Høringsversjon

Strategi for eID og e-signatur i offentlig sektor

Versjon 1.0

Forslag fra arbeidsgruppe nedsatt av Fornyings- og administrasjonsdepartementet

Innholdsfortegnelse

Scenarie 2010

Amalie Skrot våknet i riktig dårlig humør den dagen. Hun har nå lenge sett frem til å få en flott, ny vinterhage til å tilbringe kjølige høstkvelder i, men så tok det jo så forbasket lang tid med denne behandlingen i Plan – og bygningsetaten! Saken trakk ut i langdrag, fordi søknaden om påbygg på hennes flotte, gamle, verneverdige hus stadig ble revurdert på grunn av ulike innspill fra involverte instanser. Nå måtte hun gjøre noe for å få fremdrift!

Hun labbet ut på kjøkkenet, spiste et beger yoghurt til frokost og satte kursen mot badet. Etter en stund var hun klar for dagen.

Hun satte seg godt til rette i sofaen, løftet frem sin tablet-PC i fanget og fant frem smartkortet sitt. Hun stakk det inn leseren i siden av PC-en og dro fingeren sin over den biometriske avlesningsstripen ytterst. Påloggingsinformasjon kom frem på skjermen og hun var inne

Amalie ville aller først vite hva er status i hennes byggesak. Hun pekte på ikonet ”Minside” overst på skjermen med sin lille pekepinne og Minside sitt åpningsbilde kom frem – med spørsmål om hvem som skulle inn. Amalie skrev inn navnet sitt og dro igjen fingeren over kortet som satt i leseren.

Hennes personlige side kom frem, med mappen ”Plan og byggesaker” øverst i oversikten. Hun pekte på mappen og status i saken kom frem på skjermen. Samtidig så hun at det var en melding til henne i hennes meldingsboks. Hun pekte på boksen og der lå en melding fra Plan- og bygningsetaten! Hun ble opprømt – kanskje var det endelig den etterlengtede tillatelsen som kom? Der var det et lite ikon som indikerte at hun kunne hente frem et dokument fra etaten. Hun pekte på det og opp kom et vedtaksbrev – det var et avslag!! Hun stirret vantro på skjermen og fikserte øynene sine på et lite merke nederst til høyre under teksten – der sto det ”Signatur”, under et navn til en saksbehandler som hun ikke har sett før. Hun pekte på merket og etter to sekunder kom det en boks på skjermen som sa: ”Signert av Plan og bygningsetaten i Bergen, den 26. april 2010”. Pokker heller! Nå var hun i kjempedårlig humør – hun tenkte å ringe og dele noen av sine meninger med dem i denne etaten, men så kom hun på at det var bedre å dra og møte opp personlig – nå, med en gang!

Hun skulle til å logge av Minside da hun plutselig husket at hun hadde en legetime hos fastlegen sin for en vanlig sjekk. Den måtte hun avbestille, det var en tjeneste for dette i Minside. Ja, men så kunne hun også ta ting opp direkte med legen – hun logget av Minside, dro opp e-post programmet sitt og skrev en rask beskjed til legen, med noen punkter som hun hadde tenkt å ta opp i timen, men som hun bestemte seg for heller å ta opp på e-post. Da hun var ferdig med å skrive, pekte hun på fanen ”signer og krypter” øverst til venstre i skjermbildet – så ble hun bedt om å gi personlig validering – hun dro fingeren over den biometriske stripen på smartkortet og programmet kvitterte med ”Signert og kryptert – sende?”. Hun pekte på OK-boksen og e-posten kom avsted.

Hun dro på seg jakken og skulle gå ut av døren da hun oppdaget at hun glemte PC-en...

Hun dro ut kortet fra leseren og stakk det i lommeboka, klappet sammen PC-en og stappet den i vesken. Nå var hun klar – med alle ”sakspapirer” i vesken.
De skal få høre der i Plan- og bygningsetaten!!

Bruksscenarier Pasient – helsetjenesten

Casene illustrer bruk av eID (nivå 4) for å gi pasienter tilgang til egen helseinformasjon i pasientjournaler – evt. via Minside. All bruk av eID for å autorisere for tilgang til eller overføring av helseinformasjon forutsetter høyt sikkerhetsnivå, med sterk autentisering.

Pasientkommunikasjon
Pasienter og helsevesenet ønsker fra hver sin kant å øke den elektroniske kommunikasjonen seg i mellom. Radiumhospitalet og Rikshospitalet har utviklet og evaluert slike løsninger siden 2002, og erfaringene, som er validert i randomiserte studier, viser at slike løsninger har store positive effekter for både pasienter og helsepersonell. Helsesektoren vil ønske å innføre slike løsninger i aksellererende tempo i årene framover, og det vil da være behov for å gå over fra dagens skreddersydde autentiseringsløsninger til offentlige standardløsninger, noe som igjen forutsetter at landets borgere har tilgang til sikre former for elektronisk ID. eID kan benyttes til å gi pasienten tilgang til flere funksjoner over Min Side til, som f.eks. timebestilling og annen kommunikasjon med fastlege, føring av egenjournal.

Innsyns- og samtykketjenester
Pasienten vil kunne gis tilgang til egen helseinformasjon som er tilrettelagt med et web-grensesnitt. En slik løsning vil også gjøre det mulig for pasienter som oppholder seg i utlandet å få utlevert informasjon fra egen journal. I tillegg muliggjør dette utvikling av tjenester hvor pasienter kan gi samtykke til at konkrete opplysninger fra egen pasientjournal utleveres til annet helsepersonell eller eksempelvis til et forsikringsselskap for behandling av søknad om forsikringsutbetaling eller ved behandling av en uførepensjonssøknad.

Egenregistrering
Pasienten kan bidra med egenregistrering av helseopplysninger og registrere måleresultater i helsedagbok eller egenjournal, f.eks. som ledd i hjemmebehandling /oppfølging av behandling, eller for registrering ifm. “grønn resept”. Samme eID vil kunne benyttes til Nettbaserte diskusjonsfora/behandlingsgrupper ledet av helsepersonell med sterk sikkerhet for innholdet og hvem som er deltagere i gruppen.

e-Resept
Når løsningen for elektroniske resepter tas i bruk i Norge vil borgerne kunne få tilgang til informasjon om sine gyldige resepter gjennom nettstedet "Mine Resepter" som også er tilgjengelig over Minside. Dette nettstedet vil presentere detaljene om alle egne aktive resepter som ligger i Reseptbanken på det aktuelle tidspunktet, inkludert hva som har vært utlevert, hvor mye som ennå kan utleveres, mm. Denne løsningen vil gi tilgang til sensitive personopplysninger, og vil derfor kreve sikker autentisering av brukerne. Den aktuelle løsningen vil måtte ligge på sikkerhetsnivå 4.

Ordliste

Altinn	En felles tjenesteportal, som gir samlet tilgang til offentlig sektors tjenester for næringslivet.
Ansattsertifikater	Et sertifikat som knytter en fysisk person til en virksomhet og på den måten bekrefter personens tilknytning til virksomheten.
Autentisering	Autentisering er å verifisere påstått identitet.
Autentiseringsfaktor	Når noen skal autentisere seg over nettet, må de ha noe som kan bekrefte deres identitet. Dette kalles autentiseringsfaktorer. En bruker kan ha én eller flere av disse avhengig av sikkerheten i løsningen. Det finnes tre forskjellige typer autentiseringsfaktorer: • noe personen vet; for eksempel et passord, • noe personen har; for eksempel en passordkalkulator, • noe personen er; for eksempel et fingeravtrykk.
Autorisasjon	Autorisasjon vil i denne sammenheng si at en identitet har fått godkjent tilgang til ressurser, eller rett til å utføre en viss type handlinger, i et system. Autorisasjon bygger på autentisering, fordi en identitet må verifiseres før tilgang kan gis.
Biometri	Løsninger som benytter måling av ulike biometriske kjennetegn, som for eksempel fingeravtrykk, ansikt, osv.
Chip	En liten elektronisk brikke, som er laget for å kunne utføre spesielle oppgaver. Kommer gjerne på et plastkort med fysiske kontakter iht. ISO standarder, eller med en trådløs kommunikasjonsanordning (RFID).
CRL	Certificate Revocation List, Tilbakekallingsliste, er en liste over sertifikater som er kalt tilbake.
D-nummer	Når en innvandret person skal få tildelt fødselsnummer, gis det ofte først et midlertidig D-nummer. For utlendinger som har lovlig opphold i Norge, brukes dette i forbindelse med skatt og offentlige tjenester. D-nummeret er ellevesifret, og består av modifisert fødselsdato og et femsifret nummer. Fødselsdatoen modifiseres ved at det legges til 4 på det første sifferet: en person født 1. januar 1980 får dermed 410180, mens en som er født 31. januar 1980 får 710180. Det femsifrede tallet gis ikke i serier, men tildeles fortløpende. [8]
Drifts- og utviklingsavtale	Drifts- og utviklingsavtale inngåes mellom Kunden og Leverandøren. Avtalens omfang, både med hensyn til hva som skal leveres og pris, er fastsatt i en gjensidig bebyrdende avtale mellom Kunden og Leverandøren.
Dynamisk autentiseringsfaktor	Med dynamisk menes her at informasjonen som presenteres for de som skal verifisere påstått identitet, endres fra gang til gang.
EbXML	ebXML er også kalt "Web Services for B2B" og består av et sett spesifikasjoner som til sammen etablerer et komplett generisk rammeverk for e-business som inkluderer alt fra semantisk interoperabilitet, sikker meldingsoverføring, grensesnittsbeskrivelser og registreringsfunksjonalitet.

Elektronisk ID	Elektronisk ID er en eller flere tekniske innretninger, som kan benyttes til å autentisere seg eller signere på nett, og som er knyttet opp mot samme brukernavn (fysisk person sitt folkeregistrerte navn eller pseudonym, eller en juridisk persons enhetsregistrerte navn eller pseudonym).
Elektronisk signatur	Data i elektronisk form som er knyttet til andre elektroniske data og som brukes som autentiseringsmetode [6] Arbeidsgruppen har valgt å tolke begrepet elektronisk signatur i denne strategien som løsninger som knytter et innhold til en identitet på en uavviselig måte.
Engangspassord	Et passord som ikke er likt fra gang til gang, men som endrer seg.
Enhetsregisteret	Enhetsregisteret samordner opplysninger om næringslivet og offentlige etater som finnes i ulike offentlige registre, og som er gjengangere på spørreskjemaer. Enhetsregisteret inneholder grunndata om enheter som har registreringsplikt i NAVs AA-register, Merverdiavgiftsmanntallet, Foretaksregisteret, Statistisk sentralbyrås bedriftsregister, Skattemanntallet for etterskuddspliktige eller Stiftelsesregisteret. [9]
FEIDE	**FEIDE** står for **F**elles **E**lektronisk **IDE**ntitet. FEIDE skal sørge for at autentifisering, autorisasjon og forvaltning av brukernes identitet i universitets- og høgskolesektoren (UH-sektoren) skjer uavhengig av de datasystemer som studentene benytter. Feide lar personer som har tilknytning til norske utdanningsinstitusjoner identifisere seg via en felles innloggingstjeneste. FEIDE ble startet i 2000 og skal være ferdig utbygd i 2010. [9]
Forsyningsstrategi	En strategi for hvordan man skal sørge for at innbyggere, næringsliv og offentlige virksomheter er utstyrt med felles løsninger for elektronisk ID og e-signatur.
Forvaltningsstandard	En standard vedtatt av forvaltningen for forvaltningen. Forvaltningsstandarden kan være anbefalt eller obligatorisk. Formålet med en slik standard er å tilrettelegge for bedre samspill mellom offentlige etater med det formålet å effektivisere og/eller kvalitetsforbedre sektoren.
Fysisk person	En fysisk person er et anskuelig menneske underlagt fysiske lover.
Fødselsnummer	Et fødselsnummer er et ellevesifret registreringsnummer som tildeles av den norske stat til alle landets innbyggere. Nummeret skiller enkeltpersoner fra hverandre, men kan ikke brukes som legitimasjon. Fødselsnumre ble innført i 1964 og administreres av Skatteetaten. Alle som er bosatt i Norge og innført i folkeregisteret har enten et fødselsnummer eller et D-nummer. Ifølge personopplysningsloven kan fødselsnummer kun brukes når det er saklig behov og når det er umulig å oppnå tilfredstillende identifikasjon ved bruk av andre metoder, som for eksempel navn, adresse, fødselsdato, medlems- eller

	kundenummer. [8]
Fødselsnummeroppslag	Et oppslag mot en oppslagtjeneste, for å finne fødselsnummer på bakgrunn av navn eller annen sertifikatinformasjon.
Hash-verdier	En hash funksjon er en matematisk funksjon som ”omregner” informasjon av vilkårlig lengde til et tall av fast lengde. En god hash funksjon har egenskaper som gjør at det er praktisk umulig å få laget samme tall ut fra to ulike informasjonsmengder. Resultatet av hash-funksjonen – hash-verdien - benyttes for å generere en digital signatur.
Helsetrygdkort	Et europeisk helsetrygdkort viser rett til nødvendig helsehjelp når man er på reise i et EØS-land eller Sveits.
Ikke-benekting	Se uavviselighet.
Informasjonsintegritet	Informasjonsintegritet innebærer at informasjonen ikke kan endres ved lagring eller overføring. Sikres gjerne gjennom at informasjonen følges av en hash verdi, slik at en ny beregning av denne vil vise om informasjonen er endret eller ikke.
Innsynsarkiv	Et arkiv, som tjenesteyter gjør tilgjengelig for sluttbruker, slik at sluttbruker til enhver tid skal ha oversikt over hva tjenesteyteren har lagret om seg selv i forhold til informasjon om sluttbruker og transaksjoner utført mellom tjenesteyter og sluttbruker.
Juridisk person	En juridisk person er et selvstendig rettssubjekt som for eksempel stater, kommuner, aksjeselskap, stiftelse eller forening.
Kodekort	Et kort med en liste over koder, som kan benyttes for å autentisere seg overfor en tjenesteyter. Kodene kan være nummerert og/ eller konfidensialitetsbeskyttet gjennom såkalt ”skrapelodd” funksjon.
Konfidensialitet	Konfidensialitet innebærer at informasjonen ikke skal kunne fanges opp av uvedkommende.
KS	KS er kommunenes arbeidsgiver-, interesse- og medlemsorganisasjon.
MinID	MinID er autentiseringsløsningen som benyttes ved pålogging til første versjon av Minside hos norge.no.
Minside	Minside er innbyggeres personaliserte sider hos norge.no. Minside er et offentlig servicekontor på Internett. Minside gir: • En felles inngang til enkelte elektroniske tjenester fra det offentlige • Mulighet for enkel dialog med offentlige etater • Oversikt over informasjon som er registrert om den enkelte innbygger i ulike offentlige registre.
Mobilpassord	Se SMS-passord.
OCSP	Online Certificate Status Protocol. En oppslagtjeneste for å finne ut om en eID (sertifikat) er kalt tilbake eller ikke.
Oppslagstjeneste for fødselsnummer	Se fødselsnummeroppslag.

Passordkalkulator	En kalkulator som beregner nye passord på bakgrunn av tid, en teller eller annen grunninformasjon. Benyttes for å generere dynamiske passord. Noen passordkalkulatorer kan være beskyttet med PIN-kode, for å sikre at bare eieren kan ta den i bruk. Se også dynamisk autentiseringsfaktor.
Personsertifikater	Et sertifikat, der sertifikatinnehaver er en fysisk person.
PIN-koder	PIN (Personlig IdentifikasjonsNummer, ofte kalt PIN-kode) er en personlig tallkode som må oppgis for å få adgang til bestemte tjenester, som f.eks. minibanker, nettbanker, adgangskort eller mobiltelefoner. Den fungerer som et passord. En PIN-kode er vanligvis på fire siffer, noe som gir 10000 mulige kombinasjoner. Blir PIN-koden på en mobiltelefon sperret, må man enten bruke en lengre PUK-kode eller kontakte leverandøren av tjenesten for å få tilgang. En PIN-kode bør aldri oppbevares tilgjengelig for uvedkommende, og bør være umulig å gjette seg frem til. PIN-koder til bruk ifm elektronisk signatur (PKI) kan være opptill 8 siffer lange.
PKI	”Public Key Infrastructure” - Infrastruktur for offentlig nøkkelkryptering er en teknologi for å utstede, administrere og bruke elektronisk ID og e-signatur basert på en standardisert krypteringsteknologi.
PKI-anvendelser	Tjenester og applikasjoner som benytter elektronisk ID og signatur (basert på PKI) for autentisering, sikring av integritet, konfidensialitet eller uavviselighet.
Privat nøkkel	PKI baserer seg på offentlig nøkkelkryptering, som fungerer ved at man har to nøkler som kompletterer hverandre slik at når det krypteres med den ene, kan det kun dekrypteres med den andre. I en PKI benyttes disse nøklene slik at den ene holdes hemmelig og kun tilgjengelig for sertifikatinnehaveren, dette kalles den private nøkkelen, Den andre offentliggjøres for eksempel i en katalog og er tilgjengelig for alle, dette kalles den offentlige nøkkelen.
RA	Når noen skal utstede et sertifikat, har de behov for å registrere og identifisere sertifikatinnehaverne. Den som utfører denne oppgaven kalles RA, Registreringsautoritet.
Rammeavtale	Rammeavtalen er inngått mellom Kunden og Leverandøren. Avrop og betaling skjer imidlertid direkte mellom den enkelte etat og Leverandøren. De etater som skal kunne gjøre avrop under en rammeavtale, må enten være underlagt Kundens instruksjonsmyndighet eller på forhånd ha gitt Kunden fullmakt til å inngå rammeavtalen på etatens vegne. Rammeavtalen inngås typisk etter anbudskonkurranse eller forhandlinger iht. anskaffelsesregelverket, mens det enkelte avrop skjer direkte i forhold til Leverandøren iht. enkle prosedyrer som fremgår av selve rammeavtalen.

Rammeverk	Et sett med felles retningslinjer og overordnede krav som danner grunnlag for virksomhetsinterne prosesser og vurderinger.
Risiko	Risiko kan uttrykkes som et produkt av konsekvenser og sannsynlighet for at disse inntreffer. Å ta en risiko er å sette ett eller annet på spill. Når noe risikeres, tar man en sjanse for å miste det. Hva man risikerer å miste, kommer an på hva man satser og hva slags risikopreferanser en person/virksomhet har.
Risiko- og sårbarhetsanalyse	Risiko og sårbarhetsanalyse (ROS) er et verktøy for å kunne foreta en risikovurdering og sette opp en prioritert liste over risikoreduserende tiltak, frister og ansvar for oppfølging.
Samtrafikk	Samtrafikk innebærer et samspill mellom ulike eID-leverandører på fire nivå: teknisk, policymessig, forretningsmessig og juridisk. Samtrafikk mellom to eID-leverandørenes løsninger vil si at man som bruker av deres tjenester kun trenger å forholde seg til en av dem (i likhet med telefonitjenester).
Samtrafikknav	Et samtrafikknav vil tilby en tjeneste som sørger for samtrafikk av tjenester fra flere eID-leverandører som ikke har samtrafikk seg i mellom. Navet skal sørge for teknisk, juridisk, policymessig og forretningsmessig samspill mellom eID-leverandørene. Offentlige virksomheter vil kun trenge én avtale med, og én teknisk tilkobling til, samtrafikknavet.
Sertifikat	Et sertifikat er en form for elektronisk identitetsbevis som kan benyttes til å verifisere/ validere elektroniske signaturer basert på PKI-teknologi. Sertifikatet knytter innehavers navn til informasjon om egenskaper ved innehavers elektroniske signatur som gjør det mulig å verifisere den. Sertifikatet bør være utstedt av en tredjepart som alle stoler på, slik at det kan benyttes til å verifisere hverandre på bakgrunn av en elektronisk signatur selv om man ikke kjenner den andre part på forhånd.
Sertifikatutsteder	En som står juridisk ansvarlig for utstedelsen av sertifikat, og dermed knytningen mellom innehavers navn og informasjon om egenskaper ved innehavers elektroniske signatur som gjør det mulig å verifisere den, samt oppdatert statusinformasjon.
Sikkerhetsparameter	Sikkerhet i løsninger kan beskrives ved hjelp av forskjellige sikkerhetsparametere. En sikkerhetsparameter er en faktor som påvirker sikkerhetsnivået i løsningen hvis den endres. Et eksempel er ”Utlevering til bruker”. For en passordløsning vil utlevering være hvordan passord deles ut til brukeren. Er passordene delt ut til bruker på bakgrunn av fysisk legitimering, er det vanskelig å skaffe seg et passord i andres navn. Deles passordene ut over Internett på bakgrunn av påstått identitet er det lett å skaffe et passord i andres navn.

SIM	Subscriber Identity Module (SIM eller SIM-kort) er et kort som legges inn i en GSM mobiltelefon for å identifisere mobiltelefonen opp mot et mobilabonnement. SIM-kortet forteller telefonen hvilken ID kode den skal presentere seg for basestasjonen og sentralen med. [9]
SkattePIN	PIN-kodene som trykkes på skattekortet.
Sluttbruker	Er den som til slutt benytter tjenesten. Dvs. at hvis en tjenesteyter kjøper tjenester av andre, vil tjenesteyter selv være bruker, mens tjenesteyterens kunder igjen vil være sluttbrukere (med mindre disse også er tjenesteytere til andre). F.eks. kan en etat være bruker av samtrafikknavet, mens publikum kan være sluttbrukere av etatens elektroniske tjenester.
Smartkort	Smartkort er et plastkort med chip integrert i seg.
SMS-passord	Er et engangspassord sendt over til en sluttbruker via mobiltelefonen ved bruk av SMS.
SSØ	Senter for statlig økonomistyring (SSØ) har som oppgave å styrke den statlige økonomistyringen og forbedre ressursutnyttelsen på området. SSØ er en rådgiver for sentrale myndigheter innen statlig økonomistyring, og håndterer også statens konsernkontoordning, statsregnskapet og regelverket for økonomistyring i staten. Det er også etablert en gruppe innenfor samfunnsøkonomiske analyser. Samtidig leverer SSØ tjenester innen budsjettering, regnskap, lønn/personal og rådgivning.
Statisk	Med statisk menes her at dokumentasjonen som presenteres for andre som skal verifisere påstått identitet, ikke endres fra gang til gang.
Sårbarhet	Er en svakhet i et system som kan bli utnyttet.
Tilbakekallingslister	Se CRL
Tjenesteportal	En webside, som er en overbygning for flere tjenesteytere. Den gir oversikt og hjelper sluttbrukere å finne frem i tjenesteyternes tjenestetilbud.
To-faktor	En løsning som baserer seg på to autentiseringsfaktorer. Se også autentiseringsfaktor.
Trappetrinnsmodell	Er her benyttet til å beskrive en prismodell der prisen varierer avhengig av bruk. Prisen øker ikke lineært med bruken, men i trappetrinn, med utgangspunkt i et sett med terskelverdier.
Uavviselighet	Uavviselighet er å bekrefte at en handling eller et informasjonselement er uendret (informasjonsintegritet) og at den kan knyttes til en bestemt identitet. Uavviselighet er i mange sammenhenger også omtalt som ikke-benekting.
Uninett	UNINETT-konsernet driver nett og nettjenester for universiteter, høgskoler og forskningsinstitusjoner, og håndterer andre nasjonale IKT-oppgaver. Konsernet eies av Kunnskapsdepartementet og består av morselskap og fire

	datterselskaper.
Universalnøkkel	En nøkkel som kan benyttes overalt. En slik universalnøkkel gir høyere brukervennlighet, men øker risikoen da alt av verdi beskyttes av samme nøkkel.
USB-token	Minnepinne-aktig enhet som kan kobles til USB-utgangen på datamaskinen for lesing og skriving. Den kan for eksempel inneholde signeringsdata eller lagrede filer.
Utstedertjeneste	Er i denne sammenheng betegnelse for en tjeneste der man utsteder autentiseringsløsninger (eID).
Velferdsmeldingen	Er en stortingsmelding om sosial velferdspolitikk. St. meld. nr. 35 (1994-95).
Virksomhetssertifikat	Et sertifikat der sertifikatinnehaver er en juridisk person.

1 Sammendrag og forslag.

Foreliggende forslag til strategi er utarbeidet av en arbeidsgruppe nedsatt av Fornyings- og administrasjonsdepartementet sommeren 2006, med mandat å fremme et forslag til ny/revidert strategi for bruk av elektronisk ID (eID) og elektronisk signatur (e-signatur) i samband med elektronisk kommunikasjon med, og i offentlig sektor. Strategiarbeidet skulle ta utgangspunkt i erfaringer høstet i forbindelse med realisering av foregående strategi.[1] Mandatet for arbeidet finnes i vedlegg 2 til dette dokumentet. Mandatet legger til grunn en teknologinøytral forståelse av begrepene ”eID” og ”e-signatur”.

Gruppen har hatt 11 møter høsten 2006 og januar 2007, herunder også flere møter med relevante markedsaktører. Foreliggende forslag har vært på intern høring i deltagende virksomheter. Strategiforslaget inneholder anbefalinger på følgende områder:

1. Rammeverk[2] for autentisering og signering (uavviselighet)
2. Forsyning av innbyggere med eID og e-signatur
3. Forsyning av virksomheter med eID og e-signatur
4. Etablering av et offentlig samtrafikknav for eID og e-signatur
5. Forretningsmodeller for punktene 2-4 ovenfor.

Forslagene er sammenfattet i to dokumenter:

1. Strategi for eID og e-signatur i offentlig sektor (dette dokumentet).
2. Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor (vedlegg 1).

Rammeverket legger grunnlaget for de nødvendige felles sikkerhetsnivåer som offentlig sektor har behov for. Strategidokumentet skal vise hvilke strategiske valg som bør tas for at det kan etableres løsninger som legger til rette for felles bruk av eID og e-signatur på utvalgte sikkerhetsnivåer.

1.1 Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor

Arbeidsgruppen anbefaler at det vedlagte rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlige sektor, legges til grunn som en anbefaling for alle offentlige virksomheter som har tatt, eller planlegger å ta i bruk, løsninger for elektronisk autentisering og signering i slik kommunikasjon.

Rammeverket omfatter 4 risikonivåer beskrevet i henhold til kriteria som konsekvenser for liv eller helse, økonomisk tap/ merarbeid/ økte kostnader, tap av renommé (anseelse,

[1] ”Utbredelse av PKI-anvendelser i offentlig sektor. Strategivalg”. Moderniseringsdepartementet, februar 2005.

[2] Som kan forstås som et sett av feller retningslinjer og krav til bruk av autentisering (med ulike eID) og uavviselighet (som tilsvarer krav til elektronisk signering) i elektroniske tjenester i forvaltningen.

tillit og integritet), hindring i straffeforfølgelse, uaktsomt bidrag til lovbrudd, bryderi/ulempe.

Nivå 1 er det lavest/ingen risiko for negative konsekvenser ved sikkerhetsbrudd i forbindelse med autentisering eller signering. Nivå 4 medfører store konsekvenser.

Videre definerer rammeverket 4 sikkerhetsnivåer for autentisering og signering. Nivåene er definert ut fra kriteria som krav til autentiseringsfaktor(er), utlevering til bruker, sikring av autentiseringsfaktorer ved lagring, krav til uavviselighet (ekstra krav for å sikre ikke-benekting og integritet), krav til offentlig godkjenning (dvs. uavhengig verifisering av at offentlige krav er oppfylt).

Det er definert 4 sikkerhetsnivåer for autentisering/uavviselighet, der nivå 1 innebærer intet behov for autentisering (åpen informasjon), mens nivå 4 er ment å anvendes på tilgang til, og sikring av sensitiv informasjon.

Hver offentlig virksomhet, i kraft av sitt ansvar for informasjonssikkerhet i egne IT-systemer, vil måtte foreta en vurdering av sensitiviteten av informasjonen som behandles i virksomheten og deretter velge hvilket risikonivå, og tilhørende sikkerhetsnivå, som vil være passende for den aktuelle informasjonen. Denne vurderingen må gjennomføres før etablering av elektroniske tjenester der informasjonen kan bli kommunisert elektronisk til inbyggere eller næringslivet.

Rammeverket omtaler eksempler på teknologiske løsninger som kan anvendes på de ulike sikkerhetsnivåer. Strategiens anbefalinger vedrørende forsyning av befolkningen og virksomheter med eID/e-signatur tar utgangspunkt i **sikkerhetsnivåene 3 og 4**. eID på nivå 3 tilsvarer den type påloggingsløsninger som i dag benyttes på Minside og Altinn, mens eID/e-signatur på nivå 4 tilsvarer en eID på nivå Person Høyt i Kravspesifikasjon for PKI i offentlig sektor.

Det vil også bli utviklet en veileder til rammeverket, der eksempler på elektroniske tjenester som er plassert på de ulike risiko- og sikkerhetsnivåene, vil bli tatt med.

1.2 Forsyning av innbyggere med eID og e-signatur

En sentral problemstilling i forbindelse med bruk av eID for tilgang til elektroniske tjenester fra forvaltningen er spørsmålet om utbredelse av eID blant aktuelle brukere av disse tjenester. I tidligere strategier antok man at markedet vil sørge for at de innbyggere som aktivt bruker Internett vil besitte en eID av tilstrekkelig kvalitet og brukervennlighet. Det har imidlertid vist seg at at en slik utbredelse går nokså langsomt og at spredning av eID til innbyggere er tett knyttet sammen med bestemte private tjenester, som nettbank og tipping. Offentlig sektor har små muligheter for å styre takten i denne utbredelsen, målgruppene det siktes på, og kvaliteten / typen på eID som utstedes.
Det oppstår derfor et behov for at det offentlige tar ansvaret for forsyningen av eID til sine målgrupper blant innbyggere og næringslivet.

Når det gjelder forsyning av brukere av tjenester fra offentlig sektor med eID og e-signatur anbefaler gruppen for det første at Skattedirektoratet gis i oppdrag å etablere en felles ordning for utstedelse av **eID på sikkerhetsnivå 3**. Distribusjon av slik eID til innbyggere skal basere seg på gjenbruk av den distribusjon av PIN-koder som skjer i forbindelse med Skattekort fom 2007. Det skal utvikles nærmere tekniske kravspesifikasjoner for denne type eID. Ordningen samordnes med de påloggingsløsningene som er etablert i Minside og Altinn.

Gruppen anbefaler videre at alle offentlige virksomheter som tilbyr elektroniske tjenester på nett som ikke krever høyere sikkerhetsnivå , legger til rette for bruk av denne felles eID så snart ordningen er operativ. Virksomheter som i dag benytter egenutviklede typer eID anbefales i løpet av en overgangsperiode å innpasse sine sikkerhetsnivåer til de som er definert i rammeverket, og konvertere til bruk av felles løsning for eID på dette sikkerhetsnivå på et tidspunkt der helhetlig vurdering av brukervennlighet og kostnads-nytteforhold tilsier det.

