Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

Produktstrategi for ID-porten 2020-2025

Forord

ID-porten er en nasjonal fellesløsning fra Digitaliseringsdirektoratet som leverer en sikker og enkel innloggingsløsning til offentlige tjenester på nett. ID-porten nyter stor tillit blant brukere og virksomheter i offentlig sektor, og bruken øker hvert år. Hver dag er det 450.000 innlogginger i ID-porten. Løsningen benyttes av over 800 virksomheter og 4 000 tjenester.

I 2018 ble ID-porten tildelt Rosing-prisen i kategorien IT-sikkerhet. Juryen pekte på at ID-porten siden oppstarten i 2008 har klart å tilpasse seg ny sikkerhetsteknologi og lagt til rette for å dekke nye og fremtidige behov for offentlige digitale tjenester. I dag kan innbyggerne som logger seg på, velge mellom fem alternative løsninger for elektronisk ID.

I løpet av 2020 skal Difi og Altinn samles til et nytt digitaliseringsdirektorat (Digdir). Regjeringens mål er at det nye direktoratet skal bidra til bedre og mer tilgjengelige offentlige tjenester, forenkling og økt verdiskaping for næringslivet og en enklere hverdag for folk flest. ID-porten er en hjørnestein i digitaliseringen av Norge, og er en viktig bidragsyter til å oppnå regjeringens mål. Skal ID-porten beholde denne viktige posisjonen, må vi være med på utviklingen - og helst ligge i front. Derfor er dette strategidokumentet viktig.

Mye er på gang. Vi har i 2019 lansert ID-portens "tvilling" - Maskinporten - som autentiserer virksomheter og gjør det enklere og tryggere å dele data. Mekanismene bygger på ID-porten og vil bidra til at det utvikles flere og nye sammenhengende tjenester på tvers, slik regjeringens digitaliseringsstrategi legger opp til.

ID-porten er blitt en viktig byggekloss for digitaliseringen av offentlig sektor og skal også fremover være et virkemiddel for å dekke forvaltningens behov for autentisering på en sikker, effektiv og brukervennlig måte. Denne produktstrategien for 2020-2025 peker ut mål og retning for arbeidet vi gjør for å utvikle ID-porten i årene som kommer.

Torgeir Strypet
Avdelingsdirektør, Digitale fellesløsninger

Innholdsfortegnelse

1 Sammendrag

ID-porten sin produktstrategi skal understøtte de teknologiske og samfunnsmessige endringene, mulighetene og utfordringene som beskrevet i bla. *Digital Agenda* og regjeringens digitaliseringsstrategi *Én digital offentlig sektor*, samt innmeldte behov. Samordning på tvers av forvaltningsnivåer og sektorer, og ivaretakelse av personvern og informasjonssikkerhet er avgjørende for å lykkes i digitaliseringsarbeidet i offentlig sektor.

ID-porten er en etablert nasjonal innloggingsløsning for offentlige og kommunale tjenester på nett. I 2018 var det totalt 139 419 010 innlogginger i ID-porten, og per september 2019 er det over 820 virksomheter og 4 000 tjenester som benytter løsningen.

Visjonen for ID-porten de neste fem årene er at den skal sikre digital forvaltning og tillit til fremtidens digitale tjenester fra det offentlige. Det skal skje gjennom å levere en robust og sikker løsning, at brukerne opplever høy brukskvalitet og tilgjengelighet, at ID-porten virker sammen med andre løsninger i et felles digitalt økosystem, og at den bidrar til en mer effektiv og innovativ offentlig sektor.

For å lykkes med dette peker denne strategien på fem overordnede mål med innsatsområder.

1) Dekke offentlig sektors behov for et nasjonalt tillitsanker
   Utviklingen av én digital offentlig sektor som leverer proaktive, sammenhengende tjenester til innbyggere, næringsliv og forvaltningen forutsetter bruk av digitale fellesløsninger. I dette digitale økosystemet har ID-porten en viktig rolle som tillitsanker for autentisering.
2) Dekke offentlig sektors behov for identifisering og autentisering av personer
   Ettersom det utvikles stadig flere digitale tjenester i offentlige virksomheter og kommuner, oppstår nye behov og bruksområder. ID-porten skal videreutvikles slik at løsningen dekker de nasjonale fellesbehovene for identifisering og autentisering av personer.
3) Dekke offentlig sektors behov for autentisering av virksomheter
   Utviklingen av nye og mer komplekse tjenester på tvers av forvaltningsnivåer og sektorer utfordrer den tradisjonelle bruken av virksomhetssertifikater bilateralt mellom virksomheter. ID-porten skal videreutvikles slik at den dekker offentlig sektors fellesbehov for autentisering av virksomheter på en måte som er enklere, sikrere og mer kostnadseffektiv.
4) ID-porten skal være en sikker autentiseringsløsning
   ID-porten må tilpasse seg ny sikkerhetsteknologi og ha gode sikkerhetsrutiner og prosesser for å opprettholde en sikker og robust autentiseringstjeneste. Alle sikkerhetsmekanismer skal være dokumenterte, evaluerte og åpne for revidering.

5) ID-porten skal være en brukerrettet autentiseringsløsning
   Regjeringens digitaliseringsstrategi peker på at brukeren skal kunne møte én offentlig sektor som leverer proaktive næringsliv- og innbyggertjenester. Som en nasjonal innloggingsløsning er det avgjørende at ID-porten oppleves som tilgjengelig, er enkel å bruke, gratis for innbygger og at løsningen bidrar til å skape tillit. Samarbeid med andre aktører er avgjørende for å bidra til at ID-porten når dette målet.

Teknologisk utvikling, politiske og samfunnsmessige endringer over tid kan medføre endrede rammevilkår knyttet til områder som berører ID-porten. Dette er forhold som må tas med i den samlede vurderingen av utviklingstiltak og prioriteringer frem mot 2025.

