Kommunal- og distriktsdepartementet
(inkl. regjeringslogoen)

Strategi

Nasjonal strategi for eID i offentlig sektor

Forord

Svært mange offentlige digitale tjenester krever innlogging slik at virksomheten som tilbyr tjenesten er sikker på at de har dialog med riktig person. Når stadig flere offentlige tjenester løses digitalt er det en forutsetning at offentlig sektor kan være sikker på at man kommuniserer med rett person. Videre er det avgjørende at alle har anledning og kompetanse til å få utstedt og bruke en eID, slik at de kan benytte digitale offentlige tjenester.

Vi har kommet langt med digitaliseringen i Norge og mye fungerer godt med dagens markedsbaserte strategi for eID fra 2008. En medvirkende årsak til at Norge har klart seg så bra gjennom koronapandemien er at vi har mange digitaliserte tjenester, har en digitalt kompetent befolkning og en høy utbredelse av eID. Disse faktorene sørget for at de fleste offentlige tjenestene fortsatte å fungere godt, til tross for store fysiske begrensninger.

Likevel har pandemien også bidratt til å tydeliggjøre mangler ved dagens løsning. Målet med den nye strategien for eID er å adressere svakheter ved eID-løsningene som er avgjørende for å nå ut til alle relevante brukergrupper, redusere digitalt utenforskap og understøtte bedre, mer robuste og helhetlige eID-løsninger for både brukere og sektorer. Strategien er en viktig komponent i ID-forvaltningen i Norge, og legger til grunn målet om *en person, en identitet* i Norge.

Vi har et svært godt utgangspunkt i Norge med høy grad av digitalisering og utbredelse av eID. Dette gir de beste forutsetningene fremover for å lykkes med strategien og muligheter til å utvikle nye digitale tjenester i offentlig sektor.

Oslo, dato

Sigbjørn Gjelsvik

Innholdsfortegnelse

Forord 1
1. Innledning 3
2. Om eID og utvikling på området 5
2.1. eID er en grunnpilar for digitale tjenester 5
2.2. Dagens markedsbaserte strategi har gitt god utbredelse 6
2.3. Utvikling av europeisk regelverk 8
2.4. Vellykkede sektorløsninger 9
2.5. eID er enkelt å få for de fleste 9
2.6. Sikkerhet i eID-løsningene 11
3. Mål og tiltak 13
3.1. Mål 1: Alle relevante brukergrupper skal enkelt kunne skaffe seg en eID på det sikkerhetsnivået de har behov for 13
3.2. Mål 2: Løsning for innlogging og bruk av offentlige digitale tjenester skal være sikker, kostnadseffektiv og helhetlig 22
3.3. Mål 3: Rammer for sikre og effektive løsninger for eID til offentlig ansatte skal være angitt 27
3.4. Mål 4: Løsninger skal være tilpasset markeds- og teknologiutviklingen 30
3.5. Mål 5: Samordningen av eID-utviklingen mellom sektorene og forvaltningsnivåer skal være kostnadseffektiv og god 33
4. Økonomiske og administrative konsekvenser 36

1. Innledning

Norge er blant de ledende landene på digitalisering i Europa[1]. Dette har blant annet vært mulig på grunn av høy digital kompetanse i befolkningen, god bredbåndsdekning og høy utbredelse av elektronisk identifikasjon (eID). En velfungerende infrastruktur for eID er en av grunnpilarene for at offentlige tjenester kan digitaliseres, og at alle har mulighet til å samhandle digitalt med offentlig sektor. Befolkningen har behov for en sikker måte å identifisere seg på digitalt og tjenesteeiere i offentlig sektor har et behov for å vite hvem de kommuniserer med.

Dagens strategi for bruk av eID[2] er fra 2008. Strategien går i hovedsak ut på å benytte markedsløsninger for eID for innlogging via ID-porten[3] for tilgang til offentlige digitale tjenester. En medvirkende årsak til at det ble valgt å benytte markedsbaserte eID-er var at disse hadde god utbredelse i befolkningen. Bruken av eID i samfunnet har generelt økt. Både antall innlogginger via ID-porten til offentlige digitale tjenester og antall digitale offentlige tjenester har vokst kraftig hvert år siden 2008. I dag er innbyggernes interaksjon med offentlig sektor i hovedsak digital, og innbyggerne benytter ID-porten i gjennomsnitt seks ganger per måned.

Som følge av den økte digitaliseringen av offentlig sektor har det dukket opp nye utfordringer og behov hos brukere og forvaltning som ikke dekkes av nåværende strategi. Det er grupper i samfunnet som av ulike årsaker ikke kan benytte en eID og det er heller ikke alle som har skaffet seg en eID. Både for å sikre at alle relevante brukergrupper får tilgang til eID på det sikkerhetsnivået[4] de har behov for og for å sørge for en velfungerende konkurranse innenfor eID-leverandørmarkedet, er det behov for en ny strategi.

Denne strategien erstatter nåværende strategi for eID og er en oppfølging av digitaliseringsstrategien for offentlig sektor 2019-2025[5], samt deler av områdegjennomgangen av ID-forvaltningen fra 2019[6]. Strategien beskriver overordnede retningsvalg og tiltak for å realisere ønskede ambisjoner. Den bygger videre på dagens strategi hvor markedsløsninger for eID i hovedsak benyttes. Samtidig vil offentlig sektor ta et utvidet ansvar for å sikre at nye identifiserte behov blir ivaretatt. Dette innebærer blant annet at det offentlige tar økt ansvar for utbredelse av eID til alle relevante brukergrupper, for kjerneinfrastrukturen[7] for utstedelse av eID, for bruk av eID for offentlige ansatte, samt for samordning mellom sektorene relatert til eID. Strategien skal følges opp med en handlingsplan som konkretiserer tiltakene med tanke på innhold, ansvarlig

---

[1] European Commission, *Digital Economy and Society Index (DESI)*, 2020, tilgjengelig her.
[2] Kommunal- og moderniseringsdepartementet, *Strategi for eID og e-signatur i offentlig sektor*, 2008.
[3] ID-porten er en nasjonal innloggingsløsning til offentlige tjenester på nett, som tilbyr sikker innlogging ved bruk av eID. Se kapittel 2.1 for mer informasjon.
[4] Det skilles mellom tre sikkerhetsnivåer for elektronisk identifikasjon: lavt, betydelig og høyt. Se kapittel 2.2 for mer informasjon.
[5] Kommunal- og moderniseringsdepartementet, *Én digital offentlig sektor*, 2019, tilgjengelig her.
[6] Finansdepartementet, *Områdegjennomgang av ID-forvaltningen*, 2019, tilgjengelig her og her.
[7] Dagens kjerneinfrastruktur for utstedelse av eID består i hovedsak av tre deler: Folkeregisteret, gjennomføring av ID-kontroll og selve utstedelsen av en aktiveringsnøkkel. Se kapittel 3.2 for mer informasjon.

departement/virksomhet, frister, samt økonomiske og administrative konsekvenser der dette er relevant.

En viktig del av grunnlaget for strategien er to behovsanalyser som Digitaliseringsdirektoratet (Digdir) gjennomførte våren 2021[8]. Den første behovsanalysen hentet innspill fra virksomheter, organisasjoner og prosjekter i offentlig, privat og frivillig sektor, mens den andre behovsanalysen hentet innspill direkte fra utvalgte sluttbrukere av eID. Analysene har sikret god dokumentasjon av eksisterende behov og utfordringer knyttet til å få utstedt og bruke en eID. I tillegg har strategien vært behandlet i en interdepartemental referansegruppe hvor også Kommunesektorens organisasjon (KS) har vært representert.

Denne strategiens primære målgruppe er virksomheter og myndigheter i offentlig sektor. Strategien omfatter fysiske personer og omfatter både bruk av eID til pålogging og til signering.

Målet for ID-forvaltningen er *én person, én identitet i Norge*[9] [10]. Dette har stått sentralt i utformingen av strategien. Sikre og brukervennlige eID-er forutsetter en helhetlig identitetsforvaltning som fungerer[11]. En helhetlig identitetsforvaltning omfatter også fastsettelse av identitet, tildeling av identitetsnummer, utstedelse av fysiske ID-bevis og avvikling av identitet. Dette foretas enten av Skatteetaten, politiet eller utlendingsmyndighetene, hvor pass og nasjonale ID-kort utstedes av politiet. Spesielt for sikkerhet i utstedelse og bruk av eID er det viktig at kvaliteten i prosessene tilknyttet identitetsfastsettelse, utstedelse av identitetsnummer og fysiske ID-bevis er høy. For eID er det videre viktig at eID-en utstedes og benyttes av rett person og at sikkerheten i den tekniske løsningen for eID er høy. eID er således et personvernfremmende tiltak, som gjør det mulig for brukeren å sikre at andre ikke får tilgang til sin informasjon og for å kunne identifisere seg for å få tilgang til rettigheter og plikter.

Det er fem overordnede mål for strategien:

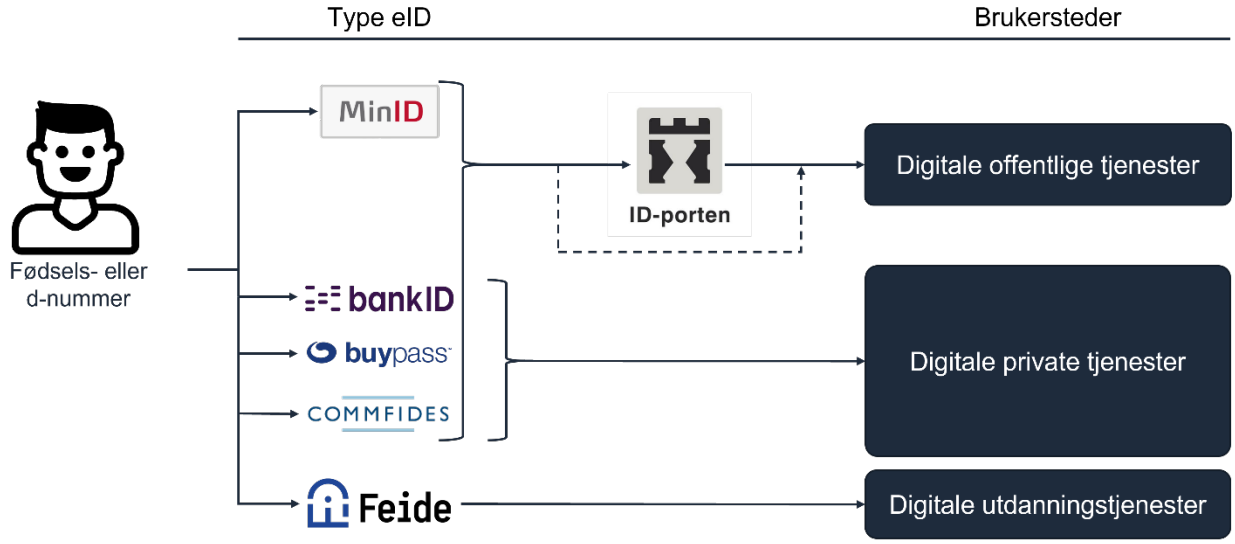
1. Alle relevante brukergrupper skal enkelt kunne skaffe seg en eID på det sikkerhetsnivået de har behov for
2. Løsning for innlogging og bruk av offentlige digitale tjenester skal være sikker, kostnadseffektiv og helhetlig
3. Rammer for sikre og effektive løsninger for eID til offentlig ansatte skal være angitt
4. Løsninger skal være tilpasset markeds- og teknologiutviklingen
5. Samordningen av eID-utviklingen mellom sektorene og forvaltningsnivåer skal være kostnadseffektiv og god

[8] Digdir, *Behovsanalyser eID,* tilgjengelig her (link oppdateres når dokumentene er lagt ut).
[9] Utarbeidet av Koordineringsorganet for ID-forvaltningen (KoID). KoID består av Digdir, Skatteetaten, UDI og Politiet.
[10] Finansdepartementet, *Områdegjennomgang av ID-forvaltningen*, 2019, tilgjengelig her og her.
[11] Helheten og sikkerhet i eID-løsningene forklares nærmere i kapittel 2.6.

2. Om eID og utvikling på området

2.1. eID er en grunnpilar for digitale tjenester

Pålitelige eID-er er en avgjørende forutsetning for digital kommunikasjon og samhandling med offentlig sektor. eID til alle brukergrupper er blant annet nødvendig for å realisere sammenhengende tjenester og arbeidet med livshendelsene i Digitaliseringsstrategien. På samme måte som for et fysisk ID-bevis, benyttes en eID for å bekrefte at en person er den som vedkommende utgir seg for å være digitalt.



Figur 1: Overordnet eksempel på hvordan eID-er brukes i dag

Som illustrert i figuren over, kan en bruker få tilgang til offentlige og private digitale tjenester med en eID. For innlogging gjennom ID-porten kan brukeren i de fleste tilfeller velge enten å benytte den offentlige eID-løsningen MinID, eller en av de markedsbaserte eID-løsningene BankID, Buypass og Commfides. Unntaksvis kan en eID benyttes direkte inn i de digitale offentlige tjenestene, uten å gå via ID-porten. I enkelte sektorer benyttes egne sektorløsninger. Eksempelvis benyttes Feide for digitale tjenester innenfor utdanningssektoren.

Faktaboks: ID-porten

ID-porten, som driftes av Digitaliseringsdirektoratet, er den nasjonale innloggingsløsningen til offentlige tjenester på nett. Løsningen tilbyr innlogging ved bruk av eID og videreformidler innloggingsinformasjon fra eID-leverandører til offentlige tjenester. Ved å benytte ID-porten, slipper virksomheter å kjøpe og administrere egne innloggingsløsninger, og brukeren kan benytte sin foretrukne eID for innlogging til offentlige tjenester. Det er tre markedsbaserte eID-er som har avtale med ID-porten per i dag. Dette er BankID, Buypass og Commfides. I tillegg kan brukerne benytte den offentlig eID-en MinID. Av nærmere 300 millioner innlogginger på offentlige digitale tjenester i 2021, sto MinID for 5,5 prosent av innloggingene, BankID for 93,44 prosent, Buypass for 1,02 prosent og Commfides for 0,01 prosent.