Når det gjelder forsyning av befolkningen med **eID på sikkerhetsnivå 4** er behovsbildet noe mer uklart. Sterke signaler er likevel kommet fra helsesektoren og NAV, om at deres utviklingsplaner for elektroniske tjenester rettet mot innbyggere som involverer sensitive personopplysninger, forutsetter at det bør finnes en betydelig utbredelsesgrad av eID-løsninger på dette nivået før 2009. Gruppen vurderer det dit hen at både de sterk markerte behovene i helse og sosialsektoren, og den generelle teknologiutviklingen, samt utviklingen vi ser i bruk av Internett, tilsier at brukere av elektroniske tjenester etter hvert vil måtte besitte eID og e-signatur løsninger som ligger på sikkerhetsnivå 4. Man kan her peke f.eks. på utviklingen i banksektoren (som er en stor tilbyder av elektroniske tjenester), der kravene til sikkerhet skjerpes i takt med utviklingen i nettkriminalitet. Også i offentlig sektor observerer man en trend der brukere gjerne benytter den sikkerhetsløsningen som både er enkel å bruke, og tilstrekkelig sikker til å kunne gi tilgang til flere tjenester. Eksemplet på dette er bl.a. Altinn-portalen, der brukere som har anskaffet seg smartkort med eID i markedet benytter nå dette til alle tjenester i Altinn, selv om de også er registrert med eID på lavere sikkerhetsnivå. Dessverre er smartkortene forholdsvis kostbare og derfor er det lite omfang på bruk av disse.

Gruppen mener derfor at det er viktig å gjøre rimelig raske samordningsgrep for eID på sikkerhetsnivå 3 og samtidig sørge for at en utvikling blir satt i gang som leder an til at eID-løsninger på sikkerhetsnivå 4 gradvis vil overta fra 2009 og utover.

Gruppen har vurdert flere alternativer for forsyning av innbyggere med eID på sikkerhetsnivå 4, ikke minst med utgangspunkt i at det finnes flere leverandører av godkjente løsninger i markedet. Markedet er imidlertid umodent, og løsningene som finnes i større omfang oppfyller bare delvis de offentlige krav, i den forstand at de ikke er selvdeklarert og har slik teknologisk beskaffenhet at de ikke kan brukes i alle sammenhenger som er aktuelle i offentlig sektor. Samtidig gjør forretningsmodeller som enkelte aktører legger til grunn for salg av sine eID-konsepter det vanskelig å inngå kontrakter som sikrer nødvendig samordning i det offentlige.
Det har også kommet innspill fra flere hold i offentlig sektor om sterkere statlig styring med elektronisk ID som vil kunne benyttes til tilgang til opplysninger som har høye

krav til konfidensialitet, selv om disse ikke faller under sikkerhetsloven, der det gjelder egne, meget strenge regler.

Parallelt med arbeidet i denne gruppen har det i regi av Justisdepartementet pågått en utredning av en mulig ordning med et nasjonalt ID-kort. Ordningen vil innebære at et nasjonalt ID-kort med eID på nivå "Person Høyt" utstedt av en offentlig utsteder på frivillig basis distribueres til befolkningen gjennom politiets passutstederfunksjon, med nødvendige tillegg. Kortet planlegges å kunne tilbys til alle norske statsborgere samt alle ikke-statsborgere som enten har et fødselsnummer eller et D-nummer tildelt av norske myndigheter. Gruppen mener at dersom ordningen blir realisert, er dette det beste alternativet for forsyning med eID på dette sikkerhetsnivå, særlig sett fra samfunnsøkonomisk perspektiv og offentlig ressursbruk samlet sett.
Dette er derfor alternativ A for eID på nivå 4, jfr. kap. 4.4.

Den offentlige utsteder som etableres ifm med utstedelse av eID på nasjonalt ID-kort bør også, hvis behovsvurderinger tilsier det, kunne tilby utstedelse av eID av typen "Person Høyt" på andre kort eller eID-bærere, f.eks. NAV-etatens helsetrygdkort eller private kort, ev. SIM-kort i mobiltelefoner, i samarbeid med private tjenestetilbydere, som banker og mobilselskaper. Det finnes erfaringer med den type multibærer-strategi fra Finland og Sverige som tilsier at slik diversifisering bidrar til raskere spredning av løsninger i befolkningen. **Dette er alternativ A1 og A2 for eID på nivå 4.**

Dersom ordningen med nasjonalt ID-kort ikke blir realisert, anbefaler gruppen at en konkurranse utlyses i markedet for eID på sikkerhetsnivå 4, med sikte på å inngå en avtale som vil sikre utbredelse av en eID som oppfyller de offentlige krav, og som når ønskede målgrupper på de tidspunkter når offentlige elektroniske tjenester på dette nivået blir bredt tilgjengelig. **Dette er alternativ B for eID på nivå 4.**

1.3 Forsyning av virksomheter med eID

Når det gjelder distribusjon av **virksomhets-eID** (virksomhetssertifikater) har gruppen vurdert ulike modeller, der felles rammeavtale var ett aktuelt alternativ. Gruppen har imidlertid vurdert det dit hen, at med den foreliggende forretningsmodellen for salg av slike sertifikater i markedet (anskaffelsespris og periodisk vedlikehold) vil forretningspotensialet for en aktuell leverandør være lite, tatt i betraktning at behovsbildet i offentlig sektor er usikkert og at det er begrensede mengder sertifikater som vil anskaffes i de nærmeste årene. Samtidig erkjenner gruppen at Brønnøysundregistrene er "ID-forvalter" for alle norske organisasjoner gjennom sitt ansvar for Enhetsregisteret. Det er en naturlig forlengelse av en slik rolle å også ta ansvaret for den elektroniske identiteten til virksomhetene. På grunnlag av dette anbefaler gruppen at Brønnøysundregistrene antar rollen som ansvarlig utsteder og etablerer et tilbud for utstedelse av virksomhets-eID (virksomhetssertifikater) til alle organisasjoner som er registrert i Enhetsregisteret. Tilbudet kan realiseres gjennom en konkurranse i markedet for kjøp av nødvendige produkter og/eller tjenester. Gruppen anbefaler videre at offentlige virksomheter som vil skaffe seg en virksomhets-eID skal skaffe seg den fra Brønnøysundregistrene. Ordningen skal være frivillig for ikke-offentlige virksomheter. Virksomhets-eID skal prises på en ikke-diskriminerende måte i forhold til etablerte markedspriser.

1.4 Etablering av et offentlig samtrafikknav for eID og e-signatur

Behovet for en felles løsning som kan tilby enkel og kostnadseffektiv bruk av elektronisk ID og e-signatur i og av offentlige virksomheter som er engasjert i elektronisk kommunikasjon med brukere eller andre offentlige etater, har ikke blitt mindre siden rammeavtalen om en offentlig sikkerhetsportal ble avviklet sommeren 2006. Gruppen har derfor vurdert ulike modeller for hvordan en slik felles løsning kan etableres og særlig hvilken rolle og hvilken funksjonalitet en slik løsning skal ha.

Gruppen kom, på bakgrunn av bl.a. erfaringer med tidligere modeller, til at behovet for felles, grunnleggende funksjonalitet for bruk av eID og e-signatur i offentlig sektor best kan ivaretas ved at det i offentlig regi etableres et **samtrafikknav** for eID / e-signatur. Et slikt "nav" vil i praksis være en teknisk innretning som ikke vil være synlig for sluttbrukere av tjenester, men den vil tilby fellestjenester for alle offentlige virksomheter som tilbyr elektroniske tjenester til sluttbrukere.

Samtrafikknavet etableres som en offentlig forvaltet løsning, hvor den tekniske infrastrukturen etableres og leveres av en markedsaktør etter konkurranse. Drift og vedlikehold gjennomføres gjennom en langsiktig drifts- og vedlikeholdsavtale med markedsaktøren. Forvalteren av navet skal også ha ansvaret for å inngå nødvendige avtaler med utstedere av felles eID og e-signatur på hhv. sikkerhetsnivå 3 og 4, som skal kunne benyttes gjennom navet. Det foreslås at Brønnøysundregistrene skal ha ansvaret for å forvalte samtrafikknavet.

Samtrafikknavet skal i første omgang tilby et begrenset utvalg tjenester, som kan utvides etter behov. Utvalget av tjenester i første versjon vil dog være begrenset til:

- Autentisering av sluttbrukere med ovenfor nevnte typer felles eID, som også vil omfatte funksjoner knyttet til validering av sertifikater og fødselsnummeroppslag
- Signering på webskjema, og i en lokal løsning (grensesnitt for integrasjon i fagsystemer, som f.eks. pasientjournalsystemer)
- Digitalt arkiv (innsynsarkiv) for signerte dokumenter/hash-verdier, som et tilbud til de virksomheter som selv ikke vil ha tekniske forutsetninger til å lagre digitalt signerte dokumenter over lengre tid.
- Videreformidling av ferdig validert eID (felles pålogging), som en generell funksjonalitet, som kan tas i bruk av ulike sammenslutninger av offentlige etater som tilbyr tjenester på nett.

Flere funksjoner, herunder konfidensialitetssikring (dvs. kryptering), skal kunne integreres i samtrafikknavet etter hvert, basert på prioriteringer og krav fra brukervirksomheter.

Det legges i utgangspunktet opp til at bruk av samtrafikknavet skal være frivillig. Offentlige virksomheter som har tjenester på nett vil imidlertid pålegges å legge til rette

for bruk av felles eID på nivå 3 og 4, så snart ordninger for å utstede disse er operative. Dette pålegget bør sannsynligvis gis gjennom en forskrift.

1.5 Forretningsmodell

Med utgangspunkt i at samtrafikknavet skal være en offentlig forvaltet løsning, som i utgangspunktet støtter offentlig utstedte eID, vil forretningsmodellvalget begrense seg til valget mellom sentral offentlig finansiering eller desentralisert finansiering basert på bruksavgifter fra brukervirksomheter. Gruppen legger til grunn at innbyggeren ikke skal belastes med brukskostnader for bruk av eID eller e-signatur mot offentlige tjenester. Innbyggeren kan imidlertid belastes kostnader ved selve anskaffelse av eID.
Vurderinger som gruppen har gjort peker bl.a. i retning av at det er svært vanskelig å etablere kostnadsdelingsmodeller i en tidlig fase av bruken av transaksjonsbasert verktøy som eID/ e-signatur er. Det er først når bruksmønsteret er etablert / er observerbart at slike modeller kan tas i bruk.
Arbeidsgruppen anbefaler på grunnlag av dette **en forretningsmodell** som innebærer at kostnadene ved etablering og bruk sentraliseres hos forvalter av samtrafikknavet. Videre legger gruppen til grunn at den enkelte statlige virksomhet ikke belastes med kostnadene siden bruken rammefinansieres i sin helhet. Samtrafikknavet skal inngå nødvendige avtaler med eID-leverandørene, slik at de offentlige virksomhetene som knyttes til samtrafikknavet skal kunne bruke aktuelle eID i sine tjenester. Den enkelte statlige virksomhet skal inngå en ikke-økonomisk avtale med samtrafikknavet. Avtalen vil regulere tilgang og ytelse til de tjenester som inngår i navet, og bruk av de eID-løsningene som er tilknyttet samtrafikknavet.
Kommunale virksomheter vil måtte håndteres på linje med de statlige, etter at finansieringsspørsmålet er avklart.

Forholdet mellom samtrafikknavet og eID-leverandørene vil reguleres med ikke-økonomiske avtaler som primært vil dekke tekniske forhold og ansvarsforhold. Samtrafikkforvalter vil ev. inngå og forvalte en økonomisk avtale med en kommersiell leverandør av eID på nivå 4 (alternativ B) hvis alternativ A ikke lar seg gjennomføre.

1.6 Økonomiske og administrative konsekvenser

Forslagene fremmet i denne strategien vil kreve noen investeringer fra offentlig sektors side, særlig knyttet til etablering av offentlige utstdere av eID. Disse investeringer kan sammenlignes med investeringer i en veginfrastruktur, som muliggjør trafikk på strekninger som tidligere ikke var fremkommelige. eID må betraktes som en grunnleggende infrastruktur for offentlig sektors muligheter til i stor skala å legge om tjenesteyting fra papirbaserte kanaler til elektroniske. eID-infrastrukturen er "tosidig" av natur og preget av nettverkseffekter, dvs. det er nødvendig **både** med stor utbredelse av eID hos innbyggere **og** stort antall tjenester som kan nyttigjøre seg denne eID, **samtidig**. Å kunne oppnå en slik nødvendig koordinering uten at offentlig sektor tar grep om infrastrukturen har vist seg å være svært vanskelig, om ikke umulig.
Gevinsten ved felles grep er bl.a. at de virksomheter som per i dag ikke har utviklet egne eID løsninger for innbyggere og virksomheter, ikke vil behøve å bruke ressurser for å etablere løsning for dette. Ressursbruken hos de enkelte offentlige virksomheter kan isteden konsentreres om utvikling av nye elektroniske tjenester. Dette vil igjen gi

gevinster både for sluttbrukere og for offentlig sektor. Brukere vil få et mer brukervennlig tilbud (”døgnåpen” forvaltning), og offentlige virksomheter vil kunne fokusere ressursbruken på viktige utviklingsoppgaver fremfor rutinepregede tjenester.

Felles, offentlig forsyning av eID vil gi direkte besparelser for de offentlige virksomheter som i dag distribuerer egne eID til ”sine” målgrupper, ved at disse eID kan fases ut. For brukere vil den umiddelbare gevinsten være en betydelig forenkling av hverdagen, ved at hun slipper å forholde seg til mange typer ID for ulike tjenester.

Flere elektroniske tjenester fra offentlig sektor er for lite brukt i dag, bl.a. fordi tungvinn håndtering av eID ”skremmer” potensielle brukere. Tilbudet om felles eID vil kunne øke bruken av allerede eksisterende tjenester, og derved gi raskere retur på investeringer i disse, samt skape incentiver til både utvikling og bruk av nye tjenester.

Senter for statlig økonomistyring (SSØ) har på oppdrag fra arbeidsgruppen utarbeidet en samfunnsøkonomisk analyse av ulike modeller for felles løsninger for bruk av eID og e-signatur, som grunnlaget for valg av samtrafikknav som felles løsning. Analysen påviste bl.a. at det ligger en besparelsesgevinst på 233 MNOK bare ved at offentlige virksomheter ikke vil behøve å utarbeide egne kravspasifikasjoner og foreta anskaffelser av egne eID-løsninger i markedet. Investeringskostnaden for etablering av navet estimeres til ca 10 MNOK, og selv med årlige driftskostnader av samme størrelse gir bruk av et felles samtrafikknav en betydelig samfunnsøkonomisk gevinst.

Det er samtidig viktig å påpeke at forslagene i strategien også må konsekvensvurderes i forhold til **krav til universell utforming**, slik at regjeringens målsettinger på dette området vil bli ivaretatt. Personer med nedsatt funksjonsevne skal ha mulighet til personlig utvikling, deltakelse og livsutfoldelse på linje med andre samfunnsborgere. Alle skal ha like rettigheter og så langt som mulig kunne bestemme over sitt eget liv. Det videre arbeidet med tilrettelegging for felles eID må derfor ta høyde for at personer med nedsatt funksjonsevne kan ivareta sine rettigheter og plikter som samfunnsborgere. I forhold til forslagene fremsatt i dette dokumentet vil dette praktisk innebære at det ved utvikling av kravspesifikasjoner for eID av ulike typer må inntas krav til universell utforming, i den grad kravene er eID-spesifikke, og ikke tjenestespesifikke. Det er derfor på nåværende tidspunkt vanskelig å anslå de eventuelle økonomiske konsekvensene av disse kravene. Dette må gjøres etter at aktuelle kravspesifikasjoner foreligger.

2 Innledning

2.1 Bakgrunn

Utviklingen av tilrettelagte elektroniske selvbetjeningstjenester og elektronisk innrapportering til det offentlige står sentralt i Regjeringens arbeid med fornying av offentlig sektor. Regjeringen har også ansvaret for å få til den nødvendige *samordningen* av offentlig infrastruktur og offentlige tjenester på IKT-området. Utviklingen av elektroniske tjenester må tilpasses brukere med ulike behov. Innbyggere og bedrifter skal enkelt finne frem til det elektroniske tjenestetilbudet uten å måtte forholde seg til ulike metoder for identifisering og signering, samt sikring av konfidensialitet i den elektroniske dialogen. For å kunne realisere dette er det behov for å etablere en felles infrastruktur for offentlig sektor.

Formålet med å etablere en slik infrastruktur er todelt. For det første er det et mål å forenkle slik at den enkelte bruker skal kunne benytte de samme sikkerhetsmekanismene på elektroniske selvbetjenings- eller innrapporteringstjenester fra ulike offentlige virksomheter. For det andre er det et mål å redusere kompleksiteten og kostnaden knyttet til implementering av sikkerhetsløsninger for den enkelte offentlige virksomhet.

I 2004 ble det iverksatt et arbeid for å samordne offentlig sektors behov og krav knyttet til anvendelse av PKI til autentisering, signering og konfidensialitetssikring. Dette arbeidet munnet ut i ”Kravspesifikasjon for PKI i offentlig sektor”. Kravspesifikasjonen definerte tre sikkerhetsnivåer for eID basert på PKI: ”Person Høyt”, ”Person Standard” og ”Virksomhet” med tilhørende tekniske og administrative krav.
Det ble videre utarbeidet en strategi for utbredelse av PKI-anvendelser i offentlig sektor som regjeringen besluttet iverksettelse av den 17.2.2005. Strategien var utarbeidet av en bred sammensatt gruppe med representanter fra store statlige etater og kommuner. Strategien hadde en tidshorisont ut 2006. Strategien definerte tre hovedtiltak – etablering av en offentlig sikkerhetsportal gjennom en rammeavtale med en markedsaktør, etablering av en offentlig godkjenningsordning for PKI-baserte eID, definert i Kravspesifikasjon for PKI i offentlig sektor og etablering av en rammeavtale for virksomhetssertifikater og ansattsertifikater til bruk internt i offentlig sektor.
Den inngåtte rammeavtalen om sikkerhetsportalen måtte avvikles grunnen manglende oppslutning fra PKI-leverandører om den forretningsmodellen som ble lagt til grunn for avtalen. Godkjenningsordningen ble etablert i Post- og teletilsynet i desember 2005. Flere leverandører med flere sertifikatklasser har deklarert sine løsninger i ordningen pr. idag. Brønnøysundregistrene påbegynte arbeidet med virksomhetssertifikater og ansattsertifikater våren 2006. Dette arbeidet blir nå samkjørt med en ny strategi for eID og e-signatur i offentlig sektor. Arbeidsgruppen legger til grunn en bredere forståelse av eID og dette dokumentets forslag til strategi skal avløse den forrige strategien, som var basert på PKI.

2.2 Mandat for strategiarbeidet

Mandat til arbeidsgruppen er gjengitt i vedlegg 2. Arbeidsgruppen skal på oppdrag fra FAD foreslå en ny strategi for eID og elektronisk signatur i offentlig sektor. Den nye strategien baseres på de erfaringer som offentlig sektor har vunnet i forbindelse med den gjeldende strategien.

Strategiarbeidet skal frembringe to resultater (dokumenter):

- Sikkerhetsrammeverk for elektronisk kommunikasjon med og i offentlig sektor
- Strategidokument med forslag til beslutninger knyttet til etablering, organisering og forvaltning foruten langsiktige veivalg for bruk av eID og e-signatur i og for kommunikasjon med offentlig sektor, med kobling til sikkerhetsrammeverket.

Arbeidsgruppen er i mandatet bedt om å utrede en rekke ulike aspekter og problemstillinger knyttet til utbredelse og anvendelse av eID med og i offentlig sektor. Innen følgende tematiske områder skal gruppen gi sine anbefalinger:

- forsyning av publikum med eID/e-signatur, herunder gjenbruk av eksisterende løsninger
- felles offentlige løsninger for validering av eID og e-signatur.
- offentlig styring og spesielt for statens rolle
- forretningsmodeller for bruk av fellesløsninger for eID og e-signatur
- forsyning av offentlig sektor med virksomhetssertifikater og ansattsertifikater til eget bruk

2.2.1 Gruppens fortolkning av mandatet

Arbeidsgruppen har drøftet mandatet og har overfor oppdragsgiver bedt om at mandatet har blitt presisert med hensyn på begrepet eID/signatur. Denne strategien tar utgangspunkt i en bred forståelse av eID som elektronisk identitet, som kan benyttes til autentisering og realiseres med ulike teknologier, herunder PIN-koder, sms-passord, PKI osv. Elektronisk signatur forstås her som løsninger som knytter et innhold til en identitet på en uaviselig måte. Løsningene kan realiseres gjennom PKI eller bruk av eID i kombinasjon med andre teknologier.

Arbeidsgruppen legger til grunn at strategien i hovedsak retter seg mot elektronisk kommunikasjon for brukere av offentlige elektroniske tjenester, som innbyggere og næringslivet. Behovet for forsyning av personer og virksomheter med elektronisk eID, og behov for en felles samtrafikkløsning er derfor vurdert og beskrevet i dette perspektiv. Anbefalingene omfatter ikke de rent interne behov for elektronisk kommunikasjon i offentlig sektor. Personsertifikater er i enkelte virksomheter tatt i bruk som ansattsertifikater, en slik tilnærming kan fungere dersom man godtar en kobling av roller. Samtidig kan det være grunner for at ansatte ønsker å skille mellom sin rolle som ansatt og privatperson. Arbeidsgruppen mener at det å utrede og gi anbefalinger om bruk av ansattsertifikater internt i forvaltningen er en omfattende problemstilling som bør være gjenstand for en separat utredning som bør ta utgangspunkt i en behovsvurdering hos de enkelte virksomheter. Arbeidsgruppen valgte likevel å gi en anbefaling vedrørende forsyning av virksomhetssertifikater til offentlige virksomheter. Anbefalingen er gitt bl. a. på bakgrunn av kartleggingsarbeidet og behovsvurderinger gjennomført av Brønnøysundregistrene og i særlig grad av helsesektoren.

Tematisk har arbeidsgruppen valgt å utarbeide strategien gjennom å gruppere mandatpunktene i tre hovedkategorier; forsyning av eID/e-signatur, samtrafikk i offentlig sektor og forretningsmodeller for eID /e-signatur.

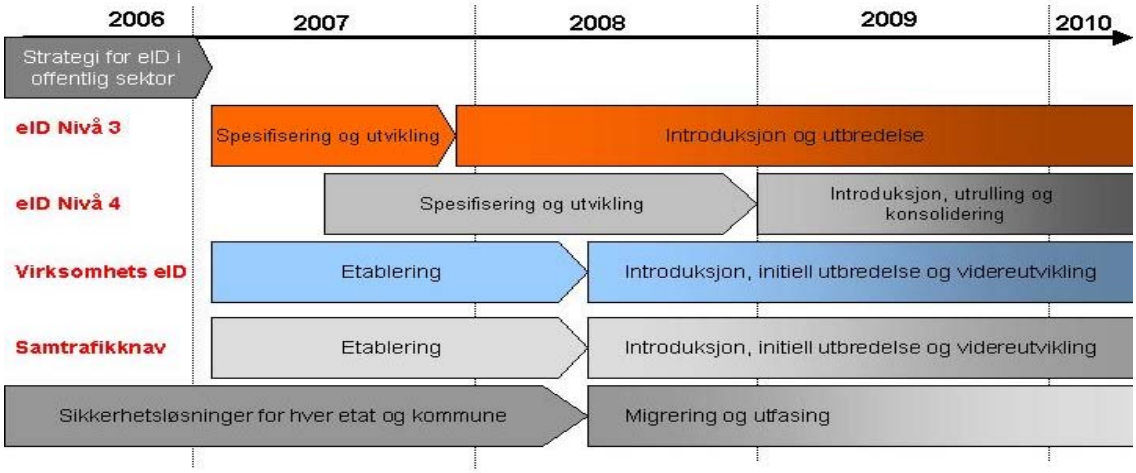
2.3 Visjon, virketid og milepæler for strategien

Etableringen av en robust og fremtidsrettet infrastruktur på eID-området sammenfaller med offentlig sektors arbeid med å realisere en elektronisk forvaltning i henhold til stortingsmelding nr. 17 2006 om IKT og eNorge 2009. Dette vil stille store krav til endringsprosesser i forvaltningen, organisatoriske, juridiske, og tekniske.

Visjonen for arbeidet med bruk av eID i og med offentlig sektor peker mot en ønsket tilstand på lang sikt. Arbeidsgruppen legger til grunn følgende visjon:

> *Innen 2014 skal elektronisk kommunikasjon være den foretrukne kommunikasjonsmåten mot offentlig sektor. Kommunikasjonen skal foregå på en trygg og tillitvekkende måte ved bruk av eID og e-signatur. Alle landets innbyggere vil ha en offentlig elektronisk ID og alle næringslivsforetak vil benytte virksomhets-eID i sin samhandling med offentlige virksomheter.*

Dette dokumentet inneholder forslag til strategi for realisering av den ovenstående visjonen. Strategien beskriver veivalg og tiltak for de første 3 årene frem mot 2014. Gruppen anbefaler tiltak som gjennomføres raskt, dvs ved utgangen av 2007. I tillegg består perioden 2008-2009 av flere tiltak som gjennomføres i parallell.



Figur 1 Gjennomføringsplan

Umiddelbar gjennomføring (2007): etablering av en offentlig utsteder av eID på sikkerhetsnivå 3

Parallell gjennomføring (2008-2009): etablering av en offentlig utstedelse av eID på sikkerhetsnivå 4, etablering av et felles samtrafikknav for eID, etablering av en offentlig utstedelse av virksomhets-eID.

2.4 Rammeverket for autentisering og uavviselighet.

Et rammeverk i denne sammenhengen innebærer et sett av felles krav og retningslinjer for bruk av autentiseringsløsninger og håndtering av uavviselighet i elektronisk samhandling mellom forvaltningen og brukere.

Behovet for slike rammeverk bunner i ønsket om en brukerorientert elektronisk forvaltning, der brukerne møter en enhetlig grenseflate, og ikke må forholde seg til mange teknologiske løsninger og fragmentert tilgang til tjenester. Enkelte land, som f.eks. Canada og Australia, har tuftet sine rammeverk på bruk av én, bestemt teknologi, nemlig PKI, mens andre land, som USA og Storbritannia, har valgt en mer teknologinøytral tilnærming og utviklet rammeverk som kan realiseres med ulike typer autentiseringsteknologier.

For å dekke behovet for uavviselighet, som her forstås som sikring av ikke-benekting og integritet av elektroniske dokumenter eller transaksjoner, må slike teknologinøytrale rammeverk også stille tilleggskrav til autentiseringsløsninger.
I arbeidet med denne strategien har vi valgt å ta utgangspunkt i den teknologinøytrale tilnærmingen, som også ligger til grunn for det vedlagte rammeverket.

En egen arbeidsgruppe ble nedsatt av strategigruppen for å fremme et forslag til rammeverk. Gruppens sammensetning omtales i Vedlegg 2. Gruppen leverte et komplett utkast til rammeverk, som strategigruppen justerte noe, bl.a. når det gjelder beskrivelse av krav til sikkerhetsnivå 4. For fullstendig oversikt over rammeverkets innhold viser vi til Vedlegg 1.

Strategianbefalinger som gjelder forsyning av forvaltningens brukere med eID tar utgangspunkt i de sikkerhetsnivåer som er definert i rammeverket. Anbefalinger for felles løsninger for eID kan betraktes i to konkrete brukssammenhenger – nemlig eID brukt for tilgang til enkelttjenester hos ulike offentlige virksomheter, og eID brukt for tilgang til mange tjenester på en gang, gjerne gjennom en tjenesteportal, som Minside eller Altinn. Det kan være løsninger på ulike sikkerhetsnivåer som vil være egnet for disse to ulike måter å bruke offentlige e-tjenester på.

Dette kan illustreres på følgende måte:

Sikkerhetsnivå 4	Felles tilgang til mange tjenester som krever høy sikkerhet, også tilgang til slike tjenester i virksomhetene. Vil etter hvert overta for løsninger på nivå 3.
Sikkerhetsnivå 3	Felles tilgang til mange tjenester, også virksomhetenes egne tjenester som krever middels høy sikkerhet.
Sikkerhetsnivå 2	De fleste eksisterende tjenester i virksomhetene. Skal over tid flytte slike tjenester over på sikkerhetsnivå 3.
Sikkerhetsnivå 1	Åpen informasjon, direkte eller via portal.

Rammeverket skal dermed danne utgangspunkt for gradvis standardisering av løsninger for autentisering og uavviselighet som vil benyttes mot brukere av elektroniske tjenester fra forvaltningen. Konklusjoner og anbefalinger knyttet til bruk av eID på de ulike sikkerhetsnivåene er inntatt i kapitlene som omfatter strategi for forsyning av innbyggere og virksomheter med eID (kap. 4 og 5).

2.5 Dokumentets struktur og oppbygning

Kapittel 1 gir et sammendrag av rapporten og oppsummerer de strategiske veivalg som arbeidsgruppen anbefaler knyttet til anvendelse og bruk av eID og elektronisk signatur i offentlig sektor.

Kapittel 2 presenterer arbeidsgruppens mandat og dets fortolkning, definerer visjonen for strategien og setter arbeidet inn i en kontekst. Kapitlet gir også en oversikt over tidshorisonten for realisering av foreslåtte tiltak.

Kapittel 3 gir en kort oversikt over utviklingstrekk i eID- og elektronisk signatur-markedet samt beskriver hvordan offentlig sektor benytter elektroniske autentiserings- og signeringsløsninger i dag. Videre omgandelr kapitlet erfaringer sektoren har med bruk av eID-løsninger og hva de fremtidige behovene på området vil være.

Kapittel 4 behandler mandatpunkt **b**. Kapitlet drøfter ulike forsyningsmodeller for eID/e-signatur på to ulike sikkerhetsnivå for innbyggere og anbefaler tiltak på dette området.

Kapittel 5 behandler mandatpunkt **f**. Det drøfter ulike modeller for forsyning av virksomhetssertifikater i Norge. Den anbefalte modell inkluderer en løsning for offentlig sektor og et tilbud til privat sektor.

Kapittel 6 behandler mandatpunkt **c**. Kapitlet drøfter samtrafikkmodeller for validering av eID/e-signatur og anbefaler en felles løsning for offentlig sektor.

Kapittel 7 behandler mandatpunkt **e**. Det drøfter ulike forretningsmodeller for etablering av felles løsninger for bruk av eID/e-signatur i offentlig sektor og anbefaler et modellvalg.

Kapittel 8 gir en kort beskrivelse av de administrative og økonomiske konsekvensene av arbeidsgruppens anbefalinger.

Vedlegg 1 besvarer mandatpunkt **a**. Det inneholder et felles rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor.

Mandatpunkt **d** behandles i flere kapitler – både kap. 4, 5 og 6, samt også kap. 7 inneholder vurderinger knyttet til dette mandatpunktet.