2 Innledning

Dette dokumentet beskriver ID-portens visjon de neste fem årene, og hvilken strategi som vil ligge til grunn for visjonen. Målgruppen for dokumentet er alle virksomheter som benytter ID-porten til autentisering av sine brukere, samt leverandører, styringsorgan og sluttbrukere av produktet.

Gjeldende produktstrategi for perioden 2015-2020 ble utarbeidet i 2014. Endringer i samfunnet, teknologi og rammeverk gjør det nødvendig med en revisjon av strategien. Formålet med arbeidet er å videreføre brukervennlig, sikker, robust og kostnadseffektiv anvendelse av e-ID til autentisering for offentlig sektor. Målet er at oppdatert produktstrategi skal være et langsiktig styringsdokument som gir en tydelig retning for videreutvikling av ID-porten som produkt, og et virkemiddel for at offentlig sektors behov for autentisering er dekket på en effektiv, brukervennlig og sikker måte. ID-porten skal også i nevnte periode være markedsbasert.

For å gjøre rede for hvilke føringer, muligheter og trusler som er gjeldene for å sette en strategisk retning, tar denne strategien utgangspunkt i behovene som ID-portens kunder og interessenter har meldt inn. Noen av behovene må adresseres og løses sammen med andre offentlige aktører eller med det private markedet, og andre må utredes videre.

Dette er ikke en strategi for digitalisering av offentlig sektor, men skal beskrive hvordan ID-porten frem mot 2025 skal understøtte de eksisterende strategiene for digitalisering av offentlig sektor. Disse beskrives blant annet i *Én digital offentlig sektor*[1]*, Digital Agenda for Norge*[2]*,* og presiseres i det årlige digitaliseringsrundskrivet. Produktstrategien tar utgangspunkt i gjeldende føringer slik de kommer frem i styringsdokumenter

2.1 Kort beskrivelse av ID-porten

ID-porten er en nasjonal innloggingsløsning for norske innbyggere som benytter offentlige tjenester på nett, og leverer sikker autentisering av sluttbrukere til over 820 offentlige virksomheter. Med ID-porten trenger ikke kundene å administrere brukernavn, passord eller brukerstøtte for egne innloggingsløsninger.

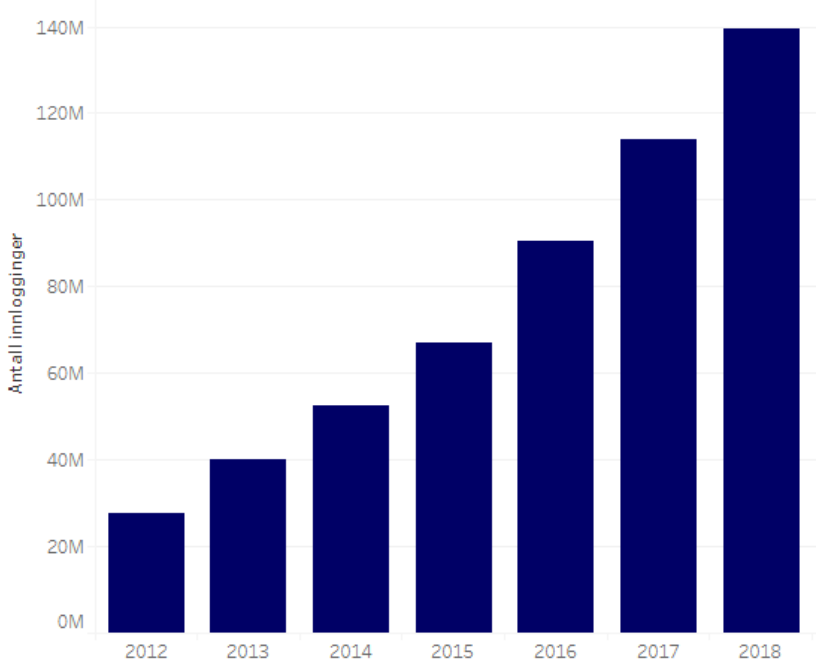
I tillegg til MinID har Digitaliseringsdirektoratet (Digdir) i dag avtale med markedsleverandører som leverer e-ID på høyeste sikkerhetsnivå i ID-porten. ID-portens kunder leverer tjenester til sluttbruker. Sluttbruker har et kundeforhold med leverandøren av den elektroniske identiteten (e-ID) de benytter. I dag omfatter dette BankID, BankID på mobil, Buypass,

[1] Én digital offentlig sektor - Digitaliseringsstrategi for offentlig sektor 2019–2025

[2] Meld. St. 27 (2015-2016) Digital Agenda

Buypass ID i mobil og Commfides. I tillegg er det mulig å benytte MinID, som tilbys av Digdir. Digdirs avtale med e-ID-leverandørene sikrer at sluttbruker kan benytte sin e-ID for å autentisere seg mot digitale tjenester levert av ID-portens kunder.

I 2018 var det totalt 139 419 010 innlogginger i ID-porten.



Figur 1 Antall innlogginger i ID-porten, per år

2.2 Avgrensninger

Denne strategien omhandler hvordan ID-porten skal utvikles som produkt og tjeneste. Det er ikke en strategi for hvordan den enkelte virksomhet skal ta i bruk ID-porten og tilpasse egne systemer, som er kundenes eget ansvar i samarbeid med Digdir. Strategien omhandler visjon, mål og innsatsområder, og er avgrenset til enkelte områder:

Tiltaks- og utviklingsplan
Strategien inneholder ikke konkrete tiltaks- og utviklingsplaner, men skal legge føringer for videreutviklingen av ID-porten. Konkrete beslutninger blir fattet gjennom ordinære prioriteringsprosesser i Digdir og nedfelt i egne tiltaks- og utviklingsplaner.

e-ID
Strategien er avgrenset til *produktet ID-porten* og skal ikke legge føringer for de enkelte e-ID-er som benyttes i ID-porten. Strategien blir likevel retningsgivende for inngåelse av nye e-ID avtaler fra 2021. Dette er ikke en strategi for e-ID i offentlig sektor

Endringer i rammebetingelser
Både den teknologiske utviklingen, samt politiske og samfunnsmessige endringer over tid, kan medføre endrede rammevilkår knyttet til områder som berører ID-porten. Dette er forhold som må tas med i den samlede vurderingen av utviklingstiltak og prioriteringer frem mot 2025.

