DET KONGELIGE
NÆRINGS- OG HANDELSDEPARTEMENT

Ot.prp. nr. 82

(1999-2000)

Om lov om elektronisk signatur

Tilråding fra Nærings- og handelsdepartementet av 29. september 2000, godkjent i statsråd samme dag.

1 Proposisjonens hovedinnhold

Lovforslaget i proposisjonen regulerer de rettslige rammebetingelsene for bruk av elektronisk signatur og tilknyttede tjenester. Et viktig formål med lovforslaget er å sikre kommunikasjon mellom to parter som ikke kjenner hverandre, og dermed legge til rette for elektronisk handel.

Bruk av elektronisk signatur skaper tillit mellom ukjente parter som har behov for å vite at den de kommuniserer med er den vedkommende gir seg ut for å være. For å sikre denne tilliten mellom avsender og mottaker utstedes signaturen sammen med et tilhørende elektronisk sertifikat av en tredje part, i loven omtalt som sertifikatutsteder. Systemet er avhengig av at partene stoler på denne utstederen. Sertifikatutstederen skal bl.a. kontrollere identiteten til den som signerer. I lovforslaget er denne personen omtalt som undertegner. Hvem undertegner er fremgår av sertifikatet.

En elektronisk signatur kan brukes som bekreftelse på hvem som sendte informasjonen, som sikkerhet for at elektronisk overført informasjon ikke har blitt endret underveis og som sikkerhet for at avsender ikke skal kunne benekte at han sendte den. Disse funksjonene kan benevnes som sikring av autentisitet, integritet og ikke-benekting. Den typen elektronisk signatur som i dag sikrer alle disse funksjonene kalles «digital signatur».

Elektronisk signatur kan f.eks. brukes til å treffe avtaler, til elektronisk innrapportering og ved elektronisk dokumenthåndtering. Dessuten kan signaturen brukes ved betaling over Internett.

Loven skal legge til rette for at signaturene og tilhørende sertifikater som tilbys på det norske markedet, oppfyller et bestemt sikkerhetsnivå. Disse produktene omtales som *kvalifiserte* eller *sikre*. Kravene til sikkerhet skal balanseres mellom forretningsmessige hensyn, forbrukerhensyn og samfunnsmessige hensyn. De nærmere tekniske kravene vil bli regulert i forskrifter til loven. Loven åpner for at det kan stilles tilleggskrav ved kommunikasjon med og i forvaltningen.

Loven skal dermed ikke regulere det samlede tilbudet av signaturer og tilhørende sertifikater og sertifikattjenester, men i all hovedsak regulere rammebetingelsene for bruk av kvalifiserte signaturer og kvalifiserte sertifikater. Sertifikatutstederne vil dermed falle utenfor denne lovreguleringen og det tilsynsregimet loven oppstiller ved ikke å kalle sine sertifikater for kvalifiserte, selv om de oppfyller kravene. Departementet ser for seg at sertifikater med et lavere sikkerhetsnivå eller andre sikkerhetsmekanismer, kan tilfredsstille behovene for kontroll av ekthet ved transaksjoner over nett for deler av markedet. Etterspørselen i markedet vil avgjøre hvilke sertifikater som vil bli benyttet fremover.

Loven gir ingen generell rett til å kommunisere elektronisk, men gjelder der lovgivningen for øvrig åpner for elektronisk kommunikasjon. Når det stilles krav om underskrift, vil bruk av kvalifisert elektronisk signatur alltid oppfylle et slikt krav, så fremt disposisjonen kan skje elektronisk. Dette betyr at en kvalifisert elektronisk signatur gis samme rettsvirkning som en håndskreven signatur.

Markedet for elektroniske signaturer er i rivende utvikling. Det er viktig at reguleringen på dette området ikke begrenser, hindrer eller på annen måte påvirker utviklingen negativt. En svært detaljert regulering vil sannsynligvis også føre til et behov for hyppige justeringer. For å unngå dette er reguleringen så langt som mulig nøytral i forhold til valg av tekniske løsninger. Samtidig må man være klar over at det er vanskelig å gi rettslige virkninger til en ukjent eller ikke definert teknisk løsning. Her må det således skje en avveining mellom å være teknologinøytral og å gi de teknologier som omfattes av loven rettslige virkninger.

Regjeringen ser behov for regulering av elektronisk signatur for å legge til rette for utviklingen av elektronisk handel og elektroniske tjenester i Norge. Lovreguleringen skal søke å påvirke det norske markedet for sertifikatutstedere og elektroniske signaturprodukter i en positiv retning. Ved å regulere tilbudet av kvalifiserte sertifikater, vil lovforslaget stimulere til bruk av sertifikater med et bestemt sikkerhetsnivå som kan brukes i mange sammenhenger. Videre er det behov for lovregulering på området for å bidra til at tilliten til markedet og tilliten til bruk av elektronisk signatur i samfunnet øker, slik at signaturteknologi blir tatt i bruk på bred basis. Bruk av elektronisk signatur er en viktig forutsetning for utviklingen av sikker elektronisk handel.

Loven er en gjennomføring av EU-direktivet om en fellesskapsramme for elektroniske signaturer.

