontroll og status «kontrollert» av utlendinger i Skatteetaten avhenger av om personen befinner seg i Norge eller i utlandet. Befinner personen seg i Norge kreves det status «kontrollert» på d-nummer ved fysisk oppmøte på et skattekontor for å få utstedt skattekort og bli beskattet. Det samme kontrollkravet gjelder ikke for mottak av tjenester og ytelser fra NAV som beskrevet i alternativ 3.

Dersom personen befinner seg i utlandet anses det som byrdefullt å pålegge vedkommende å reise til et skattekontor for å gjennomføre fysisk kontroll for å få skattekort (ref. kapittel 6.1.2). Personen er i disse tilfellene unntatt fra kravet om oppmøte for ID-kontroll og det kreves derfor ikke at d-nummeret er «kontrollert». For å kunne motta tjenester og ytelser fra NAV er det i dag ingen krav til «kontrollert». Dette er oppsummert i figuren nedenfor.

	Skatteetaten	NAV
Utenlandsk statsborger i Norge	Krever status «kontrollert»	Krever ikke status «kontrollert»
Utenlandsk statsborger i utlandet	Krever ikke status «kontrollert»	Krever ikke status «kontrollert»

Tabell 24 Dagens krav til status «kontrollert» til utenlandske statsborgere i Norge og i utlandet

Leverandøren er ikke kjent med omfanget av NAVs utbetalinger til utlendinger i Norge i 2018, men totalt 2,9 mrd. kroner ble utbetalt til utlendinger bosatt i utlandet.[469]

Implementering av alternativ 4 medfører krav om status «kontrollert» ved rekvirering av d-nummer for alle utenlandske personer slik presentert i tabellen nedenfor.

	Skatteetaten	NAV
Utenlandsk statsborger i Norge	Krever status «kontrollert»	Krever status «kontrollert»
Utenlandsk statsborger i utlandet	Krever status «kontrollert»	Krever status «kontrollert»

Tabell 25 Krav til status «kontrollert» til utenlandske statsborgere i Norge og i utlandet

[469] NAV, «Utbetalinger til personer i utlandet», 2019

For ID-kontroll av utlendinger som oppholder seg i utlandet anses det per i dag som utfordrende å kreve at personen møter opp til fysisk kontroll. Gjennomføring vil kreve samarbeid med andre aktører og/eller eventuelt implementering av nye tekniske løsninger for ID-kontroll. Leverandøren er ikke kjent med at det per i dag gjennomføres «kontroll» av d-nummer på noen av utenriksstasjonene per i dag.

På lengre sikt kan krav om status «unik» erstatte krav om status «kontrollert».

Styrker:

- En høyere andel rekvirerte d-nummer får status «kontrollert»
- Høyere terskel og vanskelighetsgrad for å utnytte det norske velferdssystemet

Svakheter:

- Å sikre status «kontrollert» for alle utenlandske personer er en omfattende prosess og potensielt vanskelig gjennomførbart. Særlig utfordrende og lite brukervennlig vil det være for utenlandske privatpersoner og næringsdrivende som søker d-nummer fra utlandet
- Utfordrende å kommunisere/implementere krav om status «kontrollert» for utenlandske personer med dårlige språkferdigheter og begrenset kjennskap til det offentlige systemet
- En ID-kontroll utført for å få status «kontrollert» vil ikke ha samme sikkerhetsnivå som en ID-kontroll for status «unik». Om en person selv kan velge en av de to kontrollene, og etatenes ansvar og oppgaver ikke endres fra dagens situasjon, vil dette medføre et potensielt sikkerhetshull

12.3 Oppsummering av alternativer opp mot sikkerhet, brukervennlighet og ressursbruk

Under har leverandøren overordnet oppsummert drøftingen med tanke på sikkerhet, brukervennlighet og ressursbruk. Tabellen under oppsummerer drøftingen basert på rammeverket for pluss-minusmetoden beskrevet i kapittel 1.3.

Alternativ 1a: *Felles rutinebeskrivelse for d-nummerrekvirente*r, vurderes å ha en liten positiv konsekvens for sikkerheten da det kan bidra til en noe mer enhetlig tilnærming til ID-kontrollen. Alternativet vurderes å ha ubetydelig konsekvens for brukervennlighet og ressursbruk.

Alternativ 1b: *Felles rutinebeskrivelse for hvilke ID-bevis som er gyldig for ID-kontrollen som ligger til grunn for tildelingen av fødselsnummer,* vurderes å ha en liten positiv konsekvens for sikkerheten da det kan bidra til en noe mer enhetlig tilnærming til ID-kontrollen. Alternativet vurderes å ha ubetydelig konsekvens for brukervennlighet og ressursbruk.

Alternativ 2*: Gjøre folkeregistermyndigheten ansvarlig for rekvirering og tildeling av d-nummer*, vurderes å ha en middels positiv konsekvens på sikkerheten. Dette er basert på at en aktør vil ha helhetsansvar for rekvirering og tildeling av d-nummer og dette legger til rette for økt kvalitet og sikkerhet. Videre antas det at andel «kontrollert» vil øke fra dagens nivå. Alternativet vurderes å ha en middels negativ konsekvens på brukervennligheten da flere personer vil henvises videre til folkeregistermyndigheten (fysisk/digitalt) og disse vil få ytterligere et kontaktpunkt med ID-forvaltningen.

Alternativet vurderes å ha en stor negativ konsekvens på ressursbruk ettersom folkeregistermyndigheten må vurdere begrunnet behov på saksfelt de ikke har fagmyndighet på.

Alternativ 3: *Kreve status «kontrollert» på d-nummer for å kunne motta tjenester og ytelser fra det offentlige (for å bidra til at statens inntekter og utgifter behandles likt).* Alternativet vurderes å ha en stor positiv konsekvens for sikkerheten ettersom det store flertallet av rekvirerte d-nummer vil få status «kontrollert». Alternativet vil som beskrevet i alternativ 2 medføre ytterligere et kontaktpunkt med ID-forvaltningen, men for et lavere antall mennesker, og det vurderes derfor å ha en middels negativ konsekvens på brukervennligheten. Videre innebærer alternativet økt aktivitet på skattekontorene og dette vurderes å ha en middels negativ konsekvens på ressursbruk.

Alternativ 4: *Kreve status «kontrollert» for å kunne motta skattekort og/eller tjenester og ytelser fra det offentlige, uavhengig om personen befinner seg i Norge eller utlandet.* Alternativet innebærer å gjennomføre ID-kontroll på alle d-nummer rekvirert av Skatteetaten og NAV og vurderes å ha en meget stor positiv konsekvens for sikkerheten i ID-forvaltningen. Å sikre status «kontrollert» for alle utenlandske personer er en omfattende prosess og særlig utfordrende for utenlandske privatpersoner og næringsdrivende som søker d-nummer fra utlandet. Basert på dette vurderes alternativet å ha en meget stor negativ konsekvens på brukervennlighet. Alternativet vil videre medføre økt ressursbruk både i Norge, og for eventuelle virksomheter som bistår skattekontorene med å gjennomføre ID-kontroll i utlandet, og det vurderes derfor å ha en meget stor negativ konsekvens på ressursbruk.

	Sikkerhet	Brukervennlighet	Ressursbruk
Alternativ 1a: Felles rutinebeskrivelse for d-nummerrekvirenter	+	0	0
Alternativ 1b: Felles rutinebeskrivelse for hvilke ID-bevis som er gyldig for ID-kontrollen som ligger til grunn for tildelingen av fødselsnummer	+	0	0
Alternativ 2: Gjøre folkeregistermyndigheten ansvarlig for rekvirering og tildeling av d-nummer	++	--	---
Alternativ 3: Kreve status «kontrollert» på d-nummer for å kunne motta tjenester og ytelser fra det offentlige (for å bidra til at statens inntekter og utgifter behandles likt)	+++	--	--
Alternativ 4: Kreve status «kontrollert» for å kunne motta skattekort og/eller tjenester og ytelser fra det offentlige, uavhengig om personen befinner seg i Norge eller utlandet	++++	----	----

Tabell 26 Oppsummering av drøfting for rekvirering og tildeling av identitetsnummer i Folkeregisteret

13 Vurdering av alternativer knyttet til biometri

13.1 Oppsummering vurdering nåsituasjonen

Som påpekt under nåsituasjonen (kapittel 6.1.6) og funn og vurderinger (kapittel 6.2.12), er biometri et komplekst område. Biometri er et virkemiddel hvor det er mange uavklarte forhold knyttet til regelverk, personvern og hva som gjelder for de ulike brukergruppene i og utenfor Norge. Det er et stort antall pågående initiativ, hvor biometri er en sentral faktor.

13.2 Drøftinger av alternativer for opptak, lagring og søk i biometri

Biometri vurderes som en nøkkelfaktor for å oppnå visjon, hovedmål og delmål for ID-forvaltningen, dette er nærmere beskrevet i kapittel 9.2.2. Biometri er et viktig element for kvalitet og sikkerhet i ID-forvaltningen, enten gjennom å sikre *en person, en identitet i Norge*, sikre et Folkeregister med høy datakvalitet, eller for å øke kvaliteten i ID-kontroll generelt for både politi og utlendingsmyndigheten. Biometri bidrar også til bedre kvalitet og kontroll for øvrige offentlige tjenesteytere som sikrer at rett person mottar ytelsene de har krav på.

I den påfølgende drøftingen forutsettes det at vedtatte planer og pågående arbeid som beskrevet i del 1 gjennomføres. Det er leverandørens oppfatning at disse tiltakene vil bidra positivt til å øke sikkerheten og kvaliteten i ID-forvaltningen. Likevel er det alternativer leverandøren mener bør drøftes relatert til opptak, lagring og søk i biometri som kan bidra til en ytterligere kvalitets- og sikkerhetsheving av ID-forvaltningen. Disse alternativene kan implementeres hver for seg, men vil ha størst effekt ved samlet implementering.

13.2.1 Alternativ 1: Opptak av biometri for alle brukergrupper (EØS-borgere, norske statsborgere og tredjelandsborgere)

Som beskrevet i del 1, pågår det et arbeid med knytning av biometri mellom Folkeregisteret, passregisteret og utlendingsregisteret. Dette arbeidet er en forutsetning for å kunne sikre «unike» identiteter i Folkeregisteret og «låse» en person til et identitetsnummer (fødselsnummer eller d-nummer) og således etablere en grunnidentitet. Dette arbeidet er en forutsetning for visjonen: *En person, en identitet i Norge.*

For å sikre *en person, en identitet i Norge* er det videre en forutsetning at den enkelte person avlegger biometri i ett eller flere av biometriregistrene. Som beskrevet i del 2 avhenger dagens praksis av hvilken brukergruppe personen tilhører. For å oppnå høyest mulig sikkerhet og kvalitet i ID-forvaltningen, vil det ideelle være om alle avlegger biometri uavhengig av brukergruppe. Det erkjennes at dette er en utfordring, og da særlig for EØS-borgere med rett til fri personbevegelighet ved opphold under tre måneder[470]. Isolert sett er det leverandørens vurdering at «jo flere, jo bedre» gjelder når det kommer til å avlegge biometri og at det har en verdi for status «unik» i Folkeregisteret selv om ikke alle personer som oppholder seg i Norge har avlagt biometri.

Under følger en kort drøfting for opptak av biometri for de ulike brukergruppene:

[470] Direktivet om fri personbevegelighet gir EØS-borgere og deres familiemedlemmer rett til å reise inn i et annet medlemsland og ta opphold og arbeid der i inntil tre måneder uten andre formaliteter enn å oppfylle et legitimasjonskrav

Norske statsborgere: Opptar kun biometri i forbindelse med utstedelse av pass, hvilket betyr at det fortsatt er en liten andel av norske statsborgere som ikke har avlagt biometri. Hvis målet er at det skal være registrert biometri for alle norske statsborgere, må opptak av biometri i en eller annen form bli obligatorisk. Opptak av biometri for resterende andel kan skje på ulike måter, dette er beskrevet nærmere i kapittel 10.2 for de ulike brukergruppene.

EØS-borgere: Opptar ikke biometri i Norge, verken ansiktsfoto eller fingeravtrykk, da de i utgangspunktet skal kunne fremvise gyldig ID-bevis fra hjemland i form av pass eller nasjonalt ID-kort.

Som beskrevet i del 2 (kapittel 6.1.5) er EØS-borgere en gruppe som trekkes frem som en utfordring i dagens ID-forvaltning, og da særlig med henblikk på ID-misbruk relatert til arbeidskriminalitet. I 2016 ble det avdekket at ca. 40 prosent av ID-misbruk knyttet til registrering av EØS-borgere var relatert til tredjelandsborgere med EØS-dokumenter. Politiet mener dette kan tilskrives uklare regler, rutiner og praksis for identitetskontroll før de registreres (gjelder kun for opphold i mer enn tre måneder).[471]

Et alternativ for å kunne oppta biometri på denne brukergruppen kan være å gi EØS-borgere muligheten til å få utstedt nasjonalt ID-kort eller at tjenesteeiere krever at ID-kort fremvises for å få tilgang til sentrale offentlige tjenester og ytelser der det kreves fysisk legitimasjon. For nærmere beskrivelse se kapittel 10.2. Det er leverandørens vurdering at det kan være mulig å samkjøre nødvendig registrering knyttet til utstedelse av nasjonalt ID-kort med prosessen for d-nummer rekvirering og at dette kan være mer brukervennlig og hensiktsmessig med tanke på kvalitet og sikkerhet, samt mer effektiv ressursbruk. Et annet alternativ er å pålegge EØS-borgere å avlegge biometri når de kommer til landet, men dette anses som mindre realistisk, da det strider med direktivet om fri personbevegelighet innenfor EØS, slik det er beskrevet i dag.

Tredjelandsborgere: I motsetning til overnevnte grupper opptas biometri i en eller annen form for alle tredjelandsborgere, men det er stor forskjell i praksis for hvor det lagres, om det lagres og hvor lenge det eventuelt lagres. Dette avhenger om personen søker opphold, visum eller asyl. Hvilken biometri som opptas og praksis for lagring er nærmere beskrevet i kapittel 6.1.6.

Styrker:

- Bidrar til å oppnå visjonen *en person, en identitet i Norge* ved at alle med tilknytning til Norge vil ha kvalitetsindikatoren «unik» registrert i Folkeregisteret (avhenger av valgt modell for nasjonalt ID-kort, jf. kapittel 10)
- Økt kvalitet i ID-forvaltning av EØS-borgere og utstedelse av et sterkere ID-bevis
- Anvendelse av biometri kan være med å effektivisere tjenestetilbudet fra det offentlige som igjen bidrar til økt brukervennlighet
- Bidrar til å redusere ID-misbruk og arbeidskriminalitet

[471] POD, «UNIK-utredning», 2017

Svakheter:

- Utfordrende å gjennomføre opptak og lagring av biometri for EØS-borgere som i dag er underlagt EU-direktivet om fri personbevegelighet
- For norske statsborgere hvor det ikke tidligere har vært krav om å besitte minst et gyldig ID-bevis, og for EØS-borgere hvor det har vært tilstrekkelig å bære pass eller ID-bevis fra hjemland, vil nye krav til å avlegge biometri redusere brukervennligheten
- Obligatorisk ID-bevis for alle som oppholder seg i Norge kan oppleves som et retningsskifte fra å være et samfunn basert på tillit til et samfunn hvor «staten» får mer kontroll over innbyggerne

13.2.2 Alternativ 2: Opptak, lagring og søk i fingeravtrykk i tillegg til ansiktsfoto

Som beskrevet i del 2 er det behov for å jobbe med de rettslige rammene, herunder vurdere personvernkonsekvenser, for å kunne ta stilling til om det skal åpnes for sentrallagring av fingeravtrykk i pass- og ID-kortloven. Det er leverandørens oppfatning at nødvendige endringer i lovverket for opptak, lagring og søk i fingeravtrykksbiometri er mer krevende enn de teknologiske tilpasningene.

Søk med både fingeravtrykk og ansiktsfoto gir større treffsikkerhet enn søk basert på kun en av biometriformene. Leverandøren er gjort oppmerksom på at det kan ha betydning for biometrisøket om det er forskjeller i kvaliteten ved opptak av ansiktsfoto i utlendingssaker og pass/ID-kort saker, og at søk ved bruk av begge biometriformer vil påvirke muligheten til effektiv utfylling av status «unik». Om søk i biometri ikke gjøres med flere biometriformer, forringes kvaliteten på søket og risiko for etterslep på ID-avklaringer øker. Dette alternativet drøfter hvorvidt fingeravtrykk og ansiktsfoto bør ses i sammenheng i opptak, lagring og søk i biometri.

Det er i praksis to biometriregistre i dagens ID-forvaltning; passregisteret og utlendingsregisteret. Med bakgrunn i planene for innføring av nasjonalt ID-kort omtales passregisteret som pass og ID-kortregisteret.

Lagring og søk i fingeravtrykk utover ansiktsfoto i pass og ID-kortregisteret

I dagens register lagres ansiktsfoto med hjemmel i passloven. I forbindelse med utstedelse av pass innhentes fingeravtrykk fra søker, hvor bildet av fingeravtrykket lagres i passets elektroniske brikke og senere slettes fra saksbehandlingssystemet og opptaksutstyr for biometri, dette hindrer fremtidig søk i biometri på fingeravtrykk.

POD har påpekt at fingeravtrykk i pass- og ID-kortregistrene ikke bare vil effektivisere ID-kontrollen ved utstedelse av pass og ID-kort, men også redusere faren for misbruk av identitet og identitetsdokumenter, effektivisere grensekontrollen og lette identifiseringsarbeid etter ulykker og katastrofer (døde og savnede) og personer som ikke kan gjøre rede for seg.

Gjennomføring av alternativet innebærer at passmyndigheten vil være i besittelse av begge biometriformene for en betydelig andel av befolkningen (fingeravtrykk i tillegg til ansiktsfoto). For å oppnå et komplett biometriregister for hele befolkningen må alternativ 1 og 2 implementeres samlet.

Alternativet kan potensielt øke muligheten for formålsutglidning ved at data som først er samlet inn for et formål etter hvert brukes til å dekke et annet formål enn det opprinnelig var tiltenkt. Alternativet kan innebære sikkerhetsutfordringer ved at en så vidt stor database med biometriske opplysninger vil være svær verdifull for andre. Dette bør imidlertid ikke være avgjørende for alternativet, men det er viktig at det tas nødvendige hensyn som i varetar tilstrekkelig sikkerhet.

For brukerne vil opptak og lagring av begge biometriformer gjøre brukerreisen mer smidig, da søknadsprosessen ved fremtidig tap og fornyelse av pass og ID-kort kan forenkles ved at biometri kan gjenbrukes og at bruker således slipper fysisk oppmøte. Dette med utgangspunkt i at fingeravtrykk er lagret i pass- og ID registeret, utover kun å være lagret fysisk i passet. Personen slipper derfor å møte opp fysisk og for å avlegge ny biometri. Åpnes det for lagring av, og søk med fingeravtrykk i pass- og ID-kortregistrene vil kvaliteten på søkene bli enda bedre og arbeidsbelastningen vil reduseres ved mindre manuelle søk, eksempelvis for Kripos.

Lagring og søk av fingeravtrykk og ansiktsfoto i Utlendingsregisteret

For denne brukergruppen innebærer det ingen endring fra gjeldende regelverk. Etter utlendingsloven § 100 første ledd kan det, ut fra et formål om identifisering og verifisering, tas fingeravtrykk og ansiktsfoto av alle utlendinger som ikke kan dokumentere sin identitet, eller hvor det er grunn til å mistenke falsk identitet. Det arbeides med en mulig forskriftsendring som sier at det skal tas fingeravtrykk og ansiktsfoto av alle som søker om opphold, visum eller grensebeboerbevis. Dette er beskrevet nærmere i kapittel 6.1.6.

Styrker:

- Et mer komplett biometriregister for de brukergrupper det i dag opptas biometri. Dette bidrar til å effektivisere ID-kontrollen ved utstedelse av pass og ID-kort og ID-kontroll knyttet til inn- og utreise
- Mer enhetlig praksis for opptak av biometri mellom brukergruppene bidrar til en enklere og mer robust ID-forvaltning
- Reduserer arbeidsbelastningen knyttet til manuelle søk i biometriregistrene da fingeravtrykk har mer treffsikre algoritmer for automatiske søk
- Legger til rette for bedre brukerreise med enklere søknadsprosess for tap og fornyelse av pass- og ID-kort, ved at søker slipper oppmøte for nytt opptak av biometri
- Fjerner noe av utfordringene med kvalitet og begrensninger i ansiktsfoto (ulik bildekvalitet) som vanskeliggjør sammenligning, men dette blir delvis løst ved at ansiktsfoto erstattes med ansiktsbiometri (svakere algoritmer for gjenkjenning enn fingeravtrykk)

Svakheter:

- Fare for formålsutglidning hvor lagret biometri potensielt benyttes til andre formål enn opprinnelig tiltenkt
- Et samlet biometriregister vil være svært verdifullt for andre og nødvendige sikkerhetstiltak kan være ressurskrevende

13.3 Oppsummering av alternativer opp mot sikkerhet, brukervennlighet og ressursbruk

Under har leverandøren overordnet oppsummert drøftingen med tanke på sikkerhet, brukervennlighet og ressursbruk. Tabellen under oppsummerer drøftingen basert på rammeverket for pluss-minusmetoden beskrevet i kapittel 1.3.

Alternativ 1, *opptak av biometri for alle brukergrupper*, vurderes å ha en stor positiv konsekvens for sikkerheten da dette vil muliggjøre status «unik» for alle identitetsnummer og legger til rette for at alle får utstedt sterke ID-bevis i form av et pass eller nasjonalt ID-kort. Alternativet vil videre sikre at det blir vesentlig mer krevende å overta identiteter eller operere med flere identiteter. Alternativet vil ikke medføre noen konsekvens for brukervennlighet ettersom biometrien tas i forbindelse med oppmøte/ID-kontrollen for pass- og nasjonalt ID-kort (jf. kapittel 10.2). På samme grunnlag vil ikke alternativet ha noen konsekvens for ressursbruk, utover konsekvensene beskrevet tilknyttet kapittel 10.2.

Alternativ 2, *opptak, lagring og søk i fingeravtrykk i tillegg til ansiktsfoto*, vurderes å ha en middels positiv konsekvens for sikkerheten ettersom dette muliggjør bedre og mer effektive algoritmer for biometrisøk. Videre anses alternativet å ha en liten positiv konsekvens for brukervennlighet da man betydelig kan redusere antall oppmøter som følge av sentrallagring av fingeravtrykk. Denne konsekvensen er nærmere beskrevet og behandlet i kapittel 14. Det er leverandørens vurdering at tiltaket vil ha en liten positiv konsekvens for ressursbruk ettersom det vil være et redusert behov for manuelle søk og redusert oppmøte fra søker ved tap eller fornyelse av pass- og ID-kort. Fingerbiometrien tas allerede i forbindelse med pass- og ID-kort og forventes dermed ikke å påvirke ressursbruken negativt.

	Sikkerhet	Bruker-vennlighet	Ressursbruk
Alternativ 1: Opptak av biometri for alle brukergrupper	+++	0	0
Alternativ 2: Opptak, lagring og søk i fingeravtrykk i tillegg til ansiktsfoto	++	+	+

Tabell 27 Oppsummering av drøfting for opptak, lagring og søk i biometri

14 Vurdering av alternativer knyttet til behov for fysiske oppmøter

14.1 Oppsummering vurdering nåsituasjonen

Som beskrevet i kapittel 5 har brukerne generelt høy tillit til de fleste aktører i ID-forvaltningen. Særlig Folkeregisteret anses å ha stor nytteverdi for aktører i ID-forvaltningen, men også fra et brukerperspektiv. Det poengteres likevel at samlet dokumentasjon på brukervennlighet direkte knyttet til ID-forvaltning er relativt begrenset. Høy grad av digitalisering og tilrettelegging for eID medfører videre at tilgang på tjenester i offentlig sektor innebærer få fysiske oppmøter og relativt lavt behov for fremvisning av fysiske ID-bevis.

For utstedelse (og fornyelse) av de fleste ID-bevis er det derimot krav om at bruker møter fysisk. En gjennomsnittlig norsk borger vil eksempelvis med dagens regelverk måtte regne med opptil 30 oppmøter i et livsløp for å anskaffe og fornye de mest brukte fysiske ID-bevisene (pass, førerkort og bankkort med bilde). Som nevnt i nåsituasjonsanalysen står også EØS-borgere og tredjelandsborgere overfor oppmøtekrav som kan virke overflødige. Eksempelvis vil EØS-borgere måtte møte hos politiet for å registrere seg ved opphold over 3 måneder, i tillegg til dette må de møte opp hos en annen aktør for å anskaffe identitetsnummer i form av d-nummer eller fødselsnummer (beskrevet nærmere i kapittel 3.1.3). For tredjelandsborgere må eksempelvis asylsøkere oppta biometri to ganger ved ankomst til Norge. I lys av dette er det leverandørens vurdering at det foreligger et potensial for å forbedre brukeropplevelsen ved at frekvensen av påkrevde fysiske oppmøter, og antall ganger biometri må avlegges, blir redusert.

Det fremkommer videre fra nåsituasjonsanalysen at det eksisterer enkelte utfordringer knyttet til deling av data og registertilgang mellom aktører. Fra et juridisk standpunkt er dette omtalt i kapittel 4.2.4, der kartleggingen viser at det ikke finnes et sektorovergripende regelverk for samhandling på og koordinering av ID-området. Som også påpekt i kapittel 3.2.9 oppleves datadeling som en utfordring for effektivt samarbeid. I samtaler med aktørene fremkommer det flere ønsker om økt datadeling. For eksempel har enkelte banker gitt uttrykk for et ønske om økt registertilgang, blant annet for å ha bedre forutsetninger for sikre utstedelser og opprettelse av kundeforhold.[472] Mangelen på deling av ansiktsfoto og signatur, mellom utstedere av ID-bevis, medfører i praksis at den samme informasjonen må opptas flere ganger. Mangelen på transparens og tilgang til data på tvers utgjør derfor, etter leverandørens vurdering, en forklarende årsak til at brukere står overfor mange fysiske oppmøter.

14.2 Drøfting av alternativer knyttet til behov for fysiske oppmøter

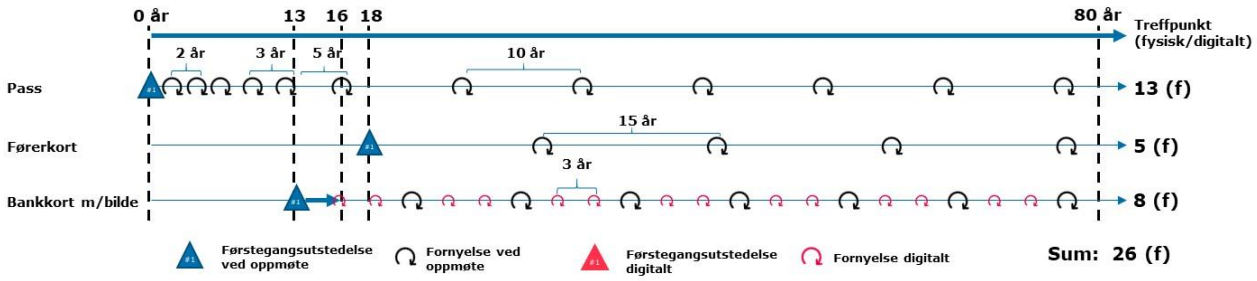
Alternativene under har til hensikt å øke brukervennligheten i ID-forvaltningen og redusere behovet for fysiske oppmøter. Alternativene bygger ikke direkte på hverandre, men kan på enkelte områder ha gjensidig påvirkning.

[472] Informasjon forelagt leverandøren i korrespondanse med enkelte banker og Finans Norge

14.2.1 Alternativ 1: Legge til rette for deling og gjenbruk av data for en mer effektiv brukerreise, eksempelvis ansiktsfoto, signatur og annen personinformasjon

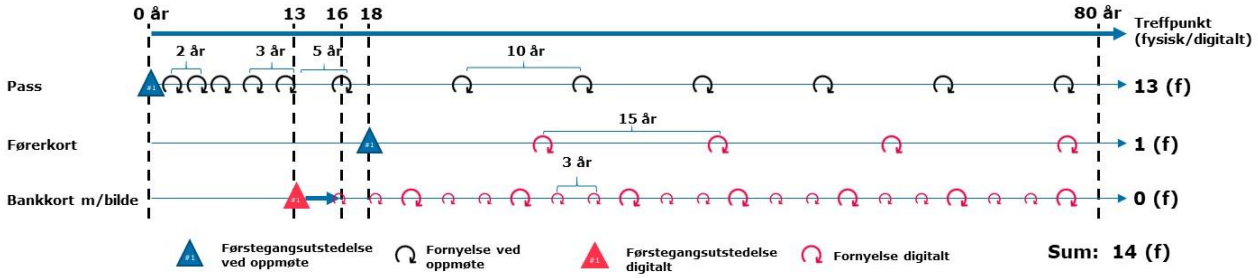
Som poengtert over er det et betydelig potensial for å forenkle brukerreisene ved å legge til rette for økt deling av data på tvers i ID-forvaltningen. Gjennom å tilrettelegge for at ansiktsfoto som opptas i forbindelse med passutstedelse (og i fremtiden, nasjonalt ID-kort) kan gjenbrukes til andre ID-bevis kan brukerreisen gjøres mer effektiv. Dette vil også kunne gjelde for opptak og gjenbruk av signatur.

Et relevant og konkret eksempel er dagens prosess for utstedelse av førerkort. Under dagens reglement må bruker fornye sitt førerkort minst hvert 15. år. Nødvendig informasjon for fornyelse kan oppgis på nett, men for å oppta nytt ansiktsfoto på førerkortet stilles det krav om oppmøte på trafikkstasjon. Oppmøtekravet for å fornye bilde på førerkortet medfører at bruker i et livsløp må møte på trafikkstasjon fire ganger etter førstegangsutstedelse for å fornye kortet (se visualisering av antall treffpunkt i et livsløpsperspektiv, kapittel 5.1.7). Gjennom tilrettelegging for deling og gjenbruk av data kan SVV gis tilgang til ansiktsfoto og signatur som opptas og lagres i forbindelse med utstedelse av pass og nasjonalt ID-kort. En slik løsning vil i praksis muliggjøre at fornyelsen av førerkort i sin helhet kan foregå digitalt, uten behov for oppmøte. En reduksjon av fire fysiske treffpunkt for bruker innebærer en besparelse på 960 kroner (240 kroner per fornyelse)[473], samt en reduksjon i total brukertid på ca. 4 timer[474] i et livsløp. Gitt forutsetningene for tidsverdi og antall førerkort i omløp (nærmere beskrevet i kapittel 5.1.7 og 5.1.8) vil en digitalisering av fire fornyelser av førerkort medføre om lag 30 millioner kroner årlig i spart brukergebyr, samt 45 millioner kroner årlig i verdi av redusert brukertid. Tilsvarende vil en digitalisering av 8 oppmøter for førstegangsutstedelse og fornyelse av bankkort med bilde innebære en besparelse på 6 timer brukertid i et livsløp per bruker, og 54 millioner kroner i årlig redusert tidsverdi. Gitt trendene som beskrevet i kapittel 9 og øvrige vurderte alternativ i del 3 er trolig det fremtidige behovet for banknæringen for bankkort med tilhørende bilde begrenset. Dette er ikke tatt hensyn til i beregningene eller figurene under. Eksemplene over knytter seg til fornyelse av førerkort og bankkort med bilde, men tankesettet vil også kunne gjelde for andre offentlige og private utstedte ID-bevis. En illustrasjon av reduksjonen i antall fysiske oppmøter for førerkort og bankkort er vist i figurene under.



Figur 64 Oppmøter og fornyelser av pass, førerkort og bankkort med bilde, uten deling av ansiktsfoto/signatur

[473] Brukergebyr for å fornye førerkort med bilde på trafikkstasjon er 240 kroner høyere enn kostnaden ved å fornye på nett (uten opptak av bilde): (380 kroner – 140 kroner) = Besparelse på 240 kroner
[474] Brukertid per fornyelse av førerkort estimert til 61 minutter (nærmere beskrevet i kapittel 5.1.7)



Figur 65 Oppmøter og fornyelser av pass, førerkort og bankkort med bilde, med deling av ansiktsfoto/signatur

Videre vil deling av biometrisk informasjon være et område med potensial for å gjøre brukerreisen mer effektiv. Eksempelvis vil det ved passutstedelse til tredjelandsborgere som får innvilget statsborgerskap kunne være mulig å støtte seg på biometriopptak fra utlendingsregisteret (beskrevet nærmere under 13.2.2).

I sum er det leverandørens oppfatning at økt tilrettelegging for deling av ansiktsfoto, signatur, fingeravtrykk og annen informasjon, vil bidra til å redusere behovet for fysiske oppmøter og forenkle brukerreisen for både norske og utenlandske borgere. For å kunne legge til rette for deling og gjenbruk av data vil det kreves endringer i eksisterende regelverk. Implementering av alternativ 1 forutsetter regelverksendringer som muliggjør deling av data mellom aktørene. Leverandøren mener at endring av regelverket for å forbedre brukerreisen og effektivisere forvaltningen bør være løsbart. Det legges til grunn at bruker som standard gir samtykke til deling av bilde og signatur til definerte formål som en del av regelverket.

Styrker

- Bygger opp under flere av de sentrale trendene i kapittel 9.1. Omfatter blant annet en økende kundeforventning om at data skal kunne avgis «kun en gang», samt økte krav til ID-aktører om å optimalisere brukerreisen gjennom selvbetjeningsløsninger
- Mer tids- og kostnadseffektive brukerreiser for brukerne i ID-forvaltningen, jf. besparelser beskrevet over
- For aktørene i ID-forvaltningen
    - Høyere sikkerhet og kvalitet ved behandling av personinformasjon (eksempelvis høyere forventet kompetanse og bedre teknisk utstyr ved pass- og ID-kontor tilknyttet billedtaking enn ved trafikkstasjoner og bankfilialer)
    - Redusert belastning på virksomhetenes kapasitet og ressursbruk som følge av færre oppmøter og mindre behov for fysisk utstyr
- Vil bidra til å sikre konsistent datagrunnlag på tvers av aktørene i ID-forvaltningen

Svakheter

- Å tilrettelegge for økt deling av data mellom register vil medføre kostnader knyttet til tekniske løsninger

- Hver løsning vil kreve hjemmel i lovverket, og vil måtte vurderes opp mot krav til personvern. Særlig vil dette måtte ses i sammenheng med en styrket vektlegging av at brukere i større grad eier sine egne data (omtalt i kapittel 9.1)

- Stiller større krav til at personinformasjon som opptas er korrekt og verifisert

14.2.2 Alternativ 2: Optimalisere brukers krav til fysisk oppmøte og gjenbruk av ID-kontroll

Leverandøren har i 14.1 pekt på eksempler der det kan stilles spørsmål ved det reelle behovet for fysisk oppmøte. Alternativet som utdypes under drøfter tiltak som medfører reduksjon i oppmøtene som brukere står overfor utover det beskrevet i kapittel 14.2.1.

For det første er det leverandørens oppfatning at det benyttes unødvendige ressurser ved at brukere må gjennomføre samme ID-kontroll hos flere aktører. Leverandøren vurderer det til å være et potensial for å optimalisere antall fysiske oppmøter som EØS-borgere og tredjelandsborgere må gjennom ved ankomst til landet. Slik beskrevet i kapittel 15 vil samling av aktører som gjennomfører ID-kontroll, og gjenbruk av denne ID-kontrollen til andre formål, etter leverandørens oppfatning kunne bidra til å redusere brukers oppmøtekrav.

For det andre eksisterer det til dels et uutnyttet potensial i å la eID i større grad erstatte fysisk legitimering ved oppmøte. I tilfeller der bruker ikke må avlegge biometrisk informasjon, eller ta nytt ansiktsfoto, bør det vurderes å i større grad legge til rette for å kunne fornye ID-bevis digitalt ved bruk av eID. Leverandøren viser her til gjeldende praksis for fornyelse av statlige ID-bevis i Finland, der fornyelse av pass og nasjonalt ID-kort under visse vilkår kan fornyes elektronisk.[475] En modell til etterfølgelse kan også være nåværende prosess for erstatning av tapte norske førerkort, som p.t. ikke krever oppmøte. Alternativ 2 må ses i sammenheng med nye løsninger for deling av data mellom utstedere.

For det tredje vil gjenbruk av ID-kontrollen som gjennomføres ved registrering, utstedelse og fornyelse av pass som grunnlag for senere utstedelse av private eID-er, slik beskrevet i kapittel 11.2.2, øke brukervennligheten og redusere krav til fysisk oppmøte for brukerne. Brukere kan få utstedt private eID på tilsvarende sikkerhetsgrunnlag som pass, og vil ikke behøve å gjennomføre en fysisk ID-kontroll ved en bankfilial eller ved et postkontor/post i butikk senere.

Spesielt om gyldighetstid for pass og nasjonalt ID-kort

Et potensielt ytterligere tiltak for å redusere frekvensen av fysiske oppmøter vil være å til dels fristille kravet om fysisk oppmøte fra fornyelsen av relevante ID-bevis. I høringsforslaget til ny forskrift for pass og nasjonale ID-kort planlegges det for at gyldighetstiden for nasjonalt ID-kort settes til fem år og nye pass settes til enten fem år eller at dagens gyldighetstid på ti år videreføres. Leverandøren mener at mange av sikkerhetsbehovene i pass og nasjonalt ID-kort potensielt kan ivaretas ved fornyelse uten behov for fysisk oppmøte, spesielt ved at fysisk oppmøte for å oppdatere ansiktsfoto og fingeravtrykk gjennomføres sjeldnere enn hvert femte år. En slik løsning vil muliggjøres ved sentrallagring av biometri, slik beskrevet i kapittel 13.2.2. Med sentrallagring av fingeravtrykk ser leverandøren et potensial i å kutte opptil 13 fysiske oppmøter for fornyelser av pass og nasjonale ID-kort i et livsløp. En reduksjon i 13

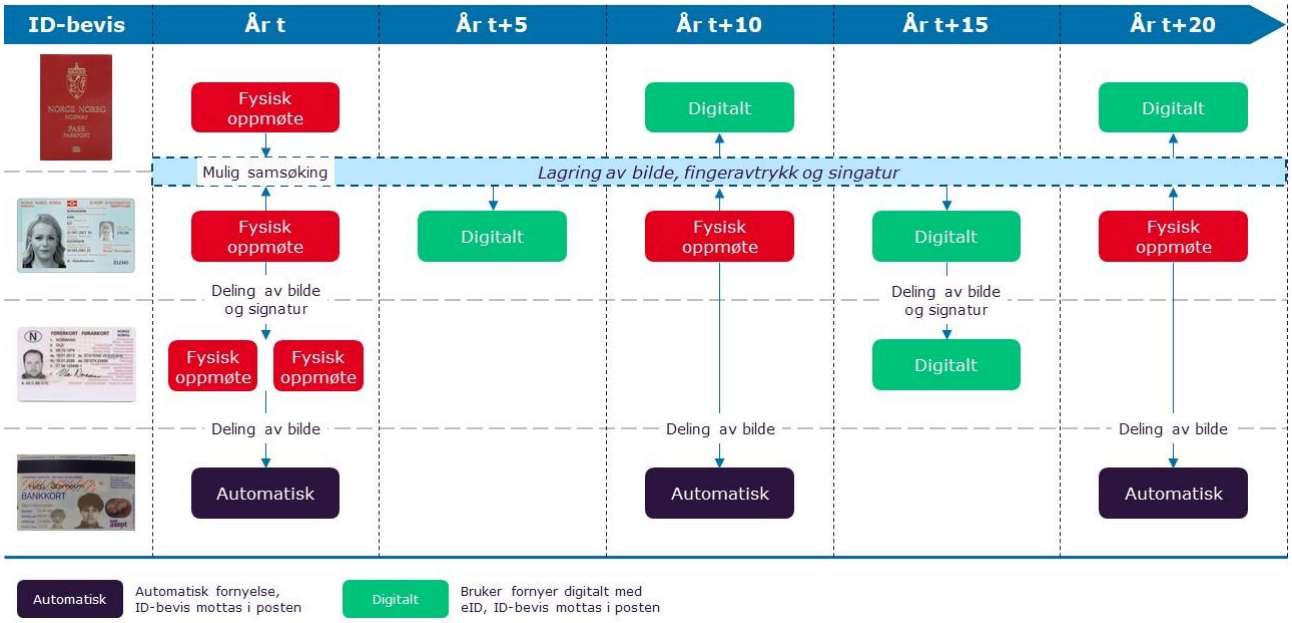
[475] Leverandøren viser til samtaler gjennomført med POD 10.06.2019 og informasjon oppgitt på poliisi.fi

oppmøter for pass og nasjonale ID-kort vil etter leverandørens estimater kunne redusere brukertid og brukergebyr per bruker med henholdsvis ca. 16 timer og 1 908 kroner i et livsløp.[476] For samfunnet vil reduksjonen årlig tilsvare omtrent 120 millioner kroner i redusert brukergebyr og 375 millioner kroner i verdi av påløpt brukertid.[477]

Den potensielle forbedringen i brukervennlighet av et slikt tiltak må i tilfellet også vurderes fra et sikkerhets- og personvernsperspektiv. Leverandørens vurdering av lengden på gyldighetstid på de to ID-bevisene er avhengig av omfanget av fysiske oppmøter det stilles krav om.

Eksempler på fremtidige brukerreiser for førstegangsutstedelse og fornyelse av identitetsnummer og ID-bevis

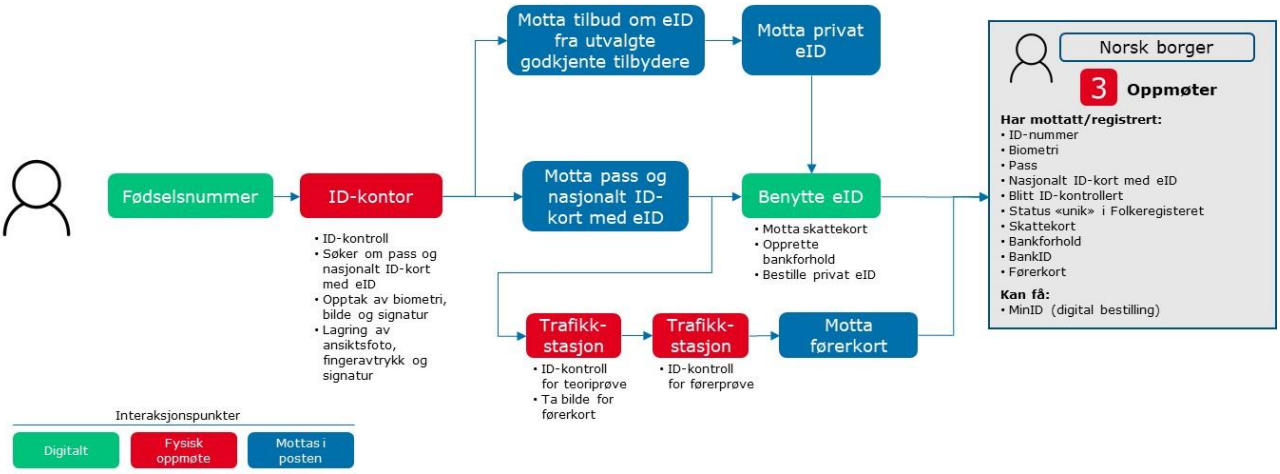
Figuren under illustrerer hvordan deling av data og bruk av eID for digital fornyelse av ID-bevis vil påvirke antall fysiske oppmøter for brukeren. Sammenlignet med figuren for dagens praksis i kapittel 5.1.3, vil brukeren kun trenge å møte opp hvert tiende år for å avgi oppdatert biometri etter at førstegangsutstedelse av ID-bevisene i figuren er gjennomført.