3 Status knyttet til anvendelse og utbredelse av eID

Dette kapitlet gir status for hvilke tekniske løsninger for autentisering og tjenester som finnes i markedet. Videre beskrives hvilke autentiseringsløsninger som benyttes i offentlig sektor i dag. Til slutt i kapitlet redegjøres det for de fremtidige behovene til offentlig sektor innenfor området eID/signatur.

3.1 Tilgjengelige eID/e-signatur-teknologier – status

Det finnes en rekke ulike typer eID/e-signatur-teknologier i det norske markedet. Nedenstående oversikt beskriver kort hovedtyper av løsninger, deres anvendelsesområde og utbredelse i det norske markedet. Oversikten er av overordnet art og danner ikke en uttømmende liste over alle tilgjengelige løsninger.

Passord og brukernavn Teknologien innebærer et fast passord og brukernavn, som kan presenteres for en server. En av de mest utbredte teknologier for autentisering. Benyttes av en rekke private og offentlige tjenester på Internett. Løsningene er som regel utviklet og implementert som en integrert del av nettjenestene.

Engangspassord Dette er en løsning som ved bruk av tidssynkronisering, el.l. og en kryptoalgoritme genererer et nytt, unikt passord for eksempel hvert minutt. Løsningen kan fåes i en rekke ulike former. Meget utbredt i banksektoren, rulles også ut i form av smartkort (bankkort med chip) med en offline leser. Vil trolig være dominerende løsning for tilgang til nettbanker.

Biometri. Dette er løsninger som benytter måling av ulike biometriske kjennetegn til personer. Det finnes mange ulike typer biometri som måling for eksempel iris, fingeravtrykk, håndflåte, ansikt, stemme, tastaturbruk, duft, signatur og øre. Begrenset utbredelse i Norge, enkelte adgangskontroll anvendelser er aktive. Biometriske pass er nå under utrulling, men er kun til grensepasseringskontroll.

Mobilpassord. Slike løsninger fungerer slik at et engangspassord blir sendt via mobiltelefonen til sluttbruker. Denne løsningen kan være kostnadskrevende ved store volumer. Løsningen kan styrkes gjennom bruk av fast passord, samt gjennom sjekk mot eier av mobiltelefon. Benyttes av flere nettjenester, men de fleste benytter denne teknologien til utsendelse av glemt passord eller kode for å endre passord.

PKI-baserte løsninger. Løsningen kan fås på smartkort, USB-token, mobil (SIM) og i software. Software løsningene kan variere i sikkerhet avhengig av lagringsmetode for den private nøkkelen. Smartkortløsningene kan variere i sikkerhet avhengig av type smartkortleser (eget display og tastatur). Løsninger innenfor denne teknologien er i dag utbredt i helsesektoren og i privat sektor.

Helsesektoren har valgt PKI som eID for samhandling mellom virksomheter. Det er utstedt PKI-basert eID til ca. 1800 leger (600 legekontor). Disse gjør bruk av både virksomhetssertifikat og personsertifikat for kommunikasjon med NAV. I tillegg har ca. 500 apotek og mange sykehus tatt i bruk PKI (virksomhetssertifikat), for meldingsutveksling.

En kommersiell PKI-aktør har distribuert, hovedsaklig gjennom Norsk Tipping, ca. 200.000 smartkort med PKI og 1,8 mill smartkort med "forenklet" eID som kan oppgraderes til PKI ved at kunden logger seg på et nettsted og laster ned PKI-sertifikat til kortet. I tillegg finnes det en annen PKI-leverandør i det norske markedet som satser på bedriftsmarkedet, som pt. antas å ha foreløpig liten spredning.

Kodekort: Prinsippet her er at man har en rekke koder på en papirlapp i nummerert rekkefølge. Noen typer har økt sikkerheten ved at man har puttet på en skrapelodds-funksjon for å synliggjøre hvilke koder som er brukt. En annen måte å øke sikkerheten på, er valg av rekkefølgen kodene benyttes i. Flere banker benytter denne typen løsninger for tilgang til nettbank.

3.2 Samtrafikkløsninger i det norske markedet – oversikt og bruk

Det norske markedet for samtrafikkløsninger er i likhet med markedet for eID preget av et fåtall aktører. Etter det arbeidsgruppen erfarer er det i dag fire kommersielle leverandørkonstellasjoner som tilbyr løsninger for samtrafikk. I tillegg har det offentlige samtrafikkløsninger knyttet til Altinn, Minside og utdanningssektoren.

De kommersielle samtrafikkleverandørene som eksisterer opererer hovedsakelig som uavhengige tredjeparter. Det vil si at de ikke har noen direkte knytning eller eierskapsforhold til eID-leverandører, men integrerer de sikkerhetsløsninger som kundene ønsker. Imidlertid innebærer dette at kunder må inngå separate avtaler med eID-leverandører i tillegg til avtaleforholdet med samtrafikkleverandøren. Løsningene tilbyr i de fleste tilfeller støtte for (sentral) signeringsfunksjonalitet og felles pålogging(single sign on). Samtrafikk-leverandørene har inngått partnerskapsavtaler med eID-leverandører og deres produkter støtter til dels løsninger som tilsvarer det offentlige sikkerhetsnivå 3 og 4 (jfr vedlegg 1).
Arbeidsgruppen er kjent med at to av samtrafikkleverandørene i løpet av høsten 2006 introduserte partnerskapsavtaler med systemleverandører av administrative systemer til offentlig sektor.

3.3 Offentlig bruk av eID/e-signatur

En rekke offentlige virksomheter har i dag systemer for å autentisere sine brukere for webbaserte elektroniske tjenester. I desember 2005 foretok FAD en kartlegging blant femten offentlige etater som yter webbaserte tjenester til innbyggere og næringsliv. FAD mottok i denne kartleggingen svar fra 10 offentlige etater. De dominerende eID-løsninger som benyttes blant disse virksomhetene er pinkoder og passord.

Statens lånekasse for utdanning har to autentiseringsløsninger. En for innlogging på "Dine Sider" og en for signering.

- Brukernavn og PIN-kode til bruk på "Dine Sider" sendes ut samtidig til alle brukerne på et forutsigbart tidspunkt. Brukeren skal selv alltid bytte PIN-koden mot et selvvalgt passord ved første gangs pålogging. Lånekassen har ikke tilgang til dette passordet.

- Løsningen for signering av gjeldsbrev benytter smartkortløsning som er tilgjengelig via Altinn.

Statens pensjonskasse har tre løsninger som krever autentisering. En for bedrifter og to for personer. Til personløsningen sendes det passordbrev til medlemmer av SPK.

FEIDE er Kunnskapsdepartementets satsing på enhetlig identitetsforvaltning i utdanningssektoren. FEIDE er en enhetlig identitetsforvaltning for utdanningssektoren. FEIDE har en elektronisk identitet som bygger på kvalitetssikrete personopplysninger som navn, fødselsnummer og utdanningsinstitusjonen som personen er tilknyttet. Til denne identiteten hører et unikt brukernavn og passord. Grunnlaget for elektronisk identitet er uavhengig av hvilken utdanningsinstitusjon personen er tilknyttet. FEIDE-identiteten skal kunne brukes av en person til å få tilgang til mange ulike tjenester for sektoren. FEIDE tilbyr også en felles påloggingstjeneste for sektoren. Denne tjenesten er tilrettelagt for å kunne integrere eventuelle andre felles eID'er som personer kan være forsynt med.

I dag er FEIDE innført for rundt femti prosent av alle personer tilknyttet høgere utdanning i Norge. Kunnskapsdepartementet har besluttet at FEIDE også skal innføres i grunn- og videregående skoler. Utrullingsprosessen har startet høsten 2006. I 2006/2007 ligger departementets hovedfokus på de videregående skolene, og prosessen med å innføre FEIDE til disse er allerede i gang. UNINETT ABC arbeider med FEIDE-innføring i videregående utdanning, gjennom bl.a. å drive praktisk utprøving og erfaringshøsting, utarbeide teknisk dokumentasjon som skal lette innføringen av FEIDE for kommuner og fylkeskommuner, tilrettelegge for at flest mulig tjenester klargjøres for FEIDE, beskrive arkitektur og grensesnitt basert på åpne standarder, og tilby veiledning til skoleeiere som vil innføre FEIDE.

Skatteetaten har egne PIN-kodeløsninger for skattekort og for preutfylt selvangivelse, som sendes ut til flertallet av befolkningen. Totaldistribusjonen av "skattePIN" er på 3.6 mill. skattekort og 0.36 mill. frikort av totalt 4,66 mill. nordmenn (de som ikke mottar noe er i hovedsak antakelig under 13 år). PIN kodene kan brukes fra portalene Skatteetaten.no og Altinn.no. For brukere som benytter Altinn.no som portal kan det i tillegg benyttes Altinn sine egne PIN koder (både via papir og via SMS). I dagens Altinn bruker man også en kombinasjon av logg og autentisering til signering på nivå 2 (jfr vedlegg 1). På nivå 4 (tilsvarer Person Høyt) brukes PKI ved hjelp av smartkort.)

NAV har en PIN-kodeløsning knyttet til meldekorttjenesten der PIN-koden sendes til folkeregistrert adresse.

Etaten har også brukernavn og passord i forbindelse med arbeidsgiveres innsending av AA-meldinger, samt en egen løsning med brukernavn og passord for IA-bedrifter.

I tillegg har NAV etablert flere elektroniske system-til-system-løsninger med aktører i helsesektoren som benytter personlig digital signatur med smartkort og

virksomhetssertifikat. En tilsvarende løsning er etablert mellom NAV og alle landets apotek. Dette tilsvarer sikkerhetsnivå 4.

Helsevesenet benytter i dag to ulike løsninger for signering med PKI i forbindelse med informasjonsutveksling mellom virksomheter i helsetjenesten, og mellom NAV og helsetjenesten:

- personlig signering (med personlig sertifikat) av skjema, meldinger, slik at signaturen entydig knyttes til innhold i en melding som skal kommuniseres.
- signering og kryptering av transportkonvolutt på virksomhetsnivå (m/virksomhetssertifikat).

3.4 Erfaringer med bruk av eID/e-signatur

Trygdeetaten og helsevesenet var tidlig ute med å ta i bruk PKI, men det har gått tregt å få utbredt løsningene i sektoren. Det skyldes flere forhold: umodent marked, høye kostnader, ny teknologi, lite følt behov fra legenes side og begrensede anvendelsesmuligheter. Hittil har Sosial- og helsedirektoratet finansiert det meste av PKI-anskaffelsene for legekontorene. Sykehusene har i oppstartsperioden vært avventende, først og fremst på grunn av kostnader samt usikkerhet rundt behov, ambisjonsnivå og løsningsvalg.. Det er kostbar for en sektor å stå alene om krav og utvikling av løsninger. Utfordringer knyttet til å igangsette egne prosesser og etablere løsninger uten felles nasjonale grep og felles standarder, gjør det sårbart å være først ute med tjenester og skaper en "vente-og-se" holdning hos virksomheter som skal utvikle e-tjenester.

Kombinasjonen av et generelt personlig sertifikat for signering av meldingsinnhold, og virksomhetssertifikat på transportnivå, som nevnt under pkt 3.3, sikrer nødvendig knytning mellom person og virksomhet. Det gjør det mulig for helsepersonell å benytte en felles eID på sikkerhetsnivå 4, både for profesjonell bruk og for private formål. Helsevesenet har derfor ikke sett behov for egne ansattsertifikater for elektronisk kommunikasjon mellom virksomheter.

Flere helseforetak ønsker å ta i bruk eID for autentisering og tilgang til systemer. Imidlertid har anskaffelse av PKI-løsninger for alle ansatte vist seg å være svært kostbart. Nye AHUS har valgt enklere løsninger for ansattsertifikater for intern bruk.

Rikshospitalet/Radiumhospitalet (RR HF) sine erfaringer i forbindelse med kreftpasienters bruk av pasientportal (MinJournal), er at terskelen for å *komme i gang* med PKI er for høy. I forbindelse med pilotbruk av MinJournal og bruk av forskningsprosjektet Webchoice for kreftpasienter, får pasienten et "anonymt" Buypass kort som RR HF betaler for. Deretter må de hente kortleser og kort på postkontoret, installere programvare, sette i kortleseren, finne frem pin-koden og nettadressen før de kan koble seg opp. For disse pasientene som både er eldre mennesker, og har en alvorlig sykdom, viser det seg at omtrent halvparten gir opp før de kommer så langt som til å logge seg inn for første gang. Dette til tross for at funksjonaliteten gir viktige råd

og hjelp rundt selve sykdommen og gir viktig støtte til pasienten i en rehabiliteringsperiode. Her ville en telefonbasert brukerstøtte trolig kunne avhjelpe mye.

I Altinn finnes det en løsning på sikkerhetsnivå 4, som først og fremst ble utviklet til bruk for Lånekassen. Erfaringen viser at denne løsningen med smartkort og PKI-sertifikater i stor grad gjenbrukes av de som innehar smartkortet, også til tjenester som ikke krever dette sikkerhetsnivået. Løsningen anses som mer brukervennlig enn PIN-kode og passord løsninger når man først har begynt å ta det i bruk. Dette fordi selve påloggingen krever bare at kort settes i leseren og en firesifret PIN-kode tastes inn.

Erfaringer viser med andre ord at brukerterskelen særlig ligger på å ta løsningen i bruk, i forhold til anskaffelse og installering. I tillegg viser erfaringene at det er kostbart for de enkelte tjenestene å utvikle egne løsninger. Det er derfor viktig at løsningene kan gjenbrukes i flere sammenhenger, og at det utvikles løsninger med e-tjenester som brukes mye.

3.5 Fremtidige behov for eID i offentlig sektor

Offentlig sektor står foran en periode med omfattende modernisering og utvikling av selvbetjeningsløsninger. Til nå har det vært utbredt å utvikle løsninger som ikke har omfattet utveksling av sensitive personopplysninger, eller hvor brukergruppen har vært begrenset.

Det gjenstår å bygge løsninger som både kan omfatte alle borgere i landet samtidig som det er sikkert å utveksle sensitive personopplysninger. I mange tilfeller vil selvbetjeningsløsninger også handle om krav på ytelser eller rettigheter med til dels stor verdi både for den enkelte og for samfunnet. Det innebærer et behov for å knytte avsender til innholdet som formidles på en sikker måte.

Sosial- og helsesektoren

Helsevesenet vil fortsatt satse bredt på PKI for sikring av meldingsutveksling mellom ulike tjenesteytere i helsetjenesten, som en felles løsning for autentisering av kommunikasjonsparter, signering av informasjon som overføres samt for kryptering (integritets- og konfidensialitetsbeskyttelse).

PKI med virksomhetssertifikat er vedtatt tatt i bruk som en standard for all rutinemessig meldingsoverføring mellom ulike aktører i helsetjenesten. Det er innført et standard ebXML-rammeverk for bruk av virksomhetssertifikat ved meldingstransport. Ved bruk av dette for signering og kryptering av transportkonvolutt, blir behovet for personlig eID for meldingsutveksling mellom virksomheter begrenset. Et område hvor det likevel er krav om signering med personlig eID (nivå 4), har vært for kommunikasjon med NAV (sykmelding, legeerklæring og oppgjørsmeldinger).

Innføring av eResept (elektronisk utsendelse av resepter med elektronisk signering eID) forventes å bli innført som en tjeneste i løpet av 2007/2008. Det er derfor et behov for helseforetakene å anskaffe personlige sertifikater på nivå 4 til leger ved helseforetakene for elektronisk signering av resepter. Det antas at dette behovet kan oppfylles gjennom den nye rammeavtalen om ansattkort som sykehuset Ahus nylig har inngått.

Innføring av trådløs infrastruktur på helseforetakene, samt løsninger for hjemmekontor hvor pleiepersonell skal ha tilgang til personsensitive opplysninger stiller krav til to-faktor-autentisering. Flere helseforetak ser behov for og ønsker å ta i bruk en PKI/Smart kort for autentisering og pålogging til systemer internt. For autentisering og tilgang til systemer for alle ansatte, har St.Olavs hospital tatt i bruk samme type PKI som det som benyttes for sykemelding. Nye AHUs har inngått en felles rammeavtale for PKI for spesialisthelsetjenesten, til bruk både for autentisering og pålogging til systemer, og for signering. Ved slik bruk av PKI er det viktig at det ikke påløper kostnader per transaksjon, og valideringstjenester bør være tilgjengelig lokalt.

Helsevesenet bruk av eID for signering og utveksling av sensitiv informasjon, krever en lokal signeringsløsning. En lokal signeringsløsning stiller krav om lokal oppbevaring og tilgang til egen privat nøkkel over et standardisert grensesnitt. I tillegg stilles det krav til tilgang til offentlig nøkkel for den man samhandler med. Det er derfor avgjørende at PKI-leverandøren tilbyr dette for at et samtrafikknav skal kunne tilby denne funksjonaliteten. Åpne standardiserte grensesnitt må derfor vektlegges ved valg av leverandør. Disse grensesnittene må omfatte tilgang til privat nøkkel og tilgang til sperreinformasjon og katalog.

Full innføring av PKI/eID i helsevesenet vil omfatte 2-300 000 profesjonelle brukere i spesialisthelsetjenesten og kommunehelsetjenesten.

Arbeids- og velferdsetaten (NAV)

Arbeids- og velferdsetaten skal i løpet av perioden 2007 – 2009 realisere tre større forvaltningsreformer:

- Pensjonsreformen
- NAV-reformen
- Helsetjenestereformen

I tillegg skal etaten realisere de tiltak som initieres gjennom Velferdsmeldingen i løpet av samme periode. Sett i et etatsperspektiv, vil det samlet dreie seg om betydelige endringer i et flertall av de sentrale områder som etaten forvalter.

Det er et overordnet politisk mål at den nye NAV-etaten skal bli en effektiv etat. Dette brede reformarbeidet vil ikke kunne gjennomføres uten omfattende utvikling av selvbetjeningsløsninger mot publikum og samarbeidspartnere, bl.a. arbeidsgivere, leger og behandlere.

- Organisasjonsutvikling og selvbetjening

Reformene omfatter organisasjonsutvikling i alle deler av etaten og baserer seg på overgang til selvbetjening fra brukerens side ut fra en kostnyttebetraktning. Arbeidet med å realisere gevinster i den nye etaten vil være avhengig av at tjenestens brukere er i stand til å ta nye selvbetjeningsløsninger i bruk. Det forutsetter at de aktuelle brukerne blant publikum og arbeidsgivere er forsynt med sikkerhetsløsning på tilstrekkelig nivå i henhold til rammeverket for autentisering og uavviselighet som ligger til grunn for dette strategidokumentet.

Generelt gjelder at en vesentlig del av de elektroniske tjenestene mot publikum, leger, behandlere og arbeidsgivere vil handle om helseopplysninger og således inneholde

sensitive personopplysninger. Det er bare de brukere som har en eID på nivå 4 (Person Høyt) som kan bruke tjenestene. Etaten har således behov for en forsyningsstrategi som fokuserer på rask spredning av sikkerhetsnivå 4, eventuelt en målrettet forsyning til brukerne i takt med hvilke tjenester som utvikles.

- Fremdrift på etablering av elektroniske tjenester

Etaten har, gjennom pensjonsprosjektet forpliktende planer overfor bl.a. Arbeids- og inkluderingsdepartementet og Finansdepartementet, konkretisert og tidsfestet når elektroniske tjenester knyttet til både gammelt og nytt regelverk vil være etablert. Selv om konkretiseringen av nye tjenester foreløpig ikke er uttømmende, foreligger det nå forpliktende planer om når de forskjellige typer tjenester må være ferdigstilt for test mot våre tjenester:

- Fra 1.5.07 er løsninger som krever autentisering med nivå 3 klare
- Fra 2.kvartal 2008 er løsninger som krever autentisering/signering med sikkerhetsløsning på nivå 4 i rammeverket klare.

Skattedirektoratet

Skatteetatens strategi er å få en felles påloggingsløsning for alle etatens tjenester. Det ideelle vil være dersom en slik påloggingsløsning er felles for hele forvaltningen.

Pr. 2006 kan alle etatens tjenester i Altinn nås via **PIN-kodene** for Skattekort, PSA og Altinn.
Det gjøres løpende vurderinger av nye tjenester og deres krav til sikkerhetsnivå. På nåværende tidspunkt har SKD ikke identifisert nye sluttbrukertjenester som krever høyere sikerhetsnivåer. Eventuelle nye tjenester knyttet til bruk av Folkeregisterdata vil derimot kunne ha strenge sikkerhetskrav.

For virksomhetssertifikater må etaten gjøre en mer omfattende behovsanalyse. I utveksling av data mellom forvaltningsenheter (stat og kommune), vil virksomhetssertifikater kunne benyttes mellom systemløsninger. Innen dette området har SKD med stor sannsynlighet sammenfallende behov med andre forvaltningsenheter.

Kommunesektoren

Bruk av autentiserings- og signeringsmekanismer er aktuelt innenfor en rekke forvaltnings- og tjenesteområder i kommunesektoren, bl.a.:

- Avtaler (anbud, kontrakter, rammeavtaler)
- Bevillinger (serveringsbevilling, skjenkebevilling)
- Byggesak (byggesøknad, nabovarsel, melding om tiltak)
- Tinglysing (begjæring om oppdeling i eierseksjoner)
- Fast eiendom (søknad om konsesjon)
- Kultur og fritid (søknad om leie av kommunale anlegg, søknad om ledsagerbevis, søknad om tilskudd)
- Landbruk (søknad om statstilskudd til skogsveier)
- Oppmåling (rekvisisjon av oppmålingsforretning)
- Skole og barnehage (flyttemelding, søknad om SFO-plass, søknad om barnehageplass, søknad om redusert foreldrebetaling)

- Helse- og omsorg (søknad om hjemmetjenester, søknad om sykehjemsplass, meldingsutveksling med helseforetak, fastleger, legevakt)
- Sosialtjenester (søknad om økonomisk sosialhjelp, barnevernsaker)
- Husbanken (søknad om boligtilskudd, søknad om kommunalt etableringslån,, søknad om lån til utbedring av bolig)
- Tilgangskontroll (portaler, hjemmekontor, saksdokumenter)
- Stillingssøknader
- Sikker arkivering av sensitive dokumenter

Ulike tjenester vil kreve ulike sikkerhetsnivåer. Også innenfor samme tjeneste kan det være nødvendig med to nivåer. Et eksempel er barnehagesøknad, som normalt ikke vil kreve et høy sikkerhetsnivå (nivå 4), men som i noen tilfeller, for eksempel søknad om barnehageplass for barn med spesielle funksjonshemminger eller spesielle familieforhold, vil kreve et høyt sikkerhetsnivå. Anbefaling av sikkerhetsnivå for de viktigste tjenestene vil bl.a. bli klarlagt i KS-prosjektet ”Tjenester på nett”.

Tjenesteportalen Altinn

Altinn har i dag autentiserings og signeringsløsninger med stor utbredelse over den eksisterende drifts- og utviklingsavtalen. I et brukerperspektiv er det viktigste at det finnes et fåtall mekanismer som kan benyttes av alle. Det er vanskelig å orientere seg om hva som er den beste løsningen og det skaper usikkerhet å ha for mange løsninger å velge mellom. De etater som benytter Altinn signaliserer behov for to nivåer av både autentisering og signering. Hvis det høyeste nivået har tilstrekkelig brukervennlighet og utbredelse, vil det derimot bare være behov for ett nivå.

Altinn kommer i framtiden til å baseres på bruk av standardløsninger og felleskomponenter. I målbildet for Altinn er både autentisering og signering basert på et felles offentlig samtrafikknav eller standardløsninger. Det samme gjelder for krypteringsfunksjonalitet. I den videre utviklingen av Altinn må det videreføres/videreutvikles funksjonalitet knyttet til autentisering, signering og videreformidling. Ettersom dagens løsning ikke er basert på standardløsninger, må dette anskaffes, hvis det ikke kommer et samtrafikknav i løpet av kort tid (dvs slutten av 08-første dels av 09). Det som vil bli den store kostnadsmessige besparelsen ved å benytte en felles løsning vil ligge på det forvaltningsmessige. For brukeren vil det utvilsomt være en stor fordel å slippe å forholde seg til ulike løsninger for offentlig sektor.

Altinn ser et framtidig behov for å kunne benytte ansattsertifikater og virksomhetssertifikater til signering. Dette vil kunne bidra til å løse problematikken både rundt utenlandske brukere og rettighetsproblematikk. Brukere uten norsk personnummer er i dag en stor utfordring i forhold til sikker identifikasjon og utlevering av autentiseringsmekanismer. Det er sterkt ønskelig at det tas et nasjonalt ansvar for å løse dette.

4 Forsyning av innbyggere med eID

Arbeidsgruppen skal foreslå:
Strategier for forsyning av publikum med eID/e-signatur - privat sektors og offentlig sektors rolle (bl.a. pågående arbeid med nasjonalt ID-kort), herunder også gjenbruk av eksisterende autentiserings- og signeringsløsninger fremskaffet i statlig regi (f.eks. skattePIN som skal benyttes i forbindelse med MinSide, Altinns løsninger og e-signaturløsninger som benyttes av helsesektoren og NAV.).

4.1 Innledning

Kapitlet beskriver de strategier som arbeidsgruppen anbefaler for forsyning av innbyggere med eID. Med forsyning menes distribusjonsmåte, målgrupper, knytningen til elektronisk tjenesteutvikling, samt finansiering av etablering og bruk.

Arbeidsgruppen tar utgangspunkt i at målgruppen for forsyning er hele landets befolkning fom. 13 år. Målgruppen vil omfatte både innbyggere med norsk fødselsnummer, samt de som får utstedt såkalte D-nummer. Tilbud om løsning vil imidlertid ikke være ensbetydende med faktisk samtidig utstedelse. Arbeidsgruppen erkjenner at fullskaladistribusjon til hele landets befolkning vil måtte skje over flere år og at det er hensiktsmessig at utvikling av offentlige elektroniske tjenester og distribusjon av eID på nødvendig nivå skjer i parallell.

I mandatet har arbeidsgruppen fått oppgitt en grunnleggende premiss i det at strategien skulle ha en utvidet horisont, teknologisk sett, i forhold til "Strategi for utbredelse av PKI-anvendelser i offentlig sektor". En slik premiss innebærer at det er nødvendig å revurdere valget av PKI som "foretrukken teknologi" for implementering av eID og e-signatur i elektronisk kommunikasjon med og i offentlig sektor. Den foregående PKI-strategien la til grunn at:

> *"Det er ønskelig at publikum skal kunne bruke felles sikkerhetsløsning ved all elektronisk kontakt med offentlig sektor, og at det ikke etableres ulike løsninger i ulike etater som har publikumskontakt. PKI vurderes som sikker nok teknologi når det gjelder utstrakt gjenbruk mot mange ulike tjenester."*

Dersom man nyanserer påstanden om behov for bare én løsning, kan det gjøres flere valg. Det er den enkelte offentlige virksomhet som har et selvstendig ansvar for å vurdere om sikkerheten i deres elektroniske dialog med publikum er god nok. Samtidig skal sikkerhetsløsningen(e) være tilpasset det sikringsbehovet som hver enkel tjeneste har. Disse prinsippene fører naturligvis til at det etableres varierende løsninger, fra virksomhet til virksomhet. Med utgangspunkt i rammeverket (Vedlegg 1) kan det imidlertid tenkes at man kan samle løsningene til et fåtall, med tilstrekkelig styrke til å håndtere store grupper av anvendelser.

En annen premiss for arbeidsgruppens arbeid er hensynet til brukere og brukervennlighet. Innbyggere blir i stadig økende grad "plaget" av store mengder ulike typer brukerID, passord og lignende. En ettertraktet løsning for mange vil være å ha en eID som kan brukes mot tilstrekkelig mange tjenester på Internett. For andre vil nettopp

en slik ”universalnøkkel” oppfattes som lite ønskelig, særlig med tanke på konsekvensene av at en slik nøkkel kunne bli misbrukt av uvedkommende. Arbeidsgruppen har derfor lagt til grunn at brukere kan ha ulike ønsker og preferanser i forhold til hvordan de vil benytte sin eID. Enkelhet i bruk er imidlertid et universelt behov, uansett hvor mange eIDer en bruker måtte besitte. Brukerens motivasjon for å gå gjennom komplekse prosedyrer for anskaffelse av eID vil stige dersom hun visste at denne eIDen kan brukes til mange tjenester, med en gang etter at den er anskaffet.

Statistiske undersøkelser i andre land indikerer at antallet offentlige elektroniske tjenester som innbygger vil komme i kontakt med gjennom et år er forholdsvis lavt. Dette taler sterkt for at det i nye strategier *ikke sperres* for muligheten for slik flerbruk av eID, inkludert bruk av eID mot private tjenester, samtidig som det foreligger et valg å kunne skaffe seg flere forskjellige eID til ulike formål.

Arbeidsgruppen har valgt å fokusere på forsyningsstrategier på rammeverkets sikkerhetsnivå 3 og 4, jfr. kap. 2.4 og vedlegg 1. Begrunnelsen for dette valget er at en samlet offentlig satsning på eID må kunne innebære at sluttbrukere kan få tilbud om færre løsninger i forhold til de som i dag blir distribuert fra offentlige virksomheter, løsninger som samtidig åpner flere bruksmuligheter. Videre er de løsninger som i dag er på sikkerhetsnivå 2, robuste og sikre for det bruksmønster som de er etablert for, men disse vil ikke kunne håndtere et større antall tjenester med pålogging med den samme eID-løsning.
Sikkerhetsnivå 4 ansees som en løsning som vil være sikker nok til å håndtere flere tjenester med høyere sikkerhetskrav enn nivå 3. Dette nivåets betydning vil øke betraktelig i årene fremover, fordi en rekke tunge tjenesteområder krever løsninger på dette nivået, for eksempel helse og sosialsektoren.

Erfaringer med tidligere satsinger og behovsvurderingene beskrevet i kap. 3 understreker nødvendigheten av en helhetlig forankring av arbeidet med eID og e-signatur i offentlig sektor på departementalt nivå.

