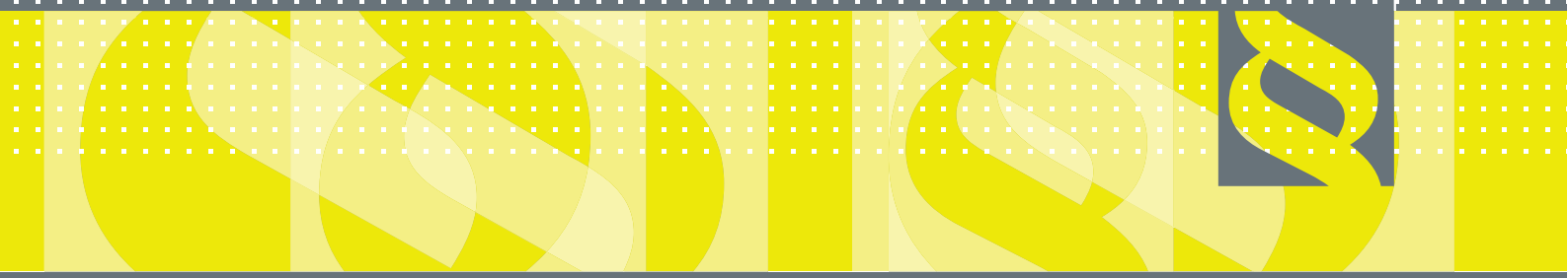
Sluttrapport februar 2007

Nasjonalt ID-kort



JUSTIS- OG POLITIDEPARTEMENTET

DEFINISJONER

***autentisering,** verifisering av en påstått identitet i elektronisk kommunikasjon mellom to ukjente parter.

***biometri**, kommer av to greske ord, *bios* som betyr liv, og *metri* som betyr å måle. *Biometri* blir brukt som kortform for *biometrisk personinformasjon*.

***biometrisk pass,** se *elektronisk pass*.

***biometrisk personinformasjon** *(eng. biometrics),* målbare unike fysiske kjennetegn ved en person (f.eks. ansiktsfoto, fingeravtrykk, irismønster, DNA) eller personens væremåte (f.eks. stemme, signatur (skrivemåte), ganglag), som egner seg for identifisering eller verifisering av identiteten. Se også *elektronisk pass*.

***digitalt sertifikat,** en elektronisk melding som gjør det mulig å knytte en eID til en person eller en virksomhet, gjennom å kople sammen en offentlig nøkkel og personens eller virksomhetens navn. Se også *offentlige nøkler*.

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

***elektronisk pass** *(e-pass, ePassport),* pass med personinformasjon lagret elektronisk i en brikke. I hht. ICAOs anbefalinger lagres personinformasjonen, herunder ansiktsfoto (biometri), i en kontaktløs elektronisk brikke koblet til en antenne i passet for såkalt fjernavlesing (RFID-teknologi). Elektronisk lagring av biometri (ansiktsfoto) åpner for en automatisert sammenligning av biometri lagret i passet mot biometri opptatt av vedkommende person på stedet, se *verifisering*.

***elektronisk signatur,** data i elektronisk form som er knyttet til andre elektroniske data og som kan brukes som autentiseringsmetode.

***identifikasjonsdokument,** dokument med opplysninger om en persons *identitet* sammen med annen informasjon (som biometriske karakteristika) for å verifisere identiteten til innehaveren av dokumentet. Et identifikasjonsdokument kan være utstedt for ulike formål, så som en kompetanse til å føre motorvogn (førerkort), adgang til bygning (adgangskort), tillatelse til grensepassering (passet), eller rett til å disponere en bankkonto (bankkort). Et ID-kort er en type identifikasjonsdokument der opplysninger lagres i et plastkort med eller uten elektronisk brikke. Kortets utforming skal følge internasjonale standarder.

***identifisering,** fastsettelse av en bestemt persons identitet, dvs. den prosessen som går ut på å etablere en knytning mellom den fysiske personen og vedkommendes *identitet*. Identifisering kan også beskrives som den prosess som har som mål entydig å skille *en* person ut fra en gruppe personer, f.eks. inntatt i et register. *Identifisering* foretas blant annet ved utstedelse av et identifikasjonsdokument. Fastsettelse av identitet kan foretas på grunnlag av ulike karakteristika ved personen (biometri), dokumenter som det kan festes lit til, og vitnesbyrd fra andre personer.

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

---

* definisjoner i samsvar med definisjoner brukt i OECD

identitetsforvaltning, et bredt administrativt område som dekker det å identifisere personer innenfor et system (som f.eks. kan være et land, et datanettverk eller en organisasjon) og knytte disse til rettigheter og begrensinger til bruk av ressurser i dette systemet.
nasjonalt ID-kort*,* (her) et ID-kort utstedt av kompetent nasjonal myndighet.
offentlige nøkler, infrastruktur for – en teknologisk infrastruktur som muliggjør en stor skala bruk av elektronisk ID og e-signatur på Internett. Infrastrukturen benytter s.k. asymmetrisk kryptering med bruk av privat og offentlig nøkkel. Infrastrukturen er basert på standarder utarbeidet av ISO og IETF. Også referert til som PKI, se vedlegg B.
pass*,* identifikasjonsdokument (reisedokument) som dokumenterer innehaverens nasjonalitet og som kan benyttes for innreise til andre land. Pass produseres med såkalte viseringssider som skal kunne brukes av andre land for å gi påtegning om *visum*, eventuelt innklebing av visumetikett, som bekreftelse på tillatelse til innreise i vedkommende land.
PKI, public key infrastructure, se offentlige nøkler
RFID*,* Radiofrekvens-basert identifikasjon. En metode for automatisk verifikasjon av identitet basert på lagring av identitetsopplysninger i små enheter kalt RFID-brikke. Informasjonen i enheten kan avleses kontaktløst over radiobølger. Avlesning skjer fra mottaksenheter (RFID-base) som må befinne seg i en gitt (avgrenset) avstand fra RFID-brikken for å kunne motta informasjonen. Det skilles mellom aktive og passive RFID-brikker, avhengig av egen kraftforsyning eller ikke.
verifisering *(*av *identitet),* en prosess der påstått identitet sjekkes mot et identifikasjonsdokument fremlagt av personen som påberoper seg identiteten.
visum*,* tillatelse til innreise gitt av myndighetene i ett land til borgere fra andre land. Der det er inngått avtale om visumfrihet behøves ikke visum for innreise. Visum innføres normalt i passet til vedkommende person som har fått visum.

FORKORTELSER

CEN – Comité Européen de Normalisation (Europeisk Standardiseringsorganisasjon)
ETSI – European Telecommunications Standards Institute
ICAO – Den internasjonale luftfartsorganisasjon (International Civil Aviation Organisation) - er en FN–organisasjon med hovedkontor i Montreal i Canada, som blant annet fastsetter anbefalinger og standarder for pass og andre reisedokumenter.
IETF – Internet Engineering Task Force
ILO – International Labour Organization
ISO – International Standards Organisation
ITU – International Telecommunications Union
OASIS – Liberty Alliance (sammenslutning av markedsaktører som fremmer bruken av åpne standarder innen elektronisk meldingsutveksling mv.)
SN – ***Standard Norge,*** organisasjonen som utarbeider og leverer standarder på ulike områder, herunder for ulike typer ID-kort og smartkort, der bruk av standarder vil være en forutsetning for interoperabilitet. Hovedproduktene fra Standard Norge er kjent som Norske Standarder (NS). Standard Norge har medlemmer fra næringsliv, offentlige myndigheter osv. Standard Norge har en grunnbevilgning fra Nærings- og handelsdepartementet, for å opprettholde et apparat for internasjonal standardisering, men tar på seg oppdrag finansiert av næringsliv og myndigheter. Standard Norge deltar i internasjonal standardisering, først og fremst gjennom ISO, ISO/IEC og CEN.
W3C – World Wide Web Consortium

1 OPPSUMMERING

1.1 Innledning

Over de siste tiår har det vært en sterk økning i bruken av ulike ID-kort for å bekrefte egen identitet. Dette er dels et utslag av samfunnsutviklingen med økt mobilitet, og med nye krav til sikker identifisering. Tradisjonelle former for ID-kort har vist seg å være beheftet med svakheter som åpner for misbruk. Det er viktig å sikre seg mot at det kan utstedes to identiteter ("dobbel id") til en person. Samtidig har utviklingen av e-handel og andre former for elektronisk kommunikasjon også åpnet for nye former for identitetstyverier og bedragerier på nettet. Utviklingen har gjort det nødvendig å se på nye løsninger for identifisering, som både ivaretar hensynet til personvernet og samfunnets behov for sikker identifisering.

Løsninger for såkalte nasjonale ID-kort er tatt i bruk, eller er under vurdering, i flere land.

Arbeidsgruppen har valgt å dele fremstillingen i to. Første del (kapittel 2-7) gir en beskrivelse av dagens situasjon, herunder beskrivelse av fremtidige krav til identifisering på ulike områder. I andre del (kapittel 8-17) skisserer arbeidsgruppen innføring av et nasjonalt ID-kort.

1.2 Forslag

Arbeidsgruppen foreslår at:

1. Det innføres et frivillig **nasjonalt ID-kort,** som skal kunne utstedes til alle norske statsborgere og andre søkere med fast opphold i Norge, dvs. som er registret i Folkeregisteret.
2. Kortet utstedes med visuelt lesbare personopplysninger sammen med personfoto og signatur, optisk maskinlesbar tekst, samt **RFID-brikke** der samme data som fremgår av kortets visuelle del lagres.
3. Det nasjonale ID-kortet utstedes med funksjonalitet som et **EU/Schengen ID-kort**[1] til alle norske statsborgere som ønsker slik funksjonalitet. Dette kortet skal inneholde informasjon om norsk statsborgerskap.
4. Kortet skal inneholde en kontaktbrikke der **en elektronisk ID** kan lagres i kortet etter ønske fra søker over 13 år og en elektronisk signatur etter ønske fra en søker over 18 år. Najonalt ID-kort med eID skal i utgangspunktet kunne brukes overfor det offentlige og overfor private aktører for privatrettslige disposisjoner.
5. Ordningen med nasjonalt ID-kort **administreres av politiet.** Søknader behandles av politiet på stedet, eventuelt ved vedkommende norske utenriksstasjon. Det velges samme identifikasjons- og utstedelsesprosess for nasjonalt ID-kort som for pass, og politiets eksisterende infrastruktur og personell benyttes.
6. Det etableres et **sentralt register over alle innehavere av nasjonalt ID-kort.**
7. Ordningen med nasjonalt **ID-kort forankres i en egen lov om nasjonalt ID-kort.**
8. Kortene gis en gyldighetstid på 5 år.
9. ID-kortet finansieres ved selvkost gebyrordning. Etablering av ID-kortordningen forutsetter en del investeringskostnader, jf. kap. 15.

[1] ID-kortet må være utstedt av offentlig myndighet og må vise innehaverens statsborgerskap, jf. kap. 7.8

Etablering av nasjonalt ID-kort er ikke ment å endre dagens rettslige utgangspunkt om at det i Norge ikke foreligger noen alminnelig plikt til å legitimere seg, eller å ha med seg legitimasjonsdokumenter.

Kortene er kun ment som et tilbud til personer for at disse lett skal kunne identifisere seg når det foreligger et saklig behov.

DEL I

2 BAKGRUNN

Samfunnsutviklingen har medført en sterk økning i bruk av ulike identitetsdokumenter for å bekrefte egen identitet. Økt mobilitet reiser nye krav til sikker identifisering, samtidig som internasjonalisering har ført til at ulike former for ID-kort forankres i globale standarder.

Behov for sikker og pålitelig identifikasjon, både fysisk og elektronisk (på nett), har økt de siste årene. Kort utstedt av bl.a. banknæringen og av posten er blitt brukt til dette formål i flere år. Dette er imidlertid kort utstedt i forbindelse med konkrete kundeforhold og disse kan derfor ikke oppfylle det alminnelige behovet for identifisering i alle sammenhenger.

En av de største utfordringene er å sikre seg mot at det kan utstedes to identiteter ("dobbel id") til en person, eller at flere personer kan benytte samme identitet. De siste årene har vi sett en fremvekst av internasjonal kriminalitet og terrorisme hvor bruk av falske ID-dokumenter står sentralt, samtidig som utviklingen av e-handel og andre former for elektronisk kommunikasjon har åpnet for helt nye former for identitetstyverier og bedragerier på nettet.

Utviklingen medfører at vi stadig oftere må kunne legitimere oss i forskjellige sammenhenger, både visuelt og på nettet. Denne utviklingen har fremtvunget nye løsninger for identifisering, som på den ene siden ivaretar hensynet til personvernet og trygghet for den enkelte, men samtidig også gir en tilstrekkelig grad av effektivitet, sikkerhet og tillit.

Minst 18 EU land har allerede tatt i bruk løsninger for såkalt nasjonalt ID-kort, og andre EU/Schengen land vurderer å innføre slike ID-kort.

Justisdepartementet besluttet på denne bakgrunn å nedsette en arbeidsgruppe for å vurdere innføring av en ordning med nasjonalt ID-kort i Norge.

3 ARBEIDSGRUPPENS MANDAT, SAMMENSETNING OG GJENNOMFØRING

Mandat

Arbeidsgruppen skal utrede og eventuelt legge fram forslag til etablering av en ordning med ID-kort som skal være et *tilbud* til den enkelte for sikker og enkel verifisering. Herunder skal arbeidsgruppen:

- beskrive og begrunne *behovene* for et nytt, frivillig nasjonalt ID-kort,
- vurdere, samt ta stilling til hvilken *informasjon* som bør legges inn i kortet, herunder om personinformasjon sammen med eventuell *biometrisk personinformasjon,* bør lagres elektronisk eller på annet maskinlesbart medium i kortet. Arbeidsgruppen skal også vurdere om det kan legges opp til flere *valgmuligheter* ut fra brukerens behov og ønsker,
- vurdere en lovmessig forankring for et nasjonalt ID-kort, samt foreslå rettslige rammer og konsekvenser ved ordningen,
- beskrive og vurdere ulike aspekter ved sikkerheten, brukervennligheten og personvernet i forbindelse med et nytt ID-kort,
- vurdere hvordan ID-kortet vil kunne påvirke utstedelsen og bruken av *andre* kort som benyttes til identifisering,
- vurdere, samt foreslå plassering av det administrative ansvaret for utstedelse og forvaltning av et nasjonalt ID-kort. Det forutsettes at det vurderes om administrasjonen kan baseres på eksisterende infrastruktur og rutiner for utstedelse av pass,
- beskrive den samfunnsmessige kost-nytte ved ordningen, herunder administrative og økonomiske konsekvenser. Arbeidsgruppen skal også vurdere og eventuelt foreslå bruk av gebyr knyttet til ordningen.

Det forutsettes at arbeidsgruppen gir en beskrivelse av bruken av nasjonalt ID-kort i andre land, særlig innenfor EU/Schengen-området. Det bes spesielt om at det gis en nærmere redegjørelse for situasjonen i øvrige nordiske land, og hvilke erfaringer som er gjort med bruken av nasjonalt ID-kort.

Arbeidsgruppen kan påpeke behovet for ytterligere utredninger på konkrete temaer, samt eventuelt foreslå etablering av piloter eller prøveprosjekter.

Arbeidsgruppens sammensetning

Avdelingsdirektør (politimester fra 8. mai 2006) Håkon Skulstad, Justisdepartementet (leder frem til levering av delrapport)
Avdelingsdirektør Knut Fosli, Justisdepartementet (leder fra 11. september 2006)
Avdelingsdirektør Magnar Aukrust, Justisdepartementet
Førstekonsulent Morten Thomsen, Justisdepartementet (frem til 15. september 2006)
Seniorrådgiver Unni Norum, Politidirektoratet (sektretær)
Seniorrådgiver Kristin Hefre, Utenriksdepartementet (Lars Løberg, vara)
Rådgiver Svenn Bjerkem, Utenriksdepartementet (frem til levering av delrapport)
Seniorrådgiver Thomas Myhr, Nærings - og handelsdepartementet (rådgiver Espen Børset, vara)
Avdelingsdirektør Sissil Pettersen, Arbeids- og inkluderingsdepartementet
Prosjektleder Tom Halvorsen, Arbeids- og inkluderingsdepartementet
Seniorrådgiver Katarina de Brisis, Fornyings- og administrasjonsdepartementet
Underdirektør Signe Moe, Samferdselsdepartementet (seniorrådgiver Pierre Chauvin, vara)

Observatører:
Avdelingsdirektør Leif T. Aanensen, Datatilsynet (senioringeniør Atle Årnes, vara)

Gjennomføring av utredningen

Arbeidsgruppen har til sammen hatt 13 møter. På et av møtene ble det fra Sparebankforeningen gitt en presentasjon om banklegitimasjon. Videre har arbeidsgruppen hatt besøk av Sveriges prosjektleder for e-pass og nasjonalt ID-kort som informerte om prosessen med innføring av ID-kort i Sverige. Deler av arbeidsgruppen har deltatt på et kurs i biometri. Deler av arbeidsgruppen ble invitert til Fornyings- og administrasjonsdepartementet i forbindelse med besøk av en delegasjon fra Estland som blant annet presenterte Estlands ID-kortløsning.

Morten Thomsen har gitt en presentasjon av gruppens arbeid for arbeidsgruppen for "utveksling av grunndata på personinformasjonsområdet".

Katarina de Brisis har gitt en presentasjon for arbeidsgruppen for "strategi for bruk av eID og e-signatur i offentlig sektor".

Innholdet i kap. 12 (eID) er blitt utarbeidet av en undergruppe ledet av FAD, med deltagelse fra NHD, Datatilsynet og invitert observatør fra Post- og teletilsynet. Undergruppen har også hatt bistand fra advokatfirma Wikborg Rein.

Arbeidsgruppen legger fram sin endelige innstilling innen 10. februar 2007.

4 DAGENS SITUASJON

4.1 Innledning

Formålet med kapitlet er å gi en oversikt over eksisterende ID-dokumenter (kapittel 4.2), herunder formål, rettslig forankring, utstedelsesprosess, utbredelse og utviklingstrekk. Det eksisterer ingen samlet oversikt over ID-dokumenter, verken i offentlig eller i privat sektor. Det vil bli gitt en oversikt over dokumenter som i dag benyttes som ID-bevis. Oversikten er ikke uttømmende. Det vil også bli gitt en beskrivelse av elektronisk identifisering ved samhandling over internett (kapittel 4.3) og en oversikt over bruk av ID-kort i andre EU/Schengen-land (kapittel 4.4).

4.2 Oversikt over eksisterende identitetsdokumenter

4.2.1 ID-dokumenter utstedt av offentlig myndighet

Pass

Passet er i utgangspunktet et *reisedokument*, men er i dag det eneste offisielle norske identitetsdokument som godtas i utlandet. Det utstedes årlig ca. 550.000 pass. I det sentrale passregisteret (PASS) lagres opplysninger om alle maskinlesbare pass (e-pass etter 1. oktober 2005).

Pass utstedes med hjemmel i passloven av 19. juni 1997 med tilhørende forskrift. Passøker må møte personlig og godtgjøre sin identitet og sitt norske statsborgerskap.

Passet følger standarder fastsatt av ICAO og EU. Passet har en *elektronisk brikke* i personaliasiden hvor det i tillegg til personopplysninger lagres et digitalt bilde av passinnehaveren. Fingeravtrykk må implementeres innen 28.juni 2009[2].

Diplomat-, spesial- og tjenestepass (totalt ca. 2000 pr. år) utstedes av Utenriksdepartementet med hjemmel i Utenriksinstruksen, fastsatt ved Kgl. res. 13.12.2002. I Utenriksinstruksen kapittel 5, § 4 er det fastsatt nærmere regler om hvem som er berettiget til denne type pass. Passet følger samme standard som ovennevnte pass og tilsvarende krav for passutstedelse legges til grunn. Digitalt bilde og signatur innhentes ved personlige fremmøte i UD. Opplysninger om passene lagres i det sentrale passregisteret (PASS).

Førerkort

Formålet med førerkort er å angi identitet og dokumentere førerrett ved trafikkontroll. Rutinene for utstedelse av førerkort fastsettes i Vegdirektoratet. Førerkort bestilles på de enkelte trafikkstasjonene.

Førerkortforskriften med vedlegg inneholder reguleringer av førerkortets utforming osv. Førerkortforskriften er en gjennomføring av EUs førerkortdirektiv, Rådsdirektiv 91/439 som senest er endret ved Rådsdirektiv 2003/59. Det er i Norge utstedt i underkant av 2,9 millioner førerkort, registrert i et nasjonalt førerkortregister. Det ble 19. desember 2006 vedtatt et nytt

[2] Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Members States.

direktiv om førerkort som blant annet tidfester pliktig utfasing av førerkort av eldre modeller i papp som ennå brukes i enkelte EØS-land, og med dette også en forsering av overgangen til førerkort av den "kredittkorttype" som Norge har benyttet i noen år. For denne modellen førerkort er det en rekke krav til sikkerhet mot forfalskning.

Adgangskort til havner (offentlig og private/industrihavner)
Den enkelte havneterminal utsteder sine egne ID-kort for adgangs- og identifikasjonskontroll av personer.

ID-kort utstedes med hjemmel i det nye internasjonale sikkerhetsregimet for skip og havner, inntatt i SOLAS[3] kapittel XI-2 og den tilhørende ISPS-koden[4]. Regelverket skal sikre skip i internasjonal fart og havneanlegg som betjener disse mot terroranslag, og/eller at skip skal bli benyttet som redskap til slike handlinger. Dette krever til dels omfattende sikkerhetstiltak i havnene, herunder inngjerding, adgangs- og identifikasjonskontroll av personer, kjøretøy og gods m.m.

Utstedelse av adgangskort er basert på de retningslinjer og krav som er nedfelt i den enkelte havneterminals sikkerhetsplan. Havnens sikkerhetssjef godkjenner de som skal få utstedt slike kort. Det foreligger ingen oversikt over antall utstedte kort. Disse er heller ikke registrert i et eget sentralt register.

Adgangskort til lufthavner
Det er krav om at enhver som i tjenestelig øyemed har behov for adgang til en lufthavns flyside, skal være utstyrt med adgangskort utstedt av lufthavnoperatøren. Adgangskort for regelmessig adgang til flyside skal være et identitetskort (ID-kort). Likestilt regnes identitetskort for Luftfartstilsynets ansatte som er autorisert av luftfartsdirektøren, gyldige luftfartssertifikater utstedt av Luftfartstilsynet eller luftfartsmyndighet i annen stat, og politi- og tolltjenestebevis båret av politi- og tolltjenestemann i tjeneste på lufthavnen. (Forskrift av 30. april 2004 nr. 715 om forebyggelse av anslag mot sikkerheten i luftfarten.)

Forskriften gjennomfører EUs securityregelverk som stiller krav om ID-kort. Lufthavnoperatøren skal utstede et identitetskort for lufthavnen til alt personale som arbeider i lufthavnen, eller som besøker den ofte (også til ansatte i lufthavnen, luftfartsselskapene og andre organisasjoner). ID-kort for lufthavnen skal minst inneholde kortinnehaverens navn og bilde, opplysninger om hvilke områder det gir adgang til, og om gyldighetstiden. ID-kortet skal bæres slik at det er synlig, og til enhver tid når innehaveren er i tjeneste.

For ID-kort som skal gi adgang til flyside, kreves det fremlagt uttømmende politiattest. Luftfartstilsynet skal på bakgrunn av slik attest avgjøre hvorvidt søker har slik vandel at ID-kort kan utstedes. ID-kort utstedes med gyldighet i inntil 5 år.

Det er gjennomført omfattende sikkerhetstiltak på lufthavnene de senere årene. Bestemmelsene om ID-kort er ett av mange tiltak innrettet mot forebyggelse av anslag mot sikkerheten i luftfarten.

Kravene til ID-kort er gjennomføring og utdyping av kravene som finnes i Chicagokonvensjonen, Annex 17 og anbefalingene i ECAC Doc. 30[5]. Når det gjelder selve

[3] International Convention for the safety for life and sea (1974)

[4] International Ship and Port Facilities Security Code (2002, i kraft 2004)

[5] European Civil Aviation Conference, Policy Statement of the field of civil aviation facilitation

utformingen av ID-kortene, finnes det forslag i veiledningsmateriellet til disse internasjonale forpliktelsene/anbefalingene.

Sjøfartsbok
Sjøfartsbok utstedes kun til norske sjøfolk og er et reise- og ID-dokument i henhold til ILO-konvensjonen nr. 108, samt et dokument som legger til rette for dokumentasjon av fartstid. Sjøfartsboken gir rett til innreise og landlov i de land som har ratifisert ILO-konvensjonen 108. (Etter terroraksjonen i USA 11. september 2001 fungerer ikke dette i alle land.)

Sjøfartsboken utstedes med hjemmel i forskrift av 25. november 1988 nr. 940 om kontroll av maritim tjeneste. Sjøfartsbøker blir utstedt av 16 bemyndigede NAV-kontorer[6] med kontroll av maritim tjeneste. Norske sjøfolk som bor i utlandet, eller som har behov for å få utstedt sjøfartsbok i utlandet, kan fremme søknad på norsk utenriksstasjon. Det kreves som hovedregel pass for å dokumentere identitet ved søknad om sjøfartsbok, ev. tidligere sjøfartsbok eller førerkort i tillegg til dåpsattest/fødselsattest.

I 2005 ble det utstedt 4572 sjøfartsbøker. Det ble laget et kvalitetssikringssystem i 2005 og de bøker som er utstedt etter dette er i et register hos Sjøfartsdirektoratet.

Utlendingsfeltet
Innvandringsmyndighetene utsteder i dag utlendingspass og reisebevis for flyktninger, oppholds- og arbeidstillatelser og registreringsbevis for asylsøkere.

Utlendingspass og reisebevis for flyktninger (reisedokumenter)
Reisedokumentene brukes ved reiser utenfor Norge. Dokumentene brukes også for innsetting av oppholdstillatelse i form av en standardisert Schengenetikett. Reisedokumentene følger samme standard som ordinære pass.

Flyktning som får lovlig opphold i Norge skal gis reisebevis for flyktning, dersom ikke særlige grunner taler mot det. En person som har søkt asyl, og som ikke får flyktningstatus, men arbeids- eller oppholdstillatelse, skal gis utlendingspass dersom vedkommendes forhold til hjemlandets myndigheter tilsier det, jf. utlendingsloven § 19.

Det utstedes til sammen mellom 10.000 og 15.000 reisedokumenter per år.

Vedtak om innvilgelse av reisedokumenter lagres i utlendingsdatabasen (tidligere DUF). Opplysninger om utstedte reisedokumentet lagres i utlendingsdatabasen og i det sentrale passregisteret (PASS).

Registreringsbevis for asylsøkere
Registreringsbeviset brukes i forbindelse med kontrolloppgaver utført av utlendingsforvaltningen og er dokumentasjon på at personen har midlertidig opphold i Norge mens asylsaken er under behandling. Registreringsbeviset gjelder ikke som reisedokument. Registreringsbeviset anses ikke som dokumentasjon på at de angitte personopplysninger er korrekte.

Politiets Utlendingsenhet utsteder registreringsbevis i form av et kort til asylsøkere ved første gangs registrering hos politiet. Kortet gis gyldighet for inntil seks måneder.

---

[6] NAV er en sammenslåing av Trygdeetaten og Aetat. NAV lokalkontorer er samlokalisert med sosialkontorene i kommunene.

Registreringsbevis utstedes med hjemmel i Utlendingsforskriften § 54a. Det utstedes ca. 10.000 registreringsbevis per år.

Informasjon om utstedelse av registreringsbevis lagres i utlendingsdatabasen.

Residence card of a family member of a Union Citizen
Kortet vil bli innført dersom Norge gjennomfører EU direktiv 2004/38[7]. Formålet med kortet er å identifisere at en person er familiemedlem av EU borger som bor i Norge og derved har tillatelse til å oppholde seg i landet. Tillatelsen gir også mulighet til å reise visumfritt i Schengen-området dersom vedkommende har et gyldig reisedokument.

Det antas at UDI vil behandle søknaden og at politiet utsteder dokumentet. Det vil antagelig bli utstedt relativt få kort per år.

Vedtak om innvilgelse og data om utstedelse av Residence card of a member of a Union Citizen vil trolig bli lagret i utlendingsdatabasen (tidligere DUF).

Utenriksdepartementets ID-kort til diplomater m.m
ID-kortene har som formål å dokumentere overfor norske myndigheter (e.g. politiet) at vedkommende har opphold i Norge ved akkreditering til Utenriksdepartementet, samt at vedkommende har krav på ukrenkelighet i henhold til Wien-konvensjonen. Kortet benyttes ved adkomstkontroll til sentralforvaltningen og statlige virksomheter (blant annet Forsvaret).

ID-kortene har sin forankring i kutyme. Det utstedes ca. 600 ID-kort pr. år

ID-kortet er av plastlaminat med dobbeltsidig plastfolie med hologram på personaliasiden. Kortet er preget med riksvåpenet påtrykt Det Kgl. Utenriksdepartement. Kortet inneholder personalia og opplysninger om hvilken grad av immunitet vedkommende har krav på.

Utenriksdepartementet utsteder ID-kort til:
1. Diplomatiske representanter samt deres medfølgende familiemedlemmer (rød)
2. Administrativt og teknisk personale ved diplomatisk stasjon samt deres medfølgende familiemedlemmer (blå)
3. Hjelpepersonale ved diplomatisk stasjon (brun)
4. Andre lands utsendte konsuler (grønn)

Det anses ikke som naturlig at ID-kort til diplomatisk personell m.m. inkluderes i arbeidet med nasjonalt ID-kort. Angjeldende gruppe omfattes av unntaksbestemmelsen i Utlendingsforskriften § 159 og har således strengt tatt ikke oppholds- eller arbeidstillatelse i forskriftens forstand. Det foreligger for øvrig ingen hjemmel for utstedelse av ID-kort til diplomater m.m. Utstedelse av ID-kort til diplomater m.m. bør forbli en særordning i Utenriksdepartementet.

[7] Directive 2004/38/EC of the european parliament and of the council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC

4.2.2 ID-kort i ansettelsesforhold, adgangskort og myndighetsbevis

ID-kort til ansatte arbeidstakere er vanlig både i offentlig og privat virksomhet. Disse kan ha flere funksjoner, men det er vanlig å bygge inn funksjon som adgangskort til bygninger, evt. også til bedriftsinterne IT nett. Utad vil slike kort kunne benyttes som bekreftelse på hvilken institusjon innehaveren representerer, eventuelt som bekreftelse på et fullmaktsforhold.

I en særlig stilling står ID-kort som benyttes som myndighetsbevis. Et eksempel på dette er ID-kort som utstedes til politiansatte med politimyndighet. Det nevnes også at det er svært vanlig å utstyre personer som er gitt begrenset politimyndighet etter politilovgivningen, med et eget ID-kort som angir bærerens myndighet.

Forsvaret utsteder ID-kort både for vernepliktige og ulike kategorier av ansatte. Kortene reflekterer etter omstendighetene også vedkommendes myndighet, f.eks. om innehaveren kan utøve myndighet som militærpoliti eller som grensevakt.

4.2.3 Bankkort

Bankkort utstedes til innehavere av bankkonti. Formålet er å dokumentere et kundeforhold og retten til å disponere en bestemt konto i en bank. Disse utstedes i dag i stor grad med personinformasjon sammen med foto for å kunne benyttes til verifisering av identitet. Bankkort inneholder fødselsnummer. Gjennom utformingen er det tatt hensyn til at kortet skal kunne benyttes ved kontotransaksjoner i en hvilken som helst bank/bankfilial i inn- og utland. I siste generasjons bankkort er det også lagt inn elektronisk kontaktbrikke slik at kortet skal kunne benyttes til netthandel og elektroniske banktjenester.

Bankkort utstedes ved etablering av konto, og mot nødvendig dokumentasjon av blant annet identitet til den bank det etableres kundeforhold til. Fra 1. mars 2007 har banknæringen lagt opp til at det skal kreves fremlagt pass ved utstedelse av såkalt bankkort med ID, dvs. bankkort som blant annet inneholder visuell personinformasjon. Dette kommer som en oppfølgning av reglene for bekjempelse av hvitvasking, der det er forutsatt at bankene skal gjennomføre en kvalifisert kontroll av kortinnehavers identitet før utlevering av bankkort med ID.

I henhold til oppgave fra Norges Bank er det pr. 2005 utstedt nærmere 5 millioner kort med bankaksept-funksjon. Den overveiende andel av disse er utstedt med bilde av kontoinnehaver. Det antas at slike bankkort er det mest utbredte ID-kort i Norge, også med hensyn til å benytte kort som ren legitimasjon når det er behov for å bekrefte egen identitet.

4.2.4 Andre ID-kort

I ulike samfunnssektorer benyttes for øvrig en rekke ID-dokumenter med forskjellige bruksområder og derved ulikt innhold og sikkerhetsnivå.

Av de mer utbredte typene ID-kort regnes elevkort eller studentkort, men det kan også være kort som bekrefter medlemskap i frivillige foreninger, eller som gir adgang til bestemte lokaler.

Det finnes ingen formelle regler for utstedelse og bruk av slike kort. Der kortene skal leses i f.eks. elektroniske terminaler, kreves en standardutforming som tar hensyn til dette. I stor grad benyttes i slike tilfeller etablerte internasjonale standarder for produksjon og utstedelse av kort. Også slike kort vil bli benyttet for verifisering eller bekreftelse av egen identitet utenfor de formålene kortene er utstedt til.

4.3 Elektronisk identifisering ved samhandling over internett

I forbindelse med *elektronisk samhandling over Internett* vil det eksistere behov for å godtgjøre sin identitet overfor kommunikasjonsmotparten. Dette behovet vil eksistere i mange ulike sammenhenger. Videre kan det være behov for signering av transaksjoner, dvs. bekreftelse av bindingen mellom avsender og innholdet i forsendelsen (uavviselighet). Behovene kan dekkes av elektronisk ID (eID), lagret i et smartkort, som også kan være et fysisk identitetskort. I sammenheng med et identitetskort er det særlig bruk innen elektroniske tjenester fra offentlig sektor til innbyggerne, elektronisk handel på Internett inkludert nettbank, og samhandling mellom privatpersoner f.eks. via elektronisk post som vil være mest relevant.

Til bruk for disse formål eksisterer det i dag minst to typer kort utviklet i markedet – bankenes smartkort for bruk av BankID mot nettbank og Buypass' smartkort til bruk mot Norsk Tippings tjenester og Lånekassens gjeldsbrevstjeneste. BankID er tenkt distribuert til 2,1 millioner brukere av nettbank.[8] Videre ruller Buypass ut smartkort gjennom kommisjonærleddet til Norsk Tipping. Det regnes med at antallet brukere vil nå 2 millioner (dvs. antall holdere av tippekort). Bankkortet utstedes i samsvar med vanlige prosedyrer for bankkort, eller ved å følge en prosedyre i sin nettbank.

Buypass-kort utstedes på tre ulike måter – ved bestilling på sidene til Norsk Tipping, ved registrering direkte på Buypass' nettsider, eller ved oppmøte hos en tippekommisjonær[9].

Kravspesifikasjon for PKI i offentlig sektor beskriver tre typer eID med hensyn til sikkerhetsnivå – Person Standard, Person Høyt og Virksomhet. Kravspesifikasjonen er obligatorisk for offentlig sektor. Det er eID av typen Person Høyt som er aktuelt å utstede på kort.

4.4 Bruk av nasjonalt ID-kort i andre land

4.4.1 Innledning

Dette kapitlet har til hensikt å gi en oversikt over løsninger med nasjonalt ID-kort i andre land. Arbeidsgruppen har valgt å presentere de øvrige nordiske land fordi dette er land det er naturlig for Norge å sammenligne seg med. Arbeidsgruppen har videre funnet det naturlig å velge ut enkelte EU-land fordi Norge gjennom Schengen-avtalen har en nær tilknytning til EU. Det vil også bli gitt en skjematisk oversikt over situasjonen i de fleste EU-land.