Figur 66 Oppmøter ved utstedelse og fornyelse av ID-bevis med deling av data og digital og automatisk fornyelse av ID-bevis

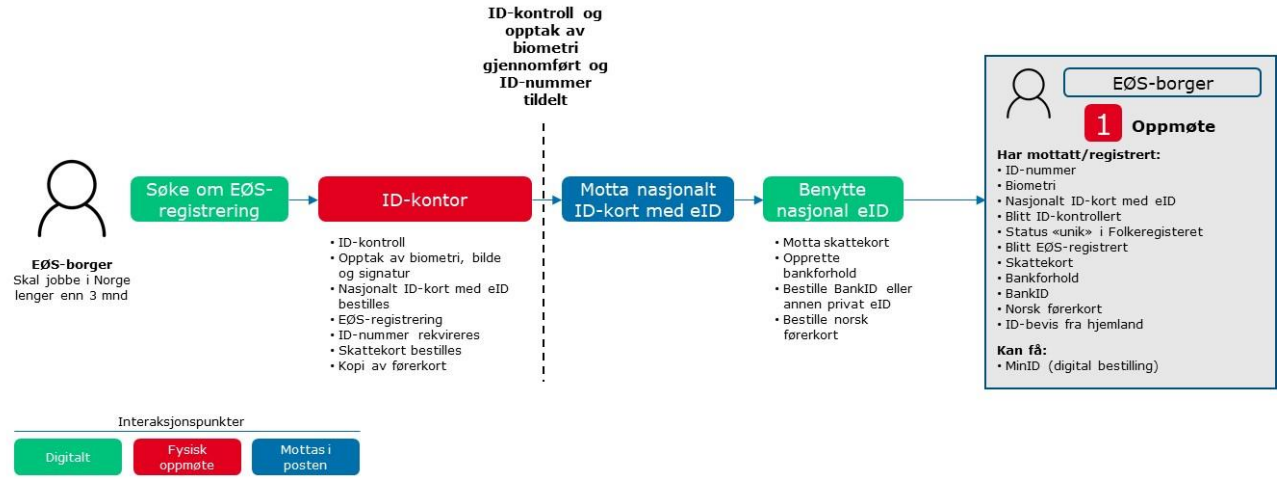
Leverandøren har under illustrert hvordan prosessen for førstegangsutstedelse av ID-bevis for en norsk borger basert på alternativet beskrevet over. Sammenlignet med brukerreisen for førstegangsutstedelse skissert i kapittel 5.1.5, vil en norsk borger ha behov for ett mindre fysisk oppmøte.

[476] Utregningen legger til grunn at kostnaden for digital fornyelse av pass eller nasjonalt ID-kort utgjør 40 prosent av kostnaden tilknyttet utstedelse ved fysisk oppmøte
[477] Utregningen bygger på forutsetninger for tidsverdi, antall pass og ID-kort i omløp og antall år i et livsløp lagt til grunn i kapittel 5.1.7 og 5.1.8



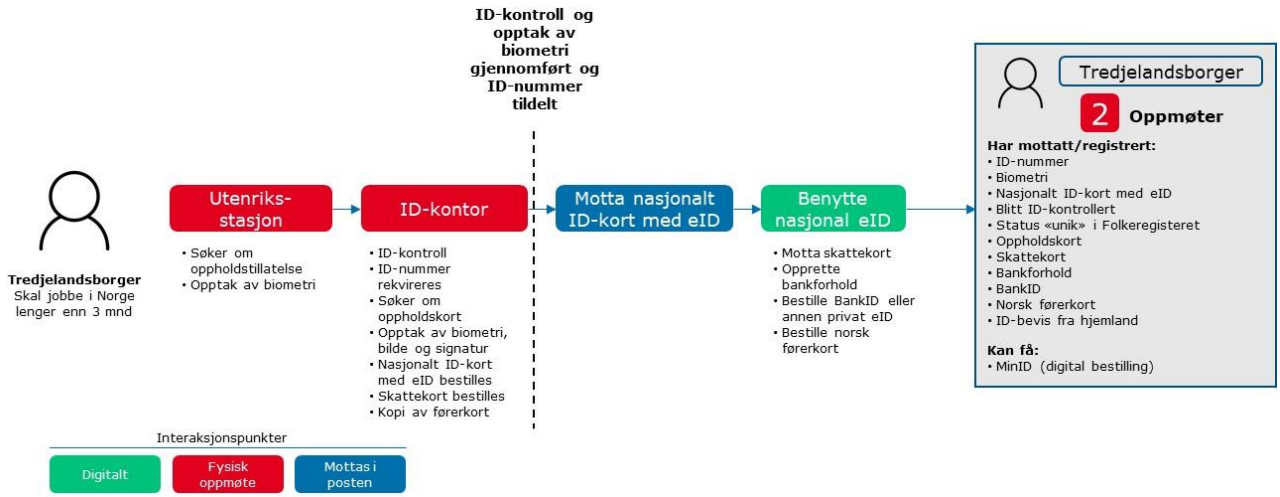
Figur 67 Eksempel på fremtidig brukerreise for norsk borger for førstegangsutstedelse av identitetsnummer og ID-bevis

Figuren under viser et eksempel på hvordan en EØS-borgers prosess for førstegangsutstedelse av ID-bevis kan se ut. Sammenlignet med brukerreisen for registrering og førstegangsutstedelse av identitetsnummer og ID-bevis skissert i kapittel 5.1.6, vil en EØS-borger kunne redusere antall oppmøter med tre eller fire.



Figur 68 Eksempel på fremtidig brukerreise for EØS-borger for førstegangsutstedelse av identitetsnummer og ID-bevis

Tredjelandsborgere vil kunne ha behov for tre færre oppmøter, slik illustrert i figuren under og sammenlignet med brukerreisen i kapittel 5.1.6.



Figur 69 Eksempel på fremtidig brukerreise for tredjelandsborger for førstegangsutstedelse av identitetsnummer og ID-bevis

Styrker

- Færre krav til oppmøte reduserer belastningen på virksomhetenes kapasitet og ressursbruk
- Tids- og kostnadsbesparende for brukere med færre oppmøtekrav, jf. besparelser beskrevet over

Svakheter

- Det kan stilles spørsmål ved om reduserte oppmøtekrav vil ha negative sikkerhetsmessige konsekvenser. Oppmøte er blant annet et sentralt element i å oppnå høyeste sikkerhetsnivå for elektronisk ID. Færre oppmøter reduserer også mulighetene for kontinuerlig oppdatering av biometrisk informasjon (fingeravtrykk og ansiktsfoto)

14.3 Oppsummering av alternativer opp mot sikkerhet, brukervennlighet og ressursbruk

Under har leverandøren overordnet oppsummert drøftingen med tanke på sikkerhet, brukervennlighet og ressursbruk. Tabellen under oppsummerer drøftingen basert på rammeverket for pluss-minusmetoden beskrevet i kapittel 1.3.

Alternativ 1, *legge til rette for deling og gjenbruk av data for en mer effektiv brukerreise, eksempelvis ansiktsfoto, signatur og annen personinformasjon*, vurderes å ha en liten positiv konsekvens for sikkerheten da deling av data vil medføre økt kvalitet i saksbehandlingen ved opptak av ansiktsfoto, signatur og annen personinformasjon. Alternativet vurderes å ha stor positiv konsekvens med tanke på brukervennlighet ettersom brukere kun trenger å ta ansiktsfoto, avgi signatur og annen personinformasjon ett sted. Videre vurderer leverandøren at alternativet vil ha middels positiv konsekvens på ressursbruken, ettersom det vil gi økt effektivitet i saksbehandlingen hos flere aktører, reduserte antall oppmøter og mindre behov for fysisk utstyr.

Alternativ 2, *optimalisere brukers krav til fysisk oppmøte og gjenbruk av ID-kontroll*, vurderes å ha liten negativ konsekvens for sikkerheten, ettersom færre oppmøter betyr at brukerne sjeldnere vil bli ID-kontrollert og sjeldnere vil avgi oppdatert biometri (i

sammenligning med ikke vedtatte planer). Leverandøren vurderer at den negative konsekvensen er liten da oppmøte og oppdatering av biometri vil gjøres hvert tiende år og ID-kontroller i større grad vil bestå elektroniske autentiseringer i fremtiden, slik beskrevet i kapittel 11.2.2. Videre vurderes alternativet å ha en meget stor positiv konsekvens for brukervennligheten, da reduserte behov for fysiske oppmøter vil føre til betydelige besparelser i både brukergebyr og brukertid i et livsløpsperspektiv. Leverandøren vurderer at alternativet også vil ha en meget stor positiv konsekvens på ressursbruken, da færre krav til oppmøter vil redusere belastningen på aktørenes saksbehandlingskapasitet og dermed virke ressurseffektiviserende.

	Sikkerhet	Bruker-vennlighet	Ressursbruk
Alternativ 1: Legge til rette for deling og gjenbruk av data for en mer effektiv brukerreise, eksempelvis ansiktsfoto, signatur og annen personinformasjon	+	+++	++
Alternativ 2: Optimalisere brukers krav til fysisk oppmøte og gjenbruk av ID-kontroll	-	++++	++++

Tabell 28 Oppsummering av drøfting knyttet til behov for fysiske oppmøter

15 Vurdering av alternativer knyttet til styring og struktur

Kapittelet om styring og struktur behandles isolert, men skisserte alternativene er sentrale virkemidler som kan bidra til å realisere effekten av alternativene omtalt i kapittel 10-14.

15.1 Oppsummering vurdering nåsituasjonen

Som nevnt i kapittel 3 er det en økende forståelse for og oppmerksomhet rundt ID-relaterte problemstillinger i Norge. Flere av virksomhetene i privat og offentlig sektor har gjennomført individuelle og tverrsektorielle tiltak for å møte utfordringer innen ID.

Sektorprinsippet står sterkt i Norge og ID-forvaltningen kjennetegnes ved tverrsektorielle problemstillinger. Leverandørens inntrykk er at bevisstheten rundt denne typen problemstillinger har økt, og det finnes flere gode eksempler på vellykket omstilling på tvers av departementsområder, for eksempel ID-porten og modernisering av Folkeregisteret. Det er mange gode intensjoner, men likevel kjennetegnes dagens ID-forvaltning av lav endringstakt og gjennomføringsevne. Dette er beskrevet i kapittel 3.2.1 om tidkrevende beslutningsprosesser og gjentatte forsinkelser knyttet til nye pass og ID-kort.

Det er ikke en ansvarlig eier eller en aktør som er samordner, har en premissgiverrolle og/eller instruksjonsmyndighet i ID-forvaltningen. Leverandøren oppfatter at en del roller og ansvar ikke er tydelig definert. Det er lav grad av strategisk og overordnet styring av ID-forvaltningen, noe som gir en sektoriell og fragmentert tilnærming. Utvalgte etater og virksomheter har, gjennom arbeidet i KoID, i stor grad en omforent visjon for fremtidens ID-forvaltning. Imidlertid er det få felles mål og styringsparametere på tvers av sektorer. Hver sektor ivaretar sitt formål og ansvarsområde, men en mer helhetlig ivaretagelse av området er savnet blant de fleste involverte aktører.

Videre er det ingen aktører som har ID som sin kjerneoppgave med unntak av NID som diskutert i kapittel 3.2.2. Et stort antall offentlige og private virksomheter har det som deloppgave eller er involvert i deler av prosessen. Leverandørens inntrykk er at det er en risiko for at det legges for stor vekt på egne resultater og ikke på ID-forvaltningen samlet. Et eksempel er at det etableres kompetansemiljøer innen ID med delvis overlappende roller og ansvar i mangel på en helhetlig plan og organisering av området.

Antall registre og saksbehandlingssystemer i ID-forvaltningen er, som nevnt i kapittel 3.2.9, stort og komplekst, og det påvirker samarbeidet mellom aktørene. Hvert register og system tjener sitt formål og dette gir datadublering innad i registrene og mellom registre. Leverandørens inntrykk er at prinsippet om ett register til ett formål skaper høyere terskler for datadeling, og manglende integrering mellom registre og systemer vanskeliggjør effektiv saksbehandling og samhandling.

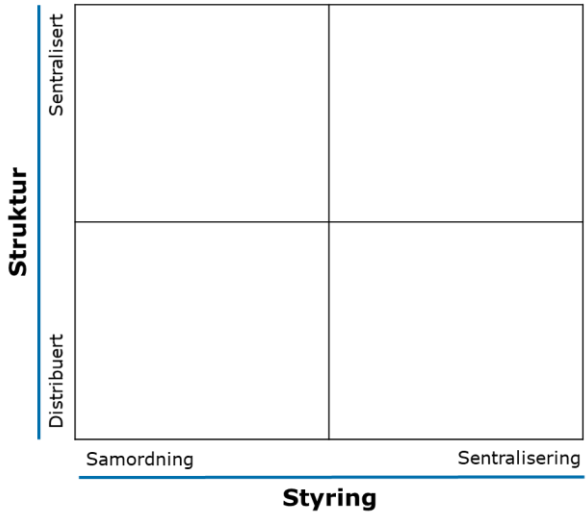
Norge får et nytt og moderne folkeregister i 2019, men med dette eksisterer kjente svakheter og utfordringer knyttet til datakvalitet. Dette gjelder for eksempel status om en ID er «kontrollert» eller «ikke kontrollert». Videre er påkrevd biometri en forutsetning for status «unik» i Folkeregisteret, noe som forventes å være utfordrende å implementere.

15.2 Drøftinger av alternativer for styring og struktur

Organisering er kun ett av flere styringsvirkemidler i offentlig sektor. For at organisatoriske virkemidler skal gi effekt må det sees i sammenheng med andre styringsvirkemidler som juridiske, økonomiske og pedagogiske.[478]

Leverandøren skisserer fem alternativer og vurderer disse langs to dimensjoner:

1. *Styring (f.eks. arbeidsdeling, fullmakter, koordinering og myndighet)*
2. *Struktur (f.eks. organisering, prosesser, retningslinjer, rutiner og systemer)*



Figur 70 Matrisestruktur for vurdering av alternativer

Hver dimensjon i matrisen belyses med ytterpunkter. Leverandøren skiller mellom samordning og sentralisering horisontalt, samt distribuert og sentralisert struktur vertikalt.

Alternativ 1 til 5 forklares nærmere i påfølgende delkapitler. Alternativene bygger til en viss grad på hverandre og øker langs styring- og strukturdimensjonen fra alternativ 1 til alternativ 5, men alternativ 3 til 5 tar ulik retning med hensyn til strukturdimensjonen.

I de påfølgende drøftingene er først prinsippet for endret styring og struktur beskrevet. For å sikre en mer helhetlig styring av og tydeliggjøring av ansvar for ID-forvaltningen, er det for hvert alternativ også vurdert tilhørighet, både på departements- og/eller etats/direktoratsnivå, med utgangspunkt i følgende temaer:

- Nærhet til største aktør/bruker innen ID-forvaltningen
- Kompleksitet i øvrig oppgaveportefølje og antall underliggende etater
- Gjennomføringsevne
- Politikkområder og skillet mellom politifaglige oppgaver og øvrig forvaltning
- Oppfattet vektlegging av sikkerhet, brukervennlighet og ressursbruk
- Nærhet til førstelinje, oppmøtested eller skrankepunkt

[478] Difi, «Statlig styring av kommunene – En kartlegging av virkemiddelbruk og utviklingstrekk på tre sektorer i perioden 1999-2015», 2015. Difi definerer styringsvirkemidler som følger: Juridiske omfatter lover og forskrifter. Økonomiske omfatter blant annet overføringer over statsbudsjettet, både rammebudsjettering eller øremerkede budsjettmidler, rett til å kreve inn skatter og avgifter. Pedagogiske virkemidler er en samlebetegnelse for ulike tiltak av mindre formell karakter enn juridiske og økonomiske. Det dekker blant annet rundskriv, retningslinjer, veiledere, endrings-/innovasjonsprogrammer, kompetanseutvikling og opplæringstiltak

15.2.1 Alternativ 1: Utarbeide en felles strategi for ID-forvaltningen

Alternativ 1 innebærer å

- *styrke departementenes rolle som strategiske aktører*

Alternativ 1 er en videreføring av dagens struktur for ID-forvaltning, men i tillegg utarbeides en felles strategi for ID-forvaltning i Norge som vil styrke den strategiske styringen. En viktig del av strategiarbeidet er å etablere et omforent kunnskapsgrunnlag som synliggjør omfanget av feil og misbruk av ID basert på statistikk over ID-kriminalitet med tilhørende samfunnsmessige kostnader og konsekvenser (ref. kapittel 6.1.5). Alternativet kan sees på som et nullpluss-alternativ.

Når departementer utarbeider en strategi forankret i regjeringen får det respektive området erfaringsmessig økt oppmerksomhet og fokus. Kjente eksempler på tverrsektorielle strategier er regjeringens strategi mot arbeidslivskriminalitet, nasjonal strategi for digital sikkerhet og regjeringens digitaliseringsstrategi for offentlig sektor. Innsatsen på tvers av sektorer blir mer målrettet og samordnet. Hensyn knyttet til brukervennlighet, sikkerhet og ressursbruk må vurderes og prioriteres basert på et omforent kunnskapsgrunnlag om samfunnsmessige kostnader av feil og misbruk av ID.

I dette alternativet definerer berørte departementer formål og/eller målsetninger med ID-forvaltning i Norge basert på eksisterende dokumentasjon. Strategien bør inneholde pågående og planlagte tiltak, samt nye tiltak basert på områdegjennomgangen. Det etableres en felles og forankret strategi for ID-forvaltning med tilhørende oppfølgingsmekanismer som omfatter ansvar for tiltak, prioritering i tid og ressurser til gjennomføring av tiltak. Leverandøren legger til grunn at det finnes ulike mekanismer og tilnærminger for å forankre og følge opp en strategi. For eksempel:

- JD og FD har fått overordnet ansvar for å følge opp *nasjonal strategi for digital sikkerhet*, men hvert departement er ansvarlig for at prioriteringer og tiltak blir fulgt opp innenfor sin sektor. Oppfølgingen av strategien gjennomføres i en interdepartemental gruppe og et offentlig-privat samarbeidsforum[479]

- Strategi mot arbeidslivskriminalitet blir fulgt opp av Statsministerens kontor og ni departementer. Ifølge strategien er det et eget statssekretærutvalg som følger den opp og saker drøftes jevnlig med partene i arbeidslivet. Videre gjennomføres toppmøter ledet av statsministeren, og samarbeidet med partene følges opp av Regjeringens kontaktutvalg[480]

- Regjeringens digitaliseringsstrategi for offentlig sektor ble offentliggjort 11.juni 2019. Difi har fått i oppdrag å lage en handlingsplan for oppfølging av regjeringens digitaliseringsstrategi innen 31.12.2019[481]

Leverandøren ser for seg forankring og oppfølging tilsvarende regjeringens strategi mot arbeidslivskriminalitet basert på de gode erfaringene fra arbeidet de siste årene.

I det følgende oppsummeres styrker og svakheter ved alternativ 1.

[479] Regjeringen, «Tiltaksoversikt til nasjonal strategi for digital sikkerhet», 2019
[480] Regjeringen, «Strategi mot arbeidslivskriminalitet», 2019
[481] KMD, «Tildelingsbrev – direktoratet for forvaltning og IKT», 2019

Styrker:

- En felles strategi for ID-forvaltningen legger til rette for mer helhetlig og strategisk styring ved å prioritere og balansere hensyn til brukervennlighet, sikkerhet og ressursbruk. Erfaringsmessig blir sikkerhet vektlagt over de to andre hensyn uten et tilstrekkelig faktagrunnlag

- Det vil være forholdvis enkelt å utarbeide og implementere en felles strategi for ID-forvaltning i Norge basert på eksisterende dokumentasjon og pågående arbeid i KoID, samt leverandørens skisse til mål, jf. kapittel 9
    - Strategien kan potensielt være en døråpner for å etablere utvidede hjemler tilsvarende som i strategien mot arbeidslivskriminalitet beskrevet i kapittel 4.2.4

- Strategien legger til rette for at alle aktører på ulike nivåer har en felles forståelse av hovedutfordringer og hovedmålsettinger i ID-forvaltningen, samt at de trekker i samme retning. En viktig del av strategiarbeidet er å etablere statistikk over ID-kriminalitet og et bedre kunnskapsgrunnlag om samfunnsmessige kostnader og konsekvenser knyttet feil og misbruk av ID for å øke bevisstheten og ta faktabaserte beslutninger

- Tydeligere avklaringer av roller og ansvar som del av oppfølgingen av strategien. Det vil fortsatt være en distribuert struktur, men med sterkere grad av samordning enn i dag som følge av strategien og det kan påvirke ressursbruken positivt

- ID-relaterte aktiviteter vil være en integrert del av ulike sektorers ansvarsområder og saksbehandling og synergier utnyttes på tvers av sektorer, spesielt for å sikre god brukervennlighet

Svakheter:

- Det er usikkert om en felles strategi for ID-forvaltning i Norge alene vil gi effekt knyttet til brukervennlighet, sikkerhet og ressursbruk – og om det vil løse de største utfordringene i dagens ID-forvaltning. Å sikre prioritering av de riktige tiltakene kombinert med ID-forvaltningens gjennomføringsevne vil være avgjørende

- Det er begrenset med systemstøtte for å etablere statistikk over ID-kriminalitet og samfunnsmessige kostnader knyttet til feil og misbruk av ID. Berørte aktører har i dag data på mindre enkeltområder for eksempel feil og misbruk av ID-dokumenter, men ikke samfunnsmessige konsekvenser for ID-forvaltningen som helhet. En viktig del av strategiarbeidet kan potensielt utgjøre en del manuelt arbeid som vil kreve ressurser fra de berørte aktørene uten at det vil ha effekt på brukervennlighet, sikkerhet og ressursbruk på kort sikt

- Fortsatt fragmentert organisering og det drøftes i dette alternativet ingen vesentlige endringer i organiseringen av ID-forvaltningen på departementsnivå og direktorats-/etatsnivå med hensyn til aktørers ansvar, prosesser og systemer. Det vil ha begrenset effekt på brukervennlighet, sikkerhet eller ressursbruk

15.2.2 Alternativ 2: Gi én statsråd ansvar for ID-forvaltningen og utarbeide en felles strategi for ID-forvaltningen

Alternativ 2 innebærer å

- *styrke departementenes rolle som strategiske aktører*
- *gi én statsråd ansvar for å samordne ID-forvaltningen i Norge*

Leverandøren viser til kapittel 15.2.1 for beskrivelse av første kulepunkt over.

Alternativ 2 er likt alternativ 1 med en videreføring av dagens struktur for ID-forvaltning og utarbeidelse av en ID-strategi, men vil i tillegg innebære at én statsråd får et overordnet ansvar for å samordne ID-forvaltningen i Norge.

Med samordning mener leverandøren her en prosess der ulike mål, verdier, aktiviteter og/eller ressurser blir sett i sammenheng, prioritert, avveid og/eller tilpasset hverandre.[482] Samordning er ikke et mål i seg selv, men et virkemiddel for å realisere mål som fordrer at flere aktører medvirker.

I dette alternativet vil ansvar innebære at statsråden gis myndighet til å samordne innsatsen på tvers av sektorer. Samordningsdepartementet vil kunne utøve myndighet, gjennomføre politikk og følge opp underliggende etater og tilknyttede virksomheter på saksområdet, i tillegg til å ivareta en pådriverrolle for ID-forvaltningen. Hvilke styringsvirkemidler samordningsdepartementet får til rådighet (juridiske, organisatoriske, pedagogiske og/eller økonomiske), samt samordningsdepartementets oppgaver, ansvar og rolle må spesifiseres i fullmakt, for eksempel i form av en kongelig resolusjon.

Ansvarlig statsråd definerer i samarbeid med særlige berørte statsråder formål og/eller målsetninger med ID-forvaltning i Norge, basert på eksisterende dokumentasjon. Det etableres en felles og forankret strategi for ID-forvaltning med tilhørende oppfølgingsmekanismer som omfatter ansvar for tiltak, prioritering i tid og ressurser til gjennomføring av tiltak.

Ved ansvarliggjøring av en statsråd og et samordningsdepartement kan ID-forvaltningen få større gjennomføringsevne, spesielt for omstillinger på tvers, og få nødvendig prioritering av tverrsektorielle problemstillinger og satsinger. Kjente eksempler på samordning av politikk- og saksområder er beredskap (JD), digitalisering (KMD), familie (BFD) og likestilling (KUD) med ansvarlig departement i parentes.

Leverandørens vurdering er at ved å gi en statsråd og et departement ansvar og eierskap til helheten i ID-forvaltningen, og ikke kun enkeltområder, vil det erfaringsmessig kunne bidra til økt gjennomføringsevne.

Leverandøren er kjent med at det finnes politikkområder som er spredt på flere statsråders ansvarsområder, og det er i mange tilfeller nødvendig og hensiktsmessig. Samtidig er det bestemte områder som er tydelig plassert konstitusjonelt, men hvor styring og gjennomføringsevne likevel vurderes som svak. Enkelte representanter fra departementer stiller spørsmål ved om en slik ansvarsplassering og rollefordeling vil bidra til en tydeligere eller en mer fragmentert ID-forvaltning.

Leverandørens syn er likevel at med ID-forvaltningens egenskaper og karakter, samt utfordringsbilde fremover, som beskrevet i kapittel 3 og kapittel 8, er det behov for å

[482] Difi, «Ikke bare pådriver… Om utøvelsen av KMDs samordningsroller», 2016

tydeliggjøre ansvar og roller både på politisk nivå og departementsnivå for å sikre en mer helhetlig styring. Alternativet fordrer at ansvar og roller til et samordningsdepartement er tydelig definert og ikke bidrar til ytterligere fragmentering. Når ulike hensyn skal balanseres må tverrsektorielle vurderinger og prioriteringer av ressurser være basert på en helhetlig tilnærming til politikkområdet for å sikre riktige avveininger mellom brukervennlighet, sikkerhet og ressursbruk. Det er sentralt med felles mål og styringsparametere som understøtter dette for å sikre fremdrift og utvikling på området.

Det er kun en statsråd som kan være konstitusjonelt ansvarlig for en underliggende etat, men i den grad andre statsråder skal gi føringer på et politikk- og saksområde må det koordineres på departementsnivå i forkant. Et samordningsdepartement kan utøve sin rolle ved for eksempel å gi oppdrag eller styringssignaler som koordineres på departementsnivå og innarbeides i tildelingsbrev til primæraktørene i ID-forvaltningen.

Det er flere eksempler hvor ansvarlig departement koordinerer føringer og styringssignaler i tildelingsbrev til underliggende etat for å sikre at et saksområde vurderes og prioriteres helhetlig. For eksempel i styringsdialogen mellom ASD og Arbeids- og velferdsdirektoratet inviteres Barne- og likestillingsdepartementet til å gi styringssignaler på familieområdet som innarbeides i tildelingsbrev eller gi innspill til dagsorden og delta på styringsmøter, samt at Barne- og likestillingsdepartementet også kan ta initiativ til egne særmøter med Arbeids- og velferdsdirektoratet.

Difi har i sin rapport «Departementene i førersetet for omstilling?» fra april 2019 påpekt at sektorprinsippet bør tolkes mer fleksibelt og viser til støtte fra juridiske miljøer.

> *«Det står i regjeringens makt å modifisere sektorinndelingen når dette fremstår som hensiktsmessig».* Det er ikke noe i veien for *«avledet ansvar for et saksområde til statsministeren, en samordningsminister, to statsråder i fellesskap eller et utvalg av statsråder..»* (Smith, 2015)[483]

Slik leverandøren ser det er det i praksis tre ulike statsråder som peker seg ut når det gjelder å ha helhetlig ansvar for ID-forvaltningen i Norge: Justis- og innvandringsministeren, Finansministeren eller Digitaliseringsministeren. Det er grunn til å tro at statsrådene vil vektlegge brukervennlighet, sikkerhet og ressursbruk forskjellig og det vil være ulike styrker og svakheter avhengig av hvilken statsråd som får et tydeligere ansvar:

Justis- og innvandringsministeren

- Har ansvar for rettsvesenet, kriminalomsorgen, politi- og påtalemyndigheten og utlendingsmyndigheter.[484] Å gi statsråden et tydeligere ansvar for ID gir nærhet til etatsstyringen av flere underliggende etater som har viktige roller i ID-forvaltningen blant annet POD, UDI og UNE. JD har forvaltningsansvaret for 8 av 19 ID-relaterte lover, jf. kapittel 4.1.21 Som beskrevet i kapittel 7.1.1 utgjorde ressursbruken i justissektoren over 60 prosent av total ressursbruk i ID-forvaltningen i 2018

- Hvert departement må alltid tilpasse sin etatsstyring til de gjeldende forholdene på et aktuelt område, og kan tilpasse styringen til mer sektorstyring når det er hensiktsmessig. Sektorstyring kan typisk omfatte et område som er større enn

[483] Smith, Eivind 2015: Ministerstyre – et hinder for samordning? Nytt Norsk Tidsskrift nr 3
[484] Regjeringen, «Om departementene», 2019

hver av de underliggende etatene.[485] Leverandøren erfarer at koblingen mellom sektor- og etatsstyring kan være utfordrende, men vurderer likevel at statsråden i større grad har mulighet til å innrette styringen relatert til ID mer effektivt og helhetlig på tvers av straffesak-, samfunnssikkerhets- og trygghetskjeden. Det bør gi et mer samordnet og koordinert uttrykk for faglige og administrative interesser og mål som er relevante for ID-forvaltningen

- En risiko ved å plassere ansvaret for ID i JD er at porteføljen til statsråden allerede er svært stor med 8 underliggende etater og virksomheter[486], samt 7 tilknyttede virksomheter[487]. Det er derav fare for at andre «mer kritiske» ansvarsområder prioriteres over ID-forvaltningen, for eksempel nærpolitireformen. Videre er gjennomføringsevnen knyttet til implementeringen av nye pass og ID-kort av ulike årsaker lav. Det er også en fare for at ved å plassere ansvaret hos JD, så vil autoritet, kvalitet og sikkerhet vektlegges på bekostning av brukervennlighet og ressurseffektivisering. Det er derfor viktig å etablere overordnede mål som angir retning for ID-forvaltningen og balanserer de ulike hensyn tilstrekkelig

Finansministeren

- Har ansvar for å planlegge og iverksette den økonomiske politikken, budsjettpolitikken, skatte- og avgiftspolitikken, finansiell stabilitet og forvaltningen av Statens pensjonsfond.[488] Å gi statsråden et tydeligere ansvar for ID gir nærhet til etatsstyringen av Skatteetaten, som er en sentral aktør i ID-forvaltningen med særskilt ansvar for Folkeregisteret. FIN har forvaltningsansvaret for 3 av 19 ID-relaterte lover, jf. kapittel 4.1.21. Folkeregisteret er grunnmuren i ID-forvaltningen og som beskrevet i kapittel 7.1.1 utgjorde rundt 20 prosent av totalt ressursbruk i ID-forvaltningen i 2018

- FIN har et samordningsansvar for den økonomiske politikken. Det kan gi frihetsgrader for ID-forvaltningen å ligge utenfor justissektoren. Hvis ID i større grad oppfattes som en forvaltningsoppgave fremfor politioppgave, kan det skape større aksept for opptak av biometri og deling av data. Folkeregisteret utgjør en viktig, men begrenset del av ID-forvaltningen, og en plassering av ansvar hos statsråden vil ikke nødvendigvis bidra til mer helhetlig styring og mindre fragmentering. En vesentlig del av oppgaveløsningen og saksbehandlingen gjennomføres i justissektoren, og leverandørens vurdering er at det kan medføre et større behov for koordinering og samordning på tvers av sektorene ved å plassere ansvaret i FIN enn i JD. Dette til tross for en vellykket gjennomføring av et tverretatlig prosjekt, modernisering av Folkeregisteret

- En risiko ved å plassere ansvaret for ID i FIN er at porteføljen til statsråden er stor med blant annet landets økonomiske politikk og statsbudsjettet. Slik statsforvaltningen er bygd opp i dag, er ikke et helhetlig ansvar for ID en naturlig del av finansministerens portefølje etter leverandørens syn. Ved å plassere ansvaret hos FIN, er det også en fare for at ressurseffektivisering vektlegges på bekostning av brukervennlighet og sikkerhet. Det er derfor viktig å etablere overordnede mål som angir retning for ID-forvaltningen og balanserer de ulike hensyn tilstrekkelig

[485] FIN, «Veileder i etatsstyring», 2011
[486] JD, «Etater og virksomheter», u.å.
[487] JD, «Tilknyttede virksomheter», u.å.
[488] Regjeringen, «Om departementene», 2019

Digitaliseringsministeren

- Har ansvar for IKT-politikk, Altinn, næringsrettet IKT, Digital21 og arbeidet med elektronisk kommunikasjon.[489] Å gi statsråden et tydeligere ansvar for ID gir nærhet til etatsstyringen av Digitaliseringsdirektoratet, som fra 01.01.2020 vil ha et særskilt ansvar for nasjonale felleskomponenter blant annet Altinn, ID-porten og eID. Regjeringens digitaliseringsstrategi med en digital offentlig sektor samsvarer godt med fremtidsbildet for ID-forvaltningen og viktige trender innen eID. KMD har forvaltningsansvaret for 3 av 19 ID-relaterte lover, jf. kapittel 4.1.21. Likevel utgjør drift og forvaltning av ID-porten og arbeidet med eID, som beskrevet i kapittel 7.1.1, kun rundt 5 prosent av total ressursbruk i ID-forvaltningen i 2018

- KMD har et samordningsansvar innen digitalisering og forvaltning og et større ansvar knyttet til ID kan gi samordningsgevinster. Det kan gi frihetsgrader for ID-forvaltningen å ligge utenfor justissektoren. Hvis ID i større grad oppfattes som en forvaltningsoppgave fremfor politioppgave, kan det skape større aksept for opptak av biometri og deling av data. På den andre siden utgjør eID og ID-porten en viktig, men begrenset, del av ID-forvaltningen, og en plassering av ansvar hos statsråden vil ikke nødvendigvis bidra til mer helhetlig styring og mindre fragmentering. En vesentlig del av oppgaveløsningen og saksbehandlingen gjennomføres i justissektoren, og leverandørens vurdering er at det kan medføre et større behov for koordinering og samordning på tvers av sektorene ved å plassere ansvaret i KMD enn JD

- Porteføljen til statsråden er relativt uensartet og begrenset sammenlignet med FIN og JD. En risiko ved å plassere ansvaret for ID i KMD er at digitalisering i mindre grad vil få nødvendig fokus og prioritering. ID kan potensielt utgjøre majoriteten av porteføljen. Etter leverandørens syn er KMD et bedre alternativ enn FIN, men det er en fare for at brukervennlighet vil vektlegges på bekostning av ressurseffektivisering og sikkerhet. Det er derfor viktig å etablere overordnede mål som angir retning for ID-forvaltningen og balanserer de ulike hensyn tilstrekkelig

Leverandøren har i dette alternativet ikke drøftet om det å gi én statsråd ansvar for ID-forvaltningen vil påvirke fagmiljøene på departementsnivå, enten mellom departementer eller mellom departement og etat/direktorat. Det må vurderes nærmere og vil avhenge av hvilken statsråd som får ansvaret.

I det følgende oppsummeres styrker og svakheter ved alternativ 2.

Styrker:

- En felles strategi for ID-forvaltningen legger til rette for mer helhetlig og strategisk styring ved å prioritere og balansere hensyn til brukervennlighet, sikkerhet og ressursbruk. Erfaringsmessig blir sikkerhet vektlagt over de to andre hensyn uten et tilstrekkelig faktagrunnlag

- Det vil være forholdvis enkelt å utarbeide og implementere en felles strategi for ID-forvaltning i Norge basert på eksisterende dokumentasjon og pågående arbeid i KoID, samt leverandørens skisse til mål, jf. kapittel 9

[489] Regjeringen, «Om departementene», 2019

- Strategien kan potensielt være en døråpner for å etablere utvidede hjemler tilsvarende som i strategien mot arbeidslivskriminalitet beskrevet i kapittel 4.2.4

- Strategien legger til rette for at alle aktører på ulike nivåer har en felles forståelse av hovedutfordringer og hovedmålsettinger i ID-forvaltningen, samt at de trekker i samme retning. En viktig del av strategiarbeidet er å etablere statistikk over ID-kriminalitet og et bedre kunnskapsgrunnlag om samfunnsmessige kostnader og konsekvenser knyttet feil og misbruk av ID for å øke bevisstheten og ta faktabaserte beslutninger

- En statsråd får et helhetlig ansvar for ID-forvaltningen i Norge som gir tydeligere roller og ansvar i oppfølgingen av strategien. Det vil fortsatt være en distribuert struktur i ID-forvaltningen, men med sterkere grad av samordning med en ansvarlig statsråd enn i alternativ 1 og det kan påvirke ressursbruken positivt

- En ansvarlig statsråd vil kunne løfte viktigheten av en helhetlig ID-forvaltning, og styrker forutsetningene for bedre gjennomføringsevne/-kraft

- ID-relaterte aktiviteter vil være en integrert del av ulike sektorers ansvarsområder og saksbehandling og synergier utnyttes på tvers av sektorer, spesielt for å sikre god brukervennlighet

Svakheter:

- Det er usikkert om en felles strategi for ID-forvaltning i Norge alene vil gi effekt knyttet til brukervennlighet, sikkerhet og ressursbruk – og om det vil løse de største utfordringene i dagens ID-forvaltning. Å sikre prioritering av de riktige tiltakene kombinert med ID-forvaltningens gjennomføringsevne vil være avgjørende

- Det er begrenset med systemstøtte for å etablere statistikk over ID-kriminalitet og samfunnsmessige kostnader knyttet feil og misbruk av ID. Berørte aktører har i dag data på mindre enkeltområder for eksempel feil og misbruk av ID-dokumenter, men ikke samfunnsmessige konsekvenser for ID-forvaltningen som helhet. En viktig del av strategiarbeidet kan potensielt utgjøre en del manuelt arbeid som vil kreve ressurser fra de berørte aktørene uten at det vil ha effekt på brukervennlighet, sikkerhet og ressursbruk på kort sikt

- Fortsatt fragmentert organisering og det anbefales ingen vesentlige endringer i organiseringen av ID-forvaltningen på direktorats-/etatsnivå med hensyn til aktørers ansvar, prosesser og systemer. Det vil ha begrenset effekt på brukervennlighet, sikkerhet eller ressursbruk

- Det er få representanter fra departementene gir uttrykk for at de ønsker å ta et helhetlig ansvar for ID-forvaltningen i Norge og det kan være en gjennomføringsrisiko

- Avhengig av hvilken statsråd som får ansvaret kan alternativet medføre et større behov for direktorats/etats- og departementsdialog på tvers av sektorer med koordinering og samordning uten at det går noe fortere eller skaper økt gjennomføringskraft

15.2.3 Alternativ 3: Gi én statsråd ansvar for ID-forvaltningen og utarbeide en felles strategi for ID-forvaltningen, samt tydeliggjøre ansvar og oppgaver relatert til ID i justissektoren

Alternativ 3 innebærer å

- *styrke departementenes rolle som strategiske aktører*
- *gi én statsråd ansvar for å samordne ID-forvaltningen i Norge*
- *tydeliggjøre ansvar og oppgaver relatert til ID i justissektoren*

Leverandøren viser til kapittel 15.2.1 og 15.2.2 for beskrivelse av første og andre kulepunkt over.

Alternativ 3 er lik alternativ 2, men i tillegg innebærer dette alternativet at ansvar og oppgaver relatert til ID i justissektoren tydeliggjøres.

Justissektoren er en viktig sektor med mange underliggende direktorater og etater som har en avgjørende rolle i ID-forvaltningen. Med en tydeliggjøring mener leverandøren at ansvar og oppgaver relatert til ID avklares, defineres, koordineres og/eller gjennomgås med sikte på å øke sikkerhet, bedre brukervennlighet og sikre mer effektiv ressursbruk i justissektoren. Etter leverandørens syn er utfordringene i ID-forvaltningen og potensial for forbedring generelt størst i justissektoren og i grensesnittet til justissektoren. Som beskrevet i kapittel 7.1.1 er ressursbruk i JD relatert til ID over 60 prosent av total ressursbruk i ID-forvaltningen. Samtidig er leverandøren gjort kjent med utfordringer knyttet til gjennomføringsevne og måloppnåelse som beskrevet i kapittel 3 og kapittel 8.

Som beskrevet i kapittel 3.2 er det behov for å tydeliggjøre ansvar og roller i justissektoren for å få en felles forståelse. Overordnet fremstår det for leverandøren som en del overlapp i ansvar og oppgaver. Videre bør tildelingsbrev i ID-forvaltningen samkjøres bedre med vekt på mål, styringsparametere og oppdrag relatert til ID for å sikre en mer helhetlig tilnærming i sektoren.

Leverandøren vurderer at det overordnet er to tilnærminger for å tydeliggjøre ansvar og oppgaver relatert til ID i justissektoren: *Samle fagmiljøer i færre enheter* eller *spesialisere fagmiljøer i eksisterende enheter*.

Leverandøren anser at det ikke er innenfor mandatet for områdegjennomgangen å vurdere hvilke fagmiljøer i et underliggende direktorat eller etat i justissektoren som bør samles og/eller spesialiseres og eventuelt hvordan det kan gjennomføres. Det vil derfor være behov for at ansvarsområder og oppgaver som leverandøren peker på utredes, kost/nytte-vurderes og detaljeres nærmere før det eventuelt besluttes endringer. JD bør være ansvarlig for prosessen i dialog med underliggende direktorater og etater.

Tabellen nedenfor oppsummerer forslag til potensielle ansvarsområder og oppgaver som det bør sees nærmere på innenfor temaene som områdegjennomgangen adresserer i kapittel 3 til 7. Leverandøren understreker at dette er ikke er en uttømmende liste, men kun eksempler på funn som leverandøren har identifisert i områdegjennomgangen.

Tema	Potensielle ansvarsområder og oppgaver
Styring og struktur	• Tydeliggjøre ansvaret for å sikre en *helhetlig tilnærming til ID-forvaltningen i justissektoren* og bygge felles kompetanse og kapasitet på relativt smale fagområder f.eks. identifisering, dokumentundersøkelser, laboratoriekapasitet og internasjonalt samarbeid. Tydeliggjøre når skillet mellom forvaltnings- og straffesakssporet er hensiktsmessig og nødvendig i ID-arbeid • Avklare og tydeliggjøre *ansvar og roller i ID-forvaltningen i justissektoren* mellom underliggende etater, enten ved å samle fagmiljøer i færre enheter eller tydeliggjøre spesialiseringen • Avklare og tydeliggjøre *ansvar og rolle tilknyttet eID* • Bidra til *økt samordning og samarbeid i politiet* ved å sikre at det ikke er overlappende ansvar og oppgaver i fagmiljøer eller konkurrerende fagmiljøer f.eks. NID og Kripos, enten ved å samle fagmiljøer i færre enheter eller tydeliggjøre spesialiseringen • Avklare og tydeliggjøre *ansvars- og arbeidsdelingen i utlendingsforvaltningen* for ID-relatert arbeid for å sikre bedre saksflyt i utlendingssaker mellom politidistriktene, PU, UDI og UNE. For eksempel skal saker om tilbakekall av statsborgerskap til UDI og UNE eller domstolen • Avklare og tydeliggjøre ansvar til *1., 2. og 3. faglinje* for å effektivisere informasjonsdeling og koordinering f.eks. ved å etablere arenaer og formelle strukturer for å *øke samhandling på tvers i justissektoren.* Det er avgjørende å skape tillit og tiltro til hverandres arbeid og redusere opplevelsen av konkurranse og kamp om faget • Avklare og tydeliggjøres Norges rolle i *internasjonalt i ID-arbeid* ved å styrke et felles fagmiljø for internasjonalt samarbeid og én stemme ut fra justissektoren i Norge
Lover og regelverk	• Avklare formål med de ulike regelverkene som justissektoren er ansvarlige for, samt sikre at regelverk legger til rette for samhandling og deling av data på felt der dette er nødvendig, herunder utlendingsfeltet • Sikre at regelverket i justissektoren er tilstrekkelig fremtidsrettet for å understøtte videre utvikling av ID-forvaltningen og følger teknologiske trender f.eks. politiregisterloven
Brukerreiser	• Sikre helhetlig, koordinert og lik informasjon fra justissektoren ut til brukerne underveis i saksbehandlingsprosessen • Sikre en felles standard og felles beviskrav for å fastsette ID • Avklare dokumentasjonskrav for å effektivisere brukernes tidsbruk • Sette brukeren i sentrum og prinsippet «kun en gang» ved å legge til rette for f.eks. å dele ansiktsfoto med relevante etater som har hjemmel til å gjenbruke eller for tredjelandsborgere som får innvilget norsk statsborgerskap kan potensielt biometri tatt i utlendingsregisteret gjenbrukes av passregisteret (ved passutstedelse)
Kvalitet og sikkerhet	• Avklare og tydeliggjøre ansvar for fag- og metodeutvikling, samt koordinering av opplærings- og kompetanseutviklingstiltak og materiell relatert til ID på tvers av justissektoren • Avklare og tydeliggjøre ansvar for koordinering av rutiner og retningslinjer relatert til ID på tvers av justissektoren f.eks. mangler felles nasjonale standarder • Avklare og tydeliggjøre ansvar for å yte bistand og veiledning for å sikre oppfølging felles standarder og enhetlig praksis f.eks. hva er sikker identitet og hva er en ID-kontroll • Avklare og tydeliggjøre hvem som har ansvar for hva når det gjelder oversikt over avdekket ID-misbruk og potensielle samfunnsmessige konsekvenser slik at data blir delt med relevante aktører for å bekjempe kriminalitet
Ressursbruk	• Gjennomgang av ressursbruk og kostnader tilknyttet ID-arbeid i egen sektor for å øke bevissthet rundt temaet • Gjennomgang av ressursbruk og kostnader tilknyttet administrasjon og støttefunksjoner for ID-arbeid i egen sektor f.eks. teknologiske valg og innkjøp

Tema	Potensielle ansvarsområder og oppgaver
	• Sikre at kapasitet og spisskompetanse utnyttes bedre enn i dag med vekt på gjenbruk og mindre dobbeltarbeid • Sikre et tilstrekkelig datagrunnlag om feil og misbruk av ID for å skape bedre beslutningsgrunnlag slik at ressurser benyttes til målrettede tiltak for å forebygge kriminalitet

Tabell 29 Forslag til potensielle ansvarsområder og oppgaver

Leverandøren har i dette alternativet ikke drøftet om det å gi én statsråd ansvar for ID-forvaltningen vil påvirke fagmiljøene på departementsnivå, enten mellom departementer eller mellom departement og etat/direktorat. Det må vurderes nærmere og vil avhenge av hvilken statsråd som får ansvaret.