Eksempler på offentlige digitale tjenester som krever en eID for innlogging via ID-porten, og er mange av tjenestene på nav.no, helsenorge.no, lanekassen.no og skatteetaten.no. En eID kan også benyttes som personlig signatur for eksempelvis signering av avtaler. Videre benyttes ulike eID-løsninger både i privat og frivillig sektor. Privat sektor, og da særlig finansnæringen med BankID, har vært den største pådriveren for utviklingen og bruk av eID. Av BankIDs totale innlogginger i 2021 utgjorde offentlige tjenester om lag en tredjedel[12].

2.2. Dagens markedsbaserte strategi har gitt god utbredelse

Samarbeidet mellom privat og offentlig sektor har vært en sentral faktor for at eID-strategien fra 2008 har lykkes. Dette samarbeidet har sørget for at vi har god utbredelse av eID og høy grad av digitale tjenester i offentlig sektor i Norge i dag. Figuren nedenfor illustrerer de viktigste hovedelementene i den markedsbaserte strategien.

Figur 2: Hovedelementer i dagens markedsbaserte strategi

Lov om elektroniske tillitstjenester[13] med forskrifter regulerer bruken av eID. Loven gjennomfører EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (eIDAS-forordningen). eIDAS-forordningen er i utgangspunktet teknologinøytral og beskriver blant annet regler for anerkjennelse av eID-er på tvers av landegrensene i EU/EØS og ulike sikkerhetsnivåer for eID.

Med hjemmel i lov om elektroniske tillitstjenester, har Norge en frivillig meldingsordning[14] (selvdeklarasjonsordning) for eID-er, der Nasjonal kommunikasjonsmyndighet (Nkom) er tilsynsmyndighet. Dette innebærer at norske eID-tilbydere selv vurderer og melder inn hvilket sikkerhetsnivå deres løsning oppfyller til Nkom.

Identifikasjonsnivåforskriften[15] som er hjemlet i lov om elektroniske tillitstjenester, definerer tre sikkerhetsnivåer: lavt, betydelig og høyt. Selvdeklarasjonsforskriften beskriver norske tilpasninger til disse nivåene. Det er den enkelte tjenesteeier som vurderer hvilket sikkerhetsnivå som skal kreves for tilgang til sine digitale tjenester. En slik vurdering skal bygge på virksomhetens egen

[12] Beregnet basert på antall BankID-transaksjoner for offentlig sektor og privat sektor.
[13] Lovdata, *Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester)*, tilgjengelig her.
[14] Tilbydere av eID-ordninger kan etter selvdeklarasjonsforskriften sende inn skjema for melding om selvdeklarasjon, det vil si en beskrivelse av hvordan sine ordninger for elektronisk identifikasjon oppfyller kravene for et gitt sikkerhetsnivå (Lovdata, *Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon,* tilgjengelig her).
[15] Kravene bygger på de europeiske sikkerhetsnivåene, slik de er definert i identifikasjonsnivåforskriften *(Kommisjonens gjennomføringsforordning 2015/1502)*, tilgjengelig her.

vurdering av trusselbildet for sin tjeneste og hvilke konsekvenser en eventuell identifikasjonssvikt vil medføre. eID-løsninger på ulike sikkerhetsnivåer gir dermed tilgang til ulike offentlige digitale tjenester. Kommunal- og distriktsdepartementet har laget en veiledning[16] for tjenesteeiere, som kan være til hjelp ved valg av sikkerhetsnivå. Utover dette bidrar Digdir med beste praksis og veiledning relatert til eID.

Faktaboks: Definisjon av sikkerhetsnivåer for eID

I lov om elektroniske tillitstjenester med forskrifter skilles det mellom tre sikkerhetsnivåer: lavt, betydelig og høyt. Sikkerhetsnivåene angir grader av tillit til at identiteten som benyttes for tilgang til en digital tjeneste er korrekt. Sikkerhetsnivåene skiller seg fra hverandre relatert til hvilke krav som stilles til identitetsfastsettelse og utlevering av eID-en, samt hvilke autentiseringsfaktorer som benyttes i bruksfasen. Autentisering vil si å verifisere en identitet, ved å be om opplysninger som kun den enkelte bruker har tilgang til. Passord, kodebrikke og fingeravtrykk er noen eksempler på ulike autentiseringsfaktorer. De tre sikkerhetsnivåene kan i praksis skilles fra hverandre slik:

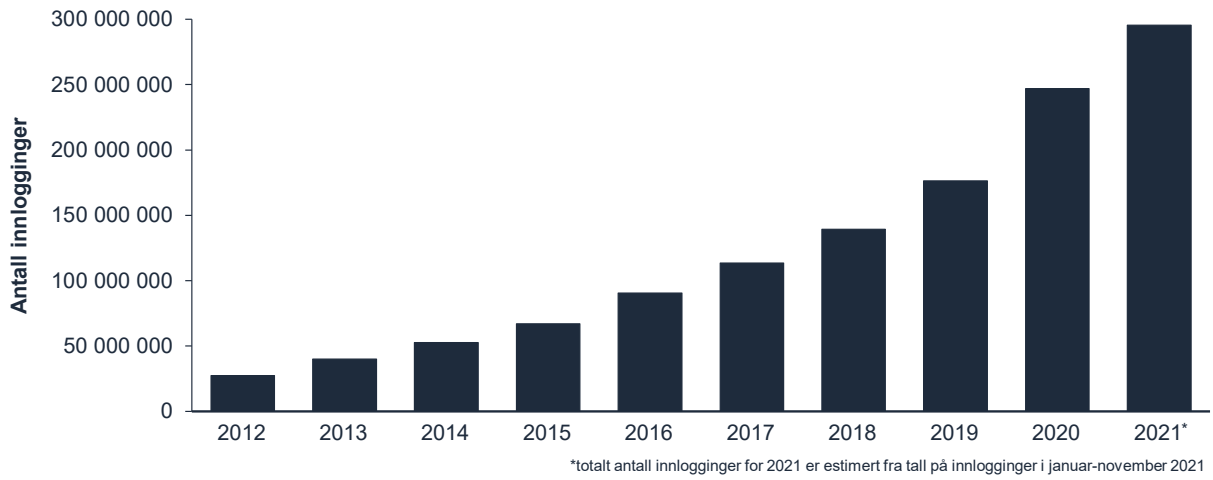
- *Sikkerhetsnivå lavt* krever kun én autentiseringsfaktor, og gir enkel pålogging med bruk av en engangskode eller et egenvalgt passord. Nivået gir en viss sikkerhet for at personen er rette vedkommende og benyttes blant annet til elevpålogging.
- *Sikkerhetsnivå betydelig* krever en tofaktorinnlogging som består av to elementer: noe personen vet (personlig passord eller kode) og noe personen har (kodegenerator eller SIM-kort). De fleste tjenester med taushetsbelagte opplysninger benytter nivå betydelig.
- *Sikkerhetsnivå høyt* krever, i tillegg til en tofaktorløsning, også ID-kontroll[17] ved utstedelse av eID-en. Nivå høyt benyttes for digitale tjenester som behandler taushetsbelagt informasjon, slik som helseopplysninger og annen informasjon med særlig beskyttelsesbehov.

Den offentlige eID-en MinID er den eneste eID-løsningen som er selvdeklarert på sikkerhetsnivå betydelig til Nkom, mens de tre private eID-ene BankID, Buypass, og Commfides er selvdeklarert på sikkerhetsnivå høyt. Ingen løsninger er per i dag selvdeklarert på sikkerhetsnivå lavt.

Offentlig sektor har avtaler om tjenestekjøp med eID-tilbyderne om bruk av eID, både innlogging og signering, som oftest gjennom ID-porten. Bruken av offentlige digitale tjenester som forutsetter bruk av eID har hatt en formidabel økning etter at eID-strategien ble etablert i 2008. Antall offentlige tjenester som bruker ID-porten har økt fra omtrent 200 i 2012 til over 8 000 i 2021. I samme tidsperiode har antall offentlige virksomheter som benytter ID-porten økt fra 3 til 1 200. Den store økningen i antall offentlige digitale tjenester har også ført til stor vekst i antallet innlogginger. Veksten i innlogginger tiltok ytterligere under koronapandemien slik figuren nedenfor viser. Disse tallene viser hvor viktig det er med brukervennlige og tilgjengelige eID-løsninger for digitale tjenester.

[16] Digitaliseringsdirektoratet, *Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor*, tilgjengelig her.

[17] ID-kontroll innebærer en kontroll av brukerens biometri mot gyldig legitimasjon. Se kapittel 2.5 for mer informasjon.



Figur 3: Utvikling i antall innlogginger i ID-porten i perioden 2012-2021

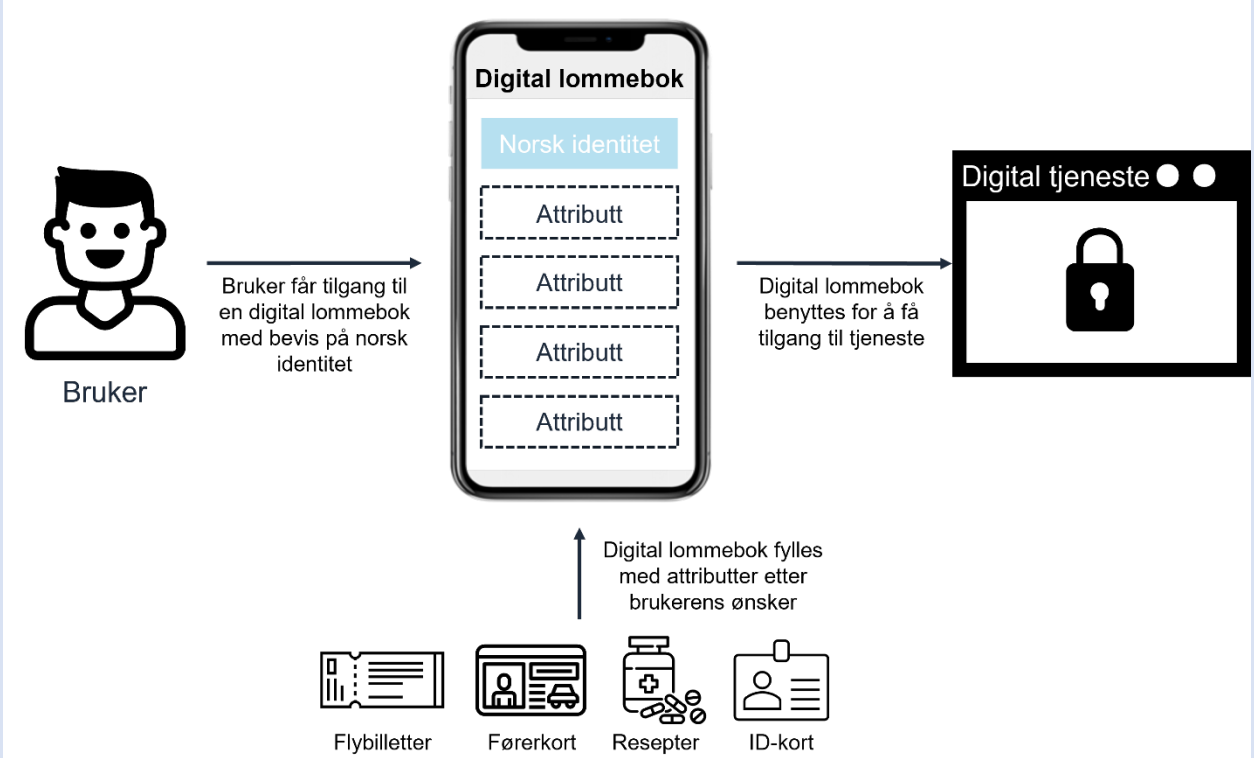
2.3. Utvikling av europeisk regelverk

Det pågår en omfattende revisjon av det europeiske regelverket for eID[18]. Resultatene fra revisjonen vil kunne legge viktige premisser for hvordan Norge regulerer bruken av eID i offentlig sektor fremover. Formålet med revisjonen er blant annet å gjøre det enklere å bruke eID på tvers av landegrenser i EU/EØS, samt styrke personvernet og brukerens kontroll over egne personopplysninger. I tillegg inneholder revisjonen et forslag om at medlemsland skal tilby en digital lommebok med bevis på identitet på sikkerhetsnivå høyt, som skal være gratis i bruk for innbyggerne. Det er påbegynt utarbeidelse av funksjonelle krav til lommebok-løsningen i EU, og Norge, ved Digdir, er en aktiv bidragsyter i dette arbeidet. EU-kommisjonen har som ambisjon å påbegynne utrullingen av en digital lommebok i EU før 2024.

Faktaboks: Digitale lommebøker

En digital lommebok skiller seg fra en standard eID ved at lommebok-løsningen gjør det mulig å legge inn ulike attributter etter brukerens ønsker. Attributter er ulike type bevis eller data som kan deles videre med tredjeparter etter brukers ønske for å få tilgang til en tjeneste. Eksempler på slike attributter er betalingskort, resepter, førerkort og flybilletter. Figuren nedenfor viser hvordan løsningen kan fungere.

[18] EU-kommisjonens lovforslag (eIDAS), *A trusted and secure European eID – Regulation*, 28.05.2021, tilgjengelig her.



Figur 4: Illustrasjon av en digital lommebok

2.4. Vellykkede sektorløsninger

Utover den nasjonale fellesløsningen ID-porten er det to sektorløsninger med utstrakt bruk, Feide og HelseID. Feide er den nasjonale løsningen for sikker innlogging og datadeling innen utdanning og forskning. Omlag 1,3 millioner personer i grunnskolen, videregående skole, samt i forskning og høyere utdanning bruker Feide for tilgang til digitale læremidler og tjenester. I løpet av 2021 hadde løsningen nærmere 210 millioner innlogginger. Feide har etablert seg som et kjent påloggingssystem for brukerne og sikker inngangsport for leverandører som ønsker å tilby digitale tjenester til utdanningssektoren. HelseID[19] er en felles påloggingsløsning for helse- og omsorgssektoren, som legger til rette for enklere pålogging for helsepersonell, og styrket informasjonssikkerhet ved digital samhandling i sektoren. Både Feide og HelseID er vellykkede løsninger med god utbredelse i sine respektive sektorer og med et høyt antall innlogginger.