2 Bakgrunnen for lovforslaget

2.1 Behovet for regulering

Av St. meld. nr. 41 (1998-99) «Om elektronisk handel og forretningsdrift» fremgår det at:

> «Regjeringen har som mål at elektronisk kommunikasjon og bruk av nett som infrastruktur for samhandling skal bli like akseptert, tillitsvekkende og ha samme juridiske holdbarhet som tradisjonell skriftlig kommunikasjon og dokumentasjon».

I regi av Rådet for IT-sikkerhet (RITS) ble det i 1998 utarbeidet en rapport med anbefalinger om hvilke tiltak sentrale myndigheter bør sette i verk for å legge til rette for bruk av digitale signaturer og sertifikatutstedere. Rapporten har tittelen: «Digitale signaturer gir tillit til elektronisk kommunikasjon - Forslag til tiltak for aksept og utbredelse». Denne rapporten ligger til grunn for mye av det arbeidet som senere har blitt gjort på området i regi av departementet, se ellers kapittel 4.1.

Rettslig likestilling mellom elektroniske dokumenter og signaturer, og papirbaserte dokumenter og signaturer, ble særlig fremhevet i denne rapporten. Ett av de viktigste oppfølgingstiltakene av rapporten er således beslutningen om å pålegge alle departementer å gå igjennom regelverket i sine respektive sektorer, med sikte på å avdekke og endre regler som unødvendig hindrer elektronisk kommunikasjon. Denne relativt store gjennomgangen omtales gjerne som «Kartleggingsprosjektet», se kapittel 4.3. Fjerning av hindringer, kombinert med dette lovforslaget, vil langt på vei skape klarhet og legge til rette for bruk av elektronisk signatur ved elektronisk kommunikasjon.

2.2 Gjennomføring av direktivet om elektronisk signatur i norsk rett

EU-kommisjonen la 13. mai 1998 frem forslag til Europaparlaments- og Rådsdirektiv om en fellesskapsramme for elektroniske signaturer, med utgangspunkt i EF-traktatens artikkel 57(2), 66 og 100A, og i henhold til prosedyren i artikkel 189 B.

Forslaget følger opp en henstilling fra Rådet om å utarbeide et forslag til direktiv, basert på en «Communication to the Council» av 8. oktober 1997. Direktivet ble endelig vedtatt den 13. desember 1999 og ble publisert i De Europeiske Fellesskaps Tidende (EF-Tidende) den 19. januar 2000, med en implementeringstid for medlemslandene på 18 måneder. Denne fristen gjelder også for Norge.

Bakgrunnen for EU-direktivet er at utviklingen av elektronisk handel over åpne globale nett nødvendiggjør elektroniske signaturer med tilhørende tjenester som sørger for autentisering. Dersom EU-landene har ulike regelverk hva angår rettslig anerkjennelse av elektroniske signaturer og akkreditering av sertifikatutstedere, kan dette skape barrierer for elektronisk handel og hin-

dre utviklingen av det indre marked. Det er derfor behov for et harmonisert rammeverk for bruk av elektronisk signatur.

Det finnes per i dag ingen formell norsk oversettelse av EU-direktivet. På bakgrunn av dette vil sitering skje ut fra den offisielle engelske versjonen av direktivet.

2.3 Behovet for regulering i egen lov

Deler av EU-direktivet om elektroniske signaturer stiller absolutte krav overfor statene og må implementeres i lov eller forskrift. Andre deler av bestemmelsene står statene derimot fritt til å implementere, f.eks. regulering av frivillige akkrediteringsordninger eller godkjennelsesordninger. Det er mulig å sikre at virkningene av disse bestemmelsene oppnås på annen måte enn ved lovregulering dersom det er mest hensiktsmessig, f.eks. ved å arbeide for frivillig regulering av markedets parter.

Spørsmålet her er hvordan den først nevnte typen bestemmelser skal implementeres i norsk rett. I utgangspunktet finnes det to alternativer. Implementeringen kan skje ved at det opprettes et helt nytt regelverk, eller den kan skje i allerede eksisterende regelverk.

Deler av EU-direktivet gjelder områder som allerede er regulert i norsk rett, f.eks. bestemmelser om erstatning og bevisregler. Hoveddelen av bestemmelsene gjelder likevel forhold som ikke uten problemer kan legges til allerede eksisterende lover eller forskrifter. Dessuten er mange av direktivets bestemmelser tekniske og har en så nær tilknytning til hverandre at det ikke ville være hensiktsmessig å gjennomføre direktivet i forskjellige regelverk. Det vil også være enklere for sertifikatutstederne, som direktivet i hovedsak regulerer, dersom de særregler som omfatter deres virksomhet så langt som mulig er samlet i ett regelverk. Bestemmelsene regulerer noe helt nytt slik at det ikke er noen større risiko for dobbeltregulering i forhold til eksisterende regelverk. På denne bakgrunn er departementet kommet til at EU-direktivet bør implementeres i en ny lov med tilhørende forskrifter.

Et ytterligere argument for å implementere direktivet i en ny lov, er at Sverige og Danmark har implementert EU-direktivet i en egen lov. Også Finland og Island vil i løpet av året utarbeide en egen lov for å implementere direktivet. For å ivareta den nordiske rettstradisjonen bør implementeringen i Norge skje på en tilnærmet identisk måte som i de øvrige nordiske land. Vedrørende arbeid i de nordiske land, se kapittel 6.