I det følgende oppsummeres styrker og svakheter ved alternativ 3.

Styrker:

- En felles strategi for ID-forvaltningen legger til rette for mer helhetlig og strategisk styring ved å prioritere og balansere hensyn til brukervennlighet, sikkerhet og ressursbruk. Erfaringsmessig blir sikkerhet vektlagt over de to andre hensyn uten et tilstrekkelig faktagrunnlag

- Det vil være forholdvis enkelt å utarbeide og implementere en felles strategi for ID-forvaltning i Norge basert på eksisterende dokumentasjon og pågående arbeid i KoID, samt leverandørens skisse til mål, jf. kapittel 9
    - Strategien kan potensielt være en døråpner for å etablere utvidede hjemler tilsvarende som i strategien mot arbeidslivskriminalitet beskrevet i kapittel 4.2.4

- Strategien legger til rette for at alle aktører på ulike nivåer har en felles forståelse av hovedutfordringer og hovedmålsettinger i ID-forvaltningen, samt at de trekker i samme retning. En viktig del av strategiarbeidet er å etablere statistikk over ID-kriminalitet og et bedre kunnskapsgrunnlag om samfunnsmessige kostnader og konsekvenser knyttet feil og misbruk av ID for å øke bevisstheten og ta faktabaserte beslutninger

- En statsråd får et helhetlig ansvar for ID-forvaltningen i Norge som gir tydeligere roller og ansvar i oppfølgingen av strategien. Det vil fortsatt være en distribuert struktur i ID-forvaltningen, men med sterkere grad av samordning med en ansvarlig statsråd enn i alternativ 2 som følge av tydeliggjøring av ansvar og oppgaver i justissektoren. Det kan påvirke ressursbruken positivt

- En ansvarlig statsråd vil kunne løfte viktigheten av en helhetlig ID-forvaltning, og styrker forutsetningene for bedre gjennomføringsevne/-kraft

- ID-relaterte aktiviteter vil være en integrert del av ulike sektorers ansvarsområder og saksbehandling og synergier utnyttes på tvers av sektorer, spesielt for å sikre god brukervennlighet

- Felles forståelse av ansvar og roller vil legge til rette for bedre koordinering og samhandling mellom viktige aktører i ID-forvaltningen, samt økt bevissthet rundt samfunnsmessige konsekvenser og ressursbruk relatert til feil og misbruk av ID

- Tydeliggjøring av ansvar og oppgaver i én stor og viktig sektor setter et godt eksempel for andre sektorer og kan øke mulighet for at det initieres tilsvarende prosesser

Svakheter:

- Det er usikkert om en felles strategi for ID-forvaltning i Norge alene vil gi effekt knyttet til brukervennlighet, sikkerhet og ressursbruk – og om det vil løse de største utfordringene i dagens ID-forvaltning. Å sikre prioritering av de riktige tiltakene kombinert med ID-forvaltningens gjennomføringsevne vil være avgjørende

- Det er begrenset med systemstøtte for å etablere statistikk over ID-kriminalitet og samfunnsmessige kostnader knyttet feil og misbruk av ID. Berørte aktører har i dag data på mindre enkeltområder f.eks. feil og misbruk av ID-dokumenter, men ikke samfunnsmessige konsekvenser for ID-forvaltningen som helhet. En viktig del av strategiarbeidet kan potensielt utgjøre en del manuelt arbeid som vil kreve ressurser fra de berørte aktørene uten at det vil ha effekt på brukervennlighet, sikkerhet og ressursbruk på kort sikt

- Fortsatt fragmentert organisering og det anbefales ingen vesentlige endringer i organiseringen av ID-forvaltningen på direktorats-/etatsnivå med hensyn til aktørers ansvar, prosesser og systemer. Det vil ha begrenset effekt på brukervennlighet, sikkerhet eller ressursbruk

- Det er få representanter fra departementene som gir uttrykk for at de ønsker å ta et helhetlig ansvar for ID-forvaltningen i Norge og det kan være en gjennomføringsrisiko

- Avhengig av hvilken statsråd som får ansvaret kan alternativet medføre et større behov for direktorats/etats- og departementsdialog på tvers av sektorer med koordinering og samordning uten at det går noe fortere eller skaper økt gjennomføringskraft

- Risiko for at resultatet av tydeliggjøring av ansvar og oppgaver kun blir inkrementelle justeringer innad i justissektoren uten nevneverdig effekt for ID-forvaltningen i stort

15.2.4 Alternativ 4: Gi én statsråd ansvar for ID-forvaltningen og utarbeide en felles strategi for ID-forvaltningen, samt konsolidere ansvar for utvalgte ID-relaterte oppgaver på tvers av sektorer i en eksisterende etat/direktorat

Alternativ 4 innebærer å

- *styrke departementenes rolle som strategiske aktører*

- *gi én statsråd ansvar for å samordne ID-forvaltningen i Norge*

- *konsolidere ansvar for utvalgte ID-relaterte oppgaver på tvers av sektorer i en eksisterende etat/direktorat*

Leverandøren viser til kapittel 15.2.1 og 15.2.2 for beskrivelse av første og andre kulepunkt over.

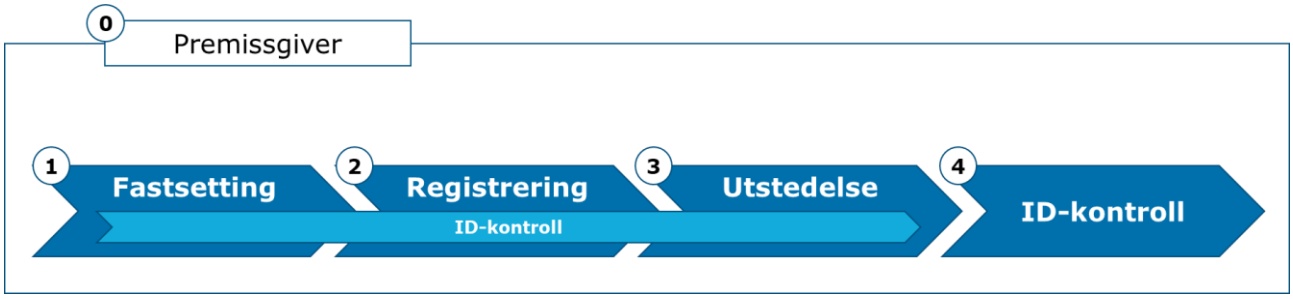
Alternativ 4 innebærer endringer i styringen og strukturen av ID-forvaltningen, både på departementsnivå og direktorats-/etatsnivå, ved at ansvaret for ID-forvaltningen sentraliseres under en statsråd. Videre konsolideres ansvaret for utvalgte ID-relaterte oppgaver i en eksisterende etat/direktorat. En eksisterende etat/direktorat gis

myndighet av et departement til å være premissgiver for ID-forvaltningen og tar en samordningsrolle på tvers av sektorer. ID blir en av kjerneoppgavene i direktoratets/etatens samfunnsoppdrag på linje med øvrige kjerneoppgaver.

Som beskrevet i kapittel 8 vurderer leverandøren at dagens styring og struktur i ID-forvaltningen ikke er tilstrekkelig tilrettelagt for å sikre økt brukervennlighet, sikkerhet og ressurseffektivitet. Dette har tidligere vært omtalt i flere rapporter fra departementer og direktorater at det må vurderes om en kvalifisert myndighet bør gis et større og mer helhetlig ansvar for ID-forvaltningen. I utredningen om helhetlig ansvar for EØS-borgere var et alternativ at én etat skal ha et mer helhetlig ansvar for ID-forvaltningen av EØS-borgere, uten at rapporten tok standpunkt til løsning.

I dette alternativet drøfter leverandøren en konsolidering av ansvar på direktorats-/etatsnivå, på tvers av sektorer, for utvalgte ID-relaterte oppgaver i en eksisterende etat/direktorat. Konsolidering av ansvar avgrenses til å gjelde den overordnede ID-prosessen som er beskrevet i kapittel 2.4 med tilhørende oppgaver, prosesser og systemer i saksbehandlingen. Som premissgiver får etaten/direktoratet et overordnet ansvar for ID-prosessen, men dette innebærer ikke at etaten/direktoratet vil være ansvarlig for å gjennomføre alle stegene i ID-prosessen. Enkelte ID-relaterte aktiviteter vil fortsatt være en integrert del av andre sektorers ansvarsområder og saksbehandling, men alternativet innebærer en tydelig konsolidering fra dagens nivå.

ID-prosessen er illustrert i figuren nedenfor.



Figur 71 Overordnet ID-prosess

Potensielt ansvar, oppgaver, prosesser og systemer:

Med utgangspunkt i nåsituasjonen av ID-prosessen er det leverandørens vurdering at:

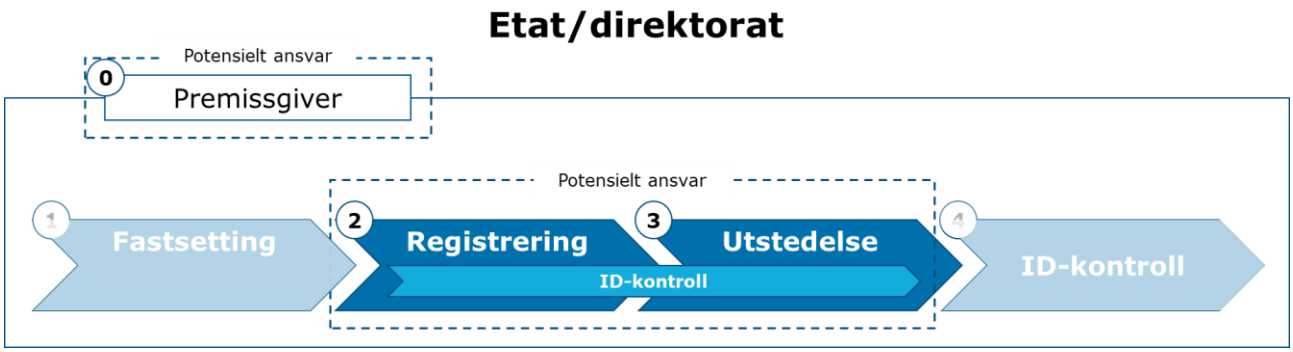
- Ansvar og oppgaver relatert til premissgiverrollen (steg 0) er ikke en rolle noen av aktørene utfører i dag, men etter leverandørens syn en oppgave som kan opprettes og tillegges en etat/direktorat med konsolidert ansvar. Det omfatter bl.a. å utarbeide/sikre enhetlige standarder, krav, rutiner, retningslinjer, kompetanse, praksis mv. på tvers av ID-prosessen. Premissgiverrollen må utøves i samarbeid med relevante aktører

- Ansvar og oppgaver relatert til fastsettelse (steg 1) er etter leverandørens syn potensielt krevende å flytte ettersom fastsettelse av ID naturlig tilfaller Helseforetakene og utlendingsforvaltningen for henholdsvis norske statsborgere og tredjelandsborgere. Tilhørende bakgrunnssjekk og/eller kontrollaktiviteter har ikke samme nære tilknytning til disse aktørenes øvrige oppgaver og kan vurderes flyttet

- Ansvar og oppgaver relatert til registrering (steg 2) og utstedelse (steg 3) er etter leverandørens syn potensielt flyttbare sammen med tilhørende kontrollaktiviteter. I enkelte tilfeller vil det være mulig å flytte ID-kontroll uten å gjøre endringer i registering av ID eller utstedelse av ID-bevis

- Ansvar og oppgaver relatert til ID-kontroll (steg 4) er etter leverandørens syn lite hensiktsmessig å flytte da ID-kontroller som foretas i etterkant av utstedt ID-bevis gjerne er tilknyttet en spesiell tjeneste eller ytelse og at en etat/direktorat vanskelig kan ta ansvar for kontroll i tilknytning til andre direktoraters/etaters tjenester

Direktoratets/etatens potensielle ansvar totalt sett er illustrert i figuren nedenfor.



Figur 72 Konsolidering av ansvar for utvalgte ID-relaterte oppgaver, prosesser og systemer

Tabellene nedenfor gir eksempler på hva slags oppgaver, prosesser og systemer relatert til premissgiverrollen og stegene registrering og utstedelse med tilhørende ID-kontroll i ID-prosessen, som kan være flyttbare. Det er også oppsummert kort hvilke konsekvenser flytting av oppgaven gir for virksomheten i hvert tilfelle. Det understrekes at listene ikke anses som uttømmende og er basert på leverandørens vurdering. Konsekvensene av flytting må utredes, kost/nytte-vurderes og detaljeres nærmere før det eventuelt besluttes endringer.

ID-relaterte oppgaver som flyttes fra en aktør vil potensielt kunne frigjøre ressurser ved å legge til rette for en mer effektiv og helhetlig ID-forvaltning. Det er også et poeng at ingen aktør har ID som kjerneoppgave i dag, og at en eventuell flytting av ID-relaterte oppgaver ikke vil være relatert til deres kjernevirksomhet, det vil derimot redusere deres totale oppgaveportefølje. Begge disse punktene gjelder gjennomgående og poengteres ikke eksplisitt i tabellene under.

Steg 0: ID-relaterte oppgaver/prosesser/systemer tilknyttet rollen som premissgiver		
	Potensielt flyttbar	Konsekvenser for virksomheten
Politiet	Fagmiljø relatert til ID (ikke straffesaksbehandling) i POD, politidistriktene, PU og Kripos som er ansvarlig for å etablere og videreutvikle standarder, krav, rutiner, retningslinjer, kompetanse, praksis i ID-prosessen	Positivt: Samler ansvar som per i dag er spredt på flere aktører i ID-forvaltningen, dette legger til rette for styrket kompetanseutvikling og -deling. Et samlet fagmiljø antas også å være mer robust og gi mer fleksibel kapasitetsutnyttelse. Negativt: Fragmentering av eksisterende fagmiljø. Reduserer nærheten til politiets samfunnsoppdrag og skaper større avstand til straffesakssporet og kriminalitetsbekjempelse.
	Fag-/metodeutvikling, opplæring og kursing innen ID-relaterte emner i POD, politidistriktene, PU og Kripos	Positivt: Samler ansvar som per i dag er spredt på flere aktører i ID-forvaltningen, dette legger til rette for styrket kompetanseutvikling og -deling. Et samlet fagmiljø antas også å være mer robust og gi mer fleksibel kapasitetsutnyttelse. Negativt: Fragmentering av eksisterende fagmiljø. Reduserer nærheten til politiets samfunnsoppdrag og skaper større avstand til straffesakssporet og kriminalitets-bekjempelse.

Steg 0: ID-relaterte oppgaver/prosesser/systemer tilknyttet rollen som premissgiver		
	Potensielt flyttbar	Konsekvenser for virksomheten
	NID i sin helhet med spisskompetanse på ID- og underlagsdokumenter, verktøy og metode for å avklare identitet til utlendinger, tar initiativ til samarbeid og fellesløsninger, samt tilbyr opplæring, verktøy, utvikler statistikk og analyser, bistand og råd	Positivt: Forenkler styringslinjer og reduserer byråkrati og koordinering. Tydeligere kobling mellom premissgiver og nasjonalt ekspertorgan. Muliggjør å realisere effektene som var tiltenkt ved etableringen av NID. Negativt: Potensielt mer utfordrende å bevare sin rolle som uavhengig ekspertorgan.
UDI	Relevant fag-/metodeutvikling, opplæring og kursing innen ID-relaterte emner i UDI	Positivt: Samler ansvar som per i dag er spredt på flere aktører i ID-forvaltingen, dette legger til rette for styrket kompetanseutvikling og -deling. Et samlet fagmiljø antas også å være mer robust og gi mer enhetlig tilnærming til brukergrupper og fleksibel kapasitetsutnyttelse. Negativt: Fragmentering av eksisterende fagmiljø. Reduserer nærheten til utlendingsforvaltningen.
Difi	Regelverk, internasjonale standarder, prosedyrer, policy og styringsrammeverk for eID	Positivt: I dag har Difi, Nkom og POD roller i arbeidet med eID, men leverandøren opplever at ingen har et helhetlig ansvar og styring. Negativt: Fragmentering av eksisterende fagmiljø. Reduserer nærheten til forvaltningens digitale plattform – økosystem. Det er fare for å svekke digitaliseringsarbeidet ved å dele ansvaret opp i nye enheter.
	Drift og forvaltning av ID-porten og eID	Positivt: Mulighet til å samlokalisere ansvaret for eID med øvrige ID-relaterte oppgaver. Negativt: Leverandørens oppfatning er at dette fungerer godt i dag og at det medfører en risiko å flytte ansvaret for drift og forvaltning.
Skatteetaten	Premissgiverrolle for identitetsnummer (f- og d-nummer)	Positivt: Reduserer oppgaveporteføljen til Skatteetaten. Økt felles forståelse for rekvirering blant rekvirentene, i tillegg til at ansvar som per i dag er spredt på flere aktører samles slik at identitetsnummer og ID-bevis kan sees i større grad i sammenheng. Negativt: Reduserer nærheten til Skatteetatens samfunnsoppdrag, spesielt innbetaling av avgifter og skatt, samt forebygging av arbeidslivskriminalitet. I tillegg til oppgaver tilknyttet Folkeregisteret som ikke nødvendigvis er ID-relatert.
	Ansvar for koordineringsgruppe (KoID)	Positivt: Mindre behov for formelle og uformelle samarbeidsarenaer ved å gi et helhetlig ansvar til en aktør. Sikrer mer kontinuitet ved at ansvaret ikke rulleres hvert andre år. Negativt: Mindre mulighet til å påvirke arbeidet i KoID, men siden ansvaret for KoID er rullerende er konsekvensen begrenset.
KD	Statsborgerloven	Positivt: UDI, UNE og politiet, som er utøvende myndigheter, jf. loven § 2, får potensielt ett departement mindre å forholde seg til. Negativt: Kunnskaps- og integreringsministeren får mindre mulighet til å påvirke forvaltningen av loven, som er et viktig integreringspolitisk styringsinstrument.

Tabell 30 Vurdering av områder som potensielt kan være gjenstand for konsolidering og konsekvenser for gjenværende virksomhet (premissgiver, steg 0)

En tydelig premissgiver for ID-forvaltningen styrker forutsetningene for bedre samordning og en mer helhetlig tilnærming til ID-forvaltningen. Med premissgiver er det naturlig å anta at oppgavene relatert til steg 1-4 i verdikjeden vil endre sin karakter og at de ulike aktørene i større grad vil være en utførende part for premissgiveren.

Disse endringene er ikke hensyntatt i tabellen under. Her fokusere leverandøren på oppgaver/prosesser/systemer relatert til registrering (steg 2) og utstedelse (steg 3) slik de foreligger i dag.

Steg 2: ID-relaterte oppgaver/prosesser/systemer tilknyttet registrering		
	Potensielt flyttbar	Konsekvenser for virksomheten
Politiet	Drift og forvaltning av passregisteret og ID-kort registeret (når implementert, herunder opptak av biometri for norske statsborgere (kun i forvaltningssporet))	Positivt: Reduserer oppgaveporteføljen til politiet. Det er leverandørens inntrykk at kritiske områder eller kjerneoppgaver i politiets oppgaveportefølje i større grad prioriteres foran ID-området. Negativt: Større avstand til straffesakssporet og kriminalitetsbekjempelse.
	Registrering av EØS-borgere med tilhørende ID-kontroll	Positivt: En mer enhetlig tilnærming til ulike brukergrupper og få bedre kontroll på EØS-borgere. Negativt: Større avstand til straffesakssporet og kriminalitetsbekjempelse.
	Utlendingsforvaltningen i politi-distriktene etter 3.landsregelverket: Mottak av søknader om oppholdstillatelse, utlendingspass, reisebevis, statsborgerskap og ID-kontroll ved mottak av alle disse + effektuering av vedtak og bestilling av oppholdskort	Positivt: Reduserer oppgaveporteføljen til politiet. En mer enhetlig tilnærming til ulike brukergrupper og ulike ID-bevis. Øke utnyttelsen av ID-faglig kompetanse Negativt: Større avstand til straffesakssporet og kriminalitetsbekjempelse. Muligens behov for å se nærmere på utlendingsforvaltningen uavhengig av ID for å sikre en mer helhetlig organisering og styring.
Skatteetaten	Drift og forvaltning av det sentrale Folkeregisteret med tilhørende tildeling av f- og d-nummer	Positivt: Mulighet til å samlokalisere Folkeregisteret med øvrige ID-relaterte registre og oppgaver. Negativt: Modernisering av Folkeregisteret er i hovedsak ferdigstilt, og leverandørens oppfatning er at drift og forvaltning fungerer godt og det medfører risiko å flytte ansvaret.
	Skattekontorenes ansvar for ID-kontroll på vegne av d-nummerrekvirenter, bekreftelse av farskap og melde innflytting til Norge[490]	Positivt: Reduserer oppgaveporteføljen til Skatteetaten. Mulighet til å samle ID-relaterte oppgaver i en felles 1.linje. Negativt: Fortsatt behov for skattekontor og en fysisk 1.linje for å bistå med å søke om skattekort, men behovet og omfanget av oppgaver reduseres vesentlig.
UDI	*Ikke identifisert*	*Ikke identifisert*
Alle rekvirenter	Ansvar for rekvirering av d-nummer med tilhørende rutiner, prosesser og systemer overføres til en etat/direktorat	Positivt: samler ansvar som i dag er spredt på flere aktører og legger til rette for mer bruk av «ID-kontroll». Dette forventes å redusere risiko for feil og misbruk av ID. Negativt: Kan gi øke saksbehandlingstiden til aktøren som ikke lenger kan rekvirere d-nummer.

Tabell 31 Vurdering av områder som potensielt kan være gjenstand for konsolidering og konsekvenser for gjenværende virksomhet (registrering, steg 2)

Steg 3: ID-relaterte oppgaver/prosesser/systemer tilknyttet utstedelse		
	Potensielt flyttbar	Konsekvenser for virksomheten
Politiet	Utstedelse av pass- og nasjonale ID-kort med tilhørende ID-kontroll	Positivt: Reduserer oppgaveporteføljen til politiet. Ifølge POD er det tenkt at pass og ID-kontorene i de store byene i stor grad skal jobbe med utstedelse av pass og nasjonale ID-kort. Negativt: Oppgaven med å utstede pass og nasjonale ID-kort kan være avhengig av informasjon fra politiet, og politiet bør ha tilgang til informasjonen i passregisteret eller utledningsdatabasen. Om en annen myndighet bemyndiges til å utstede nevnte ID-bevis, vil

[490] Skatteetaten.no, «Bestill tid», 2019

		politiet således fortsatt måtte kobles inn i arbeidet med å behandle søknader.[491] Ifølge POD vil pass- og ID-kontor ved de mindre tjenestestedene vil oppgaver knyttet til utstedelse av pass og nasjonalt ID-kort være én blant mange oppgaver.
	Utlendingsforvaltningen i politi-distriktene etter 3.landsregelverket: Utstedelse av oppholdskort, utlendingspass, reisebevis, statsborgerskap og tilhørende ID-kontroll	Positivt: Reduserer oppgaveporteføljen til politiet. En mer enhetlig tilnærming til ulike brukergrupper og ulike ID-bevis. Øke utnyttelsen av ID-faglig kompetanse. Negativt: Oppgaven med å utstede oppholdskort/utlendingspass/reisebevis kan være avhengig av informasjon fra politiet, og politiet bør ha tilgang til informasjonen i passregisteret eller utledningsdatabasen. Om en annen myndighet bemyndiges til å utstede nevnte ID-bevis, vil politiet således fortsatt måtte kobles inn i arbeidet med å behandle søknader. Større avstand til straffesakssporet og kriminalitets-bekjempelse. Muligens behov for å se nærmere på utlendingsforvaltningen uavhengig av ID for å sikre en mer helhetlig organisering og styring.
Statens vegvesen	ID-kontroll og innhenting av ansiktsfoto og signatur til førerkortutstedelse og ved fornyelse av førerrettsbevis	Positivt: Samles kompetansen på identitetssjekk for flere formål i en organisasjon, vil det bidra til å redusere muligheten for falske identiteter i Norge. Gir mulighet for SVV å spisse sin kompetanse for egen oppgaveportefølje og effektivisere saksbehandlingsprosessen. Negativt: SVV må fortsatt ha en ID kontroll i «skranke» ved teoriprøve og praktisk prøve
Private aktører	ID-kontroll i forbindelse med utstedelse av eID	Positivt: Økt kvalitet og sikkerhet i utstedelse ved at biometri legges til grunn. Medfører dermed samme sikkerhet i utstedelse av private ID-bevis som for nasjonal eID. Medfører også redusert ressursbruk for banker samt et potensial for å kutte antall bankfilialer. Negativt: Noe økt ressursbruk for staten, samt et behov for oppdaterte tekniske løsninger.

Tabell 32 Vurdering av områder som potensielt kan være gjenstand for konsolidering og konsekvenser for gjenværende virksomhet (utstedelse, steg 3)

Den nye etaten/direktoratet vil potensielt overta et stort antall oppgaver, prosesser og systemer som ligger i andre virksomheter. Blant virksomhetene som vil bli påvirket er politiet og Skatteetaten, begge store offentlige virksomheter målt i antall ansatte og samlede utgifter. Med utgangspunkt i DFØ sin oversikt[492] er politiet er nr. 1 i antall ansatte og nr. 16 i samlede utgifter og Skatteetaten er nr. 5 målt i antall ansatte og nr. 8 i samlede utgifter. Med et ansvar for pass og ID-kontorene med tilhørende ID-kontroll, Folkeregisteret, samt utvalgte øvrige oppgaver har leverandørens estimert at dette vil tilsvare 550-600 årsverk og 800-850 mil. i samlede utgifter for den nye etaten/direktoratet. Dette vil medføre at den nye etaten/direktoratet potensielt blir blant de 30 største bruttobudsjetterte virksomhetene målt i antall ansatte og blant de 60 største målt i samlede utgifter.

Drøfting av ansvar for ID-relaterte oppgaver i eksisterende etat/direktorat:

Slik leverandøren ser det er det i praksis tre ulike etater/direktorater som peker seg ut når det gjelder konsolidering av ansvar i en eksisterende etat/direktorat: Politiet, Skatteetaten og Digitaliseringsdirektoratet (fra 01.01.2020). Alle har ID-relaterte oppgaver, men de gjennomføres med noe ulike formål og det påvirker brukervennlighet, prosesser, kvalitet og krav til sikkerhet. Det er grunn til å tro at etatene/direktoratene vil vektlegge brukervennlighet, sikkerhet og ressursbruk forskjellig og det vil være ulike styrker og svakheter avhengig av hvilken etat/direktorat som får et helhetlig ansvar for ID:

[491] JD, «Prop. 61 LS (2014-2015), Endringer i politiloven mv. (trygghet i hverdagen – nærpolitireformen)», 2014-2015
[492] DFØ, «statsregnskapet», 2018

Politiet og Politidirektoratet

- Har i dag en sentral rolle i ID-forvaltningen generelt og utlendingsforvaltningen spesielt. JD er største aktør samlet sett i ID-forvaltningen, og i justissektoren står POD med underliggende virksomheter for 76,5 prosent av totale kostnader relatert til ID-forvaltningen, mens UDI og UNE står for hhv. 21 prosent og 2,5 prosent av totale kostnader. På bakgrunn av dette påpeker flere at POD vil være det mest naturlige valget for en konsolidering av ansvar og oppgaver i ID-forvaltningen

- Politiet er utstedere av pass, reisebevis og utlendingspass, samt fremtidens nasjonale ID-kort og har god kompetanse på digital kriminalitet, biometri og ID gjennom Kripos og NID. Nylig har politiet gjennomført større investeringer i førstelinjen for å sikre pass og ID-kort lokalene. Det er mulig å legge til rette for at brukere får ett oppmøtested/skrankepunkt for ID ved pass- og ID-kontorene ved å samle ansvar i POD, samt øke kapasitetsutnyttelsen av ID-faglig ekspertkompetanse. Høyere antall ID-kontroller på ett sted øker kvaliteten på ID-arbeidet. Utregninger viser at 91 prosent av de 46 skattekontorene/SUA-kontorene som tilbyr ID-kontroll (ekskludert Svalbard) har mindre enn 15 km avstand til nærmeste pass- og ID-kontor, og 59 prosent har mindre enn 1 km avstand til nærmeste pass- og ID-kontor. For brukere av skattekontorene vil trolig brukervennligheten øke ved at reisetiden reduseres når de kan benytte pass- og ID-kontor fremfor skattekontor som oppmøtested for ID i fremtiden. I tillegg har politiet Automated Biometric Identification System (ABIS) som inneholder både Pass- og Nasjonalt ID-kort registeret og Utlendingsregisteret. Ettersom pass og ID-kort med eID har de høyeste kravene til sikkerhet og kvalitet av prosessene vil det trolig være sikkerhetsnivået det styres etter på bekostning av brukervennlighet og ressurseffektivisering

- På den andre siden har politiet allerede svært mange ansvarsområder og et bredt kontrollspenn med dagens oppgaveportefølje. Det er derfor en risiko at ID-området blir nedprioritert for andre områder som blir sett på som mer kritiske som kriminalitetsbekjempelse, straffesaker, nærpolitireformen og liknende. Dette påpeker også politiet selv, og mener at ID-forvaltning ikke nødvendigvis er et ansvarsområde som bør ligge i deres oppgaveportefølje. Dette understøttes også av politianalysen.[493] Videre er gjennomføringsevnen knyttet til implementeringen av nye pass og ID-kort av ulike årsaker lav. Endringer i rammebetingelser kan hindre fremdriften i programmet ytterligere. Politiet har heller ikke nødvendigvis de beste forutsetninger for å forvalte fremtidige digitale løsninger med eID

Skatteetaten og Skattedirektoratet

- Har i dag en viktig rolle som folkeregistermyndighet. Folkeregisteret er en nasjonal felleskomponent, men det utgjør fortsatt en relativt begrenset del av den samlede ID-forvaltningen. SKD og Skatteetaten står for rundt 20 prosent av totale kostnader relatert til ID-forvaltningen, som er knyttet til både Folkeregisteret og utøving av ID-kontroll ved skattekontorene, som beskrevet i kapittel 7.1

- Folkeregisteret er en nasjonal felleskomponent med masterdata om grunnidentitet og personinformasjon. Det legger til rette for gjenbruk og videre bruk av data for private og offentlige virksomheter. Alle brukergrupper har i dag

[493] JD, «NOU 2013:9 Ett politi – rustet til å møte fremtidens utfordringer», 2013

et kontaktpunkt med Skatteetaten i løpet av livet. Det er mulig å legge til rette for at brukere får et oppmøtested for ID ved skattekontorene ved å samle ansvar og oppgaver som i dag er hos pass og ID-kontorene. Det kan potensielt øke kapasitetsutnyttelsen på skattekontorene og være ressurseffektviserende. Utregninger viser at kun 55 prosent av de 77 pass- og ID-kontorene (ekskludert Svalbard) har mindre enn 15 km avstand til nærmeste skattekontor, og 33 prosent har mindre enn 1 km til nærmeste skattekontor. Pass og ID-kontorene har flere lokasjoner enn skattekontorene og det kan dermed være en risiko ved å samle ansvar og oppgaver relatert til ID ved skattekontorene, da brukerne vil få færre oppmøtesteder og lengere reisetid. Det kan gi frihetsgrader for ID-forvaltningen å ligge utenfor justissektoren. Hvis ID i større grad oppfattes som en forvaltningsoppgave fremfor politioppgave, kan det skape større aksept for opptak av biometri og deling av data. En mulighet er at SKD får et helhetlig ansvar for ID-forvaltningen, men at førstelinjen fortsatt er hos politiet. Det fremstår for leverandøren som en kompleks styringsmodell og er ikke vurdert nærmere

- I samtaler med leverandøren gir flere uttrykk for at Skatteetaten er kjent for å levere på nye ansvarsområder og oppgaver som for eksempel overføring av avgift fra Tolletaten og innkreving fra NAV. Leverandøren ønsker likevel å påpeke at disse oppgavene har vært nærmere SKDs kjerneoppgaver og at en flytting av ansvar og oppgaver relatert til ID fra politiet i mindre grad oppfattes som en del av Skatteetatens samfunnsoppdrag

- En vesentlig del av oppgaveløsningen og saksbehandlingen gjennomføres i justissektoren. Leverandørens vurdering er at det kan medføre et større behov for koordinering og samordning på tvers av sektorene ved å plassere et helhetlig ansvar i SKD. På kort sikt er det også risiko for kritisk fagkompetanse knyttet til ID blir igjen i justissektoren

Digitaliseringsdirektoratet (sammenslåing av Difi og Altinn)

- Vil fra 1.1.2020 ha ansvaret for en digital plattform for forvaltningen – både som premissgiver og leverandør. Digital identitet er en viktig del, sammen med andre byggeklosser, i et økosystem for å digitalisere prosesser i forvaltningen og understøtte digitale tjenester til innbyggere og næringsliv. I dag står Difi for rundt 5 prosent av totale kostnader relatert til ID-forvaltningen. Det er i hovedsak knyttet til drift og forvaltning av ID-porten og arbeid med eID, men utgjør et relativt lavt antall årsverk, som beskrevet i kapittel 7.1. Digitaliseringsdirektoratet vil ressursmessig være en mindre statlig virksomhet sammenlignet med politiet og Skatteetaten. Hensikten med å etablere et digitaliseringsdirektorat er samle digitaliseringsarbeid i staten. Det er fare for å svekke digitaliseringsarbeidet ved å legge til nye ansvarsområder i direktoratet eller ved å dele ansvaret for digitalisering opp i nye enheter. Etter leverandørens syn vil trolig tyngdepunktet i direktoratet endres fra digitalisering til ID ved å samle ansvar og oppgaver her

- Samle ansvaret i digitaliseringsdirektoratet er ei fremtidsrettet løsning med tanke på økende bruk av eID og digital autentifisering. God identitetsforvaltning er sammen med andre fagområder som informasjonssikkerhet, arkitektur, styring, forvaltning og utvikling en forutsetning for levere et økosystem. Tilliten til eID er basert på reguleringer, internasjonale standarder, sertifiseringer og felles prosedyrer som skal garantere for ID på tvers av aktører og landegrenser. En tilhørighet i Digitaliseringsdirektoratet samler et fragmentert ansvar ved at både Difi og Nkom har ulike roller på dette området, i tillegg til PODs ansvar knyttet til eID på nasjonale ID-kort

- I dialog med leverandøren gir flere uttrykk for at lokal tilstedeværelse er gårsdagens modell. Dette understøttes i beskrivelsen av viktige utviklingstrekk og målbilde i kapittel 9. Det er mulig å legge til rette for at brukere får et oppmøtested for ID ved å samle ansvar, samt øke kapasitetsutnyttelsen, men det er ikke planlagt en førstelinje som del av Digitaliseringsdirektoratet. Etter leverandørens syn er det ikke hensiktsmessig å drøfte etablering av en ny førstelinje. Gjenbruk av pass og ID-kontorene eller skattekontorene er mulig, men det kan potensielt skape en mer krevende styringsmodell på tvers av sektorene sammenlignet med de to andre løsningene

- En vesentlig del av oppgaveløsningen og saksbehandlingen gjennomføres i justissektoren. Leverandørens vurdering er at det kan medføre et større behov for koordinering og samordning på tvers av sektorene ved å plassere et helhetlig ansvar i Digitaliseringsdirektoratet. Leverandøren vurderer at direktoratet har bedre forutsetninger for å overta drift og forvaltning av Folkeregisteret, enn oppgaveløsningen og saksbehandlingen som ligger i justissektoren. På kort sikt er det også risiko for kritisk fagkompetanse knyttet til ID blir igjen i justissektoren

Leverandøren har i dette alternativet ikke drøftet om det å gi én statsråd ansvar for ID-forvaltningen og konsolidere ansvar for utvalgte ID-relaterte oppgaver i en eksisterende etat/direktorat vil påvirke fagmiljøene på departementsnivå, enten mellom departementer eller mellom departement og etat/direktorat. Det må vurderes nærmere og vil avhenge av hvilken statsråd og eksisterende etat/direktorat som får et helhetlig ansvar for ID-forvaltningen.

Det er grunn til å tro at departementene vil vektlegge brukervennlighet, sikkerhet og ressursbruk forskjellig, og det vil være ulike styrker og svakheter avhengig av hvem som blir eierdepartementet for ny etat/direktorat. I det følgende oppsummeres styrker og svakheter ved alternativ 4.

Styrker:

- En felles strategi for ID-forvaltningen legger til rette for mer helhetlig og strategisk styring ved å prioritere og balansere hensyn til brukervennlighet, sikkerhet og ressursbruk. Erfaringsmessig blir sikkerhet vektlagt over de to andre hensyn uten et tilstrekkelig faktagrunnlag

- Det vil være forholdvis enkelt å utarbeide og implementere en felles strategi for ID-forvaltning i Norge basert på eksisterende dokumentasjon og pågående arbeid i KoID, samt leverandørens skisse til mål, jf. kapittel 9
    - Strategien kan potensielt være en døråpner for å etablere utvidede hjemler tilsvarende som i strategien mot arbeidslivskriminalitet beskrevet i kapittel 4.2.4

- Strategien legger til rette for at alle aktører på ulike nivåer har en felles forståelse av hovedutfordringer og hovedmålsettinger i ID-forvaltningen, samt at de trekker i samme retning. En viktig del av strategiarbeidet er å etablere statistikk over ID-kriminalitet og et bedre kunnskapsgrunnlag om samfunnsmessige kostnader og konsekvenser knyttet feil og misbruk av ID for å øke bevisstheten og ta faktabaserte beslutninger

- En statsråd, et departement og en etat/direktorat får et helhetlig ansvar for ID-forvaltningen i Norge. En ansvarlig statsråd vil kunne løfte viktigheten av området, og styrker forutsetningene for bedre gjennomføringsevne/-kraft. Felles forståelse av ansvar og roller vil legge til rette for bedre koordinering og

samhandling mellom viktige aktører i ID-forvaltningen. Det vil være en mer sentralisert struktur i ID-forvaltningen og sterkere grad av styring med en ansvarlig statsråd enn i alternativ 3 og det kan påvirke ressursbruken positivt

- Det er grunn til å tro at JD og POD vil legge stor vekt på sikkerhet og at sikkerhetsnivået vil være styrende, mens KMD og Digitaliseringsdirektoratet i større grad vil vektlegge brukervennlighet. Det kan også være tilfelle at ID-forvaltningen får større frihetsgrader ved å ligge utenfor justissektoren. Hvis dette i større grad oppfattes som et forvaltningsoppgaven fremfor politioppgave, kan det skape større aksept for opptak av biometri, deling av data mv

- Ved å sentralisere styring og struktur i ID-forvaltningen er det mulig med en felles førstelinje og et oppmøtested for ID-relaterte oppgaver. Det vil øke brukervennligheten. Det er potensial for samlokalisering, noe som kan bidra til bedre service for brukeren og større innsikt i hverandres fagområder. Det kan gi ressurseffektivisering og synergieffekter for eksempel ved bedre utnyttelse av ID-faglig kompetanse, økt antall ID-kontroller og økende gjenbruk av ID-kontroller

- Det er momentum i ID-forvaltningen nå, som bør utnyttes til å gjøre nødvendige og større grep for å sikre at ID blir prioritert som en kjerneoppgave fremover. Ved å flytte ansvar og oppgaver fra en av de største statlige virksomhetene hva gjelder ansatte, budsjett og oppgaveportefølje noe som, for disse, vil bidra til økt fokus på kjerneoppgaver, mer effektiv drift og prioritering av nødvendige utviklingsaktiviteter

- Det vil være betydelige omstillingskostnader på kort sikt ved å flytte ansvaret for ID-forvaltningen til en eksisterende etat/direktorat, men det vil i større grad støtte ambisjonene i avbyråkratiseringsreformen enn å etablere en ny etat/direktorat for ID

Svakheter:

- Det er usikkert om en felles strategi for ID-forvaltning i Norge alene vil gi effekt knyttet til brukervennlighet, sikkerhet og ressursbruk – og om det vil løse de største utfordringene i dagens ID-forvaltning. Å sikre prioritering av de riktige tiltakene kombinert med ID-forvaltningens gjennomføringsevne vil være avgjørende

- Det er begrenset med systemstøtte for å etablere statistikk over ID-kriminalitet og samfunnsmessige kostnader knyttet feil og misbruk av ID. Berørte aktører har i dag data på mindre enkeltområder f.eks. feil og misbruk av ID-dokumenter, men ikke samfunnsmessige konsekvenser for ID-forvaltningen som helhet. En viktig del av strategiarbeidet kan potensielt utgjøre en del manuelt arbeid som vil kreve ressurser fra de berørte aktørene uten at det vil ha effekt på brukervennlighet, sikkerhet og ressursbruk på kort sikt

- Det er få representanter fra departementene som gir uttrykk for at de ønsker å ta et helhetlig ansvar for ID-forvaltningen i Norge og det kan være en gjennomføringsrisiko. Politiet og Skatteetaten er blant de største statlige virksomhetene med viktige samfunnsoppdrag og brede oppgaveporteføljer. Representanter fra FIN, JD og KMD har uttrykt skepsis til om det er hensiktsmessig å gi deres respektive underliggende etat/direktorat større og/eller et helhetlig ansvar for ID-forvaltningen. Det er en ambisjon i større grad å spesialisere oppgaveporteføljene. Dette støttes også av representanter fra underliggende etater/direktorater. Flere av aktørene i ID-forvaltningen

gjennomgår eller har nylig gjennomgått omstillinger eksempelvis «Nye Skatt», nærpolitireformen og etableringen av nytt digitaliseringsdirektorat. Det er uklart hvilke konsekvenser ytterligere endringer vil ha på etatene/direktoratene

- Avhengig av hvilken statsråd og etat/direktorat som får ansvaret kan alternativet medføre et større behov for dialog på tvers av sektorer med koordinering og samordning uten at det går noe fortere eller skaper økt gjennomføringskraft av den grunn – samle alt i en boks løser ikke nødvendigvis utfordringene i ID-forvaltningen. Når ID-relaterte ansvar og oppgaver samles i en eksisterende etat/direktorat vil de i mindre grad være en integrert del av andre sektorers ansvarsområder og saksbehandling og det kan ha konsekvenser for dagens synergieffekter

- De tre etatene/direktoratene har alle ID-relaterte oppgaver, men de gjennomføres med ulike formål og det kan påvirke krav til brukervennlighet, kvalitet, prosesser og sikkerhet. Leverandøren har ikke tilstrekkelige faktagrunnlag for å kost/nytte-vurdere hvilke av de tre etatene/direktoratene som vil være mest samfunnsøkonomisk lønnsom og gi en mer brukervennlig, sikker og ressurseffektiv ID-forvaltning. Det vil være behov for investeringer for å ta over ansvar og oppgaver relatert til ID som i dag ligger spredt på flere ulike aktører. Det vil være ulike kulturer, rutiner, retningslinjer, metodikk, rammeverk mv. som skal integreres. Det krever ledelse, styring, infrastruktur, organisasjon og kompetanse som ikke er tilstrekkelig tilstede i dag. Erfaringsmessig vil det være energitap i berørte virksomheter og fare for å miste spesifikk fagkompetanse i slike omstillingsprosesser

- Felles førstelinje og samlokalisering for ID-relaterte oppgaver uten å gjøre endringer på direktorats/etats/departementsnivå er heller ikke kost/nytte-vurdert isolert da leverandøren ikke har hatt tilstrekkelig data til å vurdere det. Derimot ser vi at det er flere prosesser med likhetstrekk mellom tre skrankepunkter hos politiet, Skatteetaten og SVV. Det vil være en krevende styringsmodell med det kan eventuelt arbeides videre med. Leverandøren erfarer at det vil være utfordrende å etablere og styre en felles førstelinje med oppmøtested for ID-relaterte oppgaver uten å endre dagens styring og struktur i ID-forvaltningen: fire departementer, fire direktorater, flere lover, forskrifter og ulike sett at instrukser og retningslinjer. Dersom førstelinjen skal samlokaliseres og fungere ressurseffektivt, sikkert og brukervennlig krever det at lokaler, systemer, ledelse, rutiner og retningslinjer er integrert og koordinert

- Det vil være vesentlige omstillingskostnader på kort sikt ved å flytte ansvar og oppgaver til en eksisterende etat/direktorat, men trolig lavere enn ved å etablere en ny etat/direktorat. Erfaringsmessig vil det uavhengig av det være effektivitetstap hos berørte aktører ved større omstillinger. Det vil ta tid før effekten av en eventuell ny struktur i ID-forvaltningen realiseres

- Det vil være et betydelig behov for å bygge opp Digitaliseringsdirektoratet og/eller SKD for å ta over ansvar og oppgaver relatert til ID som i dag ligger i politiet. Dette vil også gjelde for POD, men trolig i mindre grad de har en vesentlig del av ID-forvaltningen i dag. For SKD og Digitaliseringsdirektoratet vil det kreve en infrastruktur, organisasjon, kompetanse og sikkerhet som ikke er til stede i dag og det kan stilles spørsmål ved om det er samfunnsøkonomisk lønnsomt i lys av tilsvarende rapporter og utredninger på området. På den andre siden har politiet allerede svært mange ansvarsområder og et bredt kontrollspenn med dagens oppgaveportefølje. Det er derfor en risiko at ID-området blir nedprioritert for andre områder som blir sett på som mer kritiske som kriminalitetsbekjempelse, straffesaker, nærpolitireformen og liknende

15.2.5 Alternativ 5: Gi én statsråd ansvar for ID-forvaltningen, utarbeide en felles strategi for ID-forvaltningen, samt opprette en ny etat/direktorat med ansvar for ID-forvaltningen

Alternativ 5 innebærer å

- *styrke departementene sin rolle som strategisk aktør*
- *gi én statsråd ansvar for å samordne ID-forvaltningen i Norge*
- *konsolidere ansvar for utvalgte ID-relaterte oppgaver, prosesser og systemer i en ny etat/direktorat*

Leverandøren viser til kapittel 15.2.1 og 15.2.2 for beskrivelse av første og andre kulepunkt over.