4.4.2 Norden

Sverige

Sverige innførte nasjonalt ID-kort 1. oktober 2005. Kortet dekker kravene til et EU/Schengen ID-kort. Ordningen er frivillig og gjelder svenske statsborgere.

Kortet inneholder foto og innehavers personopplysninger, samt elektronisk chip med biometrisk informasjon. ID-kortet inneholder også en kontaktchip, som man i fremtiden vil kunne anvende

[8] Ikke alle banker vil utstede smartkort til bruk mot Bankkort med ID. Enkelte banker kan velge andre former for to-faktor beskyttelse av tilgangen til Bankkort med ID, f.eks. en passordkalkulator.

[9] Kortet inneholder kun en forenklet eID til bruk ved tipping på maskiner hos kommisjonærene. For å få lastet ned en fullverdig eID, må brukeren gå på Buypass' nettsider, registrere seg og få tilsendt en kortleser til sin adresse. Etter installasjon av kortleser settes kortet i, og en prosedyre på Buypass' nettsider følges for å laste ned en eID til kortet som deretter brukes i egen kortleser.

for elektronisk ID. Kortinnehaver har ingen valgfrihet i forhold til hvilken informasjon som legges inn i kortet sett hen til vedkommendes behov.

Passmyndigheten (dvs. politiet) utsteder ID-kortet. Søknadsprosedyre/identitetskontroll en den samme som ved søknad om pass. For utstedelse av ID-kort er det krav om svensk statsborgerskap og at man kan identifisere seg.

Det skal utredes om innføring av ID-kort har påvirket bruken av andre identitetskort, herunder utstedelse av pass.

Pass og ID-kort koster hver 400 svenske kroner og er gyldig i 5 år.

Finland

Finland har en ordning med nasjonalt ID-kort som er frivillig. Kortet dekker kravene til et EU/Schengen ID-kort. Kortene utstedes til finske statsborgere og utlendinger med permanent oppholdstillatelse og hvor det har vært mulig med pålitelig verifisering av identitet.

Kortet kan benyttes til elektronisk identifisering, blant annet i forhold til elektroniske tjenester fra offentlig sektor.

Kortene brukes som identitetsbevis og som reisedokument innenfor EU/Schengen. Det finske ID-kortet følger ICAO-standard. Kortet inneholder ikke biometriske kjennetegn. Det er hittil utstedt ca. 100.000 slike kort.

ID-kortet utstedes av det lokale politiet og man følger samme utstedelsesprosedyrer som for pass.

Ordinært ID-kort koster 40 Euro, ID-kort til mindreårige koster 21 Euro og midlertidige ID-kort koster 30 Euro. Gyldighetstiden for de to førstnevnte ID-kortene er 5 år. Midlertidig ID-kort kan ha en gyldighetstid inntil 4 måneder.

Pass koster 40 Euro og gyldighetstiden er 5 år.

Danmark

Danmark har i dag ikke et nasjonalt ID-kort. Myndighetene har utredet om det eksisterende helseforsikringskortet skal utvides til å gjelde som et elektronisk, nasjonalt ID-kort. Løsningen ble funnet for kostbar og ideen ble forkastet.

Et offentlig utvalg ble gitt i oppdrag å levere en innstilling innen utgangen av 2006 om hvorvidt Danmark skal arbeide videre med etableringen av et slikt identitetsdokument.

Danske pass har gyldighetstid på 2 år for barn 0-2 år, 5 år for barn mellom 2 og 18 år. Pass til personer over 18 år har 10 år gyldighetstid. Pass til barn koster 115 danske kroner, pass til voksne mellom 18 og 65 år koster 600 danske kroner og pass til personer over 65 år koster 350 danske kroner.

Island

Island har et gammeldags ID-kort system, som så og si ikke benyttes i praksis. Island har foreløpig ikke besluttet om det skal tas i bruk nye ID-kort i tråd med EU-standardene. Gyldighetstiden for islandske pass er 5 år.

4.4.3 Andre land

En felles standard for nasjonalt ID-kort er under utarbeidelse innen EU, jf. kapittel 7.8. Det foreligger ingen plikt etter Schengen-avtalen til å ha et nasjonalt ID-kort.

Tyskland

Tyskland har hatt nasjonalt ID-kort siden 1986. Kortet dekker kravene til et EU/Schengen ID-kort. Kortet benyttes også som legitimering ved valg etc.

ID-kortet utstedes bare til tyske statsborgere. Alle statsborgere må ha nasjonalt ID-kort da det er legitimasjonsplikt i Tyskland. Kortet skal i løpet av de neste 2-3 år erstattes av et nytt kort med elektroniske funksjoner.

ID-kortet inneholder foto, underskrift, opplysninger om kjønn, gyldighet, nasjonalitet og adresse. Kortinnehaveren kan ikke velge hvilke data som skal fremgå av kortet.

Søknad om ID-kort fremsettes ved personlig oppmøte hos lokal ID- og passmyndighet.

Når det gjelder bestillingsvolumet for nye dokumenter er forholdet 2/3 for ID-kort og 1/3 for pass.

Man kan søke om ID-kort fra fylte 16 år. For personer under 26 år er kortet gyldig i 5 år, deretter er kortet gyldig i 10 år om gangen.

Gebyr for ID-kort er ca. 8 Euro.

Pass koster 59 Euro for personer over 26 år. Gyldighetstiden er 10 år. For personer under 26 år koster passet 37,50 Euro og gyldighetstiden er 5 år.

Østerrike

Det østerrikske ID-kortet har siden 2002 hatt bankkort-format. Kortet dekker kravene til et EU/Schengen ID-kort. Ordningen med ID-kort er frivillig og gjelder bare østerrikske statsborgere.

Pr. i dag lagres ikke biometriske opplysninger eller andre opplysninger enn informasjon om eierens identitet, som f.eks. foto, fødselsdato og underskrift på ID-kortet. Korteier kan ikke påvirke hvilke opplysninger som skal lagres i kortet. Kortet brukes ikke til elektronisk identifisering.

Ved søknad om ID-kort må man vise frem bostedsbekreftelse, fødselsattest, ev. vielsesattest og bekreftelse på at man er østerriksk statsborger. ID-kortet utstedes av egne passkontor underlagt myndighetene på by - eller storkommuneplan.

Det er ikke tilgjengelig tallmateriale over fordelingen mellom pass og ID-kort, men pass har antagelig større utbredelse.

Gyldighetstiden for ID-kortet er 10 år for personer over 12 år. For barn mellom 6 og 12 år er kortet gyldig i 5 år. For barn mellom 1 og 6 år er kortet gyldig i 4 år. For barn under 1 år er kortet gyldig i 1 år. ID-kortet koster 56 Euro. Gyldighetstiden for pass er 10 år for personer over 12 år.

Italia
Italia har et ID-kortsystem. Kortet dekker kravene til et EU/Schengen ID-kort. Kortet utstedes bare til italienske statsborgere. Alle statsborgere over 15 år er pålagt å ha ID-kort.

Det ble innført et nytt ID-kort 1. januar 2006 (prøveprosjekt fra 2001). ID-kortet er elektronisk med microchip der alle typer informasjon kan lagres. Kortet kalles Carta d'Identità Elettronica (CIE). I tillegg er et papir-ID-kort med basisinformasjon fremdeles i bruk.

ID-kortet brukes også for tilgang til nettjenester. Videre er det lagret en elektronisk underskrift på kortet. Kortet kan også brukes ved interaksjon med andre borgere, i banker og andre typer institusjoner.

På kortet er det lagret informasjon om kortholders fornavn og etternavn, kjønn, fødested, bosted, fødselsdato og codice fiscale (tilsvarer norsk personnummer). Videre er det bilde av kortholder, underskrift og to digitale fingeravtrykk. Avtrykkene er lagret både som bilde og som template. I tillegg er det mulighet for å lagre ytterligere informasjon på kortet. Dette gjelder både for borgerne og kommunene.

Alle kommunene er pålagt å sjekke og samkjøre personalia og opplysninger med Indice Nazionale delle Anagrafi (Nasjonalt folkeregister). Det må fastslås at opplysningene er korrekte og samkjørte. Videre må det også kontrolleres om personen har begått straffbare handlinger som umuliggjør utstedelse av ID-kort.

I Italia benyttes først og fremst ID-kort fremfor pass ved reise. Dette var også tilfellet før CIE ble innført. Dermed er det ingen direkte nedgang i passutstedelser da ID-kortet allerede har vært det primære reisedokument, og kun byttes ut med en ny type ID-kort.

Det er ennå ikke offisielt avgjort hvor mye CIE ID-kortet vil koste. Uoffisielle kilder anslår at det kan koste opp til 30 Euro. ID-kortet er gyldig i 5 år.

Et italiensk pass koster 371 norske kroner og er gyldig i 10 år.

Nederland
Nederland har hatt nasjonalt ID-kort siden 1995. Kortet dekker kravene til et EU/Schengen ID-kort. Kortet er en frivillig ordning og utstedes bare til nederlandske statsborgere.

ID-kortet inneholder foto, signatur og personinformasjon om innehaveren. Fra 26. august 2006 ble det innført et nytt ID-kort med biometrisk informasjon i henhold til EU- og ICAO-krav. Kortinnehaver kan ikke påvirke hvilken informasjon som legges inn i kortet.

ID-kortet utstedes av kommunale myndigheter. I 2005 ble det utstedt ca. 1.581.796 ID-kort og 1.761.260 pass i Nederland. ID-kortet koster 31,26 Euro og er gyldig i 5 år. Passet koster 39,40 Euro og er gyldig i 5 år.

Irland
Irland har i dag ikke et nasjonalt ID-kort, men det har vært en mediedebatt vedrørende dette på grunn av britiske myndigheters beslutning om å innføre et slikt ID-kort. Spørsmålet om innføring av ID-kort er foreløpig kun på utredningsstadiet og det er så langt ikke lagt frem noe forslag for regjeringen.

4.4.4 Oversikt over utbredelse av nasjonalt ID-kort i EU-land

Av 25 EU-land mangler arbeidsgruppen informasjon om 3 land. Av de 22 EU-land arbeidsgruppen har informasjon om, har 18 land nasjonalt ID-kort, mens 4 land ikke har nasjonalt ID-kort (Storbritannia har imidlertid vedtatt å innføre nasjonalt ID-kort fra 2008/2009). I de landene hvor det i dag ikke er nasjonalt ID-kort pågår et utredningsarbeid på dette feltet.

Land	**Har/har ikke ID-kort**	**Under planlegging**	**Lagring av biometrisk personinforma-sjon**	**Innlevering av søknad ved utenriks-stasjoner?**	**Merknader**
Belgia	Ja		Ja		
Danmark	Nei	Off. utvalg utreder om Danmark skal arbeide videre m/etablering av ID-kort			
Estland	Ja		Nei, men kortet inneholder chip hvor persondata bortsett fra foto og signatur lagres	Nei	
Finland	Ja		Nei	Nei, men det er under vurdering	
Frankrike	Ja		Nei, men under planlegging (chip m/digitalt ansiktsfoto og fingeravtrykk)	Ja	
Hellas	Ja				Har ikke mottatt info., men er kjent med at Hellas har nasjonalt ID-kort
Irland	Nei				
Italia	Ja		Ja	Nei	
Kypros					Har ikke mottatt info.
Latvia	Nei	Startet arbeid i 2002, men ble stanset. Gjenopptas etter implementering av nytt pass aug. 2006			
Litauen	Ja		Nei		

Land	Har/har ikke ID-kort	Under planlegging	Lagring av biometrisk personinforma-sjon	Innlevering av søknad ved utenriks-stasjoner?	Merknader
Luxemburg					Har ikke mottatt info.
Malta					Har ikke mottatt info.
Nederland	Ja		Ja	Ja, ved ambassader og konsulater i land som godtar nasjonalt ID-kort som reisedokument	
Portugal	Ja		Pilotprosjekt med elektroniske ID-kort i løpet av 2006	Ja	
Polen	Ja		Nei		
Slovakia	Ja		Ja	Nei	
Slovenia	Ja		Nei		
Spania	Ja		Ja		
Sverige	Ja		Ja	Ja	
Tsjekkia	Ja		Nei	Nei	
Tyskland	Ja		Nei, men under planlegging	Ja	
Ungarn	Ja		Nei	Nei	
UK	Nei	Utstedelse fra 2008/2009		Nei	
Østerrike	Ja		Nei	Nei	

5 BEHOVET FOR IDENTIFISERING

5.1 Generelt

Det foreligger i Norge ingen alminnelig plikt til å legitimere seg, eller å ha med seg legitimasjonsdokumenter. Behovet for å legitimere seg knytter seg ofte til muligheten for utnyttelse av personlige rettigheter. Dette kan gjelde både i forhold til offentlige og private institusjoner, f.eks. i forbindelse med utbetaling av trygdeytelser, eller for å ta ut penger fra bankkonto. Hvis rettighetshaveren ikke er kjent av den som skal prestere en ytelse, må det i de fleste situasjoner anses som rettmessig å kreve fremlagt legitimasjon for at tjenesteleverandør skal prestere ytelsen med befriende virkning. I ansettelsesforhold vil det kunne fremstå som både en rett og en plikt å kunne bekrefte egen identitet, f.eks. for å få adgang til bygning (adgangskort). Tilsvarende vil rettigheter som følge av medlemskap i en forening kunne utnyttes utelukkende mot fremvisning av en gyldig legitimasjon.

I enkelte situasjoner er det imidlertid slik at rettigheter knyttes til et ihendehaverdokument, f.eks. en kinobillett eller billett til transportmiddel. Utgangspunktet her er at vedkommende rettighetshaver ikke har noen plikt til å legitimere seg for å gjøre gjeldende rettigheten, f.eks. å gå på bussen. Hvis rettigheten likevel kan knyttes til alder (ulik pris for ungdom og pensjonister), medlemskap eller annen tilhørighet (student på X-universitetet), vil det likevel kunne være rettmessig å kreve fremlagt legitimasjon.

Ved utlevering av en ytelse ved kontantkjøp, vil heller ikke den som utleverer en vare kunne kreve legitimasjon fra mottaker, det vil si at mottaker kan forbli anonym. Viktige unntak gjelder der myndighetene har fastsatt krav om aldersgrense, f.eks. ved salg av tobakk eller alkoholholdige drikkevarer, eller krav om at vedkommende kjøper skal registreres, f.eks. ved kjøp av bil eller skytevåpen, eller der kjøper av kontantkort til mobiltelefoner skal registreres som bruker.

Lovgivningen inneholder også på andre områder krav om at kunder fremlegger legitimasjon. Typisk for utviklingen på området er i så måte kravet som nå er pålagt finansinstitusjoner om å kreve fremlagt gyldig legitimasjon av kunden ved etablering av kundeforhold, dette med formål å forbygge hvitvasking av penger. Hvitvaskingsregelverket strekker seg imidlertid lengre enn til denne typiske situasjonen.

I enkelte situasjoner forutsetter utøvelse av rett i henhold til identitetsdokumenter at dette er utstedt av offentlig myndighet. Slike forhold vil som regel være forankret i lovgivningen. Et typisk eksempel er førerkort som dokumenter rett til å føre motorvogn. Pass står på mange måter i en særstilling i det pass som regel er nødvendig for å kunne reise inn i andre land, og vil bli krevd fremlagt for verifisering av identitet i grensekontroller.

5.2 Identifisering og verifisering av identitet

En persons identitet er et sett med attributter som til sammen danner en unik referanse til en bestemt fysisk person. Historisk har det i flere land vært slik at identiteten ble knyttet til et egennavn kombinert med referanse til fars navn. Sammen med fødselsdato kunne dette gi en unik identitet som dekket behovet for å knytte vedkommende til rettsforhold som f.eks. eiendomsrett og arv. Hvis identiteten skulle ha betydning utenfor lokalsamfunnet, kunne det i tillegg f.eks. brukes en referanse til fødested eller bosted.

I vår moderne tidsalder er det blitt behov for i mange sammenhenger å utvikle måter å fastsette og verifisere identitet på som er enklere og sikrere å håndtere, og mer funksjonelle, blant annet

for bruk i elektroniske lagrings- og kommunikasjonssystemer. Et eksempel er Folkeregisteret, som inneholder en katalog over norske stasborgere og andre personer bosatt i Norge. Hver person gis en unik referanse ved hjelp av fødselsnummer.

Identifisering, det å fastslå en fysisk persons identitet, var ingen problemstilling i tidligere samfunn der alle kjente alle, og hvor folk som regel ble boende på samme sted fra fødsel til død. I det moderne samfunn, preget av mobilitet, vil muligheten for å gjøre gjeldende sine rettigheter i "fremmede" omgivelser, ofte avhenge av at man er i stand til å få bekreftet identiteten. Også i forhold til offentlige myndigheter, f.eks. som reisende i andre land, som skattebetaler og som stemmeberettiget, er det flere og flere situasjoner i hverdagslivet som krever fremleggelse av identifikasjonsdokumenter, ofte etter særskilte lovbestemte krav. Det er ikke uvanlig at det i forbindelse med verifisering av identiteten ofte også foretas en registrering av den transaksjonen der identitetsverifikasjon var involvert (eksempelvis ved mottak av et pengebeløp eller ved en grensekontroll).

Kravene til sikker identifisering (og verifisering) vil variere innenfor ulike bruksområder. Der det skal gis tilgang til svært sensitive områder, som f.eks. et hemmelig forsvarsanlegg, vil det stilles strenge krav til identifisering av autorisert personell, mens det neppe vil være særlig store krav til verifisering for å få adgang til subsidiert mat på en studentkantine. Der identifiseringen knyttes til bruk av et ID-kort, er det imidlertid viktig at ektheten (det vil si rett person mot rett identitet) er avhengig av identitetskontrollen ved utstedelsen (eng. enrolment). En senere sikker verifisering (kontroll av ID-kortet mot innehaveren) vil ikke kunne reparere slike feil. Der et ID-kort blir benyttet som utgangspunkt for utstedelse av andre ID-kort, vil feil i opprinnelig identitetsfastsettelse bli videreført, og kan i enkelte situasjoner være fatale. (Et eksempel på dette vil være der en bevisstløs person blir lagt inn på sykehus for akutt medisinsk behandling, og blir utsatt for feilbehandling ved forveksling av den elektroniske legejournalen til en annen person.)

Mens lovgiver på stadig flere områder har stilt krav om identifisering er det sjelden at innholdet i dette kravet blir konkretisert. Dette etterlater ofte usikkerhet med hensyn til gjennomføringen. Som regel vil private aktører som skal etterleve påbudet, måtte benytte seg av eksisterende ID-løsninger, eventuelt basere utstedelse av nye ID-kort på en dokumentasjon som kan bestå av tidligere utstedte ID-kort.

En typisk situasjon i så måte er der bransjen for sikker identitetskontroll ved utstedelse av bankkort med ID, tar sikte på å kreve fremlagt pass ved utstedelse av slike kort etter 1. mars 2007.

At passet har fått en særlig status ved verifisering av ID, herunder for utstedelse av nye ID-kort, er forståelig ut fra de grunnleggende krav til *sikker identifisering ved utstedelsen*. Dagens pass er dessuten utformet med sikte på å gjøre dem robuste mot *forfalsking eller endring*. I tillegg kommer nye teknologiske løsninger for *sikker verifisering* gjennom bruk av biometrisk personinformasjon. Bruken av denne teknologien for verifisering av identitet er imidlertid begrenset til bruk i grensekontroll.

5.3 Særskilte krav til identifisering

Hvitvasking

Hvitvaskingsloven § 5 bestemmer følgende: "Rapporteringspliktige[10] skal ved etablering av kundeforhold kreve gyldig legitimasjon av kunden. Plikten gjelder også for den

[10] hvitvaskingsloven § 2 nr. 1, jf. § 4

rapporteringspliktiges ansatte. Som gyldig legitimasjon regnes alltid fysisk legitimasjon." I hvitvaskingsforskriften § 4 om krav til legitimasjon angis det nærmere blant annet: "Legitimasjonsdokumenter skal være utstedt av offentlig myndighet, eller av annet organ som har betryggende kontrollrutiner for dokumentutstedelse og det er allment akseptert at dokumentet for øvrig har et tilfredsstillende sikkerhetsnivå." Det kreves normalt personlig oppmøte ved etablering av kundeforhold.[11] Se også kapittel 4.2.3 annet avsnitt.

Luftfart

EØS-basert regelverk[12] stiller blant annet krav om at innsjekket bagasje ikke skal tas ombord i et luftfartøy uten at det er truffet tiltak om at "…*den passasjer som bagasjen tilhører, skal være innsjekket til flygningen som bagasjen skal medføres på*,…".[13] Formålet med bestemmelsen er å unngå at passasjerer sender kofferter og lignende fylt med f.eks. eksplosiver, uten selv å følge med på flyet. Siden 1. juli 2005 har Luftfartstilsynet stilt krav om at passasjerer må vise legitimasjon sammen med billetten ved *utenriksflygninger*. EU-Kommisjonen anser at kravet om ID-sjekk også gjelder for innenriksflygninger. Det ble 2. januar 2007 vedtatt et midlertidig opplegg for ID-legitimasjon for innenriksflygninger. Ordningen trer i kraft 1. mars 2007.

Konsekvensene ved ikke å ha en ordning med ID-kontroll er at Norge kan få såkalt "avvik"[14] som følge av manglende oppfyllelse av kravet om passasjer og bagasjegjenforening. Det vil si at hvis EFTAs overvåkingsorgan, EFTA Surveillance Authority (ESA) under inspeksjoner på norske lufthavner avdekker at ovennevnte regelverk ikke er gjennomført for innenlands flytrafikk, vil det måtte rapporteres til EU-Kommisjonen. I verste fall kan det føre til at flytrafikk fra Norge til andre EU-land kan bli separert fra andre passasjerer ved ankomstlufthavnene. Det kan påføre kostnader for flyselskapene og forsinkelser med mer for passasjerene.

Følgende ID-kort - med navn og bilde - er vurdert som akseptable for flyselskaper:

- Norske pass
- Reisedokument for flyktninger, utstedt av norske myndigheter
- Norsk bankkort
- Norsk førerkort
- Politiets tjenestebevis
- Forsvarets ID-kort
- Luftfartstilsynets ID-kort
- Avinors ID-kort

Når det gjelder barn under 16 år som reiser alene, finner Luftfartstilsynet det urimelig å kreve pass. Det er for øvrig heller ikke mange barn som sjekker inn bagasje alene. For barn ifølge med voksne, anses det tilstrekkelig at ledsageren fremviser ID-kort ved innsjekkingen av bagasje. En person som reiser uten innsjekket bagasje behøver ikke å vise ID-kort.

---

[11] Se også Kredittilsynets veiledning til Hvitvaskingsforskriften (Kredittilsynets rundskriv 9/2004)

[12] Det vises til forskrift av 30. april 2004 nr. 715 om forebyggelse av anslag mot sikkerheten i luftfarten, jf. Europaparlaments- og rådsforordning (EF) nr. 2320/2002 om fastsettelse av felles bestemmelser om sikkerhet i sivil luftfart, vedleggets pkt. 5.1 Tilknytning mellom passasjer og innsjekket bagasje.

[13] EU-Kommisjonen har i forbindelse med sine inspeksjoner i EU-landene tolket nevnte krav slik at tilknytningen mellom passasjer og bagasje i første rekke skal sikres gjennom fremvisning av ID-kort.

[14] Jf. Kommisjonsforordning (EF) nr. 1486/2003 av 22. august 2003 om fastsettelse av fremgangsmåter for gjennomføring av kommisjonens inspeksjoner av sikkerhet i sivil luftfart, jf. § 3 nr. 4 i forskrift av 30. april 2004 nr. 715 om forebyggelse av anslag mot sikkerheten i luftfarten.

5.4 Følger av manglende evne til å identifisere seg

Manglende evne til å kunne identifisere seg, eller verifisere sin identitet, vil kunne resultere i at vedkommende ikke får utnyttet sine rettigheter. Mangel på egnet ID-kort vil f.eks. kunne føre til at det ikke er mulig å hente rekommandert verdipost. Uten pass vil man bli avvist ved de fleste grenser. I dag vil de fleste flyselskaper kontrollere om passasjerene har pass før de tillates å gå om bord på utenlandsflygninger. Med andre ord vil muligheten for å fremlegge dokumentasjon på identitet være et absolutt krav. Etter omstendighetene vil det dessuten være særskilte krav til dokumentasjonen, jf. f.eks. pass som grunnlag for å reise inn i andre land.

Kravet til identifisering kan gå på bekostning både av retten til anonymitet, samt det å ikke ville etterlate spor. En slik utvikling må motvirkes gjennom informasjon og bevisst håndhevning av personvernrettighetene.

5.5 Forholdet til anonymitet

Retten til anonymitet er en viktig del av personvernet. Det sentrale innhold i denne rettigheten er å kunne ferdes i det offentlige rom uten å måtte tilkjennegi identitet. Dette innebærer også retten til å ferdes anonymt på Internett. Retten til anonymitet må imidlertid holdes opp i mot behovet for, eller retten til, å kunne identifisere seg når man skal gjennomføre en rettskraftig disposisjon eller gjøre rettigheter gjeldende. Identifiseringsbehovet må ses opp mot behovet for å beskytte seg mot at andre misbruker ens identitet eller rettigheter. På Internett kan bruk av elektronisk identitet - eID - etterlate seg spor som i ekstreme tilfeller kan gjøre det mulig å rekonstruere en persons handlinger og kartlegge hva slags tjenester personen benytter på nettet og til hvilke formål. Dette kan forebygges ved streng håndheving av retningslinjer for bruk av eID til autentisering i ulike nettjenester, jf. kap. 12.3. Samtidig kan eID-teknologien skape muligheter for å opptre under pseudonym, slik at kun aktuelle egenskaper ved personen blir gjort kjent for tjenesten, mens den egentlige identiteten forblir skjult. Et eksempel på slik bruk av elektronisk identitet kan være pålogging til chattetjenester, der det er av betydning hvilket kjønn og alder personen har, mens vedkommende ikke behøver å opplyse sitt egentlige navn. Avansert bruk av eID kan sikre at identiteten til personen kan kontrolleres, men bare kjønn og alder blir oppgitt til selve tjenestetilbyder. På denne måten kan brukere av tjenesten være sikre på at ingen "seiler under falskt flagg" samtidig som man bevarer anonymiteten til deltagere.

6 BRUK AV URIKTIG IDENTITET

6.1 Innledning

Formålet med dette kapitlet er å gi et bilde av bruk av uriktig identitet som samfunnsproblem, herunder ulike former for ID-tyveri og utilsiktet bruk av uriktig identitet, samt oversikt over tap av ID-dokumenter. Det vil også bli gitt en beskrivelse av konsekvensene ved å bruke uriktig identitet.

6.2 Generelt

ID-tyveri eller ID-bedrageri er å benytte en annens personlig identitet for å oppnå en uberettiget vinning eller status. De vanligste tilfellene er knyttet til det å få uberettiget tilgang til finansielle midler, erverve materielle verdier eller få tilgang på informasjon og benytte informasjon som kan true andre eller utnyttes til bedrageri, illegal innvandring, terrorisme, spionasje etc. Personlig identitet har tidligere i stor grad blitt stjålet gjennom tap av førerkort og pass. Forfalskning av utstedte pass, eller produksjon av falske pass er fortsatt en betydelig utfordring på verdensbasis. Misbruk av norske pass inngår i denne kriminelle virksomheten. I de senere år har kriminelle i tillegg utviklet nye metoder for å stjele identiteten til andre. Dette er i større grad kommet gjennom fysisk tap av elektroniske betalingskort, tap av kreditkortinformasjon via internett, datainnbrudd i datamaskiner i banker og kreditinstitusjoner, tap av personinformasjon i ulike databaser og PC'er på internett.

6.3 Former for ID-tyveri

ID - tyver kan få tilgang til personinformasjon gjennom forretningsvirksomhet og offentlig virksomhet på ulike måter, som f.eks. ved å:

- stjele informasjon på eget arbeidssted,
- få arbeidstakere på et sted til gi fra seg slik informasjon,
- foreta en uautorisert tilgang /datainnbrudd på bedriftens eller institusjonens datasystemer,
- stjele personlig informasjon og bankinformasjon gjennom falske tilsendte epost og telefonoppringninger. Falske representanter for firmaer og offentlige institusjoner tapper en for personlig eller forretningsmessig informasjon som senere kan utnyttes til svindel (phishing),
- få tilgang til informasjon fra søppelkasser hvor det er kastet regninger, persondatainformasjon etc,
- stjele betalingskortopplysninger gjennom å feste en kortleser og kamera utenpå f.eks. minibanken slik at opplysninger i kortet kopieres i et nytt kort eller misbrukes på annen måte (skimming),
- stjele ID-informasjon over internett gjennom å gjøre datainnbrudd på datamaskiner. Sårbarheten i datasystemene utnyttes ved at det innplasseres trojanske programmer som kan rapportere personinformasjon og bankinformasjon til kriminelle uten at brukeren av datamaskinen vet om det.

6.4 Tap av ID-dokumenter

Et ID-dokument er et personlig dokument. ID-dokumenter på avveie vil kunne åpne for misbruk av annens identitet, både fysisk og i den elektroniske verden. Omfanget av *misbruk* av tapte pass og bankkort er usikkert. Det er kjent at in blanco passblanketter har kommet kriminelle miljø i hende.

Tapte pass

I 2006 ble det meldt 23.238 pass tapt. Tallene fordelte seg som følger:

- Bortkommet i posten: 210
- Stjålet: 1302
- Tapt: 21.643
- Ukjent: 83

Tap av pass kan medføre ulike former for misbruk. Pass på avveie kan brukes til "look alike" misbruk ved at passet benyttes av en som ligner innehaveren. Det er kjent at denne metoden er benyttet for urettmessig innreise til Norge. Videre kan pass på avveie forfalskes ved at opplysningene i personaliasiden, f.eks. bilde og eventuelle øvrige personopplysninger, endres. Personopplyninger i passet kan også benyttes til å etablere en ny identitet for den som har passet i hende.

Tapte (mistet/stjålne) bankkort

Tall fra BBS (Bankenes betalingssentral) viser at det de senere år er sperret mellom 90.000 og 119.000 bankkort årlig. I tillegg sperrer bankene kort direkte. Det skilles ikke på mistet/stjålne kort. Det skal imidlertid her gjøres oppmerksom på at sperringen i utgangspunktet gjelder bruken av en bankkonto. Det er derimot vanskeligere å sperre uvedkommendes bruk av bankkortet som ID-kort på en effektiv måte.

6.5 Følgene av å bruke uriktig identitet

Som regel vil bruk av uriktig identitet skyldes bevisste handlinger, ofte i forbindelse med gjennomføring av kriminalitet. Bruk av uriktig identitet kan imidlertid også skyldes utilsiktede handlinger. Dette vil være situasjonen der det ved en feil blir registrert uriktig identitet på person, f.eks. ved en kontroll eller ved inngåelse av en avtale. For den som bevisst benytter uriktig identitet vil konsekvensen som regel være straffeansvar, eventuelt også erstatningsansvar overfor den som har lidt rettstap.

Følgene for den hvis identitet er misbrukt vil kunne variere. I mange situasjoner vil det imidlertid innebære at vedkommende har fått etterlatt sine "spor", med det potensial som ligger i fremtidige rettstap eller krenkelse av personvernet. I ytterste fall vil det kunne føre til mistanke om straffbare handlinger. Det typiske i dag er imidlertid trusselen om tap gjennom kontobedragerier. Dette utgjør i dag en av de største trusler mot tilliten i elektronisk handel.

7 NASJONALT ID-KORT SETT OPP MOT FREMTIDIGE KRAV TIL IDENTIFISERING

Formålet med dette kapitlet er å beskrive fremtidige krav til identifisering som et grunnlag for vurderinger og forslag til nytt nasjonalt ID-kort.

7.1 Generelt

Dagens utvikling i retning av økt misbruk av identitetsdokumenter, samt nye krav til sikker identifisering, gjør at det kontinuerlig utvikles nye løsninger for identifisering. Den teknologiske utviklingen gjør at vi ser en dreining mot stadig mer avanserte løsninger og krav til sikker identifisering.

Løsningen for nasjonalt ID-kort bør så langt som mulig kunne imøtekomme fremtidige krav til identifikasjon, verifikasjon og brukervennlighet. Kortløsningen bør derfor allerede ved innføringen kunne utvides til å implementere ulike teknologiske løsninger.

Det vil imidlertid være en fremtidig vurdering om og når de ulike alternativene skal implementeres i kortet.

Arbeidsgruppen har derfor sett nærmere på hvilke fremtidige krav kortløsningen bør ta høyde for.

7.2 Legitimasjonskrav ved utstedelse av bankkort

På grunn av stadig mer svindel og ID-tyverier, opplever bankene større utfordringer forbundet med identitet og verifikasjon enn tidligere. Det blir stadig flere som forsøker å skaffe seg falske identiteter, eller stjele andres identitet, samtidig som "godkjente" legitimasjonsdokumenter ofte utstedes på svakt grunnlag. Fra 1. mars 2007 vil derfor bankene ha et separat krav om legitimering med pass i tilknytning til utstedelse av bankkort med legitimasjon til nye kunder. Etablering av kundeforhold skal imidlertid skje i henhold til kravene i hvitvaskingsregelverket, og i tråd med Kredittilsynets anbefalinger der tilsynet også utpeker legitimasjonsdokumenter som må anses å oppfylle kravene.[15]

7.3 Førerkort

Den 19. desember 2006 ble det vedtatt et nytt førerkortdirektiv i EU. Direktivet skal gjennomføres i norsk rett. Direktivet pålegger blant annet utfasing av førerkort av eldre modeller i papp, og med dette også en forsering av overgangen til førerkort av den "kredittkorttype" som Norge har benyttet i noen år. Videre innføres det administrativ gyldighet på 10 år for lette klasser (A+B) og 5 år for tyngre klasser (C+D). I tillegg vil helsekravene bli skjerpet for enkelte særlige grupper som da vil kunne få førerkort med gyldighet helt ned til ett år. Begrensning i gyldighet finnes i dag i hovedsak kun for enkelte førerkortklasser for tyngre kjøretøy.

Innføringen av det nye harmoniserte førerkortet i det nåværende EØS-området vil ha betydning både i forhold til muligheten for å forfalske førerkort og som tiltak for å hindre at personer har

[15] Jf. Kredittilsynets rundskriv 9/2004 "Veiledning til ny lov og forskrift med tiltak mot hvitvasking av utbytte fra straffbare handlinger mv."

førerkort fra mer enn en stat. Direktivet åpner imidlertid for en lang gjennomføringstid, slik at medlemsstatene forpliktes til å utstede alle nye førerkort i nytt format fra 2012. Alle førerkort i EØS-området skal være byttet til ny harmonisert modell innen 2032.

7.4 Sjøfolks identitetsbevis (SID) etter ILO-konvensjon 185

Sjøfolks identitetsbevis (SID) er ikke et reisedokument, men sammen med pass er det tenkt å lette transitt for sjøfolk. Det skal ikke kreves visum ved landlov hvis sjøfolkene har et SID.

Kortet kan kontrolleres av f.eks. havnemyndigheter og immigrasjonsmyndigheter med en leser mot sjømannens fingeravtrykk (fingeravtrykket skal gjøres om til en tallrekke i en strekkode som lagres i kortet). Dersom det i kontrollen er noe som ikke stemmer kan kontrollmyndigheten kontakte en nasjonal database for å få kortet verifisert.

Bakgrunnen for denne ILO konvensjonen er terroraksjonen i USA 11. september 2001. Man ønsker en strengere kontroll av personer om bord, ved landlov og reise. Videre er skipsfart en internasjonal virksomhet som krever rask transitt. Landlov ses som en viktig del av arbeidsmiljø, helse og sikkerhet for sjøfolkene.