2.5. eID er enkelt å få for de fleste

I dag er det mulig å velge mellom flere eID-er. Den offentlige eID-en MinID, som er på sikkerhetsnivå betydelig, kan bestilles og tas i bruk fra det året brukeren fyller 13 år. De fleste bestiller MinID når de skal søke plass på videregående skole. Det er et pågående arbeid med å

[19] HelseID er ingen eID i seg selv, men tilbyr innlogging for ansatte i helsesektoren ved bruk av ulike eIDer sammen med informasjon fra helsepersonellregisteret. HelseID forklares ytterligere i kapittel 3.5.

modernisere MinID, som innebærer at brukeren fra og med 2022 enkelt skal kunne logge inn med MinID gjennom engangskoder fra en applikasjon på mobilen. I dag får brukeren utstedt en eID ved at det blir sendt melding til bostedsadressen i Folkeregisteret. I en senere fase av moderniseringsprosessen tas det sikte på at utstedelsesprosessen skal skje ved hjelp av digital ID-kontroll. En digital ID-kontroll innebærer en teknisk løsning som sjekker brukerens biometri[20] opp mot bildet som er lagret i brukerens pass eller nasjonale ID-kort. Dette vil øke sikkerheten i utstedelsen av MinID betydelig.

En eID på sikkerhetsnivå høyt kan anskaffes gjennom private eID-leverandører som BankID, Buypass eller Commfides som vist i figuren under. Ved gjennomføring av fysisk ID-kontroll må brukeren møte personlig og vise frem gyldig legitimasjon. I praksis gjennomføres ID-kontroll gjennom en tjeneste fra Posten, i bankfilial eller via arbeidsplass. Det er mulig å få utstedt flere eID-er til ett og samme fødsels- eller d-nummer, men koblingen mot identiteten skal være entydig. Tilbyderne av eID opererer med forskjellige nedre aldersgrenser, en av dem har ingen nedre aldersgrense[21].

Figur 5: Utstedelse av en eID på sikkerhetsnivå høyt

Selv om eID er enkelt å få utstedt for de fleste, er det likevel flere brukergrupper som har utfordringer. Behovsanalysene avdekket utfordringer med å få utstedt eID på nivå høyt særlig for eldre, hjelpetrengende[22] og ikke-digitale brukere[23], unge mellom 12 og 15 år, samt utenlandske borgere, herunder studenter, andre lands diplomater som tjenestegjør i Norge, samt asylsøkere. I tillegg er utfordringene også knyttet til mangelfull informasjon og veiledningstilbud, krav til fysisk oppmøte, og barrierer knyttet til både språk og digital kompetanse[24].

[20] Biometriske kjennetegn kan beskrives som kjennetegn som utgår fra kroppen, som er unike for deg som enkeltperson og samtidig permanente eller stabile over tid. Ved å måle disse kjennetegnene kan de benyttes til å gjenkjenne en person, eller bekrefte en persons påståtte identitet (Datatilsynet, *Biometri*, tilgjengelig her).
[21] Se kapittel 3.1 for mer informasjon.
[22] Med hjelpetrengende menes personer som har behov for hjelp til å benytte eID og tilknyttede tjenester.
[23] Ikke-digitale brukere er personer som har generelle utfordringer med å benytte digitale verktøy og tjenester. Eksempler på dette kan være eldre, personer med verge eller personer som ikke evner å ta vare på en eID grunnet eksempelvis utfordringer med rusavhengighet.
[24] Utfordringene for de ulike brukergruppene utdypes ytterligere i kapittel 3.1.

2.6. Sikkerhet i eID-løsningene

Sikkerhet i eID-løsninger beskrives i regelverket ved hjelp av ulike sikkerhetsegenskaper og hvordan disse overholdes. Oppsummert omfatter dette egenskaper tilknyttet identifisering, og utstedelse, bruk av eID-løsninger, samt organisering og drift. Identifisering betyr å påvise eller fastslå en identitet. Spesielt for egenskaper tilknyttet identifisering hviler sikkerheten i eID-løsninger på øvrige prosesser i identitetsforvaltningen i Norge. Dette innebærer at eID-en utstedes på grunnlag av sikre fysiske ID-bevis og med en entydig kobling til unike identiteter i Folkeregisteret.

Det er strenge krav til identifisering og utstedelse på sikkerhetsnivå høyt. Regelverket tilsier at eID-tilbyderen må sikre at identifikasjonen gir en sikker og entydig kobling til personens identitetsnummer i Folkeregisteret (fødsels- eller d-nummer)[25] ved alle sikkerhetsnivå. Regelverket skal således ivareta at en eID utstedes til rett person. Sikkerheten i eID-løsningene er dermed avhengig av høy kvalitet i prosessene tilknyttet identitetsfastsettelse og utstedelse av identitetsnummer, samt utstedelse av fysiske ID-bevis som viser en slik tilknytning. Dette er prosesser som politiet, Skatteetaten og Utlendingsdirektoratet i hovedsak ivaretar. Det er en risiko for at det kan være registrert falske eller uriktige identiteter i Folkeregisteret, og at det på grunnlag av dette kan bli utstedt et ID-bevis med uriktig identitet. Etablering og registering av unike identiteter i Folkeregisteret vil øke kvaliteten i Folkeregisteret, som igjen kan danne et sikrere grunnlag for utstedelse av eID. Det foreligger i liten grad dokumentasjon på at det foreligger sikkerhetsbrudd i utstedelsesprosessen direkte relatert til utstedelse av eID.

Faktaboks: Utstedelse av pass og nasjonalt ID-kort

Pass og nasjonalt ID-kort utstedes ved politiets pass- og ID-kontor, og ved utvalgte utenriksstasjoner. Pass og nasjonalt ID-kort er i tillegg til å være reisebevis, det eneste offentlige utstedte ID-beviset i Norge.

For å øke sikkerheten i utstedelsesprosessen for pass og nasjonalt ID-kort er det gjort betydelige endringer de siste årene. Dette omfatter både ny teknologi, videreutvikling av saksbehandlingsløsningen, kompetanse hos ansatte som utfører ID-kontroll og sikkerhet i lokalene hvor søker fysisk møter opp. Politiet har tatt i bruk ansiktsgjenkjenningsteknologi for å sikre at pass og ID-kort ikke blir utstedt til feil person. Samme prosess sikrer også at en person ikke kan få utstedt pass på flere enn et identitetsnummer fra Folkeregisteret.

Faktaboks: UNIK

Prosesser i identitetsforvaltningen medfører en risiko for at samme person kan få mer enn ett identitetsnummer i Folkeregisteret. Risikoen for dette er størst ved tildeling av identitetsnummer til EØS-borgere. Til hvert fødsels- eller d-nummer kan det registreres opplysninger om på hvilket grunnlag vedkommende identitet er registrert, jf. Folkeregisterloven § 3-2. Det er lagt til rette for å registrere status «unik» i Folkeregisteret. For å understøtte målsetningen om *én person, én*

[25] Lovdata, *Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon, § 18. Identifikasjonen skal gi entydig kobling til Folkeregistrert person,* tilgjengelig her.

identitet i Norge har Skatteetaten, politiet og utlendingsforvaltningen utredet muligheten for registrering av «unike» identiteter i Folkeregisteret ved bruk av biometri. Søk i biometriregistrene i justissektoren danner grunnlaget for at status «unik» kan oppnås i Folkeregisteret. Status «unik» vil distribueres til brukerne av Folkeregisteret og klargjøre kvaliteten på de lagrede opplysningene. Ved bruk av «unik» kan offentlig sektor med større grad av sikkerhet vite at en person ikke har eID-er i flere forskjellige identiteter. Selv om en person får status «unik», så må identitetskontroll ved utstedelse av eID sikre utstedelse til rett person, slik regelverket krever.

Dagens løsninger på høyeste sikkerhetsnivå gir god teknisk beskyttelse ved bruk, men kan være utsatt for misbruk i nære relasjoner og ved identitetssvindel[26]. Dette innebærer at eID-en benyttes av andre enn den rettmessige eieren av eID-en, eksempelvis for å skaffe tilgang til tjenester og ytelser. Det er på dette området det erfares mest svindel og misbruk tilknyttet eID.

For egenskaper relatert til organisering og drift må en eID-tilbyder ha dokumentert praksis for blant annet håndtering av informasjonssikkerhet, strategier og metoder for risikohåndtering, samt for gjennomføring av anerkjente kontroller og revisjoner som dokumentasjon på at god praksis er innført.

[26] Misbruk i nære relasjoner er nærmere forklart i kapittel 3.4.

3. Mål og tiltak

Dette kapittelet beskriver tiltak som skal realisere strategiens mål og gir en tydelig retning for det videre arbeidet med eID i offentlig sektor. For hvert av målene presenteres dagens situasjon, før ambisjoner og tiltak beskrives.

3.1. Mål 1: Alle relevante brukergrupper skal enkelt kunne skaffe seg en eID på det sikkerhetsnivået de har behov for

Dagens situasjon

I dag kan en eID fra BankID, Buypass eller Commfides benyttes for tilgang til digitale tjenester, både de som krever sikkerhetsnivå høyt og de som er på nivå betydelig. Den offentlige eID-en MinID kan benyttes til tjenester som er på sikkerhetsnivå betydelig. Som beskrevet i kapittel 2 er de ovennevnte markedsbaserte eID-ene på sikkerhetsnivå høyt godt utbredt i befolkningen med en meget god utbredelse på personer over 18 år. Per 1. januar 2022 har BankID omtrent 4,3 millioner aktive brukere, mens Buypass og Commfides samlet har om lag 150 000 brukere på sikkerhetsnivå høyt. eID på sikkerhetsnivå betydelig er også godt utbredt, særlig blant unge. Per 1. januar 2022 har MinID i underkant av én million aktive brukere.

Dagens markedsbaserte strategi er utformet blant annet for å legge til rette for konkurranse innenfor eID-leverandørmarkedet. Gitt dagens utbredelse av BankID, Commfides og Buypass, har BankID en dominerende markedsposisjon. Denne fordelingen av brukere har vært relativt lik de siste ti årene og ingen nye aktører har kommet til. Dette kan innebære en risiko i forhold til robusthet- og sikkerhet og en ulempe i forhandling med markedsaktørene om priser.

Ikke alle brukergrupper har skaffet seg en eID på sikkerhetsnivå høyt gjennom markedsaktørene. Dagens eID-løsninger er heller ikke tilrettelagt for alle brukergruppers behov. Flere brukergrupper har dermed utfordringer med å benytte seg av offentlige digitale tjenester som krever innlogging ved bruk av eID på sikkerhetsnivå høyt. Dette utfordrer et digitalt førstevalg for offentlige tjenester og kan lede til digitalt utenforskap for flere brukergrupper som risikerer å ikke ha tilgang til digitale offentlige tjenester som de enten har krav på eller har plikt til å bruke. Behovsanalysene avdekket at særlig *eldre, hjelpetrengende og ikke-digitale brukere*, *unge mellom 12 og 15 år*, samt *utenlandske borgere og asylsøkere* har utfordringer med å få utstedt og/eller bruke en eID. Behov og utfordringer for disse brukergruppene er nærmere beskrevet i de påfølgende avsnittene.

Det er ulike årsaker til at flere *eldre, hjelpetrengende og ikke-digitale* brukere kan ha utfordringer med å få utstedt og/eller bruke en eID på sikkerhetsnivå høyt. I denne gruppen inngår eksempelvis personer med nedsatt funksjonsevne, pårørende og verger til hjelpetrengende, samt eldre som av ulike årsaker trenger hjelp til å benytte eID og digitale tjenester. For flere av brukerne i brukergruppen kan det være utfordrende både å få utstedt en eID og å benytte den. De gjennomførte behovsanalysene viser at flere i denne gruppen får hjelp av familie og nærstående personer til bruk av eID. Det kan skyldes at de ikke anser dette som problematisk med tanke på personvern eller datasikkerhet. Dette kan skyldes at de har begrenset kunnskap om hva en eID er og hvordan den skal behandles. Det kan også tyde på at de aktuelle brukerne har stor tillit til

personene som de overlater sin eID til. Det fremkom videre av behovsanalysene at enkelte eldre også kan oppleve utfordringer med å få utstedt en eID. Det kan for eksempel være fordi banken anser at de ikke er i stand til å bruke en BankID, eksempelvis dersom en pårørende kontakter banken for en av sine foreldre. Tilsvarende problemstilling gjelder også rusmisbrukere som av ulike grunner ikke får et kundeforhold i en bank og dermed ikke en BankID. Videre kan det være vanskelig å få utstedt en eID på sikkerhetsnivå høyt for personer med nedsatt funksjonsevne på grunn av markedsaktørenes vurdering av brukerens evne til å inngå BankID-avtale. Det kom også frem i behovsanalysene at personer som er pårørende eller verger for eldre, hjelpetrengende og ikke-digitale brukere kan oppleve utfordringer med bruk av eID på vegne av en annen bruker. 14 prosent av nordmenn fra 16 år og oppover (tilsvarende 600 000 personer) er definert som ikke-digitale[27]. Ifølge Direktoratet for høyere utdanning og kompetanse (HK-dir) betyr dette at deres digitale ferdigheter ikke er tilstrekkelige til å kunne bruke mange av de digitale tjenestene som finnes. Videre er det omtrent 65 000 personer som er satt under vergemål av omtrent 45 000 verger[28]. Mangel på gode løsninger for disse brukerne gjør at verken brukeren, pårørende eller verge kan få tilgang til digitale tjenester fra det offentlige, slik at papir- eller oppmøtebaserte løsninger må benyttes. Dette medfører lav brukervennlighet for de ikke-digitale brukerne, pårørende eller verger. Dette kan dessuten gi lavere sikkerhet og være lite kostnadseffektivt for offentlig sektor. Behovsanalysene viser at det er behov for brukervennlige digitale fullmaktsløsninger som muliggjør tilgang til offentlige tjenester på vegne av en annen bruker. Digdir har påbegynt et arbeid med et fullmaktsregister-prosjekt (FUFINN[29]) som delvis adresserer dette behovet.