Alternativ 5 innebærer vesentlige endringer i styringen og strukturen av ID-forvaltningen, både på departements- og direktorats-/etatsnivå, ved at ansvaret for ID-forvaltningen sentraliseres under en statsråd og det etableres en ny statlig etat/direktorat. Leverandøren bygger i liten grad videre på eksisterende styringsstrukturer i dette alternativet. Det vil være samme grad av sentralisert styring som i alternativ 4, men større grad av sentralisert struktur, som følge av konsolideringen av ansvar hos en ny etat/direktorat som har ID som sin kjerneoppgave.

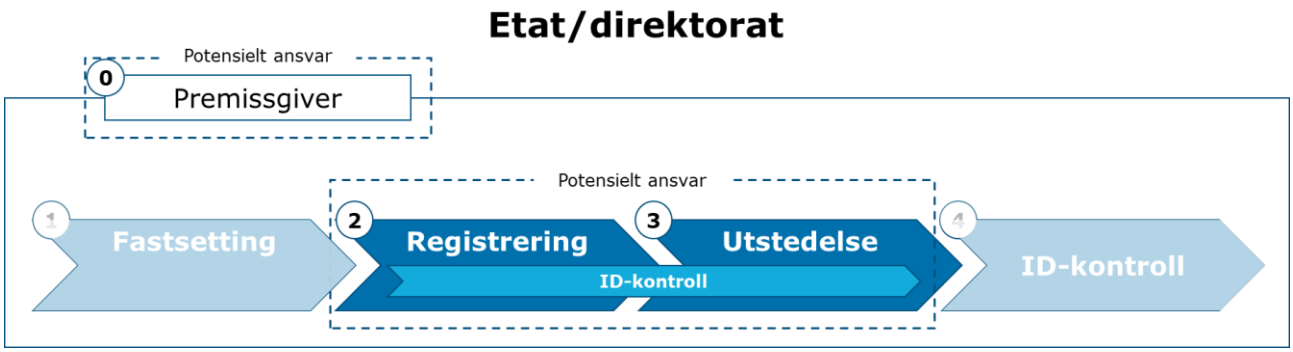
En ny etat/direktorat gis myndighet av et departement til å være premissgiver for ID-forvaltningen og tar en samordningsrolle på tvers av sektorer. Etaten/direktoratet vil være et landsdekkende myndighetsorgan som har ID-forvaltning som sin kjerneoppgave.

Som beskrevet i kapittel 8 vurderer leverandøren at dagens styring og struktur i ID-forvaltningen ikke er tilrettelagt tilstrekkelig for å sikre økt brukervennlighet, sikkerhet og ressurseffektivitet. Det har tidligere vært omtalt i flere rapporter fra departementer og direktorater at det må vurderes om en kvalifisert myndighet bør gis et større og mer helhetlig ansvar for ID-forvaltningen. I utredningen om helhetlig ansvar for EØS-borgere var et alternativ at én etat skal ha et mer helhetlig ansvar for ID-forvaltningen av EØS-borgere, uten at rapporten tok standpunkt til løsning.

I dette alternativet drøfter leverandøren en konsolidering av ansvar for utvalgte ID-relaterte oppgaver, prosesser og systemer ved at det samles i en ny etat/direktorat for ID.

Potensielt ansvar, oppgaver, prosesser og systemer:

I likhet med alternativ 4 avgrenses alternativ 5 til å gjelde den overordnede ID-prosessen med tilhørende oppgaver, prosesser og systemer i saksbehandlingen, som beskrevet i kapittel 15.2.4. Direktoratets/etatens ansvar totalt sett er illustrert i figuren nedenfor.



Figur 73 Konsolidering av ansvar for utvalgte ID-relaterte oppgaver, prosesser og systemer

Som premissgiver får etaten/direktoratet et overordnet ansvar for ID-prosessen, men dette innebærer ikke at etaten/direktoratet vil være ansvarlig for å gjennomføre alle stegene i ID-prosessen. Enkelte ID-relaterte aktiviteter vil fortsatt være en integrert del av ulike sektorers ansvarsområder og saksbehandling, men alternativet innebærer en tydelig konsolidering fra dagens nivå.

Etaten/direktoratet vil ha ID-forvaltning som sin kjerneoppgave og ha et premissgiveransvar for hele ID-prosessen. Ansvar for gjennomføring av oppgaver, systemer og prosesser knyttet til registrering (steg 2) og utstedelse (steg 3) som er oppsummert i tabellen nedenfor flyttes til etaten/direktoratet. Dette er de samme oppgavene som i tabellene i kapittel 15.2.4. Tabellene i alternativ 4 er benyttet som underlag for vurderingene i alternativ 5.

Videre er det også kort oppsummert i tabellene hvilke konsekvenser flytting av oppgaven gir for virksomheten i hvert tilfelle. Det understrekes at listene ikke anses som uttømmende og er basert på leverandørens vurdering. Konsekvensene av flytting må utredes, kost/nytte-vurderes og detaljeres nærmere før det eventuelt besluttes endringer.

ID-relaterte oppgaver som flyttes fra en aktør vil potensielt kunne frigjøre ressurser ved å legge til rette for en mer effektiv og helhetlig ID-forvaltning. Det er også et poeng at ingen aktør har ID som kjerneoppgave i dag, og at en flytting av ID-relaterte oppgaver ikke vil være relatert til deres kjernevirksomhet, det vil derimot redusere deres totale oppgaveportefølje. Begge disse punktene gjelder gjennomgående og poengteres ikke eksplisitt i tabellene under.

Steg 0: ID-relaterte oppgaver/prosesser/systemer tilknyttet rollen som premissgiver		
	Flyttes til «ID-etat/direktorat»	Konsekvenser for virksomheten
Politiet	Fagmiljø relatert til ID (ikke straffesaksbehandling) i POD, politidistriktene, PU og Kripos som er ansvarlig for å etablere og videreutvikle standarder, krav, rutiner, retningslinjer, kompetanse, praksis i ID-prosessen	Positivt: Samler ansvar som per i dag er spredt på flere aktører i ID-forvaltningen, dette legger til rette for styrket kompetanseutvikling og -deling. Et samlet fagmiljø antas også å være mer robust og gi mer fleksibel kapasitetsutnyttelse. Negativt: Fragmentering av eksisterende fagmiljø. Reduserer nærheten til politiets samfunnsoppdrag og skaper større avstand til straffesakssporet og kriminalitetsbekjempelse.
	Fag-/metodeutvikling, opplæring, og kursing innen ID-relaterte emner i POD, politidistriktene, PU og Kripos	Positivt: Samler ansvar som per i dag er spredt på flere aktører i ID-forvaltningen, dette legger til rette for styrket kompetanseutvikling og -deling. Et samlet fagmiljø antas også å være mer robust og gi mer fleksibel kapasitetsutnyttelse.

Steg 0: ID-relaterte oppgaver/prosesser/systemer tilknyttet rollen som premissgiver		
	Flyttes til «ID-etat/direktorat»	Konsekvenser for virksomheten
		Negativt: Fragmentering av eksisterende fagmiljø. Reduserer nærheten til politiets samfunnsoppdrag og skaper større avstand til straffesakssporet og kriminalitets-bekjempelse.
	NID i sin helhet med spisskompetanse på ID- og underlagsdokumenter, verktøy og metode for å avklare identitet til utlendinger, tar initiativ til samarbeid og fellesløsninger, samt tilbyr opplæring, verktøy, utvikler statistikk og analyser, bistand og råd	Positivt: Forenkler styringslinjer og reduserer byråkrati og koordinering. Tydeligere kobling mellom premissgiver og nasjonalt ekspertorgan. Muliggjør å realisere effektene som var tiltenkt ved etableringen av NID. Negativt: Potensielt mer utfordrende å bevare sin rolle som uavhengig ekspertorgan.
UDI	Relevant fag-/metodeutvikling, opplæring og kursing innen ID-relaterte emner i UDI	Positivt: Samler ansvar som per i dag er spredt på flere aktører i ID-forvaltningen, dette legger til rette for styrket kompetanseutvikling og -deling. Et samlet fagmiljø antas også å være mer robust og gi mer enhetlig tilnærming til brukergrupper og fleksibel kapasitetsutnyttelse. Negativt: Fragmentering av eksisterende fagmiljø. Reduserer nærheten til utlendingsforvaltningen.
Difi	Regelverk, internasjonale standarder, prosedyrer, policy og styringsrammeverk for eID	Positivt: I dag har Difi, Nkom og POD roller i arbeidet med eID, men leverandøren opplever at ingen har et helhetlig ansvar og styring Negativt: Fragmentering av eksisterende fagmiljø. Reduserer nærheten til forvaltningens digitale plattform – økosystem. Det er fare for å svekke digitaliseringsarbeidet ved å dele ansvaret for opp i nye enheter.
	Drift og forvaltning av ID-porten og eID	Positivt: Mulighet til å samlokalisere ansvaret for eID med øvrige ID-relaterte oppgaver. Negativt: Leverandørens oppfatning er at dette fungerer godt i dag og at det medfører en risiko å flytte ansvaret for drift og forvaltning.
Skatteetaten	Premissgiverrolle for identitetsnummer (f- og d-nummer)	Positivt: Reduserer oppgaveporteføljen til Skatteetaten. Økt felles forståelse for rekvirering blant rekvirentene, i tillegg til at ansvar som per i dag er spredt på flere aktører samles slik at identitetsnummer og ID-bevis kan sees i større grad i sammenheng. Negativt: Reduserer nærheten til Skatteetatens samfunnsoppdrag, spesielt innbetaling av avgifter og skatt, samt forebygging av arbeidslivskriminalitet. I tillegg til oppgaver tilknyttet Folkeregisteret som ikke nødvendigvis er ID-relatert.
	Ansvar for koordineringsgruppe (KoID)	Positivt: Mindre behov for formelle og uformelle samarbeidsarenaer ved å gi et helhetlig ansvar til en aktør. Sikrer mer kontinuitet ved at ansvaret ikke rulleres hvert andre år. Negativt: Mindre mulighet til å påvirke arbeidet i KoID, men siden ansvaret for KoID er rullerende er konsekvensen begrenset.
KD	Statsborgerloven	Positivt: UDI, UNE og politiet, som er utøvende myndigheter, jf. loven § 2, får potensielt ett departement mindre å forholde seg til. Negativt: Kunnskaps- og integreringsministeren får mindre mulighet til å påvirke forvaltningen av loven, som er et viktig integreringspolitisk styringsinstrument.

Tabell 33 Vurdering av områder er gjenstand for konsolidering i «ID-etat/direktorat» og konsekvenser for gjenværende virksomhet (premissgiver, steg 0)

En tydelig premissgiver for ID-forvaltningen styrker forutsetningene for bedre samordning og en mer helhetlig tilnærming til ID-forvaltningen. Som premissgiver er det naturlig å anta at oppgavene relatert til steg 1-4 i verdikjeden vil endre sin karakter og at de ulike aktørene i større grad vil være en utførende part for premissgiveren. Disse endringene er ikke hensyntatt i tabellen under. Her fokuserer leverandøren på oppgaver/prosesser/systemer relatert til registrering (steg 2) og utstedelse (steg 3) slik de foreligger i dag.

Steg 2: ID-relaterte oppgaver/prosesser/systemer tilknyttet registrering		
	Flyttes til «ID-etat/direktorat»	Konsekvenser for virksomheten
Politiet	Drift og forvaltning av passregisteret og ID-kort registeret (når det er implementert, herunder opptak av biometri for norske statsborgere (kun i forvaltningssporet))	Positivt: Reduserer oppgaveporteføljen til politiet. Det er leverandørens inntrykk at området blir nedprioritert mot andre mer kritiske områder eller kjerneoppgaver i politiets oppgaveportefølje. Negativt: Større avstand til straffesakssporet og kriminalitetsbekjempelse.
	Registrering av EØS-borgere med tilhørende ID-kontroll	Positivt: En mer enhetlig tilnærming til ulike brukergrupper og få bedre kontroll på EØS-borgere. Negativt: Større avstand til straffesakssporet og kriminalitetsbekjempelse.
	Utlendingsforvaltningen i politi-distriktene etter 3.landsregelverket: Mottak av søknader om oppholdstillatelse, utlendingspass, reisebevis, statsborgerskap og ID-kontroll ved mottak av alle disse + effektuering av vedtak og bestilling av oppholdskort	Positivt: Reduserer oppgaveporteføljen til politiet. En mer enhetlig tilnærming til ulike brukergrupper og ulike ID-bevis. Øke utnyttelsen av ID-faglig kompetanse. Negativt: Større avstand til straffesakssporet og kriminalitetsbekjempelse. Muligens behov for å se nærmere på utlendingsforvaltningen uavhengig av ID for å sikre en mer helhetlig organisering og styring.
Skatteetaten	Drift og forvaltning av Folkeregisteret med tilhørende tildeling av f- og d-nummer	Positivt: Mulighet til å samlokalisere det Folkeregisteret med øvrige ID-relaterte registre og oppgaver. Negativt: Modernisering av Folkeregisteret er i hovedsak ferdigstilt, og leverandørens oppfatning er at drift og forvaltning fungerer godt i dag og at det medfører en risiko å flytte ansvaret.
	Skattekontorenes ansvar for ID-kontroll på vegne av d-nummerrekvirenter, bekreftelse av farskap og melde innflytting til Norge[494]	Positivt: Reduserer oppgaveporteføljen til Skatteetaten. Mulighet til å samle ID-relaterte oppgaver i en felles 1.linje. Negativt: Fortsatt behov for skattekontor og en fysisk 1.linje for å bistå med å søke om skattekort, men behovet og omfanget av oppgaver reduseres vesentlig.
UDI	*Ikke identifisert*	*Ikke identifisert*
Alle rekvirenter	Ansvar for rekvirering av d-nummer med tilhørende rutiner, prosesser og systemer overføres til en etat/direktorat.	Positivt: samler ansvar som i dag er spredt på flere aktører og legger til rette for mer bruk av «ID-kontroll». Dette forventes å redusere risiko for feil og misbruk av ID. Negativt: Kan gi øke saksbehandlingstiden til aktøren som ikke lenger kan rekvirere d-nummer.

Tabell 34 Vurdering av områder som er gjenstand for konsolidering i «ID-etat/direktorat» og konsekvenser for gjenværende virksomhet (registrering, steg 2)

Steg 3: ID-relaterte oppgaver/prosesser/systemer tilknyttet utstedelse		
	Flyttes til «ID-etat/direktorat»	Konsekvenser for virksomheten
Politiet	Utstedelse av pass- og nasjonale ID-kort med tilhørende ID-kontroll	Positivt: Reduserer oppgaveporteføljen til politiet. Ifølge POD er det tenkt at pass og ID-kontorene i de store byene i stor grad skal jobbe med utstedelse av pass og nasjonale ID-kort.

[494] Skatteetaten.no, «Bestill tid», 2019

		Negativt: Oppgaven med å utstede pass og nasjonale ID-kort kan være avhengig av informasjon fra politiet, og politiet bør ha tilgang til informasjonen i passregisteret eller utledningsdatabasen. Om en annen myndighet bemyndiges til å utstede nevnte ID-bevis, vil politiet således fortsatt måtte kobles inn i arbeidet med å behandle søknader.[495] Ifølge POD vil pass- og ID-kontor ved de mindre tjenestestedene vil oppgaver knyttet til utstedelse av pass og nasjonalt ID-kort være én blant mange oppgaver.
	Utlendingsforvaltningen i politi-distriktene etter 3.landsregelverket: Utstedelse av oppholdskort, utlendingspass, reisebevis, statsborgerskap og tilhørende ID-kontroll	Positivt: Reduserer oppgaveporteføljen til politiet. En mer enhetlig tilnærming til ulike brukergrupper og ulike ID-bevis. Øke utnyttelsen av ID-faglig kompetanse. Negativt: Oppgaven med å utstede oppholdskort/utlendingspass/reisebevis kan være avhengig av informasjon fra politiet, og politiet bør ha tilgang til informasjonen i passregisteret eller utledningsdatabasen. Om en annen myndighet bemyndiges til å utstede nevnte ID-bevis, vil politiet således fortsatt måtte kobles inn i arbeidet med å behandle søknader. Større avstand til straffesakssporet og kriminalitets-bekjempelse. Muligens behov for å se nærmere på utlendingsforvaltningen uavhengig av ID for å sikre en mer helhetlig organisering og styring.
Statens vegvesen	ID-kontroll og innhenting av bilde og signatur til førerkortutstedelse og ved fornyelse av førerrettsbevis	Positivt: Samles kompetansen på identitetssjekk for flere formål i en organisasjon, vil det bidra til å redusere muligheten for falske identiteter i Norge. Gir mulighet for SVV å spisse sin kompetanse for egen oppgaveportefølje og effektivisere saksbehandlingsprosessen. Negativt: SVV må fortsatt ha en ID kontroll i «skranke» ved teoriprøve og praktisk prøve
Private aktører	ID-kontroll i forbindelse med utstedelse av eID	Positivt: Økt kvalitet og sikkerhet i utstedelse ved at biometri legges til grunn. Medfører dermed samme sikkerhet i utstedelse av private ID-bevis som for nasjonal eID. Medfører også redusert ressursbruk for banker samt et potensial for å kutte antall bankfilialer. Negativt: Noe økt ressursbruk for staten, samt et behov for oppdaterte tekniske løsninger.

Tabell 35 Vurdering av områder som er gjenstand for konsolidering i «ID-etat/direktorat» og konsekvenser for gjenværende virksomhet (utstedelse, steg 3)

Den nye etaten/direktoratet vil potensielt overta et stort antall oppgaver, prosesser og systemer som ligger i andre virksomheter. Blant virksomhetene som vil bli påvirket er politiet og Skatteetaten, begge store offentlige virksomheter målt i antall ansatte og samlede utgifter. Med utgangspunkt i DFØ sin oversikt[496] er politiet er nr. 1 i antall ansatte og nr. 16 i samlede utgifter og Skatteetaten er nr. 5 målt i antall ansatte og nr. 8 i samlede utgifter. Med et ansvar for pass og ID-kontorene med tilhørende ID-kontroll, Folkeregisteret, samt utvalgte øvrige oppgaver har leverandørens estimert at dette vil tilsvare 550-600 årsverk og 800-850 mil. i samlede utgifter for den nye etaten/direktoratet. Dette vil medføre at den nye etaten/direktoratet potensielt blir blant de 30 største bruttobudsjetterte virksomhetene målt i antall ansatte og blant de 60 største målt i samlede utgifter.

Sammen med overføring av oppgaver, systemer og prosesser må også ansvar for forvaltningen av tilhørende regelverk overføres til ny etat/direktorat. I forlengelsen av dette bør antakelig også det formelle forvaltningsansvaret for de relevante

[495] JD, «Prop. 61 LS (2014-2015), Endringer i politiloven mv. (trygghet i hverdagen – nærpolitireformen)», 2014-2015
[496] DFØ, «Statsregnskapet», 2018

regelverkene overføres til departementet som får etatsstyringsansvar for etaten/direktoratet.

Drøfting av førstelinje for ny etat/direktorat:

Med utgangspunkt i viktige utviklingstrekk og målbilde i kapittel 9 vurderer leverandøren at det ikke er hensiktsmessig å drøfte etablering av en ny førstelinje som del av en ny etat/direktorat. Gjenbruk av eksisterende førstelinjer vil være fordelaktig for å utnytte eksisterende infrastruktur, samt unngå relativt betydelig investeringer spredt geografisk. Leverandøren har derfor ikke vurdert å opprette en ny førstelinje som del av å etablere en etat/direktorat for ID nærmere.

Etter leverandørens syn er det overordnet to tilnærminger: *Gjenbruke førstelinjen hos politiet* eller *gjenbruke førstelinjen i Skatteetaten.*

- Politiet er involvert i alle de fire stegene i ID-prosessen. Leverandøren vurderer at politiet samlet sett har en større faglig og mer fremtredende rolle i ID-forvaltningen enn Skatteetaten med både bredde- og spisskompetanse. Videre besluttet JD nylig å etablere totalt 78 pass- og ID-kontor. Ombyggingen og fysisk sikring av kontorene vil i hovedsak være ferdig i 2019. Da skal de oppfylle fastsatte kvalitets- og sikkerhetsmessige krav etter merknader fra Riksrevisjonen. Politiet har også gjennomført store investeringer i utstyr som biometrikiosker og annet teknisk utstyr for ID-kontroll og dokumentgransking. Pass og ID-kontorene har en større geografisk utstrekning enn skattekontorene og det gir mindre reisetid for brukerne. Leverandøren har ikke mottatt data til å anslå hvor stor andel av den totale ressursbruken i politiets førstelinje som er relatert til ID, herunder arbeid tilknyttet politiets oppgaveutførelse og politidistriktenes rolle i utlendingsforvaltningen

- Skatteetaten er folkeregistermyndighet og ID-arbeidet er i all hovedsak rettet mot drift og forvaltning av Folkeregisteret og tildeling av d-nummer og f-nummer med tilhørende ID-kontroll. De har spisskompetanse på et smalere fagfelt i ID-forvaltningen enn politiet. Skatteetaten overtok ansvaret for ID-kontroll på vegne av øvrige d-nummerrekvirenter i 2017. Det er 42 skattekontorer som utfører ID-kontroll. Hvis ID i større grad oppfattes som et forvaltningsoppgaven fremfor politioppgave, kan det skape større aksept for opptak av biometri, deling av data og lignende. Leverandøren anslår overordnet at inntil 40 prosent av ressursbruken på skattekontorene er/kan være relatert til Folkeregisteret.[497] Øvrige oppgaver og veiledning er i hovedsak relatert til skatt for privatpersoner og næring

Til tross for manglende data over politiets ressursbruk i førstelinjen er leverandørens overordnede vurdering at ved å gjenbruke politiets førstelinje vil det være:

1) Større mulighet for å få til en felles førstelinje med et oppmøtested for ID

2) Større potensial for ressurseffektivisering på kort og lang sikt

I den videre drøftingen vil leverandøren legge til grunn at en ny etat/direktorat for ID vil gjenbruke førstelinjen i politiet.

[497] Eksempler på oppgaver og veiledning relatert til Folkeregisteret som ikke er ID-kontroll: Adresse, farskap, flytte, forespørsel om opplysninger, fødselsnummer, førstegangs navnevalg, navn, sivilstand, statsborgerskap og attester Folkeregister

Drøfting av eierskap og styringsmodell for ny etat/direktorat:

Som beskrevet i kapittel 15.2.2 drøfter leverandøren at det er tre statsråder og departementer som er aktuelle for et helhetlig ansvar for ID-forvaltningen: FIN, JD og KMD. Eierskap og tilhørighet for en ny etat/direktorat bygger videre på denne drøftelsen og gjentas ikke her.

For å sikre en mer helhetlig styring og tydeliggjøring av ansvar for ID-forvaltningen ble følgende temaer drøftet: *Nærhet til største aktør/bruker, kompleksitet i øvrig oppgaveportefølje, gjennomføringsevne, politikkområder og skille mellom politifaglige oppgaver og øvrig forvaltning, oppfattet vektlegging av sikkerhet, brukervennlighet og ressursbruk, samt nærhet til førstelinje*.

Overordnet vurderer leverandøren at det er en mer utfordrende styringsmodell med KMD eller FIN som eierdepartement når politiets førstelinje benyttes enn å rendyrke en styringsmodell innenfor JD. Videre har FIN og KMD en begrenset rolle i dagens ID-forvaltning sammenlignet med JD, selv om begge har god erfaring som samordningsdepartementer på andre politikk- og saksområder og viser gjennomføringskraft. Dersom det ikke er ønskelig å endre departementenes ansvar og porteføljer kan det vurderes om en etat/direktorat skal få styringssignaler fra flere departementer som tilfellet er med Nasjonal sikkerhetsmyndighet. Etter leverandørens syn er det ikke en foretrukket løsning og drøftes derfor ikke nærmere i dette alternativet.

I den videre drøftingen vil leverandøren legge til grunn at JD er eierdepartement for ny etat/direktorat. Leverandøren skisserer to alternative styringsmodeller for etat/direktorat for ID med førstelinje.

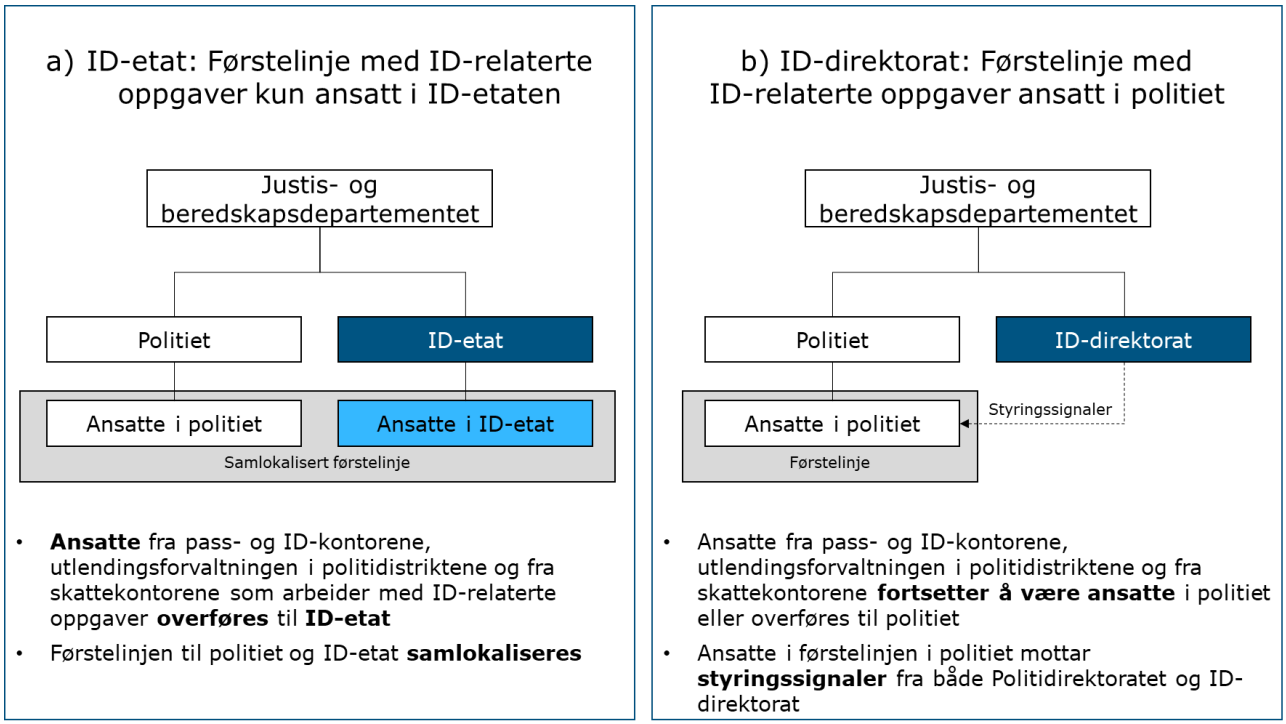
Ny etat/direktorat vil ha en andrelinje og tredjelinje på lik linje med andre direktorater og etater, men det vil være behov for en separat gjennomgang av faglinjene for å sikre en felles forståelse av avhengigheter og hensiktsmessig arbeidsdeling.

Alternativ 5 innebærer å følge én av styringsmodellene, enten i form av en ID-etat eller et ID-direktorat, og er fremstilt i figuren nedenfor:

a) En styringsmodell der ansatte fra førstelinjen i både politiet (i form av de 78 pass- og ID-kontorene og utlendingsforvaltningen i politidistriktene) og Skatteetaten (i form av de 42 skattekontorene) som arbeider med ID-relaterte oppgaver overføres til «ID-etaten». De ansatte i førstelinjen som arbeider med ID-relaterte oppgaver vil sådan være ansatt i «ID-etaten», mens de resterende ansatte i politidistriktenes førstelinje og skattekontorene vil jobbe med andre henholdsvis politifaglige og skattefaglige oppgaver. Ansatte i politiet og «ID-etaten» i førstelinjen vil være samlokalisert i samme lokaler. Med samlokalisering mener leverandøren at «ID-etaten» kan leie lokaler og teknisk utstyr fra politiet. Eierskap til lokaler og teknisk utstyr kan potensielt endres på lengre sikt. Det understrekes at leverandøren forutsetter at det på mindre tjenestesteder kan inngås lokale avtaler og tilpasninger slik at ansatte i førstelinjen til «ID-etaten» som arbeider med ID-relaterte oppgaver også har mulighet til å arbeide med politifaglige oppgaver dersom kapasitet og saksvolum tilsier det

b) En alternativ styringsmodell der ansatte fra førstelinjen i politiet (i form av de 78 pass- og ID-kontorene og utlendingsforvaltningen i politidistriktene) fortsetter å være ansatt i politiet. Mens ansatte i førstelinjen i Skatteetaten (i form av de 42 skattekontorene) som arbeider med ID-relaterte oppgaver overføres til politiet. De resterende ansatte ved skattekontorene vil jobbe med andre skattefaglige

oppgaver. Førstelinjen vil kun bestå av ansatte i politiet og vil dekke både politifaglige oppgaver og ID-relaterte oppgaver. Førstelinjen vil motta styringssignaler fra både POD og «ID-direktoratet»



Figur 74 Styringsmodeller for ytterpunktene «ID-etat» og «ID-direktorat» underlagt JD med gjenbruk av politiets førstelinje. ID-relaterte oppgaver slik definert i tabell 33-35

Leverandøren har i dette alternativet ikke drøftet om det å gi én statsråd ansvar for ID-forvaltningen og konsolidere ansvar for utvalgte ID-relaterte oppgaver i en ny etat/direktorat påvirke fagmiljøene på departementsnivå, enten mellom departementer eller mellom departement og etat/direktorat. Det må vurderes nærmere og vil avhenge av hvilken statsråd og ny etat/direktorat som får et helhetlig ansvar for ID-forvaltningen.

Det er grunn til å tro at departementene vil vektlegge brukervennlighet, sikkerhet og ressursbruk forskjellig, og det vil være ulike styrker og svakheter avhengig av hvem som blir eierdepartementet for ny etat/direktorat. I det følgende oppsummeres styrker og svakheter ved alternativ 5.

Styrker:

- En felles strategi for ID-forvaltningen legger til rette for mer helhetlig og strategisk styring ved å prioritere og balansere hensyn til brukervennlighet, sikkerhet og ressursbruk. Erfaringsmessig blir sikkerhet vektlagt over de to andre hensyn uten et tilstrekkelig faktagrunnlag

- Det vil være forholdvis enkelt å utarbeide og implementere en felles strategi for ID-forvaltning i Norge basert på eksisterende dokumentasjon og pågående arbeid i KoID, samt leverandørens skisse til mål, jf. kapittel 9
    - Strategien kan potensielt være en døråpner for å etablere utvidede hjemler tilsvarende som i strategien mot arbeidslivskriminalitet beskrevet i kapittel 4.2.4

- Strategien legger til rette for at alle aktører på ulike nivåer har en felles forståelse av hovedutfordringer og hovedmålsettinger i ID-forvaltningen, samt at de

trekker i samme retning. En viktig del av strategiarbeidet er å etablere statistikk over ID-kriminalitet og et bedre kunnskapsgrunnlag om samfunnsmessige kostnader og konsekvenser knyttet feil og misbruk av ID for å øke bevisstheten og ta faktabaserte beslutninger

- En statsråd, et departement og en etat/direktorat får et helhetlig ansvar for ID-forvaltningen i Norge. En ansvarlig statsråd vil kunne løfte viktigheten av en helhetlig ID-forvaltning, og styrker forutsetningene for bedre gjennomføringsevne/-kraft. Felles forståelse av ansvar og roller vil legge til rette for bedre koordinering og samhandling mellom viktige aktører i ID-forvaltningen. Det vil være en mer sentralisert struktur i ID-forvaltningen og sterkere grad av styring enn i alternativ 4 med en ansvarlig statsråd, departement og etat/direktorat som har ID som kjerneoppgave og det kan påvirke ressursbruken positivt

- Ved å sentralisere styring og struktur i ID-forvaltningen er det mulig med en felles førstelinje og et oppmøtested for ID-relaterte oppgaver. Det vil øke brukervennligheten. Det er potensial for samlokalisering, noe som kan bidra til bedre service for brukeren og større innsikt i hverandres fagområder. Det kan gi ressurseffektivisering og synergieffekter for eksempel ved bedre utnyttelse av ID-faglig kompetanse, økt antall ID-kontroller og økende gjenbruk av ID-kontroller

- En etat/direktorat underlagt JD får rollen som premissgiver og sikrer tilstrekkelig kvalitet og sikkerhet ved å etablere enhetlige rutiner, standarder, prosesser og systemer, samt koordinerer innsatsen på tvers av den overordnede ID-prosessen. Det utnytter dagens førstelinjestruktur i politiet samtidig som forutsetningene for økt styring og profesjonalisering av ID-forvaltningen muliggjøres. En sentralisert struktur reduserer antall aktører ved å samle spesialiserte fagmiljøer på de mest kritiske områdene i ID-forvaltningen. Videre vil det distansere og spesialisere forvaltningsoppgaver relatert til ID fra politifaglige oppgaver, samtidig som nærhet til justissektoren opprettholdes

- Det er momentum i ID-forvaltningen nå, som bør utnyttes til å gjøre nødvendige og større grep for å sikre at ID blir prioritert som en kjerneoppgave fremover. Ved å flytte ansvar og oppgaver fra to av de største statlige virksomhetene hva gjelder ansatte, budsjett og oppgaveportefølje noe som, for disse, vil bidra til økt fokus på kjerneoppgaver, mer effektiv drift og prioritering av nødvendige utviklingsaktiviteter

Svakheter:

- Det er usikkert om en felles strategi for ID-forvaltning i Norge alene vil gi effekt knyttet til brukervennlighet, sikkerhet og ressursbruk – og om det vil løse de største utfordringene i dagens ID-forvaltning. Å sikre prioritering av de riktige tiltakene kombinert med ID-forvaltningens gjennomføringsevne vil være avgjørende

- Det er begrenset med systemstøtte for å etablere statistikk over ID-kriminalitet og samfunnsmessige kostnader knyttet feil og misbruk av ID. Berørte aktører har i dag data på mindre enkeltområder f.eks. feil og misbruk av ID-dokumenter, men ikke samfunnsmessige konsekvenser for ID-forvaltningen som helhet. En viktig del av strategiarbeidet kan potensielt utgjøre en del manuelt arbeid som vil kreve ressurser fra de berørte aktørene uten at det vil ha effekt på brukervennlighet, sikkerhet og ressursbruk på kort sikt

- Det er få representanter fra departementene som gir uttrykk for at de ønsker å ta et helhetlig ansvar for ID-forvaltningen i Norge og det kan være en gjennomføringsrisiko. Flere av aktørene i ID-forvaltningen gjennomgår eller har nylig gjennomgått omstillinger eksempelvis «Nye Skatt», nærpolitireformen og etableringen av nytt digitaliseringsdirektorat. Det er uklart hvilke konsekvenser ytterligere endringer vil ha på etatene/direktoratene

- Avhengig av hvilken statsråd som får ansvaret og hvor eierskapet til ny etat/direktorat plasseres kan alternativet medføre et større behov for dialog på tvers av sektorer med koordinering og samordning uten at det går noe fortere eller skaper økt gjennomføringskraft av den grunn – samle alt i en boks løser ikke nødvendigvis utfordringene i ID-forvaltningen. Når ID-relaterte ansvar og oppgaver samles i en ny etat/direktorat vil de i mindre grad være en integrert del av andre sektorers ansvarsområder og saksbehandling og det kan ha konsekvenser for dagens synergieffekter. Det kan øke behovet for koordinering knyttet til andre viktige samfunnsoppdrag

- Leverandøren har ikke tilstrekkelige faktagrunnlag til å kost/nytte-vurdere om å etablere en ny etat/direktorat vil være mer samfunnsøkonomisk lønnsom og gi en mer brukervennlig, sikker og ressurseffektiv ID-forvaltning enn å legge ansvar og oppgaver relatert til ID til en eksisterende etat/direktorat. Videre kan det stilles spørsmål ved om det er samfunnsøkonomisk lønnsomt i lys av tilsvarende rapporter og utredninger

- Felles førstelinje og samlokalisering for ID-relaterte oppgaver uten å gjøre endringer på direktorats/etats/departementsnivå er ikke kost/nytte-vurdert isolert, da leverandøren ikke har hatt tilstrekkelig data til å vurdere det. Derimot ser vi at det er flere prosesser med likhetstrekk mellom tre skrankepunkter hos politiet, Skatteetaten og SVV. Det vil være en krevende styringsmodell med det kan eventuelt arbeides videre med. Leverandøren erfarer at det vil være utfordrende å etablere og styre en felles førstelinje med oppmøtested for ID-relaterte oppgaver uten å endre dagens styring og struktur i ID-forvaltningen: 4 departementer, 4 direktorater, flere lover, forskrifter og ulike sett at instrukser og retningslinjer. Dersom førstelinjen skal samlokaliseres og fungere ressurseffektivt, sikkert og brukervennlig krever det at lokaler, systemer, ledelse, rutiner og retningslinjer er integrert og koordinert

- Uheldig signaleffekt å etablere nytt direktorat parallelt med avbyråkratiserings- og effektiviseringsreform. Det vil være vesentlige omstillingskostnader på kort sikt ved å etablere og flytte ansvar og oppgaver til en ny etat/direktorat, og de er trolig høyere enn ved å legge det til en eksisterende etat/direktorat. Erfaringsmessig vil det uavhengig av det være effektivitetstap hos berørte aktører ved større omstillinger. Det vil ta tid før effekten av en eventuell ny struktur i ID-forvaltningen realiseres

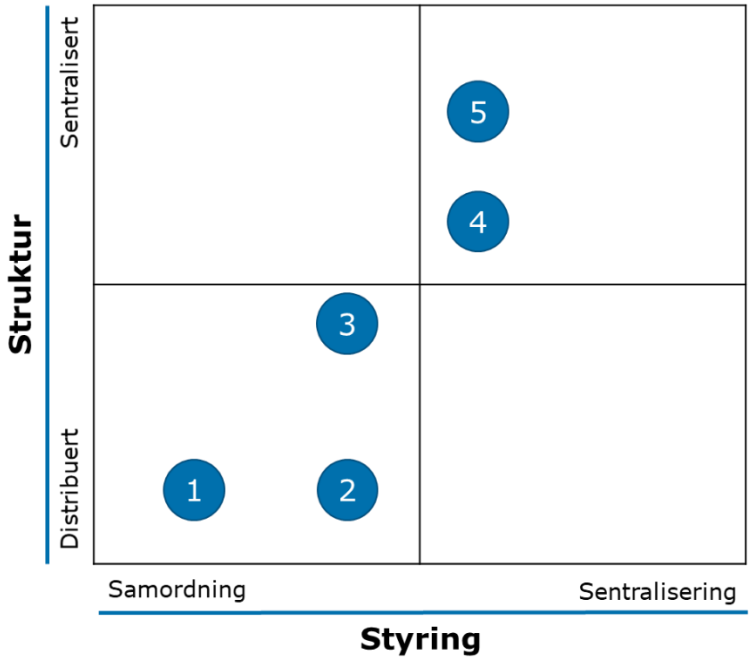
- Aktørene ID-forvaltningen gjennomfører sine oppgaver med ulike formål og det påvirker krav til brukervennlighet, kvalitet, prosesser og sikkerhet. Det vil være et betydelig behov for investeringer for å bygge opp en etat/direktorat som skal ta over ansvar og oppgaver relatert til ID som i dag ligger spredt på flere ulike aktører. Det vil være ulike kulturer, rutiner, retningslinjer, metodikk, rammeverk mv. som skal integreres. Det krever ledelse, styring, infrastruktur, organisasjon og kompetanse som ikke er tilstrekkelig tilstede i dag. Erfaringsmessig vil det være energitap i berørte virksomheter og fare for å miste spesifikk fagkompetanse i slike omstillingsprosesser

- Det er grunn til å tro at JD vil legge stor vekt på sikkerhet og at sikkerhetsnivået vil være styrende, mens KMD i større grad vil vektlegge brukervennlighet. Det kan også være tilfelle at ID-forvaltningen får større frihetsgrader ved å ligge utenfor justissektoren. Hvis dette i større grad oppfattes som et forvaltningsoppgaven fremfor politioppgave, kan det skape større aksept for opptak av biometri, deling av data mv. Utfordringer med implementering av nye pass og nasjonale ID-kort med eID påvirker tilliten til JD. Svak gjennomføringsevne vil være en risiko ved å tillegge JD et helhetlig ansvar for ID-forvaltningen, samt å gjenbruke førstelinjen hos politiet som de siste årene har vært kjent for lange passkøer i sentrale strøk

15.3 Oppsummering av alternativer opp mot sikkerhet, brukervennlighet og ressursbruk

Alternativene som er drøftet i kapittel 15 bygger til en viss grad på hverandre. Sentraliseringen øker langs styring- og strukturdimensjonen fra alternativ 1 til 5, men alternativ 4 og 5 tar ulik retning med hensyn til strukturdimensjonen.