3 Bakgrunn

Fra ID-porten ble lansert i 2010 har det skjedd teknologiske og samfunnsmessige endringer som krever at offentlig forvaltning må arbeide på nye måter. Regjeringens digitaliseringsstrategi for offentlig sektor 2019-2025 peker på samordning og samarbeid på tvers av forvaltningsnivåer, og sektorer som nøkkelen til å kunne ta ut gevinster ved bruk av ny teknologi.[1] Gjennom sammenhengende og tilgjengelige tjenester skal man gi én enklere hverdag for innbyggere, næringsliv og frivillig sektor i møte med en digital offentlig sektor. Brukeren skal være det sentrale utgangspunktet ved digitaliseringen av offentlig sektor.[2]

Det er vanskelig å forutse hvordan teknologien kommer til å påvirke hverdagen til privatpersoner og næringslivet fremover, men vi vet at den kontinuerlig er i endring. Kunstig intelligens, robotisering, stordata og raskere prosessering av data er eksempler på teknologiske fremskritt som kommer til å ha en innvirkning. Innenfor digital identitet er bruk av biometri et sentralt tema i utviklingen av passordfri autentisering.[3] Her er det viktig å nevne at biometri bør kombineres med andre autentiseringsfaktorer for å styrke sikkerheten. Et annet eksempel er en sentralisert og gjenbrukbar anonymiseringsløsning som reduserer mengden informasjon som behøver ekstra høy beskyttelse. Man benytter da pseudonymer, noe som vil innebære mindre konsekvenser ved tap av data på individnivå.

Økt deling av data er en forutsetning for utvikling av flere digitale sammenhengende tjenester. Måten man bruker og utnytter data på er i stor endring, og åpner for helt nye måter å løse oppgaver på. Konseptvalgutredningen (KVU) for deling av data anbefaler en smidig tilnærming, der forvaltningen og næringsliv skal skape nye verdier ved

[3] Beyond Passwords: Simpler, Stronger Authentication with FIDO2

bedre deling og bruk av data. [4] Det skal legges til rette for videre bruk av åpne data på en måte som gjør at informasjonen kan brukes i nye sammenhenger, skape nye tjenester og gi økt verdiskaping og vekst for samfunnet. Digital identitetshåndtering er en sentral komponent for å oppfylle dette.

Digitaliseringen har også medført at samfunnets risikobilde har endret seg, både for enkeltindividet og for samfunnet i stort. Digitale systemer utsettes kontinuerlig for uønskede hendelser, både tilsiktede og utilsiktede. Det kan utgjøre en trussel mot systemene i seg selv, informasjonen som er i systemene, og tjenestene de bidrar til å levere. Slike hendelser omtales med ulike begreper: hacking, digitale angrep, IKT-sikkerhetshendelser, digitale hendelser med mer. Ingen sektor eller nasjoner kan i dag kontrollere sin digitale sårbarhet alene, og det er avgjørende at virksomhetene i offentlig sektor har en felles forståelse av og tilnærming til sikkerhetsutfordringer.[5]

Digitaliseringsstrategien påpeker at ivaretakelse av personvern og informasjonssikkerhet er avgjørende for at offentlig sektor skal lykkes med sitt digitaliseringsarbeid. Meld.St. 27 *Digital Agenda for Norge* (2015-2016) understreker at informasjonssikkerhet og personvern, på lik linje med IKT-sikkerhet, er en forutsetning for tillit til digitale løsninger. Behandling av personopplysninger skal baseres på gode forholdsmessighetsvurderinger med utgangspunkt i behandlingsformålet, og de grunnleggende rettighetene i personvernregelverket må ivaretas og tilpasses. Anonymiserte data kan for eksempel gi økt beskyttelse av personvern.

Regjeringen har som mål at Norge skal delta i EUs digitale i indre marked. Et tett samarbeid med EU er viktig for at næringsliv og privatpersoner effektivt og enkelt kan samhandle digitalt over landegrenser. I arbeidet med digital identitet er Norges involvering og bidrag til eIDAS-forordningen en forutsetning for elektroniske transaksjoner i det indre marked. [6]

[4] Difi-rapport 2018:7 Deling av data – KVU

[5] NOU 2018:14. IKT sikkerhet i alle ledd – organisering og regulering av nasjonal IKT-sikkerhet

[6] eIDAS regulation

4 Visjon

Med bakgrunn i ID-portens rolle i offentlig sektor, videreføres nåværende visjon:

ID-porten sikrer digital forvaltning

Visjonen skal legge føringer for strategiske mål og innsatsområder, og skal sikres gjennom fire grunnleggende prinsipper som til enhver tid legges til grunn:

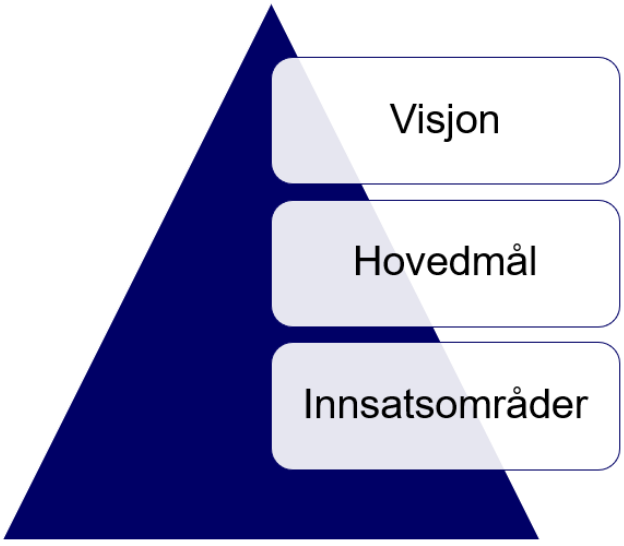
- Robust
- Brukerorientert
- Samordnet
- Innovativ og effektiv

Robust: Sikkerheten, kvaliteten og tilgjengeligheten i ID-porten skal være tilstrekkelig for både kunder og sluttbrukere, samt tilfredsstille krav satt i lover og forskrifter.

Brukerfokus: ID-porten skal ha høy brukskvalitet. ID-porten skal være brukervennlig for sluttbruker, enkel å ta i bruk og tilgjengelig på sluttbrukers ønskede plattform til enhver tid.

Samordnet: ID-porten skal være tilpasset kundenes digitale tjenester, virke i sammenheng med andre fellesløsninger i offentlig sektor og samhandle i et felles digitalt økosystem for nasjonal digital samhandling og tjenesteutvikling.

Innovativ og effektivt: ID-porten skal bidra til en smartere og mer kostnadseffektivt offentlig sektor.

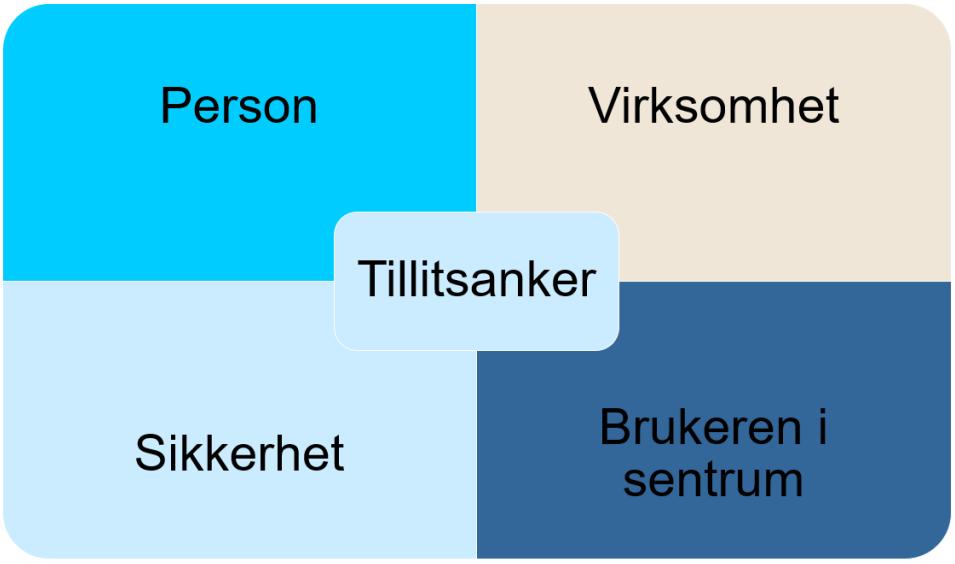


Figur 2 Strategirammeverk for ID-portens produktstrategi

5 Strategi – fem overordnede mål med tilhørende innsatsområder

For å sikre oppnåelse av ID-portens visjon og strategiske mål må det legges til rette for nye bruksområder, samtidig som ID-portens kjerneområdet er godt ivaretatt. ID-portens hovedoppdrag er sikker og enkel autentisering, og behov som omhandler andre områder (for eksempel autorisasjon) må løses i samarbeid med andre virksomheter.

Bruksområdet for produktet og dermed rammevilkårene er blitt vesentlig endret siden etableringen, noe som krever en fornyelse av strategien. Bakgrunnen for dette er blant annet utvidelse til å gjelde personautentisering i «stort», som autentisering av ansatte og virksomheter, utvidelse av felles rammeverk for elektronisk identifikasjon og et generelt økt trusselnivå.



Figur 3 Målbilde for ID-porten

De strategiske satsningsområdene for ID-porten i forrige periode (2015-2020) var *e-ID-tjenester, brukerretting og profesjonalisering*.[7] Arbeidet med ny strategi har vist behov for å videreføre disse innholdet i de satsingsområdene, men omformulert gjennom en fornyet strategi og målbilde.

For å realisere visjonen har Digdir kartlagt og identifisert fem overordnede mål for ID-porten i strategiperioden 2020-2025:

- **Dekke offentlig sektors behov for et nasjonalt tillitsanker**
- **Dekke offentlig sektors behov for identifisering og autentisering av personer**
- **Dekke offentlig sektors behov for autentisering av virksomheter**

[7] Produktstrategi ID-porten 2015-2020

- **ID-porten skal være en sikker autentiseringsløsning**
- **ID-porten skal være en brukerrettet autentiseringsløsning**

5.1 Dekke offentlig sektors behov for et nasjonalt tillitsanker

Som omtalt i kapittel 3 skal offentlige digitale tjenester fremstå sammenhengene og helhetlige for sluttbrukere, uavhengig av hvilke virksomheter som tilbyr dem. Arbeidet med helhetlige, brukerrettede løsninger må derfor koordineres og samhandles i forvaltningen og mellom sektorene, slik at de er tilpasset brukerens behov og livssituasjon. En viktig forutsetning for dette er bruk av digitale fellesløsninger. Felles for disse løsningene er at de bidrar til å effektivisere offentlig sektor, og kan gjenbrukes av forvaltningen til å utvikle flere og nye sammenhengende tjenester på tvers for innbyggere, organisasjoner og næringsliv.ID-porten skal være en del av denne sfæren, som et tillitsanker for autentisering.