Det er en lav andel blant *unge i alderen 12-15 år* som har en eID på sikkerhetsnivå høyt. Av omtrent 257 000 personer i denne aldersgruppen, er det 237 000 som ikke har en eID på sikkerhetsnivå høyt. Behovsanalysene viser at krav til fysisk oppmøte, aldersgrense, dokumentasjon og samtykke fra foresatte er medvirkende årsaker til dette.

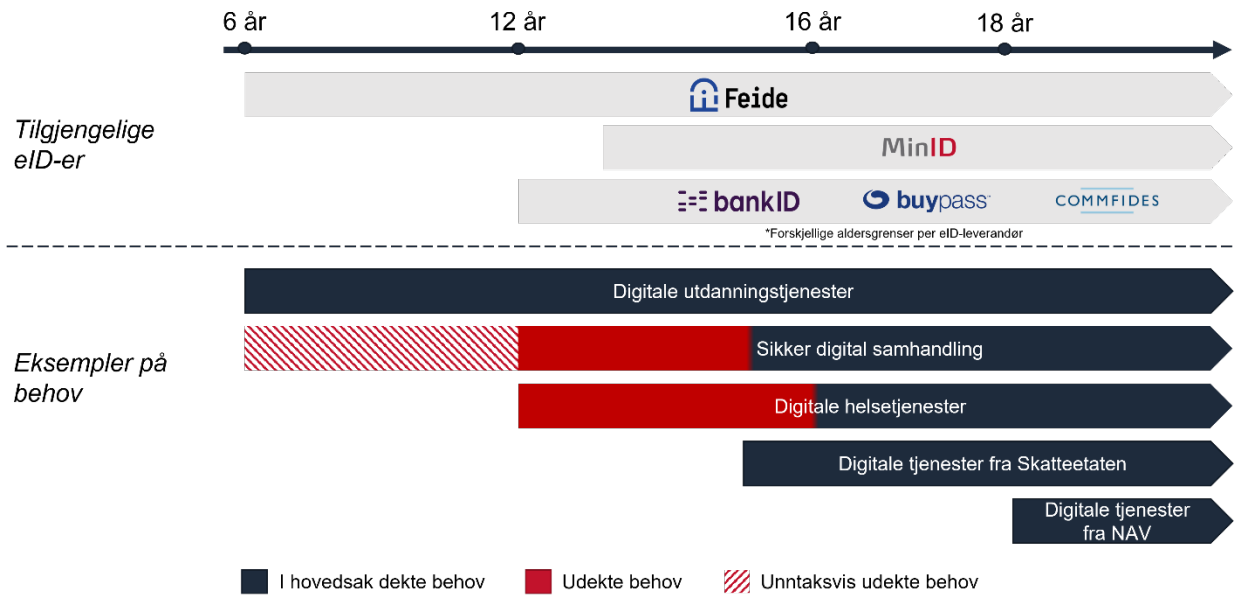
Faktaboks: Unge brukere og eID

Unge får utstedt en Feide-bruker fra kommunen når de starter i grunnskolen for innlogging til skolesystemer og læringsmateriale, og ved oppstart på videregående skole får unge utstedt en ny Feide-bruker fra fylkeskommunen. Feides bruksområde er begrenset til utdanningssektoren. MinID kan bestilles fra året unge fyller 13 år, men de fleste får den utstedt i forbindelse med søknadsprosessen til videregående skole. MinID kan benyttes til digitale offentlige tjenester på sikkerhetsnivå betydelig. Unge kan videre få en eID på sikkerhetsnivå høyt gjennom en av de private eID-leverandørene BankID, Buypass eller Commfides. Aktørene opererer med ulike aldersgrenser og mange banker utsteder ikke BankID til unge under 15 år. Commfides opererer imidlertid ikke med en nedre aldersgrense.

---

[27] Kompetanse Norge, *Befolkningens digitale kompetanse og deltagelse*, 2021, tilgjengelig her.
[28] Statens sivilrettsforvaltning, *Årsmelding vergemål*, 2020, tilgjengelig her.
[29] FUFINN er et prosjekt som drives av Digitaliseringsdirektoratet. Målsettingen med prosjektet er å legge til rette for mer effektive representasjonsordninger for personer med nedsatt funksjonsevne (Digitaliseringsdirektoratet, *Statens sivilrettsforvaltning: FUFINN Vergemål*, 2020, tilgjengelig her).

Det er flere udekte behov for unge i dagens situasjon, slik Figur 6 viser. Den økte digitaliseringen medfører behov for både økt tilgang og utbredelse for eID på sikkerhetsnivå høyt for unge brukere, særlig for tjenester som involverer utveksling av sensitive personopplysninger. Dette gjelder lovbestemte offentlige tjenester for eksempel innenfor helsesektoren, hvor det ikke er mulig å kommunisere digitalt med brukerne så lenge de ikke har en eID på tilstrekkelig høyt sikkerhetsnivå.



Figur 6: Oversikt over tilgjengelige eID-er for unge og eksempler på denne brukergruppens behov

Flere tjenesteeiere har uttrykt behov for sikker digital kommunikasjon og samhandling med brukere helt ned til 12 år[30]. Det kan oppstå behov for sikker kommunikasjon om sensitive opplysninger mellom unge brukere og offentlig sektor, for eksempel kommunikasjon og samhandling med barnevernet uten at foresatte er involvert. Helsesektoren skal tilby tjenester for unge ned mot 12-års alderen og potensielt yngre, uten at deres foresatte trenger å være involvert. Begrenset tilgang til eID på sikkerhetsnivå høyt for denne gruppen gjør dette svært utfordrende. Dessuten mister foreldre digital tilgang til spesialisthelsetjenesten når barnet fyller 12 år. Siden barnet ikke selv får tilgang før fylte 16 år, blir det et gap der ingen har digital tilgang til spesialisthelsetjenester når barnet er mellom 12 og 16 år.

For *utenlandske borgere og asylsøkere* er utfordringene tilknyttet eID svært ulike gitt brukernes livssituasjon, men felles for alle er barrierer knyttet til både språk og digital kompetanse. Behovsanalysene viser at det særlig er udekte behov for noen undergrupper, og som i stor grad er relatert til livshendelsen «ny i Norge»:

[30] Unntaksvis finnes det også enkeltsituasjoner som kan gi behov for en eID på nivå høyt for unge under 12 år.

- Mange utlendinger bosatt i Norge mangler tilgang til eID på høyt sikkerhetsnivå. Eksempelvis har mange utenlandske arbeidstakere[31] med norsk d-nummer[32] kun MinID[33]. De har derfor ikke en eID som gir tilgang til norske offentlige digitale tjenester som krever høyeste sikkerhetsnivå. Flere aktuelle tjenester for de utenlandske arbeidstakerne krever en eID på sikkerhetsnivå høyt, slik som å søke om dagpenger digitalt eller tilgang til helseopplysninger. «MinID Passport[34]» ble utviklet våren 2020 som en midlertidig løsning for å gi arbeidstakere fra EØS-land uten en norsk eID på sikkerhetsnivå høyt, tilgang til NAVs tjenester. Løsningen innebærer at det er mulig å få en slik eID uten å møte opp fysisk, noe som har bidratt til å løse flere utfordringer for denne brukergruppen under koronapandemien.
- Selv om asylsøkere og flyktninger med bekreftet identitet og gyldige ID-papirer i utgangspunktet skal ha mulighet til å få utstedt en eID på sikkerhetsnivå høyt, opplever de imidlertid at praksisen for å få utstedt BankID varierer fra bank til bank og at det kan være vanskelig å få opprettet et kundeforhold. Personer med midlertidig oppholdstillatelse i Norge uten gyldige ID-papirer, har ingen mulighet til å få utstedt en eID og følgelig ingen tilgang til digitale offentlige tjenester. Dette gjør at det blir behov for manuell saksbehandling, som krever mer ressurser både for brukeren og offentlige virksomheter.
- Utenlandske borgere uten norsk personidentifikator som oppholder seg i Norge for en kortere periode eller som verken kvalifiserer til fødsels- eller d-nummer, kan også ha behov for en eID som gir tilgang til digitale offentlige tjenester. Det er identifisert flere brukstilfeller på tvers av sektorer hvor slike behov oppstår, og hvor det i dag benyttes ulike former for hjelpe- eller saksbehandlingsnummer. Dette kan eksempelvis være for studenter, sensorer eller forskere i utdanningssektoren, i forbindelse med kortvarig akutt helsehjelp, søking av oppholdstillatelse fra utlandet, innkreving fra utenlandske parter med videre. For å imøtekomme slike behov vurderes en tredje nummeridentifikator i tillegg til fødsels- og d-nummer. For at disse brukerne skal kunne kommunisere digitalt med offentlig sektor vil det uansett være behov for sikker identifisering og gode eID-løsninger. Koronapandemien har også vist at det er behov for en eID for personer uten fødsels- eller d-nummer.

Mangelen på tilgang til det digitale Norge med eID for EØS-borgere med d-nummer kan være til hinder for fri bevegelse. «MinID Passport» er et viktig steg på veien for å løse disse utfordringene, men er ikke en permanent løsning for behovene til EØS-borgere. eIDAS-noden[35] i Norge har gjort det mulig å benytte en eID fra andre europeiske land til å logge seg på til digitale tjenester i Norge.

---

[31] I 2020 var det registrert 435 532 utenlandske sysselsatte i Norge mellom 20 og 66 år (SSB, *Sysselsetting blant innvandrere, registerbasert*, 2021, tilgjengelig her).

[32] Det finnes to typer identitetsnummer i Norge: fødselsnummer og d-nummer. Et d-nummer kan tildeles personer som planlegger å oppholde seg i Norge mindre enn 6 måneder, eller som planlegger å oppholde seg i Norge mer enn 6 måneder, men som ikke oppfyller vilkårene for å få tildelt et fødselsnummer (Skatteetaten, *D-nummer*, 2020, tilgjengelig her).

[33] Personer med fødsels- eller d-nummer har anledning til å anskaffe en eID fra Buypass eller Commfides på sikkerhetsnivå høyt, men dette kan være lite brukervennlig grunnet dokumentasjonskrav. Lav kjennskap til disse eID-ene og kostnad er også en barriere. For BankID kreves også at banken ønsker arbeidstakeren som kunde.

[34] MinID Passport ble utviklet av Digdir for NAV våren 2020 og kan brukes av EØS-borgere med norsk fødsels- eller d-nummer. eID-løsningen bruker pass-verifisering som en del av registreringen for å identifisere seg og en to-faktorløsning ved innlogging.

[35] eIDAS-noden tillater gjensidig anerkjennelse av elektroniske identiteter (eID) i Europa.

Grunnet utfordringer knyttet til regelverk og tekniske løsninger for å koble utenlandske identiteter til identiteter i Folkeregisteret, er dette imidlertid ikke tatt i bruk av tjenesteeiere. Når identitetsmatching er på plass, vil det kunne bli enklere for en EØS-borger å benytte en eID fra sitt hjemland for tilgang til digitale offentlige tjenester i Norge.

Behovsanalysene avdekket at de fleste brukergruppene generelt har lav kunnskap om eID. Det eksisterer ikke et helhetlig tilbud for opplæring og veiledning for anskaffelse og bruk av eID som dekker etterspurte behov og er tilpasset målgruppene. Ifølge behovsanalysene har flere som skal få utstedt og benytte en eID for første gang behov for opplæring og veiledning, mens andre brukergrupper har behov for veiledning tilknyttet de tekniske aspektene og bruk av eID generelt. Videre opplever flere at det stadig blir vanskeligere å få fysisk hjelp og veiledning om tilgang til digitale offentlige tjenester, og at eventuelle digitale veiledningstilbud oppleves som for lite tilgjengelig og for lite brukervennlig.

Som beskrevet i kapittel 2, er det ifølge eForvaltningsforskriften[36] opp til hver enkelt virksomhet og tjenesteeier å bestemme hvilket sikkerhetsnivå (lavt, betydelig eller høyt) som skal kreves for innlogging til sine tjenester. I dag krever 79 prosent av tjenestene som er tilgjengeliggjort via ID-porten at brukeren benytter en eID på sikkerhetsnivå betydelig, mens 21 prosent av tjenestene krever sikkerhetsnivå høyt. De fleste tjenestene som har satt krav om pålogging med en eID på sikkerhetsnivå høyt, er tjenester som har et høyt antall innlogginger per dag eller som uttrykker et særlig behov for nivå høyt, slik som helsenorge.no og nav.no. Derfor utgjør innlogging til tjenestene med nivå høyt 66 prosent av de totale årlige innloggingene med eID via ID-porten. 94 prosent av brukerne velger uansett å benytte sin eID på nivå høyt, uavhengig av hvilket sikkerhetsnivå tjenesten krever. Flere virksomheter krever innlogging på sikkerhetsnivå høyt kun for enkelte av sine tjenester, mens resten av tjenestene krever betydelig. Behovsanalysene viser imidlertid at enkelte virksomheter vurderer å innføre et gjennomgående krav om pålogging med en eID på sikkerhetsnivå høyt for tilgang til sine tjenester, for å forenkle sin infrastruktur og gjøre det mer sømløst for brukeren. Samtidig er det viktig for tjenesteeiere at alle som kan, har en eID, slik at de får effektivitet i tjenestene sine, og slipper å håndtere tjenesteproduksjon manuelt der mulig.

Oppsummert er det følgende udekkede behov og utfordringer:

- Lav utbredelse av eID på sikkerhetsnivå høyt blant enkelte brukergrupper kan lede til digitalt utenforskap. Særlig gjelder dette eldre, hjelpetrengende og ikke-digitale brukere, unge mellom 12 og 15 år, samt utenlandske borgere og asylsøkere
- Mangel på digitale fullmaktsløsninger gjør at pårørende eller verger for eldre, hjelpetrengende og ikke-digitale brukere opplever store utfordringer med hensyn til å ivareta vergehavers eller den hjelpetrengendes interesser

[36] Lovdata, *Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)*, tilgjengelig her.