Figuren nedenfor fremstiller alternativene i matrisen presentert i starten av kapittelet med alternativene vurdert etter struktur og styring. Alternativ 1 totalt sett har lavere grad av samordning og desentralisert struktur, mens alternativ 5 har høyere grad av styring og sentralisert struktur.



Figur 75 Overordnet vurdering av alternativ 1-5

Detaljering av administrative og økonomisk konsekvenser

Implementering av et helhetlig ansvar for ID-forvaltningen med sentralisert styring og struktur på departements- og direktorats/etatsnivå vil ha administrative og økonomiske konsekvenser. Spesielt vil alternativ 4 og 5 ved å overføre ansvar og oppgaver til en eksisterende etat/direktorat eller etablere en ny etat/direktorat for ID være ressurskrevende. Alternativene må kost/nytte-vurderes for å sikre at det er samfunnsøkonomisk lønnsomt.

Leverandørens første anslag er 100 mill. kroner i midlertidige omstillingskostnader ved etablering av en ny etat/direktorat for ID, basert på erfaringstall fra tilsvarende prosesser. Dette dekker ikke nye kostnader som følge av alternative tiltak som er drøftet i kapittel 10-14. Leverandørens vurdering er at alternativ 4 og 5 ikke skal kreve økt bemanning tilknyttet ID-forvaltning samlet, selv om enkelte fagmiljø må styrkes ressursmessig som følge av endrede oppgaver og at det stilles høyere krav til sikkerhet og brukervennlighet.

Tabellen under viser leverandørens vurdering av alternativer sett opp mot sikkerhet, brukervennlighet og ressursbruk.

Oppsummering av alternativer basert på pluss-minusmetoden

Under har leverandøren overordnet oppsummert drøftingen med tanke på sikkerhet, brukervennlighet og ressursbruk. Tabellen under oppsummerer drøftingen basert på rammeverket for pluss-minusmetoden beskrevet i kapittel 1.3.

Alternativ 1: *Utarbeide en felles strategi for ID-forvaltning i Norge,* vurderes å ha liten positiv konsekvens på sikkerhet, brukervennlighet og ressursbruk. Strategien vil kunne bidra til å legge til rette for mer helhetlig og strategisk styring ved å prioritere og balansere hensyn til brukervennlighet, sikkerhet og ressursbruk. Det er forøvrig usikkert om alternativet vil ha tilstrekkelig gjennomføringskraft og løse de viktigste utfordringene i dagens ID-forvaltning.

Alternativ 2: *Gi én statsråd ansvar for ID-forvaltning i Norge og utarbeide en felles strategi for ID-forvaltning*, vurderes å ha tilnærmet samme effekt som alternativ 1, det vil si liten positiv konsekvens på sikkerhet, brukervennlighet og ressursbruk. Én ansvarlig statsråd vil potensielt sørge for økt gjennomføringskraft for å løse de viktigste utfordringene i dagens ID-forvaltning.

Alternativ 3*: Gi én statsråd ansvar for ID-forvaltning og utarbeide en felles strategi for ID-forvaltningen, samt tydeliggjøre ansvar og oppgaver relatert til ID i justissektoren.* Alternativet vurderes til å ha middels positiv konsekvens på sikkerhet, brukervennlighet og ressursbruk. Tydeliggjøring av ansvar og oppgaver i justissektoren vil legge til rette for bedre koordinering og samhandling mellom involverte aktører og øke bevissthet rundt samfunnsmessige konsekvenser og ressursbruk relatert til feil og misbruk av ID.

Alternativ 4: *Gi én statsråd ansvar for ID-forvaltning og utarbeide en felles strategi for ID-forvaltningen, samt konsolidere ansvar for ID-relaterte oppgaver, prosesser og systemer i en eksisterende etat/direktorat*. Alternativet vurderes å ha middels positiv effekt på sikkerhet grunnet mer sentralisert styring og struktur, samt felles forståelse av ansvar og roller blant involverte aktører. Videre vurderes alternativet å ha stor positiv konsekvens på både brukervennlighet og ressursbruk, hovedsakelig grunnet bedre utnyttelse av kapasitet og kompetanse i ID-forvaltningen. De varige effektene ved å konsolidere ansvar vurderes som større enn omstillingskostnaden på kort sikt. Leverandøren påpeker at det for dette alternativet overordnet er svært utfordrende å vurdere konsekvenser på sikkerhet, brukervennlighet og ressursbruk uten at det er nærmere utredet hvilke oppgaver, prosesser og systemer som skal flyttes og hvor de skal flyttes.

Alternativ 5: *Gi én statsråd ansvar for ID-forvaltningen og opprette ny etat/direktorat med ansvar for ID*, vurderes å ha tilnærmet samme effekt som alternativ 4, det vil si middels positiv konsekvens på sikkerhet og stor positiv konsekvens på brukervennlighet og ressursbruk. Det vurderes også her at varige effektene vil være en del høyere enn omstillingskostnadene knyttet til å opprette ny etat/direktorat. Leverandøren påpeker at det for dette alternativet overordnet er svært utfordrende å

vurdere konsekvens på sikkerhet, brukervennlighet og ressursbruk uten at det er nærmere utredet hvilke oppgaver, prosesser og systemer som skal flyttes og hvor de skal flyttes.

	Sikkerhet	Brukervennlighet	Ressursbruk
Alternativ 1: Utarbeide en felles strategi for ID-forvaltning i Norge	+	+	+
Alternativ 2: Gi én statsråd ansvar for ID-forvaltning i Norge og utarbeide en felles strategi for ID-forvaltning	+	+	+
Alternativ 3: Gi én statsråd ansvar for ID-forvaltning og utarbeide en felles strategi for ID-forvaltningen, samt tydeliggjøre ansvar og oppgaver relatert til ID i justissektoren	++	++	++
Alternativ 4: Gi én statsråd ansvar for ID-forvaltning og utarbeide en felles strategi for ID-forvaltningen, samt konsolidere ansvar for ID-relaterte oppgaver, prosesser og systemer i en eksisterende etat/direktorat*	(++)	(+++)	(+++)
Alternativ 5: Gi én statsråd ansvar for ID-forvaltningen og opprette ny etat/direktorat med ansvar for ID*	(++)	(+++)	(+++)

Tabell 36 Oppsummering av drøfting for styring og struktur
**) Alternativ 4 og 5 avhenger av hvilke oppgaver, prosesser og systemer som flyttes. Dette vil påvirke endelig vurdering av konsekvenser.*

Del 4: Anbefalinger

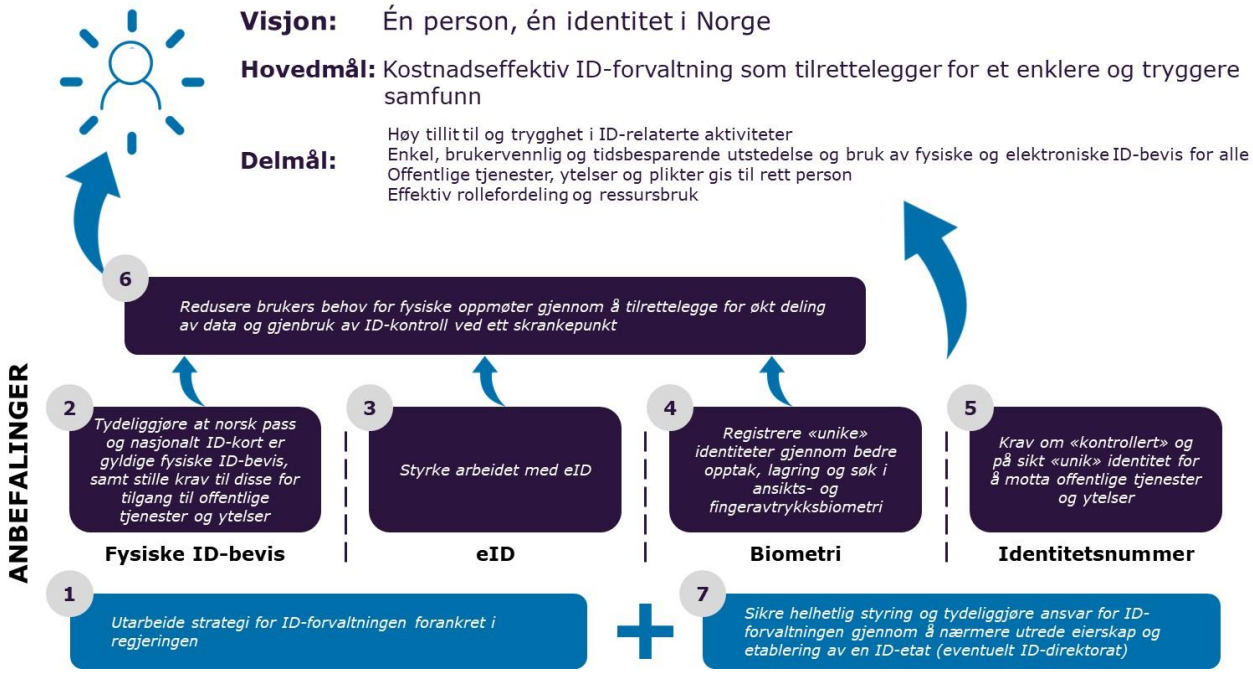
16 Anbefalinger

Leverandørens anbefalinger er gitt med utgangspunkt i områdegjennomgangens mandat, analyser, funn og vurderinger gitt i del 2, samt leverandørens helhetlige vurderinger, skisse til mål og drøftinger av alternativer i del 3. Effekten av de samlede anbefalingene vil være økt brukervennlighet, økt sikkerhet og økt ressurseffektivitet i ID-forvaltningen i et samfunnsmessig perspektiv.

Leverandøren understreker at flere av anbefalingene er avhengig av hverandre, enkelte kan allikevel implementeres separat, men gir høyest effekt om de implementeres samlet.

Videre er anbefalingene utarbeidet med mål om å sette retning. Dette medfører at anbefalingene vil være gjenstand for ytterligere detaljering og konsekvensutredning før de kan implementeres.

Figuren under oppsummerer leverandørens anbefalinger, samt visjon og mål for ID-forvaltningen. Anbefaling 2-5 omhandler nødvendige tiltak innen de fire temaene fysiske ID-bevis, eID, biometri og identitetsnummer, mens anbefaling 6 spesielt adresserer reduksjon i fysiske oppmøter. Anbefaling 2-6 vil bidra til å øke sikkerheten, brukervennligheten og ressurseffektiviteten i ID-forvaltningen, og er sentrale elementer for å kunne oppnå visjon, hovedmål og delmål. Anbefaling 1 og 7 omhandler styring og struktur i ID-forvaltningen og vil være virkemidler for å få gjennomført anbefaling 2-6, samt for å realisere visjon og mål.



Figur 76 Visjon, mål og anbefalinger for ID-forvaltningen

16.1 Hovedanbefalinger

16.1.1 Utarbeide strategi for ID-forvaltningen forankret i regjeringen

Leverandøren anbefaler at én statsråd får et overordnet ansvar for å utarbeide en felles strategi for ID-forvaltningen som forankres i regjeringen. Som del av strategiarbeidet bør det etableres et kunnskapsgrunnlag som omfatter samfunnsmessige kostnader og konsekvenser knyttet til ID-kriminalitet (jf. kapittel 15.2.1).

Berørte departementer utarbeider strategien i felleskap basert på erfaringer fra områdegjennomgangen. Videre anbefaler leverandøren at strategien forankres i regjeringen, da dette bidrar til mer målrettet og samordnet ressursinnsats. Regjeringens strategi mot arbeidslivskriminalitet, nasjonal strategi for digital sikkerhet og regjeringens digitaliseringsstrategi for offentlig sektor er eksempler på hvordan en slik strategi kan utformes og forankres.

Strategi for ID-forvaltningen skal definere langsiktig retning, mål og styringsparametere, samt tiltak for å styrke denne. Leverandørens skisse til mål for ID-forvaltningen, slik beskrevet i kapittel 9 og basert på visjonen for KoID, danner utgangspunktet for strategien:

> *Visjon: Én person, én identitet i Norge*
>
> *Hovedmål: Kostnadseffektiv ID-forvaltning som tilrettelegger for et enklere og tryggere samfunn*
>
> *Delmål:*
> - *Høy tillit til og trygghet i ID-relaterte aktiviteter*
> - *Enkel, brukervennlig og tidsbesparende utstedelse og bruk av fysiske og elektroniske ID-bevis for alle*
> - *Offentlige tjenester, ytelser og plikter gis til rett person*
> - *Effektiv rollefordeling og ressursbruk*

Øvrige anbefalinger 16.1.2 til 16.1.7 bygger på visjon, hovedmål og delmål slik skissert over.

Mål for ID-forvaltningen skal bygge opp under samfunns- og brukereffekter. Et begrenset antall styringsparametere for målene utvikles. Det anbefales videre at måltall for styringsparametere tidfestes, og at det settes konkrete krav om bedret brukervennlighet, sikkerhet og ressurseffektivitet innen 2022 og 2025. Ressursinnsatsen for ID-forvaltningen på tvers av sektorer blir med dette mer målrettet og samordnet. Eksisterende tiltak og planer, anbefalinger fra områdegjennomgangen, samt eventuelle nye tiltak vil samlet være viktige delelementer i strategien.

Strategien skal bidra til å prioritere og balansere ulike hensyn for å realisere en mer brukervennlig, sikker og ressurseffektiv ID-forvaltning. Anbefalingen er viktig for å sikre at ID-forvaltningen behandles mer strategisk og enhetlig, at det legger grunnlag for prioriteringer basert på en ønsket retning, og at ambisjoner for brukervennlighet, sikkerhet og ressurseffektivitet får forankring på tilstrekkelig nivå. Anbefalingen legger til rette for at gjennomføringsevnen i ID-forvaltningen øker.

For ytterligere beskrivelse og vurderinger som er lagt til grunn for anbefalingen se kapittel 9 og 15, samt helhetlige vurderinger av dagens situasjon i kapittel 8.

16.1.2 Tydeliggjøre at norsk pass og nasjonalt ID-kort er gyldige fysiske ID-bevis, samt stille krav til disse for tilgang til offentlige tjenester og ytelser

Leverandøren anbefaler at det tydeliggjøres i regelverket at norsk pass og nasjonalt ID-kort er gyldige fysiske ID-bevis i Norge. Anbefalingen bygger på det pågående arbeidet for utstedelse av nasjonalt ID-kort og medfører at det blir allment kjent hvilke ID-bevis man kan ha tillit til og skal betrakte som gyldige. Dette innebærer at førerkort og bankkort med bilde, samt utenlandske ID-bevis ikke vil være ansett som gyldig legitimasjon annet enn for sine formål. Tilpasningene i regelverket kan gjøres på flere forskjellige måter. Én mulig løsning er at det slås fast i henholdsvis ID-kortloven og passloven at de to ID-bevisene skal anses som gyldige ID-bevis i Norge.

Den samfunnsmessige verdien av nasjonalt ID-kort vil etter leverandørens vurdering være avhengig av en høy utbredelse i befolkningen, også hos utenlandske brukergrupper. I lys av dette anbefaler leverandøren at nasjonalt ID-kort utstedes til norske statsborgere, samt utenlandske borgere med tilknytning til Norge (herunder både EØS-borgere og tredjelandsborgere). Leverandøren anbefaler videre at det stilles krav til alle brukergrupper om fremvisning av enten norsk pass eller nasjonalt ID-kort for tilgang til sentrale tjenester og ytelser der det kreves fysisk legitimasjon. Anbefalingen medfører videre at hver enkelt tjenesteeier ikke gis anledning til å selv definere gyldig legitimasjon for tilgang til tjenester eller opprettelse av ulike rettighetsbevis. Som del av implementeringen bør det finnes løsninger for enkelte utsatte brukergrupper, brukere som har utfordringer med å godtgjøre sin identitet, samt borgere som har tilknytning til Norge men oppholder seg i utlandet. Det er leverandørens oppfatning at kravet ikke strider mot det EØS-rettslige ikke-diskrimineringsprinsippet, da behandlingen vil følge praksis for norske borgere. Det understrekes at anbefalingen ikke innebærer en generell legitimasjonsplikt i Norge.

Kravet om legitimasjon med norsk pass eller nasjonalt ID-kort bør etter leverandørens syn i prinsippet gjelde for tjenester og ytelser som krever fysisk legitimasjon hos SKD, NAV og SVV. Det presiseres at det må foreligge en mer inngående utredelse forut for en endelig beslutning om hvilke tjenester og ytelser med pålagt oppmøte eller fysisk legitimasjon som vil omfattes av legitimasjonskravet. Anbefalingen henger tett sammen med krav om «kontrollerte» og på sikt «unike» identitetsnummer, hvor utstedelse av pass eller nasjonalt ID-kort er viktige virkemiddel. Leverandørens anbefalinger tilknyttet autentisering for tilgang til digitale offentlige tjenester og ytelser er dekket i anbefaling 16.1.3.

Anbefalingen sikrer bedre samsvar mellom krav til kvalitet og/eller sikkerhet for opprettelse av ID-bevis og de tjenester og/eller ytelser ID-beviset gir tilgang til. Anbefalingen vil sikre god utbredelse av pass og det nasjonale ID-kortet.

For ytterligere beskrivelse og vurderinger som er lagt til grunn for anbefalingen se kapittel 10, samt helhetlige vurderinger av dagen situasjon i kapittel 8.

16.1.3 Styrke arbeidet med eID

Gitt allerede påstartet arbeid, anbefales implementering av nasjonal eID tilknyttet det nasjonale ID-kortet som et supplement til eksisterende private eID-er i markedet, men med enkelte tilpasninger. Følgende anbefales nærmere utredet:

1. Det anbefales at vederlagsmodellen endres ved å innføre en transaksjonskostnad som belastes tjenesteeiere ved autentisering til digitale tjenester gjennom nasjonal eID, på lik linje som for private tilbydere av eID

2. ID-kontrollen ved pass- og ID-kontor anbefales gjenbrukt ved utstedelse av norske private eID-er, slik beskrevet i kapittel 16.1.6. Anbefalingen medfører at utstedelsen av norske private eID-er gjøres på samme sikkerhetsgrunnlag som nasjonal eID, inkludert opptak av biometri for alle eID-brukere

3. Leverandøren anbefaler at det ved bruk av norske private eID-er regelmessig blir sendt en spørring til Folkeregisteret for å sjekke om eID-brukeren har status «unik». Frekvensen av en slik spørring må nærmere utredes. En slik elektronisk ID-kontroll vil øke sikkerheten ved bruk av eID, og gjøre det mulig å adgangsbegrense tilgangen til offentlige digitale tjenester dersom brukeren ikke har blitt ID-kontrollert og avgitt biometri eksempelvis de siste ti år

4. Dersom løsningene beskrevet i punkt 2 og 3 over ikke lar seg implementere, anbefaler leverandøren at det bør vurderes om det skal settes krav til nasjonal eID for autentisering til enkelte offentlige digitale tjenester og ytelser

5. Det anbefales at konsekvenser av eIDAS utredes nærmere. Spesielt anbefales utredning av sikkerhetsnivåene tilknyttet norske eID-er opp mot sikkerhetsnivåene som benyttes i eIDAS i kombinasjon med hvilke offentlige tjenester og ytelser dette gir tilgang til. Gitt at anbefalingene over implementeres vil nasjonal eID og alle private eID-er med sikkerhetsnivå 4 i Norge ha biometri som krav for utstedelse og bruk. Det høyeste sikkerhetsnivået i eIDAS, «high», har ikke krav til unike identiteter og vil dermed være mindre sikkert enn sikkerhetsnivå 4 i Norge gitt at anbefalingene i punkt 2 og 3 over gjennomføres.

16.1.4 Registrere «unike» identiteter gjennom bedre opptak, lagring og søk i ansikts- og fingeravtrykksbiometri

For å kunne oppnå visjonen *en person, en identitet i Norge* er det avgjørende at et identitetsnummer kan kontrolleres for «unik». For å kunne gjennomføre denne kontrollen og sikre at en person *låses* til identitetsnummeret kreves det opptak, lagring og søk i minst en av biometriformene. Biometri er et sentralt element for å heve sikkerhet og kvalitet i ID-forvaltningen og kan være med på å øke brukervennligheten. Leverandørens anbefaling støtter opp om det pågående arbeid med knytning av biometri mellom Folkeregisteret, utlendingsregisteret og pass- og ID-kortregisteret og vurdering av de rettslige rammene for lagring av fingeravtrykk i pass- og ID-kortregistrene.

Leverandøren anbefaler at alle personer med tilknytning til Norge skal avlegge biometrisk personinformasjon, dette for å kunne kontrollere at personen er «unik» mot sitt identitetsnummer. For å dekke gapet mellom dagens andel av befolkningen som har avlagt biometri og anbefalingen om at alle norske statsborgere og utenlandske borgere med tilknytning til Norge skal avlegge biometri, anbefales det å stilles krav om pass eller nasjonalt ID-kort for å få tilgang til sentrale tjenester og ytelser der det kreves fysisk legitimering og at biometrien opptas som en del av denne utstedelsesprosessen (jf. kapittel 16.1.2).

Leverandøren anbefaler i tillegg at opptak av biometri utvides til å gjelde både ansiktsfoto og fingeravtrykk og at det tillates lagring av begge biometriformer i biometriregistrene, slik at de blir tilgjengelige for en-til-mange søk. Opptak og søk på

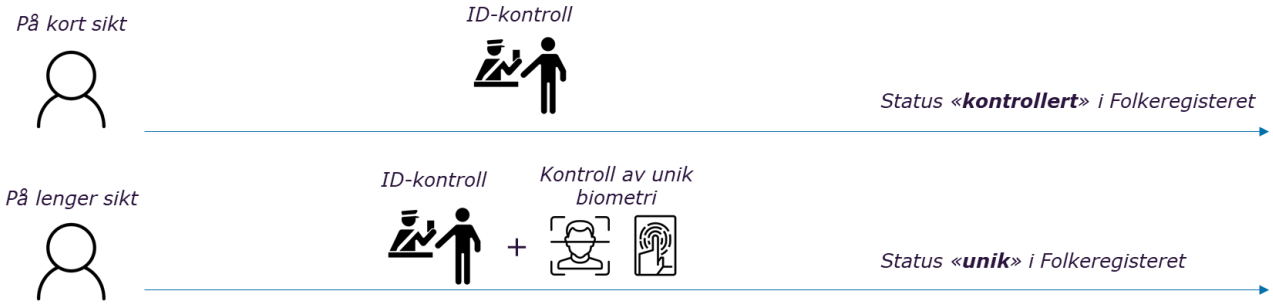
begge biometriformene vil gi større treffsikkerhet, enn søk kun basert på en av biometriformene.

På sikt bør det vurderes hvorvidt bruker selv kan være med å styre hva biometrien kan benyttes til, utover det opprinnelige formålet biometrien ble tatt for. Brukerstyrt deling av biometri kan benyttes til å forenkle identifisering av personen for utvalgte tjenester i det offentlige. Dette kan bidra til å gjøre forvaltningen mer brukervennlig og effektiv.

For ytterligere beskrivelse og vurderinger som er lagt til grunn for anbefalingen se kapittel 13, samt helhetlige vurderinger av dagen situasjon i kapittel 8.

16.1.5 Krav om «kontrollert» og på sikt «unik» identitet for å motta offentlige tjenester og ytelser

Leverandøren anbefaler at det skal ligge en kontrollert identitet til grunn for en større andel av Folkeregisterets identitetsnummer enn i dag. En viktig forutsetning for å oppnå dette er at det stilles krav om gjennomført ID-kontroll av identitetsnummer, som vil gi identitetsnummeret status «kontrollert», for utbetaling av offentlige ytelser eller tilgang på bestemte tjenester. Dette vil være tilsvarende praksisen man i dag har for tilgang på skattekort og vil sikre mer enhetlig behandling av statens inntekter og viktigste kostnader. På lengre sikt anbefaler leverandøren at status «unik» kan erstatte krav om status «kontrollert», men dette vil først kunne innføres når anbefalingen om at norsk pass og nasjonalt ID-kort skal være eneste gyldige fysiske ID-bevis er implementert.



Figur 77 Status «kontrollert» og status «unik» i Folkeregisteret

Leverandøren anbefaler at krav om «kontrollert» identitetsnummer i første omgang skal gjelde alle personer som oppholder seg i Norge.

For personer som befinner seg i utlandet anbefaler leverandøren at det gjøres en strukturert gjennomgang av eksisterende aktive d-nummer for å øke andelen «kontrollert». Gjennomgangen gjøres basert på vesentlighetsbetraktning, der blant annet type tjeneste og/eller ytelsens størrelse inkluderes i vurderingen. Dette gjennomføres av folkeregistermyndigheten i samarbeid med berørte aktører. For etablering av nye identitetsnummer for personer som befinner seg i utlandet utarbeides i tillegg en felles rutine for hva som utgjør om situasjonen er «byrdefull» og derav kvalifiserer for å ikke stille til ID-kontroll. Samarbeidet med utenriksstasjonene og utenlandske myndigheter kan vurderes nærmere.

Leverandøren anbefaler at antall d-nummerrekvirenter reduseres betydelig fra dagens nivå. Videre er det leverandørens anbefaling at den enkelte rekvirent fortsatt skal vurdere begrunnet behov, men at folkeregistermyndigheten som ansvarlig for datakvalitet i Folkeregisteret aktivt må vurdere om mottatt informasjon tilfredsstiller vilkårene i Folkeregisterforskriften eller om rekvisisjonen ikke fyller disse kravene og må avslås.

For ytterligere beskrivelse og vurderinger som er lagt til grunn for anbefalingen se kapittel 12, samt helhetlige vurderinger av dagen situasjon i kapittel 8.

16.1.6 Redusere brukers behov for fysiske oppmøter gjennom å tilrettelegge for økt deling av data og gjenbruk av ID-kontroll ved ett skrankepunkt

Leverandøren anbefaler at det legges til rette for at personopplysninger som opptas med tilhørende ID-kontroll i forbindelse med pass og nasjonale ID-kort kan benyttes ved utstedelse og fornyelse av andre ID-bevis og til andre definerte formål. Et viktig virkemiddel vil være at ID-kontroll og opptak av personopplysninger i større grad gjøres ved ett skrankepunkt.

Det anbefales at det tilrettelegges for økt deling av ansiktsfoto og signatur, noe som vil ha særlig stor innvirkning ved anvendelse for norsk førerkort. SVV gis nødvendig tilgang til ansiktsfoto og signatur som opptas og lagres i forbindelse med utstedelse av norsk pass og nasjonalt ID-kort. Dette vil i praksis muliggjøre at fornyelsen av førerkort i sin helhet kan foregå digitalt, uten behov for oppmøte. Det anbefales videre at det gjennomføres en separat vurdering av hvilke offentlige og private aktører som bør få tilgang til ansiktsfoto og signatur. Gitt øvrige anbefalinger er behovet for bankkort med bilde begrenset, men dersom finansnæringen velger å opprettholde et slikt tilbud gis de også nødvendig tilgang. Nødvendige tilpasninger i regelverk og registre gjennomføres, og det vurderes separat hvilket register delingen av ansiktsfoto og signatur foretas fra. Anbefalingen medfører en reduksjon i fire oppmøter for førerkort og syv oppmøter for bankkort med bilde i et livsløpsperspektiv alt annet likt.

Leverandøren anbefaler videre at det tilrettelegges for at ID-kontrollen som gjennomføres ved et skrankepunkt for utstedelse av pass og nasjonalt ID-kort kan benyttes som grunnlag for å utstede privat eID. Effekten av tiltaket vil være at sikkerheten ved utstedelse av privat eID blir bedre. Samtidig reduseres de samfunnsmessige kostnadene da ressursbruk og brukertid tilknyttet krav om oppmøte i skrankepunkt ved bankfilial eller postkontor/post i butikk fjernes.

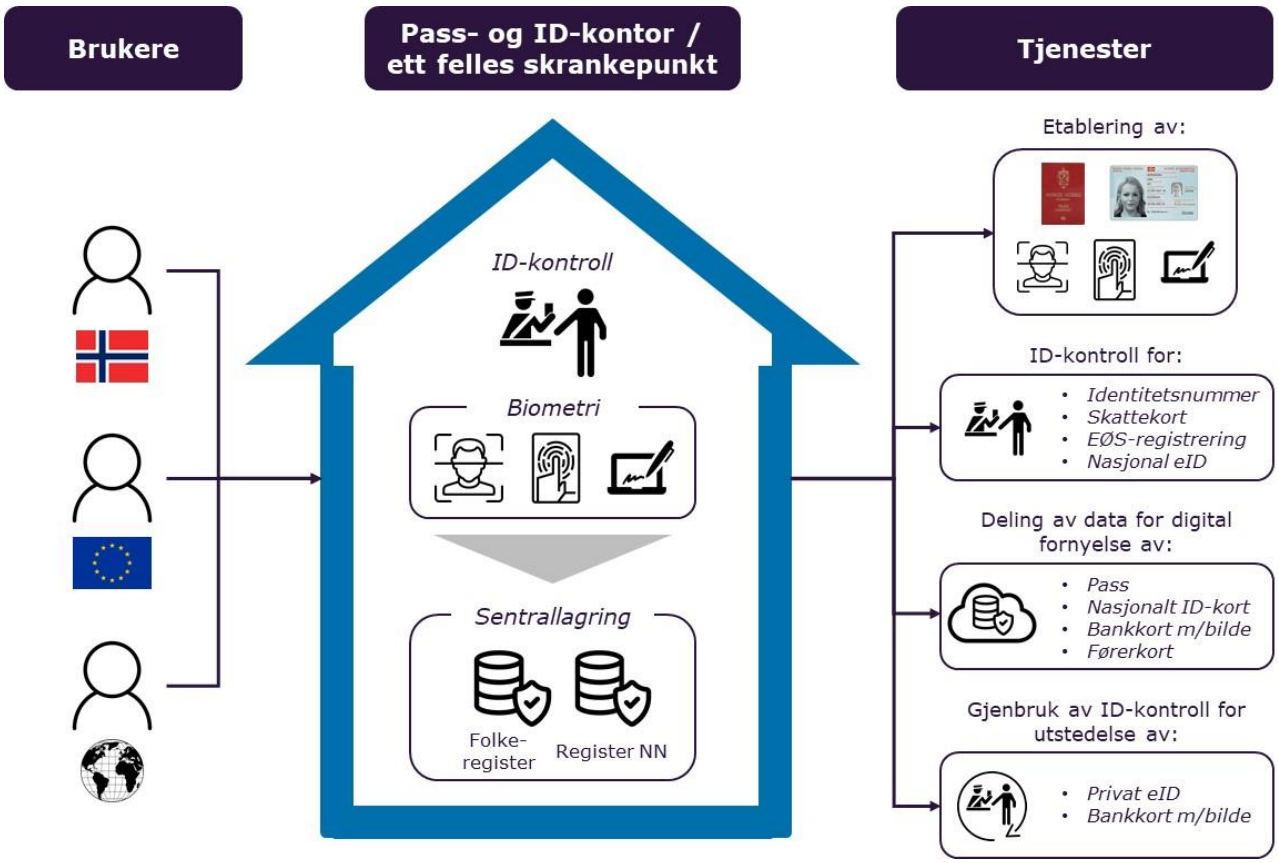
Det er også leverandørens anbefaling at oppmøtekrav som stilles til EØS-borgere i større grad samkjøres ved ett skrankepunkt. Leverandøren anbefaler spesielt at registreringen etter ankomst til Norge, etablering av identitetsnummer, etablering av skattekort, samt tilhørende ID-kontroll gjennomføres med ett oppmøte. Oppmøtet kan gjennomføres ved skrankepunkt på pass- og ID-kontoret. Tilsvarende gjennomføres etablering av oppholdskort og etablering av identitetsnummer med ett oppmøte i samme skrankepunkt for søkere av oppholdstillatelse.

Gjennomføring av teoriprøve og praktisk prøve for førerkort vil fortsatt kreve fysisk oppmøte. Pass eller nasjonalt ID-kort er legitimasjonsgrunnlaget. SVV kan kreve at enkelte søkere av førerkort møter til ekstra ID-kontroll hos pass- og ID-kontoret.

Det planlegges for at gyldighetstiden for nasjonalt ID-kort settes til fem år og nye pass settes til enten fem år eller at dagens gyldighetstid på ti år videreføres. Leverandøren mener at mange av sikkerhetsbehovene i pass og ID-kort potensielt kan ivaretas ved fornyelse uten behov for fysisk oppmøte, spesielt ved at fysisk oppmøte for å oppdatere ansiktsfoto og fingeravtrykk gjennomføres sjeldnere enn hvert femte år. Sentrallagring av fingeravtrykk er en forutsetning og vil i prinsippet muliggjøre digital fornyelse av nasjonalt ID-kort og norsk pass, gitt at brukeren har avgitt biometri de siste ti år. Videre vil det i fremtiden kunne tilrettelegges for at biometriske opplysninger i seg selv vil kunne avgis uten behov for fysisk oppmøte, eksempelvis ved at brukeren selv benytter egen smarttelefon eller tilsvarende for opptak av biometri. Gitt

forutsetningene som er lagt til grunn er det et potensial for å kutte totalt 13 oppmøter tilknyttet fornyelse av norsk pass og nasjonalt ID-kort i et livsløp for norske borgere. Leverandøren anbefaler at det i det videre utredes nærmere i hvilken grad fornyelse av norsk pass og nasjonalt ID-kort kan gjennomføres uten krav til fysisk oppmøte.

Figuren under illustrerer hvordan brukernes behov for fysiske oppmøter kan reduseres.



Figur 78 Forenkling av brukernes interaksjon med ID-forvaltningen

For ytterligere beskrivelse og vurderinger som er lagt til grunn for anbefalingen se kapittel 14 og kapittel 11, samt helhetlige vurderinger av dagen situasjon i kapittel 8.

16.1.7 Sikre helhetlig styring og tydeliggjøre ansvar for ID-forvaltningen gjennom å nærmere utrede eierskap og etablering av en ID-etat (eventuelt ID-direktorat)

Leverandøren anbefaler å gi én statsråd, ett departement og én etat (eventuelt direktorat) et helhetlig ansvar for ID-forvaltningen. ID-forvaltningen er et tverrsektorielt politikk- og saksområde og ansvaret kan ligge i flere departementer hvor vektlegging av sikkerhet, brukervennlighet og ressursbruk vil være ulik. Drøftelsen i kapittel 15.2 viser at ulike forhold har betydning for etatens (eventuelt direktoratets) tilhørighet. Leverandøren har i sin vurdering av ansvarlig departement vektlagt forutsetningene for å sikre en helhetlig styring, relevant oppgaveportefølje, gjennomføringsevne, førstelinje, samt grensesnitt til departementets øvrige politikkområder. Disse hensyn kan hver for seg trekke i retning av ulike departementer.

Leverandøren anbefaler å gi Justis- og innvandringsministeren et helhetlig ansvar for ID-forvaltningen. Tydeliggjøring av ansvaret vil styrke departementets rolle som

strategisk aktør. Ansvaret for ID-forvaltningen kan i utgangspunktet ligge i andre departementer, men en helhetlig styring av underliggende virksomheter, stor andel av total ressursbruk i ID-forvaltningen, nærhet til relevant førstelinje, nærhet til JDs øvrige politikkområder og samfunnsoppdrag er avgjørende.

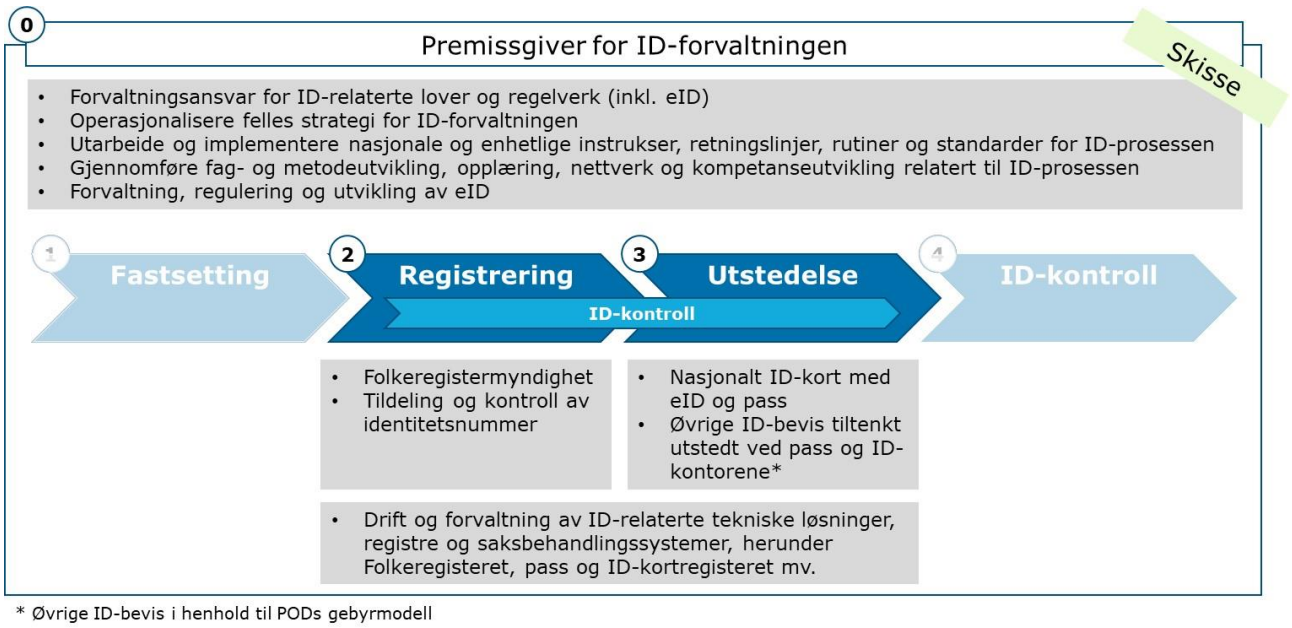
Det formelle forvaltningsansvaret for utvalgte ID-relaterte lover og regelverk legges til JD. JD får et tydelig mandat og konkrete virkemidler til å ta en premissgiver- og samordningsrolle for helheten i ID-forvaltningen, men hvor hvert departement fortsatt er ansvarlig for egen sektors arbeid. Rollen vil være knyttet til operasjonalisering av regjeringens politikk innen ID, samt oppfølging av fastsatte mål og resultatkrav.

For å bedre departementenes forutsetninger for helhetlig styring, og styrke gjennomføringsevnen, anbefaler leverandøren å konsolidere ansvar for utvalgte ID-relaterte oppgaver, prosesser og systemer ved at det samles i en ny etat for ID (eventuelt nytt ID-direktorat). Dette er i tråd med departementenes ambisjoner om å rendyrke og spesialisere oppgaveporteføljene til politiet, Skatteetaten og Digitaliseringsdirektoratet. Videre er det leverandørens forståelse at ingen av departementene i dagens ID-forvaltning vurderer det som hensiktsmessig at deres underliggende virksomheter tar et utvidet ansvar innen ID. Dette begrunnes med at ID ligger utenfor underliggende virksomheters kjerneområder.

Anbefalingen innebærer videre at det utredes å etablere en ny etat som vil være et landsdekkende myndighetsorgan underlagt JD. Myndighetsorganet kan potensielt organiseres som et direktorat avhengig av valgt tilnærming til førstelinje slik nærmere beskrevet under, men vil i denne anbefalingen omtales som en etat. JD vil få etatsstyringsansvar for den nye etaten.

Leverandøren anbefaler at en ny eventuell ID-etat er premissgiver for helheten av ID-forvaltningen og tar en samordningsrolle på tvers for ID-prosessen. Denne rollen har ingen aktør hatt tidligere. For hvert av de fire stegene i ID-prosessen implementeres tydelige felles nasjonale instrukser, retningslinjer, rutiner og standarder for å sikre bedre brukervennlighet, sikkerhet og ressurseffektivitet.

Figuren nedenfor skisserer ansvar for ID-relaterte oppgaver, prosesser og systemer til den eventuelle etaten for ID og innenfor hvilke deler av ID-prosessen dette gjelder. Etaten vil i hovedsak ikke være ansvarlig for oppgaver som relaterer seg til fastsettelse av identitet eller ID-kontroll i etterkant av utstedte ID-bevis.



Figur 79 Skisse med ansvarsområder for den nye etaten for ID

Anbefalingen innebærer å benytte allerede eksisterende infrastruktur i form av politiets førstelinje ved at den nye etaten for ID leier lokaler og teknisk utstyr fra politiet. Anbefalingen innebærer videre at ansatte i politiets førstelinje som arbeider med ID-relaterte oppgaver, samt ansatte som arbeider med ID-relaterte oppgaver på skattekontorene, formelt overføres til den nye etaten og er nærmere detaljert og illustrert i figur 74 i kapittel 15.2.5. På denne måten opprettes det ett felles skrankepunkt for flere ulike ID-relaterte oppgaver. Ny etat vil ha en andrelinje og tredjelinje på lik linje med andre etater, men det vil være behov for en separat gjennomgang av faglinjene for å sikre en felles forståelse av avhengigheter og hensiktsmessig arbeidsdeling.

En beslutning om å gi et departement et helhetlig ansvar og etablere en ny etat er strategisk viktig. Anbefalingen er et viktig virkemiddel for å sikre mer enhetlig styring og profesjonalisering av ID-relatert kompetanse i et spesialisert fagmiljø. Anbefalingen må utredes ytterligere med vekt på kost-/nytte-effekter. Leverandøren anbefaler at dette arbeidet ledes av FIN og gjennomføres i samråd med JD. Parallelt må ansvar og oppgaver relatert til ID tydeliggjøres i justissektoren med mål om forenkling og ressurseffektivisering. Dette er i tillegg nødvendige, forberedende aktiviteter i forkant av en eventuell etablering av et nytt myndighetsorgan.

For ytterligere beskrivelse og vurderinger som er lagt til grunn for anbefalingen se kapittel 15 og spesielt kapittel 15.2.5, samt helhetlige vurderinger av dagen situasjon i kapittel 8.

16.2 Plan for gjennomføring

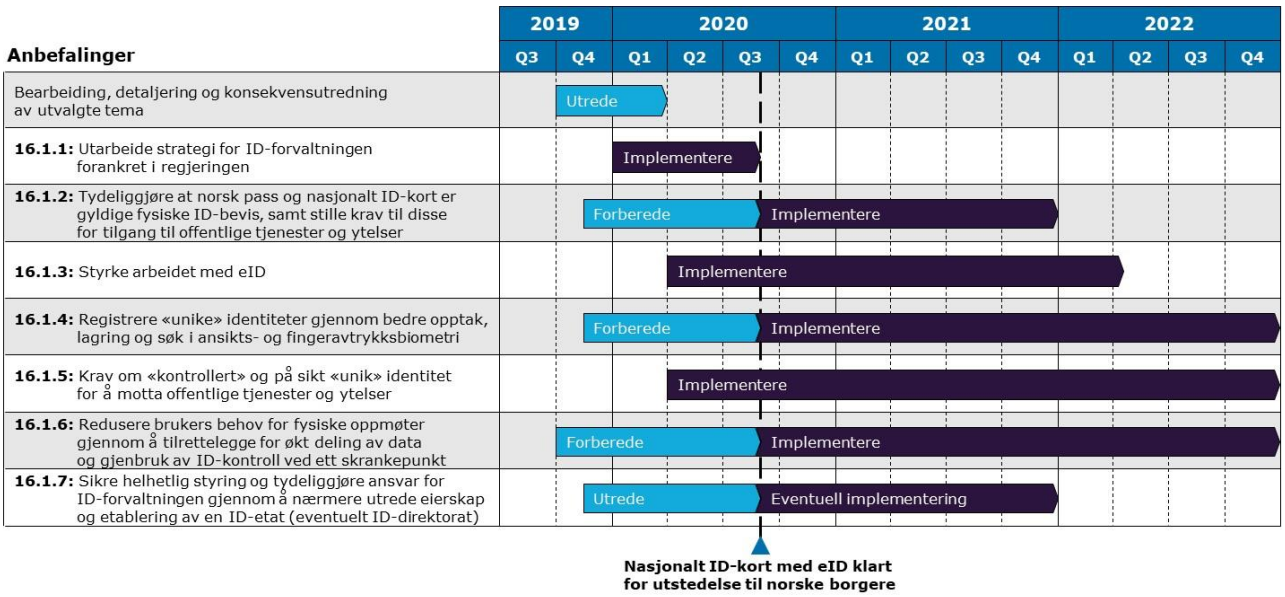
Leverandørens anbefalinger er utarbeidet med mål om å sette retning for ID-forvaltningen. Som følge av områdets omfang, kompleksitet og tid avsatt for områdegjennomgangen er anbefalingene på et nivå hvor det vil være behov for ytterligere detaljering og konsekvensutredning før de kan implementeres.