Innsatsområder for å nå målet:

5.1.1 Sikre ID-porten posisjon som offentlig sektors autentiseringstjeneste

Regjeringens digitaliseringsstrategi,[1] peker på elektronisk identifikasjon som avgjørende for en digital forvaltning. Som et tillitsanker for sikker autentisering i et økosystem for identitet i offentlig sektor, knytter ID-porten virksomheter og e-ID-leverandørene sammen og skaper tillit mellom sluttbruker, leverandører og tjenestene. En viktig forutsetning for dette er god dialog og koordinering med kunder, samt offentlige og private samarbeidspartnere, slik at man i felleskap er best rustet for fremtiden. Dette krever at ID-porten har en fleksibilitet som både sikrer vedlikehold av infrastruktur og kjernefunksjonalitet, gjør det mulig å utnytte ny teknologi og innovasjon, og samtidig ivaretar at ID-porten skal være behovsstyrt. Dette er avgjørende for at ID-porten fortsatt skal være et godt virkemiddel i omstillingen av offentlig sektor, og realisere regjeringens mål om et felles økosystem for nasjonal digital samhandling og tjenesteutvikling.

5.1.2 ID-porten skal bidra til sømløs samhandling i det digitale økosystemet.

God samhandling er en forutsetning for å kunne videreutvikle løsninger og bygge nye sammenhengende tjenester. Som aktører i offentlig sektor er man avhengig av å utfylle hverandre for å redusere noe av kompleksiteten i et digitalt økosystem. I stedet for at en løsning skal løse store behov, kan man bygge komplementære løsninger på tvers. Et eksempel er kombinasjonsgevinsten av ID-porten, folkeregisteret og enhetsregisteret for å identifisere og verifisere brukere på forskjellige nivå. Et annet eksempel er Helse ID, som en felles påloggingsløsning for helse- og omsorgssektoren. Den legger til rette for at helsepersonell kan få engangspålogging med høyt sikkerhetsnivå, blant annet ved å gjenbruke ID-porten. Gevinsten mellom Altinn autoriasjon og ID-porten, som muliggjør styring av tilganger, er også et godt eksempel på samhandling ved komplementære løsninger.

ID-porten skal også bidra til et styrket samarbeid, og unngå å utvikle digitale løsninger i konkurranse med privat sektor. Samhandling med markedet kan gi grunnlag for gode tjenester som kan stimulere til innovasjon, drive videreutviklingen av digital identitet og utfordre offentlige samfunnsoppdrag[1]

5.1.3 ID-porten skal være fremoverlent på teknologivalg og legge til rette for innovasjon

ID-porten er behovsstyrt og stadig i utvikling, som gjør at måten man produserer og leverer tjenester på er kontinuerlig i endring. Dette betyr at visse funksjonaliteter og bruksområder kan bli utdaterte, lite helhetlige og ikke sammenhengende. ID-porten skal være fremoverlent på teknologi som er i utvikling, og tilrettelegge for at ny teknologi skal samhandle med identitet i offentlige tjenester. ID-porten skal utvikles sammen med den teknologien som muliggjør at hver funksjonalitet kan realiseres på en mest mulig hensiktsmessig måte. Se kapittel 3 for eksempler på teknologiske mulighetsrom innen digital identitetshåndtering.

For å opprettholde tillit er det viktig å beholde ID-porten som en innovativ plattform for sikkerhetstjenester. Dette betyr at ID-porten, innenfor sitt funksjonsområde, skal være en plattform for innovative løsninger. Et eksempel på nyskapende arbeidsområder er DifiCamp (sommeren 2019) sitt arbeid med å undersøke hvordan man kan kobler ID-porten med Internet of Things. Eksempelvis om det er mulig å gi digitale assistenter som Alexa fra Amazon og Google Home tilgang til beskyttet informasjon gjennom ID-porten.[8]

Et annet eksempel på innovativ tilrettelegging er Oslo kommune sin applikasjon *Oslonøkkelen*.[9] Den gir innbygger i kommunen utvidet og enklere tilgang til byens lokaler og tjenester via appen, ved å bruke ID-porten som nøkkel. Dette er et eksempel på at ID-porten leverer sikker og kjent pålogging, mens kommunen leverer den innovative tjenesten.

5.2 **Dekke offentlig sektors behov for identifisering og autentisering av personer**

Stortinget gav ved behandling av Meld St.27. (2015-2016) sin tilslutning til målsettingen om å styrke det digitale førstevalget.[2] Som resultat av dette tilbyr statlige virksomheter og kommuner stadig flere digitale tjenester, og bruken av disse øker betydelig. Dette gjør at kravene og behovene knyttet til de digitale fellesløsningene økes, og at nye bruksområder dukker opp.

[8] Difi-camp

[9] Oslonøkkelen

ID-porten som autentiseringstjeneste skal videreutvikles slik at den dekker nasjonale fellesbehov. I løpet av forrige strategiperiode har det dukket opp nye behov knyttet til personautentisering med et ønske om å utvide dagens bruk av ID-porten. Mange av behovene treffer områdene autentisering, autorisasjon, nasjonal arkitektur, og noen sektorer og etater har spesifikke behov knyttet til sine bruksområder. Dette må følges opp av riktige aktører i samarbeid med Digdir

Innsatsområder for å nå målet:

5.2.1 Levere sikker autentisering av personer

Sikker autentisering av innbyggerne er fremdeles kjerneområdet til ID-porten, selv om det åpnes for nye bruksmuligheter og bruksområder. Med over 4 millioner brukere og 450 000 innlogginger hver dag er det avgjørende at ID- porten opprettholder standarden som nasjonal innloggingsløsning for innbyggere til offentlig tjenester på nett.