- Mangelfull konkurranse i eID-leverandørmarkedet kan gi offentlig sektor en svekket posisjon i forhandlinger om enhetspriser. I tillegg kan funksjonaliteten i ID-porten bli påvirket negativt i ut fra et robusthets- og sikkerhetsperspektiv

Ambisjon og tiltak

Digitaliseringsstrategien for offentlig sektor for 2019-2025[37] har satt som mål at flere oppgaver skal løses digitalt, og at alle innbyggere som har evne til det, skal kunne kommunisere digitalt med offentlig sektor. Alle[38] med behov skal derfor enkelt kunne skaffe seg for en eID på sikkerhetsnivå høyt. Det er en ambisjon å videreføre dagens eID-strategi som innebærer bruk av markedsløsninger for eID for innlogging på sikkerhetsnivå høyt. Offentlig sektor må imidlertid ta et ansvar for at identifiserte brukerbehov blir ivaretatt. eID-er skal på en brukervennlig måte også støtte innlogging på et lavere sikkerhetsnivå når det er behov for dette. Det er en ambisjon at alle som er gitt tilgang til en eID skal kunne benytte den og at eID-ene skal kunne brukes på ulike enheter avhengig av brukerens behov. Alle som har behov for det, skal ha mulighet til å få bistand til å benytte en eID. Bistanden kan være i form av opplæring og oppfølging tilknyttet bruk av eID, tilrettelagte løsninger eller at andre kan opptre på vegne av brukeren. Det er derfor en ambisjon at alle personer som ønsker det, skal kunne la seg representere digitalt av andre, slik at alle får tilgang til digitale tjenester. Det er videre en ambisjon om trinnvis å etablere gode fullmaktsløsninger for de største brukerbehovene.

For å realisere ambisjonene ovenfor er det behov for syv tiltak:

1) MinID skal videreutvikles for å bli mer robust og brukervennlig. Påbegynt modernisering av den tekniske løsningen for MinID skal fullføres. Dette er nødvendig for å ivareta økt krav til sikkerhet og understøtte identifiserte brukerbehov. Ny prosess for utstedelse av eID, ny mobilapplikasjon for bruk og ny teknisk løsning for drift og forvaltning vil sikre bedre sikkerhet, brukervennlighet og effektivitet. En modernisert MinID vil i teorien kunne brukes til langt flere tjenester enn i dag. Modernisering av MinID kan også være en viktig forutsetning for å kunne utvikle en offentlig eID-løsning på nivå høyt, dersom dette løsningsalternativet på et senere tidspunkt anses som aktuelt. Et sentralt element i arbeidet er også å styrke veiledning og hjelp til virksomhetenes risikovurdering for hvordan eID på betydelig nivå kan benyttes i tjenesteproduksjon.

2) Realisering av en offentlig utstedt eID på sikkerhetsnivå høyt skal vurderes. Av hensyn til at mange brukere av ulike grunner ikke har tilgang til dagens markedsbaserte eID-er, samt offentlig sektors sårbarhet og dagens konkurransesituasjon, er det viktig å vurdere nærmere tiltak som kan bidra til å løse disse utfordringene. Det tas derfor sikte på å vurdere å realisere en offentlig eID på sikkerhetsnivå høyt. En offentlig utstedt eID på sikkerhetsnivå høyt vil være meget viktig for å nå målet i Digitaliseringsstrategien om *at alle innbyggere som har evne til det, skal kunne kommunisere digitalt med offentlig sektor*. Løsningen vil både være et supplement til de private utstedte eID-ene BankID, Buypass og Commfides, og et alternativ for de som ikke har en eID på høyeste sikkerhetsnivå fra før. Det tas sikte på at alle folkeregistrerte personer hvor det foreligger en entydig knytning til deres fødsels- eller d-nummer skal ha mulighet til å skaffe seg en eID på sikkerhetsnivå høyt. Når øvrige prosesser i identitetsforvaltningen muliggjør dette, kan et

[37] Kommunal- og moderniseringsdepartementet, *Én digital offentlig sektor*, 2019, tilgjengelig her.
[38] Dette innebærer at alle personer som er registrert i Folkeregisteret og hvor det foreligger en entydig knytning til deres fødsels- eller d-nummer skal ha mulighet til å skaffe seg en eID på sikkerhetsnivå høyt.

eventuelt krav om status «unik» for identitetsnummeret som legges til grunn for utstedelsen vurderes[39]. Det tas videre sikte på at en offentlig utstedt eID på sikkerhetsnivå høyt skal kunne støtte innlogging på et lavere sikkerhetsnivå på en brukervennlig måte.

Det eksisterer flere mulige tilnærminger for å realisere en eID på sikkerhetsnivå høyt, hvor både ulike anskaffelsesmodeller, markedssituasjon, teknologisk utvikling og offentlig sektors gjennomføringsevne må utredes nærmere. Det vil være viktig å velge en tilnærming som sikrer at det nås ut til brukerne som ikke har en eID på sikkerhetsnivå høyt i dag. Revisjonen av eIDAS-forordningen, slik nærmere beskrevet i kapittel 2.3, kan også legge føringer for gjennomføringen av tiltaket. Det vil antagelig være behov for lovfesting dersom en offentlig utstedt eID skal kunne tas i bruk også for innlogging til private brukersteder.

3) *Utbredelse blant brukergruppene som ikke har en eID på sikkerhetsnivå høyt i dag skal vurderes.* Realisering av en offentlig utstedt eID forutsetter at det lages en utbredelsesplan for relevante brukergrupper. Dette skal skje i tett dialog med relevante offentlige organer og markedsaktørene for eID. Spesielt viktig blir det at alle unge kan få en offentlig utstedt eID på nivå høyt. Det skal vurderes om og hvordan et tett samarbeid med utdanningssektoren og Feide kan bidra til å nå dette målet.

4) *Alle brukergrupper skal ha kunnskap om hvordan de får og bruker en eID.* Et målrettet og tilpasset opplæringstilbud er viktig for å realisere målet om å legge til rette for en eID til alle relevante brukergrupper. Det vurderes om veilednings- og opplæringstilbudet kan knyttes til oppfølging av strategien *Digital hele livet*[40]. Tilbudet skal gjelde både markedsbaserte og offentlig utstedte eID-er og være tilpasset endrede behov gjennom ulike livsfaser, eksempelvis målrettet veiledning til unge og eldre brukere. Tiltaket kan for eksempel inkludere veiledning og råd for å forhindre digitalt ID-tyveri og misbruk. Opplæringstilbudet vil bli utviklet i samarbeid med sektorene og vil være del av et generelt digitalt opplærings- og veiledningstilbud.

5) *Beste praksis og behov for sikker kommunikasjon mellom ulike sektorer og unge brukere, primært under 12 år, skal utredes.* Utredningen skal gi en bedre forståelse for behov som unge brukere har for sikker kommunikasjon og samhandling med det offentlige for ulike formål, uavhengig av om de har en eID eller ikke. Det finnes flere tilfeller der sikker og god utveksling av informasjon med ulike sektorer uten foresattes involvering er nødvendig. I all hovedsak må trolig løsningene for sikker kommunikasjon utvikles per sektor. Tiltaket innebærer utforming av veiledning og beste praksis for hvordan slike løsninger kan utformes. Dersom utredningen viser behov for fellesfunksjonalitet i løsninger på tvers av sektorer, utredes en slik fellesløsning.

6) Sikre og brukervennlige fullmaktsløsninger som muliggjør tilgang til offentlige tjenester på vegne av en annen bruker skal vurderes. Dette er nødvendig for å sikre at brukere som i dag ikke kan, eller har utfordringer med å benytte offentlige digitale tjenester, kan utøve sine rettigheter og

[39] Se kapittel 2.6 og 3.2 for øvrig beskrivelse av «unik».
[40] Kommunal- og moderniseringsdepartementet, *Digital hele livet*, 2021, tilgjengelig her.

plikter i samfunnet digitalt. Tiltaket forenkler en allerede utfordrende hverdag for de aktuelle brukerne og deres pårørende eller verger. Tiltaket innebærer også utarbeidelse av konkrete løsninger for brukerstyrte fullmakter og representasjon, eksempelvis for fremtidsfullmakt, henting av medisiner og innsyn i helseopplysninger. Det må legges til rette for fullmaktsløsninger som gir informasjon om og hvordan en fullmakt er benyttet. Det skal arbeides trinnvis for å etablere fullmaktsløsninger for å sikre realisering av løsninger som treffer en bred andel av befolkningen.

7) *Brukervennlig eID til brukere uten fødsels- eller d-nummer skal utredes*. Utredningen skal gi bedre forståelse av hvordan en eID skal fungere for utenlandske personer med tilknytning til Norge som ikke kvalifiserer for fødsels- eller d-nummer.

Regjeringen vil:

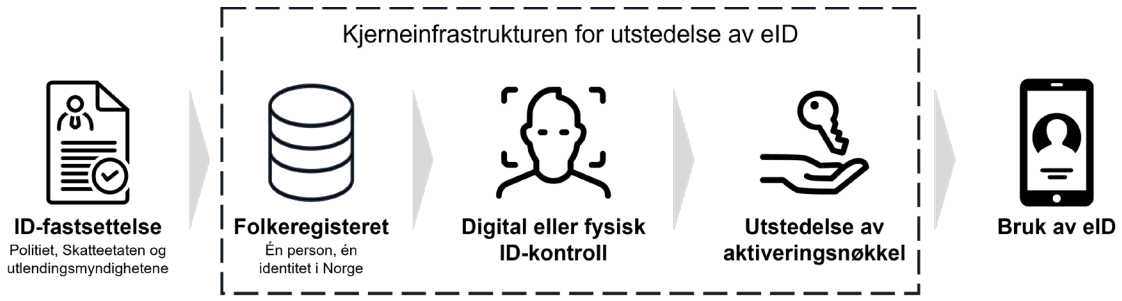
- videreutvikle MinID for å bli mer robust og brukervennlig
- vurdere å realisere en offentlig utstedt eID på sikkerhetsnivå høyt
- vurdere utbredelse av en offentlig utstedt eID på sikkerhetsnivå høyt blant brukergruppene som ikke har en eID på sikkerhetsnivå høyt i dag
- at alle brukergrupper skal ha kunnskap om hvordan de får og bruker en eID
- utrede beste praksis og behov for sikker kommunikasjon mellom ulike sektorer og unge brukere, primært under 12 år
- vurdere sikre og brukervennlige fullmaktsløsninger som muliggjør tilgang til offentlige tjenester på vegne av en annen bruker
- utrede brukervennlig eID til brukere uten fødsels- eller d-nummer

3.2. Mål 2: Løsning for innlogging og bruk av offentlige digitale tjenester skal være sikker, kostnadseffektiv og helhetlig

Dagens situasjon

ID-porten og eID-ene som benyttes for tilgang til digitale offentlige tjenester har god robusthet, meget god oppetid, god teknisk kvalitet og er motstandsdyktige for angrep og svindel. Løsningene anses som brukervennlige fra de store brukergruppene. Det er riktignok enkelte utfordringer relatert til utstedelse og bruk.

I dag består kjerneinfrastrukturen for utstedelse av eID i hovedsak av tre deler: Folkeregisteret, gjennomføring av ID-kontroll og selve utstedelsen av en aktiveringsnøkkel. En god kjerneinfrastruktur innebærer blant annet god kvalitet på grunnleggende identitetsinformasjon i Folkeregisteret, samt sikker og effektiv fysisk eller digital ID-kontroll[41] og utstedelse av aktiveringsnøkkel for å ta eID i bruk. I all hovedsak fungerer kjerneinfrastrukturen for utstedelse av eID godt, men det er enkelte utfordringer som må adresseres.



Figur 7: Kjerneinfrastruktur for utstedelse av eID

I dag kan det forekomme at en person tildeles mer enn ett identitetsnummer. Risikoen for dette er størst ved tildeling av identitetsnummer til utenlandske borgere. Dette er en grunnleggende utfordring for utstedelse av eID som kan gjøre det mulig for en person å få flere eID-er i ulike identiteter, såfremt personen har ulike ID-bevis som viser en entydig kobling til de ulike identitetsnumrene. God kvalitet i Folkeregisteret er dermed en viktig forutsetning for arbeidet med eID, slik også nærmere forklart i kapittel 2.6. Det innebærer at én person må ha én registrering i Folkeregisteret og at informasjonen til enhver tid er oppdatert. Dette understøtter målet for ID-forvaltningen, *én person, én identitet i Norge.* Folkeregisteret har nylig blitt modernisert. Blant annet er det tilrettelagt for registrering av «unike» identiteter, som vil heve kvaliteten i registeret[42]. Dette forutsetter en kontroll i justissektorens biometriregistre som er under planlegging. Folkeregisteret er i dag i begrenset grad tilrettelagt for identitetsmatching[43] eller oppdatering av profilinformasjonen til utenlandske identiteter.

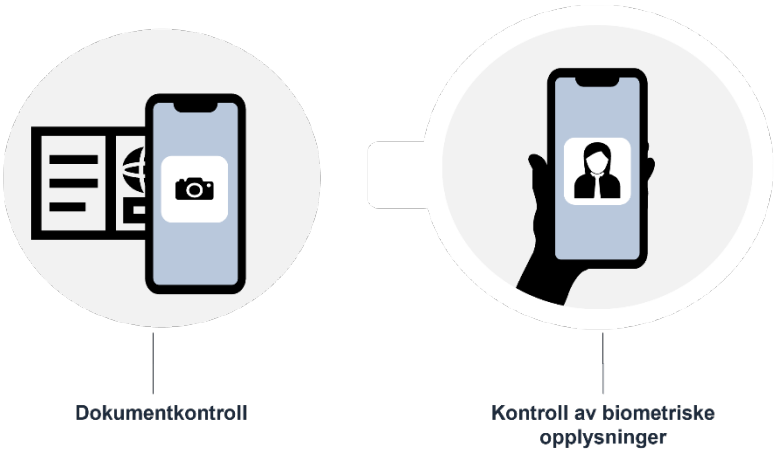
[41] En digital ID-kontroll innebærer en teknisk løsning som sjekker brukerens biometri opp mot bildet lagret i brukerens pass eller nasjonale ID-kort, enten tilknyttet en utstedelsesprosess eller tilknyttet bruk av en eID eller tjeneste.
[42] Se faktaboks kapittel 2.6 for nærmere beskrivelse av «unike» identiteter.
[43] Evne til å kunne koble en utenlandsk identitet mot en norsk identitet personen allerede har.