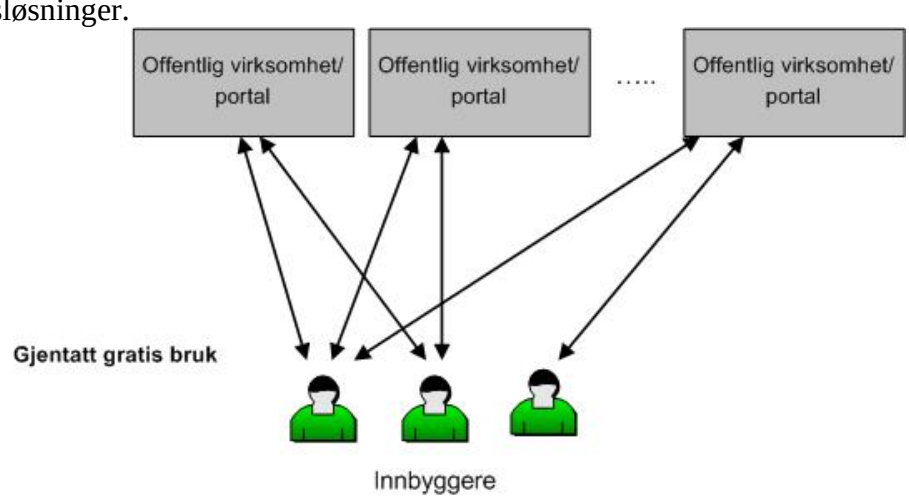
4.2 Forsyning av innbyggere med eID på sikkerhetsnivå 3

Arbeidsgruppen har tatt utgangspunkt i to ulike modeller for forsyning av eID på sikkerhetsnivå 3. De to modellene er begge i offentlig regi og det er således ikke vurdert markedsmessige alternativer til dette sikkerhetsnivået. Årsaken til dette er at det offentlige allerede har godt fungerende sikkerhetsløsninger på dette nivået. Det har vært en etablert praksis siden Internett-baserte tjenester til publikum ble etablert, at offentlige virksomheter som tilbyr slike tjenester selv sørger for de sikkerhetsløsninger, inklusive eID, som må til for å tilby tjenesten til egne målgrupper. Samtidig har det heller ikke trådt frem noen etablerte markedsalternativer for å kunne få på plass fellesløsninger for offentlig sektor. Forsyning av brukere med eID på sikkerhetsnivå 3 vil derfor i hovedsak være en problemstilling om kostnaden og nytten ved en felles, offentlig løsning vil stå i forhold til kostnadene og nytten ved at man fortsetter med etatsspesifikke løsninger, rettet mot stadig mer overlappende innbyggergrupper.

4.2.1 Etatsspesifikk distribusjon av eID.

Offentlige virksomheter har utviklet eller er i ferd med å utvikle, elektroniske tjenester for innbyggere. Innbyggertjenester krever ofte autentisering av brukeren, med middels høye krav til sikring av at det er den rette identitet man forholder seg til. Den normale fremgangsmåten som offentlige virksomheter utvikler slike løsninger på, er å etablere egenutviklede løsninger for autentisering og identifisering som kun brukes for å få tilgang til deres elektroniske tjenester. Eksempler på løsninger som er i drift i dag er listet i kapittel 3.3. En rekke kommuner bruker også en kombinasjon av brukernavn og engangspassord for å gi tilgang til elektroniske søknadsskjemaer etc.

Uten sentrale grep vil denne utviklingen fortsette i det tempo som nye tjenester legges til rette for brukeren. Brukeren vil få en mengde ulike autentiseringsløsninger, avhengig av hvilken offentlig etat vedkommende ønsker å kommunisere elektronisk med. Etatene og kommunene vil benytte utviklingsressurser på å tilrettelegge nye autentiseringsløsninger.

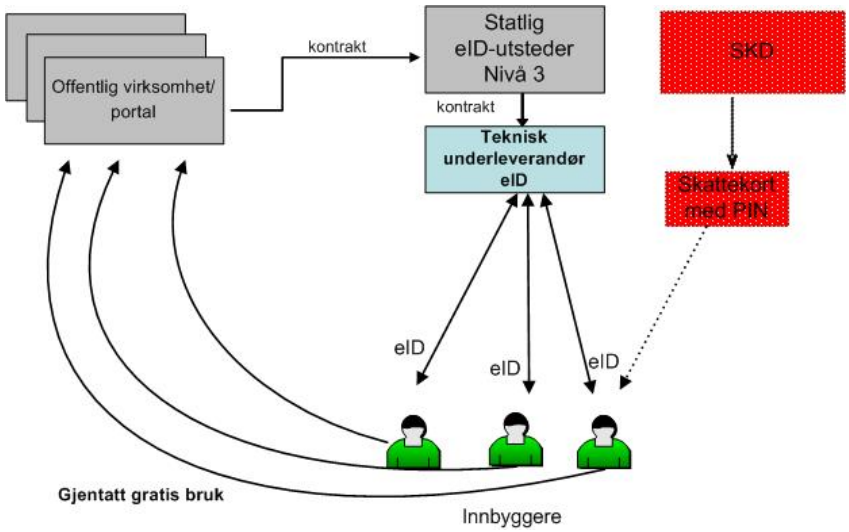


Figur 2: ***Etatsspesifikk forsyning eID sikkerhetsnivå 3***

Modellen innebærer at det ikke tas initiativ til å etablere noe felles offentlig eID på sikkerhetsnivå 3. Forsyning av eID til befolkningen vil skje gjennom at den enkelte offentlige virksomhet utsteder eID på nivå 2 eller 3 til sine målgrupper blant innbyggerne. Distribusjonsmetode vil variere ut fra hva som etaten finner formålstjenlig. Modellen har den fordelen at kostnadene ved etablering og drift av eID-løsningene blir belastet den enkelte virksomhet som faktisk har behov for slike løsninger. Det er ikke behov for sentrale initiativ for å koordinere forsyningen. Ulemper med modellen er at den enkelte innbygger som har kontakt med ulike offentlige virksomheter vil oppleve offentlig sektor som fragmentert og ukoordinert og får etter hvert betydelige ulemper ved bruken av mange ulike eIDer. Samtidig kan det identifiseres en mangfoldig resursbruk i flere offentlige etater rettet mot løsning av samme problem – nemlig autentisering av innbyggere på Internett. Gjenbruk av andre etaters løsninger kan være et mulig remedie her, men det ligger begrensninger i slike initiativer ved at ansvarslinjene blir uklare og prosjekt- og budsjettkoordineringskostnadene gjør ofte slike initiativer vanskelig å gjennomføre i praksis.

4.2.2 Forsyning av felles offentlig eID

I denne modellen vil offentlig sektor sørge for etablering av en offentlig kontrollert, felles eID-plattform (offentlig utstedt eID) til landets innbyggere på sikkerhetsnivå 3, jfr. kap. 2.4 og vedlegg 1. En offentlig virksomhet får i oppgave å stå som utsteder av en slik eID. Denne virksomheten kan knytte til seg en eller flere tekniske leverandører. Alle statlige virksomheter som tilbyr elektroniske tjenester til innbyggere må tilrettelegge for bruken av denne eID, forutsatt at tjenesten ikke befinner seg på sikkerhetsnivå 4, innenfor en avtalt tidsperiode, og på grunnlag av nyttevurderinger, jfr. kap 7.2.



Figur 3: Felles forsyning av offentlig eID sikkerhetsnivå 3

For førstegangsdistribusjon kan SKDs PIN-kodedistribusjon benyttes. Innbyggere vil gjenbruke disse PIN-kodene til registrering og utstedelse av eID på sikkerhetsnivå 3. Det skal utvikles felles kravspesifikasjoner for denne type eID, med utgangspunkt i rammeverket (vedlegg 1). Kravspesifikasjoner utvikles av den offentlige virksomheten som får i oppgave å forvalte ordningen, i samspill med berørte brukersteder.
En fordel med denne løsningen er at det er et enkelt forsyningsregime som når større deler av befolkningen enn noen annen distribusjonsløsning, da skatteetatens målgruppe dekker store deler av befolkningen. Samtidig er dette også en metode for distribusjon som ikke krever første initiativ til å være fra brukerens side, da eID-grunnlaget vil "dumpe i postkassen". Det må foretaes sentrale investeringer for å etablere den offentlige eID på nivå 3.

4.2.3 Valg av modell for forsyning av eID på sikkerhetsnivå 3

For å sikre størst mulig grad av brukervennlighet er det nødvendig at forsyningsmodellen for nivå 3 medfører at innbyggere får færre løsninger å forholde seg til i møte med offentlig sektor. Av de to modellene(figur 2 og 3) vil felles forsyning/distribusjon sikre dette i størst mulig grad (jfr figur 3).

Det andre kriteriet for valg av modell er knyttet til effektiv ressursbruk i offentlig sektor. Her vil det kunne anføres at etatsspesifikk forsyning eksisterer i mange virksomheter med elektroniske tjenester i dag. Modellen i figur 2 vil videre kunne sikre en fornuftig

kostnadsfordeling fordi kostnadene blir knyttet til dem som faktisk har tjenester som blir brukt av innbyggere. Kostnadsbelastning er imidlertid bare ett vurderingskriterie. Summen av kostnader bør også tas her i betraktning. En modell med felles forsyning (figur 3) vil både sikre at de offentlige virksomheter som ikke har etablert eID-løsninger fra før får et kostnadseffektivt tilbud, og at den samlede ressursbruken i offentlige virksomheter som allerede har eID-løsninger blir mindre på sikt. Dette ved at virksomheter som går over på felles løsning vil kunne redusere kostnader ved egen distribusjon når deres målgruppe endres eller andre forhold krever ny distribusjon av eID.

I valg mellom de to oppstilte modellene har arbeidsgruppen vurdert det derfor dit hen at det bør etableres en offentlig eID på nivå 3, med felles forsyning (jfr figur 3).

4.3 Forsyning av innbyggere med eID på sikkerhetsnivå 4

Det er i dag ikke etablert noen felles offentlig løsning for forsyning på sikkerhetsnivå 4. Det har vært tilgjengelig etablerte løsninger i markedet siden slutten av 90-tallet, men disse innebær ikke spredning av eID til alle innbyggere. Gjennom rammeavtaler er det gjennomført forsyning til spesifikke brukergrupper i helsesektoren, jfr. kap. 3.3, men ut over disse er det ingen offentlige virksomheter som har egne planer om bred distribusjon av eID på nivå 4.
I markedet har det siden 2003 foregått en del aktiviteter med tanke på forsyning av innbyggere med eID, særlig med forankring i to hovedtyper tjenester som er hyppig brukt på Internettet – tipping og bank. Aktiviteten skjøt fart i 2006, men det er fremdeles slik at eID-løsninger som oppfyller krav til sikkerhetsnivå 4 og gjeldende offentlige standarder der[3] kun i begrenset grad er distribuert til befolkningen pr. dags dato.

Det er samtidig nødvendig å fastslå at det ikke er særlig mange e-tjenester etablert i offentlig sektor som per dags dato har behov for en eID på nivå 4. Statens lånekasse for utdanning har en tjeneste som krever eID/ e-signatur på dette nivå. Denne tjenesten innebærer signering av gjeldsbrev elektronisk. Lånekassen løser imidlertid dette i dag ved å benytte de eID'er som tilbys i Altinn. Utbredelsen av den aktuelle eID er imidlertid begrenset, hovedsaklig pga kostnader som påføres brukere ved anskaffelsen. En kommende e-tjeneste i regi av Vegdirektoratet – et system for koordinering av fremføring av offentlig infrastruktur – vil etter etatens vurdering kreve eID på sikkerhetsnivå 4. Videre er identifiserte behov i NAV-etaten noen av hoveddrivere bak ønsket om å sikre forsyning av eID på dette sikkerhetsnivå til bredere lag av befolkningen, gjerne til nærmere definerte målgrupper.

For å fremme utvikling av pasienttjenester fra helsevesenet, vil det være viktig å få en felles løsning for distribusjon av eID på sikkerhetsnivå 4. eID på sikkerhetsnivå 3 er ikke aktuelt for tjenester som inneholder pasientinformasjon. Dersom utrulling av en slik løsning ikke vil være tilgjengelig før 2008/2009, kan det oppstå behov for å etablere midlertidige avtaler som sikrer at aktuelle virksomheter kan komme i gang med å tilby pasientorienterte elektroniske tjenester. I følge aktører i helsevesenet vil det vil

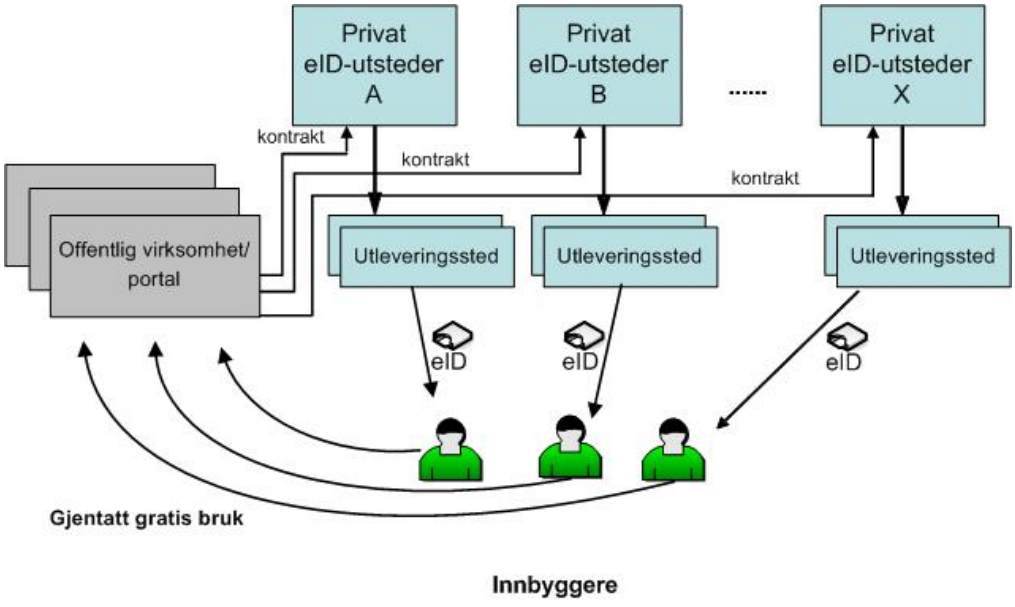
[3] Kravspesifikasjon for PKI i offentlig sektor, Person Høyt.

være svært uheldig dersom pasienttjenester fra sykehusene ikke vurderes etablert før 2009.

Arbeidsgruppen har identifisert 3 ulike modeller for forsyning av innbyggere med eID på sikkerhetsnivå 4. Arbeidsgruppen erkjenner at det er mulig å oppstille en rekke ulike varianter av disse modellene, men har i beskrivelsen er det fremstilt hovedtyper. I drøftingene som har ledet fram til konklusjonene har imidlertid gruppen vurdert en rekke av disse variantene, selv om disse ikke er beskrevet i strategien.

4.3.1 Markedsbasert distribusjon og virksomhetsspesifikke avtaler

Offentlig sektor forsyner i denne modellen sine brukergrupper enkeltvis. I tråd med prinsippene om linjeansvar blir den enkelte virksomhet selv ansvarlig for å anskaffe de eID-løsninger som de ønsker for å kunne kommunisere med sine brukere på nivå 4. Den mest nærliggende forsyningsmodellen vil være at den enkelte offentlige virksomhet foretar en anskaffelse i markedet. Den enkelte virksomhet står selv fritt å vurdere om løsningene distribueres til sluttbrukere, eller om det skal være brukerens ansvar å anskaffe og benytte løsningen. Det blir ikke tatt sentrale initiativ ut over det å spesifisere felles krav til eID-løsninger på nivå 4, siden slike krav allerede finnes for PKI-baserte løsninger[4]. Konsekvensene av en slik modell vil være – dersom virksomheter velger å forsyne brukere – at brukere vil ha flere eID løsninger på nivå 4, hver til sin bruk, eller – dersom etatene satser på at brukere anskaffer eID selv – at hver etat vil måtte inngå og vedlikeholde avtaler med alle aktuelle eID tilbydere i markedet.



Figur 4: Markedsbasert distribusjon med etatsspesifikke avtaler

[4] Jfr. Kravspspesifikasjon for PKI i offentlig sektor

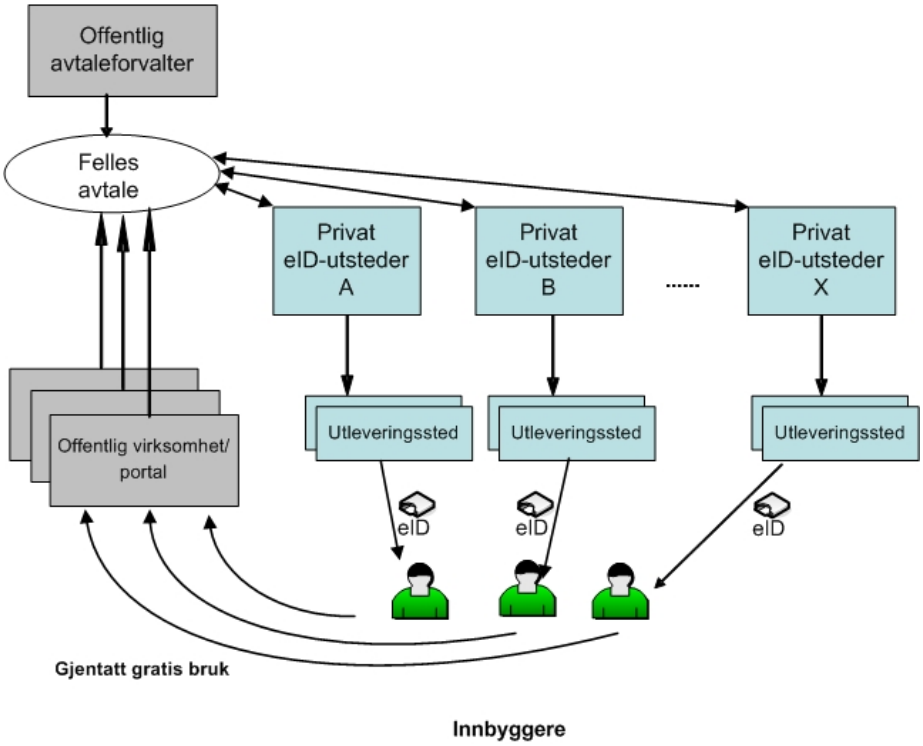
4.3.2 Felles avtale og markedsbasert distribusjon

Offentlig sektor kjøper i denne modellen eID i markedet gjennom en samordnet avtale. Dette innebærer at en offentlig avtaleforvalter lyser ut en konkurranse om å forsyne landets innbyggere med eID. Avtalene inngås på vegne av staten og kommunene. Avtaleforvalter kan velge én eller flere parallelle tilbydere av en eID-plattform, der en viktig parameter for valg vil være hvor mange innbyggere som tilbyderen kan forsyne med "sin" eID. Avtalen som avtaleforvalter inngår med eID-leverandøren(e) vil regulere forsyning, erstatningsbestemmelser, ansvarsforhold og tekniske grensesnitt. Betaling beregnes for eksempel som en funksjon av en årlig grunnavgift og en variabel årsavgift knyttet til antall innbyggere som vil besitte en eID fra den valgte tilbyderen (et "bonussystem"). En del av avgiften kan også gjøres avhengig av antall private tjenester som eID kan gjenbrukes mot. Avrop[5] på disse avtalene gjøres obligatorisk for alle statlige virksomheter som tilbyr elektroniske tjenester til innbyggere.

I denne modellen vil innbyggere kunne ha muligheten til å benytte den/ de eID som de anskaffet seg i samband med private tjenester til offentlige formål. Det vil imidlertid være en utfordring at det kan påløpe brukskostnader for sluttbruker dersom eID skal benyttes mot private tjenester, mens det ikke vil være tilfellet i bruk mot offentlige tjenester. Brukere som har anskaffet en eID fra en leverandør som ikke omfattes av rammeavtalen, vil måtte anskaffe seg en ny eID i tillegg, dersom de skulle ønske å nå aktuelle offentlige tjenester.

Når rammeavtalen opphører og sluttbrukere ev. må anskaffe nye eIDi henhold til en eventuell ny rammeavtale, vil det oppleves som en ytterligere ulempe for sluttbruker.

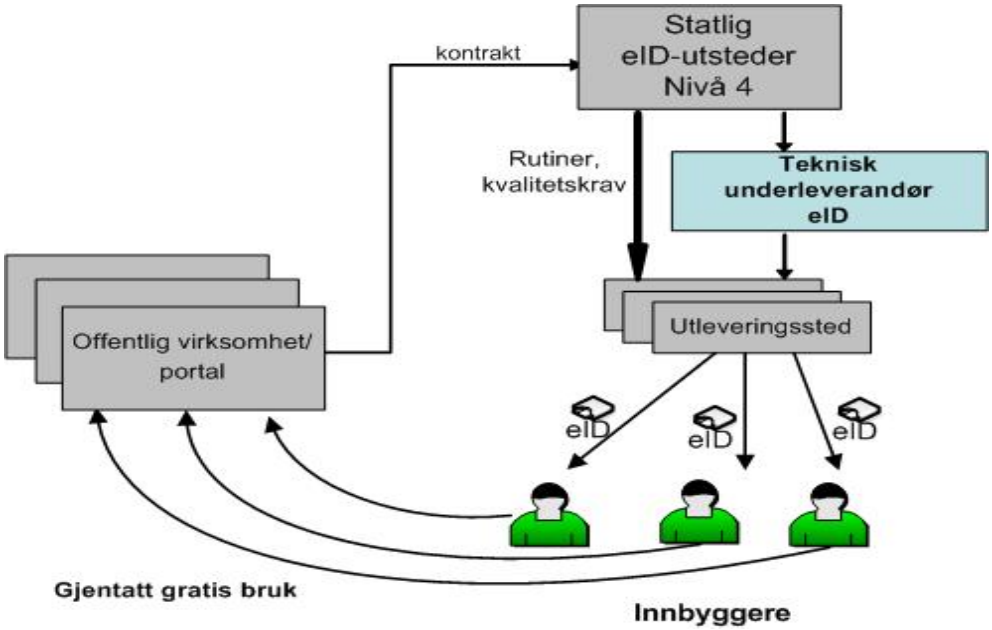
[5] Med avrop menes kjøp over felles avtale



Figur 5: Markedsbasert distribusjon med felles avtale

4.3.3 Distribusjon av offentlig eID

Modellen innebærer at staten tar ansvaret for å etablere og garantere for elektronisk ID til den enkelte innbygger, på lik linje med hva man gjør i dag knyttet til utstedelse av fysiske identifikasjonspapirer som førerkort og pass. Modellen vil innebære at staten må etablere et eget apparat for utstedelse, vedlikehold og distribusjonsapparat for eID. Modellen vil innebære at innbyggere vil kunne benytte den statlig utstedte eID for å få tilgang til alle elektroniske tjenester, også de som krever høy sikkerhet for at brukeren faktisk har den påståtte identiteten. For å øke nytten av slik offentlig utstedt eID, er det også naturlig for staten å åpne for at eID vil kunne benyttes mot private tjenester. Skjer dette, er konsekvensen den at offentlig utstedt eID må prises til brukeren ved anskaffelse på en ikke-diskriminerende måte i forhold til tilsvarende markedsutstedte eID-løsninger. Videre vil bruken av eID mot private tjenester kunne belastes brukeren.



Figur 6: Offentlig eID distribusjon

4.3.4 Valg av modell for forsyning av eID på sikkerhetsnivå 4

Arbeidsgruppen har vurdert de ulike modellene opp mot hverandre. Arbeidsgruppen har konsentrert evalueringen av modellene rundt to kriterier. Det første kriteriet er hensynet til sluttbrukere. Enkelhet i bruk er et universelt behov og brukerens motivasjon for å gå gjennom komplekse prosedyrer for anskaffelse av eID vil synke dersom hun må foreta den samme prosedyre hver gang det offentlige bytter leverandør på nivå 4. Hensynet til brukervennlighet tilsier at offentlig sektor må ha en langsiktig strategi for forsyning av innbyggere med eID på nivå 4. Det andre kriteriet i avveiningen mellom hvilken modell som bør velges er hensynet til effektiv ressursbruk i offentlig sektor. Effektiv ressursbruk innebærer både at løsningen må være samfunnsøkonomisk den mest lønnsomme, herunder iberegnet transaksjonskostnader (administrative kostnader) ved å etablere fragmenterte forsyningslinjer, og at ressursene anvendes på en mest hensiktsmessig måte, samlet sett.
En underliggende dimensjon i i forhold til valg av modell i et samfunnsøkonomisk perspektiv er også graden av styring og kontroll offentlig sektor vil ha i forbindelse med distribusjon og bruk av eID mot offentlige tjenester. Graden av styring vil variere avhengig av hvilken forsyningsmodell som velges og hvilken type kontrakt som det offentlige vil kunne forhandle frem med markedsaktørene. Kontrakter som reduserer graden av usikkerhet og risiko for offentlig sektor til et minimum vil være å foretrekke.

Markedsalternativet innebærer behovet for å se på hvilke leverandører som i dag tilbyr løsninger. De ulike leverandørene oppgir at de har distribuert eller er i ferd med å distribuere løsninger til utvalgte brukergrupper. Flere av leverandøreneoppgir at de har som målsetning at deres løsninger kan omfatte de fleste aktive Internettbrukere i landet.

Viktige forhold som må vurderes for dette alternativet (Figur 4: Markedsbasert distribusjon med etatsspesifikke avtaler) omfatter bl.a.:

- Usikkerheten i enkelte aktørers estimater når det gjelder dekningsgraden av godkjente eID-løsninger på nivå 4
- Usikkerheten om fremdriftsplaner for aktører med større utbredelse av eID på nivå 4 hva gjelder deklarasjoner om at felles offentlige krav[6] til eID er oppfylt
- Kostnader ved bruk som vil belastes offentlige brukersteder og offentlig sektors muligheter til å estimere disse i en tidlig fase av bruk (de første 2 årene)
- Krevende og fragmentert avtalestruktur.
- Manglende treffsikkerhet på målgruppe – dersom virksomhetene overlater til sluttbrukeren å anskaffe sin ID selv
- Lav brukervennlighet dersom det er den enkelte virksomhet sine nytte-kostnad-betraktninger som blir avgjørende for hvilke typer eID de velger å integrere i sine e-tjenester
- Tekniske formater og spesifikasjoner som markedsaktørene leverer, med liten offentlig påvirkningsmulighet, fare for "innelåsing"
- Samlede administrative kostnader knyttet til separate avtaleutlysninger og inngåelse av kontrakter.

Ovennevnte forhold taler for at dette alternativet ikke er å foretrekke for offentlig sektor.

Fordeler med denne modellen, sett i et bredere perspektiv, er klare styringslinjer i det offentlige (linjeansvaret gjelder fullt ut) og at markedsaktørenes investeringer i infrastrukturer for utstedelse av eID vil kunne delvis gjenvinnes gjennom gjenbruk i offentlig sektor.

Forhold som trekker i negativ retning ved felles avtale (Figur 5: Markedsbasert distribusjon med felles avtale) er bl.a.:

- Ingen utbredelse i dag, krever tilrettelegging av incentiver for rask spredning til aktuelle målgrupper
- Antatt krevende kontraktsforhandlinger for å oppnå en prisingsstruktur som sikrer kostnadskontroll for offentlig sektor i en innledende bruksfase.
- Stor sårbarhet dersom den/de valgte aktørene avvikler sin eID virksomhet.
- Forhold knyttet til struktur i forretningsmodeller hos enkelte aktører i markedet som vanskeliggjør eller gjør det umulig å inngå en felles avtale med offentlig sektor på de premisser offentlig sektor vil se som viktig.

Fordelen ved dette alternativet er mulighet for delvis gjenvinning av investeringskostnader markedsaktørene har pådratt seg gjennom gjenbruk i offentlig sektor og reduserte administrative kostnader for offentlig sektor samlet sett. For brukeren er fordelen at hun mest sannsynlig vil kunne gjenbruke eID anskaffet i samband med private tjenester på Internett i offentlige tjenester.

Viktige forhold som må vurderes ved offentlig eID (Figur 6: Offentlig eID distribusjon) er bl.a.:

- Ingen utbredelse i dag, starter på "0"
- Behov for etablering av en rekke nye funksjoner i utvalgte offentlige virksomheter. Kostnader forbundet med dette.

[6] Jfr. Kravspesifikasjon for PKI i offentlig sektor, Person Høyt

- Forutsigbarhet for sluttbrukere og offentlige virksomheter, sterk grad av offentlig styring og kontroll.
- Sentral finansiering, minimering av administrative kostnader for offentlig sektor samlet sett.
- Mulighet for målrettet forsyning av eID til utvalgte brukergrupper som prioriteres av etater som leverer og utvikler tjenester med behov for eID på nivå 4 i tjenestene sine.
- Markedsmessig ulempe ved at staten trer inn med en konkurrerende virksomhet i forhold til etablerte markedsaktører.

Etableringen og distribusjon av en eID på høyt sikkerhetsnivå vil måtte ses i sammenheng med den eventuelle etableringen av et nasjonalt ID-kort[7]. Sterke synergier som gjør seg gjeldende ved at eID kan "hektes på" en satsing som har sitt utspring i andre behov, men der bruk av infrastruktur og virkemidler for øvrig er sammenfallende, taler for at etablering av en statlig forsynt eID bør gjøres på denne måten. Utbredelsen av et mulig nasjonalt ID-kort vil bl.a. skje i takt med at brukerne har behov (anslått av JD til 500.000 årlig) for nytt pass. Brukere vil også kunne bestille og anskaffe nasjonalt ID-kort uten å måtte bestille nytt pass. Kortet skal også kunne utstedes til ikke-norske statsborgere med lovlig opphold i Norge.
Dette kortet vil imidlertid ikke være tilgjengelig for utrulling før tidligst i januar 2009.
Dersom behov for bred utbredelse av eID på nivå 4 gjør seg sterkt gjeldende i offentlig sektor før den dato, kan midlertidige avtaler vurderes. Dette vil imidlertid bidra til mindre effektiv ressursbruk i offentlig sektor samlet sett.

Skulle nasjonalt ID-kort med eID ikke bli realisert, må en statlig forsyning organiseres på en annen måte, mest sannsynlig gjennom en fellesavtale med utvalgt utsteder i markedet, som skal organisere og foreta distribusjon av kort som oppfyller offentlige krav (an variant av modellen felles avtale).

4.4 Anbefaling - forsyning av innbyggere med eID

Arbeidsgruppen har gjennom drøftinger, og etter en samlet vurdering, kommet fremt til at felles, statlig eID-løsning, på begge sikkerhetsnivå, vil være den som oppfyller de oppsatte kriterier på en best mulig måte, sett fra offentlige virksomheters ståsted. Løsningen vurderes til å være enkel og stabil (kontrollerbar) for sluttbrukere og offentlige brukersteder. Det vil være en økonomisk fordel at offentlige virksomheter ved etablering av e-tjenester ikke må utvikle eller implementere egne eID løsninger (inkludert forsyning til sine målgrupper av brukere).

Samtidig erkjenner gruppen at dagens tjenester i hovedsak ikke krever sikkerhetsnivå 4. For å sikre forenkling mot sluttbrukere, og av hensyn til tidsperspektivet, anbefales derfor en rask etablering av statlig løsning for felles eID

[7] Dette utredes ft. av Justisdepartementet, og en rapport avgitt av en interdepartemental gruppe forventes å foreligge i løpet av februar 2007.

på nivå 3. Løsningen bør kunne raskt tas i bruk av tjenesteportalene Altinn og Minside.