Leverandørens anbefalinger er delvis avhengige av hverandre, mens enkelte kan implementeres på separat basis. Tabellen under forklarer dette nærmere.

Anbefaling	Avhengigheter til andre anbefalinger
16.1.1: Utarbeide strategi for ID-forvaltningen forankret i regjeringen	Ingen
16.1.2: Tydeliggjøre at norsk pass og nasjonalt ID-kort er gyldige fysiske ID-bevis, samt stille krav til disse for tilgang til offentlige tjenester og ytelser	Delvis avhengig av 16.1.3
16.1.3: Styrke arbeidet med eID	Delvis avhengig av 16.1.2
16.1.4: Registrere «unike» identiteter gjennom bedre opptak, lagring og søk i ansikts- og fingeravtrykksbiometri	Avhengig av 16.1.2
16.1.5: Krav om «kontrollert» og på sikt «unik» identitet for å motta offentlige tjenester og ytelser	For «unik» avhengig av 16.1.2 og 16.1.4
16.1.6: Redusere brukers behov for fysiske oppmøter gjennom å tilrettelegge for økt deling av data og gjenbruk av ID-kontroll ved ett skrankepunkt	For deling av ansiktsfoto og signatur, gjenbruk av ID-kontroll for utstedelse av privat eID ingen avhengigheter. For øvrige delanbefalinger avhengig av 16.1.2, 16.1.3, 16.1.4 og 16.1.5, samt delvis avhengig av 16.1.7
16.1.7: Sikre helhetlig styring og tydeliggjøre ansvar for ID-forvaltningen gjennom å nærmere utrede eierskap og etablering av en ID-etat (eventuelt ID-direktorat)	Ingen

Tabell 37 Avhengigheter mellom anbefalinger

Figuren nedenfor illustrerer en overordnet gjennomføringsplan for leverandørens anbefalinger, med foreslått tidspunkt for forberedelse og implementering av de ulike anbefalingene.



Figur 80 Overordnet gjennomføringsplan for anbefalinger

Leverandøren vurderer endringsbehovet i ID-forvaltningen som stort og anbefaler at momentet som er skapt i forbindelse med områdegjennomgangen utnyttes for å sikre handling. Arbeidet med ytterligere detaljering og konsekvensutredning av utvalgte tema anbefales igangsatt umiddelbart. Strategiutviklingsarbeidet bør også starte opp innen starten av 2020. De øvrige anbefalingene vil i ulik grad være avhengige av arbeidet med ytterligere utredning. Flere av anbefalingene er avhengige av hverandre.

Enkelte kan allikevel implementeres separat selv om det vil gi høyest effekt om de implementeres samlet.

Videre har leverandøren identifisert flere områder som nærmere bør utredes for å bedre sikkerhet, brukervennlighet og ressurseffektivitet i ID-forvaltningen. Listen av potensielle oppfølgingspunkter under er ikke rangert og ble ikke prioritert av leverandøren i områdegjennomgangen. Enkelte av områdene adresserer tema utenfor områdegjennomgangens mandat.

- En tydeliggjøring og formalisering av ansvaret som følger av rollen som tilbyder av masterdata i form av felles krav, spesifikasjoner/standarder og veiledning for å gjøre masterdata tilgjengelig. Dette gjelder forvaltningen i stort
- Gjennomgå praksis for timeføring i staten og vurdere styrket behov for timeføring tilknyttet ulike aktiviteter. Spesielt vurdere styrket bruk av timeføring eller systemstøtte for bedre kartlegging av effektivitet i politiet
- Gjennomgå rutiner, regelverk og praksis for ID-kontroll av fysiske ID-bevis for offentlig sektor (herunder politiet, Tolletaten, helsevesenet, kommunal sektor med videre)
- Besørge at politiet og UDI har nødvendig styringsinformasjon for samlet ressursbruk tilknyttet fastsettelse og registrering av identitet i utlendingsforvaltningen

16.3 Gevinster av anbefalingene

Slik beskrevet i kapittel 8, helhetlige vurderinger av nåsituasjonen, er den reelle og enhetlige dokumentasjonen av dagens sikkerhet, brukervennlighet og ressurseffektivitet begrenset. Leverandøren har derfor ikke knyttet kvantitative effekter til hver enkelt anbefaling, men har gitt en kvalitativ vurdering av hver enkelt anbefaling i tabellen under. Metodikken beskrevet i kapittel 1.3 er benyttet, hvor det i tabellen er sammenlignet mot dagens situasjon inkludert vedtatte planer.

Anbefaling	Effekt sikkerhet	Effekt brukervennlighet	Effekt ressurseffektivitet
16.1.1: Utarbeide strategi for ID-forvaltningen forankret i regjeringen	Forutsetning for realisering av øvrige anbefalinger og effekter tilknyttet hhv. sikkerhet, brukervennlighet og ressurseffektivitet er ikke vurdert.		
16.1.2: Tydeliggjøre at norsk pass og nasjonalt ID-kort er gyldige fysiske ID-bevis, samt stille krav til disse for tilgang til offentlige tjenester og ytelser	++++	0	---
16.1.3: Styrke arbeidet med eID	++	++	+
16.1.4: Registrere «unike» identiteter gjennom bedre opptak, lagring og søk i ansikts- og fingeravtrykksbiometri	+++	0	+
16.1.5: Krav om «kontrollert» og på sikt «unik» identitet for å motta offentlige tjenester og ytelser	+++	--	--
16.1.6: Redusere brukers behov for fysiske oppmøter gjennom å tilrettelegge for økt deling av data og gjenbruk av ID-kontroll ved ett skrankepunkt	-	++++	++++
16.1.7: Sikre helhetlig styring og tydeliggjøre ansvar for ID-forvaltningen gjennom å nærmere utrede eierskap og etablering av en ID-etat (eventuelt ID-direktorat)	Anbefalingen innebærer en nærmere utredning. Denne vil ikke direkte påvirke sikkerhet, brukervennlighet eller ressurseffektivitet. En eventuell implementering av en etat/direktorat for ID vil gi betydelige effekter.		

Tabell 38 Kvantitative vurderinger av anbefalinger

Anbefaling 16.1.2 medfører høy utbredelse av nasjonalt ID-kort. Utbredelse er nøkkelen til den største samfunnsnytten da økt bruk av sterke identitetsbevis vil *sikre den enkeltes vern mot identitetstyveri*, og *bidra til å forebygge og bekjempe annen kriminalitet som involverer falsk eller stjålet identitet*[498]. Videre er høy utbredelse av pass og nasjonalt ID-kort for alle med tilknytning til Norge sentralt i å kunne støtte opp om en høy andel med status «unik» i Folkeregisteret. I tillegg vil anbefalingen redusere bruk og etablering av mindre sikre fysiske ID-bevis. Derav er anbefalingen vurdert til å ha meget stor positiv konsekvens for sikkerheten. Brukerne får mindre valgfrihet enn i dag i valg av fysisk legitimasjon, EØS-borgere og tredjelandsborgere avkreves et nytt ID-bevis, men gir også en større andel av befolkningen tilgang til ett sikkert ID-bevis. Derav er brukervennligheten overordnet vurdert som lik som dagens planer om å utstede nasjonalt ID-kort. Sammenlignet med dagens situasjon har anbefalingen isolert sett en middels negativ konsekvens på brukervennlighet, da nasjonalt ID-kort medfører flere oppmøter. Høy utbredelse av nasjonale ID-kort til flere brukergrupper vil middels negativ konsekvens sammenlignet med foreliggende planer.

Anbefalingen om å styrke arbeidet med eID (16.1.3) medfører nærmere utredning av flere ulike tiltak. Gjenbruk av ID-kontroll foretatt ved pass- og ID-kontor og regelmessig sjekk om identitetsnummer som ligger til grunn for ulike eID er «unike» eller «kontrollerte» vil styrke sikkerheten (middels positiv konsekvens). Gjenbruk av ID-kontroll vil ha middels positiv konsekvens for brukervennligheten da behov for oppmøte hos ulike utstedere av eID reduseres. En endring av vederlagsmodellen for nasjonal eID vil kunne skape økt forutsigbarhet for statens kostnader og vil derav ha en liten positiv konsekvens.

[498] JD, «Prop. 66 L (2014-2015), Lov om nasjonalt identitetskort (ID-kortloven)», 2014-2015

Effektene av anbefaling 16.1.4 er tett tilknyttet effektene av anbefaling 16.1.2 og er avgjørende for å kunne oppnå visjonen *en person, en identitet i Norge*. Opptak, lagring og søk i biometri av ansikts- og fingeravtrykksbiometri for alle brukergrupper vil primært bidra til å styrke sikkerheten (stor positiv konsekvens). Anbefalingen vil videre sikre at det blir vesentlig mer krevende å overta identiteter eller operere med flere identiteter. Anbefalingen vil på sikt kunne bidra til økt brukervennlighet med brukerstyrt deling av biometrisk informasjon. Endret prinsipp for lagring av fingeravtrykksbiometri vil medføre økte kostnader, samtidig burde kostnader tilknyttet manuelle ID-søk i biometriregistrene kunne reduseres. Leverandøren vurderer at en samlet liten positiv konsekvens for ressursbruken.

Anbefaling 16.1.5 bidrar til økt sikkerhet i prosessen med å rekvirere og tildele identitetsnummer og at andelen «kontrollert» og på sikt «unik» øker fra dagens nivå. Videre sikres at kontrollnivået for identitetsnummer tilknyttet inntekter, samt utgifter og tjenester i staten behandles mer enhetlig. Ved krav om «kontrollert» og «unik» styrkes sikkerheten og på sikt kan samfunnsmessige konsekvenser og kostnader som følge av økt sikkerhet reduseres. Grunnet datatilgjengelighet er ikke gevinster av økt sikkerhet beregnet, men leverandøren vurderer at anbefalingen har stor positiv konsekvens. For brukere i utlandet vil anbefalingen kunne medføre redusert brukervennlighet. Dette er riktignok avhengig av hva som klassifiseres som «byrdefullt» og derav kvalifiserer for å ikke stille til ID-kontroll. Omfanget av ID-kontroller, både i Norge og i utlandet, vil øke og medfører noe økt ressursbruk. Både for brukervennlighet og ressurseffektiviteten har leverandøren vurdert at anbefalingen har middels negativ konsekvens.

Anbefaling 16.1.6 vil medføre betydelige besparelser i både brukergebyr og brukertid i et livsløpsperspektiv, som følge av reduserte behov for fysiske oppmøter for bruker. Dette er riktignok sterkt avhengig av valgt gyldighetstid for pass og nasjonale ID-kort, og tilhørende omfang av fysiske oppmøter. Overordnet gir anbefalingen en meget stor positiv konsekvens for brukervennligheten. Saksgangen i ID-forvaltningen forenkles og potensialet for besparelser i ID-aktørenes ressursbruk vil også være betydelig. Dette skyldes i hovedsak at digital fornyelse av ID-bevis er vesentlig mindre ressurskrevende for forvaltningen enn fysiske oppmøter. Anbefalingen har derav også meget stor positiv konsekvens for ressurseffektiviteten.

Påfølgende en nærmere utredning muliggjør anbefaling 16.1.7 forenklinger og ressurseffektivisering ved at ID-relaterte oppgaver og fagmiljøer i større grad samles et sted. Etablering av etaten/direktoratet for ID vil i tillegg sikre at brukerne får ett kontaktpunkt for ID-relaterte aktiviteter og muliggjøre «kun en gang» for ID-relaterte oppgaver. Dette øker brukervennligheten, uten at det går ut over sikkerhet i prosessene. Anbefalingen medfører at ID-området i større grad behandles helhetlig og at en etat/direktorat har ID som sin kjerneoppgave og kan prioritere dette mer kompromissløst enn om det hadde blitt lagt under en eksisterende etat/direktorat med bredere ansvarsområde.

Overordnet estimat økonomiske gevinster for brukere og forvaltning

For å illustrere samlede økonomiske konsekvenser av anbefalingene har leverandøren overordnet estimert økonomiske effekter tilknyttet redusert ressursforbruk for forvaltningen og økonomisk effekt for brukerne, primært tilknyttet spart tidsbruk i oppmøter for norske borgere. Effekter for EØS-borgere og tredjelandsborgere er ikke estimert. Grunnet datatilgjengelighet er ikke økonomiske gevinster av økt sikkerhet beregnet.

For brukere innebærer leverandørens anbefalinger en reduksjon på 25 oppmøter i et livsløp sammenlignet med nåværende planer. Reduksjonen fordeler seg på fire

oppmøter tilknyttet førerkort, åtte oppmøter for bankkort med bilde og 13 oppmøter for pass og nasjonale ID-kort. Leverandøren beregner at reduserte oppmøter vil medføre en årlig besparelse på mellom 450 og 500 mill. kroner i tidsverdi for brukerne, se kapittel 5.1.8 for nærmere detaljering av fremgangsmåte og antagelser.[499]

Fra et forvaltningsperspektiv medfører digital utstedelse av ID-bevis lavere kostnader enn ved fysisk oppmøte. I henhold til SVVs gebyrmodell utgjør digital fornyelse ca. 40 prosent av kostnadene knyttet til utstedelse ved fysisk oppmøte. Leverandøren har antatt tilsvarende besparelse for forvaltningen av pass og nasjonale ID-kort og som vil gi årlige effekter på mellom 130 og 170 mill. kroner. Øvrige effekter er ikke beregnet.

Samlet sett for brukerne og forvaltningen er samlede effekter estimert til å være i størrelsesorden 580 – 670 mill. kroner per år. Leverandøren presiserer at estimatene over er overordnede. Verdi for brukerne, slik presentert over, er kun ment som et høynivå estimat på samlet verdi for brukers tidsbruk. Samtidig er ikke kostnadene ved implementering av anbefalingene inkludert. På samme måte som anbefalingene videre må detaljeres, anbefales det at de samlede samfunnsøkonomiske konsekvensene av anbefalingene detaljeres ytterligere. En fullstendig samfunnsøkonomisk beregning forutsetter at antagelser vurderes nærmere, samt at vurderingen gjøres med et nåverdiperspektiv.

[499] Verdi av spart tid er beregnet iht. FIN, «Rundskriv R-109/14, Prinsipper og krav ved utarbeidelse samfunnsøkonomiske analyser», 2014

17 Vedlegg

Vedlegg 1: Liste over intervjuobjekter

Navn	Tilhørighet
Ann Kristin Roheim	SKD
Anne Berit Stavseth	SD
Anne Bruland	UNE
Anne Karin Storhaug	PU
Anne Ystnes	Finans Norge
Annette Grande Tur	KD
Are Magnus Olsen	PU - Mottakssenteret i Østfold
Arne Isak Tveitan	POD
Arnt Kristiansen	NFD - Brønnøysundregistrene
Asbjørn Enge	Eika
Atle Bransøy	Finans Norge
Benedicte Sørlie	NFD- Brønnøysundregistrene
Berit Lima	Kripos
Brita Cecilie Lilaas-Skari	PU
Cecilie Uteng	KD
Dag Bervar	UDI
Dag Steinsvik	UD - Serviceavdelingen
Darlén Gjølstad	HOD - E-helseavdelingen
Edel Thomassen	Kripos
Eirik Aarre	PU
Eirik William Sandsten	UD
Eldrid Williksen	Kripos
Elisabeth Gjervan	UDI
Elisabeth Sanneland	SVV
Erik Skedsmo	KD - Integreringsavdelingen
Espen Nord Eidene	FIN - Etatssyringsenheten
Espen Ottersen	NAV
Espen Rindedal	SD- Veg-, by- og trafikksikkerhetsavdelingen
Eva Selseng	UNE
Frank Fardal	Difi
Georg Rishaug	POD
Hanne Tannvik Svendsen	POD
Hans Christian Holte	SKD
Harald Røye	SVV
Heidi Frydenberg	Kripos
Heidi Pedersen	Kripos
Heidi Øwre	SVV
Henrik Madsen	UDI
Håkon Skulstad	POD
Håvard Bekk	PU
Ida Hernes	UDI
Ingegerd Widell	Sverige – Skatteverket
Ingrid Melve	KD - Unit
Ingrid Sørlie	SVV
Jakob Dam Glynstrup	Danmark – Nationalt ID-Center
Jan Bjerved	Vipps
Jan Digranes	Finans Norge
Jannicke Valbrek	SKD
Jens Peter Riisage	Danmark - Digitaliseringsstyrelsen
Jiwan Lal Sandhu	NFD - Brønnøysundregistrene
John-Erik Kristiansen	SVV
Jon Berge Holden	Difi
Julie Mein	Finans Norge
Katarina de Brisis	KMD - Seksjon for IT-politikk
Kathrine Qvenhild	UDI
Kenneth Adale Baklund	JD - Innvandringsavdelingen
Kjetil Glad Vangen	NFD - Brønnøysundregistrene
Kjetil Havn	POD

Knut Erik Omholt	FIN - Skattelovavdelingen
Knut Øvregård	NID
Kristin Kvigne	POD
Kyrre Stensnes	FIN - Finansavdelingen
Lars Kviteng	KD
Lars Sverdrup Johansen	SVV
Lauris Linabergs	Latvia - Ministry og Regional Development (VARAM)
Lillian Angel Kvitberg	Eika
Linn Johansen	JD - Politiavdelingen
Lise Nilsen	POD
Liv Toril Berg	UD - Seksjon for utlendingssaker
Live Heltberg	KMD - Avdeling for IT- og forvaltningspolitikk
Mari Hersoug Nedberg	Kripos
Maria Henningsen	HOD - E-helseavdelingen
Marianne Henriksen	SKD
Marianne Sletten	Kripos
Marius Møller	UDI
Marte Vidnes Jensen	NAV
May Snedsbøl	NAV Kontroll Øst
Merethe Rein	JD - Politiavdelingen
Mona Ofigsbø Holsve	HOD
Norunn Breivik	UDI
Norunn Saure	Direktoratet for e-helse
Ole Anders Ulsrud	NorSIS
Ole Johan Heir	NAV Kontroll
Ole Jørgen	PU
Pernille Ødegard	NID
Pål Mathisen	JD - Innvandringsavdelingen
Rita Rix	FIN - Finansavdelingen
Silja Pettersen	Kripos
Steinar Talgø	POD
Stephan Mo	UDI
Synneve Monstad Bottolfs	KD
Synnøve Vebostad	SVV
Tanja Figenschou	SVV
Terese Olstad Bjerke	ASD - Budsjett- og styringsavdelingen
Tone Opdahl	NID
Tor Alvik	Difi
Tove Løfsnes	NFD- Brønnøysundregistrene
Trond Ingebritsen	KD
Trude Åsrum	SKD
Trym Eidsheim	NFD - Næringspolitisk avdeling
Unn Merete Gundersen Zervou	UD - Diplomatseksjonen
Unni Gunnes	JD - Politiavdelingen
Unni Norum	POD
Veslemøy Talgø	UD - Serviceavdelingen
Wenche Bjørngaard	NID
Øystein Leknes	KD

Vedlegg 2: Spørreundersøkelse tilknyttet kvalitet, rutiner og retningslinjer

Vedlegget inneholder tre ulike spørreundersøkelser som ble sendt ut per e-post til relevante aktører i ID-forvaltningen. Vedlegget tar for seg kvalitet, rutiner og retningslinjer i forbindelse med henholdsvis tildeling av fødselsnummer, rekvirering av d-nummer og utstedelse/fornyelse/tap av ID-bevis.

Kvalitet, rutiner og retningslinjer i forbindelse med registering av fødselsnummer

Ønskes tilsendt:
Som en del av kartlegging av nåsituasjonen ønsker vi å få tilsendt rutiner og/eller retningslinjer som benyttes i forbindelse med registreringen av fødselsnummer. Det er ønskelig at dette legges ved når denne eposten besvares med spørsmålene under.

Spørsmål (kan besvares direkte i malen under)

1) Vurder fra 1 (svært lite gode) til 5 (svært gode) hvor gode rutinene/retningslinjene for tildeling av fødselsnummer oppleves å være? Oppgi tallverdi og begrunn ditt svar under

2) Vurder fra 1 (svært lite tilfredsstillende) til 5 (svært tilfredsstillende) i hvilken grad du opplever at rutiner/retningslinjer for tildeling av fødselsnummer er allment kjent og følges blant alle ansatte? Oppgi tallverdi og begrunn ditt svar under

3) Eksisterer det ID-relaterte kompetansekrav for ansatte som er involvert i registreringen av fødselsnummer? (eksempler kan være krav til høyere utdanning, kurs, sertifiseringer, o.l.). Beskriv eventuelle kompetansekrav under

4) Vurder fra 1 (ikke tilstrekkelig) til 5 (tilstrekkelig) i hvilken grad de ID-relaterte kompetansekravene er tilstrekkelige for arbeidet som gjennomføres relatert til registreringsprosessen. Oppgi tallverdi og begrunn ditt svar under

5) Hva er de tre største ID-relaterte feilkildene ved tildeling av fødselsnummer? Legg inn din vurdering under

Hva er det tre viktigste tiltakene din virksomhet kan gjennomføre for å heve kvaliteten/sikkerhetsnivået på registreringsprosessen? Legg inn vurdering under.

Kvalitet, rutiner og retningslinjer i forbindelse med rekvirering av d-nummer

Ønskes tilsendt:
Som en del av kartlegging av nåsituasjonen ønsker vi å få tilsendt rutiner og/eller retningslinjer som benyttes i forbindelse med rekvirering av d-nummer. Det er ønskelig at dette legges ved når denne eposten besvares med spørsmålene under.

Spørsmål (kan besvares direkte i malen under)

1) Vurder fra 1 (svært lite gode) til 5 (svært gode) hvor gode rutinene/retningslinjene for rekvisisjon av d-nummer oppleves å være? Oppgi tallverdi og begrunn ditt svar under

2) Vurder fra 1 (svært lite tilfredsstillende) til 5 (svært tilfredsstillende) i hvilken grad du opplever at rutiner/retningslinjer for rekvisisjon av d-nummer er allment kjent og følges blant alle ansatte? Oppgi tallverdi og begrunn ditt svar under

3) Eksisterer det ID-relaterte kompetansekrav til ansatte som er involvert i rekvisisjon av d-nummer? (eksempler kan være krav til høyere utdanning, kurs, sertifiseringer, o.l.). Beskriv eventuelle kompetansekrav under

4) Vurder fra 1 (ikke tilstrekkelig) til 5 (tilstrekkelig) i hvilken grad de ID-relaterte kompetansekravene er tilstrekkelige for arbeidet som gjennomføres relatert til rekvisisjonen av d-nummer. Oppgi tallverdi og begrunn ditt svar under

5) Hva ligger til grunn for at din virksomhet krever at en søker av d-nummer møter til fysisk kontroll på et skattekontor? Begrunn ditt svar under

6) Hva er de tre største ID-relaterte feilkildene ved rekvisisjonen av d-nummer? Legg inn din vurdering under

7) Hva er det tre viktigste tiltakene din virksomhet kan gjennomføre for å heve kvaliteten/sikkerhetsnivået på rekvisisjonsprosessen? Legg inn vurdering under

Kvalitet, rutiner og retningslinjer i forbindelse med utstedelse/fornyelse/tap av ID-bevis.

Ønskes tilsendt:
Som en del av områdegjennomgangens kartlegging av nåsituasjonen ønsker vi å få tilsendt rutiner og/eller retningslinjer som benyttes i forbindelse utstedelse, fornyelse og tap ved ID-bevis. Det er ønskelig at dette legges ved når denne eposten besvares med spørsmålene under.

Spørsmål tilknyttet utstedelse av ID-bevis: (kan besvares direkte i malen under)

1) Vurder fra 1 (svært lite gode) til 5 (svært gode) hvor gode rutinene/retningslinjene for **utstedelse** av ID-bevis oppleves å være? Oppgi tallverdi og begrunn ditt svar under

2) Vurder fra 1 (svært lite tilfredsstillende) til 5 (svært tilfredsstillende) i hvilken grad du opplever at rutiner/retningslinjer for **utstedelse** av ID-bevis er allment kjent og følges blant alle ansatte? Oppgi tallverdi og begrunn ditt svar under

3) Eksisterer det ID-relaterte kompetansekrav til ansatte som er involvert i **utstedelse** av ID-bevis? (eksempler kan være krav til høyere utdanning, kurs, sertifiseringer, o.l.). Beskriv eventuelle kompetansekrav under

4) Vurder fra 1 (svært lite tilfredsstillende) til 5 (svært tilfredsstillende) ID-kompetansen til de ansatte som er involvert i prosessen for **utstedelse** av ID-bevis. Oppgi tallverdi og begrunn ditt svar under

5) Hva er de tre største ID-relaterte feilkildene ved **utstedelse** av ID-bevis? Legg inn din vurdering under

6) Hva er det tre viktigste tiltakene din virksomhet kan gjennomføre for å heve kvaliteten/sikkerhetsnivået på **utstedelsesprosessen**? Legg inn vurdering under

Spørsmål tilknyttet fornyelse av ID-bevis: (kan besvares direkte i malen under)

1) Vurder fra 1 (svært lite gode) til 5 (svært gode) hvor gode rutinene/retningslinjene for **fornyelsen** av ID-bevis oppleves å være? Oppgi tallverdi og begrunn ditt svar under

2) Vurder fra 1 (svært lite tilfredsstillende) til 5 (svært tilfredsstillende) i hvilken grad du opplever at rutiner/retningslinjer for **fornyelsen** av ID-bevis er allment kjent og følges blant alle ansatte? Oppgi tallverdi og begrunn ditt svar under

3) Hva er det tre viktigste tiltakene din virksomhet kan gjennomføre for å heve kvaliteten/sikkerhetsnivået på **fornyelsesprosessen**? Legg inn vurdering under

Spørsmål tilknyttet tap av ID-bevis: (kan besvares direkte i malen under)

1) Vurder fra 1 (svært lite gode) til 5 (svært gode) hvor gode rutinene/retningslinjene for **tap** av ID-bevis oppleves å være? Oppgi tallverdi og begrunn ditt svar under

2) Vurder fra 1 (svært lite tilfredsstillende) til 5 (svært tilfredsstillende) i hvilken grad du opplever at rutiner/retningslinjer for **tap** av ID-bevis er allment kjent og følges blant alle ansatte? Oppgi tallverdi og begrunn ditt svar under

3) Hva er det tre viktigste tiltakene din virksomhet kan gjennomføre for å heve kvaliteten/sikkerhetsnivået på **tapsprosessen**? Legg inn vurdering under

Hvor mange ID-bevis ble meldt tapt i 2018?

Vedlegg 3: Erfaringer fra utenlandske aktører

Følgende kartlegginger og vurderinger baserer seg på observasjoner av ID-forvaltningen i Sverige, Danmark, Storbritannia og Latvia. Overordnet vektlegges struktur og organisering, sentrale registre, ID-bevis, eID, samt opptak og lagring av biometri. Leverandørens kartlegging og vurdering er basert på tidligere rapporter, analyser og samtaler med ansatte og eksperter innen ID-forvaltning i de respektive landene.

Sverige

Et stort antall aktører er involvert i ID-forvaltningen[500]. Det eksisterer ikke en aktør som har det helhetlige ansvaret for ID-forvaltning. Det er leverandørens vurdering at samarbeidet og informasjonsdelingen mellom de involverte aktørene er begrenset og at Sveriges ID-forvaltning kan beskrives som fragmentert.

Sverige har i likhet med Norge et sentralt folkeregister[501] som er underlagt Skatteverket.[502] Bosatte med oppholdstillatelse i Sverige registreres med fødselsnummer. Personer med midlertidig opphold registreres med et samordningsnummer, som i stor grad tilsvarer d-nummer i Norge. Samtlige aktører henter grunndata fra "Folkbokföringen". Både offentlige og private aktører har tilgang til noe informasjon, eksempelvis migrasjonsverket.

Det nasjonale ID-kortet utstedes av svensk politi, og er ikke obligatorisk for svenske statsborgere.[503] Ifølge Skatteverket finnes det ytterligere fire allmennaksepterte fysiske ID-bevis: i) pass utstedt av politiet, ii) ID-kort for folkeregistrerte[504] utstedt av Skatteverket, iii) svensk førerkort utstedt av Transportstyrelsen[505] og iv) svensk SIS-merket ID-kort og tjenestekort utstedt av store, private og offentlige aktører, eksempelvis banker. Videre kan svensk tjenestekort utstedt av en svensk myndighet, uten SIS-merke i enkelte tilfeller benyttes til identifiseringsformål. I Sverige tilbys det et bredt spekter av fysiske ID-bevis. Det kan ses på som en utfordring for forvaltningen, da det gjør det vanskeliggjør ID-kontroll. En offentlig utredning, fra mars 2019 foreslo innføring av et ID-kort som f.o.m 2022 skal erstatte samtlige fysiske ID bevis, med unntak av pass, som hovedsakelig er et reisebevis. Kortet skal muligens inneholde en statlig eID. Innføring av dette nye ID-kortet begrunnes med at utstedelsen av flere av dagens gyldige, fysiske ID-bevis ikke overholder de pålagte sikkerhetskravene for identitetsdokumenter. Den nye ordningen er videre ment å være kostnadsbesparende samt legge til rette for enklere kontroll av ID. Det er foreslått at politimyndighetene skal tildeles hovedansvaret, da de i dag er ansvarlige for både pass og det nasjonalt ID-kort. Det foreslåtte ID-beviset skal være gyldig i 5 år, og ha samme pris som dagens ID-kort.

Per dags dato er det tre typer eID tilgjengelig for privatpersoner. Sverige opererer med egne tillitsnivåer. Etter eIDAS-forordningen tilsvarer nivå 3 «Betydelig», og nivå 4 tilsvarer «Høy». BankID eies av bankene, og er den dominerende løsningen med 7,9 mill. brukere. Løsningen har tillitsnivå 3. Brukere må ha BankID på mobil dersom de skal bruke Swish, tilsvarende til Vipps. AB Svenska Pass er eID på Skatteverkets ID-kort og har tillitsnivå 4.[506] Freja er en app fra Verisec med tillitsnivå 3.[507] Enhver privat

[500] Nettsider Skatteverket, Myndighet for Digital forvaltning, Migrasjonsverket, Polisen, mv., 2019
[501] Folkbokföring
[502] Skatteverket, «Folkbokföring», u.å.
[503] Statens offentliga utredningar, «Ett säkert statligt ID-kort – med e-legitimation», 2019
[504] ID-kort för folkbokförda
[505] Tilsvarer Vegdirektoratet i Norge
[506] Skatteverket, «E-legitimation på id-kortet», u.å.
[507] E-legitimation, «Skaffa e-legitimation», 2018

aktør i Sverige som oppfyller bestemte kriterier kan tilby eID tjenester, noe som per dags dato gjelder hovedsakelig banker. Svensk forvaltning har dermed delvis frasagt seg eID forvaltningen til private aktører. Følgelig har de stor påvirkning vedrørende utviklingen og utformingen av løsningene. Dette kan være problematisk da de kan prioritere sine egne behov fremst i utviklingen. Den offentlige utredningen nevnt over foreslår at staten skal lansere en statlig eID. Det vil bli tilgjengelig for svenske statsborgere, samt de som er registrerte svenske innbyggere over 13 år. For at svenske innbyggere skal ha tilgang på e-tjenester i andre EU-land påkreves det rapportering på høyeste tillitsnivå i henhold til eIDAS-forordningen. Det er per dags dato usikkert om de private aktørene kan imøtekomme disse påkrevde standarder fra EU. Et annet argument om ny eID er at svenske myndigheter vil at alle skal kunne ha tilgang til eID, selv om de ikke har kundeforhold i banker.[508]

Det finnes ikke et sentralt register som inneholder biometri av svenske statsborgere. Ved registrering av nasjonale ID-kort tas det ansiktsfoto, og ved passregistrering tas det ansiktsfoto og fingeravtrykk. I begge tilfeller slettes det umiddelbart etter opptak. Den offentlige utredningen foreslår lagring av fingeravtrykk og ansiktsfoto på det statlige ID-kortet.[509] For tredjelandsborgere som søker visum tas det fingeravtrykk som lastes opp til Schengens VIS-database. Dersom det søkes om beskyttelse lagres fingeravtrykkene derimot i et nasjonalt register underlagt politiet. Disse slettes etter ti år eller dersom vedkommende blir tildelt statsborgerskap.[510]

Danmark

Ved gjennomgang av dokumentasjon fremstår Danmarks ID-forvaltning som kompleks, uten en aktør med helhetlig ansvar. Nationalt ID-center ble etablert i 2018, basert på det norske modellen, med formål om å styrke sikkerhets- og kontrollarbeidet i utlendingssaker.[511] Grunnet et stort antall involverte aktører, samt mangel på tydelig styring og struktur, vurderer leverandøren landets ID-forvaltning som fragmentert. Det er leverandørens vurdering at Danmarks ID-forvaltning har mange likhetstrekk med Norge.

Danmark har et sentralt folkeregister[512] som styres av CPR-kontoret[513], underlagt Innenriksdepartementet.[514] Bosatte med oppholdstillatelse, skattepliktige og de som har krav på pensjon[515] tildeles et CPR-nummer. Både offentlige og private aktører har tilgang til registeret etter tillatelse fra myndighetene.

Det finnes tre typer fysiske ID bevis som er allmennakseptert: i) førerkort, ii) pass og iii) legitimasjonskort.[516] Det er politiet, underlagt Justisdepartementet, som er ansvarlig for regler for utstedelse av pass, og Færdselsstyrelsen, Trafik-, Bygge- og Boligstyrelsen som er ansvarlig for regler vedrørende førerkort. Likevel har Borgerservice, som er servicesentre i kommunene, myndighet til å behandle søknader, samt utstede samtlige ID-bevis. Legitimasjonskortet kan utstedes til alle danske statsborgere over 15 år, og er ment som en løsning for de som mangler pass og førerkort. Kortet har et begrenset bruksområde i forhold til pass og førerkort.[517]

[508] Statens offentliga utredningar, «Ett säkert statligt ID-kort – med e-legitimation», 2019
[509] Statens offentliga utredningar, «Ett säkert statligt ID-kort – med e-legitimation», 2019
[510] NID, «Biometri og identitet- utfordringer og nye muligheter for utlendingsforvaltningen»,u.å
[511] Nationalt ID-center, «Om Nationalt ID-center", u.å.
[512] Centrale Person Register
[513] Står for det Centrale Person Register kontoret
[514] Det Centrale Personregister, CPR-kontoret, u.å.
[515] Arbejdsmarkedets Tillægspension (ATP)
[516] Borger.dk
[517] Borger.dk, «Legitimationskort», u.å.

Per dags dato er NemID Danmarks eneste eID løsning. NemID gir mulighet til autentisering på både offentlige og private sider. Ordningen har en mobil løsning og en to-faktorløsning med brukernavn, personlig passord og et engangspassord som skrapes fra et fysisk kort. Digitaliseringsstyrelsen, bankene og Nets er ansvarlige for NemID.[518] Løsningen har over 5 mill. brukere, og det utføres rundt 55 mill. transaksjoner månedlig.[11] Ifølge Nordisk råd tilsvarer NemID sikkerhetsnivået «Betydelig» i henhold til eIDAS-forordningen.[519] Fra og med sommeren 2021 vil NemID bli erstattet av MitID, ettersom kontrakten med leverandøren Nets utgår. Digitaliseringsstyrelsen og bankene går sammen om å danne MitID, og det vil bli utviklet en felles prosjektorganisasjon som vil være likt bemannet fra offentlig sektor og bankene.[520]. De vil være felles ansvarlig for utviklingskostnadene, så skal løsningen finansieres etter forbruk. Løsningen vil i likhet med NemID kunne brukes på tvers av privat- og offentlig sektor, men er også tiltenkt å kunne brukes på tvers av Europa.[521] Da kreves det at NemID tilfredsstiller sikkerhetsnivå «Høyt» i henhold til eIDAS-forordningen.

Det finnes ikke sentrallagring av biometri av danske statsborgere. I forbindelse med pass registreres både fingeravtrykk og ansiktsfoto hos politiet, men det lagres ikke i Folkeregisteret. Ved søknad om oppholdstillatelse lagres både fingeravtrykk og ansiktsfoto i utlendingsmyndighetens registre, og kan også brukes av politiet for identifikasjon og ved kontroll av identitet. Dersom en får oppholdstillatelse lagres biometrien i ti år, om ikke lagres det i 20 år. Biometrien blir derimot slettet om statsborgerskap innvilges.[522]

Storbritannia

Slik leverandøren forstår er det ingen aktør som har det helhetlige ansvaret for Storbritannias ID-forvaltning. Landets ID-forvaltning er i stor grad er fragmentert. Det pekes på mange involverte offentlige aktører med delvis overlappende ansvar og begrenset kommunikasjonsflyt.

Storbritannia har ikke et sentralt register tilsvarende det norske Folkeregisteret, og innbyggere har ikke et unikt personnummer. Det fremgår at det kun eksisterer sektorvise registre. Eksempelvis har Department for Work and Pension-Welfare (DWP) et register som benyttes for å administrere velferdsstatens oppgaver, Her Majesty's Revenue and Customs (HMRC) et register for skatteformål og National Health Sector (NHS) et register over helsejournaler. DWP og HMRC bruker et National Insurance Number (NI) som den primære identifikatoren, mens NHS benytter et NHS nummer. DWP og HMRC deler noe informasjon og ansvaret overlapper i enkelte tilfeller, men det er ingen link mellom NHS og CIS/HMKC.[523] Videre vil britiske borgere eksempelvis ikke være registrert hos politiet, med mindre man tidligere har blitt arrestert. Leverandøren vurderer det slik at mangel på et sentralt register bidrar til ytterligere fragmentering av forvaltningen.

Det eksisterer tre allmennaksepterte, fysiske ID bevis. i) pass utstedt av Passkontoret under Innenriksdepartementet[524], ii) førerkort utstedt av The Driver and Vehicle Licensing Agency[525], iii) biometrisk oppholdstillatelse bevis[526] og iv) PASS (Proof of Age

[518] Digitaliseringsstyrelsen, Leverandør af NemiD, u.å.
[519] Nordisk råd, Nordic digital identification (eID), 2016
[520] Digitaliseringsstyrelsen, «MitID», u.å.
[521] Finans Danmark, MitID-kontrakten er underskrevet, 2019
[522] Ny i Danmark, "Biometri- Opbevaring af fingeraftryk og ansigtsfoto», 2019.
[523] The Guardian, "UK should monitor population with "unique person numbers"-thinktank", 2016
[524] Her Majesty's Passport Office, underlagt Home Office
[525] Underlagt Departement for Transport. I Norge utføres denne oppgaven av SVV, underlagt SD
[526] Biometric residence permit

Standards Scheme). Sistnevnte ordning støttes av Innenriksdepartementet[527] og politiet, men utstedes av tre regionale- og fire nasjonale tilbydere. Felles for de ulike kortene er at de har et PASS hologram som bekrefter at det er autentisk og gyldig som ID-bevis.[528] Storbritannia tilbyr ikke lenger et nasjonalt ID-kort. Det ble først implementert som en frivillig løsning i 2008, med et tilhørende register[529]. Registeret var koblet til andre databaser og inneholdt fingeravtrykk, digitalisert ansiktsgjenkjenning, iris-gjenkjenning, samt nåværende og tidligere bosteder for samtlige statsborgere gjennom livet. Grunnet stor bekymring relatert til personvern og sikkerhet av personlig informasjon ble det nasjonale ID-kortet avskaffet i 2010, og registeret ble slettet.[530] Storbritannia har utarbeidet klare retningslinjer for hvordan identitet skal bevises, både i privat og offentlig sektor. Det finnes tre ulike «ruter av ID-kontroll» som kan benyttes når en person skal bevise sin identitet. Rute 1 skal helst benyttes. Om det ikke vedkommende ikke oppfyller visse krav må retningslinjene i rute 2 følges, og om det heller ikke er mulig følges rute 3. Videre er tilgjengelige ID-bevis klassifisert i tre ulike grupper. Gruppe 1 utgjør primære ID-dokumenter, eksempelvis pass og førerkort. Gruppe 2a utgjør pålitelige regjeringsdokumenter, eksempelvis ekteskapsertifikat og bevis på arbeidstillatelse. Gruppe 2b utgjør økonomisk og sosiale historiske dokumenter, eksempelvis lånebevis og strømregning. I retningslinjene til de ulike rutene er det spesifisert hvor mange ID-bevis fra hver gruppe som må fremvises.[531] Overordnende føringer på dette området er fundamentet for en mer helhetlig ID-forvaltning. Et slikt kvalitetssystem mangler hos de fleste land i EU.

Ved gjennomgang av dokumentasjon vurderer leverandøren tilbudet av eID i Storbritannia som utilstrekkelig, sammenlignet med andre land. Det finnes ikke en universell løsning for eID, tilsvarende BankID i Norge, som man kan benytte for autentisering på tvers av offentlige og private aktører. GOV.UK Verify, underlagt The Government Digital Service, er en ordning som muliggjør autentisering og innlogging til en rekke offentlige digitale tjenester. Løsningen baserer seg på syv underleverandører som brukeren kan velge mellom. Underleverandørene sjekker så opplysninger mot valgte registre og gjennomfører autentiseringen.[532] Etter eIDAS standard tilsvarer løsningen «Lavt, Betydelig».[533] Verify-ordningen har ikke blitt implementert i privat sektor enda, men selskaper innen fintech og den private sektoren tilbyr ulike løsninger. Disse har derimot et smalere bruksområde gjerne rettet mot den spesifikke tilbyderen. Det påstås at Storbritannia mangler en nasjonal infrastruktur for digital identitet.[534]

Storbritannia lagrer ansiktsfoto i forbindelse med passøknad til evig tid. Fingeravtrykk lagres ikke, med unntak av for personer som har blitt arrestert eller anholdt mistenkt for lovbrudd.[535] Storbritannia har lang erfaring med bruk og lagring av biometri for tredjelandsborgere. Ansiktsfoto lagres så lenge Innenriksdepartementet mener det er nødvendig, til vedkommende blir en britisk statsborger eller får pass.[536] Det tas opp fingeravtrykk, uavhengig av søknadsgrunnlag som lagres i et eget register som også kan benyttes for å søke mot politiets register. Fingeravtrykkene slettes etter ti år, eller om vedkommende har fått statsborgerskap. Dersom fingeravtrykk er tatt opp med

[527] Home Office
[528] PASS, «What is PASS», u.å.
[529] National Identity Register
[530] GOV.UK, «National identity register destroyed as government consigns ID card scheme to history», u.å.
[531] GOV.UK, «Guidance: ID checking guidelines for standard/enhanced DBS check applications from 3 September 2018», 2018
[532] Government Digital Service, «GOV.UK Verify overview», u.å.
[533] eID User Community, «The United Kingdom», 2019
[534] Oix Open Identity exchange, "Digital Identity in the UK:The cost of doing nothing", 2018
[535] Scottish Government, «Fingerprint Database- IDENT 1", 2014
[536] Home Office, «Biometrics Strategy», 2018

formål om identifisering, slettes de når personens identitet er bestemt.[537] I tillegg benytter immigrasjonsmyndighetene seg av internasjonalt datamateriale gjennom medlemskapet i «FCC - Five Country Conference». Det muliggjør avgrensede søk av biometri mot databaser i Australia, New Zealand, Canada, USA og Storbritannia. Videre jobber innenriksdepartementet (Home Office) for tiden med et omfattende program for å kombinere politiets og innvandringsansvarlig sine databaser, som gir en sentral plattform for fingeravtrykk, DNA og ansiktsinformasjon.[538]

Latvia

I motsetning til andre sammenlignbare land er ID-forvaltningen i Latvia samlet i ett organ. The Office of Citizenship and Migration Affairs (OCMA) er underlagt Innenriksdepartementet og har 32 kontorer for førstelinjetjenester fordelt på Latvias fem regioner. OCMA er ansvarlige for registrering og vedlikehold av Folkeregisteret, fastsetting av juridisk status til enkeltindivider, utstedelse av pass og nasjonale ID-kort, og gjennomførelsen av statlig migrasjon- og asylpolitikk.[539] Leverandøren vurderer Latvias ID-forvaltning som lite fragmentert.