5.2.2 Bidra til at hele befolkningen har en elektronisk ID

Regjeringen har som målsetting at alle innbyggere skal ha en e-ID som kan brukes for de tjenestene de har behov for.[1] Det er en utfordring med utbredelse av sikkerhetsnivå 4 i noen målgrupper, eksempelvis 15-18 åringer og personer over 70 år. ID-porten skal, sammen med samarbeidspartnere, legge til rette for at alle skal få muligheten til sikker identifisering og føle seg trygge når de bruker digitale tjenester i offentlig sektor. Dette innebærer å utforske mulighetsrommet, potensialet og gevinsten for å kunne realisere løsninger til ulike målgrupper, samt bidra til kompetanseheving om temaet digital identitet hos innbyggere.

5.2.3 ID-porten skal legge til rette for sikker autentisering av ansatte

Dagens situasjon med autentisering av ansatte i offentlig sektor er ikke tilfredsstillende, og behovet for å øke sikkerheten og effektiviseringen av ansattautentisering er nærmere kartlagt i en egen utredning.[10] ID-porten skal legge til rette for å støtte autentisering av ansatte i ID-porten. Dette kan eksempelvis innebære å formidle autentisering som kan kombineres med autorative kilder. Autorative kilder kan for eksempel være Aa-registeret, Advokatregisteret og helsepersonellregisteret.

5.2.4 ID-porten skal bidra til sikker autentisering av utenlandske sluttbrukere

Som omtalt i kapittel 3 er et tett samarbeid med EU viktig for samhandling digitalt over landegrenser, og som en forutsetning for at utenlandske sluttbrukere kan benytte seg av norske tjenester. ID-porten er i dag knyttet til EUs infrastruktur for autentisering på tvers av landegrenser i EØS-området, på basis av eIDAS-forordningen.[6] ID-porten skal, sammen med relevante samarbeidspartnere, fortsatt tilby

[10] ID-porten. Utredning – nye bruksområder 2018

støtte for at sluttbrukere fra andre europeiske land kan benytte sin eksisterende e-ID for tilgang til norske offentlige tjenester på nett. Dette reiser samtidig utfordringer knyttet til autentisering av personer som ikke kommer fra Europa eller land som ikke støtter eIDAS-forordningen. Sammen med relevante samarbeidspartnere skal ID-porten bidra i den grad det er mulig til å løse disse utfordringene.

5.2.5 ID-porten skal legge til rette for digital verifisering

Som nevnt i kapittel 3 vil regjeringen at alle innbyggerne blir fullverdige digitale brukere dersom de ønsker det. En viktig forutsetning for dette er at alle innbyggerne skal ha en elektronisk ID (e-ID) som gjør at de kan logge seg inn via ID-porten, og benytte seg av de tjenestene man har bruk for (se mer kapittel 5.4.2). Et virkemiddel i denne prosessen er sikker digital verifisering av identitet. I dag er man avhengig av en e-ID på sikkerhetsnivå 4 for å bruke diverse tjenester, som for eksempel innenfor helsesektoren, NAV og Statens Vegvesen. I dag blir utstedelse av en e-ID på sikkerhetsnivå 4 utlevert ved personlig oppmøte, eksempelvis ved legitimering med pass i bank, som kan være ineffektivt og begrensende for visse målgrupper og sårbart i tillitskjeden for digital identitet.

ID-porten skal, sammen med leverandører, kunder og andre samarbeidspartnere, tilrettelegge for gode løsninger for sikkert digital verifisering av identitet. Løsninger som eksempelvis IDmee, gjør det mulig for digital legitimering med pass.[11] Dette muliggjør for eksempel at utenlandske sluttbrukere kan etablere et kundeforhold i en norsk bank, uten at vedkommende trenger å møte opp fysisk. Et annet eksempel er Signicat sitt arbeid med å tilby gode løsninger for digital identitet i regulerte næringer, ved å sikre digitale onboarding-løsninger og løsninger for overholdelse av regelverk.[12] Det er dog viktig å sikre at løsninger for digital verifisering blir vel så gode som ID-kontroller i den fysiske verden.

5.3 ID-porten skal dekke offentlig sektors behov for autentisering av virksomheter

En rekke av ID-portens kunder har signalisert behov for autentisering av virksomheter.[10] I dag utveksles virksomhetssertifikater bilateralt mellom virksomheter. Dette er ineffektivt, lite skalerbart og korrelerer dårlig med hvordan verdikjeder er bygd opp av andre tjenester. Man må da løse hvert enkelt tilfelle hver for seg for å kunne dele data, noe som krever manuelle arbeidsprosesser og en dataflyt som er tids- og ressurskrevende med risiko for feil. ID-porten som autentiseringstjeneste skal videreutvikles slik at den dekker offentlig sektors fellesbehov for autentisering av virksomheter.

[11] IDmee

[12] Signicat

Innsatsområder for å nå målet:

5.3.1 ID-porten skal levere sikker og effektiv autentisering av virksomheter

Det er hensiktsmessig å gjenbruke ID-portens teknologiske plattform for å autentisere virksomheter ved å kombinere ID-porten og virksomhetssertifikater (organisasjonsnummer), på samme måte som man i dag kombinerer personsertifikat (fødselsnummer). [10] Kundene ser på ID-porten som en mulighet til å legge til rette for sikker API-drevet innovasjon. Dette er knyttet til behov for standardisert utveksling, der løsningen kan tilby en enkel modell for API-sikring.[13]

ID-porten skal sørge for sikker autentisering av virksomheter som et eget produkt i løsningen, med et grunnlag for et veletablert og modent marked for tillitstjenester. Ved å bruke løsningen som en sikringsmekanisme for trygg deling av data og som sikrer at data bare flyter dit de skal, kan ID-porten benyttes som tillitstanker mellom virksomhetene, og sørge for sikker autentisering og tilgangskontroll.