Når det gjelder e-tjenester som krever sikkerhetsnivå 4, vurderer gruppen det slik at behovene vil gjøre seg gjeldende i større omfang, særlig i helse og sosialsektoren, men også på noen flere områder, i løpet av de nærmeste to år. Ettersom markedet knyttet til denne type eID og tilhørende infrastruktur er begrenset og kan karakteriseres som ustabilt, er gruppen kommet til at det er formålstjenlig å utnytte muligheten for etablering av et nasjonalt ID-kort til distribusjon av statlig utstedt og kontrollerbar eID. Utrullingshastigheten anses som den største risikoen ved denne løsningen. Arbeidsgruppen legger derfor til grunn at målrettet forsyning av nasjonal ID kort må kunne foretas. Dette i samarbeid med sentrale etater som ønsker å tilby e-tjenester som krever eID på nivå 4. I tillegg bør det åpnes for at den statlige eID'en som skal inngå på nasjonale ID-kort også kan inngå på andre "bærere" hvis det viser seg nødvendig for å sikre utrullingshastighet og brukervennlighet av eID på nivå 4.

Gruppens anbefaling kan således oppsummeres som følger:

1. Det etableres en offentlig utsteder av eID på sikkerhetsnivå 3 (brukernavn, passord, dynamisk komponent), som skal erstatte den type løsninger som i dag er utviklet og i drift i ulike offentlige virksomheter; utrullingen av den type eID skal ta utgangspunkt i Skatteetatens distribusjon av PIN-koder i tilknytning til selvangivelsen/skatteoppgjøret/skattekort.

2. Distribusjon av eID på sikkerhetsnivå 4 baseres på at det blir etablert en ordning for offentlig utstedelse av eID i regi av Justisdepartementet, som et ledd i etableringen av en frivillig ordning for utstedelse av et nasjonalt ID-kort. Distribusjon av eID til befolkningen vil da realiseres gjennom:
   - Nasjonalt identitetskort utstedt av passmyndighetene (alternativ A for forsyning på nivå 4)

   I tillegg[8] også gjennom å utnytte muligheten for at den offentlige eID kan inngå på andre "bærere" og kan distribueres gjennom andre kanaler:
   - Utstedelse av nasjonal eID gjennom NAV-kontor, eksempelvis på helsetrygdkort (alternativ A1)
   - Utstedelse av nasjonal eID gjennom privat distribusjonsapparat, eksempelvis på SIM-kort i mobiltelefoner eller eID-kort utstedt til private formål (alternativ A2).

Skulle nasjonalt ID-kort ikke bli realisert anbefaler gruppen at en alternativ forsyningsplan iverksettes (alternativ B for forsyning på nivå 4), som innebærer at:

- Offentlig sektor inngår en avtale med en utvalgt aktør i markedet etter konkurranse der antall mulige utrullede eID over en gitt tidsperiode vil være et viktig kriterium for valg av leverandør. Rammeavtalen vil innebære sentral frikjøp av transaksjoner med denne eID for hele offentlig sektor, for en

[8] Gitt at behovsvurderinger ifht dekningsgrad av ønskede målgrupper tilsier dette.

begrenset tidsperiode. Inngåelse av slik rammeavtale krever aktiv deltagelse av potensielle store brukere (statlige etater, kommuner), som kan forplikte seg til bruken av eID i et visst volum i forkant. eID utstedt av denne leverandøren må oppfylle felles offentlige krav (Person Høyt).

Den enkelte offentlige virksomhet baserer seg i perioden frem til felles offentlig løsning (for nivå 4) er på plass, på de tilbud som finnes i markedet som tilfredsstiller Kravspesifikasjonen for PKI, Person Høyt.

5 Forsyning av virksomheter med eID

Arbeidsgruppen skal beskrive:
forholdet mellom felles løsninger for forsyning av offentlig sektor med eID og e-signatur (virksomhetssertifikater og ansattsertifikater) til eget bruk, og felles løsninger for validering av eID og e-signatur, inklusive en eventuell reetablering av offentlig sikkerhetsportal.

Mandatet til gruppen refererer direkte til virksomhetssertifikater og ansattsertifikater, som begge er eID-typer realisert ved hjelp av PKI-teknologi. Grunnen til dette ligger i eForvaltningsforskriften[9] , som anbefaler bruk av slike sertifikater, til bruk i kommunikasjon med offentlig sektor – særlig i forbindelse med elektronisk utsendelse av vedtak og mottak av konfidensiell informasjon fra eksterne parter.
Det finnes foreløpig ingen andre, standardiserte løsninger for eID for juridiske personer i markedet, enn virksomhetssertifikater, slik gruppen erfarer.

Det vises til gruppens fortolkning av mandatet i kap. 2.2.1 der gruppen presiserer at det innenfor rammen av denne utredningen ikke var mulig å gi noen anbefalinger når det gjelder personlige eID til offentlig ansatte. I løpet av utredningsperioden ble det imidlertid klart at det er behov for anbefalinger vedrørende forsyning av virksomheter med eID – både de private (bedrifter) i egenskap av brukere av offentlige tjenester, og de offentlige, i egenskap av tilbydere av slike tjenester samt deltakere i intern elektronisk samhandling i forvaltningen. Kapitlet her omhandler anbefalinger for slik forsyning. Vedrørende mandatpunktets andre ledd vises det til kap. 6.

Virksomhetssertifikater er en type elektronisk ID og –signatur, basert på PKI, som kan benyttes som et ”digitalt segl” på dokumenter som ekspederes fra en virksomhet. Denne typen eID godtgjør med sikkerhet at dokumentet er avsendt fra den gitte virksomhet og at det ikke har vært manipulert underveis. Teknologien benyttes også for å sende krypterte meddelelser til virksomheten i tilfeller der meddelelsene inneholder følsomme opplysninger.
Virksomhetssertifikatet vil utstedes til virksomheten, og ikke til en enkel person. Tilbyderen av slik eID må imidlertid forsikre seg om at den utleveres til en person som kan signere på vegne av virksomheten eller har annen form for fullmakt.
Bruk av slik eID forutsetter at det etableres interne systemer for logging som kan synliggjøre hvordan et virksomhetssertifikat brukes og av hvem. Etablering av slike systemer vil være brukervirksomhetens ansvar, og systemene bør reflektere virksomhetens signaturpolicy, dvs. regler for signering av dokumenter.

Virksomhetssertifikater erstatter de papirbaserte tillitsegenskaper som et brevhode med logo, et stempel og ev. en håndskrevet underskrift gir i dag.

eForvaltningsforskriften til forvaltningsloven anbefaler bruk av virksomhetssertifikat i forbindelse med elektronisk utsendelse av vedtak fra offentlige virksomheter. Nye forskrifter som åpner for elektronisk behandling av offentlige innkjøp forventes i å

[9] Forskrift om elektronisk kommunikasjon med og i forvaltningen, gitt med hjemmel i §15A i forvaltningsloven, sist endret 15.12.2005. Forskriften forvaltes av FAD.

gjelde fra 1. januar 2007. Èn mulig teknisk infrastruktur for dette vil være basert på virksomhetssertifikater. Bedrifter kan ha behov for slike sertifikater ifm. elektronisk innrapportering til det offentlige, eller til kommunikasjon seg i mellom.

Ulike modeller for forsyning av norske virksomheter med virksomhetssertifikater kan spenne fra en ren markedsmodell, der virksomheter kjøper sertifikater i markedet, via en offentlig rammeavtale til en samfunnsinfrastrukturmodell der staten etablerer et tilbud for forsyning av alle typer virksomheter med virksomhetssertifikater, i konkurranse med andre aktører i markedet.
Markedsmodellen (nå-situasjonen) omtales ikke spesifikt, det vises bare til at det er gjennom Kravspesifikasjon for PKI definert felleskrav til slike sertifikater, og at det fra 1.12.06 gjelder et krav om selvdeklarasjon av løsninger i markedet hos Post- og teletilsynet[10] dersom løsningene skal brukes i eller av, forvaltningen.

5.1 Offentlig rammeavtale

Staten, ved Brønnøysundregistrene, inngår en rammeavtale for offentlig sektor med én eller flere utstedere av virksomhetssertifikater i markedet. Det antas at en offentlig virksomhet kun vil ha behov for et svært begrenset antall sertifikat per virksomhet[11] og antallet kjøpere er begrenset. I følge Enhetsregisteret er det registrert 5258 offentlige etater pr. dags dato, og antallet virksomheter med et behov på kort sikt er trolig langt lavere. Bruk av virksomhetssertifikat kan vise seg å være meget hyppig i forhold til antall transaksjoner. Med utgangspunkt i erfaringer som enkelte etater har høstet, er det imidlertid et svært sentralt krav at det ikke påløper transaksjonskostnader ved bruk av virksomhetssertifikater. Det kan i denne sammenheng stilles spørsmål ved om markedsandelen til offentlig sektors anskaffelser av virksomhetssertifikater vil være tilstrekkelig stor for en rammeavtale i de nærmeste årene, dersom denne skal gi en rimelig avkastning for aktuelle markedsaktører.

5.2 Statlig infrastruktur for virksomhetssertifikater

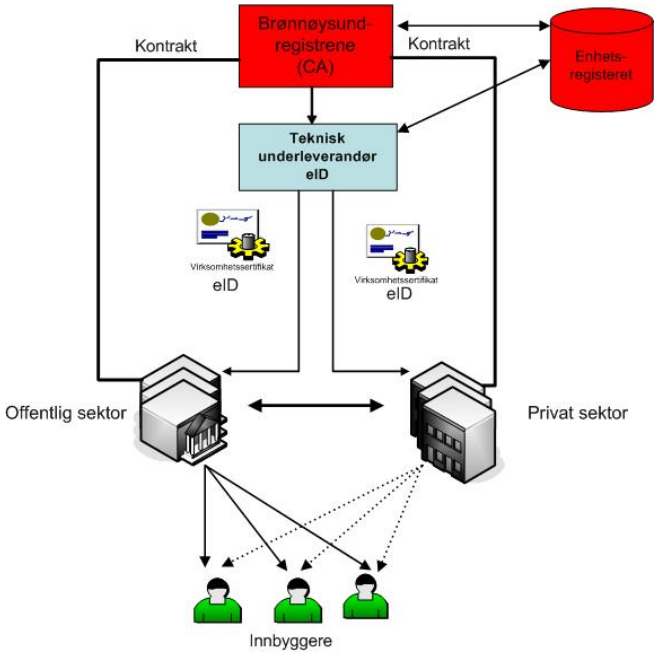
Denne modellen innebærer at Brønnøysundregistrene påtar seg rollen som utsteder av virksomhetssertifikater for norske virksomheter, som del av deres ansvar for enhetsregisteret. Denne oppgaven kan løses enten ved å kjøpe nødvendig utstyr samt programvare, og bygge opp tjenesten internt, eller ved å utlyse en konkurranse og inngå en driftsavtale med en markedsaktør som utsteder slike sertifikater.

Ordningen skal være et tilbud for utstedelse av sertifikater til bruk i privat sektor, i tillegg til tilbudene fra private aktører. For offentlige virksomheter anbefaler gruppen at det er pålagt å benytte ordningen, dersom de skal anskaffe eID for virksomheten, av hensyn til lønnsomhet og kvalitet. Kravet om at offentlige virksomheter skal velge

[10] Det er per i dag to leverandører av virksomhetssertifikater som har selvdeklarert seg hos PT
[11] Dette vil avhenge av den enkelte virksomhet sin IT-arkitekttur. Eksempelvis har NAV implementert virksomhetssertifikat i etaten ved bruk av kun ett sertifikat for hele virksomheten (som omfatter ca 500 "lokale" enheter).

virksomhetssertifikat fra Brønnøysundregistrene innebærer at tjenesten monopoliseres overfor offentlige kjøpere. Overfor de private virksomhetene vil Brønnøysundregistrene tilby sitt sertifikat i konkurranse med private tilbydere i markedet. Dette vil gi en viss fordel for Brønnøysundregistrene. Ut fra at det offentlige ikke representerer noen stor og viktig del av sertifikatmarkedet (drøyt 5000 offentlige virksomheter mot ca 800.000 juridiske enheter innen privat sektor), anses det ikke å være noe stor problem i forhold til konkurransehensyn. Under forutsetning av at man på den annen side ikke tar noe høyere pris av de offentlige virksomhetene enn de private, vil en slik løsning heller ikke vanskeliggjøre en organisering av virksomheten i forhold til statsstøtte.[12]

Tjenesten kan bygges opp etter følgende modell:



Figur 7: Statlig/offentlig infrastruktur for virksomhetssertifikater

Som det fremgår av modellen, vil Enhetsregisteret spille en sentral rolle i prosessen for utstedelse av et virksomhetssertifikat. Registeret er et grunndataregister over alle virksomheter etablert i Norge, og vil være den autoritative kilden til opplysninger knyttet til en virksomhets identitet, som skal bekreftes gjennom utstedelse av et virksomhetssertifikat.

5.3 Offentlig sertifikatdistributør

I denne modellen tar Brønnøysundregistrene på seg rollen som registreringsautoritet (RA) for virksomhetssertifikater. Oppgaven vil i så fall utføres på oppdrag fra aktører i markedet, som utsteder slike sertifikater. Begrunnelsen for at Brønnøysundregistrene i det hele tatt bør kunne påta seg en slik oppgave, er at etaten har ansvaret for

[12] Vurderingen her er basert på Konkurransepolitisk avdeling (FAD) sin tilbakemelding på problemstillingen.

Enhetsregisteret, som vil være den sentrale kilden til opplysninger ved registrering av en forespørsel om sertifikat, jfr. også 5.2.

Oppgaven som RA vil reguleres av en/flere avtaler med slike aktører. Oppgaven innebærer bl.a. at Brreg vil måtte:

- tilrettelegge for bestilling av sertifikat,
- påse at bestiller er bemyndiget til å bestille og påse at bestiller bevitner sin identitet (ved personlig oppmøte),
- igangsette sperring eller suspensjon av sertifikat på grunnlag av sertifikateiers forespørsel, ev. henstilling fra et brukersted
- igangsette fornyelse av sertifikat, etter forespørsel fra eieren.

Ansvaret knyttet til utstedelse, innhold i, og bruk av sertifikater vil være knyttet til sertifikatutsteder, som også vil måtte stå til ansvar for alle oppgaver som utføres av RA. Utstederen vil imidlertid kunne ønske regressmuligheter overfor RA og vil derfor ha en egen avtale om gjensidige plikter og rettigheter i forbindelse med utførelse av en RA-funksjon hos en annen virksomhet. Dersom Brønnøysundregistrene skal likebehandle alle utstedere av virksomhetssertifikater i det norske markedet, vil det være tale om flere slike avtaler.

5.4 Anbefalt strategivalg - forsyning virksomhetssertifikater

I dag er bruk av virksomhets-eID (virksomhetssertifikater) begrenset og forekommer i størst utstrekning i helsesektoren, også i samspill med sentrale trygdemyndigheter. En behovskartlegging hos offentlige virksomheter utført av Brønnøyssundregistrene på oppdrag fra FAD høsten 2006 gir et bilde av begrenset behov når det gjelder antallet sertifikater som vil ønskes utstedt på kort sikt (2-3 år). Dette, kombinert med krav om at virksomhetssertifikater skal prises etter anskaffelses- og vedlikeholdskostnader, og ikke etter bruk, gir lite grunnlag for å anbefale inngåelse av en felles offentlig rammeavtale om kjøp av virksomhetssertifikater. Et minimumsalternativ er å overlate anskaffelsen til hver enkel offentlig virksomhet som har behov for dette, med utgangspunkt i krav stilt i Kravspesifikasjon for PKI i offentlig sektor, som bl.a. innebærer at informasjon fra Enhetsregisteret skal benyttes ved utstedelsen av sertifikatene.

Som forvalter av Enhetsregisteret er Brønnøysundregistrene i en unik posisjon når det gjelder å borge for identiteten av norske virksomheter. Brønnøysundregistrene har allerede i dag en funksjon som en attestant for dette, gjennom utstedelse av firmaattest. Det er derfor nærliggende å tenke utvidelse av denne rollen til også å kunne sertifisere elektronisk identitet for virksomhetene. Når det gjelder prising av tjenesten, vil de samme statsstøttevurderinger gjøre seg gjeldende her som ved forsyning av innbyggere med eID. Separering fra Brønnøysundregistrenes øvrige monopolvirksomhet vil være sentralt ettersom registrene også tilbyr monopoltjenester knyttet til eksempelvis firmaattest.

En slik tjeneste – rollen som sertifikatutsteder – er en naturlig forlengelse av rollen som forvalter av Norges sentrale informasjonsressurser når det gjelder virksomheter, herunder alle bedrifter og alle offentlige virksomheter. Statlig ansvar for en slik rolle

innebærer også at staten vil ha sterkere styringsmuligheter når det gjelder hvilke forretningsmodeller og betalingsstrukturer som skal legges til grunn ved anskaffelse og bruk av virksomhetssertifikater, spesielt når det gjelder offentlige virksomheter. Prising mot ev. private kunder vil måtte ta alminnelige hensyn til konkurransen i markedet og basere seg minimum på medgåtte kostnader til drift av tjenesten.

Det understrekes at eventuelle sertifikater vil utstedes kun på forespørsel fra virksomhetene, og ikke som en automatisk del av en registrering eller endring av informasjon i Enhetsregisteret.

Brønnøysundregistrene som forvalter av Enhetsregisteret vil også være en relevant aktør for å utføre RA - oppgaver. Dette vil kunne gi fordeler både for sertifikateier og for utsteder(e), særlig med hensyn på sikring av kvaliteten i innholdet i sertifikatene. Å la sertifikatutsteder være en markedsaktør vil imidlertid introdusere en rekke juridiske og merkantile utfordringer. Det vil oppstå en situasjon der en markedsaktør har ansvar for oppgaver utført i en offentlig etat. Forhold knyttet til praktisk gjennomføring, plikter og rettigheter, ansvar og betaling for utførte oppgaver vil måtte reguleres gjennom egne avtaler med den eller de aktuelle sertifikatutstedere. En annen utfordring vil være hvordan en skal oppnå en hensiktsmessig prismodell for utstedelse og bruk av sertifikater, slik at modellen ivaretar sentrale offentlige krav samtidig som markedsaktørenes forretningsmodeller legges til grunn. Ut fra dette komplekse saksforholdet virker det derfor sannsynlig at det er mest fordelaktig å heller legge også sertifikatutsteder-rollen til Brønnøysundregistrene.

Med bakgrunn i vurderingene ovenfor anbefaler derfor gruppen at det legges opp til et forprosjekt der Brønnøysundregistrenes rolle som utsteder av virksomhetssertifikater med utgangspunkt i Enhetsregisteret avklares nærmere, med modell beskrevet i kap. 5.2., figur 7 som utgangspunkt. Modellen åpner for ulike driftsløsninger, men tar utgangspunkt i at det utlyses en offentlig konkurranse om teknisk drift av en utstedertjeneste for virksomhetssertifikater.

Løsningen vil innebære at Brønnøysundregistrene etablerer seg som en tilbyder av virksomhetssertifkater i et marked hvor det fra før er private tilbydere. Dette anses i utgangspunktet som positivt, da et marked tilføres en ny aktør som kan være et konkurransemessig korrektiv i et konsentrert marked. Brønnøysundregistrene vil kunne utstede sertifikater til alle som er registrert, på frivillig basis. Delvis er dette forslaget begrunnet i at utstedelse kun til offentlige virksomheter vil omfatte så få virksomheter at nytten ikke oppveier kostnadene. Samtidig er det et sentralt poeng ved ordningen at den også skal brukes mellom næringslivet og offentlig sektor. Dersom alle virksomheter får sertifikater vil elektronisk kommunikasjon (dokumenthåndtering) kunne få et betydelig omfang og gi gevinster både hos private og offentlige virksomheter.[13]

[13] Vurderingene er hentet inn fra Konkurransepolitisk avdeling i FAD.

6 Samtrafikknav for bruk av eID og e-signatur i offentlig sektor

Arbeidsgruppen skal foreslå:
strategiske valg for felles offentlige løsninger for validering av eID og e-signatur. Det skal vurderes mulig reetablering av en felles offentlig sikkerhetsportal, med utgangspunkt i foreliggende sikkerhetsportalkravspesifikasjonen, med nødvendige endringer og tillegg. Det må vurderes hvilke tjenester en reetablert sikkerhetsportal skal tilby ut over validering av eID og e-signatur.

6.1 Innledning

I veivalgene knyttet til realisering av en samtrafikkløsning for offentlig sektor er det nødvendig å foreta en rekke avveininger. For det første må offentlige virksomheter - store og små aktører - ta stilling til arbeidsdelingen mellom egne elektroniske løsninger og fellesløsninger. Dette vil sannsynligvis falle meget forskjellig ut for de ulike aktører. Ytterpunktene er på den ene siden halvparten av landets kommuner som betjener en befolkning på under 5000 mennesker hver og store statlige etater som betjener alle landets innbyggere. I tillegg har man aspektet knyttet til kompleksitet i forhold til eksempelvis kommuner som har mange ulike tjenestetyper versus mindre etater som kun vil ha et lite antall e-tjenester (som i stor grad befinner seg innenfor samme fagområde). Selv om arbeidsdelingen naturlig vil falle ulikt ut, vil det sannsynligvis kunne identifiseres et knippe med grunnleggende basistjenester som alle aktører har behov for. Imidlertid er det behov for å ta hensyn til hvilke modeller sikrer en mest mulig hensiktsmessig organisering av samtrafikk og hvilke aktører som skal inngå i en slik løsning. Dette kapitlet drøfter disse tre aspektene knyttet til en samtrafikkløsning for eID og e-signatur i offentlig sektor.

6.2 Funksjonalitet i et offentlig samtrafikknav.

Et felles samtrafikknav for eID og e-signatur i offentlig sektor *kan* dekke følgende sett av funksjoner:

- Autentisering med eID mot webtjenester (med ulike typer eID på både sikkerhetsnivå 3 og sikkerhetsnivå 4, minimum eID av typen Person Høyt, Person Standard og Virksomhet samt SkattePIN og MinID)
- Formidling av (ulike typer av) elektronisk identitet mot webtjenester (single sign-on / felles pålogging)
- Autentisering med eID fra fagsystemer (via web-services)
- Signering av brev, skjema og filer, både sentralt (web-applikasjon) og grensesnitt mot lokal signering, samt verifikasjon av signaturene
- Validering av sertifikater, både ved autentisering og ved verifikasjon av signaturer, enten via CRL (tilbakekallingslister) eller OCSP (online sanntidsvalidering)
- Signering og kryptering av e-post
- Kryptering generelt
- Tiltrodd digitalt arkiv over signerte dokumenter eller signerte hash-verdier (dokument-fingeravtrykk), s.k. innsynsarkiv
- Katalog med offentlige nøkler til virksomheter i Norge
- Katalog med offentlige nøkler til personer

- Oppslagstjeneste for fødselsnummer

Ut fra erfaringer med tidligere løsninger, og behovsvurderinger gjort av sentrale aktører anbefales det minste felles multiplum av tjenester i en samtrafikkløsning i første fase å være:

- Autentisering med felles eID på sikkerhetsnivå 3 og 4, som også vil omfatte validering av sertifikat for sikkerhetsnivå 4 og fødselsnummer oppslag
- Signering av webskjema og lokalt (grensesnitt for fagsystemer) med bruk av felles løsninger
- Digitalt Arkiv - innsynsarkiv
- Videreformidling av identitet (som en generisk tjeneste).

Digitalt arkiv er en tjeneste som henger tett sammen med tjeneste for signering. Det vil teknisk sett kunne være vanskelig å introdusere en tjeneste for digitalt arkiv etter at tjeneste for signering er etablert. Behovet for slikt arkiv oppstår i hovedsak av to årsaker (som også kan være komplementære):

1) vanskeligheter med å håndtere digitalt signerte dokumenter hos mindre aktører
2) behov for kopilager av elektroniske dokumenter som er digitalt signert og som skal gis tilgang til for privatpersoner som dokumentene berører (innsynsarkiv).

Digitalt arkiv bør derfor være en grunnleggende tjeneste, men med en frivillighet når det gjelder å ta den i bruk, dvs. bruk av signeringstjenesten må ikke forutsette bruk av digitalt arkiv. Det er brukerstedet (virksomheten) som velger å ta i bruk tjenesten ”digitalt arkiv” som er ansvarlig for innsyn i arkivet (i tråd med arkivloven og personopplysningslovens bestemmelser).

Når det gjelder videreformidling av identitet, kan det være hensiktsmessig å se på den som en tilleggsfunksjon, dvs. at brukeren kan logge seg på i et ”tjenesteunivers”. Man kan tenke seg flere slike ”univers” med ulikt omfang:

- Nasjonalt perspektiv hvor ny sikkerhetsløsning videreformidler til alle brukersteder som tar fellesløsningen i bruk
- Fellesportaler som videreformidler til bakenforliggende brukersteder – typisk MinSide og Altinn
- Kommunalt samarbeid der flere kommuner går sammen om felles tjenestetilbud til innbyggere
- Hvert enkelt brukersted som videreformidler mellom egne tjenester (typisk større statlige etater).

Slik sett vil dette være en tjeneste som er generisk og der implementering og omfanget av bruken bestemmes av brukerstedene som velger å kjøpe tjenesten, og ikke av samtrafikknavet selv.

Samtrafikknavet skal integrere de offentlige utstedere av eID på ulike sikkerhetsnivå. Samtidig må samtrafikknavet være et fleksibelt verktøy som også kan integrere løsninger fra forskjellige eID-leverandører (særlig viktig hvis plan B må realiseres).. Integrasjon av nye eID-leverandører må kunne skje uten at samtrafikkløsningen må

endres radikalt for hver ny eID-leverandør som blir tilsluttet. Dette tilsier at løsningen må være basert på en arkitektur som støtter en modulbasert trinnvis utvikling og innføring. Videre må løsningen støtte aktuelle åpne standarder for kommunikasjonsprotokoller og applikasjonsgrensesnitt.

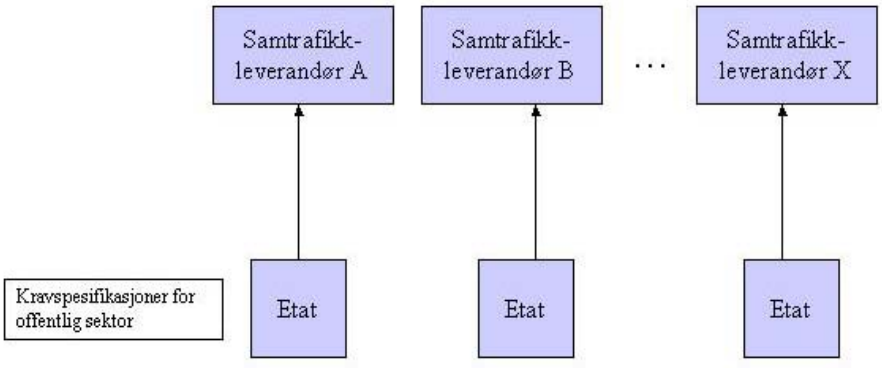
6.3 Modeller for realisering av samtrafikknav

6.3.1 ”Markedsanskaffelse”

I denne modellen forutsettes det at enkelte virksomhet som ønsker å tilby elektroniske tjenester til sine brukergrupper, selv går til anskaffelse av nødvendig programvare og sørger for integrasjon av den i egne systemer, alternativt anskaffer en eksisterende tjeneste i markedet som tilbyr ønsket funksjonalitet. Virksomheten vil selv måtte sørge for at den anskaffede løsningen integrerer anbefalte typer eID som kan benyttes mot tjenester i forvaltningen, jfr. kap. 4 og 5.

6.3.2 ”Kravspesifikasjon”

Modellen tar utgangspunkt at det nå skjer en rekke bevegelser i markedet for sikker samtrafikkløsninger. Kommersielle leverandører tilbyr sine produkter direkte til den enkelte offentlige virksomhet. Samtrafikkløsningen vil bli tilbudt offentlige virksomheter som en tilleggsfunksjonalitet til saks-/og arkivløsninger. Fordelen med modellen er at staten ikke har behov for å investere i infrastruktur og løsningen som får oppslutning i offentlig sektor tilsvarer løsningene som har generell kommersiell utbredelse. I denne modellen vil det bli utarbeidet en kravspesifikasjon for sikkerhetsportalfunksjonalitet. Utforming og innhold av felles kravspesifikasjon vil basere seg på at denne må ta opp i seg forholdet til eID leverandører og sikre samtrafikk mellom de eID leverandørene som skal aksepteres i de offentlige løsningene, dvs. samtrafikk mellom den felles offentlig utstedte eID på sikkerhetsnivå 3 og 4 samt eventuell eID leverandør(er) i markedet på sikkerhetsnivå 4 som vinner konkurransen (hvis plan B). Det må også tas høyde for implementering og samtrafikk med offentlig eID på ev. andre bærere, hvis utstedelse av dette blir nødvendig.



Figur 8: Kravspesifikasjon

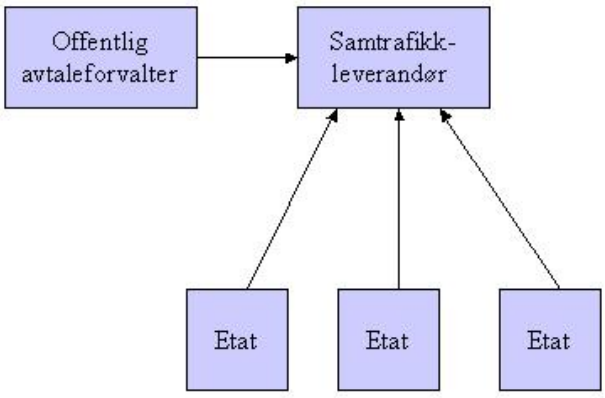
Kravspesifikasjonen kan enten gjøres obligatorisk eller frivillig for offentlige virksomheter. Utfordringen med modellen er særlig knyttet til forholdet mellom det

offentliges rolle/ansvar for utstedelse av eID versus ansvaret for samtrafikkløsningen. Ved denne kombinasjonen av distribusjons- og samtrafikkløsninger vil det offentlige ta et sentralt grep for å sikre bred og rask utbredelse av eID for innbyggere, mens det blir opp til de enkelte etater/virksomheter å etablere/anskaffe teknisk løsning og funksjonalitet for bruk av eID i de elektroniske tjenestene de tilbyr.

Modellen er urealistisk i forhold til forretningslogikken mellom samtrafikkleverandør og eID leverandør. Dette er først og fremst basert på kunnskap om de forretningsmodeller som i dag eksisterer mellom samtrafikk leverandører og eID leverandører. Hvis denne modellen skal realiseres må det offentlige i fellesskap sørge for *distribusjon* av eID, menikke *bruk* av eID. Betaling for det siste må fortsatt ligge på virksomhetsnivå.