Latvia har et sentralt register[540] som er underlagt OCMA.Både latviske statsborgere og personer med midlertidig opphold blir registrert. Registeret er modernisert og baserer seg på automatiserte løsninger. Det reguleres i henhold til the Population Register Law (PRL) og er tilgjengelig for en stor andel nasjonale informasjonssystemer, eksempelvis Residence Permits Register, National Visa Information System, Work Permits Register, samt andre autoriserte enheter som mottar tilgang fra OCMA.[541]

Latvia har et nasjonalt fysisk ID-kort med eID, som utstedes av OCMA. eID-kortet inneholder blant annet biometrisk data og informasjon i elektronisk format. Annen gyldig legitimasjon er pass, som også utstedes av OCMA. Per dags dato er det obligatorisk å ha enten nasjonalt ID-kort eller pass. I 2023 vil det nasjonale ID-kortet være obligatorisk for alle latviske innbyggere over 15 år. Pass vil da være et alternativt dokument som kun brukes ved innreise til land der det nasjonale ID kortet ikke er godkjent.

Det finnes ulike typer eID tilgjengelig for Latviske innbyggere: i) autentiseringssystemer som ulike institusjoner tilbyr sine kunder. Pålogging skjer som oftest gjennom brukernavn og passord. ii) Autentisering til banksystemer, eksempelvis SmartID som benyttes til å logge på nettbankløsningen til SEB, Luminor og Swedbank. Smart-ID har 750.000 brukere.[542] iii) Mobile ID, en løsning knyttet til SIM kort på mobilen, som kan brukes til å logge på elektroniske tjenester, gjennomføre transaksjoner og signere dokumenter. iv) eID tilknyttet det nasjonale ID-kortet som tillater både autentisering og elektronisk signatur og v) autentisering via e-signatur. Sistnevnte løsning avhenger av et smartkort og det eksisterer tre elektroniske signaturer: virtuell signatur (eParaksts), e-signatur på smart kort og e-signatur på eID.[543]

Latvia har sentrallagring av fingeravtrykk for egne borgere. Folkeregisteret, hvor både statsborgere og personer med midlertidig opphold er registrert, inneholder både fingeravtrykk og ansiktsfoto. Fingeravtrykkene benyttes som sammenligningsgrunnlag

[537] NID, «Biometri og identitet- utfordringer og nye muligheter for utlendingsforvaltningen», u.å.
[538] NID, «Biometri og identitet- utfordringer og nye muligheter for utlendingsforvaltningen», u.å.
[539] Latvijas Republikas Iekšlietu Ministrija, «About OCMA», u.å.
[540] Iedzīvotāju reģistrs
[541] Council of the European Union, "Commission questionnaire on issues related to Registration of Identity" (Working Paper), 2017
[542] The Baltic Times, «Over 2 million people using Smart-ID in Baltic countries", 2019
[543] OECD, «Access to Justice for Business and Inclusive Growth in Latvia", 2018

ved fornying av pass, ID-kort og ved grensekontroll. Av tredjelandsborgere tas det fingeravtrykk som lastes opp til Schengens VIS-database.

Oppsummering

I tabellene på de neste sidene gis et overordnet bilde av hvorvidt ID-forvaltningen er fragmentert, oversikt over fysiske ID-bevis, eID, samt biometri for landene Sverige, Danmark, Storbritannia og Latvia.

Struktur og organisering

Spørsmål	Sverige	Danmark	Storbritannia	Latvia
Er det en aktør som har et helhetlig ansvar for ID forvaltningen?	Nei. Mange aktører involvert og lite informasjonsflyt. Forvaltningen vurderes derfor som fragmentert.	Nei. Organiseringen anses som kompleks med mange involverte aktører uten et bestemt hierarki. Forvaltningen vurderes som fragmentert.	Nei. Mange aktører involvert med delvis overlappende ansvar og begrenset kommunikasjonsflyt. Forvaltningen vurderes som fragmentert.	Ja, Office of Citizenship and Migration Affairs (OCMA) har ansvar for: befolkningsregisteret, utstedelse av pass og nasjonalt ID-kort, juridisk status for enkeltpersoner og gjennomføring av statlig asyl- og migrasjonspolitikk. Forvaltningen vurderes som lite fragmentert.
Eksisterer det et sentralt register, tilsvarende Folkeregisteret?	Ja, "Folkbokföring", underlagt Skatteverket. Offentlige myndigheter og private har tilgang til registeret.	Ja, "det Centrale Person Register", er underlagt Økonomi- og Indenrigsministeriets departement. Både offentlige og private har tilgang til registeret på nærmere vilkår.	Nei, det eksisterer kun sektorvise registre etter befolkningens behov. Det er betydelig politisk motstand mot et sentralt register i Storbritannia grunnet befolkningens bekymring for manglende personvern.	Ja, "Iedzīvotāju reģistrs", underlagt Ministry of Interior. Tilgjengelig for nesten alle nasjonale informasjonssystemer, samt autoriserte enheter som mottar tilgang fra OCMA.

eID og eIDAS

Spørsmål	Sverige	Danmark	Storbritannia	Latvia
Tilgjengelig eID	BankID/Mobilt bankID, AB Svenska Pass og Freja.	BankID/Mobilt bankID, AB Svenska Pass og Freja.	Mangler en universell løsning for eID. GOV.UK Verify er en offentlig løsning, og det finnes løsninger i privat sektor med smalere bruksområde.	Autentiseringssystemer fra ulike institusjoner, til ulike banker- eksempelvis SmartID, Mobile ID, eID tilknyttet det nasjonale ID-kortet og autentisering via e-signatur: virtuell signatur (eParaksts), e-signatur på smart kort og e-signatur på eID. [544]
Sikkerhetsnivå i henhold til eIDAS forordningen	BankID: Betydelig, AB Svenska Pass: Høy og Freja: Betydelig	Betydelig.	Lavt, Betydelig.	
Grad av utbredelse	BankID: Antall brukere: 7,9 mill. (7 mill. med mobilløsning) Må være kunde i en bank som tilbyr det, ulike krav for alder men under 18: verge/forelder) AB Svenska Pass: Koblet til Skatteverkets ID. Freja: Ny, mindre aktør.	NemID er enste aktør. Antall brukere: 5 mill.	GOV.UK Verify har i underkant av 4,5 mill. brukere	

[544] OECD, «Access to Justice for Business and Inclusive Growth in Latvia", 2018

ID-bevis

Spørsmål	Sverige	Danmark	Storbritannia	Latvia
ID-bevis og utsteder	Pass (politiet), nasjonalt ID-kort (politiet), ID-kort for folkeregistrerte (Skatteverket), førerkort (transportstyrelsen) og SIS-merket ID-kort og tjenestekort (offentlige og private aktører til ansatte)	Pass (politiet), legitimasjonskort (kommunen: borgertjenesten) og førerkort (politiet). Samtlige ID kort utstedes av kommunen	Pass (Her Majesty's Passport Office), førerkort (the Driver and Vehicle Licensing Agency) og PASS (Proof of Age Standards Scheme). (Regionale tilbydere: Bracknell Forest Council, Milton Keynes Council og London Borough of Southwark. Nasjonale leverandører: CitizenCard, My ID Card, ONEID4U og ValidateUK.)	Pass (Latvian Office of Citizenship and Migration Affairs) og nasjonalt ID-kort (Latvian Office of Citizenship and Migration Affairs
Nasjonalt ID-kort (obligatorisk / ikke obligatorisk)	Ja, utstedes av politiet. Kortet er ikke obligatorisk.	Nei, mangler politisk og sosial støtte i befolkningen.	Nei. En slik ordning ble innført i 2008, men avskaffet i 2010.	Ja, utstedes av Latvian Office of Citizenship and Migration Affairs. Per dags dato er det obligatorisk å holde enten ID kort eller pass. Fra og med 2023 vil nasjonalt ID-kort vil være obligatorisk for alle innbyggere over 15 år.
Gebyr for bruker	Pass: 350 kroner[545] Nasjonalt ID kort: 400 kroner[50] ID-kort fra Skatteverket: 400[546] kroner Førerkort: 250 kr[547] SIS-merket kort Avhengig av utsteder, men utgjør som vanlig 400 SEK.[548]	Pass: 0-11 år: 115 kroner 12-18 år: 142 kroner 18år-pensionsalder: 627 kroner Pensjonsalder: 377 kroner[549] Legitimasjonskort: 150 kroner[550] Førerkort: 280 kr.[551]	Pass: (søknad online vs. papir) Over 16 år: 75.5 og 85 pund Under 16 år: 49 og 58.5 pund[552] Førerkort: (søknad online vs. papir) Førstegangsutstedelse: 17£ Fornyelse/erstatning: 14£, 17£[553] PASS: 15£[554], uavhengig av utsteder	Pass: 28.46 euro ID-kort: 14.23 euro[555]

[545] Polisen, «Pass och nationellt id-kort», 2019
[546] Skatteverket, «Villkor för att få ansöka om id-kort», 2019
[547] Transportstyrelsen, «Förnya körkortet», u.å.
[548] Statens offentliga utredningar, «Ett säkert statligt ID-kort – med e-legitimation», 2019
[549] Borgerservice, «Bestil nyt pas», u.å.
[550] Københavns Kommune, «Legitimationskort», u.å.
[551] Borgerservice, «Fornyelse af kørekort», u.å.
[552] GOV.UK, "Passport fees", u.å.
[553] GOV.UK, "Driving licence fees", u.å.
[554] Citizencard, «Your ID card", u.å.
[555] Latvia state service portal, «How to obtain a personal identification document, 2019

Spørsmål	Sverige	Danmark	Storbritannia	Latvia
Krav til utstedelse og fornyelse av pass og nasjonalt ID-kort	<u>Pass og nasjonalt ID kort</u> *Krav:* Svensk statsborgerskap og personlig oppmøte. Ytterligere krav om man er under 18 år.[556] *Gyldighetstid:* Alder over 12 år: 5 år Alder under 12 år: ID kort 5 år, pass 3 år.[557] <u>Førerkort:</u> *Krav:* Permanent bosatt i Sverige eller studert her i minst seks mnd., over 18 år.[558] *Gyldighetstid:* 5 eller 10 år, avhengig av førerkorttype[559] <u>ID-kort fra Skatteverket</u> *Krav:* over 13 år og være bokført i Sverige.[560] <u>SIS-merkede kort</u> *Krav:* Hovedregelen er at søker må ha svensk personnummer, men utenlandske statsborgere kan i enkelte tilfeller få et slikt kort. *Gyldighet:* avhenger av utsteder. For utenlandske statsborgere skal gyldighetstiden tilsvare besøkelsestiden. Utgjør bare 1-2 prosent av legitimasjonskort.[561]	<u>Pass</u> *Krav:* Dansk statsborgerskap. Danske statsborgere uten cpr nummer trenger dokumentasjon som beviser sitt danske statsborgerskap. Ved fornyelse kan man søke digitalt.[562] *Gyldighetstid:* Alder over 18 år: 10 år. Alder 2-18: 5 år Alder 0-2 år: 2 år[563] <u>Legitimasjonskort:</u> *Krav:* over 15 år, og ha folkeregistret adresse i Danmark. [564] *Gyldighetstid:* 10 år[48] <u>Førerkort</u> *Krav:* 18 år, nordisk statsborger/oppholdstillatelse *Gyldighetstid:* 15 år. [565] Ved søknad eller fornyelse om legitimasjonskort og førerkort kreves det personlig oppmøte.[566][567]	<u>Pass:</u> *Krav:* Britisk statsborgerskap *Gyldighet:* Alder over 16 år:10 år Alder under 16 år: 5 år <u>Førerkort</u> *Krav:* Britisk statsborgerskap og over 17 år. <u>PASS</u> *Krav:* britisk statsborger[568], alderskrav avhenger av utsteder *Gyldighet:* avhengig av utsteder	<u>Pass</u> *Krav:* Latvisk statsborgerskap *Gyldighet* Under 5 år: 2 år 5-20 år: 5 år Over 20 år: 10 år[569] <u>Nasjonalt ID kort</u> *Krav:* Må være over 15 år og være registrert i Folkeregisteret. *Gyldighet* Ander 5 år: 2 år Alder over 5 år: 5 år [570]

[556] Polisen, Pass och nationellt id-kort
[557] Polisen, «Svar på vanliga frågor om pass, 2019
[558] Transportstyrelsen, «B-Personbil och lätt lastbil», u.å.
[559] Transportstyrelsen, «Förnya körkortet», u.å.
[560] Skatteverket, «Villkor för att få ansöka om id-kort», u.å.
[561] Statens offentliga utredningar, «Ett säkert statligt ID-kort – med e-legitimation», 2019
[562] Gribskov Kommune, «Pas», u.å.
[563] Borger.dk, «Ansøg om eller forny dansk pas»
[564] Københavns Kommune, «Legitimastionskort», u.å.
[565] Borger.dk, «Fornyelse af kørekort», u.å.
[566] Borger.dk, «Legitimationskort», u.å.
[567] København Kommune, «Kørekort», uå.
[568] Citizencard, «Your ID card», u.å.
[569] OCMA, «Citizen`s passport», u.å.
[570] OCMA, «Identity card (EID), u.å.

Biometri

Spørsmål	Sverige	Danmark	Storbritannia	Latvia
Praksis for opptak og lagring	Ansiktsfoto og fingeravtrykk opptas ved pass. Ansiktsfoto opptas ved nasjonalt ID-kort. Biometri slettes umiddelbart etter opptak. *Tredjelandsborgere:* Fingeravtrykk opptas ved søknad om beskyttelse, men ikke i visumsprosessen eller ved søknad om oppholdskort. Ved beskyttelse lagres fingeravtrykk i et nasjonalt register hos politiet. Slettes etter ti år, eller når utlendingen blir svensk statsborger. Fingeravtrykk lagres i Schengens VIS-base, ikke i et nasjonalt register.	Ansiktsfoto og fingeravtrykk opptas ved passutstedelse. Ingen biometri i det sentrale registeret. *Tredjelandsborgere:* Ansiktsfoto og fingeravtrykk lagres i visumsøknader og alle typer oppholdssøknader, i et særskilt EDB-register hos politiet. I visumsøknader slettes biometri etter ti år, og etter 20 år ved søknad om opphold, eller når vedkommende oppnår statsborgerskap	Ansiktsfoto ved søknad om pass lagres til evig tid. *Tredjelandsborgere:* Ansiktsfoto: Ingen tidsfrist for sletting/oppnåelse av statsborgerskap Fingeravtrykk: slettes etter 10 år/oppnåelse av statsborgerskap. Medlem av "Five Country Conference" som muliggjør avgrenset søk mot Australia, Canada, New Zealand og USA. Home office jobber for en sentral plattform for fingeravtrykk, DNA og ansiktsinformasjon.	Sentrallagring av fingeravtrykk for egne borgere. Brukes for sammenligning når det søkes om fornyet pass og ID-kort. Benyttes ansiktsfoto for å verifisere identitet ved ID dokumenter. ID-kontroll med biometri, fingeravtrykk og ansiktsfoto før innrullering i Folkeregisteret. *Tredjelandsborgere:* Fingeravtrykk lagres i Schengens VIS-base.

Spørsmål	Sverige		Danmark		Storbritannia		Latvia	
	Statsborgere	**Tredjelands-borgere**	**Statsborgere**	**Tredjelands-borgere**	**Statsborgere**	**Tredjelands-borgere**	**Statsborgere**	**Tredjelands-borgere**
Opptak av biometri	Ansiktsfoto og fingeravtrykk opptas ved passutstedelse, og ansiktsfoto opptas ved nasjonalt ID-kort utstedelse[571]	Fingeravtrykk og ansiktsfoto opptas[572]	Ansiktsfoto og fingeravtrykk opptas ved passutstedelse[573]	Ansiktsfoto og fingeravtrykk opptas[574]	Ansiktsfoto opptas ved søknad om pass[575]	Ansiktsfoto og fingeravtrykk opptas[576]	Ansiktsfoto og fingeravtrykk opptas ved utstedelse av pass, nasjonalt ID kort og førerkort[577]	Ansiktsfoto og fingeravtrykk opptas ved søknad om oppholdstillatelse[578]

[571] Polisen, «Svar på vanliga fågor om pass», 2019
[572] JD, «Høring om forslag til endringer i utlendingsloven m.m. om opptak og lagring av biometri i utlendingssaker», 15.07.2019
[573] Statens offentliga utredningar, «Ett säkert statligt ID-kort – med e-legitimation», 2019
[574] JD, «Høring om forslag til endringer i utlendingsloven m.m. om opptak og lagring av biometri i utlendingssaker», 15.07.2019
[575] GOV.UK, «Types of passport", 2017
[576] GOV.UK , "Biometric residence permits (BRPs), u.å.
[577] Likumi.lv, «Biometric Data Processing System Law», 2013
[578] Likumi.lv, «Biometric Data Processing System Law», 2013

Spørsmål	Sverige		Danmark		Storbritannia		Latvia	
	Statsborgere	**Tredjelands-borgere**	**Statsborgere**	**Tredjelands-borgere**	**Statsborgere**	**Tredjelands-borgere**	**Statsborgere**	**Tredjelands-borgere**
Lagring av biometri	Slettes umiddelbart etter opptak	Fingeravtrykk lagres kun ved asylsaker i et nasjonalt register hos politiet[579] Fingeravtrykk lastes opp til Schengens VIS-base[580]	Slettes umiddelbart etter opptak	Ansiktsfoto og fingeravtrykk lagres ved visumsøknader og alle typer oppholdssøknader i et særskilt EDB-register hos politiet[581] Fingeravtrykk lastes opp til Schengens VIS-base[582]	Lagres hos Her Majesty Passport Office[583]	Lagres i en nasjonal database[584]	Lagres i et sentralt register[585]	Lagres i et sentralt register[586] Fingeravtrykk lastes opp til Schengens VIS base[587]
Hvor lenge lagres biometrien	*N/A*	Slettes etter ti år, eller når vedkommende oppnår statsborgerskap[588]	*N/A*	Ved søknad om visum: Biometri slettes etter ti år. Ved søknad om opphold: biometri slettes etter 20 år, eller etter 10 år om oppholdstillatelse innvilges. Ved oppnåelse av statsborgerskap slettes biometri umiddelbart [589]	Til evig tid[590]	Ansiktsfoto lagres til evig tid eller ved oppnåelse av statsborgerskap. Fingeravtrykk slettes etter 10 år eller ved oppnåelse av statsborgerskap [591]	På ubestemt tid[592]	På ubestemt tid[593]

[579] NID, «Biometri og identitet», 2013
[580] European Commission, "Visa Information System", u.å.
[581] JD, «Høring om forslag til endringer i utlendingsloven m.m. om opptak og lagring av biometri i utlendingssaker», 15.07.2019
[582] European Commission, "Visa Information System", u.å.
[583] Home office, "Biometrics strategy- Better public services- Maintaining public trust", 2018
[584] the Immigration and Asylum Biometric System (IABS), hentet fra: "Biometrics strategy- Better public services- Maintaining public trust", 2018
[585] Likumi.lv, «Biometric Data Processing System Law», 2013
[586] Likumi.lv, «Biometric Data Processing System Law», 2013
[587] European Commission, "Visa Information System", u.å.
[588] JD, «Høring om forslag til endringer i utlendingsloven m.m. om opptak og lagring av biometri i utlendingssaker», 15.07.2019
[589] JD, «Høring om forslag til endringer i utlendingsloven m.m. om opptak og lagring av biometri i utlendingssaker», 15.07.2019
[590] Immigration and Asylum Biometric System (IABS). Fra: Home Office, "Biometrics Strategy"
[591] NID, «Biometri og identitet», 2013
[592] Likumi.lv, «Biometric Data Processing System Law», 2013
[593] Likumi.lv, «Biometric Data Processing System Law», 2013

Vedlegg 4: Identifiserte ID-bevis i områdegjennomgangen

Vedlegget fremstiller identifiserte ID-bevis i områdegjennomgangen med tilhørende beskrivelse for hvorfor hvert av dem inkluderes eller ikke inkluderes i områdegjennomgangens omfang.

#	ID-bevis	Begrunnelse
1	Norsk pass for voksne	Inkluderes og samles under betegnelsen «Norsk pass»
2	Norsk pass for barn	Inkluderes og samles under betegnelsen «Norsk pass»
3	Norsk nødpass	Inkluderes og samles under betegnelsen «Norsk pass»
4	Norsk provisorisk pass	Utenfor omfang da det ikke lenger er i produksjon
5	Norsk diplomatpass	Inkluderes og samles under betegnelsen «Norsk pass»
6	Norsk tjenestepass	Inkluderes og samles under betegnelsen «Norsk pass»
7	Norsk spesialpass	Inkluderes og samles under betegnelsen «Norsk pass»
8	Nasjonalt ID-kort til norske borgere	Inkluderes og samles under betegnelsen «Nasjonalt ID-kort»
9	Nasjonalt ID-kort med eID	Inkluderes og samles under betegnelsen «Nasjonalt ID-kort»
10	Nasjonalt ID-kort til utenlandske borgere	Inkluderes og samles under betegnelsen «Nasjonalt ID-kort»
11	Utenlandsk nasjonalt ID-kort (ID- kort fra EU/EØS-land)	Utenfor omfang da det ikke utstedes av Norske myndigheter
12	Utenlandsk nasjonalt ID-kort (ID- kort fra EU/EØS-land) med eID	Utenfor omfang da det ikke utstedes av Norske myndigheter
13	Reisebevis for flyktninger	Inkluderes
14	Utlendingspass	Inkluderes og samles under betegnelsen «Utlendingspass»
15	Utlendingspass for enkeltreise	Inkluderes og samles under betegnelsen «Utlendingspass»
16	Utenlandsk pass	Utenfor omfang da det ikke utstedes av Norske myndigheter
17	Utenriksdepartementets ID-kort til diplomater	Vurderes som utenfor omfang grunnet lavt volum
18	Registreringsbevis EØS	Utenfor omfang da det ikke er godkjent som ID-bevis i Norge per d.d.
19	Grenseboerbevis	Utenfor omfang da det ikke er godkjent som ID-bevis i Norge per d.d.

#	ID-bevis	Begrunnelse
20	Norsk førerkort utstedt etter 1.januar 1998	Inkluderes og samles under betegnelsen «Norsk førerkort»
21	Norsk førerkort utstedt før 1. januar 1998	Inkluderes og samles under betegnelsen «Norsk førerkort»
22	Norsk bankkort med bilde	Inkluderes
23	Forsvarets ID-kort	Inkluderes
24	Norsk sjøfartsbok /Sjøfartskort	Inkluderes
25	ID-kort for tolk	Utenfor omfang da det ikke er godkjent som ID-bevis i Norge per d.d.
26	Postens ID-kort*	Utenfor omfang da det ikke lenger er i produksjon
27	HMS kort	Utenfor omfang da det ikke er godkjent som ID-bevis i Norge per d.d.
28	Oppholdskort (Schengen-standardisert)	Er i utgangspunktet ikke et ID-bevis, men vil inkluderes i oversikten etter ønske fra JD da det har mange av fellestrekkene til pass
29	Asylsøkerbevis/Registreringsbevis asylsøkere	Utenfor omfang da det ikke er godkjent som ID-bevis i Norge per d.d.
30	Fødselsattest	Utenfor omfang da det ikke er godkjent som ID-bevis i Norge per d.d.
31	Statsborgerbrev	Utenfor omfang da det ikke er godkjent som ID-bevis i Norge per d.d.
32	MinID	Inkluderes
33	Bank-ID	Inkluderes og samles under betegnelsen "BankID"
34	Bank-ID på mobil	Inkluderes og samles under betegnelsen "BankID"
35	BuyPass ID	Inkluderes
36	Commfides	Vurderes som utenfor omfang grunnet lavt volum (0.01 prosent av transaksjoner i ID-portalen i 2018)
37	FEIDE (Felles Elektronisk IDEntitet)	Vurderes som utenfor omfang da det ikke er utelukkende et ID-bevis, men en tjenesteplattform
38	HelseID	Utenfor omfang da det benytter ID-porten/BankID/Buypass til innlogging

Vedlegg 5: Politiregistre med beskrivelser

Under følger en oversikt over registrene hjemlet i politiregisterforskriften. Med mindre annet er oppgitt er Kripos behandlingsansvarlig. Politiregisterloven er beskrevet i kapittel 4.1.12.

	Register	Beskrivelse
1	Straffesaks-registeret	Opplysninger om mottak av anmeldelser og oppfølging av straffesaker. Registeret skal gi en oversikt over saksgangen for alle straffesaker og danner også grunnlaget for en rekke statistikker.
2	Etterlysnings-registeret	Inneholder opplysninger om personer og gjenstander som etterlyses eller har vært etterlyst nasjonalt i forbindelse med straffeforfølgning eller politiets øvrige oppgaver
3	Reaksjonsregisteret	Opplysninger om ilagt straff og andre tiltak som følge av lovbrudd. Det registreres opplysninger om personalia, reaksjoner og tiltak. Opplysninger fra registeret danner grunnlagt for vandelskontroll etter politiregisterloven kap. 7
4	Personidentitets-registeret	Inneholder personidentitets- og politiopplysninger og skal sikre at politiets behandling av saks-, reaksjons- og identitetsopplysninger er knyttet til rett person eller foretak. Opplysninger fra registeret danner grunnlag for vandelskontroll etter politiregisterloven kap. 7.
5	Politiopplysnings-registeret	Inneholder ulike politiopplysninger. Herunder melding om anmeldelse mot person eller foretak, tiltak som gir den registrerte status som siktet i straffesak, opplysning om personen er etterlyst/pågrepet/ i varetekt.
6	Politioperativt register	Gir politiets operasjonsledelse en fortløpende og døgnkontinuerlig oversikt over hendelser og oppdrag, og brukes for planlegging og gjennomføring av den operative polititjenesten i et politidistrikt.
7	Lydlogg	Automatisert og fortløpende opptak av kommunikasjon på telefon og annet sambandsutstyr ved politiets operasjonssentraler
8	DNA-registeret	DNA-register består av identitetsregister, et etterforskningsregister og et sporregister. Inneholder opplysninger fra DNA-prøver innhentet i tråd med straffeprosessloven 158 og politiregisterloven 12.
9	Arrestjournal	Oversikt over alle personer som er innsatt i politiarrest i henhold til bestemmelsene i straffeprosessloven, utlendingsloven og politiloven.
10	Opptak av lyd og bilde i politiarrest	Formålet med lyd- og bildeopptak i politiets arrest er å ivareta arrestantens liv og helse
11	Fotoregisteret	Inneholder foto som er innhentet i samsvar med straffeprosessloven 160 og bestemmelsene i påtaleinstruksen kap. 11.
12	Fingeravtrykk-registeret	Inneholder fingeravtrykk som er innhentet i samsvar med straffeprosessloven 160 og bestemmelsene i påtaleinstruksen kap. 11.
13	Grense og territorialregisteret	Inneholder opplysninger i forbindelse med politiets grensekontroll
14	Kriminal-etterretnings-registeret	Opplysninger for å forebygge, avdekke og stanse kriminell virksomhet, samt ivareta den enkeltes sikkerhet. Av hensyn til blant annet kriminalitetsbekjempelsen har politiet en omfattende adgang til å gjøre unntak fra innsynsretten i dette registeret, etter en konkret vurdering.
15	Sakneregisteret	Opplysninger om saknede, antatt omkomne, personer og opplysninger om identifiserte lik
16	Informantregisteret	Nasjonal oversikt over politiets informanter
17	Bekymringssamtale-register	Inneholder opplysninger i forbindelse med gjennomføring og oppfølging av politiets bekymringssamtaler med mindreårige og deres foresatte, jf. politiloven 13
18	Hvitvaskings-registeret (ASK)	Registrerer rapportering om mistenkelige transaksjoner. Av hensyn til kriminalitetsbekjempelsen har politiet en omfattende adgang til å gjøre unntak fra innsyn i dette registeret, etter en konkret vurdering. (Økokrim er behandlingsansvarlig
19	Politiets utlendingsregister	I politiets utlendingsregister kan registreres opplysninger som er nødvendig for å oppnå formål som nevnt i § 56-1, knyttet til asylregistrering, identitetsfastsettelse, iverksetting av vedtak (frivillig utreise eller tvangsretur), tvangsmidler og opphold ved utlendingsinternatet (Trandum internat). (Politiets utlendingsenhet er behandlingsansvarlig)

Vedlegg 6: Krav til legitimasjon for tilgang til offentlige tjenester og ytelser

	Legitimasjonskrav	Kilde
Utstedelse av skattekort	***Nordiske borgere (inkludert norske borgere):*** *Pass eller nasjonalt ID-kort, som viser bilde, statsborgerskap og kjønn. Flytter du til Norge fra et annet nordisk land, godtas også gyldig førerkort sammen med utskrift fra Folkeregisteret i landet du flytter fra som viser statsborgerskap og kjønn. Utskriften må være datert og ikke eldre enn 3 måneder. Den må også være underskrevet og stemplet.* *Barn under 18 år kan benytte fødselsattest/fødselsregisterutskrift fra nordisk land sammen med passfoto og utskrift fra hjemlandets folkeregister som viser statsborgerskap og kjønn. Utskriften må ikke være eldre enn tre måneder. Den må også være underskrevet og stemplet.* ***EU/EØS/EFTA borgere:*** *Pass eller nasjonalt ID-kort som viser bilde, statsborgerskap og kjønn.* ***Borgere utenfor EU/EØS/EFTA:*** *Pass.* ***Unntaksgrupper:*** • *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* *Hører du til en av disse gruppene, kan du legitimere deg 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*	Skatteetaten.no, «ID-kontroll», 2019
NAV		NAV.no, «Logg inn», 2019

	Legitimasjonskrav	Kilde
	Innlogging på NAV sin nettside kan gjennomføres gjennom ID-porten bruk av eiD (MinID, BankID, BankID på mobil, BuyPass ID på smartkort, BuyPass ID i mobil og Commfides). For brukere uten eID har NAV alternative påloggingsmetoder som kun gir tilgang til enkelte selvbetjeningsløsninger. Eksempel på alternativ innloggingsmetode: Innlogging ved bruk av engangspassord tilsendt av NAV. Det stilles krav om eID med sikkerhetsnivå 4 for å kunne søke elektronisk om ytelser. NAV oppgir ikke på sine nettsider en oversiktsliste over hvilke ID-bevis som anses som gyldige for ulike brukergrupper.	NAV.no, «Alternativ Innlogging», 05.07.2019
Behandling i primær/spesialisthelsetjeneste	Behandling hos fastlege: Ingen formelle krav til fremvisning av legitimasjon. Pasient må kunne oppgi sitt identifikasjonsnummer enten muntlig eller skriftlig. Behandling i spesialisthelsetjenesten: Ingen formelle krav til legitimasjon.	Informasjon forelagt leverandøren av HOD
Støtte fra lånekassen	Det stilles krav om innlogging på Lånekassen.no for å søke om støtte. Innlogging gjennom ID-porten med eID fra sikkerhetsnivå 3 er tilstrekkelig (MinID, BankID, BankID på mobil, BuyPass ID på smartkort, BuyPass ID i mobil og Commfides). Det opplyses ikke om ytterligere krav til identifikasjon på Lånekassen sine nettsider utover krav om innlogging med eID. Det fremkommer ikke en oversikt over hvilke ID-bevis Lånekassen anser som gyldige.	Lånekassen.no, «Logg inn», 2019

Vedlegg 7: Legitimasjons- og oppmøtekrav for førstegangsutstedelse og fornyelse av ID-bevis

	Norsk pass	
Førstegangsutstedelse		Kilde
Legitimasjonskrav	**For norske borgere:** *Gyldig legitimasjon med fødselsnummer og bilde, som for eksempel **førerkort** (må være utstedt etter 1. januar 1998) eller **bankkort** hvis du ikke har pass fra før eller det er mer enn tre måneder siden passet utløp.* **For EØS/3LB** **:** *Har du tidligere vært utenlandsk statsborger? Da bør du ha med **statsborgervedtaket.*** *Du må ha med **vedtak og dokumentasjon fra UDI** dersom du har blitt norsk statsborger og søker pass for første gang.* **For barn:** *Minst én av de foresatte med foreldreansvar må møte opp sammen med barn under 18 år. I tillegg må du vise legitimasjon for begge foresatte, og ha med en **signert fullmakt** (samtykke).* *Legitimasjonen må ha bilde og signatur, og du må ta med enten selve legitimasjonen (**pass, førerkort utstedt etter 1. januar 1998 eller bankkort**), eller en offentlig bekreftet kopi av slik legitimasjon. Kopien kan ikke være eldre enn 3 måneder.*	*Politiet.no, «Pass og timebestilling», 2019* *Politiet.no, «Pass til barn og ungdom», 2019* *Politiet.no, «Opplysninger i passet, legitimasjon og statsborgerskap», 2019*
Krav til oppmøte	Det stilles krav til oppmøte på passkontor for førstegangsutstedelse av pass	*Politiet.no, «Pass og timebestilling», 2019*
Gyldighetstid	*Pass til personer over 16 år er gyldig i ti år.* *Pass til personer under 16 år er gyldig i en kortere tid:* *0–5 år: Passet er gyldig i to år.* *5–10 år: Passet er gyldig i tre år.* *10–16 år: Passet er gyldig i fem år.*	*Politiet.no, «Pass og timebestilling», 2019*
Fornyelse		
Legitimasjonskrav	*Tilsvarende legitimasjonskrav som ved førstegangsutstedelse*	*Politiet.no, «Pass og timebestilling», 2019*
Krav til oppmøte	Bruker må møte ved passkontor for fornyelse av pass, samt ved tap av pass	*Politiet.no, «Pass og timebestilling», 2019*

	Norsk førerkort	
	Førstegangsutstedelse	Kilde
Legitimasjonskrav	**<u>Gjelder for NB/EØS/3LB:</u>** ***Statens vegvesen godtar følgende legitimasjon:*** • *norsk pass (ikke nødpass)* • *norsk førerkort utstedt etter 1.januar 1998* • *norsk bankkort* • *Forsvarets ID-kort* • *Norsk sjøfartsbok* • *postens ID-kort* • *Norsk reisebevis for flyktninger* • *utlendingspass (ikke godkjent hvis det er utstedt for enkeltreise)* • *utenlandsk pass (ikke nødpass)* • *ID-kort fra EU/EØS-land* *Legitimasjonen må være i original utgave og kan ikke ha utløpt gyldighetsdato. Bekreftet kopi av legitimasjon godtas ikke.* *All norsk legitimasjon skal ha både bilde og fødselsnummer/d-nummer (elleve siffer). Bildet må være tydelig, og det kan ikke være den minste tvil om at du er den samme som på bildet.* *Legitimasjonen vil ikke bli godtatt dersom den er ødelagt, fødselsnummer/d-nummer kun delvis vises eller at bildet av deg er for dårlig. Norsk førerkort utstedt før 1. januar 1998 er ikke godkjent som legitimasjon, uavhengig om det fortsatt er gyldig som førerkort eller ikke.* *Har du utløpt førerkort som er utstedt etter 1. januar 1998, er det likevel gyldig som legitimasjon så lenge det er mindre enn 15 år gammelt. Grunnen er at bildet på førerkortet er gyldig i 15 år.* ***Utenlandsk legitimasjon*** *Nasjonale ID-kort fra EU/EØS-land og utenlandske pass godtas dersom du i tillegg til å vise ID kan opplyse om hele ditt fødselsnummer/d-nummer (elleve siffer), enten muntlig eller skriftlig.*	Vegvesen.no, «Gyldig legitimasjon», 10.08.2018
Krav til oppmøte	For førstegangsutstedelse må bruker møte ved trafikkstasjon, fremvise legitimasjon og gjennomføre oppkjøringsprøve. Ved bestått oppkjøring tas bilde av bruker, og vedkommende kan få førerkortet sendt i posten eller velge å hente det selv på trafikkstasjon.	Vegvesen.no «Oppkjøring», 11.04.2019
Gyldighetstid	*Fra og med 19.januar 2013 er det innført administrativ gyldighet på 15 år på førerkort. Det vil si at førerkortet ditt vil få 15 års gyldighet neste gang det fornyes.* *Ble førerkortet ditt utstedt før denne datoen og er gyldig til hundreårsdagen din, må det fornyes. Fristen for når du må fornye avhenger av hvilken type førerkort du har (grønn bok, stort rosa førerkort eller rosa førerkort i bankkortstørrelse).*	Vegvesen.no «Førerkort utstedt før 19. januar 2013», 07.08.2019 SD, «Førerkortforskriften», §6.1, 19.01.2004

	Norsk førerkort	
	Er førerkortet ditt utstedt før 1. april 1979, må du fornye førerkortet før 1. januar 2020 *Er førerkortet ditt utstedt i perioden 1. april 1979 til og med 31. desember 1997, må du fornye førerkortet før 1. januar 2023* *Er førerkortet ditt utstedt i perioden 1. januar 1998 til og med 18. januar 2013, må du fornye førerkortet før 1. januar 2033* *Er førerkortet ditt utstedt etter 19. januar 2013 kan du se i kolonne 11 på baksiden av førerkortet for fristen på når det må fornyes* *Gyldighetstiden kan være kortere pga.* • *Helsemessige eller andre årsaker* • *Prøveperiode* • *Manglende mørkekjøring* • *Sikkerhetskurs på bane (gjelder tunge klasser)* • *Førerkortbildet er gyldig i inntil 15 år*	
Fornyelse		
Legitimasjonskrav	*Tilsvarende som ved førstegangsutstedelse*	*Vegvesen.no, «Gyldig legitimasjon», 10.08.2018*
Krav til oppmøte	Førerkort kan fornyes digitalt på Vegvesen.no eller ved oppmøte på trafikkstasjon. Fornyelse av bilde på førerkortet må likevel alltid gjennomføres ved fysisk oppmøte på trafikkstasjon.	*Vegvesen.no, «Fornyelse av førerkort», 27.06.2019*

	Bankkort med bilde	
Førstegangsutstedelse		Kilde
Legitimasjonskrav	*Bankens legitimasjonskontroll ved førstegangsutstedelse av Bankkort m/bilde skal skje på grunnlag av fremlagt gyldig norsk pass, gyldig utenlandsk pass eller andre dokumenter som etter en konkret risikobasert vurdering anses som gyldig legitimasjon med samme sikkerhetsnivå som pass.* *Kravet om pass kan fravikes dersom banken er sikker på kundens identitet,* • *og vedkommende etablerte sitt kundeforhold i banken før 1. mars 2007, eller* • *kravet om fremleggelse av pass vil innebære en urimelig merbelastning for vedkommende, grunnet alder, helse eller andre særlige forhold* *Så fremt kravet om pass kan fravikes skal banken i stedet kreve fremlagt annen form for legitimasjon etter de krav til fysiske legitimasjonsdokumenter som følger av hvitvaskingsloven med forskrifter.* *Administrasjonene i Bits gir nærmere veiledning om forståelsen av reglene foran, hva som menes med norsk pass, dokumenter likestilt med norsk pass og utenlandsk pass*	Bits, «Regler om utstedelse av legitimasjonsbevis (Bankkort med bilde)», 15.03.2018

	Bankkort med bilde	
	samt i hvilken grad banken skal kreve tilleggsdokumentasjon for stadfesting av utenlandske personers identitet, oppholdstillatelse i Norge og bosted. Det kan også gis anbefalinger om praktisering av kontrollreglene.	
Krav til oppmøte	*Ved utstedelse av Bankkort m/bilde skal banken forvisse seg om sertifikatholders identitet. Kontroll av sertifikatholders identitet skal skje ved personlig fremmøte hos banken eller en representant for banken, med mindre sertifikatholder allerede er identifisert ved personlig fremmøte ved etablering av kundeforholdet.*	Bits, «Regler om utstedelse av legitimasjonsbevis (Bankkort med bilde)», 15.03.2018
Gyldighetstid	*Hvor lenge et ordinært Bankkort skal være gyldig (utløpstidspunkt) fastsettes av banken, men kan maksimalt være åtte år. For kombinerte kort skal utløpstidspunktet være den samme som utløpstidspunktet for det tilknyttede betalingskortet.* *Et Bankkort skal ikke ha bilde som er eldre enn 10 år*	Bits, «Regler om utstedelse av legitimasjonsbevis (Bankkort med bilde)», 15.03.2018
Fornyelse		
Legitimasjonskrav	*Det er ikke nødvendig med ny fremleggelse av pass ved utstedelse av Bankkort med bilde dersom pass ble fremlagt ved personlig fremmøte i forbindelse med etablering av kundeforholdet.*	Bits, «Regler om utstedelse av legitimasjonsbevis (Bankkort med bilde)», 15.03.2018
Krav til oppmøte	Det stilles ikke oppmøtekrav til fornyelse utover krav til fornyelse av bilde.	Bits, «Regler om utstedelse av legitimasjonsbevis (Bankkort med bilde)», 15.03.2018

	Norsk sjøfartskort	
Førstegangsutstedelse		Kilde
Legitimasjonskrav	*Norsk pass. Legitimasjonskravene er de samme ved søknad fra Norge som i utlandet.*	Sdir.no, «Sjøfartsbok», 27.11.2015
Krav til oppmøte	*Sjøfartsboka hentes ved personlig fremmøte, og pass må fremvises for identifikasjon (gjelder både søknad fra Norge og fra utlandet)*	Sdir.no, «Sjøfartsbok», 27.11.2015
Gyldighetstid	*Sjøfartsboken er gyldig i fem år fra utstedelsesdato*	Sdir.no, «Sjøfartsbok», 27.11.2015
Fornyelse		
Legitimasjonskrav	Leverandøren legger til grunn at legitimasjonskravene for fornyelse er tilsvarende kravene ved førstegangsutstedelse	
Krav til oppmøte	Leverandøren legger til grunn at oppmøtekrav for fornyelse er tilsvarende kravene ved førstegangsutstedelse	

	MinID	
Førstegangsutstedelse		Kilde
Legitimasjonskrav	*For å registrere deg som en MinID bruker trenger du følgende:* *1) Fødselsnummer eller d-nummer* *2) Mobiltelefon eller e-postadresse* *3) PIN-kodebrev* *Mangler du PIN-kodebrevet, kan du bestille nye PIN-koder. PIN-kodene sendes kun til den adressen du har registrert i det norske folkeregister.*	Eid.difi.no, «Hva trenger jeg for å registrere en MinID bruker», u.å
Krav til oppmøte	Ingen kontroll	Informasjon forelagt leverandøren av Difi
Gyldighetstid	Ingen krav til fornyelse	Informasjon forelagt leverandøren av Difi
Fornyelse		
Legitimasjonskrav	Ingen krav til fornyelse	Informasjon forelagt leverandøren av Difi
Krav til oppmøte	Ingen krav til fornyelse	Informasjon forelagt leverandøren av Difi

	BuyPass ID	
Førstegangsutstedelse		Kilde
Legitimasjonskrav	*Ved etablering kreves at du møter opp personlig og at du viser gyldig legitimasjon. Du må akseptere at det tas fotokopi av legitimasjonsdokumentet. Dette gjøres ved utlevering hos Posten, hos et av våre brukersteder eller hos Buypass.* *Posten stiller følgende krav til legitimasjon:* • *Postens ID-kort (Produseres ikke etter 1.4.2010)* • *Norsk bankkort med legitimasjonsdel (bilde m.m.)* • *Norsk førerkort utstedt fra og med 01.01.1998* • *Norsk pass* • *Norsk utlendingspass og reisebevis* • *Utenlandske pass* • *Europeiske identitetskort (Identity Card)** • *Nordisk førerkort*** ** Dette er nasjonale ID-kort som en del europeiske land har. De er gyldig legitimasjon i EU og Schengen-landene (blant annet Norge).* *** Kun godkjent for banktjenester. Ikke PUM (Personlig utlevering med mottakingsbevis) eller andre posttjenester.*	BuyPass.no, «Kundeavtale», 04.12.2018 Posten.no, «Legitimasjon og fullmakter», u.å
Krav til oppmøte	Personlig oppmøte hos posten eller et av BuyPass sine brukersteder	BuyPass.no, «Kundeavtale», 04.12.2018
Gyldighetstid	Kortet er gyldig i 3 år	BuyPass.no «Produkter», u.å