I 2019 lanserte Difi *Maskinporten* som et eget produkt.[14]

5.3.2 ID-porten skal legge til rette for flere sammenhengende tjenester på tvers

Det er et økene behov for større grad av nasjonal standardisering, sentralisering, effektivisering av deling av data og forbedret samspill mellom autentisering og autorisasjon.[10] Gjennom sikker autentisering skal ID-porten bidra til å forenkle deling av data, ettersom virksomhetene sparer ressurser på utvikling og vedlikehold av egen sikringsmekanisme. Ved å garantere identiteten mellom virksomhetene skal ID-porten legge til rette for å binde sammen systemer og utvikle nye tjenester på en effektiv måte.

5.4 **ID-porten skal være en sikker autentiseringsløsning**

Som nevnt i kapittel 3 har digitaliseringen medført at samfunnets risikobilde har endret seg. Offentlig sektor er dermed helt avhengig av å sikre tjenester og IT-systemer som en grunnleggende forutsetning for å opprettholde tillit.

Med et stort sluttbrukeromfang er det essensielt at ID-porten kan dekke offentlig sektors grunnbehov som tillitsanker og sikkerhetsnett for identitet på nett. ID-portens autentiseringstjeneste fungerer i dag med god ytelse og høy sikkerhet, der prosesser for drift og vedlikehold gjennomgår kontinuerlig revisjon i henhold til kvalitetssikringsprosesser. Krav til å tilpasse seg ny sikkerhetsteknologi, samt ha gode sikkerhetsrutiner og prosesser, er essensielt for å opprettholde en sikker

[13] API-sikring med Maskinporten

[14] Maskinporten

og robust autentiseringstjeneste. Dette gjør at utviklingen, driften og forvaltningen av ID-porten må ha en felles sikkerhetstankegang, og alle sikkerhetsmekanismer skal være dokumenterte, evaluerte og åpne for revidering. I tillegg skal ID-porten fremdeles oppfylle formelle lovkrav og risikobasert krav.

Figur 4 ID-porten - sikker autentisering

Innsatsområde for å nå målet:

5.4.1 ID-porten skal levere robuste sikkerhetsmekanismer

ID-porten skal, i samsvar med rammeverket som er definert i *Nasjonal strategi for digital sikkerhet,*[15] understøtte en robust og pålitelig digital infrastruktur. ID-porten skal også ha tekniske og organisatoriske tiltak for å handtere sikkerhetsrisikoer, i henhold til *Lov om tillitstjenester*[16], ved å blant annet ha motstandsdyktige systemer og evne til å gjenopprette normaltilstand ved hendelser.

Man skal fortsette å basere seg på en IKT-sikkerhetsstrategi for åpenhet der man ikke tar tillit for gitt, men baserer seg på risiko, kontekst og atferd. ID-porten skal ha robuste sikkerhetsmekanismer som gjør at privatpersoner og virksomheter har tillit til offentlig sektor.

5.4.2 ID-porten skal ivareta informasjonssikkerheten i hele tillitskjeden.

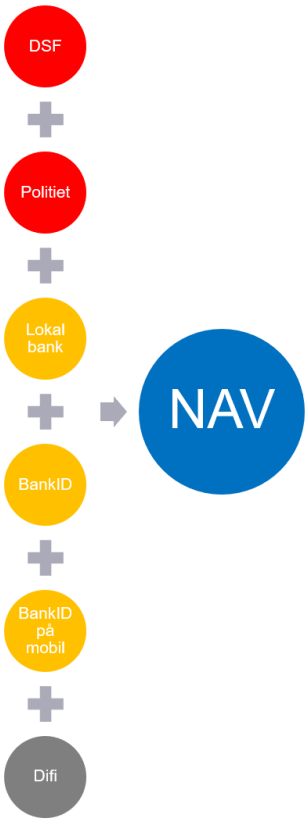
ID-porten skal ha innebygd informasjonssikkerhet.[17]
Informasjonssikkerheten i ID-porten må vurderes fra oppstart til utfasing,

[15] Nasjonal strategi for digital sikkerhet

[16] Ny lov om tillitstjenester

[17] Innebygd informasjonssikkerhet

og man skal følge informasjon fra den oppstår til den slettes. Dette innebærer en risikovurdert tilnærming når det fattes beslutninger om hvordan ID-porten skal håndtere og identifisere risikoer. Digdir skal være rustet til å ta informerte valg og prioritere deretter.



Figur 5 Eksempel på tillitskjede for digital identitet

En forutsetning for innebygd informasjonssikkerhet er at ansatte og andre personer som håndterer informasjon knyttet til ID-porten har tilstrekkelig kunnskap og bevissthet om informasjonssikkerhet. Dette blir stimulert gjennom en god sikkerhetskultur, internt og på tvers av etater og gjennom hele tillitskjeden.

5.4.3 ID-porten skal ivareta tillit gjennom en risikobasert og proaktiv tilnærming

For å ivareta tillit er det nødvendig å ha et kontinuerlig proaktivt sikkerhetsfokus i tjenesteutviklingen, slik at ID-porten fortsatt kan levere en effektiv tjeneste med høy kvalitet. Det er særlig viktig at alle tekniske og ikke-tekniske komponenter i ID-porten skal behandles ut fra et sikkerhetsbehov, som gjør at man lettere kan oppdage misbruk og sikring mot kjente og ukjente trusler. Det gjelder også trusler mot sluttbruker. ID-porten skal samarbeide med relevante aktører om risiko og sikkerhet, samt ha en oppdatert sikkerhetstilnærming i tråd med samfunnets behov.