Norge har ikke ratifisert ILO-konvensjon 185, men det arbeides mot utstedelse av et første SID i 2008. Det er ikke bestemt hva som skal kreves ved søknad om SID, men det kan bli politiattest sammen med pass. SID skal også inneholde navn, kjønn, fødselsdato og fødested, høyde, foto og signatur, samt biometrisk tallkode av fingeravtrykk. SID vil antagelig ha bankkortstørrelse.

EU har vedtatt at alle land i Schengen-samarbeidet nå fritt kan ratifisere ILO-konvensjon 185, men de går ikke inn for en felles ratifikasjon.

7.5 Legitimasjonskrav innenfor luftfartsområdet

Den 2. januar 2007 vedtok Samferdselsdepartementet en ny bestemmelse (§ 36 a) [16] om ID-kontroll av passasjerer som sjekker inn bagasje. Bakgrunnen for forslaget til ny bestemmelse er krav i forordning (EF) nr. 2320/2002 om at innsjekket bagasje ikke må tas med ombord i luftfartøyet, med mindre den passasjeren som bagasjen tilhører er sjekket inn til samme flygning. Kravet om tilknytning mellom passasjer og innsjekket bagasje er tradisjonelt løst gjennom kontroll av at antall boardingkort stemmer med passasjerlisten (boardingkortkontroll.) EU-kommisjonen og EFTA Surveillance Authority (ESA) har gjennom inspeksjoner påpekt at luftfartsselskapenes boardingkontroll ikke alene er tilstrekkelig til å oppfylle forordningens krav, ved at det er en mulighet for at noen andre enn den som har sjekket inn bagasjen overtar boardingkortet og går ombord på flyet. Innføring av ID-kontroll er ment å fjerne denne muligheten. Bestemmelsen omhandler kun tilfelle der passasjerer sjekker inn bagasje. I brev av 4. desember 2006 til SD opplyser Luftfartstilsynet at høringsinstanser har påpekt økning i arbeidsmengde og kostnader, samt risiko for forsinkelser ved en del lufthavner pga slik kontroll.

---

[16] § 36a i forskrift av 30. april 2004 nr. 715 om forebyggelse av anslag mot sikkerheten i luftfarten - ID-kontroll av passasjerer som sjekker inn bagasje

(1) Passasjerer skal forevise dokumentasjon av identitet ved innsjekking av bagasje og i forbindelse med ombordstigning. Identifikasjonsdokumenter må minst inneholde navn, bilde og fødselsdato. Luftfartsselskapet skal sjekke samsvar mellom billett eller boardingkort og fremlagt dokumentasjon.

(2) Mindreårige som reiser sammen med andre trenger ikke å forevise dokumentasjon av identitet, men identifiseres av medreisende passasjer.

(3) Luftfartsselskapet kan etablere alternativer til ID-kontrollen nevnt i første ledd, dersom kontrollhensynet kan ivaretas på annen betryggende måte

Det er anmodet om at det bør tilrettelegges for bruk av biometriske kjennetegn i forbindelse med ID-kontrollen, f.eks. fingeravtrykk.

For å lette gjennomføringen av ID-kontrollen på lufthavnene, vil forskriften tre i kraft 1. mars 2007. Det anses viktig at det gjennomføres omfattende informasjonstiltak overfor dem som blir berørt av nyordningen.

7.6 Oppholdskort for utlendinger

Dagens etikettbaserte Schengenstandardiserte oppholds- og arbeidstillatelser skal erstattes med et Schengenstandardisert oppholdskort. Oppstartsdato for de nye kortene er ikke fastsatt, men det antas at slike kort vil være i bruk i slutten av 2008. Kortet skal inneholde biometri lagret i en RFID-brikke og vil ha høy sikkerhet mot forfalskning. Opptak av biometri og prosedyre for utstedelse er ikke avklart, men det antas at dette vil bli utført av politiet i politidistriktene. Selve personaliseringen av kortene vil sannsynligvis skje sentralt. Kortet vil ikke bli brukt som identitetskort alene, men sammen med pass og reisdokumenter (reisebevis for flyktninger eller utlendingspass).

Dersom Norge gjennomfører EU direktiv 2004/38 vil det medføre en *plikt* for norske myndigheter til å utstede et *oppholdskort* til familiemedlemmer av EU borgere som er tredjelands borgere (Residence card of a family member of a Union Citizen).

7.7 Krav om ID-kort for deltakelse på byggeplasser

Arbeids- og inkluderingsdepartementet arbeider med innføring av en statlig brukerfinansiert ID-kort-ordning for bygge- og anleggsbransjen. En slik ordning er et tiltak som kan bidra til ordnede lønns- og arbeidsvilkår for alle, og er ledd i Regjeringens handlingsplan mot sosial dumping. Plikten til å utstyre arbeidstakerne med ID-kort legges på arbeidsgiver. Kortutstedelse vil bero på en kontroll av at virksomheten har foretatt lovpålagte registreringsplikter i relevante offentlige registre. Det er foreslått at ID-kortet skal inneholde følgende opplysninger: navn på kortinnehaveren, fotografi av kortinnehaveren, fødselsdato og kjønn, kortinnehaverens signatur, gyldighetsperiode, kortnummer, navn på arbeidsgiver eller enkeltpersonsforetak, organisasjonsnummer for registreringspliktige virksomheter, navn og adresse til utsteder av kortet. Forslag til forskrift om identitetskort på bygge- og anleggsplasser er nå på høring med frist 10. februar 2007. Det legges opp til at de nye ID-kortene skal tas i bruk høsten 2007.

7.8 Krav om ID-kort ved reise innen Schengen

Implementering av Schengen-avtalen fra mars 2002 innebar at grensekontrollen mellom alle Schengenland opphørte. Dette medførte at det ikke lenger var behov for pass som *reisedokument.* Etter Schengen-regelverket er det imidlertid oppstilt et krav om at reisende fra andre Schengenland skal kunne være i stand til å identifisere seg med et ID-dokument utstedt av myndighetene, og som viser vedkommendes statsborgerskap[17]. Slik legitimasjon var blant annet forutsatt å skulle benyttes på hoteller og andre overnattingssteder.

Siden Norge ikke har hatt annet identitetsdokument enn pass som fyller kravene for myndighetsutstedt identitetsdokumentasjon, har norske myndigheter konsekvent rådet alle som reiser innen Schengen å bringe med pass. Flere av Schengenlandene har imidlertid ID-kort som

[17] Dette blir også i rapporten omtalt som Schengenfunksjonalitet

fyller kravene etter Schengen-regelverket, og EU er for tiden i ferd med å utvikle standarder for EU/Schengen borgeres ID-kort, som blant annet vil innebære at det åpnes for å legge inn informasjon i en kontaktløs brikke, herunder med biometrisk informasjon for elektronisk verifisering av identiteten. Disse standardene vil medføre en harmonisering til kravene til EU/Schengen landenes krav til pass. Disse er igjen basert på ICAOs tekniske spesifikasjoner for pass (og for ID-kort som er under utarbeidelse).

DEL II

8 NASJONALT ID-KORT

Formålet med dette kapitlet er å drøfte om det er behov for et nasjonalt ID-kort, hvem som eventuelt bør utstede det, og rammene rundt et eventuelt kort.

8.1 Behov – basis identifikasjonskort, Schengenfunksjonalitet, eID

I dag utsteder offentlige myndigheter ingen kort til alminnelig identifiseringsformål. Både private og offentlige aktører utsteder imidlertid kort med personinformasjon for å kunne understøtte kontroll av identitet der det anses som en nødvendig del av kortbruken. Slike kort blir ofte benyttet for alminnelige identifiseringsbehov utenfor det formålet kortet er utstedt for. Dette gjelder f.eks. førerkort og bankkort.

I Norge foreligger det ingen alminnelig plikt til å legitimere seg, eller å ha med seg legitimasjonsdokumenter, jf. kap. 5.1. I et moderne samfunn vil det likevel ofte være nødvendig å kunne dokumentere sin identitet for å kunne utnytte sine rettigheter, jf. kap. 5.2 og 5.3, f.eks. bevise alder, gis adgang til områder underlagt restriksjoner, og for å kunne utføre økonomiske transaksjoner. Dette kan gjelde i forhold til offentlige myndigheter eller private aktører. Flere situasjoner krever fremleggelse av identifikasjonsdokumenter, ofte etter særskilte lovpålegg. Et funksjonelt og sikkert ID-kort vil således være viktig for de fleste. Pass kan brukes som identitetskort selv om dets primære funksjon er å være et reisedokument. Passet har imidlertid et upraktisk format. Videre er det dyrt og det mangler funksjonalitet som eID. Det er også grunn til å nevne at ikke alle kan få pass, og en større del av den norske befolkning har ikke pass.

Sikker identifisering er viktig av flere grunner. Misbruk av identitet er en alvorlig trussel mot personvernet, og ID-kort som er vanskelige å forfalske antas å redusere mulighetene for misbruk av identitet (identitetstyveri) og dermed krenkelse av personvernet.

Mange er i dag utstyrt med flere ID-kort for å dekke ulike behov. Et eget nasjonalt ID-kort, som godtas av alle for alminnelige identifiseringsformål, vil kunne gi økt brukervennlighet og derved begrense behovet for å ha mange forskjellige ID-kort. Dagens forskjellige kort er av ulik kvalitet både med hensyn til kontroll av identitet ved utstedelse og innebygde sikkerhetselementer for å motvirke forfalskning av kortet eller misbruk av identiteten.

Kvaliteten på et ID-kort vil særlig være avhengig av kontroll med identitet ved utstedelse. En senere kontroll av kortet mot innehaveren vil ikke kunne reparere feil begått ved identitetsfastsettelse ved utstedelse. Et ID-kort kan også bli brukt som grunnlag for utstedelse av andre ID-kort. Feil i opprinnelig identitetsfastsettelse vil da bli videreført.

Krav til sikker identifisering er økende, bl.a. med bakgrunn i den økende sårbarhet på viktige samfunnsområder. Økt mobilitet både nasjonalt og over landegrenser gjør at identifisering ikke lenger kan baseres på personlig kjennskap. "Alle" kjenner ikke lenger "alle", slik som var regelen i tidligere tiders stabile lokalsamfunn. Dette åpner nye muligheter for de som ønsker å utnytte mulighetene til kriminelle handlinger under dekke av en annen identitet. Samtidig har en rivende teknologisk utvikling gjort det mulig med forholdsvis enkle midler å fremskaffe gode

forfalskninger av forskjellige typer dokumenter, også identitetsdokumenter. Over tid er det utviklet et illegalt marked for falske identitets- og reisedokumenter, som f.eks. falske pass, førerkort og bankkort. Opprettholdelse av trygghet og tillitt i en rekke situasjoner vil derfor avhenge av at man etablerer sikre metoder for verifisering av identiteten til den enkelte.

Smidig, rask, effektiv og tillitsbasert samhandling er kjennetegn på et moderne samfunn. Kunnskap om personers riktige identitet er en viktig forutsetning for både et velfungerende næringsliv og offentlige myndigheters virksomhet.

På grunn av et endret trusselbilde med en økt terrortrussel er det også grunn til å nevne samfunnssikkerhet og betydningen av sikker identifisering. På en rekke områder, blant annet innen luft- og skipsfart, har det som en følge av terrortrusselen blitt innført skjerpede krav til identitetskontroll, se kap. 4.2 og 5.3.

Flere utstedere av identitetskort opplever det i dag som en vanskelig utfordring å knytte rett person til rett identitet (kontroll av ekthet/autentisitet). Sparebankforeningen har i en presentasjon for arbeidsgruppen opplyst at usikkerheten rundt en persons identitet kan være så stor at de fra 1. mars 2007 innfører krav om pass som grunnlagsdokumentasjon for å få utstedt et bankkort med legitimasjon til nye kunder. Dette vil for det første kunne medføre en ekstra kostnad for de som ikke har pass, og i tillegg vil det også ramme en gruppe som ikke har mulighet til å få pass.

I en situasjon hvor det er lett å skaffe seg forfalskede identitetsdokumenter, og hvor det samtidig på flere områder stilles krav til identifisering, vil det være særlig viktig å ha et kvalitativt godt dokument som kan stadfeste en persons identitet og som ikke lett lar seg forfalske. Det er i dag en situasjon med utstedelse av mange ulike kort med varierende og usikre rutiner rundt kontroll av ekthet.

Mulighetene til å forfalske et kort, eller til å produsere et uekte kort, vil i stor grad avhenge av hvilke sikkerhetselementer som bygges inn i kortet.

Arbeidsgruppen mener at det er behov for et nasjonalt ID-kort som et frivillig identifikasjonskort (”basis” ID-kort). Et slik kort bør dessuten utstedes med nødvendig Schengenfunksjonalitet. Dette vil øke kortets anvendelsesområde, i første rekke ved reise innen Schengen. ID-kort med slike funksjonaliteter må antas å ville bli akseptert som ID-kort i utlandet, herunder som reisedokument, og vil således avløse det tradisjonelle passet i en rekke sammenhenger. I tillegg ser arbeidsgruppen det alminnelige behovet for et kort med eID, og vil foreslå at det åpnes for at et nasjonalt ID-kort også inneholder en eID.

Elektronisk kommunikasjon over Internett har et betydelig potensial for effektivisering av offentlig sektor, forenkling av hverdagen for publikum og næringslivet og for økende innslag av elektronisk forretningsdrift i norske bedrifter. For å kunne oppnå det fulle effektiviseringspotensialet ved bruk av elektronisk kommunikasjon vil det ikke være nok med å ha tilgang til Internett, men det vil også være nødvendig å ha en eID/e-signatur som gjør det mulig å identifisere kommunikasjonspartnere på en sikker måte og inngå juridisk bindende avtaler med samme gyldighet som ved bruk av tradisjonell, papirbasert kommunikasjon.

I offentlig sektor er det gjennom arbeidet med ny strategi for elektronisk ID og -signatur identifisert behov for en høysikkerhets-ID, særlig for tilgang til offentlige tjenester med sensitive personopplysninger og der det er behov for signering av skjema ol. Nasjonalt ID-kort med eID vil kunne fylle dette behovet på en tilfredsstillende måte.

I privat sektor vil flere elektroniske tjenester ha behov for en sikker elektronisk identifikasjon, ikke minst i samband med finansielle tjenester. Nasjonalt ID-kort med eID vil kunne være en grunnleggende identifikasjonsmetode som gjør det mulig å etablere kundeforhold elektronisk, særlig der det stilles strenge krav til dokumentasjon av identiteten, som f.eks. i hvitvaskingsregelverket.

For å få en stor utbredelse av det nasjonale ID-kortet anbefaler arbeidsgruppen at kortet gis et så stort bruksområde som mulig. Det vil derfor være viktig at ID-kortet bl.a. kan brukes som gyldig legitimasjon innenfor bl.a. luftfartssektoren, samt at det ellers kan brukes som gyldig legitimasjon for utstedelse av andre legitimasjonsdokumenter som f.eks. bankkort og førerkort.

8.2 Offentlig utstedt kort

Hovedbegrunnelsen for å etablere et nasjonalt ID-kort er å legge til rette for at folk har et tilbud om å kunne dokumentere sikker identitet, mao knyttet til alminnelig behov for identifisering. Et nasjonalt ID-kort som har høy grad av tillitt mht. sikkerhet vil dessuten kunne fungere som et basiskort for utstedelse av alle andre ID-kort, som f.eks. bankkort eller førerkort. Dette vil kunne gi større sikkerhet i identifiseringsprosessen, samtidig som det vil forenkle arbeidet både for den som skal utstede et nytt ID-kort og for den som skal identifisere seg.

Sikker identifisering av personer og effektivitet i samhandling representerer betydelige samfunnsinteresser. Riktig identifisering er en kjerneoppgave for myndighetene, blant annet innenfor områder som berører samfunnssikkerhet. Sparebankforeningen har fremholdt at det er et myndighetsansvar å stille til disposisjon for næringslivet sikker identitet til en person.

En av de store utfordringene er å fastslå riktig identitet ved utstedelse av et ID-kort. Offentlige myndigheter har bedre kontrollmuligheter på dette feltet enn private aktører, bl.a. gjennom tilgang til ulike offentlige registre og kontakt med myndighetene i andre land. Personvernhensyn vil slikt sett også tale for at utstedelse av nasjonalt ID-kort legges til offentlig myndighet.

Ved å følge Schengenkravene vil det nasjonale ID-kortet kunne benyttes ved reise i Schengenland og dekke alle ordinære behov for å kunne identifisere seg, både overfor offentlig myndigheter og private institusjoner (f.eks. overnattingssteder og flyselskaper).

8.3 Nærmere om nasjonalt ID-kort

8.3.1 Generelt

Etablering av et nasjonalt ID-kort er ikke ment å endre dagens rettslige utgangspunkt om at det i Norge ikke foreligger noen alminnelig plikt til å legitimere seg, eller å ha med seg legitimasjonsdokumenter.

Kortet er kun ment som et tilbud til personer for at disse lett skal kunne identifisere seg når det foreligger et saklig behov. Slike behov kan blant annet følge av særskilte lovbestemmelser, og vil ikke bli behandlet nærmere her.

Anskaffelse av et ID-kort vil også naturlig måtte være frivillig. For å utnytte ulike brukerfunksjoner er det imidlertid en forutsetning at kortet baseres på internasjonale tekniske standarder for denne type kort, i tillegg til krav som må tilfredsstilles for å optimalisere sikkerhet og effektivitet ved kortbruken i ulike situasjoner.

8.3.2 Informasjon i nasjonalt ID-kort

Kortet skal ikke inneholde mer informasjon enn det som er nødvendig for en sikker identifisering. I tillegg kommer nødvendig informasjon for å administrere en ordning med ID-kort, som f.eks. kortnummer og informasjon om utstedelse. Informasjonen om kortinnehaver må være innhentet, kontrollert og sikret for å ivareta et absolutt krav til rett identitet (autentisitet) ved utstedelse, samt dernest lagret i kortet på en slik måte at den ikke kan endres (integritet). Dernest skal personinformasjonen i kortet sikres mot uautorisert bruk (konfidensialitet). Konfidensialitetskravet vil avhenge av hvor sensitive opplysningene er.

Kortets totale kvalitet – både vedrørende den informasjonen som lagres og de teknologiske løsningene som velges – bør være like høy som i passet. Dersom det velges et lavere sikkerhetsnivå vil tilliten til og utbredelsen av kortet lett reduseres. Ved å knytte kvaliteten på ID-kortet opp til gjeldende standarder vil løpende endringer i krav til opplysninger og teknologi fanges opp. Det er viktig for å forebygge forfalskninger og for å opprettholde tilliten til dokumentet.

Det kunne tenkes en ordning der ID-kortinnehaver selv kunne bestemme hvilke av de til enhver tid tilgjengelige/gjeldende sikkerhetselementer som skal være i kortet. En slik valgfrihet vil lett føre til usikkerhet knyttet til kvaliteten og derigjennom tilliten til kortene. For brukerne som får presentert et kort med begrensede sikkerhetselementer vil det kunne oppstå tvil om kortet er tilstrekkelig sikkert til formålet. I tillegg vil det også gjøre forfalskning og misbruk lettere fordi utvikling av sikkerhetsstandardene regelmessig er begrunnet i erfaring med at eksisterende sikkerhetselementer har latt seg forfalske. En slik ordning frarådes derfor innført.

Hvilken personinformasjon som lagres i kortet, og på hvilken måte, vil hele tiden være en avveining mellom på den ene siden behovet for informasjon for identifisering og sikkerhet i ulike brukersammenhenger, og på den andre siden blant annet ivaretakelse av personvernet. Kvaliteten i kortet vil i betydelig grad være et kostnadsspørsmål. I mange henseender trekker personvernhensyn og kvalitetskrav i samme retning. Misbruk av en persons identitet ved hjelp av et ID-kort vil være en krenkelse av personvernet. Samtidig er det viktig å finne riktig balanse mellom det som er nødvendig for en sikker identifisering og for å hindre misbruk. Normalt vil tilleggselementer i et kort styrke sikkerheten rundt identifisering og redusere faren for misbruk. Utilstrekkelig sikring av informasjon lagret i kortet, eller også uautorisert fjernavlesing av informasjon, vil være en krenkelse av personvernet. I tillegg kan det også åpne for misbruk av identitet og utstedelse av falske kort.

Det forutsettes etablert et register knyttet til utstedelse av ID-kort. Et register vil være nødvendig for å etablere en funksjonalitet i kortet for å verifisere gyldighet.

Følgende personinformasjon foreslås tatt inn i den visuelle delen av kortet:

1. Navn til kortinnehaver. Dette vil omfatte vedkommendes fulle navn slik dette er registrert i Folkeregisteret.
2. Fødselsnummer. Dette omfatter ved siden av fødselsdato et personnummer. Arbeidsgruppen har drøftet i kap. 9.7 nærmere om hele fødselsnummeret (dvs. fødselsdato og personnummer) skal inntas visuelt på ID-kortet, og har konkludert med at det ikke er tilstrekkelige grunner til ikke å ta med hele fødselsnummeret på ID-kortet, hensyn tatt til at fødselsnummeret i dag brukes i en rekke av dagliglivets situasjoner, både

ved kontakt mellom individ og offentlig myndighet, men også ved private rettshandler, overfor arbeidsgiver og banker mv.
3. Bilde. Dette vil utgjøre det sentrale element for verifisering av identitet.
4. Signatur. Signaturen er et viktig element ved verifisering der ID-kort benyttes ved økonomiske transaksjoner eller rettshandler som blir gjennomført ved signatur.
5. Høyde. Høyden på kortinnehaver representerer et enkelt verifiseringselement, som i noen situasjoner gjør det enkelt å oppdage forsøk på misbruk.
6. Kjønn. Kjønn er også et enkelt element å benytte i kontrollsituasjoner. Kjønn vil ofte bli gjenspeilet i navnet så lenge man bruker ID-kort innenfor en spesifikk kulturtradisjon. Navn gir ikke lengre noen entydig angivelse av kjønn.
7. Nasjonalitet for norske statsborgere som ønsker ID-kort med Schengenfunksjonalitet.

Følgende personinformasjon antas ikke å være nødvendig å ha visuelt i ID-kortet:
1. Bostedsadresse. Bostedsadresse anses ikke som noe viktig element i den visuelle del av ID-kortet. Dette er dessuten informasjon som vil kunne endre seg i løpet av kortets gyldighetstid. I enkelte situasjoner vil det også kunne utgjøre et eget kontrollelement for kontroll av innehaver. Ved tap av kort vil det dessuten hindre at for mye informasjon kan misbrukes.
2. Fødested. Heller ikke fødeland og fødested anses som nødvendig informasjon i kortet. Dette vil være informasjon som forutsetningsvis må kunne lagres i det sentrale registeret over nasjonale ID-kort.

Følgende informasjon til administrativt bruk foreslås lagt inn visuelt:
1. Kortnummer. Det forutsettes at hvert kort utstedes med et unikt kortnummer som gjør at alle utstedte kort kan "gjenfinnes" og kontrolleres av kortmyndigheten
2. Utstedelsesdato, utløpsdato og utstedende myndighet

I tillegg vil kortet inneholde sikkerhetselementer og mekanismer for å verifisere gyldighet:
- Maskinlesbarhet
- Elektronisk brikke (RFID-brikke) som inneholder samme informasjon som kortets visuelle del
- Kontaktchip som inneholder privat nøkkel og sertifikat, jf. kap. 12 og vedlegg B

8.4 Særlig om bruk av RFID

Formålet med bruk av biometrisk informasjon lagret i en kontaktløs elektronisk brikke (en spesiell utgave av RFID brikke utviklet for reisedokumenter) i et ID-kort er først og fremst å legge til rette for en sikker og effektiv verifisering av kortbærerens identitet. Dette oppnås ved at ID-kort med biometrisk informasjon etablerer en sterk forbindelse mellom kortet og dets innehaver. I økende grad må det påregnes at nødvendig leserutstyr finnes både ved grensestasjoner og hos politiet forøvrig.

En av de største utfordringer ved bruk av biometrisk gjenkjenning er å etablere teknologiske løsninger som er sikre og effektive, både for kortinnehaver og offentlige kontrollinstanser. Den må dernest baseres på etablerte tekniske spesifikasjoner (standarder) som sikrer interoperabilitet, samtidig som standardene skal ivareta kravene til datasikkerhet, herunder ekthet, integritet og konfidensialitet. Standardene som er utviklet for bruk av biometri i ID-kort er i praksis de samme som for pass.

Dette innebærer at dataene i den elektroniske brikken vil være sikret ved at kommunikasjonen mellom kortet og leseren er kryptert. Dette representerer en *konfidensialitetssikring*, og nøkkelen for

å kunne åpne/lese informasjonen distribueres til land (ICAO medlemsland) som skal lese ID-kortene (Det samme systemet gjelder for passene).

Dataene som ligger i brikken er signert med den utstedende stats sertifikat. Signering er en form for "lesbar" kryptering. Nøkkelen for å signere opplysningene i den elektroniske brikken er en forespørsel i form av et sertifikat fra produsent, og dette sertifikatet blir signert av rotsertifikatet til utstedende stat, noe som gjør at ingen av partene på egenhånd kan generere et fullverdig signeringssertifikat. Dette utgjør det viktigste elementet i *autentitets- eller ekthetssikringen* av informasjonen som er lagret elektronisk.

I det nasjonale ID-kortet forutsettes det at skrivedelen til den elektroniske brikken "brennes" av etter at ID-kortet er produsert. Dette er samme metode som benyttes ved produksjon av de nye elektroniske passene. Uten denne skrivedelen vil det ikke være mulig å legge data inn i den elektroniske brikken, hvilket representerer en viktig *integritetssikring* eller beskyttelse mot endring av informasjonen som ligger i den elektroniske brikken.

Alle stater må på forhånd levere ut den offentlige delen av sitt sertifikat til alle andre samarbeidsland, og ved hjelp av dette offentlige sertifikatet kan samarbeidende stater sjekke "signaturen" på dataene i den elektroniske brikken, og da bekrefte at det ikke er gjort endringer. Er det gjort endringer, vil ikke signaturen lenger stemme.

For å få tilgang til opplysningene i den elektroniske brikken må et utdrag av den maskinlesbare teksten (Machine Readable Zone - MRZ) leses. Denne informasjonen er grunnlaget for en nøkkel som benyttes til aksesskontroll og kryptering av kommunikasjon mellom ID-kortet og leseren. Metoden er navngitt som Basic Access Control (BAC). Dette representerer en ekstra *konfidensialitetssikring* som skal hindre at informasjonen i ID-kortet kan "fjeravleses" uten passinnehaverens kunnskap. Ved innføring av fingeravtrykk, vil ovennevnte metode (BAC) byttes ut med Extended Access Control (EAC). Denne metoden vil ha en utvidet form for autentisering (aktiv toveis autentisering). Det vil i tillegg bli innført bedre kryptering på kommunikasjonen mellom leser og brikke.

Den elektronisk lagrede informasjonen i kortet, og eventuell lagring av biometri, forutsettes å skulle følge de til enhver tid gjeldende relevante standarder.

Etter føringer fra EU vil muligheten for en elektronisk brikke for lagring av personinformasjon, herunder biometrisk informasjon, bli innført som en opsjonell løsning. Denne vil for øvrig følge de samme standarder som for pass.

I tillegg til Norge har flere land nå innført pass med elektronisk brikke (RFID-brikke) i hht. ICAO standard, og fra 2008 planlegger også EU å innføre tilsvarende brikke i et nytt oppholdskort for utlendinger. Dersom Norge gjennomfører EU-direktivet (se kap. 4.2.1 og 7.6), forplikter vi oss til å utstede tilsvarende oppholdskort med RFID-brikke til fast bosatte utlendinger.

Det at den elektroniske brikken i passet inneholder tilsvarende data som fremgår av kortets visuelle del (også bilde) vil ytterligere vanskeliggjøre en forfalskning. Siden innholdet i brikken ikke lar seg forfalske eller endre antas muligheten for å bli avslørt ved kontroll som omfatter elektronisk avlesing å virke avskrekkende for å bruke et kort der data for øvrig i passet er forfalsket. Fravær av andre supplerende kontrollmuligheter av informasjonen i kortet vil styrke argumentene for å konkludere med at en elektronisk brikke er nødvendig. Bruk av dokumentet i utlandet overfor utenlandske myndigheter eller andre, er typisk eksempel på en situasjon med

begrensede supplerende kontrollmuligheter. For et kort som har sitt anvendelsesområde i Norge er ikke de samme hensyn like sterke. Like fullt er det grunn til å peke på at det som kjennetegner en forfalskning nettopp er at det ikke foreligger noen ytre tegn på at dokumentet er uekte. Det er først ved kryssjekking av øvrige sikkerhetselementer at forfalskingen kan bli bekreftet eller avkreftet. Bruk av elektronisk lagret personinformasjon vil gjøre denne muligheten sikrere og mer effektiv.

Arbeidsgruppen er kommet til at det bør lagres personinformasjon elektronisk på en elektronisk brikke i nasjonalt ID-kort etter samme tekniske spesifikasjoner som for pass. Den teknologiske utviklingen går meget raskt og sett i sammenheng med utviklingen for øvrig på området kan et behov for nye lesermuligheter av den elektroniske brikken raskt oppstå.

8.5 Nærmere om bruk av nasjonalt ID-kort innen Schengen

Ett formål med Schengen-samarbeidet er å fjerne personkontrollen ved passering av de indre grensene mellom Schengen-landene. Selv om passkontrollen på grensene er borte, følger det likevel av Schengen-reglene at en har plikt til å fremlegge gyldig legitimasjon for å bekrefte identiteten f.eks. ved innsjekking på hoteller (se Schengen-konvensjonen artikkel 45, jf. utlendingsloven § 45). I tillegg har noen EU-land innført generell legitimasjonsplikt som innebærer at den enkelte må ha et godkjent legitimasjonskort og til enhver tid bære det på seg. Schengen-reglene pålegger ikke i seg selv landene å innføre et ID-kort. De nordiske land ble derfor heller ikke møtt med noe uttrykkelig krav om dette i forbindelse med tilslutning til Schengen-avtalen. Schengen-landene aksepterte at nordiske lands statsborgere medbringer pass som legitimasjon, som erstatning for nasjonalt ID-kort.

En viktig grunn til å innføre et ID-kort er kortets brukervennlighet gjennom et mer praktisk format sammenliknet med pass. ID-kortene som er i bruk i dag har samme størrelse og form som et vanlig bankkort. ID-kortet, som reisedokument, er kun gyldig innad i EU og det kan argumenteres med at konsekvensene av å miste et ID-kort er mindre enn å miste et pass som gir adgang fra 3. land inn i EU/Schengen-området og til land utenfor EU/Schengen. Et nasjonalt ID-kort som EU/Schengen ID-kort vil også redusere behovet for når det er nødvendig å medbringe pass. Dette vil føre til at færre pass mistes og kommer på uriktige hender. Det kan også tenkes at noen pålegges reiserestriksjoner og nektes pass, men at de kan få ID-kort fordi utleveringsavtalene med EU-landene er gode i tilfelle vedkommende forsøker å unndra seg forpliktelser i Norge ved ikke å returnere frivillig.

Avslutningsvis bør det også nevnes at symbolet på Schengen-regelverket nettopp var prinsippet med passfrihet. For Norges del vil ikke dette ha noen realitet før vi får et nasjonalt ID-kort som EU/Schengen ID-kort.

9 RETTSLIGE RAMMER FOR ID-KORT

9.1 Formål

Formålet med dette kapitlet er å vurdere ulike alternativer, samt å foreslå hvilke rettslige rammer som bør gjelde for et nasjonalt ID-kort.

9.2 Hvilke grupper kan få ID-kortet

Retten til å søke om nasjonalt ID-kort må i utgangspunktet omfatte alle norske statsborgere, herunder også norske statsborgere som har fast bopel i utlandet. Retten til å søke om et norsk nasjonalt ID-kort bør imidlertid også omfatte utenlandske statsborgere med fast opphold i Norge. Denne gruppen vil stort sett ha samme behov for å kunne identifisere seg i ulike sammenhenger som norske statsborgere, og bør derfor ikke ekskluderes fra en slik ordning.

Alle utenlandske statsborgere med fast opphold i Norge skal registreres i Folkeregisteret med et unikt fødselsnummer. Det vil derfor være naturlig å knytte utstedelse og identitetskontroll til dette kriteriet.

Flere grupper av utenlandske borgere som har opphold i Norge har ulike former for dokumentasjon for identitet og tillatelse for opphold:

- EU/Schengen borgere – nasjonalt ID-kort
- Personer med bosettingstillatelse – i løpet av 2-3 år vil dagens oppholdsetikett bli erstattet med eget oppholdskort utstedt av norske myndigheter etter EU-standard
- Flyktninger/asylsøkere – eget registreringsbevis utstedt av norske myndigheter
- 3. lands borgere – i løpet av 2-3 år vil dagens oppholdsetikett bli erstattet med eget oppholdskort utstedt av norske myndigheter etter EU-standard

Det fremgår at noen av kortene følger EU-standard og andre er norske kortløsninger. Dersom et nasjonalt ID-kort etableres, kan den enkelte utsteder av andre typer kort etter omstendighetene vurdere om det nasjonale ID-kortet kan erstatte eksisterende kortløsninger. Arbeidsgruppen har ikke funnet grunn til å gå nærmere inn på en slik vurdering.

Selv om mange utlendinger som bor/oppholder seg fast i Norge kan få ID-kort fra sitt hjemland, vil de ha behov for et ID-kort som inneholder deres norske fødselsnummer. Den informasjonen kan normalt ikke legges inn i utenlandske ID-kort og det kan være aktuelt å ha et alternativ til bankkort.

Uavhengig av andre kortløsninger vil et nasjonalt ID-kort knyttet til bosetting i Norge, jf. folkeregisterloven, kunne være et alternativ til eller et supplement til andre kort. Det vil være en forutsetning for erverv av et slikt kort at sikker identitet er fastsatt. Asylsøkere som har sin søknad under behandling bør ikke få slike kort fordi deres identitet i utgangspunktet ikke er vurdert. Endringer i opphold vil enkelt kunne registreres i ID-kort databasen ved at kortet f.eks. trekkes tilbake. Dette vil kunne forenkle situasjonen for de som har midlertidig opphold, og trygge samhandlingen for den som mottar dokumentasjon på identitet.

Utenlandske statsborgere som får oppholdstillatelse eller bosetningstillatelse i Norge, får i dag en standardisert Schengen oppholdsetikett satt inn i sitt reisedokument (hjemlands pass,

utlendingspass eller reisebevis for flyktninger). I løpet av 2-3 år vil oppholdsetikettene bli erstattet med et standardisert Schengen oppholdskort.

Denne gruppen vil gjennom oppholdskortet ha et ID-kort med samme informasjon som et nasjonalt ID-kort. Kortet vil også kunne inneholde en eID. Også denne gruppen bør omfattes av retten til å skaffe seg et nasjonalt ID-kort, som et supplement til oppholdskortet.

Arbeidsgruppen anbefaler at kortet kan erverves av norske statsborgere og personer med fast opphold i Norge. Nasjonalt ID-kort med Schengenfunksjonalitet kan bare erverves av norske statsborgere fordi det i et EU/Schengen ID-kort kreves opplysning om statsborgerskap. Tilsvarende kort utstedt i EU og andre Schengen-land kan kun utstedes til det enkelte lands egne borgere.

9.2.1 Alder

Arbeidsgruppen foreslår at ID-kort også kan utstedes til barn på samme måte som pass. [18] Dette er særlig aktuelt sett hen til reisedokumentfunksjonaliteten i Schengen ID-kortet. For særlige begrensninger vedrørende bruk av eID, se kap. 12.3.