6.3.3 ”Rammeavtale”

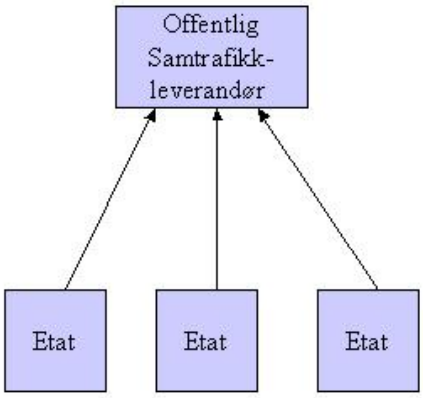
Alternativene innebærer at offentlig sektor inngår en rammeavtale hvor en privat tilbyder gis i oppdrag å etablere en samtrafikkløsning for offentlig sektor. Denne innebærer at offentlige virksomheter knytter seg direkte til leverandøren gjennom abonnementsavtaler. Modellen innebærer at offentlig sektor har minimal risiko knyttet til etablering og drift, men vil måtte overlate tekniske løsningsvalg til den leverandør som velges. Håndtering av avtaler med eID-utstedere må være hvert enkelt brukersted sitt ansvar, jfr. drøfting under modell 3.



Figur 9: Rammeavtale

6.3.4 ”Offentlig samtrafikknav”

Det offentlige eier og forvalter selv et samtrafikknav. Selve utviklingen og teknisk drift av løsning, kan overlates til private aktører på samme måte som det offentlige gjør ved etablering av andre større systemløsninger. Modellen skal basere seg på standard komponenter som finnes i markedet og åpne standarder.



Figur 10: Offentlig samtrafikknav

6.3.5 Valg av modell - forutsetninger

Arbeidsgruppen har lagt til grunn at det er behovene til offentlige virksomheter og effektiv ressursbruk som er styrende for valg av modell. I motsetning til i kapittel 4 og 5 er hensynet til sluttbrukere av mindre betydning for valg av modell for samtrafikknav. Samtrafikknavet er ikke en løsning som sluttbruker vil være direkte i kontakt med siden dette er en funksjonalitet som skal sikre at de offentlige virksomhetene har et troverdig og robust alternativ for sikkerhetsadministrasjon knyttet til elektroniske tjenester.
Det vil således være behov for et samtrafikknav som håndterer felles eID-løsninger i statlig regi på ulike sikkerhetsnivå, det vil si sikkerhetsnivå 3, 4 og virksomhetssertifikater. Dette innebærer at offentlig sektor må ha muligheten for å kunne styre utviklingen av løsningen. Videre er det nødvendig at samtrafikknavet sørger for at offentlig sektors behov blir prioritert og ivaretatt. Offentlig sektor bør ha full råderett over egen autentiserings- og signeringsløsning. Dette tilsier at markedsmodell, kravspesifikasjons-modell og rammeavtale-modell ikke vil sikre den nødvendige offentlige kontrollen over løsningen. Samtrafikknavet skal tilby et smalt utvalg av tjenester i første omgang, men på sikt skal dette bygges ut i takt med den teknologiske utviklingen og det offentliges behov. Den virksomheten som skal være ansvarlig for samtrafikknavet skal også ha ansvaret for å etablere de nødvendige avtaler med den eID-utstederen som offentlig sektor velger dersom plan B må realiseres.

6.4 Anbefalt strategivalg for samtrafikkløsning

Gruppen anbefaler at et samtrafikknav for eID etableres som et offentlig drevet tilbud, der den tekniske infrastrukturen leveres av en markedsaktør gjennom en langsiktig drifts- og vedlikeholdsavtale. Samtrafikknavet skal tilby en rekke felles funksjoner knyttet til autentisering og signering, og på sikt også konfidensialitetssikring. Utvalget av tjenester i første versjon vil dog være begrenset til:

- Autentisering med felles eID på sikkerhetsnivå 3 og 4, som også vil omfatte validering av sertifikater for sikkerhetsnivå 4 og fødselsnummeroppslag.
- Signering av webskjema og lokalt (grensesnitt for integrasjon i fagsystemer), med bruk av felles løsninger.

- Digitalt arkiv for signerte dokumenter/dokument-hash.
- Videreformidling av ferdig validert eID (felles pålogging), som en generell funksjonalitet.

Hvorvidt bruk av samtrafikknavet skal være pålagt eller valgfritt bør vurderes nærmere, herunder ev. hvilke tjenester som det ev. skal pålegges bruk av.

Flere funksjoner, herunder konfidensialitetssikring, skal kunne integreres i samtrafikknavet etter hvert, basert på prioriteringer og krav fra brukervirksomheter.

7 Forretningsmodeller for offentlig eID

Arbeidsgruppen skal foreslå:
Strategiske valg av forretningsmodeller for bruk av fellesløsninger som virker som insentiver for aktuelle aktører til å bidra til spredning og bred bruk av løsningene. Modellene skal sikre økonomisk forutsigbarhet for de ulike aktører. Løsningene som etableres bør også kunne benyttes ved avtaleinngåelser mellom private parter.

7.1 Innledning

Med forretningsmodell siktes det her til valg av innretning på avtaler mellom aktører, samt regulering av ansvar og roller mellom disse. Avtalene kan være av både økonomisk og ikke økonomisk karakter. Med ikke-økonomisk avtale menes en avtale som regulerer ansvar og plikter/rettigheter, mens de økonomiske avtalene i tillegg regulerer betalingsstrømmer.

Forretningsmodeller beskriver forholdet mellom aktørene, men omfatter ikke de underliggende leverandøravtaler aktørene eventuelt anskaffer seg (som for eksempel underleverandører av samtrafikknavet, kortutsteder, osv.).

Basert på strategivalgene som gruppen har kommet frem til under kapittel 4, 5 og 6, skisseres det her forretningsmodeller som skal kunne realisere de anbefalte løsningene. Forretningsmodellen omfatter alle de 4 områdene som det gis anbefaling for (dvs. forsyning av eID til innbyggere for nivå 3 og 4, eID til virksomheter (virksomhetssertifikater) og samtrafikknav.

I kapittelet drøftes to hovedmodeller, som i hovedsak skiller seg fra hverandre i forhold til spørsmålet om finansiering mellom samtrafikknav og brukersted. Med dette menes at den ene modellen er basert på ikke-økonomiske avtaler mellom samtrafikknav og brukersted, mens den andre er basert på økonomisk modell mellom samtrafikknav og brukersted. Etablering av en felles forretningsmodell skal synliggjøre hvilke avtaler som må inngås mellom de ulike aktørene, samt hvorvidt disse vil være av økonomisk eller ikke-økonomisk karakter. Forretningsmodellen skal omfatte begge funksjonene og vil derfor involvere mange aktører:

- Sluttbrukere (innbyggere og virksomheter)
- Offentlige brukersteder/Tjenesteiere
- Offentlige eID-leverandører/ev. kommersielle eID-leverandører
- Offentlig samtrafikknav

Sluttbruker (innbyggere og virksomheter) forholder seg i utgangspunktet til eID leverandører ved anskaffelse/forsyning av eID-er, enten i form av informasjons- og veiledningsdokument eller i form av en anskaffelses-/brukeravtale. En ansakffelse-/brukeravtale er først og fremst relevant for virksomhetssertifikater, men vil også være relevant for innbyggere i tilfelle realisering av alternativ B ifht. forsyning av innbyggere med eID på nivå 4.

Offentlige brukersteder vil på sin side forholde seg til forvalter av samtrafikknavet. Det vil være forvalter av samtrafikknavet som vil ha en sentral og koordinerende funksjon i

forhold til den totale løsningen for eID i offentlig sektor. Det vil være denne aktøren som både må ha et regulert forhold til eID-leverandørene og brukerstedene. De offentlige eID-leverandørene vil ha en ikke-økonomisk avtale med forvalter av samtrafikknavet, mens en mulig kommersiell eID leverandør vil ha en økonomisk avtale.

Valg av forretningsmodell må videre sees i sammenheng med beslutning om hvorvidt en offentlig eID skal kunne benyttes mot private tjenester, da dette kan få konsekvenser for kostnader og prisingsprinsipper.

Ved valg av offentlig eID modell oppstår det en utfordring knyttet til statsstøtte dersom eID'en tillates brukt mot private brukersteder. Den offentlige eID utstederen vil da bli aktør på linje med andre tilbydere av eID. Dersom offentlig eID bare tillates brukt mot offentlige brukersteder vil problemet med statsstøtte derimot ikke oppstå. En mellomløsning kan være å introdusere eID som en ren offentlig ordning og på et senere tidspunkt ta stilling til om bruken av eID skal utvides til også å gis tilgang til private brukersteder.[14]

7.2 Premisser og forutsetninger

Etableringen av en forretningsmodell som dekker behovene til de ulike aktørene på en tilfredsstillende måte gjør det nødvendig å stadfeste de prinsippene som danner rammebetingelsene for valg av modeller. Gruppen mener at følgende 5 prinsipper angir rammene for hvilke modeller som kan etableres.

Prinsipp 1: Gratis bruk for innbyggere og næringsliv
Det legges til grunn at det skal være gratis for bruker (innbygger/virksomhet) å *benytte* eID i kommunikasjon med offentlige tjenester. Begrunnelsen for dette er knyttet til at det som en hovedregel bør være gratis for brukere å få tilgang til offentlige elektroniske tjenester. Effekten og gevinsten ved at brukere kommuniserer elektronisk ligger hos offentlig sektor. Derfor er gratisprinsippet et avgjørende insitament for å få flest mulig til å ta denne kanalen i bruk. Det er i tillegg grunn til å anta at krav om betaling fra brukerne vil oppfattes som lite brukervennlig og dermed forsinke utbredelsen. Betaling vil dermed bli et hinder for å oppnå den ønskede overgangen fra papirbasert og manuell tjenesteyting til bruk av elektroniske tjenester. Derfor legges det opp til at løsningen i strategiens realiseringsperiode ikke baserer seg på transaksjonskostnader for bruk av og i offentlige virksomheter. Dette kan imidlertid tas opp til ny vurdering etter at bruken av offentlige e-tjenester er etablert som et fast mønster.

Kostnader for *anskaffelse* av eID for (innbygger og næringsliv) kan aksepteres. Det vil derimot ut fra hensynet til bred distribusjon være avgjørende at anskaffelse av eID og eventuelle kortlesere prises så lavt som mulig. Eksempelvis kan kostnader for eID på nasjonale id-kort (nivå 4) være "innbakt" i passgebyret. Samtidig antas det at innbyggere og næringslivet vil ha ulik aksept for prisnivået på anskaffelse. Anskaffelseskostnader for eID vil derfor kunne variere avhengig av om den er for innbyggere eller for næringslivet.

[14] Vurderinger innhentet fra Konkurransepolitisk avdeling i FAD

Prinsipp 2: Konsistens i forhold til (gjen)bruk i offentlig sektor
Alle offentlige tjenester må *akseptere og håndtere* de felles løsninger for eID som etableres (forutsatt rett sikkerhetsnivå). Dette prinsippet følger av de anbefalinger som er gitt vedr forsyning av eID, og gjør det nødvendig med felles samtrafikknav. Begrunnelsen for dette er å sikre brukervennlighet for sluttbruker. Det betyr at de som tilbyr elektroniske tjenester i det offentlige, må ta i bruk og implementere felles eID løsning(er) når disse foreligger.

Det skal ikke utvikles egne etatsspesifikke løsninger i offentlig regi for eID for elektronisk kommunikasjon med offentlig sektor. De etablerte etatsspesifikke eID-løsninger skal etter en overgangsperiode (med parallelle løsninger) fases ut, avhengig av andel distribuerte eID-er relatert til det nivået av utbredelse og dekningsgrad av målgruppen som tjenesten krever. Allerede etablerte e-tjenester hos etaten vil med andre ord i en "mellomfase" eksistere parallelt med fellesløsninger for eID. Mandatet fremhever at forretningsmodell må sikre spredning og bred bruk, prinsippet om konsistens og tilgjengelighet relaterer seg særlig til spørsmålet om bred bruk.

Bruker kan benytte de eID typene som er definert på alle offentlige tjenester avhengig av nivå. Dette medfører at bruker ikke fritt kan velge eID løsning i markedet, men den/de eID som blir besluttet (jfr kap 4), kan til gjengjeld brukes mot alle offentlige tjenester.

De eID-leverandører som vil være koblet til samtrafikknavet er de som blir besluttet for elektronisk kommunikasjon med offentlig sektor.

Samtrafikknavet er et viktig virkemiddel for å sikre konsistens overfor sluttbruker, samt et effektiv teknisk bidrag for å integrere felles eID-løsninger hos brukerstedene. Integrering mot sikkerhetsnavet er i utgangspunktet valgfritt for brukersted, men ut fra samfunnsøkonomiske vurderinger og hensiktsmessighet anses det som en viktig forutsetning at flest mulig integrerer seg mot denne felles løsningen og ikke utvikler egne samtrafikkløsninger.

Prinsipp 3: Økonomisk forutsigbarhet
Offentlige virksomheter må ha en forutsigbarhet i kostnader, ettersom deres budsjetter blir årlig fastsatt av stortinget. Virksomhetene har ikke anledning til å gå ut over de økonomiske rammer som er fastsatt for et gitt budsjettår. Økonomiske avtaler må derfor basere seg på kontrollerbare prismodeller (fastpris, årlig avgift, abonnement, eksempelvis basert på antall brukere). Økonomisk forutsigbarhet er avgjørende for raskest mulig å få brukersteder til å ta i bruk felles eID-løsninger, og dermed flytte fokus på utvikling av nye selvbetjente elektroniske tjenester. Manglende økonomisk forutsigbarhet i startfasen vil være et hinder for å motivere offentlige virksomheter til utvikling av nye tjenester og fungere som en sperre for å knytte seg til, og ta i bruk felles løsninger. På sikt kan forutsigbarheten bli et mindre absolutt krav, når mønsteret av bruken av eID er etablert blant brukere og etatene vil kunne budsjettere ut fra erfaringstall.

Erfaring fra prising ved bruk av eID

Altinn har fra starten av hatt en transaksjonsmodell for å dekke kostnadene for autentisering ved tilgang til løsningen. Dette har vært gjort ved at Altinn Sentralforvaltning (ASF) har forskuttert kostnadene og i ettertid fakturert de deltakende etater, etter en på forhånd avtalt fordelingsmodell. Dette gjelder både for autentisering med passord (passordbrev eller mobilpassord) og for autentisering med smartkort (Buypass løsning). Erfaringene er at dette har fungert tilfredsstillende for de ordninger og med det volum løsningen så langt har hatt. Det er i hovedsak Skatteetaten som har dekket disse kostnadene. Med en volumandel på ca 95 % i løsningen har fordelingsmodellen selvsagt avspeilet dette. Imidlertid er dette en ordning som i seg selv er uforutsigbar for tjenesteleverandørene til Altinn og som er krevende å administrere for ASF. Både uforutsigbarhet og kompleksitet i administrasjonen vil tilta med flere aktører og med større spredning i kostnadene på flere tjenesteleverandører.

Det er en avgjørende forutsetning at eID på et høyere nivå skal kunne brukes til å få tilgang til tjenester på et lavere nivå. Denne forutsetningen er også av betydning for foretnings- og prismodell ettersom transaksjonskostnader for autentisering på nivå 3 ofte er lavere enn kostnader på nivå 4. Dette tilsier at valg av modell må sikre at det ikke vil bli uforholdsmessig høye kostnader ved bruk av kombinasjonen autentisering og signering. Kombinasjonen autentisering og signering i samme transaksjon kan bli utbredt for tjenester som krever eID på nivå 4.

De ulike tjenestene som er planlagt å inngå i samtrafikknavet kan prises ulikt, men det må være prisingsmodeller som er enkle for brukerstedene å stipulere kostnader i forhold til. Prisdifferensiering mellom de ulike tjenestene fra navet som brukerstedene vil ta i bruk kan håndteres ved trappetrinnsmodell for prising.

Prinsipp 4: Enkle ansvars- og avtaleforhold

Det skal være enkelt for etatene/brukerstedene å kople seg opp mot samtrafikknavet. Det skal kun kreve én avtale. Denne avtalen skal dekke alle forhold, inkludert knytninger til eventuelle del-leverandører.

For å sikre ansvar og eierskap knyttet til felles samtrafikknav og videreutvikling av dette, skal man basere seg på avtale om anskaffelse av løsning, inkludert en drifts- og utviklingsavtale. Enkle ansvars- og avtaleforhold bidrar til å sikre administrative besparelser for det offentlige totalt sett, gjennom å eliminere unødige kostnader som vil oppstå hvis hvert brukersted skal forvalte egne avtaleforhold knytte til de involverte partene i denne strukturen.

Forvalter av samtrafikknavet vil på sin side inngå ulike økonomiske og ikke-økonomiske avtaler med samarbeidsparter og underleverandører. Disse avtalene skal også basere seg på kontrollerbare kostnader/størrelser, med utnyttelse av stordriftsfordeler.

Prinsipp 5: Utnytte det offentliges stordriftsfordeler /samlede kjøpekraft
Der hvor forretningsmodellene forutsetter økonomiske avtaler med markedsaktører, enten de er knyttet til *bruk* av eID eller til anskaffelse av en teknisk underleveranse, kan offentlig sektors samlede kjøpekraft redusere den totale samfunnskostnaden ved etablering av felles løsninger. F. eks. vil et felles utkjøp av eID-bruk hos en mulig kommersiell leverandør sikre bedre priser enn om hver enkelt offentlig virksomhet skulle forhandle om priser selv.

For leverandører vil dette prinsippet bidra til å sikre forutsigbarhet mhp. inntektsstrømmer, og derved balansere det offentliges krav om bedre priser. Fellesavtaler innebærer også at administrative kostnader knyttet til forhandlinger og avtaleinngåelse kan minimeres. Dette vil også redusere leverandørens administrative kostnader ved selektiv fakturering av bruk mot enkelte brukersteder.

7.3 Forretningsmodeller

Det drøftes to modeller som begge er basert på offentlig eID leverandør for nivå 3,4 og virksomhet. I tillegg tas det i modellen høyde for eventuell iverksetting av plan B for nivå 4 gjennom en felles avtaleinngåelse (anskaffelse) med én privat eID leverandør (jfr. kap 4). Videre legger forretningsmodellen til grunn at samtrafikknavet skal være i offentlig eie og tilrettelegges gjennom en offentlig aktør. Aktøren får ansvar for avtaleinngåelse både med de offentlige brukerstedene og eID-leverandørene. Et forslag til konkretisering av ansvar for de ulike rollene i modellene er som følger:

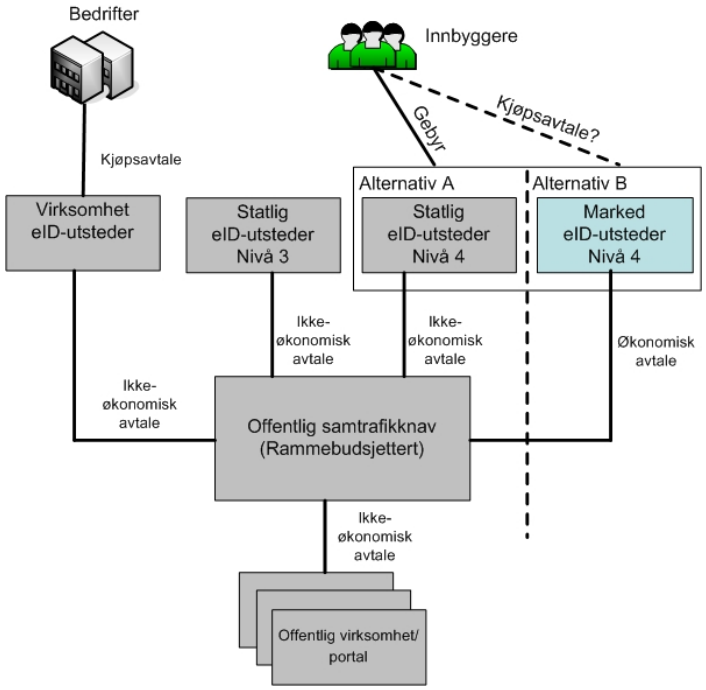
- Skatteetaten utvikler, utsteder og distribuerer eID på nivå 3. Finansiering skjer innenfor rammen av egne budsjetter.
- Justisdepartementet og POD etablerer, utsteder og distribuerer eID nivå 4, i samband med utstedelse av nasjonalt ID-kort. Finansiering skjer innenfor rammen av egne budsjetter.
- Brønnøysundregistrene etablerer en ordning for utstedelse og distribusjon av virksomhetssertifikater. Finansiering skjer innenfor egne budsjetter med mulighet for inntektsføring av salg.
- Brønnøysundregistrene forvalter samtrafikknavet.
- Hvis realisering av eID nivå 4 krever alternativ B, må en offentlig aktør utlyse og inngå avtale med en eID leverandør i markedet. Det er mest nærliggende at Brønnøysundregistrene, som forvalter av samtrafikknavet, tillegges denne oppgaven.

Med utgangspunkt i dette beskrives det videre to hovedmodeller:

1. Ikke-økonomiske avtaler mellom samtrafikknav og brukersted, en *sentralisert* forretningsmodell
2. Økonomiske avtaler mellom samtrafikknav og brukested, en *desentralisert* forretningsmodell

De enkelte aktørene vil i tillegg kunne ha egne avtaler med underleverandører, disse synliggjøres ikke i forretningsmodellene.

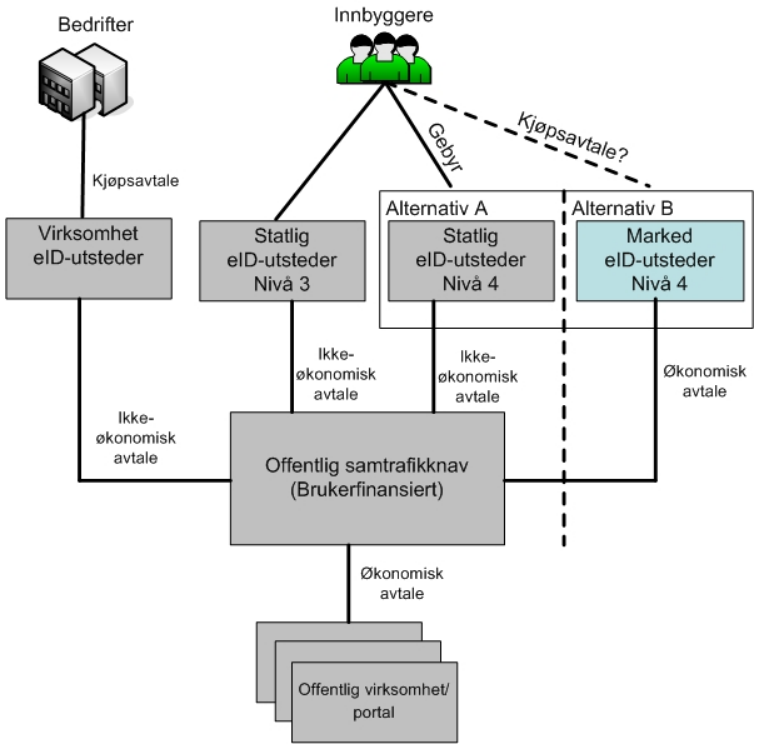
7.3.1 Sentralisert forretningsmodell



Figur 11: Sentralisert forretningsmodell

Modellen innebærer at kostnadene ved etablering og bruk sentraliseres hos forvalter av samtrafikknavet. Dette medfører at kostnadene ikke belastes den enkelte offentlige virksomhet, men at den offentlige bruken rammefinansieres i sin helhet. Samtrafikknavet inngår avtaler med eID-leverandørene på vegne av de offentlige virksomhetene som knyttes til samtrafikknavet. Den enkelte offentlige virksomhet inngår en ikke-økonomisk avtale med samtrafikknavet som regulerer tilgang og ytelser til de tjenester som inngår i navet, og tilgang til bruk av de eID-løsningene som er tilknyttet samtrafikknavet. Forholdet mellom samtrafikknavet og eID-leverandørene vil reguleres med ikke-økonomiske avtaler som primært vil dekke tekniske forhold og ansvarsforhold. Modellen innebærer at administrative kostnader mellom de offentlige deltakerne i denne strukturen vil minimeres. I modellen er det skissert en økonomisk avtale mellom samtrafikkforvalter og en kommersiell leverandør av eID på nivå 4 (alternativ B) hvis hovedstrategien A ikke lar seg gjennomføre.

7.3.2 Desentralisert forretningsmodell



Figur 12: Desentralisert forretningsmodell

Modellen innebærer i likhet med sentralisert forretningsmodell (figur 11) at kostnadene for *etablering* av samtrafikknavet finansieres gjennom en felles grunninvestering. Til forskjell fra sentralisert forretningsmodell innebærer desentralisert forretningsmodell at investeringskostnadene og bruk belastes den enkelte offentlige virksomhet i etterkant. Samtrafikknavet vil, i likhet med sentralisert forretningsmodell, inngå avtaler med eID-leverandørene. Den enkelte offentlige virksomhet vil i en desentralisert modell inngå en økonomisk avtale med samtrafikknavet som finansierer bruk av samtrafikknavets funksjonaliteter og bruken av eID i det kommersielle alternativ B. I likhet med sentralisert forretningsmodell, vil denne modellen innebære at samtrafikkforvalter må inngå en fastprisavtale med en kommersiell leverandør om tilgang på eID hvis alternativ B må realiseres for eID på nivå 4.

7.4 Anbefalt strategivalg - forretningsmodell

Sentralisert forretningsmodell har den fordel at offentlige virksomheter ikke vil være begrenset av egen budsjettsituasjon for å ta i bruk autentiseringstjenester som muliggjør utvikling og tilbud av elektroniske tjenester som krever eID. For å kunne få til et skifte fra papirbaserte og manuelle kanaler til elektroniske kanaler, er det en nødvendig premiss at sikkerhetsfunksjonaliteten som samtrafikknavet gir tilgang til fremstår som attraktivt for den enkelte offentlige virksomhet og fungerer som en muliggjører.

Imidlertid er det en ulempe med denne modellen at den ikke bidrar til å regulere ressursbruk. På den andre siden vil det være den modellen som best stimulerer til et raskere skifte fra papirbaserte og manuelle kanaler til elektroniske tjenester. Desentralisert forretningsmodell vil sikre at kostnadene for bruk vil bli fordelt på det enkelte brukersted som har elektroniske tjenester ut mot sluttbruker. Offentlig sektor som helhet unngår dermed å finansiere en løsning som ikke er riktig dimensjonert i forhold til faktisk bruk.

Etablering av et felles samtrafikknav for offentlig sektor knyttet til eID og etablering av statlige eID til befolkningen på nivå 3 og 4 er å anse som etablering av en nødvendig offentlig infrastruktur for å realisere elektronisk forvaltning som en del av visjonen om Norge som et informasjonssamfunn. Dersom slik felles infrastruktur ikke finnes vil offentlige virksomheter etablere separate løsninger som reduserer mulighetene for konsistens for sluttbruker og som mest sannsynlig øker den samlede offentlige ressursbruken utover det som bør være samfunnsøkonomisk forsvarlig.

For sterkt fokus på regulering av ressursbruk i startfasen på oppbyggingen av en nasjonal infrastruktur kan hemme omstillings- og fornyingstakten i offentlig sektor. Valget knyttet til *bruk av* offentlige elektroniske tjenester bestemmes av sluttbruker og ikke av den enkelte offentlige virksomhet. Det er i det offentliges interesse at sluttbrukere benytter elektroniske kanaler fremfor bruk av papirbaserte eller fysiske kanaler. Derfor er spørsmålet om regulering av ressursbruk ikke relevant i oppstartsfasen for felles løsning av eID i offentlig sektor. Dette spørsmålet kan likevel tas opp igjen etter at en etablerings- og innkjøringsfase for løsningen er gjennomført. I tillegg bør det stilles krav til at de enkelte tjenester som bruker samtrafikknavet er tilrettelagt på en slik måte at de ikke er unødig kostnadsdrivende for det offentlige.

Arbeidsgruppen har på denne bakgrunn konkludert med at sentralisert forretningsmodell er den anbefalte forretningsmodellen som skal legges til grunn for realisering av strategi for eID i offentlig sektor.

8 Økonomiske og administrative konsekvenser

I dette kapitlet gis det en kort beskrivelse av de økonomiske og administrative konsekvenser som arbeidsgruppen har identifisert knyttet til sine anbefalinger. Anslagene og kostnadsvurderingene er beheftet med en del usikkerhet, og er også avhengig av det endelige valget av modell for realiserig av de ulike tiltakene.

I tillegg til å oppnå forenklingsgevinster for innbyggere (fordi forsyning av felles eID vil føre til at brukere ikke må forholde seg til flere ulike eID løsninger fra offentlige virksomheter), vil etablering av felles eID for innbyggere (henholdsvis på nivå 3 og 4) og virksomheter medføre besparelser for alle de offentlige virksomhetene som i dag foretar egne forsyninger av eID løsninger (f.eks NAV, SKD, Lånekassen, Altinn samt enkelte kommuner), ettersom disse løsningene kan fases ut.

Offentlige virksomheter som per i dag ikke har utviklet egne eID løsninger mot innbyggere og virksomheter, vil ikke ha behov for å etablere egne løsninger for dette. Ressursbruk for de enkelte offentlige virksomheter kan isteden konsentreres om utvikling av nye elektroniske tjenester mot publikum. Dette vil igjen gi gevinster både for sluttbrukere og for offentlig sektor, som i større grad vil få publikum til å selvetjene seg, og derved frigjøre ressurser til viktige utviklingsoppgaver og til økt kvalitet i tjenesteytingen samlet sett.

Det er i dag utviklet enkelte løsninger som gjør bruk av eID på nivå 4, eksempelvis Lånekassen og NAV/helse (jfr kap 3.3). Disse løsningene fungerer teknisk sett bra, men tjenestene sliter med ”underforbruk” fordi utbredelsen av godkjent eID blant aktuelle målgrupper (studenter og leger) er for liten. Dette vil kunne avhjelpes ved en offentlig distribuert eID.

Felles strategi for forsyning av eID vil gi gevinster i form av økt bruk av eksisterende elektroniske tjenester og derved økt potensial for å hente ut gevinster av investeringer i disse tjenestene. I tillegg vil man ved felles forsyning av eID gi incentiver for utvikling av nye tjenester, som vil sikre merbruk/gjenbruk av eID.

NAV arbeider med å sikre at en størst mulig andel benytter de elektroniske tjenester som tilbys. Dette er en forutsetning for organisering av de framtidige pensjonsoppgavene i etaten. Dersom det ikke etableres sentrale felles løsninger som dekker behovet, må etaten gjennom pensjonsprosjektet vurdere utvikling av alternative og/eller supplerende løsninger i samforståelse med de departementer som følger opp arbeidet med realiseringen av reformen. Behovet retter seg først og fremst mot forsyning av eID på sikkerhetsnivå 4 til innbyggerne.

I forbindelse med utvikling av Altinn-løsningen har man også behov for avklaring av felles løsninger for samtrafikknav og eID forsyning. Planene til begge disse store arbeidene viser at det er behov for raske avklaringer. Ettersom det ellers kan oppstå behov for egen anskaffelse og/eller utvikling av løsninger, noe som vil medføre ressursmessige konsekvenser knyttet til økonomi, tid og personell.