ID-kontroll, enten digital eller fysisk, er en annen viktig del av kjerneinfrastrukturen for utstedelse av eID. Som forklart i kapittel 2.5 og 2.6, kan fysisk ID-kontroll tilknyttet utstedelse av eID gjennomføres enten av banker, via arbeidsgiver eller gjennom en tjeneste fra Posten. Med dagens regelverk skal det sikres en identifikasjon som skal gi entydig kobling til folkeregistrert person. Dagens tilnærming er brukervennlig, men det kan være utfordringer med å ivareta sikkerheten fordi det er krevende å sikre at alle oppmøtestedene der en bruker kan motta en eID har tilstrekkelig kompetanse på ID-kontroll. Samtidig eksisterer det lite dokumentasjon av sikkerhetsbrudd direkte relatert til ID-kontrollen ved utstedelse av en eID. Politiet og Skatteetaten utfører ID-kontroll tilknyttet andre prosesser i ID-forvaltningen med ansatte med høy kompetanse på ID-kontroll. Utstedelse av pass og nasjonale ID-kort til norske borgere, og kommende ID-kort til utlendinger, samt arbeidet med «unik» vil styrke forutsetningene for å sikre en entydig kobling til folkeregistret person.

Det er videre en utfordring at det kreves tilgang til et stort fysisk distribusjonsnett for å kunne gjennomføre ID-kontroll, som er en forutsetning for å kunne utstede eID-er til brukere. Dette kan således være en barriere for aktører som ønsker å etablere seg i markedet. Dette medfører at det er en fare for at dagens løsning for ID-kontroll hindrer tilstrekkelig konkurranse i markedet. Videre kan flere infrastrukturer for ID-kontroll ha negativ innvirkning på både samlet kostnadseffektivitet og sikkerhet. Tilknyttet dette pekte områdegjennomgangen av ID-forvaltningen på at det er lite samfunnsøkonomisk å etablere parallelle infrastrukturer med duplisert informasjon eller relativt lav brukermasse, samt at ID-kontrollene i ID-forvaltningen burde gjenbrukes. Behovsanalysene viser videre at det er flere aktører som peker på at ID-kontroll tilknyttet utstedelse av eID-er bør være et offentlig ansvar, særlig med tanke på å ivareta kvaliteten på ID-kontrollen og tilhørende kobling til identitetsinformasjon i Folkeregisteret. Gjenbruk av politiets skrankepunkt for pass og ID-kort for ID-kontroll for eID er også pekt på som en mulig løsning[44].

Det er ikke utstrakt bruk av digital ID-kontroll for utstedelse og bruk tilknyttet eID i dag, selv om teknologien finnes. En løsning for digital ID-kontroll innebærer at en persons identitet kan kontrolleres på en sikker måte uten at brukeren må møte opp fysisk. Slik vist i figuren under består en digital ID-kontroll av to deler, en dokumentkontroll og kontroll av biometriske opplysninger. Ved hjelp av en applikasjon på en smarttelefon gjennomføres først en dokumentkontroll av et ID-dokument, slik som et pass eller nasjonalt ID-kort. Eksempelvis kontrolleres gyldighet av ID-dokumentet og om det er meldt tapt eller stjålet. Deretter gjennomføres en kontroll av biometriske opplysninger ved hjelp av kameraet på smarttelefonen, hvor personens ansiktsfoto kontrolleres mot ansiktsfoto som er lagret i ID-dokumentet. Digital ID-kontroll ble blant annet brukt tilknyttet MinID Passport, en løsning som benyttes for utenlandske brukere i koronapandemien. Løsninger for digital ID-kontroll kan benyttes både i utstedelsesprosessen av eID, for bruk av eID, for ID-kontroll i andre digitale prosesser i offentlig sektor eller som et hjelpemiddel ved ID-kontroll av en bruker ved et fysisk oppmøtested. Det er viktig med god kvalitet og sikkerhet i digital ID-kontroll slik at de eksempelvis er motstandsdyktige mot presentasjonsangrep.

[44] Finansdepartementet, *Områdegjennomgang av ID-forvaltningen*, 2019, tilgjengelig her og her.



Figur 8: Illustrasjon av digital ID-kontroll

Behovsanalysene har vist at flere offentlige virksomheter har behov for sikre og brukervennlige løsninger for å gjennomføre digital ID-kontroll, også utover ID-kontroll relatert til utstedelse og bruk av eID. Et eksempel er NAV, som blant annet må innhente leveattester fra personer bosatt i utlandet for å sikre at ytelser blir utbetalt til riktig mottaker. En brukervennlig og sikker løsning for digital ID-kontroll vil i et slikt tilfelle øke sikkerheten, i tillegg til å gjøre prosessen enda mer effektiv og brukervennlig både for bruker og tjenesteeier. Slik beskrevet i kapittel 2.6 og 3.4, kan det være en utfordring med misbruk av eID i nære relasjoner. En løsning for digital ID-kontroll vil kunne redusere omfanget av misbruk i nære relasjoner, da det kan gjennomføres en kontroll av brukerens biometriske opplysninger når eID-en benyttes.

Ambisjon og tiltak

Den offentlige kjerneinfrastrukturen for utstedelse av eID skal videreutvikles for økt sikkerhet og kostnadseffektivitet på lengre sikt. Offentlig sektor skal i større grad kunne tilby ID-kontroll som eID-leverandører kan benytte for å utstede eID til brukere. Den felles kjerneinfrastrukturen skal understøtte markedsbaserte eID-er og sektorløsninger. Videre skal Norges eID-infrastruktur være robust og skalerbar.

For å realisere ambisjonene ovenfor er det behov for fem tiltak:

1) Det legges til rette for at «unike» identiteter kan realiseres i Folkeregisteret. For arbeidet med eID er det avgjørende at hver person kun er registrert én gang i Folkeregisteret. Det tverrgående arbeidet med «unik» bør dermed sluttføres. Når «unike» identiteter er etablert, kan en person kun knytte eID-er til én identitet i Norge og et eventuelt krav om «unik» tilknyttet utstedelse av eID-er kan vurderes. Kravet vil også kunne gjelde markedsbaserte eID-er. Identitetskontroll ved utstedelse av eID må fortsatt sikre utstedelse til rett person med unikt identitetsnummer.

2) *Det skal sørges* for at *staten skal på en sikker måte kunne koble en identitet fra utlandet mot en norsk identitet som brukeren allerede har*. En slik identitetsmatching er nødvendig for å gjenkjenne brukere fra utlandet og koble utenlandske identiteter til identiteter i Folkeregisteret.

Arbeid med korrekte og oppdaterte personopplysninger på disse brukerne, uten at det forringer kvaliteten i Folkeregisteret, vil være en del av arbeidet. Kommisjonens lovforslag til revisjonen av eIDAS-forordningen innebærer et forsterket lovkrav i tilknytning til dette. Tiltaket vil legge til rette for at EØS-borgere i større grad kan benytte en eID fra deres hjemland for å få tilgang til norske offentlige digitale tjenester.

3) Det skal legges til rette for at offentlig sektor evner å gjennomføre ID-kontroll digitalt og gjennom personlig oppmøte som oppfyller kravene til sikkerhetsnivå høyt. Det skal etableres én felles teknisk infrastruktur for både personlig oppmøte og digital ID-kontroll for eID. Dette innebærer tekniske løsninger som kan benyttes til ID-kontroll i digitale prosesser og som hjelpemiddel til ID-kontroll ved fysiske oppmøtesteder. Infrastrukturen skal benyttes for utstedelse av eID, men skal også gjøres bredt tilgjengelig for tjenesteeiere som ønsker å benytte løsningen til andre tjenester på sitt område. Ved ID-kontroll for utstedelse av eID ved fysiske oppmøtesteder vil sikkerheten styrkes ved at eID med større sikkerhet utstedes til rett identitet. Tiltaket kan også muliggjøre ID-kontroll uten fysisk oppmøte. I bruk av eID kan infrastrukturen for digital ID-kontroll bidra til reduksjon i misbrukssituasjoner, eksempelvis tilknyttet misbruk i nære relasjoner eller innhenting av leveattester for utbetaling av ytelser fra NAV. I tillegg vil én felles infrastruktur for ID-kontroll bidra til forenkling for brukeren og reduserte inngangsbarrierer i eID-markedet. Politiets løsninger og tjenester som allerede er etablert skal være en del av vurderingsgrunnlaget

4) Grunnlaget for et markedsbasert samarbeid om kjerneinfrastruktur for utstedelse av eID til brukere skal utredes. Som tidligere nevnt, er kjerneinfrastrukturen tredelt og består av Folkeregisteret, gjennomføring av ID-kontroll og selve utstedelsen av en aktiveringsnøkkel. Det offentlige skal ta et større ansvar for kjerneinfrastrukturen for utstedelse av eID til brukere, hvor det eksisterer flere gjennomføringsmodeller og tilnærming. En tilnærming er å etablere et markedsbasert samarbeid som innebærer at flere samfunnsaktører samarbeider for å levere kjerneinfrastrukturen for eID, hvor overordnet ansvar og kontroll ligger hos det offentlige, mens eksempelvis ID-kontrollen fortsatt kan foretas av private aktører. En annen tilnærming vil innebære gjenbruk av ID-kontrollen foretatt i skrankepunktene til politiet eller Skatteetaten.

5) Den offentlige eID-infrastrukturen i Digitaliseringsdirektoratet skal videreutvikles for å bli mer sikker, robust og skalerbar. Som beskrevet i mål 1 skal det vurderes å etablere eID-løsninger som kan benyttes som gode alternativer til markedsløsningene. En modernisert MinID på styrket betydelig nivå vil kunne benyttes for tilgang til mange offentlige tjenester, med unntak av tjenester som innebærer taushetsbelagte opplysninger med særlig beskyttelsesbehov, slik som helseopplysninger. Videre er det viktig å styrke eksisterende fellesløsninger, spesielt ID-porten. Det skal være et sterkt fokus på å bygge inn informasjonssikkerhet i utviklingen av fellesløsningene.

Regjeringen vil

- legge til rette for at «unike» identiteter kan realiseres i Folkeregisteret
- sørge for at staten på en sikker måte kan koble en identitet fra utlandet mot en norsk identitet som brukeren allerede har

- legge til rette for at offentlig sektor evner å gjennomføre ID-kontroll digitalt og gjennom personlig oppmøte som oppfyller kravene til sikkerhetsnivå høyt for eID
- utrede grunnlaget for et markedsbasert samarbeid om kjerneinfrastruktur for utstedelse av eID til brukere
- videreutvikle en sikker, robust og skalerbar eID-infrastruktur i Digitaliseringsdirektoratet

3.3. Mål 3: Rammer for sikre og effektive løsninger for eID til offentlig ansatte skal være angitt

Dagens situasjon

Offentlige virksomheter har i mange tilfeller behov for autentisering av ansatte, både interne og eksterne, herunder ID-kontroll i forbindelse med ansettelser, tilgang til interne systemer, tilgang til eksterne systemer og for ekstern samhandling. I dag lager mange offentlige virksomheter sine egne løsninger for autentisering, tilgangsstyring, fullmakter og roller basert på egne behov. Det bygges gjerne opp en brukerdatabase med ansatte internt i virksomheten som viser hvilke ansatte som har tilgang til ulike systemer. I noen tilfeller hvor det har vært behov for sterkere autentisering har ID-porten blitt tatt i bruk for digitale tjenester i jobbsammenheng.

Enkelte sektorer, spesielt helsesektorens påloggingsløsning HelseID og utdanningssektorens eID-løsning Feide, har utviklet egne løsninger som kombinerer autentisering og autorisasjon for sine ansatte og andre tilknyttede personer. Dette er løsninger som har god utbredelse i sine respektive sektorer og som i hovedsak fungerer godt for ansatte i sektoren[45]. eIDAS-forordningen har også åpnet for at virksomhetsserfikater kan benyttes for å identifisere og ha tillit til aktørene i forbindelse med samhandling, i flere forskjellige infrastrukturer[46]. Det er flere utfordringer knyttet til bruk av slike sertifikater, da det vil være behov for et internt system for tilgang til slike, og det må også bevises at en person faktisk har handlet på vegne av virksomheten.

Behovsanalysene viser at brukere, særlig ansatte innen kommunal helse- og omsorgssektor, reagerer på at de må benytte sin private eID og mobiltelefon for å kunne autentisere og logge seg inn i jobbsammenheng. Det oppleves som uriktig og prinsipielt utfordrende at de selv må bære disse kostnadene for å kunne utføre arbeidet sitt. Behovsanalysen tydeliggjorde videre en etterspørsel etter å forenkle identifikasjons- og autentiseringsløsningene for ansatte i offentlig sektor, spesielt innen hele helse- og omsorgsektoren. Ansatte opplever at systemlandskapet er stort, komplekst og lite sammenhengende, hvilket fører til at de må logge seg inn og autentisere seg svært mange ganger per dag for tilgang til ulike systemer. Mange selvstendige innlogginger med privat eID på jobbrelaterte systemer oppleves som lite brukervennlig og ineffektivt. I tillegg opplever enkelte å få tilsendt arbeidsrelatert, konfidensiell digital post og dokumentasjon direkte til sin private Altinn-innboks. Det etterspørres derfor løsninger for ansatte i offentlig sektor som muliggjør innlogging som en bestemt rolle for å få riktige tilganger til systemer og dokumenter. Utover dette opplever flere i brukergruppen utfordringer knyttet til signering av avtaler i forbindelse med tjeneste- og varekjøp i offentlig sektor. I dag gjennomfører ansatte i offentlig sektor signering av avtaler med privat eID, altså som privatperson, uten at det er en direkte knytning til rollen den offentlige ansatte har i virksomheten. Antall innlogginger i jobbsammenheng har økt betydelig gjennom koronapandemien.

[45] Se kapittel 3.5 for ytterligere detaljering av HelseID og Feide.
[46] Utfordringsbildet ved bruk av virksomhetssertifikat tilgjengelig her

Digitaliseringsdirektoratet gjennomfører for tiden en pilotering av en løsning for ansattpålogging. Løsningen vil gi ansatte i offentlig sektor en sikker autentisering gjennom ulike eID-er, på samme måte som ID-porten gir digital tilgang for brukere til offentlige tjenester gjennom ulike eID-er. Løsningen skiller mellom bruk av eID i jobbsammenheng og i privat sammenheng, slik at det tydeliggjøres hva eID-en benyttes til.