9.2.2 Frivillig ordning og retten til å få ID-kort

Ordningen med nasjonalt ID-kort skal være en frivillig ordning. Valgfrihet må også omfatte funksjonalitet, dvs. eventuell Schengen-funksjonalitet (for norske statsborgere) og e-ID.

9.2.3 Det skal ikke innføres noen plikt til å bære med seg ID-kort

Etter EU/Schengen-regelverket vil det imidlertid være et krav om et ID-kort utstedt av myndighetene med angivelse av nasjonalitet. Også for andre lovpålagte identifiseringsformål som krever en kvalitativ identitetskontroll vil et nytt nasjonalt ID-kort være det som ligger til rette for å tilfredsstille kravene. Samtidig vil en slik løsning gi mulighet for etterkontroll der det oppstår tvil om ekthet, samtidig som personvernet styrkes i forhold til risikoen for id-tyverier.

9.2.4 Forutsetning for erverv av EU/Schengen ID-kort er norsk statsborgerskap

Bare norske statsborgere vil kunne utstyres med ID-kort som kan benyttes som reisedokument innen Schengen-området. Derimot kan norske statsborgere også erverve et ID-kort uten angivelse av statsborgerskap.

For utenlandske statsborgere med fast bopel i Norge vil det imidlertid ikke – etter någjeldende regler - kunne utstedes et ID-kort som dekker behovet for reiser innen Schengen. Det foreslås at dette tilkjennegis ved at kortene utstedes med ulik farge.

9.2.5 Særlig om retten til å få ID-kort med eID

Se kap. 12

[18] Utstedelse av e-ID vil ha et alderskrav

9.3 Vilkår for utstedelse

Som pekt på innledningsvis under dette kapitlet, skal alle, uansett alder, ha rett til å få utstedt et nasjonalt ID-kort på følgende vilkår:

- Vedkommende må falle inn under personkretsen nevnt i kap. 9.2
- Søknad ved personlig oppmøte og dokumentasjon av identitet, jf. prosedyrene ved søknad om pass. Det forutsettes at det foretas kontroll mot folkeregisteret, samt en kontroll av identiteten som ligger på samme det sikkerhetsnivået som ved utstedelse av pass
- Betaling av gebyr

Arbeidsgruppen har vurdert om utstedelse av ID-kort skal kunne nektes fordi søkeren tidligere har misbrukt nasjonalt ID-kort, f.eks. ved forfalskning eller bruk av en annens kort. Formålet med ID-kortet er at innehaveren skal kunne godtgjøre sin identitet ved et "godkjent" legitimasjonsdokument. Vedkommende vil være avskåret fra denne muligheten dersom kort nektes utstedt. Arbeidsgruppen kan derfor ikke se at tidligere misbruk av ID-kort kan danne grunnlag for utstedelse av et nytt.

Det er videre et spørsmål om det skal være adgang til å nekte utstedelse av ID-kort med Schengenfunksjonalitet med tanke på å hindre utreise fra Norge fordi det foreligger utreiseforbud, unndragelsesfare i forbindelse med soning av dom eller dersom søkeren ikke er i stand til å ta vare på seg selv i utlandet, smn.l. passloven § 5. Det bør i forbindelse med lovarbeidet vurderes hvorvidt det skal åpnes for en tilvarende adgang til å nekte utstedelse av nasjonalt ID-kort som også kan benyttes som reisedokument.

Årlig blir et tyvetall nordmenn sendt hjem fra utlandet på statens regning med bistand fra norske utenriksstasjoner fordi de er alvorlig sinnslidende eller psykisk utviklingshemmet og ikke er i stand til å ta vare på seg selv i utlandet. Dette dreier seg om personer som påfører utenriksstasjonene mye ekstraarbeid, og Utenriksdepartementet har i disse sakene mulighet til å anmode passmyndigheten om tilbakekalling av pass i henhold til passlovens § 7 første ledd bokstav b, jf. § 5 tredje ledd bokstav d). Normalt dreier dette seg om personer som gjentatte ganger må ha hjelp til å komme hjem, og i noen tilfelle må de hentes hjem av medisinsk personell.

9.4 Tilbakekall

Det vil være grunnlag for tilbakekall av ID-kort, ev. utstedelse av nytt med oppdatert statsborgerforhold, dersom innehaver taper eller får tilbakekalt sitt norske statsborgerskap, jf. statsborgerskapsloven kap. 5. Det samme må gjelde som følge av andre endringer i stasborgerforhold.

Likeledes vil det være grunnlag for å tilbakekalle kortet når det er utstedt til utlending som permanent flytter fra Norge (jf. kap. 9.2 om at vilkår for utstedelse av ID-kort til utenlandske statsborgere er fast bosetting i Norge).

Arbeidsgruppen har vurdert spørsmålet om det skal være mulig å tilbakekalle et nasjonalt ID-kort som følge av at innehaveren har misbrukt kortet, f.eks ved manipulering av opplysninger i kortet. Formålet med et nasjonalt ID-kort er muligheten for innehaver til å legitimere seg. Det vil derfor ikke være grunnlag for å tilbakekalle kortet ved misbruk. Et manipulert kort vil kunne inndras fordi det ikke lenger er ekte, men innehaver kan ikke nektes et nytt identitetskort. Retten til

nasjonalt ID-kort skal gjelde uavkortet så lenge en kortsøker faller inn under gruppen som har rett til å få utstedt kortet.

Når det gjelder spørsmålet om det skal være grunnlag for tilbakekall av ID-kort med Schengenfunksjonalitet for å forhindre utreise vises til det som er uttalt i pkt. 9.3 om vilkår for utstedelse av ID-kort.

Når det gjelder tilbakekall av e-ID henvises til kap. 12.

9.5 Gyldighetstid

ICAO anbefaler en gyldighetstid på 5 eller 10 år for reisedokumenter.

Mange land har samme gyldighetstid for nasjonalt ID-kort og pass. Enkelte land har imidlertid lengre gyldighetstid for pass enn for nasjonalt ID-kort og andre igjen har lengst gyldighetstid for nasjonalt ID-kort. Det vil ofte være behov for lengre gyldighetstid for pass enn for ID-kort pga. innstemplede tillatelser og visa, som ofte har en lang gyldighetstid.

Følgende EU-land har 10 års gyldighetstid for nasjonalt ID-kort for personer over en viss alder: Estland, Frankrike, Litauen, Portugal, Slovakia, Slovenia, Ungarn og Østerrike.

Følgende EU-land har 5 års gyldighetstid for nasjonalt ID-kort:
Belgia, Finland, Italia, Nederland og Sverige.

Hellas har ubegrenset gyldighetstid for nasjonalt ID-kort for personer over 12 år. I Portugal er gyldighetstiden ubegrenset etter fylte 55 år, i Slovakia fra fylte 60 år.

Ved vurdering av hvilken gyldighetstid nasjonalt ID-kort bør ha, må det tas hensyn til flere faktorer:

- Slitasjeproblematikk: Et ID-kort vil ved hyppig bruk bli utsatt for slitasje i langt større utstrekning enn hva som gjelder for pass fordi innehaveren antagelig alltid vil bære kortet med seg.
- Aldringsprosess: Det faktum at innehaver av ID-kortet eldes, kan medføre problemer i forhold til gjenkjennelse ved bruk både av den visuelle delen og ved bruk av biometri.
- Teknologisk utvikling: Denne går meget raskt og sikkerheten knyttet til produksjon av identitetsdokumenter har gjennomgått en rivende utvikling i løpet av få år. Profesjonelle forfalskninger har presset frem høye krav til sikkerhet som fortløpende må oppdateres. I dagens situasjon vil et 10 år gammelt dokument normalt være sikkerhetsmessig utdatert lenge før gyldighetstiden utløper.
- Kortere gyldighetstid vil gi en høyere grad av sikkerhet ved at forfalskede eller påvirkede dokumenter vil ha en kortere opereringstid før de blir ugyldige.
- Gyldighetstiden for eID: Vanligvis utstedes eID for en periode på 1-3 år, avhengig av anvendelsesområde. Kravspesifikasjonen for PKI i offentlig sektor setter en nedre grense på min. 13 måneder, men setter ikke en øvre grense. Av hensyn til teknologiutviklingen og muligheter for et ondsinnet angrep på en eID, bør gyldigheten ikke settes for lang. Paralleller kan også trekkes til bankkort som følger tilsvarende prinsipper. Dette taler for en gyldighet ikke lengre enn 5 år.
- Kostnader i forbindelse med utstedelse vil være høyere ved kortere gyldighetstid.

Arbeidsgruppen legger ved vurderingen av ID-kortets gyldighetstid avgjørende vekt på hensynet til slitasje av selve kortet samt gyldighetstid for eID og anbefaler at gyldighetstiden settes til 5 år.

Gyldighetstiden til ID-kort for barn bør begrenses på samme måte som for pass til barn da det skjer store utseendemessige forandringer hos barn de første årene. Dette vil innebære at gyldighetstiden for nasjonalt ID-kort for barn fra 0-5 år vil være 2 år. For barn mellom 5 og 10 år vil gyldighetstiden være 3 år. For barn over 10 år vil gyldighetstiden være 5 år.

9.6 Elektronisk lagring av personinformasjon i kortet

Arbeidsgruppen anbefaler at personinformasjonen lagres i en elektronisk brikke i passet i tillegg til det maskinlesbare feltet og den visuelle delen. Det vises for øvrig til drøftelsen i kap. 8.4.

9.7 Bruk av fødselsnummer

Dette kapitlet skal se på de praktiske og rettslige sidene av at det nasjonale ID-kortet inneholder innehaverens fødselsnummer.

Når vi i dette kapitlet omtaler fødselsnummer omfatter det også såkalt D-nummer, så fremt annet ikke eksplisitt er uttalt. D-nummer utstedes til utlendinger som har lovlig opphold i Norge, og brukes i forbindelse med skatt og offentlige tjenester. Når en innvandret person skal få tildelt fødselsnummer, gis det ofte først et midlertidig D-nummer.[19]

Fødselsnummer er en unik indikator som skiller enkeltpersoner fra hverandre. For å foreta en kontroll av en persons identitet er det normalt ikke nødvendig med ytterligere opplysninger. På bakgrunn av dette vil det således være mange fordeler med at det nasjonale ID-kortet inneholder opplysning om innehavers fødselsnummer. Alternativet vil være å koble kortnummeret til kortinnehaverens fødselsnummer. Tilgangen til denne databasen vil kunne begrenses til de som har legitim grunn til slik tilgang. Et annet alternativ vil være å ikke benytte fødselsnummer i det hele tatt, verken direkte på kortet eller indirekte via en database, men isteden bruke et sett med attributter – navn, fødselsdato, fødested mv. – for å identifisere innehaver og kunne skille denne fra andre personer. Identifisering av en person på denne måten kan være er forbundet med en viss risiko da det aldri helt kan utelukkes at det finnes to personer med helt identiske sett av relevante attributter. Denne risikoen vil reduseres jo flere attributter som brukes. Imidlertid, jo flere attributter som kreves for å skille enkeltpersoner fra hverandre, desto mer komplisert og ressurskrevende vil identifiseringsprosessen være. Dessuten vil bruk av mange attributter kunne begrense mulighetene for automatiserte prosesser.

Således, ved å bruke fødselsnummer trenger man ikke bruke andre attributter i tillegg, og det vil være enklere at en slik sjekk kan automatiseres. Selv om det av praktiske grunner kan være hensiktsmessig å ha fødselsnummeret direkte på kortet, finnes rettslige skranker for bruk av fødselsnummeret som må etterleves. Disse skrankene finnes i hovedsak i personopplysningsloven.

Ifølge personopplysningsloven kan fødselsnummer bare brukes når det er saklig behov for det, og når det er umulig å oppnå tilfredsstillende identifikasjon ved bruk av andre metoder, som f.eks. navn, adresse, fødselsdato, medlems- eller kundenummer, jf. personopplysningsloven § 12.

[19] D-en kommer av at systemet opprinnelig var knyttet til utenlandske og utenlandsboende sjøfolk på norske skip: Direktoratet for sjømenn.

Fødselsnummer er ikke taushetsbelagt, jf. forvaltningsloven § 13. Fødselsnummeret er heller ikke ansett som en sensitiv opplysning etter personopplysningsloven, jf. personopplysningsloven § 2 nr. 8 (e contrario).

Det er således mulig å nekte å oppgi fødselsnummer dersom den som ber om fødselsnummer (i) ikke kan vise til lovhjemmel eller (ii) ikke har saklig behov, samt at det er mulig å oppnå tilfredsstillende identifikasjon ved bruk av andre metoder. Dette gjelder uansett om opplysningene føres manuelt eller elektronisk. Datatilsynet mener at det sjelden foreligger et saklig behov å trykke fødselsnummer på et ID-kort og mener at informasjon om fødselsdato på kortet normalt vil være tilstrekkelig.

Dersom bruk av fødselsnummer derimot sikrer at registrerte opplysninger får riktig kvalitet og dette er i den registrertes interesse, taler dette for bruk av fødselsnummer.

Spørsmålet er således om det er "saklig behov" for å bruke fødselsnummer i det nasjonale ID-kortet, og det ikke er mulig å oppnå tilfredsstillende identifikasjon på annen måte. For å kunne svare på dette spørsmålet må man se hen til det nasjonale ID-kortets presumerte bruksområder og hvilket behov "mottaker" har for å motta opplysning om fødselsnummeret. Bruksområdene for ID-kortet vil bl.a. være:

1. Identifisering overfor offentlig forvaltningsorgan, f.eks. folkeregister, ligningskontor, politiet, NAV (Nye Arbeids- og velferdsetaten) og kommuner.

Fødselsnummeret ble innført for å dekke det offentliges behov for å skille enkeltmennesker fra hverandre. I tillegg har en del private og offentlige virksomheter fått lovhjemmel til å bruke nummeret.

2. Identifisering overfor private aktører; herunder

    a) rapporteringspliktige etter hvitvaskingsloven

Etter hvitvaskingsloven § 5 følger at "rapporteringspliktige skal ved etablering av kundeforhold kreve gyldig legitimasjon av kunden". Ifølge hvitvaskingsforskriften § 4 skal legitimasjonsdokumenter for fysiske personer inneholde:

> *"fullt navn, navnetrekk, fotografi og fødselsnummer (eventuelt D-nummer). Legitimasjonsdokumenter skal være utstedt av offentlig myndighet, eller av annet organ som har betryggende kontrollrutiner for dokumentutstedelse og det er allment akseptert at dokumentet for øvrig har et tilfredsstillende sikkerhetsnivå."*

Nevnte opplysninger (inklusive fødselsnummer) skal oppbevares av den rapporteringspliktige i fem år, jf. hvitvaskingsforskriften § 15.[20]

[20] Det er i utgangspunktet per i dag ikke mulig å foreta identifisering av person etter hvitvaskingsregelverket på avstand (over f.eks. Internett) ved bruk av eID. Finansdepartementet har imidlertid nedsatt et lovutvalg som skal vurdere tiltak mot hvitvasking av penger og terrorfinansiering mv. I utvalgets mandat står også at det skal "vurdere, og foreslå, regler som legger til rette for elektronisk kundeidentifikasjon innenfor rammen av internasjonale forpliktelser og anbefalinger." Utvalgets utredning om dette skal være ferdig innen 1. juni 2007. Jf. http://www.odin.no/fin/norsk/aktuelt/pressesenter/pressem/006071-070789/dok-bn.html

b) om identifisering ved registrering av nytt telefon- eller mobilabonnement

Ifølge ekomforskriften § 6-2 første ledd skal:

> *"tilbyder av offentlig telefontjeneste … føre oversikt over enhver sluttbrukers navn, adresse og nummer/ adresse for tjeneste. Oversikten skal inneholde opplysninger som muliggjør entydig identifisering av de registrerte, jf. §6-3 annet ledd."*

I § 6-3 annet ledd står bl.a. at relevant informasjon er "unik ID; fødselsdato, fødselsnummer eller organisasjonsnummer der dette er registrert og ikke annet er avtalt, eller annen egendefinert unikt ID-nummer."

c) Konsesjon fra Datatilsynet

Andre enn offentlige virksomheter kan også be om å få fødselsnummeret. Datatilsynet har blant annet gitt kredittopplysningsforetak rett til å bruke fødselsnummer. Kredittopplysningsforetakene bruker fødselsnummeret til å skille enkeltmennesker med samme navn fra hverandre.

Det er arbeidsgruppens ønske at det nasjonale ID-kortet skal kunne brukes som et generelt gyldig fysisk legitimasjon, dvs. både overfor det offentlige og overfor private. Krav om legitimering stilles i mange sammenhenger, hvorav en av de mer viktige områdene er kravet om identifisering etter hvitvaskingsregelverket. Som allerede nevnt ovenfor vil kun legitimasjonsdokumenter som innholder fødselsnummer kunne brukes i denne sammenheng. Dette betyr således at alle rapporteringspliktige må få informasjon om personens fødselsnummer. Dette vil sannsynligvis skje enklest, billigst og kanskje med størst sikkerhet ved å ta inn fødselsnummeret i ID-kortet (jf. at bankkort også innholder fødselsnummer). Tatt i betraktning hvilke som er rapporteringspliktige etter hvitvaskingsloven, er det ikke sannsynlig at alle disse vil ha en "terminal" som kan lese et referansenummer i kortet og via en database koble det til personens fødselsnummer.

For det nasjonale ID-kortet som også skal kunne brukes som reisedokument innenfor Schengen vil det i tillegg til reisedokument også kunne brukes som identifikasjonsdokument internasjonalt. Kortet kan da brukes som identifikasjonsdokument overfor utenlandsk politi og andre utenlandske myndigheter, samt også overfor private subjekter som f.eks. hotell. Når ID-kortet skal brukes i slike situasjoner vil det ut fra praktiske hensyn være mange fordeler ved at det innholder samme informasjon som det som per i dag står i passet. Pass utstedes med hjemmel i passloven med tilhørende forskrift. Det følger av passforskriften § 9 at "fødselsnummeret skal innføres i passet." Fordelen ved at kortet innholder et fødselsnummer er bl.a. at utenlandsk politi og myndighet overfor norsk politi og myndigheter kun trenger å bruke ett attributt (fødselsnummeret) for å foreta en unik identifisering av innehaver.

Ved en samlet vurdering av ovenstående anbefaler arbeidsgruppen at det nasjonale ID-kortet innholder innehavers fødselsnummer. Arbeidsgruppen tar samtidig inn over seg de nevnte beskrankningene i personopplysningsloven, og foreslår derfor at det vurderes om opplysning om fødselsnummeret skal legges på baksiden av kortet. Ved å legge fødselsnummeret på baksiden av kortet vil det være mindre problematisk å la andre enn de som har rett til å få tilgang til fødselsnummeret, å ta kopi av fremsiden av kortet. Disse vil da ikke få kopiert opplysning om fødselsnummer. Samtidig vil det for bl.a. rapporteringspliktige være nødvendig å kopiere begge sider av kortet. På kortets bakside må det derfor være preget en identifikator – f.eks. det unike kortnummer – som også er preget på forsiden av kortet, slik at det etterpå er mulig å koble fødselsnummer til riktig ID-kort (forside).

10 ADMINISTRATIV OG RETTSLIG FORANKRING

10.1 Formål

Formålet med dette kapitlet er å vurdere ulike alternativer for administrativ og rettslig forankring av en ordning med nasjonalt ID-kort, og å legge fram en begrunnet anbefaling.

10.2 Hvem bør administrere ordningen med nasjonalt ID-kort

Det administrative ansvaret for utstedelse av nasjonalt ID-kort forutsettes plassert hos en offentlig myndighet. Ansvaret kan f.eks. legges til politiet, ligningskontorer, NAV-kontorer eller kommunene.

Den myndighet som skal behandle søknader og utstede ID-kort må ha lett (direkte) tilgang til Folkeregisteret. Den ansvarlige myndighet må videre ha gode og sikre rutiner for identitetskontroll som er en svært viktig del av prosessen med utstedelse av ID-kort.

Videre må det oppstilles et krav om at utstedende myndighet er desentraliserte enheter med en rimelig geografisk spredning slik at den enkeltes avstand til tjenesten ikke blir for stor. Her vil både politiet med sin desentraliserte struktur, NAV-kontorene og den enkelte kommune være aktuelle valg. Ligningskontorene er i dag regionalisert og kravet til nærhet til publikum vil ikke være oppfylt i like stor grad som for øvrige aktuelle myndigheter.

Arbeidsgruppen legger til grunn at det vil representere et betydelig ressursbehov å bygge opp kapasitet og kompetanse på mange steder for å betjene publikums behov for nasjonalt ID-kort. Dette taler for å basere administreringen av nasjonalt ID-kort på eksisterende ordning med passutstedelse. Politiet har allerede kompetanse og systemer til å foreta identifisering av personer. Den infrastruktur som skal benyttes ved utstedelse av nasjonalt ID-kort, bl. a. i form av teknisk utstyr til biometrifangst er allerede utplassert på politistasjoner og lensmannskontorer.

Utstedelsesprosessen vil bl.a. bestå av opptak av data, kontroll av om vilkår for utstedelse av ID-kort er til stede, registerføring av informasjon og produksjon av selve kortet.

Kvaliteten på identifikasjonsprosessen er avgjørende for å knytte rett person til rett identitet. I arbeidet med fastsettelse av identitet er det viktig å ha tilgang til all relevant informasjon for å unngå at noen klarer å få utstedt to identiteter til en person. Oppstår det en situasjon med to identiteter for en person vil det være ødeleggende for tilliten til dokumentet.

Ved å benytte politiets infrastruktur og personell for identifikasjon og registrering ved utstedelse av pass, vil kvaliteten bli god, og kostnadene ved innføring av nasjonalt ID-kort vil vesentlig kunne reduseres. Slik vil nasjonalt ID-kort raskt kunne utstedes, med et minimum av opplæring av personell og investeringer i infrastruktur. Samtidig benyttes en velprøvd og trygg ordning som publikum har tillitt til. Arbeidsgruppen vil for øvrig vise til at hvitvaskingsloven anser pass som "gyldig legitimasjon". Dette innebærer at denne utstedelsesprosedyren anses som betryggende for å fastslå korrekt identitet.

For norske borgere bosatt i utlandet, og som ønsker et nasjonalt ID-kort, vil det ikke være naturlig å kreve at vedkommende reiser til Norge for å få utstedt et slikt kort. Arbeidsgruppen foreslår derfor at norske utenriksstasjoner som har passutstedelsesmyndighet også gis myndighet

til å utstede nasjonalt ID-kort. Disse vil – som politiet - kunne basere utstedelse på eksisterende infrastruktur for passutstedelse. Det må også være mulig for utenlandsboende norske borgere å søke om nasjonalt ID-kort når de er i Norge.

10.3 Rettslig forankring/plassering av hjemmelen for nasjonalt ID-kort

Etter arbeidsgruppens vurdering kan hjemmelen for nasjonalt ID-kort enten forankres i passloven som et eget kapittel eller i egen lov.

Regelverket for nasjonalt ID-kort vil ha flere bestemmelser som er parallelle til bestemmelser i passloven. Dette vil f.eks være bestemmelsene om innsyn, retting og sletting. Enkelthet i regelverket, bl.a. ved behov for ending av lovbestemmelser som vil være felles for pass og nasjonalt ID-kort, taler for at regelverket for nasjonalt ID-kort tas inn som et eget kapittel i passloven.

På den annen side vil nasjonalt ID-kort ha et langt videre formål enn pass, som i utgangspunktet bare er et reisedokument. Funksjonen som reisedokument vil bare være en tilleggsfunksjon i et nasjonalt ID-kort. I tillegg vil funksjonaliteten med elektronisk ID tale for at ordningen med nasjonalt ID-kort hjemles i egen lov. En forskrift som skal regulere e-ID vil da rettslig forankres i lov om nasjonalt ID-kort, alternativt i e-signaturloven.

Arbeidsgruppen foreslår at nasjonalt ID-kort hjemles i egen lov.

11 REGISTER OVER ID-KORT

11.1 Formål

Formålet med dette kapitlet er å redegjøre nærmere for behovet for og plasseringen av et sentralt elektronisk register over nasjonale ID-kort, samt rettslige rammer rundt et register mht hvilke opplysninger som skal registreres, bruken av opplysningene og hvem som skal ha tilgang.

11.2 Behovet for registrering

Utstedelse av nasjonale ID-kort må føres i et sentralt register (database) som basis for administreringen av ordningen, samt for å kunne foreta etterkontroll av kort som er i bruk. Det vil være naturlig at et slikt register brukes ved utstedelse av nytt ID-kort. Registeret må forvaltes av utstedende myndighet.

Tilgang til registeret skal i utgangspunktet være forbeholdt vedkommende forvaltningsmyndighet (utstedende myndighet). Der ID-kortet benyttes som reisedokument i grensekontroll bør grensekontrollmyndigheten ha direkte tilgang til kortregisteret på lik linje med adgangen til passregistre.

Også andre må kunne gis opplysninger fra registeret. Dette vil bl. a. være aktuelt der kort er tapt, men det foreligger en situasjon hvor vedkommende person har et særlig behov for å få sin identitet bekreftet umiddelbart. Også der det reises tvil om identiteten til kortinnehaver eller om kortet er manipulert (endret) vil det være behov for informasjon fra registeret. Både offentlig myndighet og private må ha mulighet til å få bekreftet ekthet og informasjon i et fremlagt ID-kort ved å henvende seg til utstedende myndighet.

11.3 Eget register eller del av passregisteret

Det må antas at det ved etablering av et nasjonalt ID-kort vil være mange som vil få både ID-kort og pass. Den personinformasjonen som skal lagres vil langt på vei være identisk. Det vil derfor være naturlig å se disse registrene i sammenheng.

Arbeidsgruppen vil imidlertid foreslå at det etableres et særskilt register over utstedte ID-kort. Det må likevel være en samordning av informasjonen i de to registrene ved søknad, fornyelse osv, både når det gjelder pass og ID-kort.

11.4 Hvilken informasjon skal lagres i det sentrale ID-kort registeret

11.4.1 Generelt

Registeret må inneholde den personinformasjonen som benyttes visuelt på kortet, jf. kap. 8.3.2.

Til administrativt bruk og for senere kontroll må registeret dessuten gjenspeile alle handlinger knyttet til kortutstedelse. Dette bør forankres i at søknaden om ID-kort inngår som grunnlag for registreringen. I tillegg registreres opplysninger om fremmøte mv. Registeret må dernest ha informasjon om utstedelsesdato, utløpsdato og utstedende (behandlende) myndighet. I registeret skal det også tas med opplysninger om ansvarlig saksbehandler(e). I tillegg bør registeret inneholde informasjon om eID, se kap. 12.5.4 (nærmere om forholdet mellom eID katalog og ID-kort register).

11.4.2 Registrering av adresser

Adresse til kortinnehaver forutsettes ikke tatt inn i kortet, jf. kap. 8.3.3. Arbeidsgruppen mener imidlertid at kortsøkers mottaksadresse bør fremgå av registeret. Dette er en administrativ opplysning om blant annet forsendelsesadressen til ferdig personaliserte kort. Adresse er dessuten et nyttig kontrollelement.

11.4.3 Særlig om registrering av biometrisk informasjon.

Biometrisk informasjon i form av bilde og signatur er viktige og enkle elementer ved kontroll av ID-kort. Slik informasjon legges i dag inn i det sentrale passregisteret, og det knytter seg ikke spesielle betenkeligheter til at dette blir registrert.

Fingeravtrykk forutsettes også etter hvert å skulle tas i bruk som elektronisk lagret biometrisk element i ID-kortet. Arbeidsgruppen ser at det kan knytte seg enkelte betenkeligheter til registrering av fingeravtrykk i det sentrale ID-kort registeret. Fingeravtrykk vil imidlertid kunne utgjøre det enkleste element for fremtidig kontroll av identiteten og ektheten av kortet. Arbeidsgruppen mener også at det er uproblematisk å legge restriksjoner på bruken av fingeravtrykk slik at dette ikke benyttes utenfor det formålet det er innhentet for.

11.5 Bruk av registeret

11.5.1 Hvem skal ha tilgang til/opplysninger fra registeret og til hvilke formål

- ID-kort myndigheten (forvaltningsmyndigheten). Tilgangen skal dekke alle formål knyttet til utstedelse og kontroll av ID-kort.
- grensekontrollmyndighet (i forhold til ID-kort med EU/Schengen-funksjonalitet). Direkte (on-line) tilgang etter nærmere fastsettelse av type informasjon det kan søkes på.
- andre myndigheter på forespørsel når det er nødvendig for å kontrollere identiteten til kortinnehaver, eller der det kan reises tvil om kortet er ekte.
- private institusjoner – på anmodning når det er nødvendig å kontrollere påberopt identitet, eller det kan reises tvil om ektheten av fremlagt ID-kort - og som utsteder av (ny) id-dokumentasjon. Formålet skal være å foreta en sikker identitetskontroll. Ved utstedelse av ny id-dokumentasjon forutsettes samtykke fra den registrerte.

Der utstedende myndighet foretar kontroll av ID-kort – eller identiteter – etter anmodning fra offentlig eller privat institusjon, skal denne som utgangspunkt bestå i at rett identitet eller kortets ekthet og gyldighet bekreftes. Utlevering av biometrisk informasjon fra registeret skal ikke forekomme.

11.5.2 Vedlikehold og sletting av registeropplysninger

Registeret må så langt praktisk mulig holdes oppdatert med ny informasjon om kortinnehaver. Kortinnehaver har selv plikt til å sørge for at endringer, f.eks. i navn, blir meddelt kortmyndigheten slik at nytt kort med riktige opplysninger kan utstedes.

Også historiske data vedrørende kortinnehaver, som f.eks. tidligere utstedte kort, tidligere navn (ved navnendring) og tidligere adresser skal bli stående i registeret. Det forutsettes at det lages særskilte slettingsregler for kortinnehavere som er døde.

Ved endring av status som gjør at vedkommende ikke lenger har rett til ID-kort, f.eks. knyttet til flytting og/eller skifte av statsborgerskap, skal dette anmerkes i registeret.

Kort som er meldt tapt eller stjålet skal registreres og utsteder av eID må opplyses om dette forholdet.

11.6 Innsyn, retting og sletting

Innehaver av ID-kort har rett til innsyn i ID-kortregisteret. Vedkommende kan kreve feil opplysninger rettet eller slettet.

Likeledes har ID-kortinnehaver rett til innsyn i informasjon som er lagret elektronisk i kortet. Feil informasjon kan kreves rettet eller slettet. Der det foreligger feil som ikke skyldes kortinnehaver, har vedkommende krav på å få utstedt nytt kort uten ytterligere kostnad. Det forutsettes at det legges til rette for innsyn i den elektronisk lagrede informasjonen i ID-kortet ved særskilt tilpasset leserutstyr på søkerstedene.

12 ELEKTRONISK ID

Formålet med dette kapitlet er å se på muligheten til å integrere en eID i et nasjonalt ID-kort slik at kortet også kan benyttes f.eks. mot offentlige tjenester på nettet.

12.1 Hva er elektronisk ID og elektronisk signatur. Elektronisk autentisering.

Elektronisk ID (eID) er en måte å bekrefte sin identitet, vanligvis i form av ens vanlig brukte navn, i forbindelse med elektronisk samhandling. En eID kan imidlertid også bekrefte f.eks. et kundenummer eller et annet pseudonym, eller eventuelt en persons fødselsnummer. En eID kan også bekrefte en rolle, f.eks. at innehaveren er registrert revisor. En eID kan realiseres på mange ulike måter, fra alminnelig brukernavn og passord, via engangs PIN-koder (utsendt på et ark), engangspassord sendt til mobiltelefon, engangspassord generert fra en passord-kalkulator, til kryptografi-baserte hemmelige nøkler som enten lagres i PCen, på en USB-enhet eller på et smartkort (chipkort), som også kan være SIM-kortet i en mobiltelefon. I dette kapitlet fokuserer en videre på eID og e-signatur basert på PKI (Public Key Infrastructure) – en teknologi basert på kryptografiske metoder, og som kan benyttes til å anvende eID og e-signaturer i stor skala, over åpne nett, som f.eks. Internett.

Teknologien baserer seg på bruk av to kryptografiske nøkler (koder) – en hemmelig (dette er brukerens eID/e-signatur) og en som er offentlig tilgjengelig for alle. Nøklene passer slik sammen at eventuelt misbruk av eID/e-signatur blir avslørt. For at kommunikasjonsparter skal være sikre på at den offentlige nøkkelen faktisk tilhører den personen som besitter en eID, er det etablert tredjepartstjenester, såkalte sertifikatutstedere, som utsteder et digitalt sertifikat som bekrefter at en offentlig nøkkel tilhører en gitt brukeridentitet. På denne måten kan ukjente parter kommunisere sikkert med hverandre ved å stole på sertifikater. Ved sikkerhetsbrudd av noe slag, f. eks. tap av smartkort med eID på, skal sertifikatet plasseres på en sperreliste, etter samme mønster som kredittkort. Da vil motparten vite at eID-en ikke er å stole på lenger. Se ellers NOU 2001:10 "Uten penn og blekk" for nærmere informasjon om hvordan infrastruktur for offentlige nøkler fungerer og hva den kan brukes til.

Autentisering defineres vanligvis som en prosess der en påstått identitet kontrolleres for å slå fast at den som påberoper seg identiteten faktisk er den vedkommende utgir seg for å være.

Bruk av elektronisk ID til autentisering og elektronisk signatur for sikring av uavviselighet[21] vil i mange sammenhenger være en forutsetning for utviklingen av elektronisk handel og elektronisk forretningsdrift i næringslivet, samt elektroniske tjenester fra det offentlige (e-forvaltning).

I den senere tid har autentisering blitt satt i en større sammenheng, kalt **identitetsforvaltning**. Identitetsforvaltning er et vidtfavnende begrep som betegner aktiviteter knyttet til det å identifisere personer i forhold til et system (der system kan innebære et land, et datanettverk, en organisasjon eller et konkret datasystem) og å kontrollere deres adgang til ressurser i dette systemet. Adgangen kontrolleres ved å lage koblinger mellom brukerens identitet og rettigheter for bruk av systemets ressurser.

---

[21] Dvs. at innholdet i et elektronisk dokument knyttes sammen med identiteten til avsenderen på en måte som ikke kan benektes i ettertid.

Identitetsforvaltning omfatter blant annet regler for å oppnå felles pålogging til mange systemer (eng. single-sign-on), ved at en bruker hvis identitet er blitt verifisert og godkjent av ett system, blir overført til et annet system uten å måtte identifisere seg på nytt. En slik overføring krever at det ene systemet stoler på det andre systemets verifikasjon av identitet – man sier at systemer er i føderasjon med hensyn til autentisering av brukere.

Selve metoden som benyttes for autentisering kan være en av de som er nevnt ovenfor i dette kapitlet. Således kan kun én pålogging med en eID med høyt sikkerhetsnivå være tilstrekkelig for å få adgang til mange systemer uten at det kreves ny autentisering hver gang brukeren kommer inn i et nytt system. I en slik sammenheng er det grunn til å tro at en pålogging med nasjonalt ID-kort med eID kan oppfattes som mer sikker enn f.eks. en passordbasert pålogging.

I Norge finnes det et begrenset antall sertifikatutstedere, jf. kap. 4.3. Markedet er umodent. Det preges av såkalte "nettverkseffekter" (høna-og-egget syndromet), som gjør at det er usikkerhet for sertifikatutstedere forbundet med kostnader til utrulling av eID til alle innbyggere, og tilbydere av nettjenester er usikre på om de skal legge til rette for bruk av eID i sine tjenester.