Videre er det anbefalte *tidsløpet* satt ut fra behovsvurdering for de store aktørene, men også tilbakemelding fra andre (b.la. kommunale) virksomheter. En forskyving av tidsplanen vil få samfunnsøkonomiske konsekvenser ettersom det da vil bli brukt ressurser på realisering av virksomhetsinterne løsninger. Konsekvensen for sluttbruker ved å la være å ta et samordningsgrep vil være at offentlig sektor fortsatt vil fremstå med tilbud av ulike eID løsninger som man må forholde seg til.

8.1 Konsekvenser av forsyningsstrategier for innbyggere – eID på sikkerhetsnivå 3

Den anbefalte løsningen baserer seg på å utnytte eksisterende løsning i Skatteetaten, med tanke på gjenbruk av etatens utstedelse og distribusjon av PIN koder. Det ble etablert en løsning for MinSide som baserer seg på Skatteetatens skattePIN. En vurdering av eksisterende løsning, med tanke på hva som kan gjenbrukes og hva som eventuelt må lages nytt må foretas. Den økonomiske og administrative vurderingen baserer seg på erfaringer fra MinSide løsningen, og grove estimater.

Vurderingen tar utgangspunkt i totalkostnader etablering og forvaltning av en fellesløsning vil påføre SKD, i forhold til eksisterende løsning som allerede er etablert og som i dag distribueres av SKD til store deler av befolkningen (jfr kap 3). Egen distribusjon vil øke kostnadene. På et tidspunkt hvor det er akseptabelt / mulig å sende ut skattekort elektronisk (papirforsendelse utgår), vil dette bildet endres.

Kostnadsnivået vil avhenge av ambisjonsnivået for tilgjengelighet for publikum. Dette vil påvirke etableringskostnadene og driftskostnadene for Prosessering og Kommunikasjon. Videre er estimatet basert på en enkel, i stor grad automatisert sperretjeneste.

1. linje brukerstøtte bør kunne opprettes felles for flere av elementene beskrevet i denne strategien (sperring og bruksproblemer med nivå 3 og 4, virksomhetssertifikater og samtrafikk / tjenesteproblemer). Kostnadene i estimatene under er derfor lagt opp til 2. linje støtte.

Kostnader.
Kostnader ved å etablere en sentral løsning for eID på sikkerhetsnivå 3, basert på Skatteetatens PIN koder, kan deles i to: etablerings- og endringskostnader samt drifts- og vedlikeholdskostnader.

Usikkerheten i estimatene under vil kunne reduseres etter at aktiviteten i pkt 1 under er gjennomført, og deretter etter pkt. 2.

Etablerings- og endringskostnader:

1. Detaljere konsept, avklare gjenbruksmuligheter, sperretjenester og bruk av underleverandører

2. Design og programmering av endringer for å oppnå generell autentisering og kommunikasjon med samtrafikknavet
3. Etableringskostnader Prosessering og Kommunikasjon
4. Programvarekostnader
5. Programmering av utskriftsrutine
6. Trykking
7. Etterbehandling og konvoluttering
8. Utsendelse
9. Administrasjon av etableringsprosessen
10. Brukerstøtte ved utstedelse

SUM Estimat etableringskostnader: **16 MNOK.**

Drifts- og vedlikeholdskostnader:

11 Prosesseringskostnader knyttet til autentisering
12 Kommunikasjonskostnader knyttet til autentisering og samtrafikk
13 Trykking og utsendelse
14 Brukerstøtte
15 Vedlikehold, endringer
16 Feilretting
17 Administrasjon og Informasjon

SUM Estimat årlige drifts- og vedlikeholdskostnader: **14 MNOK.**

Konseptet kan basere seg på å utnytte eksisterende / utsendte PIN koder til å skaffe seg nye, slik at det ikke nødvendigvis må sendes ut nye PIN lister til alle regelmessig. Detaljer i hvordan dette løses avklares i aktivitet 1, og kan påvirke de årlige driftskostnadene. Anslagene er usikre og bør vurderes på nytt i lys av en bredere gjennomgang av mulig gjenbruk av andre eksisterende løsningselementer, jf. for eksempel bruk av NAV sin printfabrikk.

Ordningen vil forventes å kunne gi besparelser, forenkling og / eller sikkerhetsmessig forbedret kvalitet for de offentlige virksomheter som vil benytte en sentralt utstedt ID på sikkerhetsnivå 3. Størrelsesorden på dette er vanskelig å estimere. I en nytte-kostnad analyse her bør det tas med at det finnes gjenbruksmuligheter av flere av ovennevnte funksjoner i eksisterende løsninger.
Det antas at det pr. i dag i stor grad er enklere / rimeligere løsninger med lavere sikkerhetskvalitet, som vil kunne løftes til løsning med større sikkerhet, og at det vil være besparelser for det offentlige og forenkling for brukeren i å ha en felles, statlig, PIN-kode basert løsning istedenfor mange ulike.

8.2 Konsekvenser av forsyningsstrategi for innbyggere - eID på sikkerhetsnivå 4

Arbeidsgruppen som utredet nasjonalt ID kort foreslår å innføre et nasjonalt basis identifikasjonskort og et EU/Schengen ID-kort. For begge kortene anbefales det å utstyre dem med en kontaktchip som kan inneholde en eID/e-signatur.

Økonomiske og administrative konsekvenser for politiet.
Investeringsbehovet for å etablere en ordning med nasjonalt ID-kort antas minimalt, idet det forutsettes at politiet (og utenriksstasjonene) vil benytte samme organisasjon og infrastruktur som benyttes ved passutstedelse. Så fremt utstyr for elektronisk søknadsbehandling og datafangst - såkalte biometrikiosker er på plass - ved politistasjoner og utenriksstasjoner i løpet av 2008, vil dette også kunne benyttes for ID-kort.

Kostnader til anskaffelse/investering/oppstart:

- kravspesifikasjon og anbudsprosess: NOK 4.000.000
- utvikling og tilrettelegging av eID-tjenesten: NOK 5.000.000
- prosjektering og piloter: NOK 5.000.000

Den samlede oppstarts-/investeringskostnaden vil være om lag **NOK 14.000.000**.

Driftskostnader/kortkostnader/forsendelseskostnader som forutsettes dekket av gebyret:

- saksbehandling – kr. 130 pr. kort
- produksjonskostnad: kr. 100 pr. kort forutsatt en produksjon på 150.000 kort
- forsendelse kr. 9,- pr. kort (kan bli lavere ved forsendelse sammen med pass til personer som søker om begge deler samtidig)
- eID kr. 20 pr. kort.

I tillegg vil det påløpe årlige driftskostnader for eID-tjenesten.

- Drift av kataloger og vedlikehold av statusinformasjon: **NOK 4.000.000**.
- Varslingstjeneste og brukerstøtte**: NOK 8.000.000**.

Disse utgiftene vil utgjøre ca. kr. 80 pr. kort under forutsetning av at det produseres 150.000 kort pr. år.

ID-kort-gebyret vil derfor anslagsvis ligge på ca. **NOK 340**,-.

Administrative konsekvenser:
Innføring av nasjonalt ID-kort vil ikke ha vesentlige konsekvenser for politiet fordi ordningen baseres på samme infrastruktur som for pass. Det kan bli behov for økt antall saksbehandlere pga økt total søknadsmengde i forhold til dagens passøknader.

Konsekvenser for andre typer ID-kort: Mange andre kort er utstedt for å dekke spesifikke behov, f.eks førerkort og bankkort. Et nasjonalt ID-kort vil ikke påvirke

utstedelsen av slike kort. ID-kortet vil imidlertid langt på vei erstatte passet i de situasjoner hvor passet i dag benyttes som alminnelig identitetsdokument.

Det vises for øvrig til Justisdepartementets utredning.

Når det gjelder alternativ A2 i gruppens anbefaling, vil det her dreie seg om bl.a. gjenbruk og påbygging av en eksisterende løsning i NAV-etaten. Bestillingsrutine for og produksjon og distribusjon av dagens helsetrygdkort er vel etablert. De nye elementene vil i tilfellet være å inngå avtale med en eID-tilbyder og en chipkort-leverandør som kan innlemmes i dagens verdikjede, og at sluttbruker en gang møter på et NAV-kontor for å legitimere seg, for eksempel ved utlevering av passord. Disse elementene, og den totale kostnaden ved å legge om helsetrygdkortet til å bli et nasjonalt kort med offentlig eID på, er ikke vurdert av arbeidsgruppen.

8.2.1 Økonomiske og administrative konsekvenser ved realisering av alternativ B for eID nivå 4.

Her vil det påløpe kostnader for utlysning og etablering av en rammeavtale, dette anslås til ca **3-5 MNOK**. Driftskostnader er svært vanskelig å estimere, da disse ville være avhengig av den fremforhandlede avtalen med den aktuelle leverandøren. På grunnlag av tidligere erfaringer kan disse kostnader grovt anslås til **15-30 MNOK** pr. år.

8.3 Konsekvenser av forsyningsstrategi - virksomhets-eID

Undersøkelsen ”Ordning for virksomhets- og personsertifikater for ansatte i offentlig sektor - Behovskartlegging høsten 2006”, gir noen svar på hvor stort behovet er for denne type sertifikater i det som man definerer som offentlig sektor. I undersøkelsen ble ca. 1 000 enheter innen kommunesektoren og stats- og trygdeforvaltningen spurt om behov for å ta i bruk virksomhets- og personsertifikater. Dette utgjør ca. 14 % av en bestand på ca. 7 460 juridiske enheter innen offentlig sektor. I sum framkommer det at de spurte enhetene har behov for å ta i bruk ca. 850 virksomhetssertifikater, hovedsakelig i løpet av 2007 og 2008.

I og med at hele offentlig sektor utgjør ca 7 460 juridiske enheter, kan vi stipulere et behov for ca. 6 000 virksomhetssertifikater i løpet av 2007 og 2008.

I tillegg er det, innen offentlig sektor, knyttet ca. 35 400 bedriftsenheter til de juridiske enhetene. I kommunesektoren etterspørres det muligheter for å sikre den elektroniske kommunikasjonen mellom enhetene enklere og rimeligere enn ved hjelp av VPN (Virtual Private Network) tilknytning. Dette viser at det er et behov for virksomhetssertifikater også på bedriftsnivået.

Gruppen har på grunnlag av økonomiske vurderinger og hensynet til effektiv utnyttelse av infrastruktur kommet frem til, at det er hensiktsmessig at ordningen for virksomhetssertifikater som etableres i Brønnøysund også tilbyr sertifikater overfor

private virksomheter. Dette vil gi økonomiske synergieffekter, i tillegg vil etablering av denne ordningen være positivt for konkurransen i markedet.

8.3.1 Kostnader

En ordning for virksomhetssertifikater vil forutsette etableringskostnader[15] i størrelsesorden **12.840.000 NOK**. fordelt over to år, med størst del første året. I disse tallene ligger alle eksterne kostnader knyttet til forstudie, forberedelse, gjennomføring og evaluering av en slik løsning. I tillegg kan komme interne personalkostnader.

Drifts- og videreutviklingskostnader er vanskelig å anslå. Disse vil avhenge sterkt av i hvor stor grad tjenester kjøpes eksternt. Disse kostnadene er estimert til **10.000.000 NOK** pr år.

Med produksjonssetting medio i år 2 vil man måtte ut med drifts- og videreutviklingskostnader f.o.m. andre halvdel av år 2. Ut fra estimatene vil dette beløpe seg til **5.000.000 NOK**. Det forventes at disse utgiftene vil dekkes i form av sentrale bevilgninger. Tilsvarende kostnadsdekning må forventes for år 3.

Fra år 4 vil behovet for sentrale bevilgninger avta.. Eksempelvis vil en utstedelse av 4.000 virksomhetssertifikater á kr. 2.000 gi en inntekt på kr. 8.000.000. Nødvendig bevilgning til drifts- og videreutviklingskostnader vil da være kr. 2 000 000, for å dekke det totale behovet på kr.10.000.000.

8.3.2 Inntekter

Med utgangspunkt i gratis bruk av virksomhetssertifikater (ingen transaksjonsprisning) og pris for anskaffelse og oppgradering av sertifikater, antas det at ordningen vil være selvfinansiert fra og med år 5 (inntekter fra utstedelse og oppgradering av sertifikater dekker drifts- og videreutviklingskostnader).

På sikt er det et mål at forvaltning og drift knyttet til løsning for virksomhetssertifikater finansieres gjennom kostnadsbasert prising av sertifikater (utstedelse og oppgradering av sertifikater) tilsvarende passutstedelsen. Det antas at selvfinansiert drift er realistisk etter en 3-5 års oppstartsperiode. Dette er forsøkt illustrert i tabellen nedenfor.

År	Etableringskostnader	Bevilgning til drifts- og videreutviklingskostnader	Inntekter fra utstedelse av serftifkater	Totale kostnader
1	7 550 000			7 550 000
2	5 290 000	5 000 000	usikker	10 290 000
3		10 000 000	usikker	10 000 000
4		2 000 000	8 000 000	10 000 000
5			10 000 000	10 000 000

[15] Etableringskostnadene vil bestå av elementene: 1) maskin- og programvare, 2) infrastruktur, 3) Informasjon, markedsføring, konsulentbistand

8.4 Konsekvenser – etablering av et offentlig samtrafikknav

Nedenstående beskrivelse er en oppsummering hentet fra en forenklet samfunnsøkonomisk analyse gjennomført av SSØ.[16]

Oppsummering av virkninger og risiko ved modellene[1)]. *Sammenliknet med basisalternativet*

VIRKNINGER	Modell 1. Krav-spesifikasjon	Modell 2. Rammeavtale	Modell 3. Offentlig samtrafikknav
Nyttevirkninger			
• Uttak av stordriftsfordeler			
o Investering/drift	+	++	++
o Kravspesifikasjon	+	+	+
• Flere elektroniske tjenester til innbyggerne	0	0/+	+
• Økt kontroll	0	0/+	+
• Økt sikkerhet	0/+	0/+	0/+
• Økt tillit	0/+	0/+	+
• Bedre og mer effektiv brukerstøtte	0	0/+	0/+
Kostnadsvirkninger			
• Redusert konkurranse			
o Markedet for samtrafikkleverandører	0	- / --	--
o Markedet for e-ID-leverandører	0	-	0
• Redusert fleksibilitet	0/-	-	-
• Redusert innovasjon	0	0/-	0/-
Risiko	- Dyrere løsning	- Velge gal teknologi - Lavere tillit	- Velge gal teknologi - For lav bestiller-kompetanse

[1)] {----} til {++++} indikerer en rangering av effektene, der {++++} betyr at dette tiltaket har størst positiv effekt, mens {----} betyr at dette tiltaket har størst negativ effekt. ” 0 ” betyr at tiltaket har null virkning (tolkning: minus betyr reduksjon i nytte og/eller økning i kostnader).

Tabell 1: Oppsummering av virkninger og risiko ved ulike modeller for samtrafikknav

Som det fremgår av tabellen vil virkningene gjennomgående trekke i samme retning for alle de tre modellene, sammenliknet med basisalternativet, men styrken i virkningene kan være forskjellig.

Modell 3 med offentlig samtrafikknav vil trolig kunne gi de største gevinstene i form av uttak av stordriftsfordeler (som reduserte utgifter til investering og drift). Alle modellene vil gi gevinster i form av reduserte utgifter til utarbeidelse av krav-spesifikasjon. Et enkelt regneeksempel indikerer at denne gevinsten kan bli i størrelsesorden 200 mill. kroner. Av modellene tror SSØ også at modell 3 har de største gevinstene knyttet til økt kontroll, sikkerhet og tillit sammenliknet med basisalternativet.

[16] Senter for statlig økonomistyring. Analysen foreligger i sin helhet i notatet ”Samfunnsøkonomisk analyse av samtrafikk for eID i offentlig sektor” datert 20.12.06.

Modell 2 vil etter SSØs mening i stor grad kunne gi mange av de samme nyttevirkningene som modell 3. Nyttevirkningene av modell 1 vil trolig være relativt beskjedne

Tabell 8.4.1 viser samtidig at også kostnadsvirkningene forventes å bli størst i modell 2 og 3. Kostnadsvirkningene vil bl.a. være knyttet til redusert konkurranse i markedet for samtrafikkløsninger og redusert fleksibilitet.

Oppsummeringsmessig kan det på relativt skjønnsmessig basis argumenteres for at alle modellene kan synes å være mer lønnsomme enn basisalternativet slik dette er definert (rådende markedsforhold).

I boks 8.4.1. illustrerer SSØ, med et svært forenklet regneeksempel, at den potensielle gevinsten ved å etablere en felles kravspesifikasjon kan være betydelig. Denne besparelsen vil gjelde i alle de tre modellene – også modell 1 – sammenliknet med basisalternativet.

Boks 8.4.1 Besparelser ved felles kravspesifikasjon – eksempel

Anta at utarbeidelse av en kravspesifikasjon krever følgende ressurser:

- Intern timebruk i etaten: 1 månedsverk, dvs. 165 timer, à 400 kr (inkl. overhead kostnader), 66.000 kroner
- Konsulentbruk: 2 månedsverk, dvs. 330 timer, à 1.200 kr, 400.000 kroner

Anta at man sparer følgende antall kravspesifikasjoner:

- Kommuner: 200
- Statlige virksomheter: 300

Samlet:
(66.000 kr + 400.000 kroner)*500 = 233 mill. kroner

Kostnader
Det offentlige har erfaring fra tidligere etablering av en sikkerhetsportal. Sikkerhetsportalen ble imidlertid etablert som en rammeavtale. Det innebærer at det offentlige ikke selv eide løsningen og derfor heller ikke har fullstendig oversikt over alle kostnader leverandøren hadde i forbindelse med utvikling og drift. Erfaringen gir allikevel en indikasjon på forventede kostnader ved en drifts- og vedlikeholdsavtale der staten eier og forvalter løsningen. Disse estimatene må kvalitetssikres som en del av et forprosjekt som bør gjennomføres i 2007, der blant annet antall eID'er som skal sluses gjennom navet, og valg av forretningsmodell, vil påvirke kostnadsbildet.

Etablering av et samtrafikknav med funksjonalitet for autentisering, signering og videreformidling av identitet estimeres til å innebære en kostnad på ca. kr 20 millioner. Prosjektet forutsettes å kunne starte i begynnelsen av 2008 og løpe til medio 2009. Det er knyttet usikkerhet til realiseringen av et digitalt arkiv, også med hensyn til kostnader. Dette må utredes nærmere av forprosjektet. Etableringskostnadene er fordelt på 2008 og 2009 i tabellen nedenfor.

Ved etablert samtrafikknav medio 2009 forventes det å påløpe kostnader for videreutvikling på ca. kr 5 mill pr år og driftskostnader på ca. kr 5 mill pr år løsningen er i drift. Det er derfor tatt høyde for ½ års videreutvikling og drift av løsningen i 2009 i tabellen nedenfor. Videreutvikling av samtrafikknavet innebærer realisering av flere av de funksjoner et slikt samtrafikknav kan dekke slik det er definert i denne strategien. Videreutvikling innebærer også generell teknisk tilpasning til den teknologiske utviklingen.

Den enkelte offentlige virksomhet dekker sine egne tilknytnings- og integreringskostnader. Disse kostnadene er ikke tatt med i analysen.

Tabellen nedenfor viser estimat for kostnader i forbindelse med etablering, drift og videreutvikling av et samtrafikknav:

ÅR	Etablering (mill. NOK)	Videreutvikling (mill. NOK)	Drift (mill. NOK)	Sum (mill. NOK)
2008	13		0	**13**
2009	7	2,5 (½ år)	2,5 (½ år)	**12**
2010		5	5	**10**
Etterfølgende år		5	5	**10**

Vedlegg 1 Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor.

1. Innledning

1.1 Bakgrunn

Offentlig sektor har en strategi om å tilrettelegge for gode elektroniske tjenester til brukere (innbyggere og næringsliv), samt tilrettelegge for god elektronisk samhandling mellom offentlige virksomheter.

Forskrift for elektronisk kommunikasjon med og i forvaltningen[17] krever at en offentlig virksomhet som velger å kommunisere elektronisk, skal tilrettelegge sin kommunikasjon på en måte som ivaretar nødvendig bekreftelse av partenes identitet eller fullmakter (autentisering), at data ikke utilsiktet eller urettmessig endres (integritet), beskyttelse av informasjon mot innsyn fra uvedkommende (konfidensialitet), og at det er mulig å dokumentere henvendelser og aktiviteter og hvem som har sendt eller utført dem (ikke-benekting), i henhold til den offentlige virksomhetens sikkerhetsstrategi. Virksomheten skal likevel ikke kreve betraktelig høyere sikkerhet enn det som er nødvendig for den type informasjon som kommuniseres eller den type handling som tilbys utført elektronisk.

Økt elektronisk samhandling fører med seg et behov for å koordinere bruk av metoder for autentisering og uavviselighet på tvers av offentlig sektor. Felles sikkerhetsnivåer for dette i offentlig sektor vil gi mulighet for gjenbruk av sikkerhetsløsninger eller bruk av felles sikkerhetsløsninger, i kommunikasjon med brukere av offentlige elektroniske tjenester. Gjenbruk av løsninger gir økt brukervennlighet for brukerne og fører til besparelser i de offentlige virksomhetene. Felles sikkerhetsnivåer vil også gi økt trygghet for at samhandlende offentlige virksomheter sikrer utvekslet informasjon på en tilstrekkelig måte.

Dette dokumentet er ikke et komplett sikkerhetsrammeverk, men et rammeverk for sikkerhetstjenestene autentisering og uavviselighet. Autentisering er å verifisere påstått identitet. Uavviselighet er å bekrefte at en handling eller et informasjonselement er uendret (informasjonsintegritet) og at det kan knyttes til en bestemt identitet. Uavviselighet er i mange sammenhenger også omtalt som ikke-benekting. Rammeverket gjelder for autentisering og uavviselighet ved behandling av informasjon som er åpen, konfidensiell, taushetsbelagt eller personsensitiv. Det er derimot ikke gjort vurderinger opp i mot informasjon som har krav til konfidensialitet som følger av sikkerhetsloven og beskyttelsesinstruksen.

Det er viktig å være klar over at autentiserings-/ uavviselighetsmekanismen kun er en del av det som utgjør sikkerhetsnivået til en offentlig elektronisk tjeneste. I vurderingen av en tjenestes totale sikkerhet må mange flere elementer vurderes.

[17] Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften), Fornyings- og administrasjonsdepartementet, 2004-06-25

Autorisasjon vil si at en identitet har fått godkjent tilgang til ressurser eller å utføre en viss type handlinger i et system. Autorisasjon bygger på autentisering, fordi en identitet må verifiseres før tilgang kan gis. Denne sikkerhetstjenesten er ikke omfattet av dette sikkerhetsrammeverket.

Konfidensialitet er egenskapen at informasjon kun kan leses av autoriserte mottakere. Denne egenskapen kan blant annet realiseres ved å kryptere (kode) informasjon på en måte som gjør at kun autoriserte kan dekryptere og lese den. Konfidensialitet bygger på autentisering, fordi en identitet må verifiseres før tilgang til konfidensialitetsbeskyttet informasjon kan gis. Dette sikkerhetsrammeverket omfatter ikke konfidensialitet. Noen tekniske løsninger som benyttes for autentisering kan også benyttes for kryptering, dette gjelder for eksempel løsninger iht. Kravspesifikasjon for PKI i offentlig sektor.

Dette rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor er utformet for å være teknologinøytralt. Antall risiko- og sikkerhetsnivåer og posisjonering av disse er gjort etter faglig vurdering av arbeidsgruppen nedsatt for utforming av dette rammeverket i henhold til formulerte målsettinger. Rammeverket anbefaler felles nivåer for risiko og vurderer hvilke sikkerhetsnivåer som egner seg for de forskjellige risikonivåene.

1.2 Målsetning

Hovedmålsetningen med dette rammeverket, er å legge til rette for felles løsninger og gjenbruk av løsninger, for autentisering og uavviselighet på tvers av offentlig sektor. Offentlige virksomheter gjennomfører risiko- og sårbarhetsanalyser ved etablering av nye elektroniske tjenester og ved revidering av eksisterende tjenester. I den sammenheng skal virksomhetene kunne vurdere risikonivået i en elektronisk tjeneste opp i mot felles definerte risikonivåer i dette rammeverket. Virksomheten kan så finne anbefalte sikkerhetsnivå, og implementere en autentiserings-/ uavviselighetsløsning iht. anbefalt nivå.

Det er viktig å merke seg at sikkerhetsrammeverket er veiledende. Hver offentlig virksomhet er selv ansvarlig for de vurderinger og valg som gjøres i forhold til å sikre egne elektroniske tjenester/ elektronisk kommunikasjon, og eventuelle følger av disse valgene.

I tillegg skal dette sikkerhetsrammeverket bidra til:

- Legge til rette for felles løsninger og gjenbruk av løsninger for autentisering og uavviselighet
- å gjøre det lettere for offentlige virksomheter å vurdere hvilket sikkerhetsnivå som egner seg for forskjellig type kommunikasjon
- å gjøre det enklere for offentlige virksomheter å velge løsninger for autentisering og uavviselighet
- å muliggjøre gjenbruk av løsninger for autentisering og/ eller uavviselighet på tvers av offentlig sektor, for effektivisering internt og for økt brukervennlighet mot brukere av offentlige tjenester

- å understøtte Kravspesifikasjon for PKI i offentlig sektor, samt godkjenningsordningen i regi av Post- og teletilsynet der leverandører kan selvdeklarere egne produkter og tjenester som tilfredsstiller kravspesifikasjonen.

1.3 Målgruppe for rammeverket

Sikkerhetsrammeverket er skrevet for de som skal arbeide med vurdering av risiko, valg av sikkerhetsnivå og valg av tekniske løsninger for sikring av autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. Dette gjelder offentlige tjenestemenn som jobber med å vurdere, anbefale, beslutte og implementere slike løsninger.

1.4 Rammeverkets oppbygning

Dokumentet er bygget opp ved at kapittel 2 gir en innføring i begrepene autentisering og uavviselighet. Kapittel 3 forklarer hva dette rammeverket legger i begrepet risikonivå, og definerer fire felles risikonivåer for offentlig sektor. Kapittel 4 forklarer hva dette rammeverket legger i begrepet sikkerhetsnivå, og definerer fire sikkerhetsnivåer, og gir eksempler på tekniske løsninger som tilfredsstiller de forskjellige nivåene. Kapittel 5 anbefaler hvilke sikkerhetsnivå som egner seg for de forskjellige risikonivåene.

2. Utdypende om autentisering og uavviselighet

2.1 Autentisering

Autentisering er å verifisere en påstått identitet, og dette kan to kommunikasjonsparter velge å gjøre ensidig eller tosidig. Partene som skal autentisere hverandre over nettet kan være av to forskjellige typer:

- En fysisk person (et anskuelig menneske underlagt fysiske lover) på en klient, for eksempel en PC, mobiltelefon eller annen type kommunikasjonsterminal.
- En juridisk person (et selvstendig rettsobjekt som for eksempel stater, kommuner, aksjeselskap, stiftelse eller forening) på en tjener, for eksempel en web-server eller et system for meldingshåndtering.

Begge parter må ha maskinvare og programvare med støtte for felles autentiseringsprotokoller og nødvendige brukerdialog. Partenes utstyr må være sikret mot uautorisert tilgang og bruk.

De som skal autentisere seg må også inneha noe som kan bekrefte deres identitet. Dette kalles autentiseringsfaktorer. En bruker kan ha en eller flere av disse avhengig av sikkerheten i løsningen. Det finnes tre forskjellige typer autentiseringsfaktorer:

- Noe personen **vet**; for eksempel et passord
- Noe personen **har**; for eksempel en passordkalkulator
- Noe personen **er**; for eksempel et fingeravtrykk

Autentiseringsfaktoren(e) må på et tidspunkt bli knyttet til en identitet. Denne administrasjonen av brukere kan gjøres av en tredjepart eller av en tjenesteyter selv. Brukeradministrasjonen går ut på å identifisere brukere ved tildeling av brukernavn, se til at riktig bruker får/ har riktig autentiseringsfaktorer og at status informasjon om brukere oppdateres og tilgjengeliggjøres.

De delene som ikke regnes som en del av autentiseringsløsningen er blant annet:

- Skallsikringen rundt klient eller tjener.
- Sikringen av autorisasjon og tilgangskontroll til informasjon og ressurser.

2.2 Uavviselighet

Uavviselighet er å bekrefte at en handling eller et informasjonselement er uendret (informasjonsintegritet) og at det kan knyttes til en bestemt identitet. Uavviselighet er i mange sammenhenger også omtalt som ikke-benekting. En løsning for uavviselighet er en løsning som gjør det mulig for en part å innhente tilstrekkelig dokumentasjon for at en annen part ikke kan benekte å ha gjennomført en handling eller valgt å bekrefte/ stå bak et informasjonselement.
En løsning for uavviselighet er bygget opp på samme måte som løsninger for autentisering som beskrevet over. Forskjellen i denne sammenheng, er at brukeren skal være i stand til ikke bare å bekrefte hvem man er over nettet, men også å legge igjen dokumentasjon som entydig knytter personen til en handling eller et uendret informasjonselement.

3. Risikonivåer

Offentlige virksomheter gjennomfører risiko- og sårbarhetsanalyser ved etablering av nye elektroniske tjenester og ved revidering av eksisterende tjenester. Virksomheten må da vurdere hvilke konsekvenser forskjellige uheldige hendelser kan få, for brukere av tjenesten, den offentlig virksomheten selv og/ eller offentlig sektor som helhet. Deretter må virksomheten vurdere sannsynligheten for at identifiserte konsekvenser vil inntreffe. Produktet av identifisert konsekvens og sannsynligheten for at den inntreffer blir i dette dokumentet beskrevet som et risikonivå.

Her defineres fire felles risikonivåer for offentlig sektor. Offentlige virksomheter skal på bakgrunn av risiko- og sårbarhetsanalyser kunne plassere egne tjenester iht. disse felles risikonivåene. Dette skal igjen gi grunnlag for å finne riktig sikkerhetsnivå i neste kapittel, og på bakgrunn av sikkerhetsbehov og funksjonelle behov kunne velge en egnet løsning for autentisering og/ eller uavviselighet. En løsning som gjør det såpass vanskelig å misbruke tjenesten at den resterende risikoen skal kunne anses som forholdsmessig akseptabel.
Felles risikonivåer er dermed første steget for legge til rette for felles løsninger og gjenbruk av løsninger for autentisering og uavviselighet.