2.4 Høringen

Nærings- og handelsdepartementet sendte forslag til lov om elektronisk signatur på åpen høring den 29. februar 2000 med høringsfrist 5. mai 2000. Høringsbrevet ble sendt til følgende institusjoner og organisasjoner:

–Departementene
–Akademikernes Fellesforbund
–Aksjespareforeningen i Norge
–Alcatel Telecom Norway
–Arthur Andersen
–Bergen kommune

–Brønnøysundregistrene
–Datatilsynet
–Den Norske Advokatforening
–Den norske bankforening
–Den norske dataforening (DND)
–Den norske Revisorforening
–Det Norske Veritas
–Direktoratet for sivilt beredskap
–Dovre Sertifisering
–eforum
–Fellesdata
–Finansieringsselskapenes Forening
–Finansnæringens Hovedorganisasjon (FNH) og Sparebankforeningen
–Forbrukerrådet
–Forskningsministeriet, Danmark
–Forsvarets Overkommando/Sikkerhetsstaben (FO/S)
–Forum for IT-sikkerhet
–Grøner Certification
–Handels- og Servicenæringens Hovedorganisasjon (HSH)
–IBM
–ICL Norge
–Justervesenet
–Justisministeriet, Finland
–Kommunenes Sentralforbund
–Kompetansesentret for IT i helsevesenet (KITH)
–Kontor- og datateknisk landsforening
–KPMG Consulting AS
–Kredittilsynet
–Landsorganisasjonen i Norge (LO)
–Merkantildata
–NEMKO
–Netcom
–NITO
–Norges delegasjon til Den Europeiske Union i Brüssel
–Norges Juristforbund
–Norges forsikringsforbund
–Norman Data Defence
–Norsk Akkreditering
–Norsk Hydro
–Norsk kommuneforbund
–Norsk presseforbund
–Norsk EDIPRO
–Norsk Teknologistandardiserings forbund
–Norsk Regnesentral
–Norwegian Certification System
–n3sport
–Næringslivets Hovedorganisasjon (NHO)
–Næringslivets sikkerhetsorganisasjon (NSO)
–Næringsteknisk Forum
–Næringsdepartementet, Sverige
–Oslo Børs
–Oslo kommune

–PA Consulting
–PKI-utvalget
–Post- og teletilsynet
–Posten SDS
–Regjeringsadvokaten
–Riksarkivet
–Rikstrygdeverket
–Skattedirektoratet
–Statens forvaltningstjeneste
–Statskonsult
–Stavanger kommune
–Statoil
–Teknologibedriftenes landsforening
–Telenor
–Telia
–Toll- og avgiftsdirektoratet
–Trondheim kommune
–Universitetene
–Utvalget «Myndighetsroller og digitale signaturer»

Av høringsinstansene har 44 svart, hvorav 31 har kommet med konkrete merknader. Flere andre organisasjoner har kommet med merknader i tillegg til høringsinstansene. Det har kommet uttalelser fra i alt 52 instanser. Følgende instanser har avgitt realitetsuttalelse:
–Advokatforeningen
–Arbeids- og administrasjonsdepartementet
–Barne- og familiedepartementet
–Brønnøysundregistrene
–Datatilsynet
–eforum
–Finansieringsselskapenes Forening
–Finansnæringens Hovedorganisasjon (FNH) og Sparebankforeningen
–Forsvarets Overkommando/Sikkerhetsstaben (FO/S)
–Justervesenet
–Justisdepartementet
–Kommunal- og regionaldepartementet
–Kompetansesentret for IT i helsevesenet (KITH)
–Kredittilsynet
–Landsorganisasjonen i Norge (LO)
–Norges Eksportråd / Euro Info
–Norges forskningsråd
–Norges Rederiforbund
–Norsk Bedriftsforbund
–Norsk EDIPRO
–Norsk Regnesentral
–Norges teknisk-naturvitenskapelige universitet (NTNU)
–Norsk tele- og informasjonsbrukerforening (NORTIB)
–Næringslivets Hovedorganisasjon (NHO)
–Næringslivets sikkerhetsorganisasjon (NSO)
–Oljedirektoratet
–Oslo kommune
–Patentstyret

–Post- og teletilsynet
–Posten SDS
–Riksarkivet
–Rikstrygdeverket
–Samferdselsdepartementet
–Skattedirektoratet
–Sosial- og helsedepartementet
–Statens nærings- og distriktsutviklingsfond (SND)
–Statskonsult
–Telenor
–Toll- og avgiftsdirektoratet
–Universitetet i Oslo

2.5 Høringsinstansenes generelle merknader

Høringsinstansenes merknader som knytter seg til konkrete punkter i lovforslaget, vil bli behandlet under de respektive kapitler i proposisjonen.

Høringsinstansene stiller seg utelukkende positive til at det nå gis en lovregulering av elektronisk signatur og tilhørende sertifikattjenester. Flere høringsinstanser uttaler at lovforslaget legger til rette for anvendelse av elektroniske signaturer i større skala ved å etablere rettsstillingen for signaturene og gjennom den tillitskapende effekt reguleringen av sertifikattjenestene gir.

Arbeids- og administrasjonsdepartementet uttaler at en lovregulering av virksomheten til de som utsteder sertifikater og tilbyr relaterte tjenester vil bidra positivt til at tilliten til markedet og tilliten til bruk av elektroniske signaturer i samfunnet øker, med det resultat at slik teknologi blir tatt i bruk på bred basis. Videre uttaler departementet at utbredelsen av teknologien er en forutsetning for elektronisk handel og forretningsdrift, så vel som for realisering av en elektronisk forvaltning som kan tilby døgnåpne elektroniske tjenester til borgere via Internett.