	BuyPass ID	
Fornyelse		
Legitimasjonskrav	BuyPass ID kan fornyes ved bruk av eksisterende eID dersom den ikke allerede er utløpt	Informasjon forelagt leverandøren fra BuyPass
Krav til oppmøte	BuyPass ID kan fornyes ved bruk av eksisterende eID dersom den ikke allerede er utløpt	Informasjon forelagt leverandøren fra BuyPass

	Oppholdskort	
Førstegangsutstedelse		Kilde
Legitimasjonskrav	*Etter utf. § 10-2 annet ledd skal utlendinger som søker oppholdstillatelse i Norge, jf. utl. § 56, dokumentere sin identitet, fortrinnsvis ved å legge fram pass eller annet legitimasjonsdokument utstedt av offentlig myndighet. For utlendinger som søker beskyttelse følger det av utl. § 93 første ledd at dersom vedkommende er i besittelse av pass eller annet reisedokument, skal dette innleveres sammen med søknaden. For å kunne få oppholdstillatelse på grunn av sterke menneskelige hensyn eller særlig tilknytning til riket, jf. utl. § 38, følger det av utf. § 8-12 første ledd at det som hovedregel er et vilkår at utlendingen fremskaffer dokumentasjon for sin identitet. Disse bestemmelsene omhandler det formelle kravet til å fremlegge dokumentasjon på identitet ved søknad om opphold og beskyttelse. I tillegg vil kravet om framlagt dokumentasjon også ha betydning for om kravet til avklart identitet er oppfylt, Som hovedregel må søker ha sannsynliggjort sin identitet for å få oppholdstillatelse, og fremlagt dokumentasjon på identitet vil som oftest være et tungtveiende moment i den konkrete helhetsvurderingen av om søkers identitet er sannsynliggjort.*	UDI, «Registrering, vurdering og endring av identitetsopplysninger i saker etter utlendingsngsloven», 24.04.2012 (sist endret 04.06.2019)
Krav til oppmøte	Bruker må møte opp på et politikontor for å søke om oppholdskort. Oppholdskortet sendes deretter til brukers oppgitte adresse	UDI, «Slik skaffer du deg et oppholdskort», u.å
Gyldighetstid	*Kortet er gyldig like lenge som innehaverens oppholdstillatelse. Hvis vedkommende har permanent oppholdstillatelse er kortet gyldig i to år. Ved varig oppholdsrett er kortet gyldig i ti år.*	UDI, «Oppholdskort», u.å
Fornyelse		
Legitimasjonskrav	UDI sine nettsider opplyser at pass må medbringes ved fornyelse av oppholdskort.	UDI, «Slik bestiller du nytt oppholdskort», u.å
Krav til oppmøte	Bruker må møte opp på et politikontor for å søke om oppholdskort. Oppholdskortet sendes deretter til brukers oppgitte adresse	UDI, «Bestille nytt opphodskort», u.å

	Reisebevis for flyktninger	
Førstegangsutstedelse		Kilde

	Reisebevis for flyktninger	
Legitimasjonskrav	*Det tas ikke stilling til utlendingens identitet på nytt ved utstedelsen av reisebevis med mindre det foreligger nye ID-opplysninger, men bygger på den vurderingen av identitet utlendingsmyndighetene gjorde når det ble gitt førstegangstillatelse.* *Pass eller annet reisedokument søkeren er i besittelse av, må innleveres sammen med søknaden, jf. lovens § 64 tredje ledd.* *Politiet skal om nødvendig forlange fremlagt de legitimasjonspapirene søkeren har eller kan skaffe, og eventuell dokumentasjon av søkerens status som flyktning.*	UDI, «Registrering, vurdering og endring av identitetsopplysninger i saker etter utlendingsngsloven», 24.04.2012 (sist endret 04.06.2019) JD, «Utlendingsforskriften», 01.01.2010
Krav til oppmøte	Bruker må møte opp på et politikontor for å søke om reisebevis for flyktninger.	UDI, «Hvordan får jeg reisebeviset mitt?», u.å
Gyldighetstid	*Reisebeviset gis som regel gyldighetstid lik oppholdstillatelsen, men ikke lengre enn tre år. Når det foreligger forhold som nevnt i § 12-1 første ledd, eller andre særlige grunner tilsier det, kan det settes kortere gyldighetstid enn utlendingens oppholdstillatelse.* *Dersom flyktningen har fått innvilget permanent oppholdstillatelse, kan gyldighetstiden settes til fem år.*	JD, «Utlendingsforskriften», 01.01.2010
Fornyelse		
Legitimasjonskrav	Leverandøren legger til grunn at legitimasjonskravet ved fornyelse gjelder tilsvarende som ved førstegangsutstedelse.	
Krav til oppmøte	*Bruker må møte opp på et politikontor for å søke om reisebevis for flyktninger. Oppholdskortet sendes deretter til brukers oppgitte adresse*	UDI, «Hvordan får jeg reisebeviset mitt?», u.å

	Utlendingspass	
Førstegangsutstedelse		Kilde
Legitimasjonskrav	*Det tas ikke stilling til utlendingens identitet på nytt ved utstedelsen av utlendingspass med mindre det foreligger nye ID-opplysninger, men bygger på den vurderingen av identitet utlendingsmyndighetene gjorde når det ble gitt førstegangstillatelse.* *Dersom "det er tvil om utlendingens identitet", skal utlendingspass som hovedregel avslås. Med "tvil om identitet" menes at identiteten ikke er sannsynliggjort. Dette innebærer at utlendingens opplysninger om identitet i førstegangstillatelsen legges til grunn, dersom det ikke er holdepunkter for annet. Konkrete holdepunkter kan for eksempel være om søkeren anmoder om å endre de registrerte ID-opplysningene og utstede reisedokument på en annen identitet enn den som vedkommende allerede er registrert med.* *Pass eller annet reisedokument søkeren er i besittelse av, må innleveres sammen med søknaden, jf. lovens § 64 tredje ledd.*	UDI, «Registrering, vurdering og endring av identitetsopplysninger i saker etter utlendingsngsloven», 24.04.2012 (sist endret 04.06.2019) JD, «Utlendingsforskriften», 01.01.2010

	Utlendingspass	
	Politiet skal om nødvendig forlange fremlagt de legitimasjonspapirene søkeren har eller kan skaffe, og eventuell dokumentasjon av søkerens status som flyktning.	
Krav til oppmøte	*Bruker må møte opp på et politikontor for å søke om utlendingspass. Oppholdskortet sendes deretter til brukers oppgitte adresse*	UDI, «Hvordan får jeg utlendingspasset mitt?», u.å
Gyldighetstid	*Utlendingspasset gis gyldighet for et bestemt tidsrom fastsatt av UDIt i det enkelte tilfellet. Gyldighetstiden settes som regel lik gyldigheten av utlendingens oppholdstillatelse, men ikke lengre enn tre år. Når det foreligger forhold som nevnt i § 12-1 første ledd eller andre særlige grunner tilsier det, kan det settes kortere gyldighetstid enn utlendingens oppholdstillatelse.* *Dersom utlendingen har fått innvilget permanent oppholdstillatelse, kan gyldighetstiden settes til fem år.*	JD, «Utlendingsforskriften», 01.01.2010
Fornyelse		
Legitimasjonskrav	Tilsvarende legitimasjonskrav som ved førstegangsutstedelse	
Krav til oppmøte	Bruker må møte opp på et politikontor for å søke om utlendingspass for flyktninger. Oppholdskortet sendes deretter til brukers oppgitte adresse	UDI, «Hvordan får jeg utlendingspasset mitt?», u.å

	BankID	
Førstegangsutstedelse		Kilde
Legitimasjonskrav	*Deltagers legitimasjonskontroll ved førstegangsutstedelse av BankID til fysiske personer skal skje på grunnlag av fremlagt gyldig norsk pass, dokumenter likestilt med norsk pass, eller utenlandsk pass. Det er likevel ikke nødvendig med ny fremleggelse av pass ved utstedelse av BankID dersom pass ble fremlagt ved personlig fremmøte i forbindelse med etablering av kundeforholdet.* *Kravet om fremleggelse av pass kan fravikes dersom deltager er sikker på personens identitet, og* • *Vedkommende etablerte sitt kundeforhold i deltager før 1. mars 2007, eller* • *Kravet om fremleggelse av pass vil innebære en urimelig merbelastning for vedkommende, grunnet alder, helse eller andre særlige forhold* *Så fremt kravet om pass kan fravikes skal deltager i stedet kreve fremlagt annen form for legitimasjon etter de krav til fysiske legitimasjonsdokumenter som følger av hvitvaskingsloven med forskrifter.* *Bits kan fastsette utfyllende regler om legitimasjonskontroll og identifisering av sertifikatholdere, herunder innehavere av BankID til ansatte etter reglene i pkt. 10.3.* *Bits gir nærmere veiledning om forståelsen av reglene foran, hva som menes med norsk pass, dokumenter likestilt med norsk pass, og utenlandsk pass samt i hvilken grad deltager skal kreve tilleggsdokumentasjon for stadfesting av utenlandske personers identitet og bosted. Det kan også gis anbefalinger om praktisering av kontrollreglene.*	BITS, «Regler om BankID», 22.11.2018

	BankID	
Krav til oppmøte	Det stilles krav til fysisk oppmøte og fremleggelse av gyldig legitimasjon. Dette kan gjøres både i bankfilial eller i visse tilfeller ved postens PUM tjeneste.	BITS, «Regler om BankID», 22.11.2018
Gyldighetstid	*Din BankID er normalt gyldig i to år. Det kan skje endringer og oppgraderinger i løsningen som kan tvinge frem fornying på et tidligere tidspunkt. BankID blir automatisk fornyet av banken*	BankID.no, «Hvor lenge er min BankID gyldig», u.å.
Fornyelse		
Legitimasjonskrav	Fornyes automatisk av banken uten videre krav til oppmøte eller fremvisning av legitimasjon	BankID.no, «Hvor lenge er min BankID gyldig», u.å.
Krav til oppmøte	Fornyes automatisk av banken uten videre krav til oppmøte eller fremvisning av legitimasjon	BankID.no, «Hvor lenge er min BankID gyldig», u.å.

Vedlegg 8: Utregning av brukertid og brukerkostnad i et livsløp

	Førstegangsutstedelse		Fornyelse			Sum livsløp	
	Brukergebyr	**Brukertid**	**Brukergebyr**	**Brukertid**	**Antall (fysisk)**	**Brukergebyr**	**Brukertid**
Identitetsnr.	NOK 0	0 min	Ingen fornyelse	Ingen fornyelse	Ingen fornyelse	NOK 0	0 min
Pass	>16 år: NOK 450 <16 år: NOK 270	Bestilling av passtime: 5 min Reisetid: 41 min Tid ved passkontor: 30 min	>16 år: NOK 450 <16 år: NOK 270	Bestilling av passtime: 5 min Reisetid: 41 min Tid ved passkontor: 30 min	#12	NOK 4 770	16 timer og 28 min
Førerkort	NOK 380	Kontroll teori: 18 Kontroll oppkjøring: 2 Reisetid oppmøte: 41 Ventetid: 10 min	NOK 380	Kontroll: 10 min Reisetid oppmøte: 41 min Ventetid: 10 min	#4	NOK 1 900	6 timer og 6 min
Bankkort med bilde	NOK 0	Opprettelse av kontoforhold: 10 min Reisetid: 30 min Opphold ved bankkontor: 15 min	NOK 0	Reisetid: 30 min Opphold ved bankkontor: 15 min	#7	NOK 0	6 timer og 10 min
BankID	NOK 0	0 min	NOK 0	0 min	#0	NOK 0	0 min
MinID	NOK 0	Bestilling og aktivering: 5 min	Ingen fornyelse	Ingen fornyelse	Ingen fornyelse	NOK 0	5 min
					Sum	NOK 6 670	28 timer og 49 min

Tabell 39 Total brukergebyr og brukertid for førstegangsutstedelse og fornyelse av ID-bevis for bruker i et livsløpsperspektiv

Pass

Brukertid: 76 minutter x 13 fysiske oppmøter = 988 minutter = 16 timer og 28 minutter

Brukergebyr: (270 kroner x 6 fysiske oppmøter for barn) + (450 kroner x 7 fysiske oppmøter for voksne) = 4 770 kroner

Førerkort

Brukertid: Teoriprøve (18 min kontroll + 10 min ventetid + 41 min kjøretid) + Oppkjøring (2 min kontroll + 10 min ventetid + 41 min kjøretid) + # 4 Fornyelser (10 min kontroll + 10 min ventetid + 41 min kjøretid) = 69 min + 53 min + (4 x 61 min) = 366 min = 6 timer og 6 minutter.

Brukergebyr: 5 x 380 kroner = 1.900 kroner

Bankkort med bilde

Brukertid: 10 min opprettelse av bankforhold + (30 min reisetid + 15 min opphold ved bankkontor) x 8 = 6 timer og 10 minutter

Brukergebyr: Det påløper ingen gebyrer for førstegangsutstedelse og fornyelse av bankkort med bilde. ID-relatert brukergebyr relatert til utstedelse og fornyelse av bankkort med bilde og BankID anses derfor som tilnærmet 0 kroner. Årlig kostnad for bankkort vurderes av leverandøren å være primært tilknyttet kortets funksjon som betalingstjeneste, og ikke dirkete ID-relatert.

Vedlegg 9: Anmeldte saker fra NAV relatert til ID-misbruk

År	Antall saker	Beløp	Kommentar til saker
2010	6	7,6 mill. kroner	Hovedsakelig Rom-saker, dvs. fiktive barn registrert i Folkeregisteret
2011	9	3,4 mill. kroner	Hovedsakelig Rom-saker, Rempol (misbrukte polske identiteter) og falske albanske pass avdekket av Skatteetaten
2012	5	3,7 mill. kroner	Hovedsakelig Rom-saker
2013	3	1,4 mill. Kroner	Falske EØS-borgere/russiske borgere
2014	13	4,1 mill. kroner	Hovedsakelig Statsløs/Jordansk og Somalia/Djiobouti
2015	6	2,5 mill. kroner	Likt fordelt mellom Irak/Syria, Statsløs/Jordansk og Somalia/Djibouti
2016	1	0 mill. kroner	Et forsøk på ID-bedrageri
2017	0	0 mill. kroner	Ingen saker
2018	5	2,7 mill. kroner	Antall personer som har mottatt stønad med falsk identitet
2019	5	2,9 mill. kroner	Antall personer som har mottatt stønad med falsk identitet

Vedlegg 10: Ressursbruk

Vedlegget gir en oversikt over data på ID-relaterte årsverk og kostnader for årene 2015, 2018 og 2021, som ble innhentet fra aktørene i ID-forvaltningen. Under finnes en beskrivelse av fremgangsmåten for datainnhentingen hos hver aktør, en oversikt over antall årsverk og kostnader hos aktøren, forklaringer av drivere for årsverk og kostnader, samt eventuelle merknader til tallene.

Utlendingsdirektoratet

I samråd med UDI har det blitt estimert antall årsverk og kostnader tilknyttet ID-forvaltningen hos aktøren for 2015, 2018 og 2021. Antall behandlede saker og data fra timeregistreringssystemer er brukt som grunnlag for å estimere tiden som benyttes på ID-relatert arbeid. Ressursbruken til UDI er i høy grad knyttet til personalkostnader. For hver sakstype er det estimert tid benyttet på ID-relatert arbeid, som er multiplisert med antall saker. Nedgangen i personalkostnader, og antall årsverk, fra 2015 til 2018 henger sammen med masseankomsten av flyktninger til Norge i 2015 som førte til økt antall asylintervjuer og asylvedtak i UDI dette året. Produksjons- og distribusjonskostnadene til UDI er tilknyttet produksjon av Schengen-standardiserte oppholdskort. Videre har UDI tatt med utvalgte kostnader til drift og forvaltning tilknyttet ID, samt investeringskostnader til moderniseringsprosjektet i UDI og investeringer i EU-systemer. UDI estimerer at investeringskostnader og løpende drifts- og forvaltningskostnader vil øke fra 2018 til 2021, hovedsakelig grunnet økte investeringer i moderniseringsprogrammet, samt økte utgifter til EU-systemer og EU-lisenser. UDI anser beregningene som estimater, da det ikke foreligger eksakte tall på ressursbruk tilknyttet ID-relatert arbeid hos aktøren.

Utlendingsdirektoratet	**2015**	**2018**	**2021**
Totalt antall årsverk knyttet til ID-relatert arbeid	**190**	**150**	**155**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	190	150	155
Årsverk tilknyttet ID-kontroll	-	-	-
Personalkostnader	186 mill. kroner	147 mill. kroner	151 mill. kroner
Produksjons- og distribusjonskostnader	10,2 mill. kroner	6,5 mill. kroner	8 mill. kroner
Investeringskostnader	*Tall ikke tilgjengelig*	22 mill. kroner	51 mill. kroner
Løpende drift- og forvaltningskostnader	*Tall ikke tilgjengelig*	13 mill. kroner	24,2 mill. kroner
Sum kostnader	**196,2 mill. kroner**	**188,5 mill. kroner**	**234,2 mill. kroner**

Tabell 40 Estimater mottatt fra Utlendingsdirektoratet på antall årsverk og kostnader tilknyttet ID-relatert arbeid

Statens vegvesen

SVV har benyttet data fra timeregistreringssystemer for å gi en oversikt over antall årsverk tilknyttet ID-forvaltningen hos aktøren for 2015, 2018 og 2021. Nøkkeltall for personalkostnader er sammen med antall årsverk benyttet for å beregne totale personalkostnader i 2015 og 2018, samt estimat for 2021. Videre har SVV benyttet sin gebyrmodell og faktura fra leverandører av førerkortproduksjon og utsendelse for å gi en oversikt over produksjons- og distribusjonskostnader. Estimerte fordelingsnøkler er

benyttet for å estimere investeringskostnader og løpende drifts- og forvaltningskostnader som er tilknyttet ID-forvaltning.

Statens vegvesen	2015	2018	2021
Totalt antall årsverk knyttet til ID-relatert arbeid	**73**	**80**	**71**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	33	39	30
Årsverk tilknyttet ID-kontroll	40	41	41
Personalkostnader	51,4 mill. kroner	64 mill. kroner	56,8 mill. kroner
Produksjons- og distribusjonskostnader	9,1 mill. kroner	10,7 mill. kroner	12 mill. kroner
Investeringskostnader	10,5 mill. kroner	9,7 mill. kroner	9,7 mill. kroner
Løpende drift- og forvaltningskostnader	5,7 mill. kroner	5,8 mill. kroner	5,8 mill. kroner
Sum kostnader	**76,7 mill. kroner**	**90,2 mill. kroner**	**84,3 mill. kroner**

Tabell 41 Estimater mottatt fra Statens vegvesen på antall årsverk og kostnader tilknyttet ID-relatert arbeid

Skattedirektoratet

SKD har i samråd med leverandøren estimert antall årsverk og kostnader tilknyttet ID-forvaltningen hos aktøren for 2015, 2018 og 2021. SKD har benyttet estimater på tidsbruk for ID-relaterte aktiviteter samt antall ID-saker håndtert. Samtlige årsverk tilknyttet Folkeregisteret i informasjonsforvaltningsdivisjonen er inkludert i oversikten, da SKD anser alle deres arbeidsoppgaver som ID-relaterte. SKD har benyttet estimater for personalkostnader for å beregne totale personalkostnader for inkluderte årsverk i 2015 og 2021, samt estimat for 2021. Videre har SKD inkludert produksjons- og distribusjonskostnader tilknyttet tilgjengeliggjøring av data i Folkeregisteret via avtale med tredjepartsleverandør og investeringskostnader for prosjektet modernisering av Folkeregisteret. Løpende drifts- og forvaltningskostnader inkluderer blant annet kostnader ved forvaltning av modernisert Folkeregister, systemforvalting av eksisterende løsninger og sjablongmessig beregning av kontorkostnader. Prosjektet modernisering av Folkeregisteret fullføres i 2020 og tilhørende tidligere investeringskostnader reduseres i 2021. Fullføringen av prosjektet fører imidlertid til at drifts- og forvaltningskostnadene tilknyttet det moderniserte Folkeregisteret øker i 2021.

Skattedirektoratet	2015	2018	2021
Totalt antall årsverk knyttet til ID-relatert arbeid	**263,02**	**229,2**	**229,9**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	212	182	182
Årsverk tilknyttet ID-kontroll	51,02	47,2	47,9
Personalkostnader	145,1 mill. kroner	137,9 mill. kroner	136,3 mill. kroner
Produksjons- og distribusjonskostnader	5,3 mill. kroner	5,3 mill. kroner	5,3 mill. kroner
Investeringskostnader	29,3 mill. kroner	155,4 mill. kroner	-

Skattedirektoratet	2015	2018	2021
Løpende drift- og forvaltningskostnader	49,7 mill. kroner	38,8 mill. kroner	125,8 mill. kroner
Sum kostnader	**229,4 mill. kroner**	**337,4 mill. kroner**	**267,4 mill. kroner**

Tabell 42 Estimatet mottatt fra Skattedirektoratet på antall årsverk og kostnader tilknyttet ID-relatert arbeid

Utlendingsnemnda

UNE har benyttet data på totalt antall årsverk og antall behandlede saker i 2015 og 2018, sammen med estimater for andeler av saksbehandlingen som er ID-relatert arbeid, for å gi en oversikt over kostnader og årsverk tilknyttet ID-forvaltningen hos aktøren.. ID-relatert arbeid i UNE omfatter vurdering og fastsettelse av identitet, samt ID-kontroll i saker til behandling. Personalkostnader er estimert med bakgrunn i gjennomsnittlige årsverkskostnader og estimert andel ID-relatert arbeid for de tre årene. Reduksjonen i antall årsverk og tilhørende personalkostnader fra 2015 til 2018 skyldes masseankomsten av flyktninger til Norge i 2015, hvilket førte til økt ressursbruk dette året. UNE har for beregning av ID-relaterte produksjons- og distribusjonskostnader benyttet estimater for administrative overhead kostnader og lokalkostnader per årsverk, samt estimat for andel av det totale arbeidet som er relatert til ID-forvaltning. Årsverk og kostnader for 2021 er estimert basert på samme fremgangsmåte, men er noe lavere enn i 2018 da UNE har redusert antallet seniorrådgivere i sekretariatet i 2019 og benyttet dette som grunnlag for 2021.

Utlendingsnemnda	2015	2018	2021
Totalt antall årsverk knyttet til ID-relatert arbeid	**30**	**23**	**21**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	15	11,5	10,5
Årsverk tilknyttet ID-kontroll	15	11,5	10,5
Personalkostnader	20,5 mill. kroner	16,9 mill. kroner	15,2 mill. kroner
Produksjons- og distribusjonskostnader	5,2 mill. kroner	4,3 mill. kroner	3,8 mill. kroner
Investeringskostnader	-	-	-
Løpende drift- og forvaltningskostnader	-	-	-
Sum kostnader	**25,7 mill. kroner**	**21,2 mill. kroner**	**19,0 mill. kroner**

Tabell 43 Estimatet mottatt fra Utlendingsnemnda på antall årsverk og kostnader tilknyttet ID-relatert arbeid

Utenriksdepartementet

UD har gjennom de to underliggende enhetene «Seksjon for konsulære saker» og «Seksjon for utlendingsfeltet» oversendt data på årsverk og kostnader for departementets ressursbruk tilknyttet ID-forvaltningen. Seksjon for konsulære saker har benyttet antall søknadsregistreringer i systemet Passweb og estimater for tidsbruk per søknad for å estimere sin ID-relaterte ressursbruk. Seksjon for utlendingsfeltet har benyttet antall behandlede visum- og oppholdssaker som grunnlag for å estimere enhetens ressursbruk tilknyttet ID-forvaltningen. Personalkostnader for 2015 og 2018 er for begge enhetene basert på antall årsverk og gjennomsnittlige årsverkskostnader.

Investeringskostnadene for Seksjon for konsulære saker stammer fra innkjøp av nye passlesere i 2018, mens Seksjon for utlendingsfeltet har investeringskostnader tilknyttet «diverse ID-utstyr» i 2015, 2018 og 2021. Seksjon for utlendingsfeltet hadde i 2015 og 2018 løpende drifts- og forvaltningskostnader tilknyttet reisekostnader og kostnader ved samling for ID-ekspertene i seksjonen. Begge seksjonene benytter rapporterte årsverk og kostnader for 2018 som beste estimat for 2021, da det ikke er vedtatt spesifikke endringer frem mot 2021.

Utenriksdepartementet	2015	2018	2021
Totalt antall årsverk knyttet til ID-relatert arbeid	**21,5**	**23,2**	**23,2**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	19,3	20,2	20,2
Årsverk tilknyttet ID-kontroll	2,2	3,0	3,0
Personalkostnader	28,8 mill. kroner	30,7 mill. kroner	30,7 mill. kroner
Produksjons- og distribusjonskostnader	-	-	-
Investeringskostnader	0,4 mill. kroner	0,8 mill. kroner	0,02 mill. kroner
Løpende drift- og forvaltningskostnader	0,04 mill. kroner	0,4 mill. kroner	0,4 mill. kroner
Sum kostnader	**29,2 mill. kroner**	**31,9 mill. kroner**	**31,1 mill. kroner**

Tabell 44 Estimatet mottatt fra Utenriksdepartementet på antall årsverk og kostnader tilknyttet ID-relatert arbeid

NAV

Nav har i beregningen av antall årsverk for 2015, 2018 og 2021 inkludert årsverk som arbeider med forvalting av den digitale løsning for rekvirering av d-nummer, samt benyttet et estimat på tid brukt per rekvirerte d-nummer for å beregne årsverk som arbeider med selve rekvireringen. I tillegg er ett årsverk som arbeider med forebygging, avdekking og anmeldelser av saker der ID-bedrageri inngår. Nav estimerer at antall årsverk som arbeider med forvaltning av den digitale rekvireringsløsningen for d-nummer vil øke med ett årsverk fra 2018 til 2021. Personalkostnadene for 2015 og 21018 har blitt estimert på bakgrunn av beregningen av årsverk og en gjennomsnittlig årsverkskostnad. Investeringskostnaden i 2018 og de løpende drifts- og forvaltningskostnadene i 2018 og 2021 er relatert til den digitale løsningen for rekvirering av d-nummer.

NAV	2015	2018	2021
Totalt antall årsverk knyttet til ID-relatert arbeid	**2,0**	**4,8**	**5,5**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	2,0	4,8	5,5
Årsverk tilknyttet ID-kontroll	-	-	-
Personalkostnader	1,6 mill. kroner	3,9 mill. kroner	4,5 mill. kroner
Produksjons- og distribusjonskostnader	-	-	-
Investeringskostnader	-	6,5 mill. kroner	-

NAV	2015	2018	2021
Løpende drift- og forvaltningskostnader	-	0,7 mill. kroner	0,7 mill. kroner
Sum kostnader	**1,6 mill. kroner**	**11,1 mill. kroner**	**5,2 mill. kroner**

Tabell 45 Estimatet mottatt fra NAV på antall årsverk og kostnader tilknyttet ID-relatert arbeid

Helse- og omsorgsdepartementet

HOD har i samråd med leverandøren benyttet estimater for å beregne årsverk og kostnader i 2015, 2018 og 2021 tilknyttet aktørens rolle i ID-forvaltningen. HOD sine årsverk og kostnader stammer fra registrering av identitet ved fødsel, samt ID-kontroll ved farskapsmeldinger der mor og far til barnet ikke er gift. HOD har estimater på tidsbruk for begge aktiviteter og sammen med data på antall fødte, av gifte og ugifte foreldre, ble antall årsverk estimert. Personalkostnadene for samtlige år ble beregnet basert på estimert antall årsverk og en gjennomsnittlig årsverkskostnad. Estimatene for 2021 legger til grunn at det i 2021 vil fødes like mange barn som i 2018. Grunnet manglende faktiske tall på årsverk og kostnader er tallene for HOD å anse som estimater.

Helse- og omsorgsdepartementet	2015	2018	2021
Totalt antall årsverk knyttet til ID-relatert arbeid	**8,8**	**8,2**	**8,2**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	7,2	6,7	6,7
Årsverk tilknyttet ID-kontroll	1,6	1,5	1,5
Personalkostnader	6,1 mill. kroner	5,7 mill. kroner	5,7 mill. kroner
Produksjons- og distribusjonskostnader	-	-	-
Investeringskostnader	-	-	-
Løpende drift- og forvaltningskostnader	-	-	-
Sum kostnader	**6,1 mill. kroner**	**5,7 mill. kroner**	**5,7 mill. kroner**

Tabell 46 Estimatet mottatt fra Helse- og omsorgsdepartementet på antall årsverk og kostnader tilknyttet ID-relatert arbeid

Forsvarsdepartementet

FD utsteder gjennom underliggende virksomheter Forsvarets ID-kort til sine ansatte. FD har benyttet antall årsverk som arbeider med forvaltningen av kortsystemet for Forsvarets ID-kort, samt årsverk tilknyttet brukeradministrasjonen med arbeid relatert til Forsvarets ID-kort. I tillegg har FD estimert ressursbruken som går med til ID-kontroll av brukere som skal få utstedt Forsvarets ID-kort. Personalkostnadene er beregnet basert på en gjennomsnittlig årsverkskostnad for de relevante ressursene. Produksjons- og distribusjonskostnader, investeringskostnader og drift- og forvaltningskostnader er alle relatert til utstedelsen av Forsvarets ID-kort.

Forsvarsdepartementet	2015	2018	2021
Totalt antall årsverk knyttet til ID-relatert arbeid	**3,1**	**4,6**	**6,2**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	3,0	4,5	6,0
Årsverk tilknyttet ID-kontroll	0,1	0,1	0,2
Personalkostnader	1,8 mill. kroner	2,9 mill. kroner	4,1 mill. kroner
Produksjons- og distribusjonskostnader	1,5 mill. kroner	0,4 mill. kroner	0,6 mill. kroner
Investeringskostnader	-	0,5 mill. kroner	0,2 mill. kroner
Løpende drift- og forvaltningskostnader	-	0,3 mill kroner	0,5 mill. kroner
Sum kostnader	**3,3 mill. kroner**	**4,1 mill. kroner**	**5,4 mill. kroner**

Tabell 47 Estimatet mottatt fra Forsvarsdepartementet på antall årsverk og kostnader tilknyttet ID-relatert arbeid

Direktoratet for forvaltning og ikt

Difi har i beregningen av årsverk medregnet ansatte i avdeling for fellesløsninger tilknyttet ID-relatert arbeid gjennom ID-porten. Samtlige årsverk regnes av Difi som relatert til ID-kontroll, da utstedelse av den offentlige eID-en MinID er selvbetjent og automatisert. For Difi regnes den digitale autentiseringen som gjennomføres ved innlogging gjennom ID-porten som ID-kontroll, og samtlige ID-relaterte årsverk i Difi er knyttet til dette arbeidet.

Personalkostnadene er beregnet basert på lønn, sosiale kostnader og overhead kostnader for et årsverk i avdeling for fellesløsninger. De totale transaksjonskostnadene som autentiseringer gjennom ID-porten medfører er ført delvis under Difis produksjons- og distribusjonskostnader og delvis under drift- og forvaltningskostnader. Produksjons- og distribusjonskostnadene var i 2015 i sin helhet transaksjonskostnader, mens de i 2018 også inneholdt kostnader for driften av MinID. Drift- og forvaltningskostnadene omfattet i 2015 driftskostnadene for MinID, deler av transaksjonskostnadene, samt kostnader ved drift og forvaltning av ID-porten. I 2018 omfattet drift- og forvaltningskostnadene deler av transaksjonskostnadene og kostnader for drift og forvaltning av ID-porten. Kostnadene i 2021 vil føres på samme måte som i 2018. Difi har ikke detaljerte estimater for årsverk og kostnader i 2021. Difi arbeider kontinuerlig med effektivisering av egen organisasjon og mener at tallene for 2018 kan benyttes som estimater for 2021.

Difi	2015	2018	2021
Totalt antall årsverk knyttet til ID-relatert arbeid	**26,3**	**22,2**	**22,2**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	-	-	-
Årsverk tilknyttet ID-kontroll	26,3	22,2	22,2
Personalkostnader	19,2 mill. kroner	20,0 mill. kroner	20,0 mill. kroner
Produksjons- og distribusjonskostnader	15,2 mill. kroner	27,7 mill. kroner	27,7 mill. kroner
Investeringskostnader	-	-	-

Difi	2015	2018	2021
Løpende drift- og forvaltningskostnader	34,9 mill. kroner	20,1 mill. kroner	20,1 mill. kroner
Sum kostnader	**69,3 mill. kroner**	**67,8 mill. kroner**	**67,8 mill. kroner**

Tabell 48 Estimatet mottatt fra Direktoratet for forvaltning og ikt på antall årsverk og kostnader tilknyttet ID-relatert arbeid

Brønnøysundregistrene

Brønnøysundregistrene har for beregningen av årsverk tilknyttet ID-relatert arbeid tatt med årsverk som arbeider med drift og forvaltning av den elektroniske rekvireringsløsningen for d-nummer. Tilhørende personalkostnader er Brønnøysundregistrenes beste estimat for overnevnte årsverk. Brønnøysundregistrene har ikke andre kostnader tilknyttet ID-relaterte aktiviteter. Videre antar Brønnøysundregistrene at antall årsverk tilknyttet ID-relatert arbeid i 2021 vil være likt 2018.

Brønnøysundregistrene	2015	2018	2021
Totalt antall årsverk knyttet til ID-relatert arbeid	**3,9**	**3,5**	**3,5**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	3,9	3,5	3,5
Årsverk tilknyttet ID-kontroll	-	-	-
Personalkostnader	3,0 mill. kroner	3,0 mill. kroner	3,0 mill. kroner
Produksjons- og distribusjonskostnader	-	-	-
Investeringskostnader	-	-	-
Løpende drift- og forvaltningskostnader	-	-	-
Sum kostnader	**3,0 mill. kroner**	**3,0 mill. kroner**	**3,0 mill. kroner**

Tabell 49 Estimatet mottatt fra Brønnøysundregistrene på antall årsverk og kostnader tilknyttet ID-relatert arbeid

Nasjonalt ID-senter

NID har i oversendte data på årsverk og kostnader inkludert samtlige årsverk i virksomheten. Personalkostnadene NID har oversendt dekker samtlige årsverk i virksomheten. NID har en har en rolle som uavhengig fagorgan som yter bistand og rådgivning på ID-området, og har dermed ikke produksjons- og distribusjonskostnader. NID har heller ikke mulighet til å estimere hvor stor andel av ressursbruken som kan tilegnes henholdsvis fastsettelse, registrering og utstedelse eller ID-kontroll. Videre har ikke NID identifisert investeringskostnader i tilknytning til sitt arbeid. NID har oppgitt sine totale kostnader, som ved å trekke fra personalkostnader gir grunnlag for å beregne drift- og forvaltningskostnadene til virksomheten. NID informerer om at antallet årsverk i 2021 kan antas å være likt som i 2018, tatt i betraktning de økonomiske utsiktene de står overfor. Personalkostnadene er ifølge NID antatt å øke med ti prosent per år fra 2019, og dette er benyttet for å estimere personalkostnader i 2021.

Nasjonalt ID-senter	2015	2018	2021
Totalt antall årsverk knyttet til ID-relatert arbeid	**36**	**42**	**42**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	-	-	-
Årsverk tilknyttet ID-kontroll	-	-	-
Personalkostnader	22,1 mill. kroner	29,3 mill. kroner	38,7 mill. kroner
Produksjons- og distribusjonskostnader	-	-	-
Investeringskostnader	-	-	-
Løpende drift- og forvaltningskostnader	10,5 mill. kroner	9,5 mill. kroner	10,3 mill. kroner
Sum kostnader	**32,6 mill. kroner**	**38,8 mill. kroner**	**49,0 mill. kroner**

Tabell 50 Estimatet mottatt fra Nasjonalt ID-senter på antall årsverk og kostnader tilknyttet ID-relatert arbeid

Kripos

Kripos har for beregning av årsverk og kostnader tilknyttet ID-relatert arbeid tatt utgangspunkt i de ulike seksjonene i virksomheten og estimert antall relevante årsverk basert på oppgavene de ulike seksjonene utfører. Kripos har i all hovedsak estimert antall årsverk relatert til ID-oppgaver for å ivareta Kripos sine nasjonale oppgaver. Kripos har ikke en fullstendig oversikt over alt ID-relatert arbeid som virksomheten deltar i, og tallene i tabellen under derfor å anse som estimater. Kripos har for beregning av tilhørende personalkostnader benyttet en gjennomsnittlig årsverkskostnad. Den gjennomsnittlige årsverkskostnaden for 2021 er antatt å være lik som i 2018. Økningen i antall årsverk fra 2018 til 2021 skyldes i hovedsak et økt antall årsverk tilknyttet seksjon for Interpol og Europol (SIE), samt for SIRENE-seksjonen som er kontaktpunkt for utveksling av informasjon tilknyttet i Schengen informasjonssystem (SIS). Kostnader tilknyttet IKT-investeringer, utvikling, drift og forvaltning av sentrale register og nasjonale IKT-løsninger ligger til POD og PIT sine budsjetter og har dermed ikke blitt inkludert av Kripos.

Kripos	2015	2018	2021
Totalt antall årsverk knyttet til ID-relatert arbeid	**46,8**	**48,3**	**55,3**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	39	41,5	43,5
Årsverk tilknyttet ID-kontroll	-	-	-
Personalkostnader	46,8 mill. kroner	53,1 mill. kroner	60,8 mill. kroner
Produksjons- og distribusjonskostnader	-	-	-
Investeringskostnader	-	-	-
Løpende drift- og forvaltningskostnader	-	-	-
Sum kostnader	**46,8 mill. kroner**	**53,1 mill. kroner**	**60,8 mill. kroner**

Tabell 51 Estimatet mottatt fra Kripos på antall årsverk og kostnader tilknyttet ID-relatert arbeid

Politiets utlendingsenhet

PU har for rapportering av årsverk og kostnader valgt å benytte 2016 og 2019, fremfor 2015 og 2018. PU begrunner dette med at 2015 var et ekstraordinært år med tanke på masseankomster av flyktninger og at PU i stor grad var preget av ad hoc-løsninger. PU hadde i 2016 høyt aktivitetsnivå grunnet etterarbeid fra 2015 med tilhørende uttransporter av flyktninger. PU begrunner valget av 2019 med at 2018 inneholdt en stor intern omorganisering, og innrulling i nytt regnskapssystem. I 2019 er ny organisering i stor grad landet for ID-feltet og PU har strukturert økonomidata tilknyttet ny organisering.

Antall årsverk tilknyttet fastsettelse, registrering og utstedelse består av totalt antall årsverk på fagavdeling for ID og uttransport, med uttransport korrigert ut da PU ikke anser det som ID-arbeid. Antall årsverk tilknyttet ID-kontroll består av angitt ressursbruk i PU til ID-kontrollpunkter som er en del av andre prosesser i PU, eksempelvis uttransportering. Tilhørende personalkostnader rapportert av PU inneholder alle typer lønnskostnader, med unntak av kostnader til tolk som er ført under drift- og forvaltningskostnader. PU oppgir at det er stor usikkerhet knyttet til investeringskostnadene for 2019, da de henger tett sammen med prosjekt «Ankomstsenter Østfold» som opplever forsinkelser. For drift- og forvaltningskostnadene presiser PU at disse i 2016 var eksepsjonelt høye grunnet store utgifter til tolk som følge av masseankomstene i 2015. PU har ikke kostnader knyttet til produksjon og utstedelse. PU har for årsverk og kostnader i 2021 tatt utgangspunkt i rapporterte tall for 2019, og estimerer en ti prosent reduksjon for samtlige poster.

Politiets utlendingsenhet	2016	2019	2021
Totalt antall årsverk knyttet til ID-relatert arbeid	**247,4**	**206,5**	**185,9**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	199,4	182	163,8
Årsverk tilknyttet ID-kontroll	48	24,5	22,1
Personalkostnader	192,3 mill. kroner	154,2 mill. kroner	138,8 mill. kroner
Produksjons- og distribusjonskostnader	-	-	-
Investeringskostnader	7,0 mill. kroner	5,4 mill. kroner	4,9 mill. kroner
Løpende drift- og forvaltningskostnader	88,3 mill. kroner	16,4 mill. kroner	14,8 mill. kroner
Sum kostnader	**287,6 mill. kroner**	**176 mill. kroner**	**158,5 mill. kroner**

Tabell 52 Estimatet mottatt fra Politiets utlendingsenhet på antall årsverk og kostnader tilknyttet ID-relatert arbeid

Passutstedelse, ID-seksjonen og NPID-prosjektet

POD har sendt en samlet besvarelse for ressursbruk og kostnader tilknyttet passutstedelse i politidistriktene, arbeidet som gjøres i ID-seksjonen i POD og arbeidet med NPID-prosjektet. Gebyrmodellen til POD er i stor grad benyttet som bakgrunn for estimatene, og PODs antagelser som ligger til grunn i gebyrmodellen vil dermed gjøre seg gjeldende i estimatene i tabellen under. Antall årsverk i ID-seksjonen og NPID-prosjektet er grunnet arbeidets natur ikke spesifisert som fastsettelse, registrering og

utstedelse eller ID-kontroll, men som generelt ID-relatert arbeid. For 2015 og 2021 er årsverk i ID-seksjonen og NPID-prosjektet rapportert samlet, mens det i 2018 er vist en deling med 9 årsverk tilknyttet ID-seksjonen og 45 årsverk tilknyttet NPID-prosjektet. Årsverkene tilknyttet passutstedelse i politidistriktene er spesifisert til steget fastsettelse, registrering og utstedelse. For 2018 er 5 årsverk med ID-eksperter i Kripos regnet med under årsverkene for fastsettelse, registrering og utstedelse av pass, mens det i 2021 er ti årsverk med ID-eksperter i Kripos som er medregnet. Personalkostnadene i 2015 er PODs estimater, mens det for 2018 og 2021 er benyttet gebyrmodellen som bakgrunn for tallene. Produksjons- og distribusjonskostnader i 2015 og 2018 omfatter kostnader for pass og nødpass, mens det i 2021 omfatter kostnader for alle dokumenter som skal utstedes som del av NPID-prosjektet, inkludert nasjonalt ID-kort. Investeringskostnader omfatter kostnader til NPID-prosjekter, inkludert personalkostnader for årsverk tilknyttet prosjektet, samt ombygging av passkontorer. For 2021 er det lagt til tilbakebetalings av investeringskostnader for NPID-prosjektet. Drift- og forvaltningskostnader omfatter utstyr, forvaltning av ID-seksjonen og Politiets IKT-tjenester og husleie. POD har ikke estimater for drift- og forvaltningskostnader for 2015.

Passutstedelse, ID-seksjonen og NPID-prosjektet	**2016**	**2018**	**2021**
Totalt antall årsverk knyttet til ID-relatert arbeid	**190**	**232**	**334**
Årsverk tilknyttet fastsettelse, registrering og utstedelse	170	178	319
Årsverk tilknyttet ID-kontroll	-	-	-
Personalkostnader	125,0 mill. kroner	140,5 mill. kroner	269,2 mill. kroner
Produksjons- og distribusjonskostnader	41,0 mill. kroner	46,2 mill. kroner	83,3 mill. kroner
Investeringskostnader	39,1 mill. kroner	112,4 mill. kroner	67,9 mill. kroner
Løpende drift- og forvaltningskostnader	-	20,9 mill. kroner	128,0 mill. kroner
Sum kostnader	**205,1 mill. kroner**	**320,0 mill. kroner**	**548,4 mill. kroner**

Tabell 53 Estimatet mottatt fra POD på antall årsverk og kostnader tilknyttet ID-relatert arbeid i passutstedelsen i politidistriktene, ID-seksjonen og NPID-prosjektet