3.1 Sannsynlighet

Sannsynlighet beskrives i dette rammeverket ved hjelp av følgende parametere:

- Frekvens — Hvor ofte en sårbarhet historisk blir forsøkt utnyttet
- Kapasitet — En uautoriserts evne til å utnytte en sårbarhet. Hvor vanskelig det er å utnytte sårbarheten og hvor lett det er å skalere et angrep.
- Motivasjon/Vinning — Hvor interessant det er å utnytte en sårbarhet

I dette rammeverket vurderes sannsynlighet kun på bakgrunn av parametrene frekvens(historisk) og motivasjon. Dette fordi en uautoriserts kapasitet til å utnytte autentiserings- og/ eller uavviselighetsløsningen, først kan vurderes etter den er valgt, og denne vurderingen av risiko gjøres jo nettopp for å velge en slik løsning. (Det anbefales

imidlertid å gjennomføre en full risikovurdering etter valg av løsning for autentisering og/ eller uavviselighet, der sannsynlighetsberegningen også kan inkludere kapasitet. Da kan virksomheten vurdere om den reelle resterende risiko er blitt såpass liten at den kan anses som forholdsmessig akseptabel for virksomheten.)

På bakgrunn av frekvens og motivasjon vurderes sannsynligheten for å være til stede, eller ikke. Enten er sannsynligheten for at en konsekvens inntreffer tilstrekkelig stor - og konsekvensen inkluderes i vurdering av risikonivå, eller den vurderes som så usannsynlig at konsekvensen ekskluderes. (Sannsynligheten er lik 1 eller 0)

Motivasjonen for å utnytte sårbarheter i en løsning for autentisering og/ eller uavviselighet som dekker flere elektroniske tjenester er større, fordi det er mer innhold og større funksjonalitet som kan utnyttes. Det kan med andre ord fremprovoseres større konsekvenser. Der konsekvensene ved utnyttelse er store vil motivasjonen også være stor. På et moderat nivå vil konsekvensene være av en slik art at selv om man samler mye innhold og stor funksjonalitet, vil motivasjonen som regel fortsatt være begrenset.

3.2 Konsekvens

Konsekvens er resultatet av at en sårbarhet blir utnyttet eller en uheldig hendelse inntreffer, uavhengig av sannsynligheten for at dette skal skje (iboende risiko). Med andre ord “worst case scenario”. Det er viktig at den offentlige virksomheten i sin risikovurdering av en tjeneste, vurderer konsekvenser for alle parter, brukere av tjenesten (privatpersoner og næringsliv), den offentlige virksomheten selv og offentlig sektor som helhet.

Følgende sett med konsekvenser er benyttet til å definere risikonivåene i dette rammeverket:

- Konsekvenser for liv eller helse
- Økonomisk tap/ merarbeid/ økte kostnader
- Tap av renommé (anseelse, tillit og integritet)
- Hindring i straffeforfølgelse
- Uaktsomt bidrag til lovbrudd
- Bryderi/ulempe

Det er viktig å presisere at alle disse typer konsekvenser kan gjelde for alle målgrupper – sluttbrukere (personer, virksomheter), offentlige virksomheter og offentlig sektor som helhet. Den offentlige virksomheten som vurderer konsekvenser, må derfor vurdere alle disse konsekvenstypene for hver part.

Det er viktig å huske på de krav sentrale lover og spesiallovgivningen setter for den virksomheten som bedrives. Disse kravene har stor betydning i forhold til vurdering av konsekvenser.
Listen over er ikke uttømmende, så det kan skje konsekvenser som ikke påvirker de felles definerte risikonivå.

3.3 Risikonivåer

Risikonivåene i rammeverket beskrives i form av konsekvenser. Dette kan gjøres fordi sannsynligheten vurderes binært (1 eller 0). Risikoen som er produktet av sannsynlighet og konsekvens er dermed definert av konsekvenser som er inkludert eller ekskludert avhengig av sannsynligheten.

Det er definert følgende fire risikonivåer i tabellen under. Teksten i tabellen beskriver høyest risiko godkjent på et gitt risikonivå for den type konsekvens.

	Risikonivå 1 ingen	**Risikonivå 2 liten**	**Risikonivå 3 moderat**	**Risikonivå 4 stor**
Konsekvenser for liv eller helse	Det kan ikke forekomme fare for tap av liv og/ eller helseskader	Det kan forekomme mindre helseskader	Det kan forekomme mindre helseskader	Det kan forekomme tap av liv og/ eller store helseskader
Økonomisk tap/ merarbeid/ økte kostnader	Intet økonomiske tap/ merarbeid/ økte kostnader	Det kan føre til et mindre økonomisk tap/ merarbeid/ økte kostnader	Brudd kan føre til moderat økonomisk tap/ merarbeid/ økte kostnader	Brudd kan medføre store økonomiske tap/ merarbeid/ økte kostnader
Tap av renommé (anseelse, tillit og integritet)	Ingen skade på renommé	Eventuelle skader på renommé anses bagatellmessige	Renommé kan bli noe svekket i et kortere tidsrom	Renommé kan bli svekket i et lengre tidsrom, eventuelt varig
Hindring i straffe-forfølgelse	Ingen bidrag til hindring av straffe-forfølgning	Minimalt bidrag til hindring av straffe-forfølgning	Moderat bidrag til hindring av straffe-forfølgning	Det kan forekomme hindringer i straffe-forfølgning
Uaktsomt bidrag til lovbrudd	Det kan ikke forekomme uaktsom bistand til lovbrudd	Det kan ikke forekomme uaktsom bistand til lovbrudd	Det kan ikke forekomme uaktsom bistand til lovbrudd	Brudd kan bidra til uaktsom bistand til lovbrudd
Bryderi/ ulempe	Ingen ulempe eller bryderi	Det kan forekomme noe ulempe eller bryderi	Ikke relevant	Ikke relevant

”Risikonivå 1 – ingen”, er beregnet på åpen informasjon. Funksjoner og informasjonsutveksling i tilknytning til informasjon som er konfidensiell, taushetsbelagt eller personsensitiv, må legges på de andre risikonivåene iht. hvilke sannsynlige konsekvenser som kan oppstå hvis uheldige hendelser finner sted.

Nedenfor er det eksemplifisert uheldige hendelser som kan lede til konsekvenser i tabellen over:

1. Uautorisert endring av pasientdata.
2. En persons sykdomsdiagnose blir kjent for uvedkommende
3. Omsetningstall lekker ut før kvartalsrapportering
4. Feil i utbetalingsgrunnlag av trygd

5. Feil i utbetalingsgrunnlag for MVA
6. Uautorisert endring for å påvirke offentlige utbetalinger
7. Offentlig etat taper renommé etter oppslag i media om datainnbrudd
8. Bevismateriell blir ødelagt eller kommer på avveie, på grunn av operatørfeil.
9. Uautorisert endring av personadresse som ledd i identitetstyveri.

4. Sikkerhetsnivåer for autentisering og uavviselighet

Sikkerhet i løsninger for autentisering og uavviselighet kan beskrives ved hjelp av forskjellige sikkerhetsparametere. En sikkerhetsparameter er en faktor som påvirker sikkerhetsnivået i løsningen hvis den endres, som for eksempel ”Utlevering til bruker”. For en passordløsning vil utlevering være hvordan passord deles ut til brukeren. Er passordene delt ut til bruker på bakgrunn av fysisk legitimering, er det vanskelig å skaffe seg et passord i andres navn. Deles passordene ut over Internett på bakgrunn av påstått identitet er det lett å skaffe et passord i andres navn. Dette viser at to forskjellige krav til samme sikkerhetsparameter endrer graden av hvor vanskelig det er å kompromittere løsningen.

Sikkerhetsnivåene i dette rammeverket er definert på bakgrunn av følgende sett av sikkerhetsparametere:

- Krav til autentiseringsfaktor(er)
  Beskriver antall autentiseringsfaktorer og deres egenskaper. For eksempel om autentiseringsfaktoren er statisk eller dynamisk. Med statisk menes at dokumentasjonen som presenteres for andre som skal verifisere påstått identitet, ikke endres fra gang til gang. Et eksempel på dette er fast passord eller biometriske data. Med dynamisk menes at dokumentasjonen som presenteres for andre som skal verifisere påstått identitet, endres fra gang til gang. Eksempler på slike løsninger er tidsbaserte passordkalkulatorer, som gir nytt passord avhengig av tid, og løsninger basert på PKI, hvor det ved hver autentisering genereres en ny, tilfeldig datastreng som signeres digitalt.
- Utlevering til bruker
  Beskriver hvordan man sikrer knytningen mellom autentiseringsfaktorer og brukeridentiteter. For eksempel om brukeren har måttet møte opp fysisk og legitimere seg selv, eller om brukeren har fått noe tilsendt folkeregistrert adresse. I dette rammeverket er folkeregistrert adresse definert til å være en av adressene registrert i folkeregisteret (Folkeregisteret har definert tre typer adresser i sitt register).
- Sikring av autentiseringsfaktorer ved lagring
  Beskriver hvordan autentiseringsfaktoren er lagret lokalt, og hvordan den er fysisk og logisk sikret. Et eksempel er forhåndsdefinerte passordlister. Kommer disse på et åpent ark, er de kopierbare. Er passordene beskyttet som skrapelodd, er de ikke kopierbare.
- Krav til uavviselighet
  Beskriver i hvilken grad det i ettertid er mulig å dokumentere at en bruker står bak et informasjonselement eller har utført en handling.

- Krav til offentlig godkjenning
  Innebærer at det finnes en offentlig kravspesifikasjon (forvaltningsstandard) for den type løsninger, og at løsningen er deklarert ved en offentlig organisert ordning.

Overforstående sikkerhetsparametere er definert for å være teknologinøytrale. De forskjellige sikkerhetsparametrene er vektet likt på den måten at en løsning som skal tilfredsstille et sikkerhetsnivå, skal oppfylle kravene satt for alle sikkerhetsparametrene på det nivået.

Det settet med sikkerhetsparametere som er benyttet i dette rammeverket for å skille mellom sikkerhetsnivå er ikke uttømmende. Det finnes derfor autentiserings- og uavviselighetsløsninger som har andre sikkerhetsparametere som kan ha forskjellig nivå, og som dermed kan oppfattes sikkerhetsmessig forskjellig.

Når en offentlig virksomhet skal velge sikkerhetsnivå på bakgrunn av sitt risikonivå, er det viktig å være oppmerksom på at sentrale systemsjekker i noen tilfeller vil kunne begrense sannsynligheten for at en konsekvens inntreffer og dermed senke kravet til sikkerhetsnivå. For eksempel kan en sentral sjekk om at utbetaling går til en konto i brukers navn senke kravet til utlevering.

Det er definert fire sikkerhetsnivåer som vist i tabellen under.

Nivå	Krav til Autentiserings faktor(er)	Utlevering til bruker		Sikring av autentiserings faktorer ved lagring	Krav til offentlig godkjenning	Krav til uavviselighet
		Fysiske personer	*Juridiske personer*			
1	Ingen krav	Ingen krav	Ingen krav	Ingen krav	Ingen krav	Ingen krav
2	Enfaktor	Post til folkeregistrert adresse	Post til enhetsregisterets registrerte adresse. Navnet til den fysiske personen som kan tegne for den juridiske personen, skal stå først på forsendelsen. Alternativt kan det sendes til den som tegners folkeregistrerte adresse.	Både statiske og dynamiske kan være kopierbare	Ingen krav	Det skal foreligge rutiner og logger, som gjør at det er rimelig sikkert at kommunikasjonsparten står bak en handling eller et informasjonselement.
3	Tofaktor, hvorav en er dynamisk	Samme krav som i 2, med tilleggskrav om en eller annen form for sikring av at rette vedkommende tar dette i bruk.	Samme krav som i 2, med tilleggskrav om en eller annen form for sikring av at rette vedkommende tar dette i bruk.	Dynamiske kan være kopierbare Statiske kan ikke være kopierbare	Ingen krav	Det skal foreligge rutiner og logger, som gjør at det er rimelig sikkert at kommunikasjonsparten står bak en handling eller et informasjonselement.
4	Tofaktor, hvorav en er dynamisk	Kravene til registrering og utleveringsprosedyrer er tilsvarende Kravspesifikasjon for PKI[18], Person Høyt. Personlig oppmøte med legitimering, minst en gang.	For juridiske personer skal den fysiske personen som tegner den juridiske, enten møte opp personlig, eller gi fullmakt til en annen som kan møte personlig på personens vegne. Det skal fremlegges legitimasjon for begge, samt sjekkes mot enhetsregisteret. Krav tilsvarende Kravspesifikasjon for PKI, nivå Virksomhet.	Ikke-kopierbare	Løsningen skal være deklarert i henhold til offentlige krav.	En kommunikasjonspart skal kunne verifisere at den andre part står bak en handling eller et informasjonselement, den skal ikke selv kunne produsere eller endre på et slikt bevis i etterkant.

Praktiske eksempler på løsninger som tilfredsstiller de forskjellige sikkerhetsnivåene

Her gis det eksempler på hva slags tekniske løsninger som vil tilfredsstille de forskjellige sikkerhetsnivåene. Alle løsninger på et høyere nivå vil kunne benyttes på et lavere sikkerhetsnivå.

Sikkerhetsnivå 1

Dette sikkerhetsnivået gir liten eller ingen sikkerhet. Her fungerer helt åpne løsninger. Det finnes også noen sikkerhetsløsninger som vil havne i denne kategorien fordi de ikke tilfredsstiller kravene til sikkerhetsnivå 2. Dette gjelder løsninger som for eksempel:

- selvvalgt passord og brukernavn over nettet
- identifisering med fødselsnummer

[18] Kravspesifikasjon for PKI i offentlig sektor, Moderniseringsdepartementet, januar 2005, og til enhver tid gjeldende versjon av denne.

Sikkerhetsnivå 2
På dette sikkerhetsnivået fungerer alle løsninger som tilfredsstiller kravene til sikkerhetsnivå 2, men som ikke tilfredsstiller kravene til sikkerhetsnivå 3. Eksempler på sikkerhetsløsninger som havner i denne kategorien er:

- Fast passord, sendt ut i brev til folkeregistrert adresse
- Passordkalkulatorer uten passordbeskyttelse, minimum distribuert gjennom folkeregistrert adresse.
- Engangspassordlister distribuert til folkeregistrert adresse.

Sikkerhetsnivå 3
På dette sikkerhetsnivået fungerer alle løsninger som tilfredsstiller kravene til sikkerhetsnivå 3, men som ikke tilfredsstiller kravene til sikkerhetsnivå 4. Eksempler på sikkerhetsløsninger som havner i denne kategorien er:

- Passordkalkulatorer beskyttet med PIN-kode, der første PIN-kode er sendt i separat forsendelse
- Engangspassord på mobiltelefon, der mobiltelefonen er registrert med en egen registreringskode distribuert til folkeregistrert adresse.
- Person Standard iht. Kravspesifikasjon for PKI i offentlig sektor
- Engangspassordlister benyttet sammen med fast passord og brukernavn. Valg av fast passord skal skje på bakgrunn av en engangskode sendt til folkeregistrert adresse (eventuelt første kode på engangspassordlisten)

Sikkerhetsnivå 4
På dette sikkerhetsnivået vil det i forhold til dagens situasjon kun være løsninger basert på PKI som tilfredsstiller kravene. I henhold til gjeldende regelverk må løsningene være selvdeklarert i Post- og teletilsynet i forhold til om de oppfyller krav i Kravspesifikasjon for PKI i offentlig sektor når det gjelder Person Høyt og Virksomhet. Eksempler på teknologier som kommer, men ikke har tilstrekkelig standardiseringsgrad pr. i dag, er:

- En tofaktorløsning, hvor en av faktorene er dynamisk, hvorav en av faktorene eller en registreringsfaktor er personlig utlevert. Det benyttes en tredjepart til å registrere en logg med knytningen mellom handling/ informasjonselement og identitet. Loggen skal lagres med endringsbeskyttelse.
- En tofaktorløsning, hvor en av faktorene er dynamisk, hvorav en av faktorene eller en registreringsfaktor er personlig utlevert. Det benyttes en spesialprogramvare som hindrer brukersted i å generere falsk dokumentasjon over hvem som står bak et informasjonselement/handling og som hindrer operatører å kunne endre logging av informasjonselement/ handlingsbeskrivelse og identitet.

5. Anbefaling om bruk av sikkerhetsnivåer

Hver offentlig virksomhet er selv ansvarlig for å forvalte sine oppgaver på en forsvarlig måte, og er blant annet i forhold til personopplysninger definert som behandlingsansvarlig i personopplysningsloven[19]. Hver offentlig virksomhet må derfor selv vurdere hva som er et akseptabelt risikonivå og hvilke sikkerhetsløsninger som gir forholdsmessig akseptabel sikkerhet for virksomheten.

Dette dokumentets anbefalinger om hvilket sikkerhetsnivå som egner seg for de definerte risikonivåer fritar derfor ikke den offentliges virksomhets krav til selv å vurdere sikkerhetsbehovet i forhold til den konkrete tjenesten som skal tilbys.

Når en offentlig virksomhet skal kommunisere elektronisk må de gjennomføre en Risiko- og sårbarhetsanalyse. På bakgrunn av den analysen kan de vurdere hvilket risikonivå som er tilknyttet den type elektronisk kommunikasjon iht. kapittel 3. Dette rammeverket gir følgende anbefaling om hvilke sikkerhetsnivåer definert i kapittel 4 som egner seg for de forskjellige risikonivåer definert i kapittel 3:

Risikonivå 1 → Sikkerhetsnivå 1
Risikonivå 2 → Sikkerhetsnivå 2
Risikonivå 3 → Sikkerhetsnivå 3
Risikonivå 4 → Sikkerhetsnivå 4

Dette rammeverket er et generisk verktøy for offentlige virksomheter, som kan brukes til å "plassere" tjenester mht. sikkerhetsnivå og påfølgende valg av løsning for autentisering og/eller uavviselighet. Rammeverket kan også brukes til å velge sikkerhetsnivå eller sikkerhetsløsning for offentlige løsninger (portaler) der en autentisering kan gi adgang til flere tjenester. Rammeverket kan også benyttes i forhold til å vurdere gjenbruk av andres sikkerhetsløsninger/ felles sikkerhetsløsninger mot egne tjenester.
Det vil bli utarbeidet en veileder med en mer grundig innføring i risikovurderinger og bruken av dette sikkerhetsrammeverket.

6. Referanser

1. Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften), Fornyings- og administrasjonsdepartementet, 2004-06-25
2. Kravspesifikasjon for PKI i offentlig sektor, Moderniseringsdepartementet, januar 2005
3. NoU 2001:10 Uten Penn og blekk, Arbeids- og administrasjonsdepartementet, mars 2001
4. E-authentication Guidance for Federal Agencies, Office of Management and Budgets, Washington DC 2003 Dec 16
5. Registration and Authentication, e-Government Strategy Framework Policy and Guidelines, September 2002. Office of the e-Envoy, UK
6. Lov om elektronisk signatur (esignaturloven), Nærings- og handelsdepartementet, 2005-06-17
7. Lov om behandling av personopplysninger (personopplysningsloven), Justis- og politidepartementet, 2000-04-14
8. Wikipedia, 2007-01-22
9. www.brreg.no/registrene/enhet/ Brønnøysund, 2007-01-22

[19] Lov om behandling av personopplysninger (personopplysningsloven), Justis- og politidepartementet, 2000-04-14

Bilag 1 til Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor

Dette bilaget har som formål å svare på noen av de spørsmål som kan oppstå i forhold til begreper innen dette fagfeltet i offentlig sektor.

Dette rammeverket for autentisering og uavviselighet er teknologinøytralt og gir anbefalinger på et overordnet nivå. Kravspesifikasjon for PKI i offentlig sektor er en kravspesifikasjon for løsninger basert på en bestemt teknologi, og avgrenser seg ikke til autentisering og uavviselighet, men berører også konfidensialitet.

Løsninger som tilfredstiller nivå Person Standard i Kravspesifikasjon for PKI i offentlig sektor vil også kunne tilfredstille sikkerhetsnivå 3 i rammeverket for autentisering og uavviselighet. Sikkerhetsnivå 3 vil også kunne tilfredstilles gjennom andre teknologiske løsninger, som ikke er iht. kravspesifikasjon for PKI i offentlig sektor.

Løsninger som tilfredstiller nivå Person Høyt og Virksomhet i kravspesifikasjon for offentlig sektor vil kunne tilfredstille sikkerhetsnivå 4 i dette rammeverket for autentisering og uavviselighet. Det er foreløpig ikke avklart hvilke andre teknologier enn PKI som kan anskaffes på sikkerhetsnivå 4, fordi det ikke er etablert felles kravspesifikasjoner og selvdeklareringsløsninger i forhold til andre teknologiske løsninger som kan tilfredstille kravene til sikkerhetsnivå 4.

”Elektronisk signatur” er et vidt begrep som benyttes for alle elektroniske løsninger som knytter en person (fysisk eller juridisk) til et dokument eller en handling. I lov om elektronisk signatur er en elektronisk signatur definert som ”data i elektronisk form som er knyttet til andre elektroniske data og som brukes som autentiseringsmetode”. For å lage en elektronisk signatur kan det for eksempel benyttes teknologiske løsninger basert på passord og brukernavn, passordkalkulatorer, biometri eller PKI. Benyttes løsninger som i seg selv ikke sikrer integritet og uavviselighet, men bare autentisering, kreves det sporing av knytningen mellom autentiseringsdata og handling/ dokument. I tillegg må disse sporene sikres forsvarlig mot endring.
Begrepet ”digital signatur” er vanligvis kun benyttet når man snakker om en elektronisk signatur basert på PKI.

En ”avansert elektronisk signatur” er en elektronisk signatur som:

a) er entydig knyttet til undertegneren,
b) kan identifisere undertegneren,
c) er laget ved hjelp av midler som bare undertegneren har kontroll over, og
d) er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering,

Den vanligste måten å implementere ”avanserte elektroniske signaturer” på er ved å benytte PKI, en teknologi som baserer seg på bruk av sertifikater.Et sertifikat er et form for elektronisk identitetsbevis som kan benyttes til å verifisere/ validere elektroniske signaturer. Sertifikatet knytter innehavers navn/ pseudonym til informasjon om egenskaper ved innehavers elektroniske signatur som gjør det mulig å verifisere den. Sertifikatet skal være signert av utsteder, som bør være en tredjepart som alle stoler på, slik at sertifikatet kan benyttes til å verifisere en elektronisk signatur, selv om man ikke

kjenner den andre part på forhånd. I lov om elektronisk signatur er sertifikat definert som ”en kopling mellom signaturverifikasjonsdata og undertegner som bekrefter undertegners identitet og er signert av sertifikatutsteder”.

Et kvalifisert sertifikat er et sertifikat som er utstedt iht. bestemmelser i Lov om elektronisk signatur.

EU har gitt et direktiv om elektroniske signaturer i 1999. Dette er i Norge implementert i Lov om elektronisk signatur. Forarbeidene og intensjonen for utarbeidelsen av EU-direktivet og påfølgende norsk lovarbeid gjør det klart at direktivets bestemmelser gjelder kun for fysiske personer og ikke for juridiske personer. Sertifikater utstedet til juridiske personer som for eksempel en bedrift, kan derfor ikke ha status som kvalifisert sertifikat (Jfr. Ot. prp. 82 (1999-2000), særlig s. 49). Dette gjelder også for sertifikater på nivå Virksomhet iht. Kravspesifikasjon for PKI i offentlig sektor, selv om det sikkerhetsmessig er satt tilsvarende krav som for kvalifiserte sertifikater på dette nivået.

Lov om elektronisk signatur setter i kapittel 2 krav til ”sikre signaturfremstillingssystemer”, og godkjenning av slike. Det er også laget mer detaljerte internasjonale standarder som tilfredstiller disse kravene. Det har foreløpig ikke vært noen leverandører i det norske markedet, som har tilbudt godkjente signaturfremstillingssystemer, selv om det internasjonalt finnes godkjente løsninger for dette.

En ”kvalifisert elektronisk signatur” er en avansert elektronisk signatur som er basert på et kvalifisert sertifikat og fremstilt ved bruk av et godkjent sikkert signaturfremstillingssystem. Den løsningen som ikke gir kvalifisert signatur, men tilsvarende sikkerhet, er Person Høyt iht Kravspesifikasjon for PKI i offentlig sektor. Dersom leverandøren av Person Høyt- baserte eID også kan levere et teknisk system godkjent iht regelverket som ”sikkert signaturfremstillingssystem” vil en slik løsning kunne brukes til å generere kvalifiserte signaturer.

I Norge er det med hjemmel i Lov om elektronisk signatur etablert en selvdeklarasjonsordning for løsninger som tilfredstiller Kravspesifikasjon for PKI i offentlig sektor på nivå Person Standard, Person Høyt og Virksomhet. Denne selvdeklarasjonsordningen forvaltes av Post- og teletilsynet. Det er imidlertid ikke utpekt noen aktør som kan ivareta rollen som godkjenningsinstans for sikre signaturfremstillingssystemer. Ansvaret for vurdering av samsvar med regelverkets krav ligger derfor i Nærings- og handelsdepartementet, som forvalter av esignaturloven.

Når to parter skal kommunisere elektronisk basert på eID fra to forskjellige utstedere, krever dette samtrafikk. Samtrafikk har flere aspekter, blant annet teknisk, policymessig, forretningsmessig og juridisk. Samtrafikk vil si at man som bruker i forhold til disse aspektene kun trenger å forholde seg til sin utsteder, og det utstyret (programvaren og maskinvaren) man har anskaffet for å benytte sin eID. Er det ikke samtrafikk mellom leverandørene i markedet, kan brukeren velge å benytte et samtrafikknav, som ivaretar disse aspektene på vegne av brukeren. Alternativt må brukeren inngå avtale og skaffe utstyr som gjør det mulig å kommunisere med parter som benytter andre utstedere enn seg selv.

Finnes det en ordning for samtrafikk som på en ikke-diskriminerende måte dekker hele samfunnet (både sluttbrukere og brukersteder), kan dette kalles en samfunnsinfrastruktur for elektronisk ID og e-signatur. Er denne ordningen basert på åpne standarder og er åpen for å inkludere nye leverandører i markedet, er dette å betrakte som en åpen samfunnsinfrastruktur for elektronisk ID og e-signatur. Det er leverandører i det norske markedet som jobber med både åpne og lukkede samfunnsinfrastrukturer for eID og e-signatur. Det er derimot ikke etablert en ordning for åpen samfunnsinfrastruktur for elektronisk ID og e-signatur i Norge foreløpig.

Vedlegg 2 Mandat.

Strategiarbeid for eID og elektronisk signatur i offentlig sektor – mandat.
Strategi for utbredelse av PKI-anvendelser i offentlig sektor er i sitt siste virkeår. Det er behov for en ny strategi for eID og elektronisk signatur i offentlig sektor. Den nye strategien baseres på de erfaringer som offentlig sektor har vunnet i forbindelse med den gjeldende strategien.

Strategiarbeidet tar utgangspunkt i en bred forståelse av eID som elektronisk identitet, som kan benyttes til autentisering og realiseres med ulike teknologier, herunder PIN-koder, sms-passord, PKI osv. Elektronisk signatur forstås her som løsninger som knytter et innhold til en identitet på en uaviselig måte. Løsningene kan realiseres gjennom PKI eller bruk av eID i kombinasjon med andre teknologier.

Strategiarbeidet skal frembringe to resultater (dokumenter):

- Sikkerhetsrammeverk for elektronisk kommunikasjon med og i offentlig sektor
- Strategidokument med forslag til beslutninger knyttet til etablering, organisering og forvaltning foruten langsiktige veivalg for bruk av eID og e-signatur i offentlig sektor, med kobling til sikkerhetsrammeverket.

Arbeidsgruppen skal utrede:

a. etablering av et rammeverk for sikkerhet i elektronisk kommunikasjon med og i forvaltningen, med utgangspunkt i Vedlegg 1 til Kravspesifikasjon for PKI i offentlig sektor (Sikkerhetsnivåer). Vedlegget må gjennomgås med sikte på å foreta nødvendige utvidelser og revisjoner. Det må avklares hvilke føringer et slikt rammeverk vil gi for vedlikehold av Kravspesifikasjon for PKI og forvaltning av SEID-standardene.

b. strategier for forsyning av publikum med eID/e-signatur - privat sektors og offentlig sektors rolle (bl.a. pågående arbeid med nasjonalt ID-kort), herunder også gjenbruk av eksisterende autentiserings- og signeringsløsninger fremskaffet i statlig regi (f.eks. skattePIN som skal benyttes i forbindelse med MinSide, Altinns løsninger og e-signaturløsninger som benyttes av helsesektoren og NAV.).

c. strategiske valg for felles offentlige løsninger for validering av eID og e-signatur. Det skal vurderes mulig reetablering av en felles offentlig sikkerhetsportal, med utgangspunkt i foreliggende sikkerhetsportalkravspesifikasjonen, med nødvendige endringer og tillegg. Det må vurderes hvilke tjenester en reetablert sikkerhetsportal skal tilby ut over validering av eID og e-signatur.

d. strategiske valg for offentlig styring og spesielt for statens rolle, herunder eierskap, forvaltning og garantiansvar.

e. strategiske valg av forretningsmodeller for bruk av fellesløsninger som virker som insentiver for aktuelle aktører til å bidra til spredning og bred bruk av

løsningene. Modellene skal sikre økonomisk forutsigbarhet for de ulike aktører. Løsningene som etableres bør også kunne benyttes ved avtaleinngåelser mellom private parter.

f. forholdet mellom felles løsninger for forsyning av offentlig sektor med eID og e-signatur (virksomhetssertifikater og ansattsertifikater) til eget bruk, og felles løsninger for validering av eID og e-signatur, inklusive en eventuell reetablering av offentlig sikkerhetsportal.

Arbeidsgruppen skal videre vurdere de økonomiske, administrative og tekniske konsekvenser av de løsninger som gruppen foreslår.

Gruppens vurderinger skal løpende samstemmes med utredningsarbeidet som pågår i sikkerhetsportalforvaltningen i Brønnøysundregistrene.

Gruppen skal levere sitt forslag til FAD ultimo november.

Gruppen er sammensatt som følger:

Katarina de Brisis, Fornyings- og administrasjonsdepartementet (leder)
Elisabeth Sunde, Arbeids- og velferdsdirektoratet
Svein Mobakken, Skattedirektoratet
Hallstein Husand, Brønnøysundregistrene
Roger Stenbakk Olsen, Brønnøysundregistrene
Inger Elisabeth Kvaase, Sosial- og helsedirektoratet
Svein Erik Wilthil, KS
Hans Erik Gravdahl Sørensen, Fornyings- og administrasjonsdepartementet
Trine Lind, Fornyings- og administrasjonsdepartementet

Sammensetning av undergruppen for utvikling av sikkerhetsrammeverket:

Kristian Bergem, Fornyings- og administrasjonsdepartementet (leder)
Mari Grini, Skattedirektoratet
Ståle Norum Engen, Brønnøysundregistrene
Haakon Hertzberg, Arbeids- og velferdsdirektoratet
Jon Aarbakke, Sosial- og helsedirektoratet
Margrete Noraas, Kristiansand kommune.