5.5 ID-porten skal være en brukerrettet autentiseringsløsning

Som det kommer frem i kapittel 3 er en av hovedprioriteringene i IKT-politikken at brukeren skal settes i sentrum gjennom sammenhengende tjenester, og tjenestene skal være tilpasset brukerens behov og

livssituasjoner. Som en nasjonal innloggingsløsning til tjenester på nett er det avgjørende at ID-porten oppleves som tilgjengelig, er enkel å bruke, gratis for innbygger og at løsningen bidrar til å skape tillit.

Innsatsområder for nå målet

5.5.1 ID-porten skal levere tilgjengelige løsninger med høy brukskvalitet og opplevd tillit

Figur 6 ID-porten designguide - grunnprinsipp

Forvaltningen og videreutviklingen av ID-porten skal følge grunnprinsippene i tråd med designguiden.[18]Med høy brukskvalitet menes det også at ID-porten aktivt skal benytte tilbakemeldinger fra sluttbrukere, samt revidere grunnprinsippene med involvering fra kunder og sluttbrukere.

5.5.2 ID-porten skal bidra til brukervennlige tjenester

Sluttbrukere har høy tillit til ID-porten, men i noen sammenhenger opplever brukere utfordringer ved tjenesten. Man er avhengig av samarbeid i forvaltningen for å skape gode brukerrettede offentlige tjenestekjeder. Det er tjenesteeiernes ansvar å gjøre egne tjenester tilgjengelige på relevante plattformer, mens ID-porten skal bidra til at tjenesteeierne kan tilby tjenester som er brukervennlige, sammenhengende og selvbetjente. Ved å legge til rette for dette bidrar ID-porten til at felles behov blir løst.

Ved å eksempelvis gi tilgangsstyring til applikasjoner for bruk av ID-porten kan tjenesteeiere tilby brukervennlige innlogginger til selvbetjente løsninger. Et eksempel er applikasjonen *DFØ*. [19]Her logger man seg inn via ID-porten første gang man bruker appen, deretter kan man velge å ta i bruk biometri med fingeravtrykk for innlogging. Som en sikkerhetsmekanisme må man logge seg på ID-porten på nytt annen hver måned.

[18] ID-porten designguide

[19] DFØ-app

5.5.3 ID-porten skal bidra til godt personvern

Som omtalt i kapittel 3 skal sluttbrukernes personvern ivaretas på en hensiktsmessig måte. Personvern skal være en integrert del av forvaltning, bruk og videre utvikling av ID-porten. På samme måte som deling av data og bruk av ny teknologi gjør at det kan oppstå kryssende hensyn mellom ønsket om mer åpenhet og personvern, vil det i arbeidet med å videreutvikle ID-porten være nødvendig å håndtere avveiningen mellom sikkerhet og brukerretting.

5.5.4 ID-porten skal legge til rette for bruk av digitale fullmakter og avgivelse av digitalt samtykke

De som ikke kan opptre digitalt selv, skal ha muligheten til å la seg representere av en annen gjennom fullmakt. For å unngå ineffektivitet, reduserte gevinster og misbruksscenarioer er det viktig at offentlig sektor kartlegger behovet for en forbedret vergeløsning for autentisering. ID-porten skal, sammen med samarbeidspartnere, legge til rette bruk av digitale fullmakter og avgivelse av digitalt samtykke, der ambisjonen er å begrense misbruksmuligheter og gjøre kommunikasjonen med offentlig sektor enklere for de som ikke kan opptre digital selv.

5.5.5 ID-porten skal gi bruker innsyn i egne data

Brukerne har rett til å få informasjon om hvilke instanser som lagrer, behandler og utveksler opplysninger om dem, og til hvilke formål. I dag har alle personer som er registrert som brukere av fellesløsningene til Digdir rett til å be om innsyn i personopplysninger som er lagret i fellesløsningene. ID-porten skal lettere tilgjengeliggjøre innbygger sine data som er lagret i fellesløsningene, ved å gjøre den verdifull og relevant for innbygger. På den måten ønsker ID-porten å styrke innbyggers eierskap og rettigheter til personlige data.

6 Vedlegg 1 - videre forvaltning av strategien

Videre forvalting av strategien skal skje i henhold til beslutningsprosessen for arbeid med visjon og strategi for ID-porten som er fastsatt av Difi. Beslutningsprosessen er styrende for ID-porten og skal brukes som grunnlag for å:

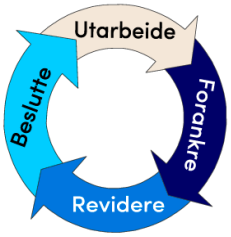
- utarbeide og beslutte visjon og strategi
- revidere visjon og strategi ved fastsatte intervaller eller hendelser

Beslutningsprosessen for visjon og strategi består av tre definerte prosesser:

1. **Visjonsprosess**
   Visjonsprosessen skal gjennomføres hvert 5.-10. år eller ved vesentlige endringer i digital postkasse til innbyggere sine rammebetingelser.
2. **Strategiprosess**
   Prosessen skal gjennomføres hvert 3.-5. år, ved endrede rammebetingelser eller ved identifisert behov for nye eller endrede tjenester.
3. **Utviklings- og tiltaksplanprosess**
   Gjennomføres årlig i henhold til endringsstyringsprosess for Digdir felleskomponenter og etter innspill fra ID-portens kunder, leverandør og sluttbrukere. Prosessen skal etablere konkrete utviklings- og tiltaksplaner som skal sikre oppfyllelse av de mål som er definert i strategien for digital postkasse til innbyggere.

Visjons- og strategiprosessene gjennomføres som en fire-stegs prosess som indikert i figur 10.

Det vil, avhengig av omfang av revisjon etter første forankring, kunne være behov for å gjenta stegene «forankre» og «revidere» inntil det oppnås tilstrekkelig samstemmighet som kan danne grunnlag for en endelig beslutning.



Det er Digdir ledelse som har besluttende myndighet både for visjon, strategi og de ulike tiltak og utviklingsplaner.