Enkelte høringsinstanser påpeker at det er sentralt at reguleringen fra lovgivers side ikke vil begrense, hindre eller på annen måte påvirke utviklingen av markedet negativt, og at det er viktig at man ikke utformer en lov som stiller norske sertifikatutstedere i en dårligere stilling konkurransemessig enn sertifikatutstedere etablert i andre land. Høringsinstansene er generelt positive til at det legges opp til en minimumsregulering og en enkel modell for tilsyn.

*Kommunal- og regionaldepartementet, Finansieringsselskapenes Forening, Norsk EDIPRO, NHO, FNH*og *Sparebankforeningen* har som utgangspunkt at loven er for teknisk og lite tilgjengelig for personer uten teknologisk bakgrunn. På den annen side etterlyser *NORTIB* nærmere regulering av bl.a. endesystemene [1)] . *Norges teknisk-naturvitenskapelige universitet (NTNU)* etterlyser ytterligere krav til sikkerhet av hensyn til at trusselbildet er svært forskjellig i forhold til papirbasert kommunikasjon og dette stiller krav til de tekniske komponentene. *FO/S* og *KITH* kommer med forslag til presiseringer i lovteksten av tekniske hensyn. Ellers viser også flere høringsinstanser til

[1)] Med endesystem menes den enheten som foretar signering og/eller verifisering av en signatur, altså utstyret hos undertegner eller mottaker.

at realiteten av innholdet i loven i stor grad ikke kan klarlegges før forskriftene er på plass.

Særlig *Justisdepartementet* og *Statskonsult* kommer med flere konkrete forslag til endringer av lovteksten slik at den gjøres lettere tilgjengelig. Disse innspillene er tatt hensyn til ved revidering av lovteksten og merknadene til bestemmelsene.

3 Noen utgangspunkter

3.1 Hva er en elektronisk signatur og digital signatur?

Elektronisk signatur er den brede og generelle betegnelsen på teknikker som kan benyttes til å «signere» digital informasjon på samme måte som en håndskreven signatur benyttes til å undertegne et papirdokument. Disse teknikkene kan f.eks. være basert på biometriske kjennetegn som avlesning av iris-øye eller fingeravtrykk. Andre mulige teknikker kan være avlesning av en elektronisk penn eller digitale signaturer basert på elektroniske nøkler og sertifikater.

Den tekniske realiseringen av elektroniske signaturer som kalles *digital signatur* [2] er for tiden mest utbredt. Ved utforming av digitale signaturer bruker man kryptering [3] som bygger på avanserte matematiske funksjoner. Den som vil bruke en slik signatur får tildelt et elektronisk nøkkelpar, en offentlig og en privat nøkkel, og et sertifikat hvor undertegners identitet blir knyttet til den offentlige nøkkelen. Den offentlige nøkkelen kan distribueres til mottakerne av de signerte meldingene omtrent som man gjør med telefonnumre. Den private er strengt personlig, akkurat som koden til bankkortet. Det er altså kun en person som kan signere meldingen ved hjelp av den hemmelige private nøkkelen, mens det er mange som kan verifisere denne signaturen ved hjelp av den offentlige nøkkelen. Dette systemet krever at det etableres en infrastruktur for distribuering av de offentlige nøklene. Denne infrastrukturen omtales gjerne som Public Key Infrastructure (PKI) [4] .

Når innehaveren av nøkkelparet koder en melding med sin private nøkkel, vil meldingen bare kunne dekodes ved hjelp av hans offentlige nøkkel. Meldingen blir kodet slik at innholdet sikres mot forandring underveis. Den offentlige nøkkelen kan sendes mottaker sammen med den signerte meldingen. Mottaker bruker den offentlige nøkkelen til å stadfeste, eller verifisere, at det er innehaveren av den private nøkkelen som har sendt meldingen. Det vil også fremgå for mottaker dersom det er gjort den minste endring i meldingen etter signering. Signaturen er på denne måten knyttet til hele den signerte meldingen, og meldingen knyttes entydig til innehaveren av den private nøkkelen. Selve teksten i meldingen er ikke forvrengt (kryptert) og kan leses også av andre enn rette mottaker.

---

[2] Nærmere om elektronisk og digital signatur og bruken av dem, se St.meld. nr. 41 (1998-1999) om elektronisk handel og forretningsdrift (http://www.dep.no/nhd/norsk/publ/stmeld/) og rapporten «Digitale signaturer gir tillit til elektronisk kommunikasjon: forslag til tiltak for aksept og utbredelse» avgitt til Rådet for IT-sikkerhet 30. november 1998 (http://www.dep.no/nhd/norsk/publ/rapporter/)

[3] Kryptering er en konfidensialitetsbeskyttelse ved kryptografiske metoder som primært brukes til å skjule informasjonsinnholdet ved overføring over nettverk.

[4] Public Key Infrastructure (PKI) er en samling infrastrukturer (datasystemer, distribusjonssystemer og rutiner) som eksisterer med det formål å generere, tilbakekalle, sende ut og på andre måter håndtere offentlige nøkkelsertifikater.