12.2 Regulering av eID og e-signatur i norsk rett

I lov av 15. juni 2001 nr. 81 om elektronisk signatur[22] (e-signaturloven) reguleres de rettslige rammebetingelsene for bruk av elektronisk signatur og tilknyttede tjenester.[23] Loven trådte i kraft 1. juli 2001. Et viktig formål med loven er å sikre autentisering mellom to parter som ikke kjenner hverandre. Loven regulerer i hovedsak utstedere av "kvalifiserte sertifikater". Til dette sikkerhetsnivået er det knyttet bestemmelser om erstatning og rettsvirkninger samt tilsyn ved Post- og teletilsynet.

I lov med tilhørende forskrift[24] stilles det blant annet krav om at identifisering av person som ønsker et kvalifisert sertifikat må skje ved personlig fremmøte, med mindre vedkommende allerede er identifisert ved personlig fremmøte gjennom eksisterende kundeforhold. Det er derimot ikke nærmere angitt hvilke typer av dokumenter som må legges frem ved en slik identifikasjon. Videre finnes det bestemmelser om at det kvalifiserte sertifikatet må innholde opplysninger om utstedelse og utløpsdato.

Loven innholder en bestemmelse om at en elektronisk signatur på et nærmere angitt nivå (en kvalifisert elektronisk signatur) kan oppfylle et krav om underskrift så fremt den aktuelle disposisjonen kan gjennomføres elektronisk. I samme bestemmelse står også at andre typer av elektroniske signaturer kan oppfylle slike krav. Det kan også nevnes i denne sammenheng at rettsvirkning av en disposisjon som skjer elektronisk kan oppnås så vel ved bruk av en digital signatur som ved ren autentisering, avgjørende er i utgangspunktet hvordan disposisjonen gjennomføres og partenes vilje til å binde seg.

E-signaturloven innholder også nærmere bestemmelser om innsamling av personopplysninger, jf. e-signaturloven § 7. Disse kravene gjelder for alle utstedere av elektroniske signaturer uansett sikkerhetsnivå og oppstiller strengere krav enn de som følger av personopplysningsloven. Datatilsynet fører tilsyn med at denne bestemmelsen etterleves.

---

[22] Jf. Ot.prp. nr. 82 (1999-2000), Ot.prp. nr. 103 (2001-2002) og Ot.prp. nr. 74 (2004-2005) .

[23] Loven er en gjennomføring av EU-direktiv av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer (1999/93/EC).

[24] Jf. forskrift om krav til utsteder av kvalifiserte sertifikater mv.

I en ny forskrift til e-signaturloven[25] er det etablert en selvdeklarasjonsordning for sertifikatutstedere. Denne forskriften åpner for at sertifikatutstedere kan selvdeklarere seg i forhold til de sertifikatklasser som er definert i *Kravspesifikasjon for PKI i offentlig sektor* utarbeidet av Fornyings- og administrasjonsdepartementet. Denne Kravspesifikasjonen definerer tre forskjellige sertifikatklasser - Person Høyt, Person Standard og Virksomhet – der blant annet kravene om utstedelse av de forskjellige sertifikatene er forskjellige. Til disse selvdeklarasjonsordningene i nevnte forskrift finnes det en kobling til e-Forvaltningsforskriften § 27 (4)[26] som lyder: *"Koordineringsorganet kan bestemme at det ved elektronisk kommunikasjon med og i forvaltningen bare skal benyttes sertifikater som er oppført på liste publisert i henhold til forskrift 21. november 2005 nr. 1296 om frivillige selvdeklarasjonsordninger for sertifikatutstedere § 11 første ledd."*

12.3 Formålet med, og premisser for, eID/e-signatur på nasjonalt ID-kort

12.3.1 Forutsetninger for utstedelse av eID i offentlig regi

En viktig forutsetning for utvikling av elektronisk handel og bredere tilbud av elektroniske offentlige tjenester er en eller annen form for elektronisk identifikasjon. De fleste aktive brukere av Internett – og det er nå det store flertall av befolkningen – er i dag eiere av stadig økende antall brukernavn, passord, PIN-koder, passordkalkulatorer, kodekort og andre hjelpemidler for å kunne identifisere seg overfor en nettjeneste. De fleste er i den forbindelse klar over at de må ta vare på, være forsiktige med, og ikke skrive ned, alle disse kodene. Dette er blitt en mer og mer umulig situasjon. Offentlig sektor er i så måte intet unntak – flere etater utsteder passord og koder som befolkningen må bruke for å få tilgang til informasjon, bestille kort og brosjyrer, levere selvangivelse osv.

Det finnes åpenbart et behov for å rydde opp i dette kaoset. Et første skritt vil være en mer enhetlig mulighet for identifisering i forhold til noen sentrale offentlige tjenester.

Dette ble forsøkt gjort gjennom satsingen på den s.k. "sikkerhetsportalen", men vanskeligheter med markedsaktørenes forretningsmodeller har satt en stopper for dette. Utvikling av et nasjonalt ID-kort med mulighet for eID, gir en god anledning til å prøve en ny tilnærming til problemstillingen.

Det er lang tradisjon i Norge for at det offentlige har tatt ansvar for den fysiske legitimasjon i forbindelse med ulike samfunnsoppgaver, gjennom bl.a. utstedelse av pass eller førerkort. Vi har erkjent behovet for et uavhengig offisiell identifikasjon gjennom nasjonalt ID-kort, som mange land allerede har innført, med elektronisk ID som en naturlig del av kortet, i flere av landene. Myndighetenes rolle som identitetsforvalter, med utstedelse av fysiske bevis for identitet, blir således utvidet i den elektroniske verden. Det er derfor naturlig at offentlige myndigheter også kan påta seg ansvaret for den elektroniske identiteten til innbyggere, særlig i tilknytning til bruk av elektroniske tjenester fra det offentlige.

Alternative identitetsutstedere i den elektroniske verden er aktører i markedet, som f.eks. bankene. Utbredelsen av deres eID-løsninger går imidlertid sakte, og det er vanskelig for offentlige virksomheter som utvikler tjenester på nett å basere seg på at innbyggere skaffer seg en eID fra en av disse. Offentlig utstedt eID (på nasjonalt ID-kort) vil kunne supplere

---

[25] Jf. forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere

[26] eForvaltningsforskriften av 25. juni 2004 nr. 988, utarbeidet med utgangspunkt i anbefalinger fra PKI-utvalget, jf. NOU 2001:10. og hjemlet i forvaltningsloven § 15 a og e-signaturloven § 5.

markedsaktørenes løsninger og gi raskere dekning av befolkningen med en eID. Videre innebærer bruk av private aktørers eID i offentlige nettjenester en kostnad for offentlige virksomheter som kan være vanskelig å forutse. Offentlig sektor trenger styring og kontroll med bruken av eID, både når det gjelder kvalitet og sikkerhet, men også når det gjelder kostnader som kan påløpe i denne sammenheng. Etablering av et nasjonalt ID-kort med offentlig utstedt eID kan gi den type styringsmuligheter. En slik løsning kunne samtidig være en stimulans for markedet til å levere løsninger som er bedre tilpasset behovene til, og til lavere kostnad for, det offentlige.

12.3.2 Utfordringer ved eID i offentlig regi - personvern

Etablering av en universell eID i offentlig regi kan samtidig skape noen utfordringer – som f.eks. sårbarhet ved at innbyggeren får en "generalnøkkel" til mange tjenester på nett. Ønsket om forenkling av hverdagen for en Internett-bruker må balanseres mot den erkjennelsen at mange gjerne vil opptre anonymt i enkelte sammenhenger, og at identitetsbevis utstedt i sammenheng med bestemte forhold (eks. etablering av en nettbankavtale) ikke nødvendigvis ønskes benyttet til andre formål.

Enkelte innbyggere vil gjerne ha et valg mellom en eID til kommunikasjon med det offentlige og andre eID til kommunikasjon med banken, nettbutikken eller flyselskapet for kjøp av billetter, osv.

Etablering av et offentlig alternativ til bankene og andre markedstilbydere vil kunne bidra til at innbyggeren får en slik valgmulighet.

Samtidig vil det være viktig å bevisstgjøre innbyggere på sammenhenger der eID ikke bør benyttes, særlig der anonymitet er vesentlig for å sikre personvernet og integriteten til nettbrukeren.

Bruk av elektronisk signatur kan samtidig anses som personvernfremmende siden slik bruk med stor sannsynlighet vil bidra til beskyttelse av personopplysninger. Dette vil være avhengig av blant annet følgende:

- typer opplysninger som skal registreres
- databehandlingsprosedyrene
- hvem skal ha tilgang til opplysningene
- personers rettigheter
- hvem kan bestemme hva som skal lagres som innholdet i eID'en
- hvilke kommersielle formål kan den anvendes mot
- sikkerhetstiltak ved bruk

I forbindelse med realisering av formålet med et offentlig alternativ må man bl.a. ta i betraktning hensynet til å sikre brukerne valgfrihet når det gjelder hvilken eller hvilke eID'er de vil benytte og fra hvilke utstedere. Det må også sikres at man, både av personvernhensyn og av konkurransehensyn, unngår å skape en situasjon der andre tilbydere av eID presses ut av markedet slik at alle brukere i praksis bare har én eID som brukes til alt.

I lys av dette og erfaringer med utvikling av andre lands nasjonale ID-kort, vil vi derfor besvare spørsmålet om hvordan inkludering av en elektronisk ID på nasjonalt ID-kort best kan løses. En slik mulighet vil høyne kortets verdi for brukeren. Dette ved at innehaveren, i tillegg til å få et

forenklet reisedokument, og et uavhengig ID-kort til generelt bruk, også kan benytte kortet som bærer for elektronisk ID, som kan benyttes f.eks. mot offentlige tjenester på nett.

I denne sammenheng forutsetter vi at det skal utstedes et nasjonalt ID-kort som er utstyrt med en kontaktchip for lagring av en eID. Det er derfor ikke gjort noen vurdering av om man bør starte utstedelse av eID på helt selvstendig grunnlag, og til andre kort enn det nasjonale ID-kortet.

12.3.3 Hva slags eID, målgruppe

eID skal baseres på sertifikatklasse Person Høyt slik det er definert i Kravspesifikasjon for PKI i offentlig sektor, publisert i januar 2005. Anbefalingen er gjort ut fra vurderinger av det norske markedet som er segmentert og lite modent, og det anses derfor som lite hensiktsmessig å etablere enda ett sikkerhetsnivå. Person Høyt er et sikkerhetsnivå som har fått gjennomslag i markedet og samtidig sikrer god nok kvalitet på en eID som kan bli brukt i stor utstrekning. Dette valget legger imidlertid føringer for organiseringen av utstedelsen, særlig når det gjelder identitetskontroll. Av hensyn til bl.a. kostnader og sikkerhet bør politiets infrastruktur i størst mulig grad gjenbrukes for bl.a. identitetskontroll, dvs kontroll av legitimasjonspapirer mv.

Primærmålgruppen for eID vil være norske statsborgere og personer med fast opphold i landet. Det følger av retningslinjene for sertifikater (eID) utstedt iht Kravspesifikasjon for PKI i offentlig sektor, at eID-innehaveren må ha norsk fødselsnummer eller D-nummer. Hvis sertifikater skal utstedes til personer uten endelig fastslått identitet kan det antakelig ikke utstedes som et kvalifisert sertifikat. Ettersom et kvalifisert sertifikat gjennom esignaturdirektivet er anerkjent i hele EØS-området, vil det ikke være mulig å ta forbehold i forhold til kvaliteten på den identitetskontroll som er foretatt før sertifikatet er utstedt, eller i forhold til at identitet ikke er endelig fastslått. Hvis eID skal utstedes i disse tilfellene må den utstedes med referanse til andre retningslinjer og ikke som et kvalifisert sertifikat. Politiet, eller eventuelt et annet forvaltningsorgan, som registrerer søknad om utstedelse av sertifikat i slike tilfelle, må påse at søknaden tydelig merkes med at identitetskontrollen er mangelfull, slik at sertifikatutstederen kan utstede riktig type sertifikat.

12.3.4 Praktiske forutsetninger for utstedelse av eID

I utgangspunktet gir eID ingen anvisning på hvor sertifikatinnehaveren har sin faste bopel, men derimot hvor sertifikatutstederen er etablert. Opplysninger om innehaverens oppholdsadresse må brukerstedene eventuelt innhente fra sertifikatutstederen. Det vil vanligvis følge av avtalen som eID-innehaveren har med sertifikatutstederen at adresseendring skal meldes til sertifikatutstederen. Hvis det er grunnlag for å inndra selve ID-kortet i forbindelse med utflytting vil imidlertid eID-innehaveren også miste disposisjonsretten over eID'en i og med at den er lagret på kortet.

Videre vil det ikke være aktuelt å tilby mer enn én eID på det nasjonale ID-kortet, uansett om den er fra en offentlig eller privat utsteder. Alle nasjonale ID-kort skal innholde en eID allerede ved utlevering. Derimot kan det diskuteres om eID må aktiveres for å kunne brukes, eller om den er klar til bruk i utgangspunktet og kan deaktiveres om brukeren ønsker det. Aktivering/deaktivering bør kunne skje på nettet, og det må finnes en sentral brukerstøttefunksjon for å hjelpe med dette. Vi legger til grunn at det nasjonale ID-kortet, på lik linje med passet, skal sendes innehaveren pr. post, og det vil derfor ikke være mulig for utsteder å aktivere/deaktivere eID ved utleveringen. Brukeren må derfor få veiledning om hvordan vedkommende kan utføre dette selv.

Vi legger til grunn at eID'en vil utgjøres av ***to nøkkelpar***, der det ene paret skal benyttes til autentisering ved pålogging til nettsider samt til dekryptering av mottatte krypterte meldinger, mens det andre paret skal benyttes til signering, jf. vedlegg B. Det legges videre til grunn at aktivering av nøkkelparet for autentisering kan skje fra fylte 13 år, mens aktivering av nøkkelparet for signering kan skje fra fylte 18 år.[27] Begrunnelsen er at ungdom allerede fra 13 års alder kan ha behov for å autentisere seg overfor forvaltningsorganer, f eks. i forbindelse med søknad om eller endring av skattekort, mens nøkkelparet som skal benyttes for signering, og forutsetningsvis for å foreta rettslig bindende disposisjoner, naturlig bør knyttes til myndighetsalderen på 18 år. Begge nøklene skal beskyttes av samme PIN-kode. I praksis vil det være signaturfremstillingssystemet som velger nøkkel og sertifikat basert på den aktuelle transaksjonstype og tilgjengelige sertifikater, og det vil følgelig være enklere for brukeren å ha én kode å forholde seg til. Man kan heller ikke regne med at brukere alltid selv er seg bevisst forholdet mellom de ulike nøklene, eller at de overhodet har "mer enn en eID". Da vil det uansett være lite hjelp i å benytte forskjellige pin-koder for de to nøklene. For mange koder kan dessuten øke sannsynligheten for at kodene blir notert ned og på den måten utgjøre en sikkerhetstrussel.

I tillegg til aldersbegrensningen kan det også legges begrensninger i eID-info som vil sikre at nøklene ikke benyttes for disposisjoner som de ikke er ment for (eks. beløpsbegrensninger).

12.3.5 Ulike måter å organisere utstedelsen av eID på

Det finnes to mulige måter å plassere en eID i et nasjonalt ID-kort:

1. Gjennom offentlig utstedelse av nøkler og sertifikater
2. Gjennom markedsbasert utstedelse av nøkler og sertifikater

I det første tilfellet vil det være én offentlig sertifikatutsteder som vil stå for utstedelse, vedlikehold og ansvar for eID og e-signatur, i samarbeid med den offentlige myndigheten som vil få i oppdrag å utstede nasjonalt ID-kort. Brukeren vil ha valgmulighet til ikke å ta i bruk eID, selv om den befinner seg i kortet. Denne modellen benyttes blant annet i Finland, der det nasjonale Folkeregistersenteret er en slik offentlig sertifikatutsteder, og politiet er den myndighet som utsteder selve kortet.

Det er ikke problematisert hvorvidt det kan bli et tillitsproblem om det offentlig selv utsteder eID som senere skal benyttes til å sikre kommunikasjonen med det offentlige, og sikre dokumentasjon av prosesser, handlinger og meldinger i samhandlingen mellom det offentlige og privatpersoner og virksomheter.

I det andre tilfellet legges det opp til at sertifikatutstedere i markedet får anledning til å utstede sertifikater for nøkler som vil plasseres i kortet. Brukeren kan da f.eks. få et valg ved utstedelse av kortet om vedkommende ønsker eID lagt inn, og da fra hvilken privat sertifikatutsteder. Det offentlige kan videre begrense dette valget, ved at kun godkjente utstedere får adgang til å legge inn en eID i et nasjonalt ID-kort. Det offentlige vil også måtte sørge for en felles standard / grensesnitt for innlegging av eID i kortet, som er uavhengig av utstederes teknologivalg. Denne løsningen ble valgt i Sverige for deres nasjonale ID-kort, men er ennå ikke operasjonalisert i

[27] Et kvalifisert sertifikat, som reguleres i esignaturloven, kan brukes til autentisering eller signering. Esignaturloven oppstiller ikke noen skranker ifht. alder og utstedelse av kvalifiserte sertifikater. Det betyr i praksis at et kvalifisert sertifikat kan utstedes til hvem som helst, uansett alder. Det er imidlertid neppe hensiktsmessig å utstede et slikt sertifikat til noen som pga. sin lave alder ikke teknisk kan bruke det eller ikke kan foreta den aktuelle disposisjonen av rettslige grunner.

praksis, slik vi forstår det. Den praktisk mest sannsynlige løsningen ville være at det offentlige inngår en avtale med én privat utsteder som vil stå for eID som legges inn i kortet.

12.4 Bruk av elektronisk ID på nasjonalt ID-kort

Elektronisk ID skal kunne benyttes til følgende formål:

- Autentisering ved pålogging til nettsider
- Digital signering av skjema på nettsider eller dokumenter i f.eks. Word eller PDF-format
- Digital signering av e-post
- Dekryptering av mottatte krypterte e-post, dokumenter eller andre typer elektroniske meldinger

Det legges til grunn at eID skal kunne benyttes til offentlige så vel som private tjenester på Internett. Bruk av eID til private tjenester skjer på disse tjenesters egne vilkår og kan påføre brukeren kostnader. Bruk av eID til offentlige tjenester på Internett skal være kostnadsfritt.

For en bruker vil motivasjonen for å skaffe seg et ID-kort med eID øke dersom vedkommende visste at eID kan benyttes til flere tjenester enn de fra offentlig sektor, som foreløpig er få og der kontakten skjer med ikke så stor grad av hyppighet. Det er en anstrengelse for brukeren å søke om, og møte opp for å skaffe seg ID-kortet, videre foreta de nødvendige skritt for å kunne benytte eID (anskaffe kortleser og aktivere eID). Det er derfor fornuftig å åpne for at private tjenestetilbydere på Internett skal kunne benytte denne eID. Den offentlige utstederen av eID skal, på grunnlag av bl.a. vurdering av tjenestetilbyderens seriøsitet, forretningsskikk, og evne til å ivareta personvern, avgjøre hvordan tilgangen til eID skal skje.

Det skal lages sentrale retningslinjer, myntet på brukersteder, for bruk av eID til pålogging og/eller signering av skjema i tjenester på Internett. Retningslinjene skal følges av alle tjenester som vil ta i bruk denne eID til autentisering av brukere eller signering av skjema. Formålet med retningslinjene skal bl.a. være å sikre at bruken av eID og/eller e-signatur støtter opp under godt personvern. Unødig bruk av logging og lagring av transaksjoner knyttet til autentisering bør unngås. Bruk av elektronisk signatur er mindre problematisk, da brukeren foretar en overveiet handling og den er begrenset til en konkret kommunikasjon (dokument eller skjema).

Retningslinjene bør bl.a. omhandle følgende problemstillinger:

- Vilkår for tilgang til valideringstjenester (merkantile og juridiske), herunder også hva slags informasjon som kan/skal utleveres til et brukersted (minimum nødvendig for autentisering i en gitt sammenheng)
- Vilkår for behandling av personopplysninger knyttet til bruk av eID, herunder vilkår for tilgang til fødselsnummer og hvem som kan få slik tilgang
- Teknologiske forutsetninger for bruk av eID – hva må til for at brukerstedet kan koples til valideringstjenesten mv.
- Varsling om behov for sperring/adgang til å sperre bruken av eID, herunder om samspillet mellom brukerstøtte hos tjenestetilbyderen og brukerstøtte hos den offentlige utsteder

For at brukeren skal kunne benytte sin eID på nasjonalt ID-kort vil vedkommende ha behov for en kortleser. Det legges i utgangspunktet til grunn at brukeren vil ha ansvaret for å skaffe seg en kortleser. Den ansvarlige utstederen av eID bør da lage en liste over godkjente/anbefalte kortlesere som finnes i det norske markedet. Det bør også vurderes hvorvidt offentlig sektor, med utgangspunkt i sin interesse for at tilstrekkelig mange privatpersoner besitter og kan bruke

en eID, etablerer et program for tilrettelegging av kortleserdistribusjonen. Dette kan gjøres ved f.eks. å innlede et samarbeid med IKT-bransjen om å tilby kortleser som en standarddel i PC-utstyret og/eller tilby kampanjer rettet mot spesielle målgrupper (som f.eks. ungdom) der kortleseren ev. subsidieres av det offentlige.

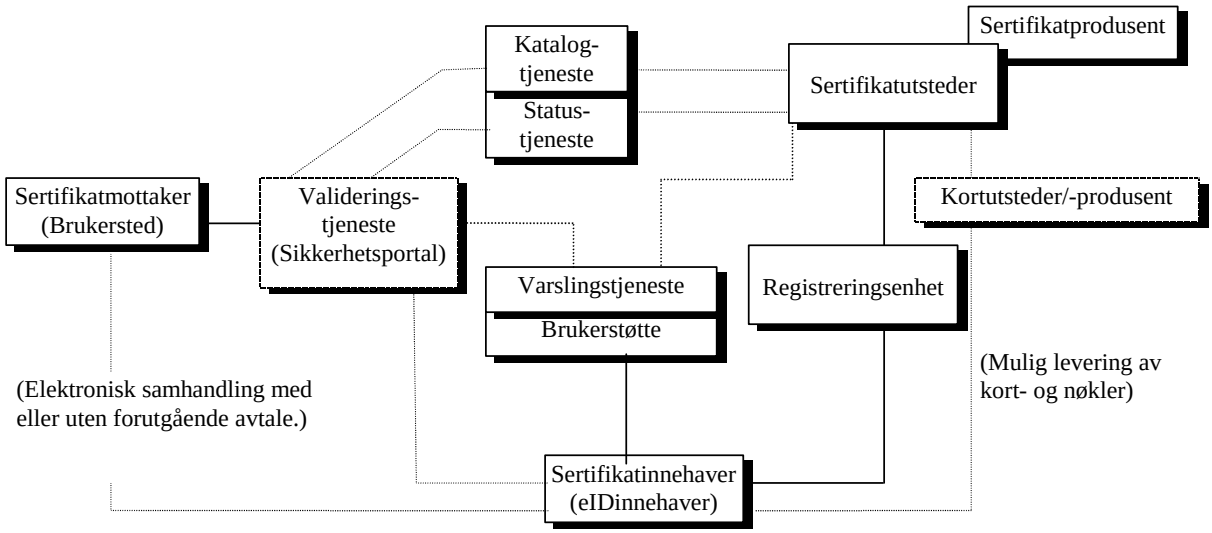
Uavhengig av eventuelle tiltak for distribusjon av kortlesere, bør det samtidig med opprettelsen av en eID-utsteder for nasjonalt ID-kort etableres en brukerstøttefunksjon med mulighet for direkte kontakt enten via telefon eller e-post, som skal gi veiledning og informasjon til publikum i forbindelse med bruken av eID. Denne funksjonen bør samarbeide med brukerstøtten som er etablert, eller vil etableres, av de ulike tilbydere av nettjenester, som vil gjøre bruk av denne eID. Disse støttefunksjoner vil ta for seg selve tjenesten, og bruk av eID mot/i den.

12.5 Det offentlige som utsteder av elektronisk ID.

12.5.1 Mulige modeller for organisering

I denne utredningen forstår vi med elektronisk ID løsninger basert på asymmetrisk kryptering (med bruk av privat og offentlig nøkkel) og som benytter digitale sertifikater. Sertifikatene utstedes og administreres innenfor rammen av en *sertifikattjeneste*. I dette delkapitlet drøfter vi hvordan en sertifikattjeneste for utstedelse og bruk av eID kan organiseres.

I forbindelse med utstedelse, vedlikehold, administrasjon og bruk av sertifikater (eID) er det en rekke funksjoner/roller som er involvert og som til sammen utgjør sertifikattjenesten. De rollene som inngår i en sertifikattjeneste, og relasjonene mellom dem, er fremstilt i figuren nedenfor.



Figur 1: Mulig struktur for en sertifikattjeneste.

Begrepet ***sertifikattjenesten*** benyttes her om summen av de funksjoner som utgjør en fungerende sertifikattjeneste.

Den sentrale rolleinnehaveren i sertifikattjenesten er ***sertifikatutstederen***. Sertifikatutstederen er den sertifikatet *utpeker* som utsteder. Denne rollen vil antakelig tilligge en sentral offentlig etat som i sertifikatet vil fremstå som utsteder. Sertifikatutstederen kan f.eks. være

Justisdepartementet. Dette kan være naturlig hvis eID skal utstedes ved gjenbruk av infrastrukturen for pass. Alternativt kan man tenke seg at eID utstedes av Folkeregisteret eller av Registerenheten i Brønnøysund. De praktiske oppgavene med å realisere sertifikattjenesten vil sertifikatutstederen vanligvis engasjere andre virksomheter til å utføre.

Teknisk produksjon av sertifikatet kan være lagt til en særskilt ***sertifikatprodusent***. Dette er primært en teknisk produksjonsoppgave, som kan settes ut til en privat virksomhet som drifter en tilstrekkelig pålitelig tjeneste for dette formålet. Men de kravene som stilles til sertifikat og sertifikatprodusenten i kravspesifikasjonen for PKI i offentlig sektor og tilknyttede standarder må være oppfylt. Sertifikatprodusenten og andre aktører som skal fylle utførende roller i sertifikattjenesten vil bli valgt i markedet etter konkurranse i henhold til regelverket for offentlige innkjøp.

Dataene som benyttes i sertifikatet hentes inn av en ***registreringsenhet***. Registreringsenheten samler inn de data som er nødvendige i forbindelse med utstedelse av sertifikat, kontrollerer og verifiserer den kommende sertifikatinnehaverens identitet og formidler de nødvendige data til sertifikatutstederen. Verifisering av dataene kan eventuelt skje i to operasjoner, f.eks. slik at den endelige identitetskontrollen skjer i forbindelse med utlevering av kort eller aktivisering av eID. Registreringsenheten er en kritisk rolle i forhold til terskelen for å skaffe seg et ID-kort med eID. For å få brukere til å søke om en offentlig utstedt eID på *selvstendig grunnlag*, uten at de samtidig har behov for det nasjonale ID-kortet til annet enn å være bærer av eID'en, er det nødvendig å gjøre prosessen så smidig som mulig. Dette stiller krav til fysisk nærhet mellom der sertifikatinnehaveren bor eller holder til, og der registreringsenheten er lokalisert, eller at den innledende kontakten med registreringsenheten kan oppnås over Internettet. Det kunne kanskje være formålstjenlig å utsette legitimasjonskontrollen til kort mv. skal utleveres, slik at søknadsprosessen for sertifikatinnehaveren blir enklest mulig, men dette kan være uforenlig med prosedyrene for utstedelse av det nasjonale ID-kortet som vil kreve at søkerens underskrift innhentes før kortet produseres. Vi kommer tilbake til dette i et særlig avsnitt om registreringsenheten nedenfor. Hvis sertifikatutsteder skal være Justisdepartementet, og gitt at man skal benytte politiets infrastruktur ifm utstedelse av det nasjonale ID-kortet, vil det være naturlig at registreringsenheten legges til de samme lokale politistasjoner eller lensmannskontorer som behandler søknader om ID-kort.

Generering av krypteringsnøkler og eventuelt nedlasting på nøkkelbærende medium som smartkort eller lignende kan være lagt til en særskilt enhet. Antakelig er det mest hensiktsmessig at nedlastingen skjer i forbindelse med produksjon av kortet hos en ***kortutsteder/-produsent***. Alternativt kan det skje i forbindelse med utlevering av kortet. Det vil i praksis bety at registreringsenheten laster nøklene ned på kortet. Hvis det ferdig produserte kortet (med nøkler) utleveres ved at det sendes til sertifikatinnehaveren med vanlig A-post, vil det være nødvendig med en egen prosedyre for utlevering av PIN-koder (for tilgang til nøklene på kortet). Dette kommer vi tilbake til i et særlig avsnitt om registreringsenheten nedenfor. Kortutstederen/-produsenten må samarbeide med sertifikatprodusenten i forbindelse med generering og nedlasting av nøkler og sertifikat på kortet. Ettersom eID skal lastes ned på det nasjonale ID-kortet vil kortutstederen være gitt av det valg som blir gjort ifm nasjonalt ID-kort.

Katalogtjenesten systematiserer, oppbevarer og gjør tilgjengelig sertifikater fra en sertifikatutsteder i form av en katalogtjeneste. Katalogtjenesten kan også gjøre tilgjengelig relevante tilleggsopplysninger om sertifikatinnehaveren, f.eks. vedkommendes fødselsnummer eller andre relevante opplysninger som sertifikatutstederen har registrert om sertifikatinnehaveren. Utlevering av slike opplysninger som fødselsnummer o.l. kan være organisert som en egen tjeneste eller et eget tjenestenivå innenfor katalogtjenesten. En

valideringstjeneste (jf. nedenfor) vil typisk hente opplysninger herfra i tillegg til fra statustjenesten. Katalogtjenesten skal være tilgjengelig ved hjelp av elektronisk kommunikasjon, og det spiller antakelig mindre rolle for realisering av formålet med offentlig utstedt eID hvilken organisasjon som utfører disse oppgavene på sertifikatutsteders vegne og hvor organisasjonen er lokalisert. Tjenesten skal imidlertid utøves i henhold til retningslinjer gitt av sertifikatutstederen. Tjenesten kan kjøpes fra en privat virksomhet og kan være samlokalisert med katalogtjenester for andre sertifikatutstedere.

For å opprettholde et hensiktsmessig sikkerhetsnivå er det nødvendig med prosedyrer som gjør det mulig å trekke tilbake, eller gjøre ugyldige, sertifikater knyttet til nøkler som av en eller annen årsak ikke lenger skal benyttes. Dette organiseres innenfor rammen av en ***varslingstjeneste*** og distribueres via en ***statustjeneste*** som *kan* være samlokalisert med katalogtjenesten, men den behøver ikke være det. Varslingstjenesten må være lett tilgjengelig for sertifikatinnehaveren, men i og med at kommunikasjonen vanligvis vil skje elektronisk, per telefon eller brev, spiller det antakelig også her liten rolle hvilken organisasjon som utfører disse oppgavene på vegne av sertifikatutsteder. eID-innehaverne kan også ha behov for brukerstøtte ifm eventuell installering av kortleser og programvare på egen maskin, og ifm bruk av sin eID. Brukerstøtte og varslingstjenesten kan tilbys av det offentlige selv eller av en privat virksomhet. Brukerstøtte vil antakelig kreve en ikke ubetydelig kapasitet til å behandle henvendelser. Man kan tenke seg at politiet, som også er registreringsenhet, kan drive en døgnåpen varslingstjeneste, mens brukerstøttetjenesten kjøpes inn fra en privat virksomhet.

Forsvarlig bruk av eID forutsetter at brukerstedet har forvisset seg om at sertifikatet er egnet for den aktuelle bruk og at det ikke er trukket tilbake. På grunn av de praktiske vanskeligheter med å innhente den nødvendige informasjon om sertifikattjenestens egnethet for brukerstedets formål, vil det være behov for en ***valideringstjeneste*** som på brukerstedets vegne utfører oppgaven. Valideringstjenesten er en viktig rolle for effektiv bruk av sertifikater. Også denne tjenesten vil være tilgjengelig elektronisk, og det spiller således liten rolle hvor den er lokalisert. Derimot har det stor betydning hvordan den er organisert. Vi kommer tilbake til dette i et eget avsnitt nedenfor. Valideringstjenesten kan være en del av en ny offentlig sikkerhetsportal, eller den kan kjøpes i markedet (slike tjenester er tilgjengelige i markedet).

En annen viktig aktør er den som skal utnytte sertifikattjenesten – nemlig *brukeren*. Brukeren opptrer i to roller. Vi bruker i det følgende begrepet ***sertifikatinnehaver*** om den som rettmessig disponerer et sertifikat, d.v.s. utpekes i sertifikatet som innehaver av den offentlige nøkkelen i sertifikatet (eID-innehaveren). Videre benytter vi begrepet ***sertifikatmottaker***, om den som foretar en handling på grunnlag av validert sertifikat (eID), typisk et brukersted, f.eks. en offentlig virksomhet.

12.5.2 Særlig om registreringsenheten og valideringstjenesten

Organiseringen av registreringsenheten og valideringstjenesten er sentral for utbredelse og praktisk bruk av eID. De er også sentrale komponenter i forhold til kvaliteten på opplysningene som inngår i, eller er knyttet til, en eID, og mulighetene for forsvarlig bruk av eID på sertifikatmottakersiden (hos brukerstedene).

Nærmere om registreringsenheten

Registreringsenheten kan organiseres slik at søknad om eID skjer ved personlig fremmøte hos registreringsenheten, og at legitimasjonskontroll mv skjer i forbindelse med innlevering av søknaden, slik ordningen er f.eks. for pass i dag. Det kan imidlertid være aktuelt å se på andre løsninger, f.eks. mulighetene for å benytte en "omvendt" registreringsenhet, der identitetskontroll

først skjer ved utlevering av kort. Søknad om eID kan da skje på nettet, f.eks. ved å gjenbruke SKDs PIN-kodeløsning som adgangskontroll til registreringsløsningen eller tilsvarende PIN-kodeløsning fra Altinn. Det er mulig at en slik fremgangsmåte vil senke igangsettingsterskelen for brukeren i forhold til en ordning der prosessen først starter når vedkommende oppsøker en politistasjon eller lignende for å søke om en eID. På den annen side kan det være hindre for en slik løsning knyttet f.eks. til at sertifikatinnehaverens håndskrevne underskrift skal fremkomme på det ID-kortet som nøklene skal lagres på, og underskriften må da samles inn før kortet produseres.

Det kan også finnes andre alternativer til organisering av registreringsenhetens virksomhet enn den "standard" løsning der enkeltpersoner må oppsøke registreringsenheten for å levere sin søknad om eID og samtidig få kontrollert sine legitimasjonspapirer mv. Søknad om eID kan f.eks. skje på nettet, ved bruk av eksisterende PIN-kodeløsning som beskrevet ovenfor. På dette grunnlaget kan produksjon av kort og koder forberedes. Når relevante kontroller er gjennomført, og nødvendige data innhentet fra bl.a. Folkeregisteret, kan brukeren varsles, f.eks. ved hjelp av SMS, om at søknadsdokumentene er klare til undertegning på nærmeste politistasjon eller lensmannskontor. I forbindelse med innsending av søknaden kan det sendes en SMS til søkeren der han bes om å bekrefte at det mobiltelefonnummeret vedkommende har oppgitt for å motta varsel er riktig registrert i søknaden. I tillegg bør det etableres en prosedyre der varsel om at søknadsdokumentene er klare til undertegning sendes ut som tradisjonelt brev hvis søkeren ikke møter innen f.eks. 14 dager etter at varsel er sendt på SMS, sml. prinsippene bak syvdagers-fristen i eForvaltningsforskriften[28] § 8.