Faktaboks: Pilotering av løsning for ansattpålogging i Digdir

En ansattpålogging er i praksis en kombinasjon av autentisering og autorisasjon. Gjennom en ansattpålogging skal man knytte personen som autentiserer seg sammen med virksomheten som vedkommende representerer, og eventuelt hvilke roller og rettigheter den ansatte skal ha på vegne av virksomheten. Løsningen for ansattpålogging som Digitaliseringsdirektoratet piloterer kan forklares slik:

- En frittstående løsning, basert på ID-porten, men med et eget brukergrensesnitt som gjør det markant forskjellig fra ID-porten. Det er ikke mulig å gå fra en tjeneste man har tilgang til som ansatt til en tjeneste man skal ha tilgang til som privatperson uten å logge inn på nytt.
- Kobling til ulike eID-leverandører. I piloten benyttes de samme eID-leverandørene som benyttes i ID-porten.
- Kobling til en autoritativ kilde. I piloten er denne kilden Altinn Autorisasjon[47], men også andre kan være aktuelle.

Ambisjon og tiltak

Det er en ambisjon at det skal etableres et tydelig skille mellom når en eID blir benyttet til private og jobbrelaterte formål for ansatte i offentlig sektor, hvor innloggingen skal være enkel og kostnadsfri for offentlige ansatte i jobbsammenheng. Offentlig sektor skal ha helhetlige løsninger som gjør det mulig å logge inn som en bestemt rolle for å få riktige tilganger til systemer og dokumenter.

For å realisere ambisjonene ovenfor er det behov for tre tiltak:

1) *Det skal fremmes beste praksis for å løse behov tilknyttet pålogging og tilgang til tjenester på jobb* for å imøtekomme etterspørsel hos virksomhetene og tilrettelegge for kostnadseffektiv oppgaveløsning. Tilgangsstyring bør løses så nærme kilden som mulig med løsninger som samspiller med nasjonale fellesløsninger. Dette innebærer at virksomhetene må ha ansvar for å bestemme hvilke ansatte som kan benytte en tjeneste innen deres virkeområde.

2) *Det bør etableres en teknisk løsning for pålogging i jobbsammenheng i offentlig sektor* for å møte brukerbehov. Løsningen skal inkludere funksjonalitet for at en bruker skal kunne benytte samme eID for jobb og private formål, men inkludere et teknisk skille mellom bruksområdene. Arbeidet skal bygge videre på erfaringer fra piloteringen av løsning for ansattpålogging via

[47] Altinn Autorisasjon er en løsning for tilgangsstyring til digitale tjenester, og gir mulighet for å styre hvem som skal kunne gjøre hva med hvilke data, i det offentlige og i samspillet mellom offentlig og privat.

Digitaliseringsdirektoratet og erfaringer fra sektorløsninger, slik som HelseID og Feide. Det skal vurderes nærmere øvrig funksjonalitet for løsningen, eksempelvis tilknyttet tilgangsstyring. Løsningen skal kunne benyttes av offentlige virksomheter og virksomheter som utfører oppgaver på vegne av det offentlige[48].

3) Retningslinjer, veiledning og råd tilknyttet bruk av eID i jobbsammenheng skal videreutvikles og implementeres. Det etterspørres tydelige fellesføringer og råd for hvordan offentlige virksomheter skal håndtere bruk av eID i jobbsammenheng for sine ansatte. I tråd med digitaliseringsstrategien for offentlig sektor[49], har Digitaliseringsdirektoratet utarbeidet en veileder[50] for bruk av eID i jobbsammenheng. Tiltaket innebærer å sørge for at veilederen blir implementert og videreutviklet, samt at konkrete råd og veiledning gis til virksomhetene. Veiledningsarbeidet må skje i samarbeid med sektorene, som har et eget ansvar for eventuell spesifikk veiledning innenfor egen sektor. Veiledningen skal videre dekke hvordan kostnader til eID i arbeidssammenheng skal dekkes av arbeidsgiver.

Regjeringen vil

- fremme beste praksis for å løse behov tilknyttet pålogging og tilgang til tjenester på jobb
- vurdere å etablere en teknisk løsning for pålogging i jobbsammenheng i offentlig sektor
- videreutvikle og implementere retningslinjer, veiledning og råd tilknyttet bruk av eID i jobbsammenheng

[48] Definisjon av alle virksomheter som kan bruke Digdir sine fellesløsninger er tilgjengelig i bruksvilkårene punkt 1.2, tilgjengelig her.
[49] Kommunal- og moderniseringsdepartementet, *Én digital offentlig sektor*, 2019, tilgjengelig her.
[50] Digitaliseringsdirektoratet, *Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor*, tilgjengelig her.

3.4. Mål 4: Løsninger skal være tilpasset markeds- og teknologiutviklingen

Dagens situasjon

Markedsituasjonen og muligheter innenfor teknologi har endret seg betydelig siden dagens eID-strategi ble etablert i 2008. I tillegg kan trussel- og sårbarhetsbildet endre seg raskt. Det er derfor viktig å følge med på endringer og muligheter innenfor teknologi og marked for å kontinuerlig kunne utvikle gode og sikre løsninger.

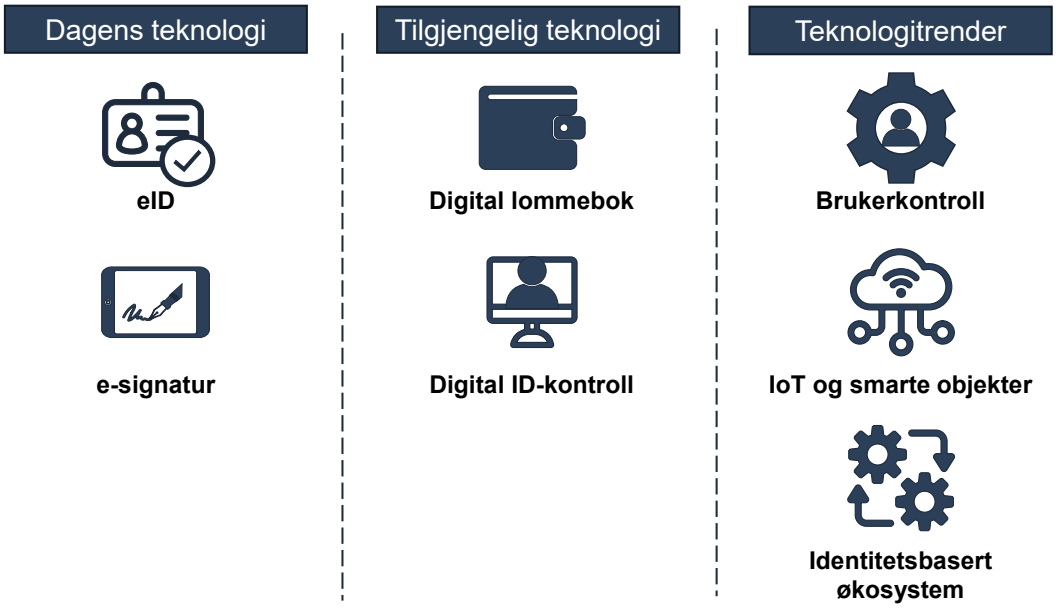
Selv om dagens eID-løsning baseres på teknologi som gir god beskyttelse, finnes det svakheter det er viktig å være klar over. Bruk av eID er spesielt utsatt for misbruk i nære relasjoner, eksempelvis ved at en eID benyttes av en ektefelle eller samboer etter avtale (i strid med reglene) og senere misbrukes til å for eksempel ta opp et lån. I tillegg er det en fare for at personer med enten språkbarrierer, lav digital kompetanse og/eller dårlig tilgang til digitale enheter oppsøker hjelp fra andre, som gjør at de er ekstra utsatt for å få misbrukt sin eID. Det er på de ovennevnte områdene at det erfares mest svindel og misbruk, og siden passord og kode i utgangspunktet er delt frivillig kan det være vanskelig å bevise om det er misbruk eller om det er rett person som bruker eID-løsningen[51]. Misbruk av eID kan gi finansielle institusjoner direkte tap[52], noe som fører til at spesielt finansnæringen har sterke insentiver til å sikre at rett identitet benytter eID-en. Det er uansett avgjørende at offentlige tjenesteeiere gjennomfører egne risikovurderinger og vurderer tiltak for hvordan eID brukes tilknyttet hver enkelt tjeneste.

Videre er tekniske løsninger for og tilknyttet eID en del av et globalt marked, som betyr at offentlig sektor sin tilnærming til eID påvirkes av valg gjennomført av internasjonale hardware- og softwareprodusenter. Dessuten, som beskrevet i kapittel 2.3, foregår det revisjon av regelverket i EU. Revisjonen vil kunne medføre tekniske og markedsmessige muligheter og begrensninger som det er viktig at offentlig sektor har god forståelse og innsikt i.

Det teknologiske landskapet har endret seg betydelig siden 2008. Figuren under oppsummerer teknologiutviklingen og viktige trender for eID-løsninger på globalt nivå.

[51] Det er utarbeidet tiltak mot svindel og misbruk av eID, i form av veiledning fra Digitaliseringsdirektoratet og aktører i næringen.

[52] I høyesteretts dom 22. oktober 2020, HR-2020-2021-A, ble en mann frifunnet for et erstatningskrav fremsatt av en bank som hadde utbetalt et forbrukslån på 100 000 kroner til personer som hadde misbrukt mannens BankID.



Figur 9: Utviklingen av eID[53]

I den venstre kolonnen i figuren over representeres teknologi som allerede er tatt i bruk og har høy utbredelse både i Norge og globalt, mens den midterste kolonnen representerer eksisterende teknologi som kan utnyttes bedre i eID-løsninger. Bruken av digitale lommebok-løsninger har økt i popularitet og utbredelse[54]. Den økende utbredelsen og etterspørselen etter digitale lommebok-løsninger kan ses i sammenheng med befolkningens økte bruk av mobile enheter og god dataoverføringskapasitet. Denne endringen gjør at prinsippet om «mobil først» i økende grad er sentral i utvikling av nye tjenester og løsninger. «Mobil først»-tilnærming handler om at nye digitale løsninger utvikles og designes for mobile enheter først, før de tilpasses til nettlesere eller andre applikasjoner.

Videre har den teknologiske utviklingen kommet langt innenfor biometri, noe som muliggjør digital ID-kontroll. Da kan brukerens biometri sammenliknes med bildet i brukerens pass eller nasjonale ID-kort, uten at det er nødvendig med personlig oppmøte og fysisk legitimering. Selv om feltet fremdeles er under utvikling, er teknologien tilstrekkelig moden for å kunne tas i bruk på en trygg måte i nye løsninger. Biometrisk teknologi kan forenkle brukeropplevelsen og vil kunne bidra til å øke sikkerheten knyttet til eID-løsninger.

I den høyre kolonnen i figuren illustreres globale teknologitrender som er av betydning for utviklingen av eID-løsninger. Prinsippet om at brukeren skal ha kontroll over sin digitale identitet blir i økende grad sentralt. Digital teknologi gir mange fordeler, men det eksponerer også brukere for sikkerhetstrusler. Når vi deler mer data, øker risikoen for misbruk. Det er derfor økt fokus på at brukerne selv skal få større kontroll over hvilke data som deles med hvilke aktører. Dette prinsippet vil være sentralt i utvikling av eID-løsninger, spesielt i forbindelse med en potensiell

[53] Tilpasset fra Gartner: *Debunking 4 Myths Around Citizen Digital Identity*.
[54] Se kapittel 2.3 for nærmere beskrivelse av digital lommebok.

lommebok-løsning. Videre vil IoT[55] og smarte objekter være en trend som må hensyntas i utvikling av eID-løsninger. eID-løsninger må i større grad enn tidligere forholde seg til den fysiske verden og samhandle med andre enheter, som for eksempel sensorer, programvare eller annen elektronikk. Dessuten må eID-løsningene fungere i et felles digitalt økosystem[56] og understøtte infrastrukturen vi har for digitale tjenester.

Ambisjon og tiltak

Norge skal fortsatt være et foregangsland når det gjelder digitalisering, også når det gjelder løsninger for eID. Et robust kompetansemiljø for eID skal følge markeds- og teknologiutviklingen tett og være en aktiv bidragsyter i europeisk utviklings- og standardiseringsarbeid. I tillegg er det viktig å arbeide med jevnlige risiko- og sårbarhetsvurderinger av eID-løsningene. Videre skal tilsynsmyndigheten sørge for sikre og robuste løsninger.

For å realisere ambisjonene ovenfor er det behov for ett tiltak:

1) *Sørge for tilstrekkelig kapasitet og kompetanse hos fagdirektorat og tilsynsmyndighet som følge av omfattende utvikling av teknologi, regelverk og marked på eID-området*. Digitaliseringsdirektoratet må kunne følge europeisk og global regelverks-, markeds- og teknologiutvikling, blant annet for å kunne gjennomføre gode risiko- og sårbarhetsvurderinger for forvaltningen. Selv om dagens løsninger baseres på teknologi som gir god beskyttelse og fungerer godt under gjeldende rammer, kan dette endre seg raskt. Offentlig sektor må forstå dagens og fremtidig risiko- og sårbarhetsbilde, samt følge opp tiltak for å redusere identifiserte risiko og sårbarheter. Vurderingene skal gjennomføres i samarbeid med andre relevante aktører i forvaltningen, og det er viktig at hele verdikjeden fra ID-fastsettelse, utstedelse og bruk av eID vurderes. Kompetansemiljøet skal være en aktiv bidragsyter i ulike ekspert- og arbeidsgrupper. Det er videre viktig å sørge for at Nasjonal kommunikasjonsmyndighet har ressurser til å følge markeds- og teknologiutviklingen, slik at tilsynet kan sikre at eID-leverandørene overholder regelverket.