Den offentlige nøkkelen kan ikke brukes til digital signering. Men i prinsippet er det mulig å kryptere selve teksten i meldingen ved å bruke den offentlige nøkkelen. Da kodes meldingen ved at avsender benytter seg av mottakers offentlige nøkkel. Mottaker vil imidlertid ikke med sikkerhet kunne stadfeste hvem meldingen er sendt fra. Dersom man skal oppnå dette er det mulig for avsender å også benytte seg av sin private nøkkel når han sender den krypterte meldingen. Mottakeren må da benytte sin private nøkkel for å dekryptere selve innholdet i meldingen, og han må også benytte avsenders offentlige nøkkel for å autentisere avsender.

Den private nøkkelen kan lagres på f.eks. et plastkort med en datachip (smartkort). Den vanlige tekniske løsningen for bruk av smartkort er at man, for å få tilgang til den private nøkkelen, må sette kortet inn i en kortleser og taste inn en personlig kode (på samme måte som ved bruk av bankkort i minibank). I stedet for kode kan man muligens i fremtiden benytte seg av fingeravtrykk eller andre biometriske kjennetegn.

3.2 Utstedelse av sertifikater - et marked med tillit

Lovforslaget regulerer et relativt nytt virksomhetsområde, der en tredjepart utsteder elektroniske sertifikater som kan identifisere en avsender av elektroniske dokumenter.

Sertifikatutstederen er en tredjepart i forholdet mellom undertegner og mottaker som skal stole på undertegnerens elektroniske signatur. Utstederens rolle kan sammenliknes med kredittkortselskapenes rolle i forholdet mellom forbruker og butikk, hvor kortselskapet garanterer overfor butikken at den vil få betalt. Sertifikatutstederen går god for at undertegner er den han utgir seg for å være i sertifikatet og innestår altså for at opplysningene i sertifikatet var korrekte på utstedelsestidspunktet. For at mottakeren skal kunne akseptere den elektroniske signaturen må han kunne stole på at undertegner er den han utgir seg for å være og at signaturen er gyldig. Dette krever at utstederen har sikre rutiner i forhold til å utstede og håndtere de elektroniske signaturene. For at systemet skal fungere må brukerne altså ha tillit til sertifikatutstederen. Utstedelse, bruken og tilbaketrekking av sertifikater er basert på en lang kjede av handlinger, der det hele tiden finnes en risiko for at noe blir feil. Denne loven skal sikre at også de svakeste leddene i denne kjeden blir sterke nok til at man skal kunne ha tillit til den elektroniske signaturen og sertifikatet.

Dette lovforslaget skal regulere rammebetingelsene for bruk av elektronisk signatur og tilhørende sertifikattjenester som oppfyller et nærmere fastlagt krav til sikkerhet. Lovforslaget inneholder regler om sertifikatutstedernes erstatningsansvar, generelle krav til utstederens virksomhet og regler om at det skal føres tilsyn med utstederne av disse kvalifiserte sertifikatene. Disse reglene skal legge til rette for sikker bruk av elektronisk signatur og dermed søke å påvirke markedet i en positiv retning. Det er lovgiverens intensjon at lovforslaget skal påvirke utbredelsen av elektroniske signaturer, slik at teknologien tas i bruk i større utstrekning så raskt som mulig. Se også kapittel 8.2.

3.3 Sertifikat

Når undertegner sender den signerte meldingen, kan hun sende med et elektronisk sertifikat som inneholder den offentlige nøkkelen og informasjon om undertegner. Mottakeren kan også få sertifikatet fra sertifikatutstederen. Sertifikatet knytter undertegnerens identitet sammen med hennes nøkkelpar. Samtidig vil altså mottaker, gjennom sertifikatet, motta den offentlige nøkkelen slik at mottaker kan verifisere undertegners signatur. Sertifikatets viktigste funksjon er å garantere koblingen mellom den private nøkkelen og undertegner.

Sertifikatutstederen signerer sertifikatet med sin egen private nøkkel. Påføringen av sertifikatutsteders signatur gjør at det ikke er mulig å endre opplysningene i sertifikatet uten at dette enkelt kan oppdages. Dersom innholdet i sertifikatet skal endres, må sertifikatet derfor trekkes tilbake og et nytt utstedes.

Sertifikatet kan inneholde mange opplysninger. Et sertifikat inneholder navn på undertegner eller eventuelt undertegners pseudonym, undertegners offentlige nøkkel, navn på sertifikatutstederen, gyldighetsperiode samt sertifikatutstederens signatur. I tillegg inneholder sertifikatet andre felt av mer teknisk karakter. Dessuten kan det også gis informasjon om eventuelle begrensninger i bruken av den elektroniske signaturen.

Det finnes flere standarder som angir hvilke opplysninger som må eller kan gis og hvordan de skal presenteres i sertifikatet, f.eks. den internasjonale standarden x.509. Lovforslaget oppstiller krav til hva et kvalifisert sertifikat skal inneholde, jf. kapittel 8.4, men er ikke direkte knyttet til en i dag eksisterende standard. I tillegg kan kravene utdypes i forskrift. Sertifikatet kan som nevnt spres på forskjellige måter, f.eks. gjennom elektroniske kataloger eller ved at de følger med den signerte meldingen.