Det er mulig at en slik fremgangsmåte vil senke igangsettingsterskelen for brukeren i forhold til en ordning der prosessen først starter når vedkommende oppsøker en politistasjon eller lignende for å søke om en eID. Det er mulig at ordningen også vil føre til mindre ventetid og behandlingstid i forbindelse med fysisk fremmøte på politistasjonen. Vi mener den samme fremgangsmåten også kan benyttes i forbindelse med søknad om pass, slik at man får én felles prosedyre og infrastruktur for søknad om pass, nasjonalt ID-kort og eID. Dette vil kunne ha gunstige effekter på effektiviteten i passekspederingen og forenkle arbeidet med passutstedelse, i tillegg til at man oppnår koordinerte og ensartede prosedyrer for søknad om nasjonale identitetsdokumenter.

I forbindelse med en ordning der søknad leveres over nettet, med fysisk fremmøte etter at søknaden er behandlet og tilrettelagt for underskrift mv, kan det være hensiktsmessig at nødvendige PIN-koder for bruk av kort med eID utleveres i forbindelse med fremmøte og legitimasjonskontroll. Dette vil kunne gi god sikkerhet for at sertifikatinnehaveren faktisk har kontroll over eID når den første gang tas i bruk fordi dette ikke kan skje uten tilgang til PIN-koden som ble utlevert i forbindelse med fremmøte (sml. kravene i esignaturloven § 3(2) og § 22 første ledd, bokstav d). Under en slik ordning skulle forholdene ligge til rette for at kortet kan sendes ut til sertifikatinnehaveren med vanlig A-post når det er ferdig produsert. Man kan naturligvis tenke seg at sertifikatinnehaveren, i forbindelse med søknad om kort og eID, kan be om å få hente kortet på politistasjonen eller et offentlig kontor, men dette synes ikke å være nødvendig for å oppnå tilfredsstillende sikkerhet i løsningen dersom PIN-koden er utlevert i forbindelse med fysisk fremmøte. En ordning med alternativ utlevering av kort vil også virke fordyrende i forhold til postutsendelse. Hvis utsendelse skal skje til annet enn folkeregistrert adresse kan dette registreres i forbindelse med nettsøknaden og bekreftes i forbindelse med fysisk fremmøte.

[28] Forskrift til forvaltningsloven om elektronisk kommunikasjon med og i forvaltningen, sist endret desember 2005.

En spesiell problemstilling er hvorvidt utenriksstasjoner kan ivareta oppgaver til en registreringstjeneste. I utgangspunktet ligger det ikke noe i veien for det, men en slik rolle vil forutsette at stasjonen har tilgang til det norske folkeregisteret, for validering av identiteten til en søker. Dersom dette ikke er tilfelle, må søknaden oversendes til en norsk politistasjon el.l. der slik validering kan skje. Deretter kan søkeren møte opp på utenriksstasjonen for å legitimere seg og avgi biometrisk informasjon, samt motta en PIN-kode konvolutt. I dette tilfellet vil det også antagelig være fornuftig at selve kortet blir sendt til utenriksstasjonen, som enten varsler søkeren om å hente det eller videresender kortet til registrert oppholdsadresse.

Nærmere om valideringstjenesten

Valideringstjenesten er betegnelsen på en rolle, og kan i prinsippet ivaretas av sertifikatmottakeren selv, men for brukersteder som aksepterer sertifikater fra flere utstedere vil det nok i mange tilfeller være hensiktsmessig å sette bort valideringstjenesten til andre. For forvaltningens del var "den offentlige sikkerhetsportalen" tiltenkt denne oppgaven. Det arbeides med en strategi for reetablering av sikkerhetsportalen, eller en variant av denne, som skal ivareta oppgaver på vegne av det offentlige.

Valideringstjenesten skal primært ivareta oppgaver knyttet til validering av sertifikat, men vanligvis ikke andre oppgaver knyttet til prosessen med verifisering av en elektronisk signatur. Det kan være grunn til å skille mellom disse to begreper. Validering av sertifikat omfatter bl.a. oppgaven med å innhente statusopplysninger om sertifikatet og verifisere at det faktisk er utstedt av den oppgitte utsteder. I tillegg kan valideringstjenesten være tillagt oppgaven med å kontrollere at sertifikatet er egnet for den aktuelle bruk, og at sertifikatutstederen tilfredsstiller de krav som følger av sertifikatmottakerens sikkerhetsstrategi, jf. prinsippene som er nedfelt i eForvaltningsforskriften § 25 og § 13. I tillegg kan valideringstjenesten medvirke til å distribuere tilleggsopplysninger om sertifikatinnehaveren som sertifikatmottakeren trenger for å kunne avgjøre hvem sertifikatinnehaveren er eller hva vedkommende anses autorisert til å gjøre. Aktuelle tilleggsopplysninger kan i visse tilfeller være et fødselsnummer. Det kan også dreie seg om et kundenummer, kjønn og fødselsår el.l. i situasjoner der det ikke er relevant, eller ikke behov for, å utlevere fødselsnummer eller andre opplysninger som identifiserer vedkommende. Dette vil avhenge av i hvilken sammenheng eID'en benyttes i.

Valideringstjenesten vil altså kunne ha flere funksjoner: å sikre at de eID'er som benyttes tilfredsstiller de kravene som brukerstedet har stilt (at kravene i Kravspesifikasjon for PKI i offentlig sektor er oppfylt), å kontrollere at eID'en fortsatt er gyldig, og å sørge for å innhente de tilleggsopplysninger brukerstedet trenger i den aktuelle brukssituasjonen. Valideringstjenesten kan også ha i oppgave å varsle sertifikattjenesten dersom det er mistanke om at en eID er kommet på avveie eller blir misbrukt m.v., samt vedlikeholde en forvaltningsintern tjeneste for å nekte bruk av elektronisk kommunikasjon med forvaltningen, i henhold til eForvaltningsforskriften § 12. Sperring av sertifikatet som sådan, som følge av misbruk, og med virkning også for andre enn forvaltningens brukersteder, må imidlertid følge retningslinjene som sertifikatutstederen har fastsatt for sperring av det enkelte sertifikat.

Valideringstjenesten utfører sine oppgaver etter retningslinjer gitt av brukerstedene og tilpasset behovene til det enkelte brukersted.

Valideringstjenesten kan organiseres som en integrert del av en ny sikkerhetsportal, eller den kan organiseres som en selvstendig tjeneste som en ny sikkerhetsportal kan samvirke med. Det er også mulig å basere seg på eksisterende valideringstjenester i markedet som får tilgang til relevante deler av den offentlige sertifikattjenesten (statustjenesten og katalogtjenesten).

Valideringstjenesten kan driftes av det offentlige selv eller den kan kjøpes i markedet etter konkurranse i henhold til regelverket for offentlige anskaffelser. I begge tilfeller må valideringstjenesten være i stand til å håndtere både offentlig utstedt eID, og eID basert på andre sertifikattjenester i markedet. I denne utredningens sammenheng er det nærliggende å se på behovet for en valideringstjeneste sammen med behovet for en "offentlig sikkerhetsportal" som tilrettelegges for ulike typer eID, herunder den som vil utstedes på nasjonalt ID-kort (jf. kap 12.3).

12.5.3 Åpen eller lukket status- og katalogtjeneste – tilgang til statusopplysninger om sertifikatet og tilleggsopplysninger om eID-innehaveren

En ordning med offentlig utstedt eID kan gjøres tilgjengelig for gjenbruk også mellom private parter hvis det anses hensiktsmessig, jf. kap. 12.3.

En offentlig utstedt eID vil ha et høyt pålitelighetsnivå, og vil ha et potensial for gjenbruk i det private markedet. Dette forutsetter imidlertid, som et minimum, at private brukersteder får tilgang til statusopplysninger om sertifikatene. Det blir et politisk spørsmål om man vil åpne for gjenbruk i det private markedet, og åpen eller lukket statustjeneste vil være et virkemiddel for å realisere et slikt valg. Det vil også være et politisk valg om tjenesten skal kunne innkreve betaling for bruk av offentlig utstedt eID fra de private brukerstedene med utgangspunkt i en avtale om bruk av tjenesten med det enkelte brukersted.

I tillegg til statusopplysninger om sertifikatet vil private brukersteder, på samme måte som det offentliges egne brukersteder, også kunne ha behov for å få tilgang til tilleggsopplysninger om sertifikatene (fra katalogtjenesten). Det kan dreie seg om utlevering av fødselsnummer hvis brukerstedet har rettslig adgang til å behandle slike opplysninger, men det kan også dreie seg om å få utlevert f.eks. eID-innehaverens fødselsår for å kunne verifisere om vedkommende er gammel nok til å ta i bruk en bestemt tjeneste eller ung nok til delta i et bestemt diskusjonsforum på nettet eller lignende, men uten at det er nødvendig å få nærmere opplysninger om hvem vedkommende er (eks. chatte-tjenester på Internett).

Hvilke opplysninger brukerstedet skal få tilgang til vil avhenge av brukerstedets art og formålet med å benytte eID på brukerstedet. Tilgangen til ulike opplysningstyper kan reguleres gjennom avtale mellom brukerstedet og sertifikattjenesten, men man kan også tenke seg muligheten for å overlate denne oppgaven til valideringstjenesten, slik at denne tar seg av oppgaven med å kontrollere at brukerstedet får utlevert bare de opplysninger det har behov for og som det har lovlig adgang til å behandle. Retningslinjene for denne behandlingen får valideringstjenesten gjennom avtalen med sertifikatutstederen.

Ved å kontrollere tilgangen til status- og katalogtjenesten på denne måten kan det offentlige bidra positivt til at personvernhensyn ivaretas i forbindelse med bruk av en offentlig utstedt eID.

Spørsmålet om graden av tilgang til statustjenesten og katalogtjenesten spiller en sentral rolle i forbindelse med vurderingen av om man skal tillate gjenbruk av en offentlig utstedt eID i det private markedet, og i så fall i hvilket omfang og for hvilke formål.

12.5.4 Regulering av forholdet rollene i mellom

Nærmere om avtaler mellom ansvarlig utsteder og sertifikatprodusent m.m.
Ettersom det er sertifikatutstederen som har ansvaret for tjenestenes kvalitet i forhold til sertifikatinnehaverne og sertifikatmottakerne, og som har ansvaret overfor tilsynsmyndigheten når det utstedes kvalifiserte sertifikater, vil sertifikatutstederen også ha den sentrale rollen når det gjelder styring av de ulike relasjonene og ytelsene aktørene imellom innenfor sertifikattjenesten. På den annen side kan sertifikatutstederen ha satt bort hele eller deler av det kontraktsadministrative og operasjonelle oppfølgingsarbeidet til f.eks. en underliggende etat. Det vil være naturlig at sertifikatutstederen og den underliggende etaten i så fall formaliserer dette i form av en avtale. Dette kan være hensiktsmessig selv om sertifikatutstederen har hel eller delvis instruksjonsmyndighet i forhold til etaten på det aktuelle området. Det er bare *utførelsen* av oppgavene som kan delegeres eller settes bort. *Ansvaret* påhviler fortsatt sertifikatutstederen.

Også forholdet til sertifikatprodusenten, katalogtjenesten og statustjenesten vil det være naturlig at er regulert gjennom avtale med sertifikatutstederen, bl.a. fordi disse tjenestene sannsynligvis vil bli kjøpt inn fra private virksomheter. Kontraktene kan i disse tilfellene være inngått mellom tjenesteyterne og den etaten som har administrasjons- og oppfølgingsansvaret på vegne av sertifikatutstederen, men det forutsetter at kontrakten gir sertifikatutstederen reell kontroll- og styringsrett når det gjelder utførelsen av tjenestene.

Det bør vurderes om avtalen som inngås med kortprodusenten om utstedelse av ID-kort også skal dekke sertifikatutstederens krav til chip og nedlasting av nøkler m.v., eller om sertifikatutstederen skal inngå separat tilleggsavtale om dette. Antakelig er det mest praktisk at sertifikatutstederens krav beskrives i et eget bilag til avtalen om produksjon av kort, ikke minst hvis ansvaret for det nasjonale ID-kortet og eID blir lagt til samme etat.

Nærmere om forholdet mellom eID-katalog og ID-kort register
Det er nødvendig å koordinere forholdet mellom registeret for nasjonale ID-kort og registeret for eID. Blant annet må det organiseres slik at registrering av varsel om at et nasjonalt ID-kort har kommet på avveie også fører til oppdatering av registeret for eID. Det vanlige vil da være at eID'en trekkes tilbake og at dette registreres hos statustjenesten. Kortregisteret bør inneholde opplysninger om serienumrene til de sertifikatene som til enhver tid er lagret på kortet for å gjøre tilbakekalling av sertifikater i eID-registeret så effektivt som mulig. Derimot er det ikke nødvendigvis behov for noen direkte kopling motsatt vei. Det kan oppstå situasjoner der eID skal tilbakekalles uten at det får betydning for kortregisteret, det kan f.eks. tenkes at eID-innehaveren rett og slett ikke ønsker å bruke eID'en mer og derfor vil ha den sperret. I den utstrekning det er behov for å kople eID til kort kan det skje via fødselsnummeret som vil være registrert i begge registrene. Årsaken er at selv om en person kan ha flere sertifikater vil de alle være registrert på samme kort. Dersom levetiden for sertifikatet er kortere enn gyldighetstiden for det nasjonale ID-kortet, eller det ellers vil være tilfeller der nye eID'er utstedes til eksisterende ID-kort, kan det imidlertid være hensiktsmessig å vurdere den alternative løsningen som drøftes i kapittel 12.6.1., dvs. at sertifikatutstederen registrerer nummeret på det kortet som det enkelte sertifikat lastes ned på, for på den måten å ivareta koblingen mellom ID-kortet og de sertifikater som skal trekkes tilbake som følge av at det nasjonale ID-kortet er blitt sperret.

Nærmere om ansvaret for behandling av personopplysninger
Det vil være sertifikatutstederen som er behandlingsansvarlig når det gjelder behandling av personopplysninger etter personopplysningsloven i forbindelse med sertifikattjenesten. De øvrige

rolleinnehaverne vil være databehandlere etter denne modellen. Det innebærer at de bare kan behandle personopplysningene slik det er avtalt med den behandlingsansvarlige, at de har selvstendige forpliktelser etter loven til å ivareta tilfredsstillende informasjonssikkerhet, og at den behandlingsansvarlige og Datatilsynet har rett til å kontrollere virksomheten. Sertifikatutstederen skal inngå en databehandleravtale med tjenesteyterne som presiserer bl.a. disse forhold. Spørsmålet er om denne avtalen må inngås direkte mellom sertifikatutsteder og henholdsvis sertifikatprodusent, katalogtjenesten mv, eller om den kan inngås med den etaten som har administrasjons- og oppfølgingsansvaret på den behandlingsansvarliges vegne.

Etter lovens ordlyd skal databehandleravtalen inngås med sertifikatutstederen. Forutsatt at avtalen sikrer sertifikatutstederen den kontroll og innflytelse som loven krever, og tydelig identifiserer sertifikatutstederen som den behandlingsansvarlige, kan man likevel tenke seg at avtalen rent faktisk inngås med sertifikatutstederens "utførende hjelper" etter fullmakt. Helt konkret kan man f.eks. tenke seg at hvis Justisdepartementet er sertifikatutsteder, kan departementet inngå en avtale med Politidirektoratet om at direktoratet, på sertifikatutsteders vegne, inngår og følger opp avtalene med de enkelte tjenesteytere som inngår i sertifikattjenesten. Politidirektoratet vil i denne rollen verken være behandlingsansvarlig eller databehandler, men opptre på den behandlingsansvarliges vegne i en rolle vi f.eks. kan kalle avtaleforvalter. Politidirektoratet behøver ikke i denne rollen å formidle eller på annen måte behandle personopplysninger på vegne av den behandlingsansvarlige (sertifikatutstederen). Man kan kanskje likevel tenke seg at direktoratets rolle er slik at direktoratet og sertifikatutstederen har delt eller felles behandlingsansvar etter personopplysningsloven, selv om bare sertifikatutstederen er synlig utad (for sertifikatmottakeren) gjennom oppføring i sertifikatet. Overfor sertifikatinnehaveren vil direktoratet bl.a. ha selvstendig informasjonsplikt hvis det foreligger delt eller felles behandlingsansvar.

Nærmere om forholdet mellom eID-utsteder og registreringsenheten

Når det gjelder forholdet mellom sertifikatutsteder og registreringsenheten er det mindre opplagt at det skal avtalereguleres, men det må uansett utarbeides rutiner og prosedyrer som registreringsenheten skal følge, og som beskriver arbeidet og oppgavene. Det vil være litt avhengig av hvem som blir tildelt rollen. Hvis den fysiske identitets-/legitimasjonskontrollen, og eventuelt utlevering av kort eller PIN-koder, skjer hos politiet, på den lokale politistasjonen eller lensmannskontoret, vil forholdet kunne organiseres direkte under Politidirektoratet uten noen mellomliggende avtale. Ordningen blir i så fall at Politidirektoratet instruerer politietaten om å gjennomføre sertifikatutstederens rutiner og prosedyrer for registrering av sertifikatinnehavere (eID innehavere). Det er naturlig å se det slik at Politidirektoratet i denne sammenheng vil være databehandler i egenskap av registreringsenhet og utøver sine funksjoner ved hjelp av underliggende enheter.

Nærmere om regulering av eID-utstedelse

Det kan vurderes om hele eller deler av ordningen bør være forankret direkte i regelverket for å sikre stabilitet rundt rammebetingelsene for utstedelse av en offentlig utstedt eID og for å bidra til å sikre eID'ens troverdighet. På den annen side, hvis kravene til en offentlig utstedt eID, gjennom henvisning fra særlov, skal baseres på kvalifiserte sertifikater, vil en rekke av de sentrale krav til de ulike rollene i sertifikattjenesten være lovregulert gjennom esignaturloven. I tillegg vil en ordning med offentlig utstedt eID som skal benyttes av forvaltningsorganene være omfattet av kravet om selvdeklarering i henhold til forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere, jf. Fornyings- og administrasjonsdepartementets vedtak i henhold til eForvaltningsforskriften § 27(4).

Det er imidlertid begrenset adgang til å selvdeklarere de ulike *deler* av sertifikattjenesten hver for seg. Og i den utstrekning det er adgang til dette, forutsetter det at forholdet mellom sertifikatutstederen og de øvrige rollene er etablert på forhånd, slik at tilsynsorganet kan vurdere tjenestene under ett. Det innebærer i praksis at selvdeklarering av en ordning for offentlig utstedt eID, som er basert på samarbeid med private aktører som skal utføre ulike deler av tjenesten, må finne sted etter at en eventuell anskaffelsesprosess er gjennomført. Man kan altså ikke basere anskaffelsesprosessen på at de som skal fylle de ulike rollene i tjenesten hver for seg er registrert hos Post- og teletilsynet på forhånd. En slik ordning vil eventuelt kreve endring av retningslinjene for selvdeklareringsordningen.

I og med at en offentlig utstedt eID er underlagt tilsyn både etter lov om elektronisk signatur, omfattet av selvdeklareringsordningen for sertifikatutstedere, og av lov om behandling av personopplysninger, synes behovet for ytterligere regelverksforankring å være begrenset. Dersom det likevel skulle utarbeides en forskrift til særloven om utstedelse av nasjonalt ID-kort som regulerte nærmere enkelte forhold knyttet til utstedelse og bruk av en eID på dette kortet, vil det måtte foretas en nærmere vurdering av hvor forskriftskompetansen bør plasseres. Aktuelle departementer i denne sammenheng vil være JD, FAD og NHD.

12.5.5 Sertifikatutsteders erstatningsansvar for feil i sertifikatene og statustjenesten mv

Ansvarsgrunnlaget
Med utgangspunkt i at eID skal baseres på sertifikatklasse Person Høyt, og følgelig skal benytte kvalifiserte sertifikater, reguleres sertifikatutstederens erstatningsansvar av esignaturloven § 22 (så langt den rekker). Bestemmelsen suppleres av alminnelige erstatningsrettslige prinsipper.

Esignaturloven § 22 innebærer bl.a. at sertifikatutstederen etter omstendighetene kan holdes ansvarlig for tap en sertifikatmottaker lider som følge av at vedkommende har stolt på innholdet i et kvalifisert sertifikat. Sertifikatutstederen kan bl.a. holdes ansvarlig for at opplysningene i sertifikatet var korrekte på utstedelsestidspunktet og at sertifikatinnehaveren på det tidspunktet disponerte de aktuelle signaturfremstillingsdata, m.a.o. hadde kontroll over den private nøkkelen. Sertifikatutstederen kan også holdes ansvarlig for tap som skyldes at et sertifikat ikke var korrekt registrert i en tilbaketrekkingsliste eller statustjeneste, men derimot ikke tap som skyldes at signaturfremstillingsdata har kommet på avveie uten at dette er meldt til sertifikatutsteder. I alle tilfeller går sertifikatutsteder fri dersom utstederen dokumenterer at han ikke har handlet uaktsomt. Loven åpner for at utsteder kan avgrense sitt ansvar ved å angi begrensninger i bruksområde eller transaksjonsbeløp i sertifikatene.

Loven bygger på en forutsetning om at sertifikatmottakere i normalsituasjonen har rimelig grunn til å ha tillit til at kvalifiserte sertifikater tilfredsstiller de krav som er angitt i loven. Det må nok likevel opereres med en generell rolleforventning til sertifikatmottakeren om at denne opptrer forsvarlig i forbindelse med bruk av sertifikatet, bl.a. ved å kontrollere sertifikatets status når det benyttes i transaksjoner som har et skadepotensial.

Hvis man skulle komme til at det offentlige vil utstede en eID som ikke er utstedt som et kvalifisert sertifikat, kommer esignaturlovens bestemmelser ikke til anvendelse. Sertifikatmottakeren kan da ikke bygge på esignaturlovens bestemmelser, men sertifikatmottaker må på annet grunnlag vise at han eller hun har hatt en berettiget forventning om at opplysningene i sertifikatet var korrekte. I tillegg må sertifikatmottaker ha lidt et tap på grunn av en feil i sertifikatet som skyldes at utsteder har handlet uaktsomt. Dersom sertifikatet er utstedt i henhold

til en policy som tilsvarer kravene til kvalifiserte sertifikater, og sertifikatmottaker er klar over dette, vil en berettiget forventning til sertifikatet kunne følge av rolleforventningen til at det offentlige som utsteder av sertifikater opptrer i henhold til, og oppfyller, sin egen sertifikatpolicy. Kravene til forsvarlig opptreden til utsteder vil i disse tilfellene være de samme som for utstedere av kvalifiserte sertifikater.

Avgrensning av det mulige erstatningsansvaret

Det følger av esignaturloven § 22 at sertifikatutsteder kan avgrense sitt erstatningsansvar ved å angi begrensninger i sertifikatene med hensyn til bruksområde eller transaksjonsbeløp. Dette er ikke ansvarsbegrensninger i tradisjonell forstand, men utsteder blir etter loven fritatt for å erstatte tap som er knyttet til anvendelse utover de angitte avgrensningene. Det er viktig å merke seg at avgrensningene, i henhold til lovens ordlyd og uttalelser i forarbeidene, må fremgå av sertifikatet selv. Det er definert standardutvidelser for angivelse av beløpsbegrensninger, men når det gjelder avgrensning av bruksområde er det noe mer problematisk. Dersom man vil begrense bruken til å gjelde overfor offentlig myndighet kan det defineres en såkalt "privat utvidelse" for dette formålet. Hvis sertifikatet også skal benyttes for visse formål innen privat sektor vil imidlertid en slik "privat utvidelse" skape praktiske problemer fordi man risikerer at den ikke blir gjenkjent av de aktuelle sertifikatmottakere. Hvorvidt dette vil utgjøre en praktisk hindring for en slik ordning vil til en viss grad bero på hvordan man innretter valideringstjenesten og om private aktører også kan benytte denne.

En alternativ fremgangsmåte er å unnlate å gjøre statusinformasjon tilgjengelig for andre enn det offentlige selv, samtidig som det fremgår av sertifikatpolicy at sertifikatet bare kan benyttes i forbindelse med samhandling med offentlig sektor. Dette bør også fremgå av teksten i meldingsfeltet i sertifikatet. Selv om løsningen ikke fullt ut skulle tilfredsstille lovens krav, vil den likevel kunne ha betydning i de fleste praktiske tapssituasjoner.

For sertifikater som ikke er utstedt som kvalifiserte sertifikater kan anvendelsesbegrensningene håndteres i sertifikatutsteders policy[29]. For slike sertifikater vil sertifikatmottakerens forventninger til anvendeligheten av sertifikatet måtte knyttes til policyen eller en annen tilsvarende utstedererklæring, og sertifikatmottakers berettigede forventning kan ikke gå lenger enn det utstedererklæringen gir grunnlag for.

Ansvarsregulering kan også skje gjennom avtale, men med mindre det velges en helt lukket løsning kan man ikke basere seg på avtaler med brukerstedene alene. I forhold til de kvalifiserte sertifikatene er det dessuten en viss usikkerhet knyttet til lovens forholdsvis strenge krav til at avgrensninger skal fremgå av sertifikatet selv. Avgrensninger må også signaliseres på andre måter overfor brukere som er i posisjon til å utnytte sertifikatet uten avtale.

Det relevante tapet – hva som kan kreves dekket

Hvorvidt det potensielle erstatningsansvaret vil utgjøre et problem for en offentlig utstedt eID vil til en viss grad avhenge av hvilket tap det kan være aktuelt for sertifikatmottakeren å kreve dekket. Esignaturloven gir i utgangspunktet sertifikatmottaker grunnlag for å kreve dekket ethvert tap der det eksisterer en tilstrekklig nærhet i årsakssammenheng mellom utsteders uaktsomhet, den aktuelle feilen og tapet.

Utgangspunktet er at den tapslidende skal stilles som om den uaktsomme handling ikke hadde blitt begått. Hvis opplysningene i sertifikatet eller statustjenesten da ville vært korrekte, og

[29] En sertifikatpolicy er et dokument som beskriver formålet med, regler for bruk, samt utstedelses- og vedlikeholdsprosedyrer for sertifikater.

vedkommende i så fall ville ha unnlatt å gjennomføre transaksjonen, har han som utgangpunkt krav på å få dekket det tap han har pådratt seg ved å stole på sertifikatet, f.eks. til forberedelser til en avtale som det ikke ble noe av. Han har derimot ikke krav på å få dekket den forventede fortjeneste eller lignende på en kontrakt som ikke blir inngått som forventet. Begrunnelsen er at hvis feilen ikke var blitt begått, og opplysningene i sertifikatet hadde vært korrekte, ville han ikke forsøkt å gjennomføre transaksjonen i det hele tatt. Derfor kan han heller ikke ha gått glipp av noen fortjeneste. På den annen side, hvis det ukorrekte sertifikatet fører til at konfidensielle opplysninger blir utlevert til feil person, kan det tilknyttede økonomiske tapet kreves dekket. Hvor omfattende dette tapet kan bli vil avhenge av opplysningenes art. Dreier det seg f.eks. om forretningshemmeligheter av strategisk betydning, vil det økonomiske tapet typisk bli større enn hvis det dreier seg om personopplysninger (som potensielt utløser skade og ulemper av annen karakter).

12.5.6 Offentlig utsteder og e-signaturloven

Utgangspunktet er at offentlig forvaltning vil utstede eID som kvalifiserte sertifikater, nærmere bestemt Person Høyt i henhold til "Kravspesifikasjon for PKI i offentlig sektor".

Esignaturloven oppstiller en rekke krav overfor utstedere av kvalifiserte sertifikater og til innholdet av slike sertifikater. Dette notatet skal se nærmere på om disse kravene stiller seg annerledes dersom offentlig forvaltning er sertifikatutsteder.

Som generell betraktning kan man konkludere med at kravene i esignaturloven ikke oppstiller krav som er til særlig vanske for offentlig virksomhet som sertifikatutsteder. Det er imidlertid krav som man trenger å særlig ta hensyn til, disse er i hovedsak følgende (jf. vedlegg A for nærmere gjennomgang av esignaturlovens bestemmelser).

- Ved innsamling av opplysninger må sertifikatutsteder gi informasjon om hva opplysningene skal brukes til. Dessuten skal sertifikatutsteder bl.a. opplyse om ev. begrensninger i sertifikatet og eksisterende selvdeklarasjonsordninger. Dette vil kreve nærmere gjennomgang av søknadsprosedyrer mv. for å sikre at disse kravene etterleves.

- Esignaturloven med forskrift stiller som utgangspunkt krav om personlig fremmøte ved utstedelse av kvalifisert sertifikat. Et slikt krav er allerede i tråd med kravene som oppstilles ved utstedelse av pass. Dersom det derimot er aktuelt at eID'ene også skal oppfylle kravene for sertifikatklassen Person-Høyt etter "Kravspesifikasjon for PKI i offentlig sektor" vil det stilles krav om identifisering av søker etter krav som oppstilles i hvitvaskingsregelverket, og det må sikres at disse kravene etterleves.

- Den offentlige etat som skal være sertifikatutsteder vil omfattes både av Post- og teletilsynet og Datatilsynet sine tilsynsvirksomheter. Her gis det både mulighet til stedlig inspeksjon og adgang til å ilegge tvangsmulkt. Dessuten skal utstedere av kvalifiserte sertifikater og av sertifikater på nivå Person-Høyt, betale et årlig gebyr til Post- og teletilsynet. Disse forhold bør vurderes nærmere når plasseringen av ansvaret for den offentlige utstedelse av eID er avklart.

For utdypende gjennomgang av loven se vedlegg A.

12.6 Elektronisk ID utstedt i markedet

Dette kapitlet skal se på de organisatoriske og rettslige konsekvensene av å ha en elektronisk ID (eID) på det nasjonale ID-kortet utstedt av en privat sertifikatutsteder. Selv om det er mulig å legge til rette for at en slik ordning åpner for at flere private aktører parallelt og i konkurranse kan legge sine eID på det nasjonale ID-kortet, vil det ikke være aktuelt til enhver tid å tilby mer enn én tilbyders eID på det nasjonalt ID-kortet. Dette skal imidlertid ikke forveksles med at andre eID'er kan brukes overfor offentlige brukersteder.

Som allerede er blitt nevnt ovenfor tas det utgangspunkt i at eID skal oppfylle kravene for sertifikatklassen "Person-Høyt" i henhold til Kravspesifikasjonen for PKI i offentlig sektor. I dette kapitlet vil dette tas som utgangspunkt i forhold til rettslige krav mv, så fremt ikke annet eksplisitt angis.

12.6.1 Mulige modeller for organisering

Når det gjelder mulige modeller for organisering er utgangspunktet her identisk med det som omtales i kapittel 12.5. Vi skal her se nærmere på hvordan disse funksjonene og rollene skal/kan organiseres og hvordan forholdet mellom den private aktøren (sertifikatutstederen), på den ene siden, og det offentlige og andre private aktører, på den andre siden, vil være. I henhold til esignaturloven menes med en sertifikatutsteder "en fysisk eller juridisk person som utsteder sertifikater eller tilbyr andre tjenester relatert til elektronisk signatur", jf. esignaturloven § 3 nr. 10. I denne sammenheng benyttes imidlertid begrepet noe mer begrenset, slik at det dekker den som sertifikatet utpeker som utsteder (dvs. den som signerer og innestår for at innholdet i sertifikatet er riktig) og - ved utstedelse av kvalifiserte sertifikater – som derved er erstatningsansvarlig i henhold til bestemmelsene i esignaturloven § 22.

Organiseringen av sertifikattjenesten kan skje på mange forskjellige måter. I denne sammenheng vil hovedskillet gå mellom løsninger der utstedelsen av eID skjer som en integrert del av søknads-produksjons- og utleveringsprosessen for det fysiske nasjonale ID-kortet, og der dette skjer frakoblet fra disse prosessene. Det finnes også flere alternative mellomløsninger, men det blir for omfattende å drøfte alle disse alternativene i denne rapporten.

Det er viktig at den valgte løsningen gjøres så enkel og kostnadseffektiv som mulig for alle involverte parter. Ved å gjøre søknadsprosessen så enkel som mulig vil dette ha en positiv påvirkning på utbredelsen av eID og derved øke den forventede bruken av dem. Med slike krav er det mye som trekker i retning av at den "integrerte løsningen" er å foretrekke, jf. nedenfor. Det er også den løsningen som i hovedsak blir drøftet nedenfor, dog med noen sammenligninger med den "frakoblede modellen".

Vedrørende de mer generelle beskrivelsene av de forskjellige rollene og funksjonene som er nødvendige for å kunne tilby en sertifikattjeneste vises det til fig. 1 i kapittel 12.5.1. Organiseringen av sertifikattjenesten blir noe forskjellig ved en privat sertifikatutsteder og også fokus på hvilke roller/tjenester som særlig må ivaretas for det offentlige. Nedenfor presenteres to skjematiske figurer over organiseringen der ID-kortet settes i sentrum, henholdsvis den ***"integrerte løsningen"*** og den ***"frakoblede løsningen"***. [30]

[30] I figurene brukes to forskjellige farger; rød – som viser at det vil være en annen part som er ansvarlig for denne rollen/funksjonen når sertifikatutsteder er en privat aktør; gul – viser at det ikke er noen endring.

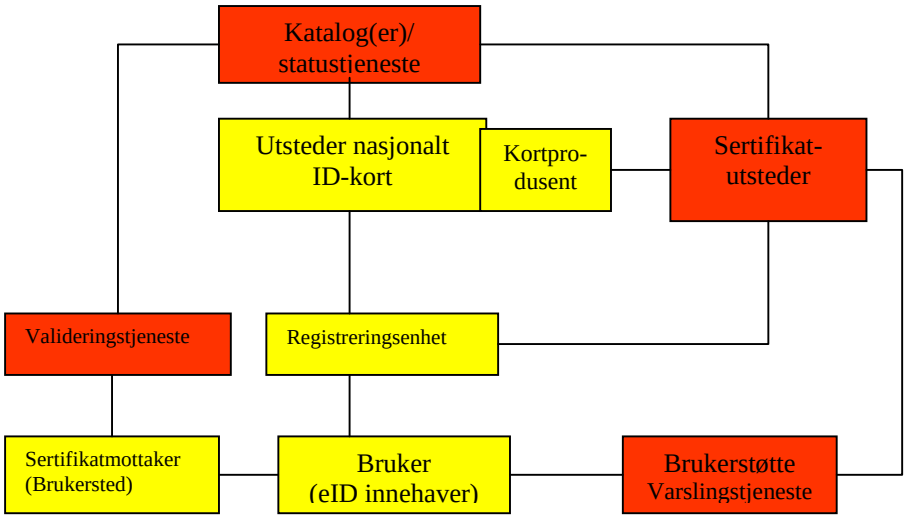


Fig. 2 Integrert løsning

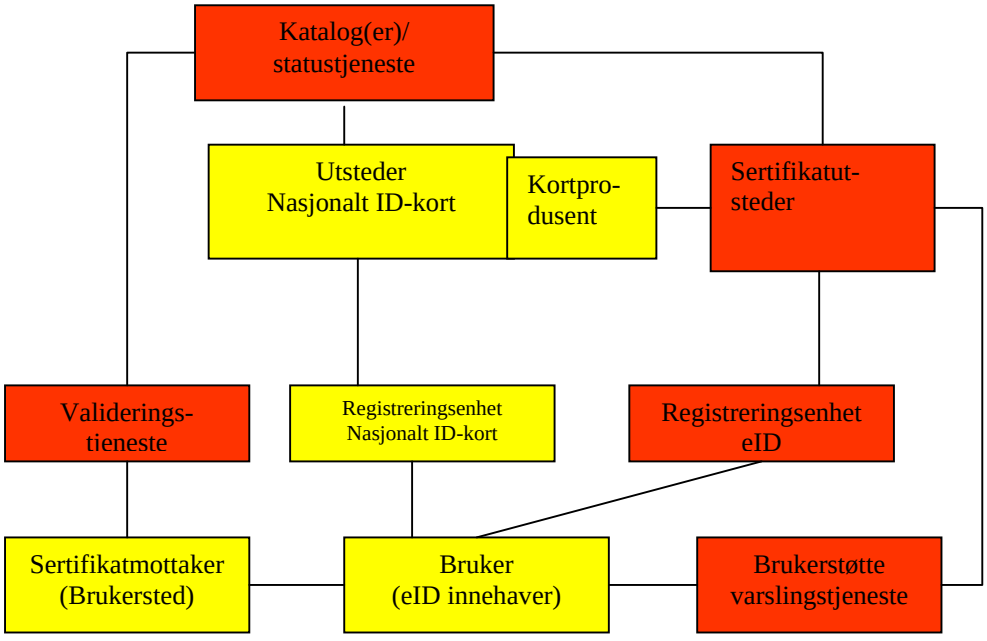


Fig 3. Frakoblet løsning.