Regjeringen vil

- sørge for tilstrekkelig kapasitet og kompetanse hos fagdirektorat og tilsynsmyndighet som følge av omfattende utvikling av teknologi, regelverk og marked på eID-området

[55] Tingenes internett (IoT) er nettverket av gjenstander som kan kommunisere med hverandre og med internett, ved hjelp av sensorer og nettilkobling.
[56] I økosystem for nasjonal digital samhandling og tjenesteutvikling er det felles IKT-løsninger og offentlige, private og frivillige virksomheter som til sammen utgjør økosystemet (Digitaliseringsdirektoratet, *Felles økosystem*, tilgjengelig her).

3.5. Mål 5: Samordningen av eID-utviklingen mellom sektorene og forvaltningsnivåer skal være kostnadseffektiv og god

Dagens situasjon

Det er i dag god utbredelse av de nasjonale fellesløsningene. I tillegg finnes sektorløsninger for eID som fungerer godt og har høy utbredelse, eksempelvis Feide for brukere og ansatte i utdanningssektoren og HelseID for helse- og omsorgsektoren.

Faktaboks: Feide

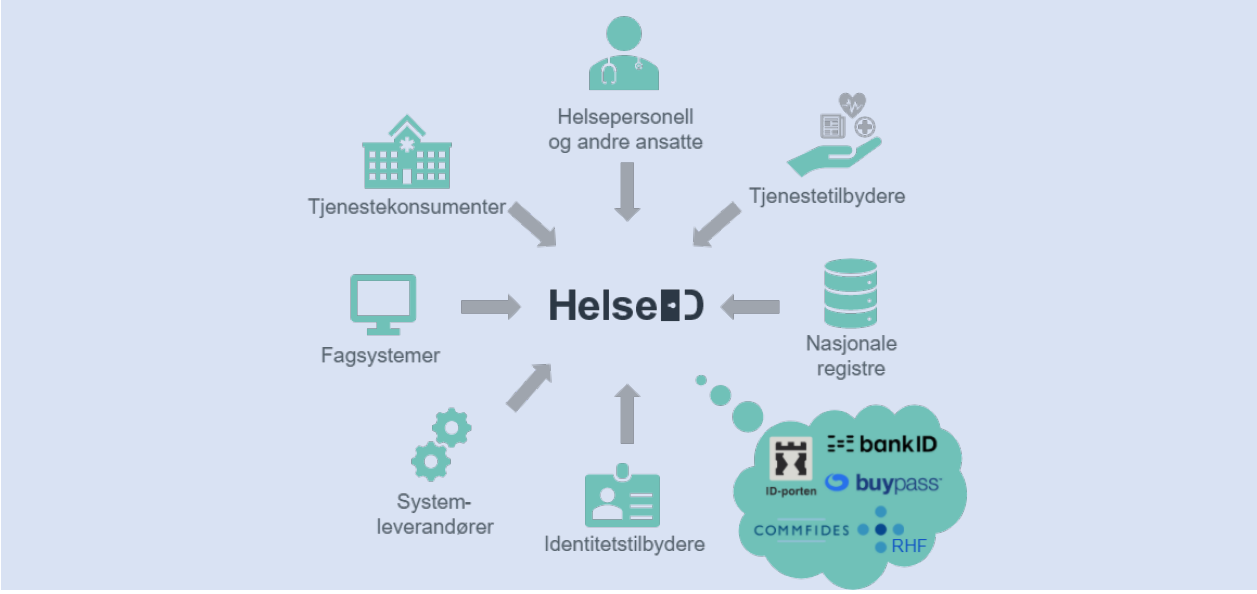
Feide[57] er den nasjonale løsningen for innlogging og datadeling i utdanning og forskning. Feide leveres av kunnskapssektorens tjenesteleverandør (Sikt) som samarbeider med Utdanningsdirektoratet om forvaltningen av tjenesten. Feide tillater studenter, forskere, elever, lærere, administrativt ansatte og andre tilknyttede personer i utdanningssektoren å logge seg inn og få tilgang til ulike digitale tjenester ved hjelp av kun én innlogging med passord og brukernavn. Feide har ikke gjennomført selvdeklarering av sin eID-løsning. Feide tilbyr også sterk autentisering for løsninger tilknyttet ansatte.

Per januar 2022 er det over 1 100 digitale tjenester som en kan logge på gjennom Feide direkte. I tillegg kan en logge seg på rundt 3 000 tjenester gjennom Feides kobling til den internasjonale utdanningsføderasjonen eduGAIN. I løpet av 2021 har Feide hatt 210 millioner innlogginger.

Faktaboks: HelseID

HelseID[58] er en felles påloggingsløsning for helse- og omsorgssektoren. Løsningen legger til rette for enklere pålogging for helsepersonell, og styrket informasjonssikkerhet ved digital samhandling i sektoren. HelseID benyttes både for brukerpålogging og for system-til-systemkommunikasjon.

[57] Nærmere beskrivelse av Feide er tilgjengelig her
[58] Nærmere beskrivelse av HelseID er tilgjengelig her



Figur 10: Overordnet beskrivelse av HelseID

Kommunene utgjør en stor andel av brukerne i ID-porten. I dag er 354 kommuner brukere av ID-porten, som tilsvarer en utbredelse på nærmere 100 prosent. Disse brukes til mange ulike typer tjenester, slik som innlogging for foresatte i skoler og barnehage og mange ulike skjematjenester. Totalt utgjør dette 3 500 tjenester, som tilsvarer omtrent 44 prosent av de 8 000 tjenestene som benytter ID-porten. De aller fleste kommunene er relativt små brukere og tjenestene de benyttes til er relativt like mellom ulike kommuner. ID-porten er således et viktig virkemiddel i digitalisering av kommunal tjenesteproduksjon.

Utover Feide, HelseID og tjenester i kommunene som benytter ID-porten, eksisterer det flere mindre innloggingsløsninger. Eksempelvis har flere kommuner og helseforetak laget eller anskaffet egne innloggings- eller eID-løsninger med relativt lav brukermasse, som medfører noen utfordringer. For det første er mindre løsninger med liten brukermasse lite kostnadseffektive å anskaffe og forvalte. Dessuten kreves det ofte flere mindre løsninger for å dekke det samlede behovet for en kommune eller enkeltsektor. I tillegg er det også utfordringer knyttet til å sikre tilstrekkelig brukervennlighet og sikkerhet i disse løsningene. Det har de siste årene vært økt utskiftelse av mindre eID-løsninger til fordel for de nasjonale fellesløsningene eller velfungerende sektorløsninger, men det gjenstår fremdeles en del mindre løsninger i flere kommuner og enkeltsektorer. Enkelte sektorløsninger blir også forespurt av tjenesteeiere til bruksområder utenfor egen sektor. Eksempelvis er det enheter utenfor kunnskap og utdanning som ønsker å ta i bruk Feide. Behovsanalysene har vist at flere tjenesteeiere etterspør tydeligere og mer klargjort sammenheng og økt samordning mellom sektor- og fellesløsninger.

Aktørene i frivillig sektor har uttrykt et ønske om å kunne benytte seg av offentlig sektors fellesløsninger. Behovet har økt fordi frivillig sektor ofte utfører samfunnsoppdrag som komplementerer eller støtter opp under områder som tradisjonelt har vært et offentlig ansvar.

Ambisjon og tiltak

Det må bygges videre på velfungerende sektorløsninger med klargjorte grensesnitt til nasjonale fellesløsninger. Sammenhengen mellom sektorspesifikke løsninger og nasjonale fellesløsninger skal videreutvikles med minimal overlapp mellom løsninger. Videre skal det legges til rette for å øke utbredelsen av nasjonale fellesløsninger.

For å realisere ambisjonene ovenfor er det behov for tre tiltak:

1) Sammenhengen mellom sektorspesifikke løsninger og nasjonale fellesløsninger for eID skal klargjøres og videreutvikles. Grensesnittet skal være tydelig og det skal være minst mulig overlapp mellom løsningene. I denne sammenheng er det spesielt behov for å klargjøre grenseflatene og potensielle sammenhenger mellom ID-porten, løsninger i kommunal sektor, Feide og HelseID. Dette vil bidra til å sikre at det ikke etableres dupliserte løsninger.

2) *Feide skal videreutvikles som en løsning for brukere og ansatte i kunnskapssektoren.* Velfungerende sektorløsninger skal bygges videre på. Feide har en tydelig rolle innenfor kunnskapssektoren og fungerer godt til tiltenkte formål. Feide skal, gjennom bruk av ID-porten, tilby autentisering på nivå betydelig og høyt til alle aktuelle brukersteder i Feide.

3) *Det skal legges til rette for å øke bruken av eID som tilbys i ID-porten, spesielt i kommunene*. Dette innebærer å stimulere kommunene til å ta i bruk nasjonale fellesløsninger, slik som spesielt ID-porten, i stedet for egne mindre eID-løsninger. Det er flere fordeler med å benytte fellesløsninger. Kostnadene fordeles på flere brukersteder, slik at enhetskostnadene vil kunne reduseres. Dessuten vil det være enklere å opprettholde god sikkerhet og brukervennlighet tilknyttet løsningene. Fordelene ved å benytte seg av nasjonale fellesløsninger framfor mindre eID-løsninger må kommuniseres og realiseres i praksis. Samarbeid med Kommunesektorens organisasjon (KS) blir et viktig virkemiddel.

4) *Forutsetninger for å gjøre fellesløsningene for eID tilgjengelig for deler av frivillig sektor skal utredes nærmere*. Et slik tiltak vil eventuelt blant annet innebære å gjøre ID-porten tilgjengelig for frivillig sektor på lik linje med slik det er i offentlig sektor i dag.

Regjeringen vil

- videreutvikle og klargjøre sammenhengen mellom sektorspesifikke løsninger og nasjonale fellesløsninger for eID
- videreutvikle Feide som en løsning for brukere og ansatte i kunnskapssektoren
- legge til rette for å øke bruken av eID som tilbys i ID-porten, spesielt i kommunene
- utrede forutsetninger for å gjøre fellesløsninger for eID tilgjengelig for deler av frivillig sektor

4. Økonomiske og administrative konsekvenser

Som utgangspunkt vil oppfølging av tiltakene i strategien i stor grad skje gjennom etatenes ordinære utviklingsarbeid, og finansieres innenfor gjeldende budsjettrammer. Enkelte tiltak vil medføre økonomiske og administrative konsekvenser. Tiltak med budsjetteffekter vil bli vurdert i den ordinære budsjettprosessen. Hvorvidt og eventuelt når disse tiltakene kan gjennomføres avhenger dermed av det økonomiske handlingsrommet og utfallet av prioriteringene i de årlige budsjettfremleggene.

Kommunal- og distriktsdepartementet har det overordnede ansvaret for å følge opp eID-strategien. Gjennomføringen av tiltakene i strategien forutsetter et tverrsektorielt samarbeid mellom departementer, statlige virksomheter, kommunesektoren, private aktører og frivillige organisasjoner. Strategiens mål og tiltak skal følges opp med en handlingsplan. I handlingsplanen vil økonomiske og administrative konsekvenser av tiltak, ansvarlige departementer og virksomheter, samt frister bli utdypet. Dette gjelder særlig det videre arbeidet med en offentlig eID på sikkerhetsnivå høyt som er omtalt under mål 1. Mål 2, om å etablere en sikker og kostnadseffektiv helhetlig løsning for innlogging og bruk av ulike typer offentlige digitale tjenester, vil også medføre økonomiske og administrative kostnader som må ytterligere utredes.

De økonomiske og administrative konsekvensene av tiltakene i strategien kan fordeles mellom kostnader forbundet med utvikling, drift og tilsyn. Det er nødvendig å skille mellom to faser når det gjelder økonomiske og administrative konsekvenser av tiltakene i strategien. Første fase er knyttet til selve gjennomføringen av tiltakene, mens den andre og viktigste fasen gjelder de langsiktige virkningene av tiltakene.

- Strategiens tiltak forutsetter etablering av en ny infrastruktur som kan håndtere videre fremtidig vekst i bruken av Digitaliseringsdirektoratets fellesløsninger, slik som modernisering og videreutvikling av MinID, videreutvikling av ID-porten, fullmaktsløsninger og utvikling av en løsning for pålogging i jobbsammenheng. Dette innebærer blant annet behov tilknyttet utvikling, etablering eller videreutvikling av nye løsninger, herunder teknisk infrastruktur, utviklerkapasitet, samt styrking av kapasitet for flere kompetanseområder i direktoratet. Det vil også kunne påløpe etableringskostnader i statlige virksomheter for å ta i bruk de nevnte fellesløsningene.
- Det må påregnes økte kostnader til drift og forvaltning som følge av økt ressursbehov og kompetanse i Digdir for å håndtere konsekvenser som økt bruk av nevnte fellesløsninger. Driftskostnader vil i tillegg inkludere kostnader tilknyttet utbredelse og drift av organisasjon som kan utstede en eID på sikkerhetsnivå høyt.
- Økte kostnader for å styrke tilsynsmyndighetens kompetanse og kapasitet til å følge markeds- og teknologiutviklingen og gjennomføre tilsyn som bidrar til sikre og robuste eID-løsninger må påregnes.

Det er krevende å måle alle direkte eller indirekte samfunnsøkonomiske konsekvenser av tiltakene i eID-strategien. Tiltakene vil samspille med andre politiske mål og hensyn som har bredere samfunnsmessige begrunnelser enn økt tilgang til digitale tjenester eller digitalisering av offentlig sektor for øvrig. Dette knytter seg for eksempel til mulighetene som bruk av eID på

sikkerhetsnivå høyt har for økt effektivisering av samfunnet som helhet, økt tillit til digitaliseringen hos virksomhetene og befolkningen, styrket informasjonssikkerhet, styrket personvern med videre. Det vil derfor ikke være mulig å fastslå konkrete anslag for hvor mye som kan spares eller effektiviseres som følge av implementering av strategien på nåværende tidspunkt. Samtidig vil en rekke av tiltakene redusere handlingsrommet for misbruk av eID og reduksjon i økonomisk kriminalitet vil således være en viktig ikke-prissatt nyttevirkning. Regjeringen antar imidlertid at summen av prissatte og ikke-prissatte nyttevirkninger vil utgjøre betydelige gevinster for departementene, for statlige virksomheter, kommunesektoren og samfunnet generelt. Samfunnsøkonomiske analyser av forventede gevinster og kostnader vil bli gjennomført som del av utarbeidelse av handlingsplanen.