Signaturen med tilhørende sertifikat har begrenset gyldighetstid, og denne gyldighetsdatoen skal fremgå av sertifikatet. Andre forhold kan også inntreffe slik at signaturen trekkes tilbake, f.eks. kan undertegner miste rådigheten over den private nøkkelen eller at opplysningene i sertifikatet blir foreldet. Ut fra innholdet i sertifikatet og utstederens tilbaketrekkingstjeneste kan et system altså avgjøre om et sertifikat er gyldig, f.eks. kan sertifikatet ha blitt sperret på samme måte som et kredittkort og dermed være ugyldig. Det er ikke slik at sertifikatet i seg selv vil angi om signaturen er gyldig eller om gyldighetstiden er utløpt. Gyldigheten av sertifikatet avgjøres gjennom en prosess som ofte benevnes som sertifikatvalidering (certificate validation).

Med katalog- og tilbaketrekkingstjeneste menes i dette lovforslaget den tjenesten at sertifikatutstederen skal sørge for nødvendige prosedyrer som gjør det mulig å trekke tilbake sertifikater eller gjøre dem ugyldige. Tilbaketrekkingen kan enten anmerkes i sertifikatet selv eller anmerkes i særskilte tilbaketrekkingslister som kan lastes ned av den enkelte bruker.

Undertegner, slik begrepet brukes i dette lovforslaget, er en fysisk person. Undertegneren kan imidlertid opptre på forskjellige måter, i eget navn eller under pseudonym, eller som representant for noen annen, typisk et selskap. For at et sertifikat skal oppfylle lovens krav til å være kvalifisert, må undertegnerens navn eller pseudonym fremgå av sertifikatet.

Det finnes også andre typer sertifikater. Et sertifikat som utstedes til undertegner i kraft av fullmakt eller stilling kalles et «rollesertifikat», da vil undertegners stilling fremgå av sertifikatet, f.eks. innkjøpssjef, men ikke navnet. Et rollesertifikat er dermed anonymt og kan brukes av flere som innehar samme rolle. Et sertifikat kan også utstedes til personer i kraft av deres yrke, f.eks. lege eller advokat. Et slikt sertifikat kalles for «profesjonssertifikat» og inneholder undertegners navn og stilling. Det kan være situasjoner hvor det er avgjørende å få informasjon om undertegners rolle, f.eks. at undertegner er revisor.

3.4 Sertifikatpolicy og sertifikatutstedelsespraksis

En *sertifikatpolicy* regulerer hvordan digitale sertifikater skal utstedes, behandles og hvem som har ansvaret for sikkerheten rundt dette. Sertifikatpolicyen fastsetter altså sikkerhetsnivået for tjenesten og derigjennom tillitsnivået. Eksempelvis kan det vises til Arbeids- og administrasjonsdepartementets arbeid med digitale signaturer i Forvaltningsnettsprosjektet, jf. kapittel 4.4. Her er det utarbeidet en konkret sertifikatpolicy. [5)]

En *sertifikatutstedelsespraksis* beskriver den praksisen sertifikatutstederen følger når sertifikater utstedes. «Praksis» skal her ikke forstås som den faktiske gjennomføringen, men som en beskrivelse av hvordan sertifikatutstederen har organisert seg og hvordan den skal oppnå det tillitsnivået som er satt opp i sertifikatpolicyen.

Sertifikatutstederen skal kontrollere identiteten til de personer som det skal utstedes sertifikater til. Dessuten vil utsteder eventuelt også kontrollere andre særlige forhold, f.eks. ansettelsesforhold, fullmakter, yrke mv. Hvordan denne kontrollen foretas vil avhenge av den sertifikatpolicy som benyttes, hvordan den aktuelle sertifikatutstederen er organisert og til hvilke formål sertifikatet skal brukes. Eksempelvis vil det være mulig å benytte en registreringsenhet, f.eks. postkontoret, slik at sertifikatutsteder setter ut denne tjenesten til et annet organ.

Sertifikatutstedere kan i visse tilfeller overlate denne kontrollen til kjøper av signaturtjenesten. For et konsern som anskaffer signaturer til sine ansatte, kan det være praktisk og hensiktsmessig å håndtere kontrollen av undertegner selv. Utstederen kan da oppnevne noen i konsernet som sikrer koblingen mellom person og opplysningene i sertifikatet.

3.5 Funksjoner som må bli særlig ivaretatt ved bruk av elektronisk signatur

Bruk av elektronisk signatur fører til flere sikkerhetsmessige spørsmål som er helt ukjente for papirbasert kommunikasjon. En papirbasert signatur kan granskes nøye fordi den er festet til et fysisk objekt, mens en elektronisk signatur kun tilbyr den informasjonen som er til stede i selve representasjonen (dvs. den informasjonen brukeren får opp på dataskjermen). Kompleksiteten

[5)] http://forvaltningsnett.dep.no/

rundt det å oppdage og å bevise at et elektronisk signert dokument er forfalsket er helt annerledes.

Den tekniske tilretteleggelsen hos brukerne, undertegner/sender og mottaker, må være sikret slik at det som sendes ut på nettet er nøyaktig det som ble signert og som vises for mottaker. Dette lovforslaget retter seg imidlertid i hovedsak mot sertifikatutstederne og de tjenestene de tilbyr, herunder for å sikre infrastrukturen for at det som sendes signert ut på nettet skal kunne mottas i samme form.