Sertifikatutsteder – Sertifikatutsteder vil være en privat aktør, ev. som allerede tilbyr sertifikattjenester i markedet, selv om det ikke er en forutsetning. Uansett må sertifikatutsteder være registrert som utsteder av kvalifisert sertifikat etter esignaturloven og ha sendt inn melding om selvdeklarasjon i henhold til kravene for sertifikatklassen "Person-Høyt" før utstedelse kan skje. Sannsynligvis vil dette være prekvalifiseringskrav for de som skal gi inn tilbud ved den offentlige anskaffelsen av sertifikattjenesten. Det er sertifikatutstederen som har det overordnede

ansvaret for sertifikattjenesten. Flere av de praktiske funksjonene som skal utføres innenfor rammen av sertifikattjenesten vil imidlertid settes ut til andre, herunder under gitte forhold også til politiet som registreringsenhet (se nedenfor). Selv ved en slik delegering av oppgaver og funksjoner, vil sertifikatutsteder ha det primære ansvaret for sertifikattjenesten, inklusive erstatningsansvaret.

Det er i utgangspunktet ikke noe hinder for at sertifikatutstederen er en utenlandsk aktør etablert i en annen stat innenfor EØS. Direktivet om elektroniske signaturer legger opp til at kvalifiserte sertifikater utstedt av utenlandske aktører skal aksepteres på lik linje med kvalifiserte sertifikater utstedt av nasjonale aktører. Det betyr at den utenlandske tilbyderen av kvalifiserte sertifikater ikke nødvendigvis må registrere seg for Post- og teletilsynet som utsteder av kvalifiserte sertifikater, men kan være registrert som dette i en annen EØS-stat. Dog må sertifikatutsteder ha foretatt en selvdeklarasjon i henhold til kravene for sertifikatklassen "Person-Høyt" etter Kravspesifikasjonen for PKI i offentlig sektor.

Registreringsenhet – Ved den integrerte løsningen vil det for alle praktiske formål være hensiktsmessig at registreringsenheten er den samme enheten som den som tar imot nødvendige opplysninger for utstedelsen av det nasjonale ID-kortet, f.eks. politiet. Politiet vil da, basert på en avtale med sertifikatutstederen, på vegne av sertifikatutstederen innhente nødvendige opplysninger for utstedelse av eID.

I henhold til kravene for sertifikatklassen Person-Høyt (som er basert på et kvalifisert sertifikat) stilles det krav om personlig oppmøte ved utstedelsen, jf. forskrift til utstedere av kvalifiserte sertifikater § 7. Dette kravet kan imidlertid fravikes dersom det allerede eksisterer et etablert forhold mellom utsteder og innehaver som er basert på et personlig fremmøte. Dette unntaket vil være mest aktuelt ved nyutstedelse av eID. Det vil derfor være hensiktsmessig å ha etablert en ordning for hvordan dette skal skje, da dette ikke nødvendigvis vil trenge en involvering av registreringsenheten men kan skje direkte mellom sertifikatutsteder og innehaveren av eID. Dessuten stiller Kravspesifikasjonen for PKI i offentlig sektor for sertifikatklassen Person-Høyt detaljerte krav om hvilke dokumenter som skal legges frem ved identifiseringen av søker. For ikke unødvendig å begrense utbredelsen av eID, vil det være hensiktsmessig at innhenting av nødvendige opplysninger og kontroll av identifikasjonsdokumenter til utstedelse av henholdsvis det nasjonale ID-kortet og eID skjer samtidig og helst av samme aktør.

Personlig fremmøte må ikke nødvendigvis skje i forbindelse med innleveringen av søknaden, men kan skje på et senere tidspunkt. Det betyr at dette kravet ikke vil være til hinder for at oppstart for søknad av nasjonalt ID-kort skjer over nett, og at identifisering av søker ved personlig oppmøte (for identifisering og undertegning) skjer på et senere tidspunkt.

I tilknytning til det personlige fremmøtet, der også nødvendig identitetskontroll gjennomføres, vil det være hensiktsmessig at nødvendig PIN-kode for aktivering/deaktivering av eID utleveres.

Dersom man ønsker å velge en "frakoblet løsning" kan oppgaven som registreringsenhet settes ut til tilnærmet hvem som helst, forutsatt at den ivaretar de ovennevnte kravene om personlig fremmøte, dokumentasjonskontroll mv. For at det skal bli en utbredelse av eID vil det imidlertid være behov for at disse registreringsenhetene er spredt rundt i hele landet, slik at det ikke blir for langt for søker å reise for det første personlige oppmøtet.

Kortprodusent – Det fysiske kortet (det nasjonale ID-kortet) med kontaktchip for lagring av eID vil bli produsert av en privat aktør som velges etter offentlig anbudskonkurranse. Generering

av nøklene for autentisering, signering og kryptering som skal legges i chipen vil også være kortprodusents ansvar.

Sertifikatprodusent – Sertifikatutstederen kan selv være sertifikatprodusent, men kan også sette den oppgaven ut til en annen part. Det avgjørende er at de regulatoriske kravene i henhold til bl.a. esignaturloven og Kravspesifikasjonen for PKI i offentlig sektor oppfylles.

Det er helt avgjørende å sikre at riktig eID legges på rett kort, slik at man unngår en situasjon der den fysiske informasjonen i kortet og informasjonen i eID ikke er i samsvar med hverandre, enten at de viser til to helt forskjellige personer (forveksling) eller at informasjonen er uriktig. Det er sannsynligvis enklest å unngå forveksling eller uriktig informasjon dersom nedlasting av sertifikatet skjer i nær tilknytning til produksjonen av det fysiske kortet. En slik løsning vil kreve et samvirke mellom kortprodusent og sertifikatprodusent. Et mulig alternativ er at mottakeren selv laster ned sertifikatet. Dette kan da skje ved at innehaveren etter mottak av kortet bruker den PIN-koden som vedkommende mottok ved innleveringen av søknaden til å koble sertifikatet sammen med nøklene på kortet og laste det ned på chipen i kortet. Det er imidlertid neppe et gangbart alternativ, bl.a. tatt i betraktning at denne typen av operasjoner krever en relativt høy teknisk innsikt og kan også føre til en dårligere sikkerhet. Dessuten vil det sannsynligvis kreve et omfattende og kostnadskrevende brukerstøtteapparat.

Katalog-/statustjeneste – Statustjeneste - Valideringstjeneste – Vedrørende disse tjenestenes oppgaver mv. vises det til kapittel 12.5.2. Det er viktig at alle offentlige etater som ønsker å ta i bruk denne eID får tilgang til disse tjenestene.

Dette er tjenester som sertifikatutsteder selv kan utføre eller sette ut til annen. Hvilket alternativ som velges vil antakelig spille mindre rolle i forhold til den rettslige reguleringen eller nødvendige avtaler mellom sertifikatutsteder og det offentlige. Derimot kan dette påvirke forholdet mellom brukerstedene, innehaveren av eID og den som tilbyr disse tjenestene, på vegne av sertifikatutstederen.

Uansett er det viktig at disse tjenestene tilbys i henhold til klare retningslinjer fra det offentlige, herunder bl.a. krav om sikkerhet og tilgjengelighet. Det er helt avgjørende at disse tjenestene er kontinuerlig tilgjenglige.

I kapittel 12.5.4 anbefales det at forholdet mellom registeret for nasjonale ID-kort og registeret for eID koordineres, bl.a. med begrunnelsen at dersom et nasjonalt ID-kort sperres etter å ha blitt meldt tapt eller stjålet, vil det normalt være behov for at eID også trekkes tilbake. På bakgrunn av dette pekes det på at det vil være behov for at registeret over nasjonale ID-kort inneholder opplysninger om serienummer til de sertifikatene som til enhver tid er lagret på kortet. Ved en slik løsning må den private sertifikatutstederen (ved regulering eller i avtale) pålegges å gi oppdaterte opplysninger kontinuerlig til det offentlige, som eier av registeret over nasjonale ID-kort, om hvilke sertifikater som er lagret på kortet. Dessuten må det offentlige videreformidle informasjon til sertifikatutstederen om at et nasjonalt ID-kort er blitt sperret, slik at sertifikatutstederen har anledning å trekke tilbake aktuelle eID. Tatt i betraktning at det i dette kapitelet er to forskjellige parter som har ansvar for de to registrene, og at tilbaketrekking av eID er sertifikatutstederens ansvar, kan koblingen mellom de to registrene løses på en alternativ måte. Alternativet vil være at sertifikatutstederen av kortutstederen mottar en katalog over de nasjonale ID-kortene, sannsynligvis begrenset til ID-kortnummer og fødselsnummer. Til dette registeret kan sertifikatutsteder selv koble de til enhver tid gyldige sertifikatene som er knyttet til det nasjonale ID-kortet. Dersom et nasjonalt ID-kort trekkes tilbake skal det offentlige umiddelbart gi opplysning om dette til sertifikatutsteder. Dette vil skje ved at det sendes en melding til

sertifikatutstederen om at et nasjonalt ID-kort med følgende kortnummer er blitt sperret. Sertifikatutsteder vil da selv ha ansvar for å finne ut hvilke sertifikater som er lagret på det aktuelle kortet og vurdere hvorvidt de skal trekkes tilbake eller ikke. På denne måten vil ansvarsforholdet hva gjelder tilbaketrekkingen av eID i sin helhet plasseres hos sertifikatutstederen. Med denne alternative løsningen vil det heller ikke være behov for at det offentlige har et eget oppdatert register over gyldige eID lagret på de nasjonale ID-kortene.

Det er imidlertid fortsatt ikke behov for noen direkte kobling mellom registrene motsatt vei, da det ikke er naturlig å trekke tilbake det nasjonale ID-kortet på grunn av at en eID på kortet er blitt trukket tilbake.

12.6.2 Åpen eller lukket status- og katalogtjeneste – tilgang til statusopplysninger om sertifikatet og tilleggsopplysninger om eID-innehaveren

I hvilken grad private aktører/brukersteder skal kunne benytte eID på det nasjonale ID-kortet i samhandling seg imellom, kan i og for seg reguleres i lov/forskrift eller i avtale mellom det offentlige og den private sertifikatutstederen. For å åpne for gjenbruk av eID i det private markedet vil det kreves av de private brukerstedene å få tilgang til statustjenesten og ev. også tilleggstjenester fra katalogtjenesten. I den situasjonen der det offentlige er sertifikatutsteder vil det offentlige kunne styre hvem som skal få denne tilgangen, og også bestemme prisen for disse tjenestene. Det er imidlertid ikke usannsynlig at det offentlige ønsker å ha denne styringsretten selv i situasjonen der eID utstedes av en privat aktør. En slik kontroll- og styringsrett for det offentlige må da nærmere reguleres i avtalen mellom det offentlige og sertifikatutstederen.

Derimot kan det være aktuelt å begrense sertifikatutstederens adgang til å tilby samme eID i andre sammenhenger, dvs. at det bør være slik at den eID som lastes ned på det nasjonale ID-kortet er dedikert til bruk på det nasjonale ID-kortet. Dette må da settes som en forutsetning allerede ved den offentlige anskaffelsen.

12.6.3 Regulering av forholdet rollene imellom

Det vil, på lik linje med offentlig utstedt eID, være sertifikatutstederen som har den sentrale rollen i forhold til sertifikattjenesten. Til å begynne med vil det være denne som har ansvar for at sertifikatene oppfyller kravene for sertifikatklassen Person-Høyt. Det betyr også at det vil være utstederen som må registrere seg som utsteder av kvalifiserte sertifikater ved Post- og teletilsynet (hvis det ikke dreier seg om en utenlandsk sertifikatutsteder, jf. ovenfor), og som må sende inn en selvdeklarasjon om at kravene for Person-Høyt etterleves.

Dersom man velger det alternativet at utstedelsen skal skje som en integrert del av utstedelsen av det nasjonal ID-kortet, kan f.eks. politiet operere som registreringsenhet på vegne av den private sertifikatutstederen. Dette vil kreve at det etableres et avtaleforhold mellom sertifikatutstederen og politiet (Politidirektoratet). Denne avtalen må bl.a. innholde krav om at politiet gjennomfører identifiseringen av søker i henhold til de kravene som oppstilles for sertifikatklassen "Person-Høyt", og ev. tilleggskrav som sertifikatutstederen mener er nødvendige. Disse ev. tilleggskravene må klarlegges i tilknytning til selve utvelgelsen av en privat sertifikatutsteder, slik at det offentlige allerede på det stadiet er klar over hvilke krav som vil stilles overfor politiet som den private aktørens registreringsenhet.

Videre vil det være hensiktsmessig at registreringsenheten utleverer den PIN-koden som søker skal bruke for å aktivere/deaktivere eID. Det vil da være viktig at alle involverte parter har klare

rutiner mv. for å sikre at utlevert PIN-kode kobles til riktig eID. Dette vil særlig være et forhold mellom sertifikatutsteder, registreringsenheten, sertifikatprodusent og kortutsteder/-produsent.

Ifølge esignaturloven § 15 skal sertifikatutsteder før avtale inngås informere søker av eID om vilkårene og begrensningene for bruken av sertifikatet, gi opplysninger om gjeldende godkjenningsordninger mv. samt om prosedyre for klage og avgjørelse av tvister. Det vil således være et behov for at utsteder og søker/innehaver av eID inngår en avtale. Dette kan ivaretas av registreringsenheten (f.eks. politiet) på vegne av sertifikatutstederen. Dersom utstedelsen av eID skal være frakoblet utstedelsen av det nasjonale ID-kortet, vil avtaleinngåelse mv. håndteres når søknad om eID ved personlig oppmøte skjer hos registreringsenheten. Uansett om man velger den integrerte eller den frakoblede løsningen, bør avtalen være tilgjengelig på nett slik at søker i forkant har anledning å gjøre seg kjent med avtalens innhold.

Ved å være registreringsenhet vil politiet være databehandler og derved omfattes av bestemmelsene i personopplysningsloven. Dette forhold, der politiet er databehandler for sertifikatutstederen (som behandlingsansvarlig) må også nærmere reguleres i avtalen mellom partene.

I en integrert løsning vil det være behov for å klargjøre hvilke oppgaver som tilligger henholdsvis kort- og sertifikatprodusent. Utgangspunktet vil være at kortprodusenten produserer selve kortet, med en kontaktchip som inneholder nøklene for autentisering, signering og kryptering. Sertifikatprodusenten vil ha i oppgave å sikre koblingen mellom nøklene og sertifikatet, og laste ned sertifikatet på chipen. Hvordan dette skal skje mv. må være klart allerede før anskaffelsen av disse tjenestene og dette forholdet må nærmere reguleres i en avtale mellom partene. Det må bl.a. sikres samsvar mellom disse to aktørenes løsninger, slik at sertifikatutsteder bl.a. kan laste ned sertifikatet på chipen. Utgangspunktet må være at det stilles krav om bruk av gjeldende standarder på området i så stor grad som mulig.

Forholdet mellom sertifikatutsteder og andre private aktører, til hvilke sertifikatutstederen setter ut funksjoner/roller innenfor rammen av sertifikattjenesten, vil i utgangspunktet reguleres i egne avtaler. Valideringstjenesten, uansett om den settes ut eller håndteres av sertifikatutstederen selv, vil måtte ha et avklart forhold til brukerstedene og/eller med en sikkerhetsportal. Det vil sannsynligvis håndteres i avtaleform, og ikke i noen større grad ved regulering.

12.6.4 Sertifikatutsteders erstatningsansvar for feil i sertifikatene og statustjenesten mv.

I kapittel 12.5.5 drøftes sertifikatutsteders erstatningsansvar, inklusive adgang til å begrense ansvaret. Presentasjonen av gjeldende rett på området gjelder uansett om sertifikatutsteder er en offentlig eller en privat aktør. Det vises derfor her til dette kapitlet. I utgangspunktet er det sertifikatutstederen som er ansvarlig for ev. feil i sertifikattjenesten. I henhold til esignaturloven § 10 annet ledd skal sertifikatutstederen ha tilstrekkelige økonomiske ressurser til å kunne drive virksomheten i henhold til kravene i loven, herunder også kunne dekke ev. erstatningskrav. Her, som i alle andre sammenhenger, vil være viktig at dette kravet etterleves. Post- og teletilsynet fører tilsyn med at dette kravet er ivaretatt.

Ansvarsforholdet mellom den private sertifikatutstederen og det offentlige
Som allerede nevnt vil det offentlige (f.eks. politiet) – dersom man velger den integrerte løsningen - være registreringsenhet på vegne av den private sertifikatutstederen. Som også er blitt uttalt er det sertifikatutstederen som er ansvarlig overfor de som har hatt tillit til eID dersom det er noen feil med sertifikatet, jf. esignaturloven § 22. Dette gjelder selv om feilen er begrunnet i en feil foretatt av registreringsenheten. Det er imidlertid ikke uvanlig at sertifikatutsteder i slike situasjoner har sikret seg en regressrett, slik at ev. erstatning som er blitt utbetalt på grunn av feil foretatt av registreringsenheten til syvende og sist betales av registreringsenheten. Det er ikke noen grunn til å tro at sertifikatutsteder i en integrert løsning ikke vil kreve en bestemmelse om regressrett overfor det offentlige (politiet) dersom denne måtte utbetale erstatning pga. en feil foretatt av politiet som registreringsenhet.

12.7 Standarder som kan være relevante for eID

For å oppnå størst mulig grad av interoperabilitet og harmonisering av eksisterende og kommende løsninger for elektronisk ID, vil det være viktig så langt som mulig å følge relevante internasjonale og nasjonale standarder på området når det gjelder valg av løsning for eID på det nasjonale ID-kortet.

Det eksisterer en rekke nasjonale og internasjonale standarder og anbefalinger som vil være relevante for eID på nasjonalt ID-kort.

Dersom eID baseres på sertifikatklasse "Person Høyt" slik det er definert i Kravspesifikasjonen for PKI i offentlig sektor, legger dette visse føringer for hvilke tekniske standarder og anbefalinger som vil være relevante. Kravspesifikasjonen fremsetter selv en rekke krav til eID, og den viser også til flere relevante internasjonale og nasjonale standarder.

Nasjonalt vil leveransene fra SEID[31]-prosjektet være relevante:

- Leveranse 1: "Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater"
- Leveranse 2: "Grensesnitt for tilgang til Oppslagstjenester"
- Leveranse 3: "SEID-SDO – format for langtidslagring av elektroniske signaturer"

Internasjonalt vil flere standarder fra både IETF, ETSI og CEN være relevante for eID og utstedere av disse. Blant de mest aktuelle er:

- ETSI TS 101 456 - Policy requirements for certification authorities issuing qualified certificates
- ETSI TS 101 862 – Qualified Certificate Profile
- RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- RFC 3739 - Internet X.509 Public Key Infrastructure Qualified Certificates Profile

En *kvalifisert* elektronisk signatur er basert på et kvalifisert sertifikat og fremstilt av et godkjent, sikkert signaturfremstillingssystem (SSCD). Når det gjelder sikre signaturfremstillingssystemer har EU kommisjonen publisert CEN-standarden CWA 14169 som den standarden som oppfyller krav i Direktivets vedlegg III (med krav til et sikkert signaturfremstillingssystem).

[31] SEID står for Samarbeid om EID og elektronisk signatur, et prosjekt mellom ledende markedsaktører for eID, som produserte et sett med nasjonale standarder på området.

Det pågår også arbeid i CEN for etablering av et "European Citizen Card" (ECC). Dette arbeidet vil også ligge til grunn for det arbeid som EU Kommisjonen gjør innenfor dette området, jf. i2010, med bl.a. det målet at man skal få på plass en paneuropeisk elektronisk ID innenfor EU/EØS innen 2010. Standardene CEN arbeider med i denne forbindelse vil bl.a. oppstille krav til format på det fysiske kortet og hvem som skal være ansvarlig utsteder av et slikt kort. Det vil derimot ikke spesifiseres krav i forhold til utstedelse av eID-en som skal legges på ECC. Dette betyr således at det ikke fra dette arbeidet legges særlige føringer når det gjelder eID på det nasjonale ID-kortet. ECC vil ikke være et reisedokument i sin egentlige betydning, men vil kunne brukes ved grensepasseringen innenfor EU/EØS. I tillegg må derfor ECC kunne leses av samme ePassleser som finnes ved grenseoverganger. Dette vil bl.a. påvirke datastrukturen i ECC og det vil utarbeides en spesiell profil for "ECC Travel Document" som skal være i samsvar med ICAO standarden. Noen EU-stater har også fremmet et ønske om at utseendet på ECC (layouten) er identisk med kravene etter ICAO. Dette vil blir fulgt opp kommende revisjoner av CENs dokumenter.

ICAO standarden gjelder ikke eID og vil heller ikke gi føringer på utstedelse av eID.

12.8 Drøfting og anbefalinger

I dette kapitlet foretar vi en nærmere drøfting av fordeler og ulemper ved at eID på nasjonalt ID-kort utstedes av hhv. offentlig forvaltning og en privat aktør (sertifikatutsteder som opererer i markedet). Vurdering av konkurransemessige forhold inngår i drøftingen, som avsluttes med en konklusjon og en anbefaling.

Fordeler ved at eID utstedes av offentlig forvaltning

Ordningen med en offentlig utstedt eID har flere formål. For det første skal en offentlig utstedt eID gi det offentlige bedre styring og kontroll med utbredelsen av eID, gjennom å bidra til utbredelsen av eID slik at det er tilgjengelig som et identifikasjonsmiddel for brukere av forvaltningens tjenester, og derved kan bidra til å utvide bruken av elektroniske tjenester fra forvaltningen, som krever høyt sikkerhetsnivå. For det andre skal en offentlig utstedt eID gi det offentlige større grad av kontroll over sikkerheten i, og tilliten til, løsningen enn det som oppnås gjennom privat utstedelse og selvdeklareringsordningen. For det tredje kan en offentlig utstedt eID gi forvaltningen bedre kontroll med prisingen og kostnadene ved bruk av eID.

Fordelene kan ellers oppsummeres som følger:

- Utstedelsesprosedyrer for fysiske ID-kort og for eID kan samordnes på en bedre måte, ved at verdikjeden for offentlig utstedelse vil være under kun én aktørs kontroll.
- "Retten" til kort og eID vil tilhøre offentlig forvaltning. Dersom det vil være aktuelt å trekke tilbake det fysiske kortet, vil det være enklere dersom også eID "eies" av det offentlige slik at en tilbaketrekking ikke vil påvirke et privatrettslig forhold mellom innehaver og en privat sertifikatutsteder.
- Risiko for at eID ikke gjelder samme person som angitt person i det fysiske kortet vil være sterkt begrenset gjennom større sannsynlighet for at informasjonen i eID og fysisk ID-kort er identiske.
- Det vil være avklart hvem som er ansvarlig for ev. feil, om de oppsto i det fysiske ID-kortet eller i eID.
- En offentlig utsteder vil bestå, selv om den/de tekniske underleverandører kan skiftes ut. Det vil derfor ikke være nødvendig med en ny offentlig anskaffelse av sertifikatutsteder hver gang en avtale basert på kjøp av private tjenester vil måtte fornyes. På denne måten unngår man organisatoriske, økonomiske og juridiske problemer.

- Fra et sikkerhetssynspunkt er det mye som kan tale for at det er en fordel at eID-ene som skal legges på det nasjonale ID-kortet utstedes av et offentlig organ. Brukerens opplevelse av tillit til kortet kan svekkes av en sammenblanding mellom offentlige og private interesser på samme kort. Det er viktig at innholdet/informasjonen på kortet og i eID er identiske, og det vil sannsynligvis være enklere å ivareta dersom det offentlige både kontrollerer informasjonen i kortregisteret og informasjonen i sertifikatkatalogen.

Ulemper ved at eID utstedes av offentlig forvaltning

Det har tatt lang tid for markedsaktørene å komme i gang med å utstede eID'er basert på PKI. Flere utstedere, herunder banker, har registrert seg som utstedere av kvalifiserte sertifikater først nylig. En grunn til dette er sannsynligvis de signaler som offentlig forvaltning har sendt om at man vil kreve kvalifiserte sertifikater, herunder sertifikatklassen Person-Høyt, for noen typer tjenester. Dersom man nå vil etablere en offentlig utstedt eID på dette nivået, er det ikke umulig at det vil få negative konsekvenser for de private sertifikatutstedernes utbredelsesstrategier. Markedet for eID domineres i dag av få aktører (jf. kap. 4). Markedet er i startfasen og ble i Konkurransetilsynets vedtak V2005-10 avgrenset til å være nasjonalt, men forventes å bli internasjonalt i fremtiden. Det er et marked der det er store fordeler knyttet til å være først ute, og det er antakelig begrenset hvor mange eID-løsninger det vil være kommersielt interessant (og samfunnsøkonomisk lønnsomt) å ha i markedet. Med en slik markedsstruktur kan en offentlig aktør utgjøre et nyttig korrektiv til et konsentrert kommersielt marked. Samtidig kan det oppstå problem med statsstøtte dersom offentlig eID tillates brukt mot private brukersteder. Den offentlige e-utstederen vil da bli en aktør på linje med andre tilbydere av eID, og spørsmål om statsstøtte reises. En vil også kunne få en situasjon der den offentlige eID presser ut andre aktører i markedet, som ikke kan tilby sine tjenester gratis. I så måte vil ordningen innebære en statlig monopolisering av tjenesten.

Dersom den offentlige eID-løsningen også skal kunne brukes av kommersielle brukersteder vil staten måtte inngå avtale med brukerstedene på linje med kommersielle aktører. Her gjelder det såkalte "markedsinvestorprinsippet": statens engasjement innebærer offentlig støtte dersom den skjer på betingelser som ikke ville vært akseptable for en privat investor som opererer under normale markedsøkonomiske forhold (f.eks. hvis staten driver med underskudd). Mao: dersom det gis gunstigere økonomiske vilkår enn en privat investor ville gjort, utgjør differensen offentlig støtte.

Fordeler ved at eID utstedes av en privat markedsaktør

- Det eksisterer allerede flere markedsaktører som utsteder eID. Sannsynligvis eksisterer det allerede i dag utstedere av en sertifikatklasse på et nivå som er tilstrekkelig sikkert, jf. Person-Høyt i Kravspesifikasjon for PKI i offentlig sektor. Ved å benytte seg av et eksisterende tilbud i markedet, vil man i offentlig sektor ikke behøve å etablere noe nytt og derved heller ikke skape negativ påvirkning på dette markedet, ved at inntekstpotensial for private aktører reduseres.

Ulemper ved at eID utstedes av en privat markedsaktør

- Dette alternativ vil kreve utlysning av en offentlig konkurranse med påfølgende anskaffelse. Det blir da vanskelig å gjennomføre en parallell anskaffelse av selve kortet til formålet, da dette trolig kan gjøres først når utstederspørsmålet er avklart, for å sikre at kortprodusenten og eID-utstederen samspiller på en hensiktsmessig måte.
- En valgt markedsaktør kan fort komme i en monopolstilling i markedet.

- En avtale med én sertifikatutsteder etter en offentlig anskaffelse vil måtte fornyes, og det kan føre til at det blir en ny utsteder. Dette kan i sin tur føre til store organisatoriske, økonomiske og juridiske problemer. (Eks. vil eID utstedt av den "gamle" utstederen måtte fornyes gjennom "resertifisering" av den hos den nye utstederen, med de ulemper for brukeren som slik prosedyre kan medføre).
- En privat sertifikatutsteder kan gå konkurs. Dette kan føre til problemer med bruk av eID som denne har utstedt. Bl.a. vil trolig alle brukere av kort med eID utstedt av denne tilbyderen måtte møte opp personlig på nytt for å etablere tilstrekkelig sikkerhet for at rett eID havner på riktig kort.
- Det vil være nødvendig å ha en avtale om ansvarsfordeling mellom offentlig forvaltning og den private sertifikatutstederen som detaljregulerer en rekke forhold (jf. kap. 12.6.3 og 12.5.4)
- Det vil være behov for større koordinering mellom utstedelsen av det fysiske ID-kortet og eID, når det er to forskjellige ansvarlige utstedere.

Tatt i betraktning at det offentlige uansett vil kunne gjøres ansvarlig – direkte dersom det offentlige er sertifikatutsteder eller indirekte ved regress fra en privat markedsaktør - er det mye som taler for at det vil være mest hensiktsmessig å la det offentlige være sertifikatutsteder, slik at all kontroll ligger hos det offentlige. Videre er målene om sikkerhet og pålitelighet, samt mer styrt utbredelse av eID til bruk i offentlige tjenester, enklest å oppnå ved offentlig utstedelse av eID. Etablering av en offentlig utsteder av eID, gitt at den gjennomføres på en hensiktsmessig måte, kan også danne et nødvendig korrektiv til et umodent marked, og derved bidra til dets videre utvikling.

Det kan på sikt være hensiktsmessig å tillate bruk av offentlig utstedt eID i utvalgte private tjenester. For å unngå problemet med statsstøtte (jf. ovenfor) kan følgende løsninger vurderes:

a. De kommersielle aktørene lever av å ta betalt pr. identifikasjon. Dersom den offentlige eID'en er gratis i bruk vil dette utgjøre en konkurransefordel for den statlige tilbyderen. Det vil også være en fare for at den offentlige eID'ene vil fortrenge de private aktørene fra markedet og i realiteten monopolisere produktet. Den eneste løsningen da vil være å lovfeste et statlig monopol på eID. En slik løsning vil av flere grunner være lite ønskelig.

b. Dersom den statlige tilbyderen krever gebyr på offentlig ID – enten det er fast årlig eller transaksjonsbasert, vil dette ikke innebære statsstøtte dersom markedsinvestorprinsippet overholdes. Kravet er at virksomheten priser sine produkter slik at inntektene dekker kostnadene og gir en normal avkastning. Det avgjørende er altså ikke på hvilken måte produktene prises (fast pris eller transaksjonsavgift).

Vi viser til vurderinger i kap. 13 når det gjelder prissetningsstrategier for nasjonalt ID-kort. Det vil måtte foretas en avveining mellom kostnaden for brukeren og incentiver denne vil ha for å skaffe seg et nasjonalt ID-kort. Gis kortet gratis på kjøpet til de som vil fornye pass, bør det likevel kreves en avgift for selve eID, dersom kortet skal kunne benyttes til mer enn offentlige tjenester.

Konklusjon:

- Det etableres en offentlig ordning for utstedelse av eID til nasjonalt ID-kort, med Justisdepartementet som ansvarlig utsteder.
- Nødvendig utstederfunksjon (CA) etableres etter en konkurranse i markedet og påfølgende kontrakt med en utvalgt tjenesteleverandør.

- Politietaten fungerer som registreringstjeneste for eID, samtidig som de fungerer som utsteder av pass og nasjonalt ID-kort.
- Bruk av eID skal være frivillig og brukeren skal gis valget om vedkommende vil ha aktiv eID på kortet sitt.
- Det utstedes to sett med nøkler til kortet – ett for signering, som vil kunne aktiveres for personer f.o.m. 18 år, og ett for autentisering og kryptering, som vil kunne aktiveres for personer f.o.m. 13 år.
- eID skal først og fremst benyttes til adgang til elektroniske offentlige tjenester, men det vil også kunne benyttes mot private tjenester.
- Bruken av eID mot offentlige tjenester skal være kostnadsfritt for brukeren, mens bruk mot private tjenester kan pådra brukeren kostnader.
- Det skal utarbeides retningslinjer for bruk av nasjonalt ID-kort med eID mot ulike nettjenester, med vekt på ivaretakelse av personvern og behovet for anonymitet der det er relevant.
- På sikt kan utstedelse av eID til andre bærere, og gjennom annet distribusjonsapparat enn politiets, vurderes. Et nærliggende alternativ er NAV-etaten og deres helsetrygdkort. En mulig samordning av nasjonalt ID-kort og NAV-etatens helsetrygdkort, etter mønster fra Finland, kan også vurderes på sikt.

13 PRISFASTSETTELSE

13.1 Generelt

Det legges til grunn at ordningen med nasjonalt ID-kort er frivillig. Kombinasjonen funksjonalitet og pris antas derfor å ha stor innflytelse på hvor mange av de som har pass som vil anskaffe seg et nasjonalt ID-kort. Det er for øvrig også grunn til å merke seg at det er mange norske borgere som ikke har pass, og at det til enhver tid er et stort antall utlendinger som er bosatt i Norge som vil kunne ha interesse av et nasjonalt ID-kort med ny funksjonalitet.

En innføring av et nasjonalt ID-kort med ny funksjonalitet ved eventuell innføring av eID/elektronisk signatur, antas å kunne gi en ikke ubetydelig samfunnsøkonomisk gevinst i form av økt sikkerhet og effektivitet. I en slik situasjon kan det tenkes en prissetting under kostpris, som et viktig incitament med særlig positiv effekt på introduksjonen og utbredelsen av kortene med ny funksjonalitet.

13.2 Nærmere om retningslinjene for gebyr og avgiftsfinansiering

Finansdepartementet har ved rundskriv R-112 gitt retningslinjer for gebyr og avgiftsfinansiering av statlige myndighetshandlinger. Grunnvilkåret for å etablere en gebyrordning er at det offentlige utfører en klart definert myndighetshandling overfor betaleren, og at det ikke betales for noe annet eller mer.

Rundskriv R-112 vil i første rekke få betydning for en eventuell gebyrordning for nasjonalt ID-kort, da gebyret for et nasjonalt ID-kort oppad vil være begrenset til å kunne reflektere de faktiske kostnadene knyttet til produksjon og utstedelse av kortet. Retningslinjene gir ingen føringer for hvor lavt man kan sette gebyret.

Rundskrivet gir imidlertid også fremtidige føringer for fastsettelse av eksisterende gebyr, herunder passgebyret. I følge retningslinjene skal det arbeides for at også eksisterende gebyrer over tid skal reflektere de faktiske utgifter knyttet til tjenesten. Dette gir klare føringer for at dagens passgebyr på NOK 990,- for voksenpass etter hvert må reduseres til å reflektere de faktiske kostnader knyttet til passutstedelse og grensekontroll.

Ved å redusere passgebyret til å reflektere de faktiske utgifter knyttet til passutstedelse og grensekontroll, vil samtidig en rekke problemstillinger knyttet til prispress mellom passet og et nasjonalt ID-kort med EU/Schengen reisefunksjon unngås. Et nasjonalt ID-kort med EU/Schengen reisefunksjonalitet vil nemlig kunne erstatte passet som reisedokument i Schengen-området. ID-kortet vil dermed kunne dekke reisebehovet for de som f.eks. reiser på tradisjonelle sydenturer til forskjellige Schengen-stater. Med dagens passgebyr vil staten dermed risikere å tape avgifter fra passutstedelsen, ved at mange avstår fra å erverve eller fornye passet til fordel for et nasjonalt ID-kort. I Tyskland utgjør prisen for et EU/Schengen ID-kort ca en sjettedel av passgebyret. Bestillingsvolumet for nye dokumenter fordeler seg i dag i Tyskland med 2/3 for ID-kort og 1/3 for pass.

Det er mulig å unngå dette ved å sette gebyret for et nasjonalt ID-kort likt passgebyret. Denne løsningen vil imidlertid prise det nasjonale ID-kortet ut av markedet, samtidig som det vil være i strid med retningslinjene i rundskriv R-112.