Den tekniske utviklingen på området går raskt og en elektronisk signatur som er sikker i dag, er neppe like sikker mot forfalskninger om noen år. Det bør overveies hvorvidt dokumenter, hvor det er behov for å identifisere undertegneren på en sikker måte også etter at sertifikatets gyldighetstid har utløpt, egner seg for elektronisk kommunikasjon, f.eks. avtaler som gjelder over lang tid eller testament. Uansett bør man i slike tilfeller kunne dokumentere hvordan identifiseringen har skjedd. NTNU uttaler at man ikke bør bruke elektroniske signaturer på dokumenter som skal være gyldige i mer enn ti år, på grunn av risikoen for at tilbakedaterte dokumenter kan signeres og dateres med et tidspunkt da signaturen var gyldig, dersom noen skulle klare å urettmessig tilegne seg signaturfremstillingsdataene.

Ved innføring av elektronisk kommunikasjon med elektronisk signatur må en også vurdere hvordan en vil lagre elektroniske dokumenter over tid. Et utgangspunkt i offentlig forvaltning vil være arkivloven av 4. desember 1992 nr. 126 med de nye forskriftene som trådte i kraft den 1. januar 1999.

Et elektronisk dokument har en begrenset levetid i forhold til et papirbasert dokument. Man kan få problemer med å lese elektroniske dokumenter etter 10-15 år fordi formatet dokumentet er generert i kanskje ikke lenger er i bruk, dataformatet er ikke lenger kjent eller maskin- og programvare ikke lenger finnes. Elektroniske dokumenter må derfor konverteres til nye formater for å forbli lesbare over tid. Under denne prosessen mister imidlertid dokumentet sin unikhet og bare innholdet består. Når dokumentet har en digital signatur, oppstår et problem ved at signaturen ikke lenger lar seg verifisere på vanlig måte etter at dokumentet er konvertert.

Det er imidlertid også mulig at man ved arkivering av et elektroniske dokument med digitale signaturer bevarer sporene etter foretatte verifiseringer av digitale signaturer. Denne løsningen med å bevare spor i ikke-forgjengelig teknisk form, kan kombineres med arkivering av dokumenter med påført signatur.

4 Arbeidet i forskjellige utvalg og lignende som berører bruken av elektronisk signatur

4.1 Rådet for IT-sikkerhet (RITS)

Rådet for IT-sikkerhet (RITS) [6] ble etablert i mars 1996 og la frem tre rapporter: sertifisering av IT-sikkerhet, kryptopolitikk og digitale signaturer. I 1998 ble det avgitt en rapport i regi av RITS med anbefalinger om hvilke tiltak sentrale myndigheter burde sette i verk for å legge til rette for bruk av digitale signaturer og tiltrodde tredjepartstjenester. Rapporten «Digitale signaturer gir tillit til elektronisk kommunikasjon - Forslag til tiltak for aksept og utbredelse» [7] kan sammenfattes i tre hoveddeler:

I del I anbefales rettslig likestilling av elektroniske dokumenter og elektroniske signaturer med de papirbaserte. Det foreslås at det utvikles regler som sikrer at elektroniske dokumenter og signaturer anerkjennes som bevis på linje med papirdokumenter, og at vilkårene for slik beviskraft klarlegges. Videre anbefales det at det iverksettes et kartleggingsarbeid for å bringe på det rene når norsk lovgivning krever bruk av papir/underskrift, slik at nødvendige endringer kan vurderes og deretter gjennomføres.

I del II anbefales det at det legges til rette for etablering og drift av sertifikattjeneste m.v. og videre utredning av myndighetsroller.

I del III anbefales tiltak for å få konkret erfaring og kunnskap vedrørende bruk av elektroniske signaturer. Her fremheves bl.a. betydningen av å få erfaring fra pilotprosjekter.

4.2 Utredningen «Elektroniske signaturer - Myndighetsroller og regulering av tilbyder av sertifikattjenester»

Under behandlingen av rapporten om digitale signaturer uttalte RITS at det var viktig å komme i gang med å klarlegge rammer og modeller for sertifikatutstedernes virksomhet i Norge. Rådet anbefalte derfor at spørsmål vedrørende myndighetsroller, finansiering av autentiseringsvirksomhet og godkjenningsordning og krav til utstedere burde utredes nærmere. Som ledd i oppfølgingen på dette punktet og som en start på arbeidet med lovregulering på dette området, nedsatte Nærings- og handelsdepartementet et utvalg som avga en rapport den 28. januar 2000. [8] I rapporten anbefaler utvalget bl.a. en form for tilsyn med sertifikatutstedere.

Hovedkonklusjonene fra utredningen er følgende:

---

[6] Rådet for IT-sikkerhet er nå videreført i Forum for IT-sikkerhet som er bredere sammensatt med representanter også fra næringslivet og det akademiske miljø. Forumet skal identifisere viktige saker og gi grunnlag for Nærings- og handelsdepartementets prioriteringer, se http://odin.dep.no/nhd/norsk/dep/utvalg/. Forumet ledes av professor Jon Bing ved Universitetet i Oslo.