13.3 Former for utstedelse

Velges det en løsning hvor utstedelsen av nasjonalt ID-kort knyttes opp til utstedelsen av pass, vil det redusere behovet for investeringer i infrastruktur og opplæring av personell samt gi god sikkerhet i forbindelse med produksjon og utstedelse. Dette vil innebære en positiv synergieffekt som vil komme forbrukerne til gode i form av lavere gebyr.

Forbrukeren vil først og fremst kunne dra nytte av en slik ordning ved å erverve det nasjonale ID-kortet samtidig som denne erverver eller fornyer passet. Årlig utstedes det omtrent en halv million nye pass. Kostnadene knyttet til å produsere et nasjonalt ID-kort i tillegg til passet vil være beskjedne, da kostnadene knyttet til biometrifangst, infrastruktur, personell m.v. i stor grad vil være dekket av passgebyret. Tilleggskostnaden knyttet til det nasjonale ID-kortet vil være tilnærmet lik trykkekostnaden for det konkrete kortet, med tillegg av kostnadene knyttet til eID og elektronisk signatur. Dette er funksjoner som ikke finnes i passet. Dette innebærer at forbrukeren ved passervervelse/fornyelse vil kunne erverve et nasjonalt ID-kort med en rekke funksjoner for et beskjedent tilleggsgebyr.

Erverv av nasjonalt ID-kort utenom passerverv/fornyelse, vil medføre kostnader knyttet til biometrifangst, infrastruktur, personell m.v. Gebyret for erverv av nasjonalt ID-kort utenom passerverv/fornyelse vil derfor være noe høyere enn ved samtidig ervervelse.

13.4 Incentiver – forholdet til konkurranselovgivning

Knyttes utstedelsen av nasjonalt ID-kort opp til utstedelsen av pass, vil forbrukerne dra nytte av positive synergieffekter som vil innebære lavere gebyr for erverv av nasjonalt ID-kort. Sett hen til at forbrukerne ved passerverv/fornyelse vil kunne erverve et nasjonalt ID-kort med en rekke funksjoner for et moderat tilleggsgebyr, er det grunn til å tro at en større del av de omlag halv million forbrukerne som årlig erverver/fornyer sitt pass samtidig vil gå til anskaffelse av et nasjonalt ID-kort.

En slik løsning vil kunne medføre at det relativt raskt kan utstedes et betydelig antall nasjonale ID-kort i samfunnet. Dette vil i så fall innebære en raskere utbredelse av moderne ID-dokumenter, med mulighet for passfri reise i EU/Schengen området. Det nasjonale ID-kortet vil slik raskt kunne bli et allment kjent og akseptert identitetsbevis, som vil kunne være det foretrukne reisedokumentet ved reiser til EU/Schengen land. En stor utbredelse av nasjonalt ID-kort vil imidlertid også medføre en større utbredelse av eID. Dette vil kunne gjøre det mer interessant for offentlige og private aktører å utvikle elektroniske tjenester på nett. Flere store offentlige etater er allerede i ferd med å utvikle tjenester som krever høyt sikkerhetsnivå ved identifisering av brukeren. Disse vil se det som en stor fordel at det ved lansering av tjenestene vil finnes innbyggere/brukere som allerede besitter et middel for slik elektronisk identifisering – nemlig det nasjonale ID-kortet med eID. Utbredelsen av kortet kan økes ytterligere dersom det på nettsider til slike tjenester gis mulighet for "bestilling" av kortet, jf. prosedyrer beskrevet i kap. 12.5.2.

De positive virkningene av funksjonene i det nasjonale ID-kortet vil få større effekt jo større utbredelsen av kortene blir. Det vil derfor være i samfunnets interesse at kortene sikres en størst mulig utbredelse og bruk. Det er i den forbindelse interessant å vurdere hvorvidt det vil være ønskelig eller nødvendig å benytte ulike incentiver for å øke utbredelsen ytterligere.

Til forskjell fra utstedelse av et offentlig og allment tilgjengelig identitetsdokument med eller uten EU/Schengen reisefunksjonalitet, vil en utstedelse av eID skje i konkurranse med private aktører. En ordning med offentlig utstedt eID vil derfor måtte gjennomføres i tråd med konkurranselov-

givningens prinsipper. En offentlig utstedelse av eID for bruk mot offentlige tjenester som for øvrig er åpne for konkurrerende private løsninger, antas ikke å være i strid med disse prinsippene. En offentlig subsidiering av ordningen for å øke utbredelsen, vil imidlertid raskt kunne være i strid med de nevnte prinsipper.

Selve eID-funksjonen i det nasjonale ID-kortet vil likevel kunne antas å bli konkurransedyktig på pris. Det offentlige vil nemlig være avhengig av å innhente eID-funksjonen fra private aktører, og vil da med stor grad av sannsynlighet kunne kjøpe inn denne funksjonen til svært konkurransedyktige vilkår på bakgrunn av ordningens antatte volum.

Da en rekke personer kan antas å ville erverve både pass og nasjonalt ID-kort, vil kostnadene knyttet til biometrifangst, infrastruktur og personell bli fordelt på et større antall dokumenter enn i dag. Den prosentvise merkostnaden knyttet til innføringen av en ordning med nasjonalt ID-kort vil antas å være lavere enn den prosentvise økningen i utstedte dokumenter. Kostnadene knyttet til selve ID-funksjonen vil derfor kunne antas å bli lavere pr. enhet etter innføringen av en ordning med nasjonalt ID-kort. Slik vil også et fremtidig passgebyr som reflekterer de reelle kostnadene knyttet til passutstedelsen, kunne være lavere enn hva de reelle kostnadene er i dag.

Det vil videre kunne ses på hvilke kostnader som skal regnes med som de reelle kostnader knyttet til utstedelse av pass og nasjonalt ID-kort. Mens kostnadene knyttet til utstedelse av eID åpenbart er relatert til det nasjonale ID-kortet, er det ikke like åpenbart at alle kostnadene som i dag knyttes opp til passutstedelsen også i fremtiden skal regnes med. Mens dagens kostnader til biometrifangst, infrastruktur og personell er direkte knyttet opp til grensekontroll, vil de tilsvarende kostnadene etter innføringen av et nasjonalt ID-kort også måtte knyttes til dets funksjon som allment identitetsbevis. En del av disse kostnadene vil derfor kunne knyttes til kortets funksjon som identitetsbevis til bruk ved f.eks. finanstransaksjoner. Dette vil gi besparelser for samfunnet som det er vanskelig å konkretisere, men som likevel bør kunne gis tilbake til forbrukeren i form av lavere gebyr.

De samfunnsmessige besparelsene knyttet til innføringen av en nasjonal ID-kortløsning med funksjoner som EU/Schengen reisedokument og eID er som tidligere påpekt vanskelig å konkretisere. Det er imidlertid grunn til å anta at et eventuelt bortfall av fiskale avgifter knyttet til passutstedelse vil kunne bli delvis kompensert gjennom besparelser for det offentlige knyttet til økt bruk av elektroniske tjenester, og gjennom økt bruk av moderne og sikre identitets-dokumenter i samfunnet som helhet.

13.5 Anbefalinger

Arbeidsgruppen anbefaler at ID-kortsøker betaler et gebyr som avspeiler de faktiske kostnader ved utstedelsesprosessen.

Ved samproduksjon av pass og ID-kort skal det ikke betales med enn ekstrakostnaden i forbindelse med ID-kortet (kortkostnaden, ekstra kostnader ved utsendelse (porto) og kostnader ved eID).

14 ANSVAR FOR STATEN KNYTTET TIL UTSTEDELSE

Staten påtar seg ved levering av ID-kort (mot gebyr) et kontraktsrettslig ansvar for at kortet er korrekt utfylt og inneholder alle sikkerhetselementer. Viser kortet seg å inneholde feil informasjon, eventuelt feil som fører til svikt i brukerfunksjoner (svikt ved maskinlesbarhet, manglende eller uriktig innlagt biometrisk informasjon mv.), som gjør at det helt eller delvis ikke vil fylle sin funksjon, må staten være ansvarlig for at vedkommende får utstedt nytt kort vederlagsfritt. Dette med mindre feilen kan tilskrives kortsøkers eget forhold (feil informasjon).

Etter omstendighetene vil staten også måtte bære særskilte kostnader knyttet til å få utstedt nytt kort, f.eks. i forbindelse med nytt fremmøte hos kortutsteder. Det samme må gjelde der kortet er blitt borte under forsendelse som del av utstedelsesprosessen.

På et erstatningsrettslig grunnlag vil staten også kunne bli ansvarlig for følgeskadene av at kortet er mangelfullt. F.eks. må det antas at staten må kunne holdes ansvarlig dersom en saksbehandler ved uaktsomhet har forårsaket en forveksling av ansiktsfoto som i en kontroll fører til at vedkommende blir avvist. Erstatningskrav vil betinge at vedkommende har lidt et økonomisk tap.

Der det kan konstateres at utenforstående tredjeperson har lidt økonomisk tap som kan tilbakeføres til feil i kortet som staten som utsteder må bære ansvaret for, vil statens erstatningsansvar etter omstendighetene også omfatte disse.

Etter omstendighetene vil staten kunne ha et refusjonsansvar hos produsenten av ID-kort. Et refusjonskrav vil dels kunne forankres i kontrakten, dels på vanlig erstatningsrettslig grunnlag.

15 ØKONOMISKE OG ADMINISTRATIVE KONSEKVENSER

Arbeidsgruppen foreslår å innføre et nasjonalt ID-kort som for norske statsborgere kan utstedes med EU/Schengen funksjonalitet. Det anbefales at kortet utstyres med en kontaktchip som kan inneholde en eID/e-signatur. Videre forutsettes kortet basert på samme standard som pass, det vil blant annet si maskinlesbarhet og utstyrt med en kontaktløs elektronisk brikke (RFID-brikke) ihht. ICAO standard.

Økonomiske konsekvenser
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 omlag **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: 4.000.000.
- Varslingstjeneste og brukerstøtte: 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 etter anslagsvis ligge på ca. **NOK 340,-.**

Kapitalkostnader for biometrikiosker er ikke tatt med i denne beregningen.

Administrative konsekvenser:
Innføring av nasjonalt ID-kort vil ikke ha vesentlige administrative 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.

Økonomisk/administrative konsekvenser for utenriksstasjonene
Ved utenriksstasjonene vil selv et relativt lavt antall henvendelser kunne få merkbare konsekvenser som følge av en sårbar bemanningssituasjon. Det kan også bemerkes at en kortere gyldighetstid for ID-kortene (og evt. også for pass) enn dagens 10 år for pass, over tid vil føre til økt etterspørsel. Utenriksdepartementet ønsker at dette utredes nærmere i forbindelse med en eventuell forberedelsesprosess.

16 VEDLEGG A - GJENNOMGANG AV NÆRMERE ANGITTE KRAV I ESIGNATURLOVEN, OG FORHOLDET TIL AT EID I DET NASJONALE ID-KORTET ER OFFENTLIG UTSTEDT

Utgangspunktet her er at den eID som skal utstedes av det offentlige vil være et kvalifisert sertifikat, eller basert på et kvalifisert sertifikat med ytterligere tilleggskrav, som f.eks. Person Høyt i henhold til "Kravspesifikasjon for PKI i offentlig sektor".

Esignaturloven oppstiller en rekke krav overfor utstedere av kvalifiserte sertifikater og til innholdet av slike sertifikater.

- Lovens virkeområde (§ 2)

Loven gjelder for sertifikatutstedere som er etablert i Norge, den vil også gjelde overfor en offentlig etat som utsteder sertifikater. I esignaturloven § 3 nr. 10 er sertifikatutsteder definert som "en fysisk eller juridisk person som utsteder sertifikater eller tilbyr andre tjenester relatert til elektronisk signatur".

- Krav til innhold i kvalifiserte sertifikater (§ 4)

Esignaturloven gir detaljerte krav til hvilken informasjon kvalifiserte sertifikater skal innholde, bl.a. oppstilles det krav om at sertifikatet innholder sertifikatutstederens identitet og den stat den er etablert i. Sertifikatet må således innholde navnet på den etat som er sertifikatutsteder. Dessuten stilles det krav om at dersom det oppstilles ev. begrensninger i sertifikatets anvendelsesområde eller ev. beløpsmessige begrensninger i sertifikatet med hensyn til hvilke transaksjoner sertifikatet kan brukes til, må disse begrensingene fremgå direkte i sertifikatet. Det er ikke tilstrekkelig med f.eks. en peker fra sertifikatet til et annet dokument (f.eks. til sertifikatpolicyen) der disse begrensningene er angitt, jf. § 22.

- Krav til kvalifiserte elektroniske signaturer brukt i kommunikasjon med og i offentlig sektor (§ 5)

Ifølge loven kan Kongen "fastsette nærmere regler om hvilke krav som skal stilles til kvalifiserte elektroniske signaturer som skal brukes ved kommunikasjon med og i offentlig sektor". Slike tilleggskrav skal være objektive, klare og forholdsmessige og sikre likebehandling, og skal bare gjelde den aktuelle anvendelsens særskilte kjennetegn. Dessuten skal de ikke utgjøre noen hindring for yting av tjenester til borgerne over landegrensene.

Selv om dette er en bestemmelse som åpner for å gi tilleggskrav til kvalifiserte elektroniske signaturer - dvs. en avansert elektronisk signatur som er basert på et kvalifisert sertifikat og fremstilt av et godkjent sikkert signaturfremstillingssystem – burde det neppe være en hindring for å stille tilleggskrav til kvalifiserte sertifikater som brukes ved kommunikasjon med og i offentlig sektor. Denne bestemmelsen åpner således for at det kan stilles særskilte krav til eID'er (basert på kvalifiserte sertifikater) som skal brukes som autentiseringsløsning ved kommunikasjon med og i offentlig sektor.[32] Esignaturloven er basert på et EU-direktiv, og i hvilken utstrekning

[32] Denne bestemmelsen er benyttet som forskriftshjemmel til eForvaltningsforskriften.

det er mulig å avvike fra direktivet (og loven) er det sannsynligvis ikke noen grunn til å vurdere på nåværende tidspunkt.

Det skal også bemerkes at kun å akseptere en eID utstedt av utpekt offentlig norsk etat ved kommunikasjon med og i norsk offentlig forvaltning, kan være i strid med EUs direktiv som esignaturloven bygger på.

- Innsamling og bruk av personopplysninger (§ 7)

Av loven følger det at sertifikatutstedere kun får innhente personopplysninger direkte fra den opplysningene gjelder, eller med dennes uttrykkelige samtykke og bare i den utstrekning som er nødvendig for å utstede eller opprettholde et sertifikat. Opplysningene må ikke samles inn eller behandles for andre formål, så fremt ikke den opplysningene gjelder har gitt sitt uttrykkelige samtykke til det. Dette er strengere krav enn hva som f.eks. følger av personopplysningsloven. Denne bestemmelsen omfatter alle sertifikatutstedere, også de som ikke usteder kvalifiserte sertifikater. Datatilsynet fører tilsyn med at denne bestemmelsen overholdes.

Hva man må være klar over i denne sammenheng er at når samme opplysninger innhentes som grunnlag for utstedelse av det nasjonalt ID-kortet, eID og ev. også pass, må skjemaet som brukes gi søker informasjon om hva opplysningene skal brukes til.

- Krav til utstederens virksomhet (§ 10)

Utstedere av kvalifiserte sertifikater skal utøve og administrere virksomheten på en forsvarlig måte slik at de kan tilby sikre, pålitelige og velfungerende sertifikattjenester. Dette byr ikke på noen særskilte problemer eller utfordringer pga. at utstederen er en offentlig virksomhet.

Dessuten stilles det krav om at sertifikatutstederen til enhver tid skal ha tilstrekkelige økonomiske ressurser til å kunne drive virksomheten i henhold til kravene som er stilt i eller i medhold av denne lov. Dette kravet kan oppfylles ved kapitaldekking, forsikringsordning, garanti eller på annen måte. Tatt i betraktning at staten er selvassurandør vil dette kravet neppe være et problem.

- Krav om kontroll av undertegners identitet (§ 13)

Ifølge loven er utstedere av kvalifiserte sertifikater ansvarlige for at identiteten til undertegner og ytterligere relevante opplysninger om vedkommende blir kontrollert gjennom sikre rutiner. Krav om identifisering er nærmere regulert i en forskrift til loven som stiller krav om personlig fremmøte hos sertifikatutsteder eller representant for denne, med mindre søker allerede er identifisert ved personlig fremmøte gjennom eksisterende kundeforhold, jf. forskrift 15. juni 2001 nr. 611 om krav til utsteder av kvalifiserte sertifikater mv. § 7.

Gruppen anbefaler at det stilles krav om personlig oppmøte ved innlevering av søknad om nasjonalt ID-kort. Dersom gyldighetstiden for det fysiske ID-kortet er lengre enn for eID'ene, vil det være behov for å kunne fornye eID før den fysiske legitimasjonen må byttes. Dette vil også gjelde i situasjoner dersom man av andre grunner må trekke tilbake eID og utstede en ny. En slik fornyelse av eID'en kan, uten å være i strid med esignaturlovens krav, foretas uten personlig oppmøte.

I tilknytning til dette bør også nevnes at dersom man ønsker å benytte sertifikatklassen Person Høyt som eID, stilles det i Kravspesifikasjon for PKI i offentlig sektor (punkt 4.3) detaljerte krav om hvilke dokument som skal presenteres for identifisering av vedkommende ved det personlige

oppmøtet. Kravspesifikasjonen viser her til hvitvaskingsforskriften § 4 første ledd. Det vil være behov for å nærmere drøfte hvordan disse kravene skal etterleves dersom det offentlige skal utstede en eID på nivå Person-Høyt.

- Krav til lagring av opplysninger (§ 14)

En utsteder av kvalifiserte sertifikater skal lagre alle relevante opplysninger om kvalifiserte sertifikater i en rimelig periode, dog minst 10 år etter at sertifikatet er registrert i tilbaketrekkingslisten. Dette er ikke et krav som er vanskelig for en sertifikatutsteder å etterleve av den grunn at den er en offentlig etat. Det kan derimot finnes annet regelverk som stiller ytterligere krav om omfang og lengde av lagringen som en sertifikatutsteder kan være nødt til å etterleve. Statens lånekasse for utdanning stiller f.eks. krav om 30 års lagringstid.

Det skal også bemerkes at dersom eID skal være på nivå Person Høyt, stilles det spesifikke krav til lagring, oppbevaring og sletting av opplysninger, jf. Kravspesifikasjonen for PKI i offentlig virksomhet punkt 4.2.6 med henvisning til hvitvaskingsloven § 6 første og annet ledd og hvitvaskingsforskriften § 15. Det vil også her være grunn til å nærmere drøfte de praktiske spørsmålene om hvordan disse kravene skal etterleves.

- Krav om informasjon om vilkår, begrensninger og lignende (§ 15)

Før en sertifikatutsteder inngår avtale om å utstede et kvalifisert sertifikat skal denne skriftlig informere motparten om:

a) vilkårene og begrensningene for bruken av sertifikatet,
b) opplysninger om eventuelle frivillige sertifiserings-, godkjennings- eller selvdeklarasjonsordninger, og
c) prosedyrer for klage og avgjørelse av tvister

Dette er sannsynligvis et informasjonskrav som skiller seg fra f.eks. de kravene politiet har å etterleve ved utstedelse av pass. Informasjonskravene er imidlertid neppe vanskelige å etterleve, men det vil kreve nye/justerte prosedyrer og skjemaer for å sikre at de blir ivaretatt.

- Tilsyn med utstedere av kvalifiserte sertifikater (§§ 17 og 19)

Post- og teletilsynet (PT) er tilsynsorgan og har store "fullmakter" for å sikre at lovens krav etterleves. PT kan bl.a. kreve at det gjennomføres IT-revisjon, kreve opplysninger og dokumenter fra sertifikatutsteder som er nødvendige for å utføre sine tilsynsoppgaver og få uhindret adgang til den del av virksomheten som omfattes av tilsynet, herunder lokaler, utstyr mv. Slik kontroll kan også skje hos sertifikatutstederens registreringsenheter. For å så langt som mulig sikre at PT kun få innsyn i de deler av virksomheten som er knyttet til utstedelsen av eID vil det være hensiktsmessig å skille denne oppgaven fra andre sensitive oppgaver.

- Tvangsmulkt og straff (§§ 20 og 21)

PT kan pålegge sertifikatutsteder tvangsmulkt for å sikre at bestemmelser som er gitt i eller i medhold av denne lov overholdes. Dessuten kan utstedere av kvalifiserte sertifikater straffes med bøter ved forsettlig eller grovt uaktsom overtredelse av angitte bestemmelser i loven.

- Erstatning (§ 22)

Med mindre en utsteder av kvalifiserte sertifikater kan godtgjøre at han ikke har handlet uaktsomt, er han erstatningsansvarlig dersom:

a) informasjonen angitt i sertifikatet ikke var korrekt på utstedelsestidspunktet,
b) sertifikatet ikke inneholder alle opplysninger som kreves i henhold til § 4,
c) signaturfremstillingsdata (privat nøkkel) og signaturverifikasjonsdata (offentlig nøkkel) ikke hører sammen på en unik måte dersom sertifikatutstederen fremstiller begge,
d) undertegner ikke disponerte korrekt signaturfremstillingsdata på tidspunktet da sertifikatet ble utstedt, eller
e) tilbaketrukket sertifikatet ikke blir registrert i tilbaketrekkingslisten

En sertifikatutsteder er imidlertid ikke erstatningsansvarlig for skade som skyldes at sertifikatet er blitt brukt i strid med tydelige begrensninger i sertifikatets anvendelsesområde eller utover beløpsmessige begrensninger. Som allerede nevnt må disse begrensningene fremgå direkte i sertifikatet (jf. § 4 ovenfor). Per i dag kan det være vanskelig å oppfylle slike krav. Dersom det vil være et absolutt krav å innføre en slik begrensning i sertifikatet, vil det være nødvendig nærmere å vurdere hvordan et slikt behov kan ivaretas.

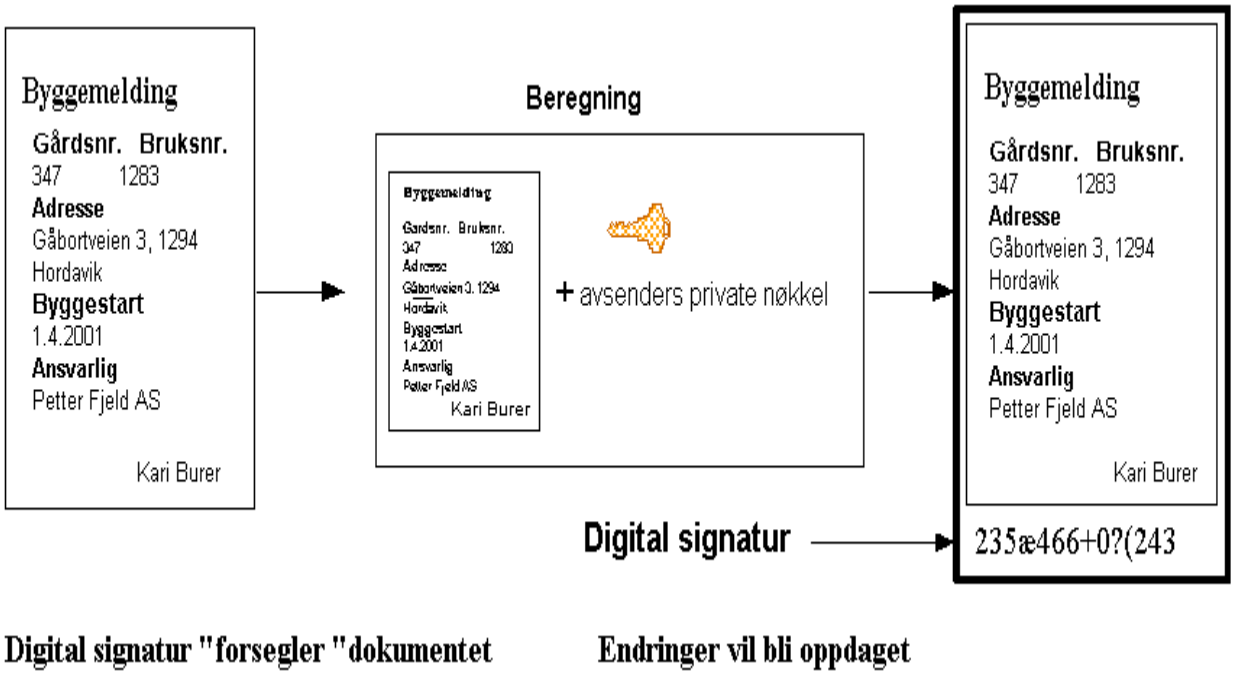
- Gebyr (§ 24)

Utstedere av kvalifiserte sertifikater må registrere seg ved PT før utstedelse av sertifikatene. Utstedere av kvalifiserte sertifikater skal dessuten betale et årlig gebyr til PT. Til dette kan også nevnes at sertifikatutstedere som har sendt inn selvdeklarasjon i henhold til krav etter Kravspesifikasjon for PKI i offentlig sektor – for enten sertifikatklassen Person-Standard, Person-Høyt eller Virksomhet – også skal betale et årlig gebyr til PT.

17 VEDLEGG B - DIGITALE SIGNATURER OG AUTENTISERING

Fra NOU 2001:10 Uten Penn og Blekk

Digitale signaturer:
Digitale signaturer er en måte å benytte asymmetrisk kryptografi på som gir sikkerhet for at det er den rette personen som har sendt meddelelsen. Metoden som benyttes gir også sikkerhet for at meddelelsen ikke er blitt forfalsket av uvedkommende underveis fra avsender til mottaker (integritet).



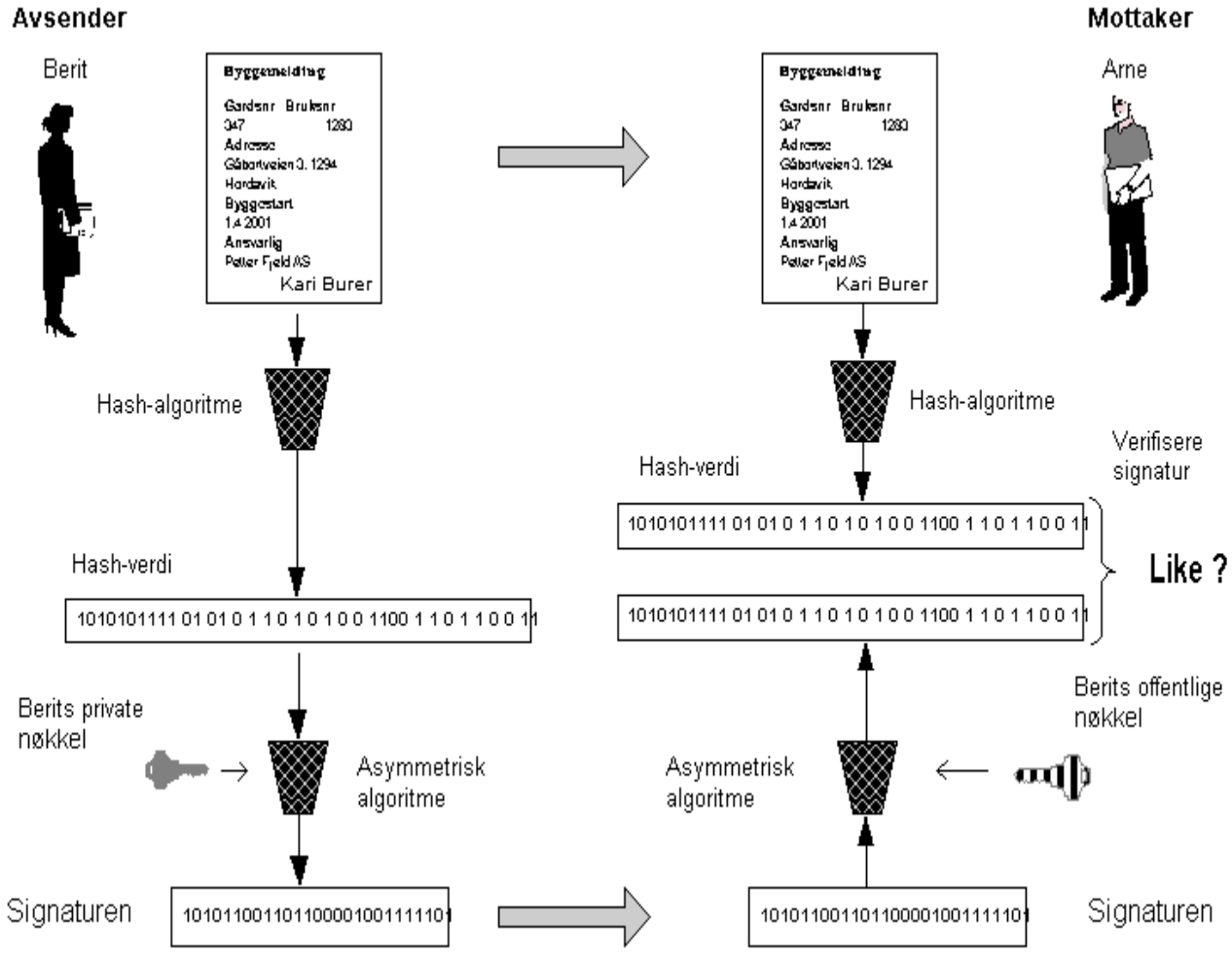
Figur - Digital signatur
En *digital signatur* er et dataelement som følger en elektronisk melding eller et dokument, og som binder dokumentet til et individ, en maskin eller et datasystem. Bindingen er slik at signaturen er praktisk umulig å forfalske. Den kan verifiseres av en mottaker eller av en uavhengig tredjepart. Hvis en bokstav i dokumentet endres, vil den digitale signaturen ikke bli godkjent.

Da kryptering av store tekstmengder med den private nøkkelen tar for lang tid, har man tatt i bruk en beregningsmåte kalt *hash-algoritme* når man skulle lage en digital signatur på et dokument. Ut fra dokumentet produserer hash-algoritmen et unikt tall (en *hash-verdi*). Den matematiske funksjonen som benyttes er slik at man ikke kan gjenskape dokumentet ut fra tallet, og to ulike dokumenter skal ikke lage samme tall. Man kan si at hash-verdien representerer et dokument på en i praksis unik måte. Hvis så mye som en bokstav blir endret i dokumentet, vil hash-verdien bli en annen. Det er hash-verdien av dokumentet som krypteres med den private nøkkelen. *Den krypterte hash-verdien er den digitale signaturen.*

Man kan derfor si at en digital signatur er en unik kombinasjon av den private nøkkelen som ble benyttet, og dokumentets innhold slik det representeres av hash-verdien. To ulike personer, med

to ulike private nøkler, vil lage to ulike digitale signaturer på det samme dokumentet. Hvis dokumentet blir endret underveis til mottakeren, vil signaturen ikke lenger la seg verifisere.

Verifisering av en digital signatur skjer ved at mottakeren av et digitalt signert dokument beregner hash-verdi av dette dokumentet. Deretter dekrypterer mottaker den krypterte hash-verdien som ble tilsendt med dokumentet (den digitale signaturen). Mottaker dekrypterer den med den offentlige nøkkelen til avsenderen. Denne nøkkelen kan enten sendes med dokumentet eller hentes fra en offentlig tilgjengelig katalog. Så sammenlikner mottaker de to hash-verdiene (tallene) mot hverandre. Er de helt like, er signaturen i orden. Er de ulike, så er noe galt, dvs. noen har prøvd å endre dokumentet underveis.

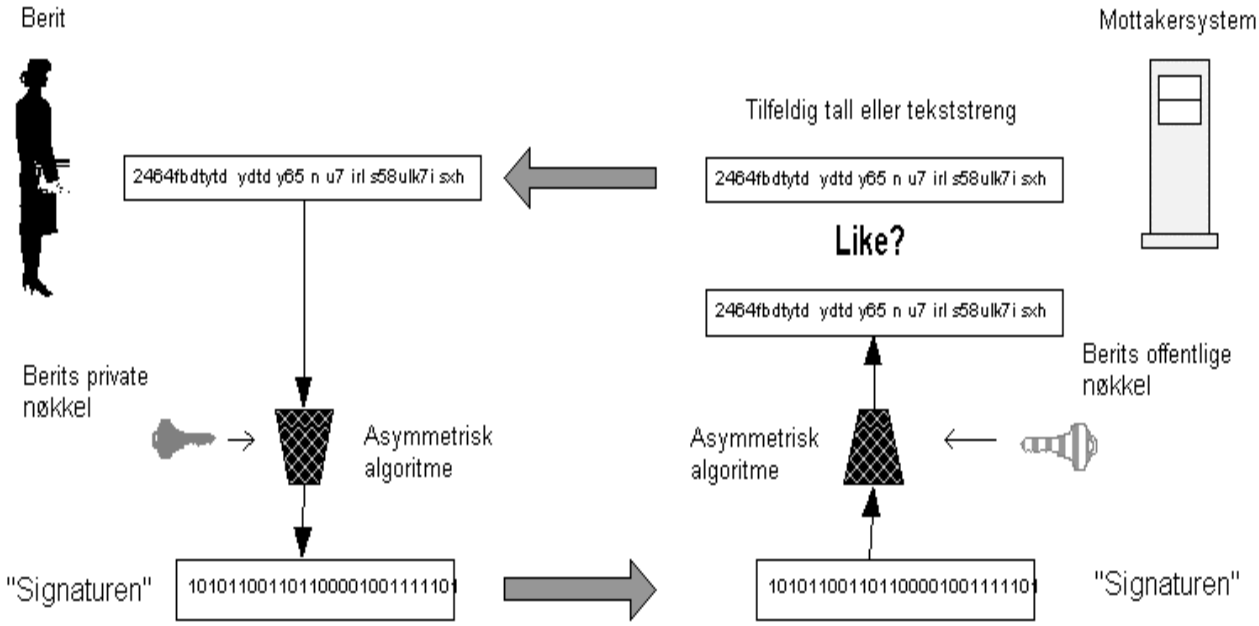


Figur - Å signere og verifisere et dokument

Dersom mottakeren ikke klarer å dekryptere hash-verdien med den offentlige nøkkelen til avsenderen, betyr det at det var en annen privat nøkkel som ble benyttet. Noen har prøvd å utgi seg for eieren av den offentlige nøkkelen, men hadde ikke den passende private nøkkelen. Figuren ovenfor illustrerer hvordan digital signatur lages og sjekkes (verifiseres).

Autentisering:
Digitale signaturer kan brukes på elektroniske dokumenter, men ikke bare til det. Man oppdaget at denne metoden, som i grunnen gir sikkerhet for hvem som brukte sin private nøkkel, også kan

benyttes for å verifisere hvem man kommuniserer med over nett. Autentisering kan brukes til å verifisere en påstått identitet eller en mottaker. Man kan med andre ord benytte digitale signaturer for å erstatte passord ved pålogging til datasystemer og tjenester i nettverk. Dette illustreres i figuren nedenfor.



Figur - Å autentisere en bruker

Mottakersystemet sender et tilfeldig tall eller en tekststreng til den som vil logge seg på. Brukeren krypterer dette tallet med sin private nøkkel. Mottakersystemet verifiserer «signaturen» med brukerens offentlige nøkkel, som enten er lagret i systemet eller hentes fra en offentlig katalog. Dersom verifiseringen av brukerens «signatur» har gått bra, kan brukeren komme inn i systemet og benytte tjenester i det. Fordelen med å benytte digitale signaturer til autentisering er at de bygger på en standardisert metode, som mange datasystemer kan ta i bruk. Brukeren behøver ikke å huske mange ulike passord eller koder som trengs for tilgang til de ulike systemene. Brukeren trenger bare sin private nøkkel, og systemene trenger brukerens offentlige nøkkel.