[7] http://www.dep.no/nhd/norsk/publ/rapporter/

[8] Hele rapporten kan leses på Odin, http://www.dep.no/nhd/norsk/publ/rapporter/

- Det utpekes en offentlig tilsynsmyndighet som skal drive tilsyn med utstedere av kvalifiserte sertifikater. Tilsynsmyndigheten legges til Post- og teletilsynet.
- Det etableres en registreringsordning for utstedere av kvalifiserte sertifikater.
- Det tas ikke initiativ fra myndighetenes side til en ordning for en total akkreditert sertifisering av sertifikatutstedere nå. De eksisterende ordningene for sertifisering av IT-sikkerhet i Norge, sammen med muligheten for IT-revisjoner av utsteder, gir et tilstrekkelig grunnlag for å vurdere tillitsnivået til en utsteder og de innretninger utstederen anvender i sin virksomhet.
- Det legges ikke opp til noen regulering av samarbeid og/eller gjensidig anerkjennelse mellom forskjellige sertifikatutstedere fra myndighetenes side, dette gjøres best gjennom avtaler. Utvalget er positivt til at frivillige godkjenningsordninger blir etablert i markedet, men myndighetene bør ikke ta noe initiativ til å etablere slike.

4.3 Kartlegging av bestemmelser i lover, forskrifter og instrukser som kan hindre elektronisk kommunikasjon (kartleggingsprosjektet)

Det er regjeringens mål at elektronisk kommunikasjon og bruk av nett som infrastruktur for samhandling skal bli like akseptert og ha samme juridiske holdbarhet som tradisjonell skriftlig kommunikasjon og dokumentasjon.

På en del områder hersker det i dag usikkerhet om bruk av elektronisk kommunikasjon oppfyller kravene i den aktuelle loven, forskriften eller instruksen. Det vil være en konkurransefordel for blant annet norsk næringsliv dersom denne usikkerheten fjernes og kommunikasjon vil kunne skje elektronisk. Regjeringens mål er også i tråd med den ministererklæring om elektronisk signatur som ble vedtatt ved OECDs konferanse i Ottawa i 1998. Der ble det oppnådd enighet om at landene skal gjennomgå sin lovgivning og endre den for å fjerne hindringer for elektronisk kommunikasjon og samhandling.

Våren 1999 besluttet Regjeringen at hvert departement skal gjennomgå lover, forskrifter og instrukser på sitt område for å identifisere bestemmelser som er til hinder for eller ikke legger til rette for elektronisk kommunikasjon, og endre disse i tråd med Regjeringens målsetting. Dette kartleggingsprosjektet er et samarbeid mellom Justisdepartementet, Arbeids- og administrasjonsdepartementet og Nærings- og handelsdepartementet.

I juni 2000 ble en prosjektrapport [9)] lagt frem basert på innrapportert materiale fra departementene. Rapporten er systematisert i forhold til forskjellige typer begrep som brukes i lover, forskrifter og instrukser. Blant de mest sentrale begrepene er krav om «skriftlighet», «underskrift», «dokument» og «original». I rapporten drøftes begrunnelsen for de forskjellige kravene. Man vurderer hvilke funksjoner som f.eks. skriftlighet kan ha, og hvilke hensyn som må ivaretas for at det skal være mulig å åpne opp for elektronisk kommunikasjon. Denne fremgangsmåten er bl.a. i tråd med UNCITRALs [10)] arbeid med å

[9)] Rapporten er lagt ut på http://odin.dep.no/nhd/norsk/publ/rapporter/

opprette en modellov om elektronisk kommunikasjon. Denne metoden er blitt kalt for «funksjonell ekvivalens».

4.4 Forvaltningsnettprosjektet

Kommunenes sentralforbund og Arbeids- og administrasjonsdepartementet har etablert et langsiktig samarbeid på tele- og dataområdet, forankret i kommunesektorens og statens IT-strategier. Forvaltningsnettsamarbeidet er ett av flere tiltak i samarbeidet mellom Kommunesektoren og Staten på IT-området (KOSTIT). Målet er å fremme enkel, sikker og kostnadseffektiv elektronisk informasjonsutveksling innad i offentlig sektor og utad mot andre brukere [11)].

Prosjektet har etablert rammeavtaler for offentlig forvaltning for anskaffelse av sertifikattjenester, programvare og utstyr for digital signatur og meldingskryptering, smartkort og kortlesere. De har utviklet en sertifikatpolicy som skal brukes ved utstedelse av sertifikater. Videre har de gjennom rammeavtalen sørget for kryssertifisering mellom sertifikatutstederne som deltar i samarbeidet. Disse har inngått en separat avtale seg i mellom.

4.5 Utvalg for å utrede bruk av digital signatur i offentlig forvaltning

Etter anbefaling fra Arbeids- og administrasjonsdepartementet ble «Utvalg for å utrede bruk av digital signatur i offentlig forvaltning» oppnevnt av regjeringen den 4. februar 2000. Utvalget skal gi anbefalinger vedrørende etablering av en infrastruktur for å muliggjøre bruk av elektronisk signatur og kryptering i offentlig sektor. Dette omtales gjerne som PKI (Public Key Infrastructure) [12)].

Det fremheves i den forbindelse at digitale signaturer har stor betydning for realisering av elektroniske tjenester til brukere, elektronisk saksbehandling og datautveksling i forvaltningen, samt elektronisk handel ved offentlige innkjøp. Flere land har utarbeidet, eller er i ferd med å utarbeide, retningslinjer eller en policy for offentlig sektor. Blant de spørsmål som utvalget skal avklare er: krav til digitale sertifikater som forvaltningen vil benytte selv eller stille krav om til andre, behov for felles sertifikatpolicy i forvaltningen og strategi for bruk av sertifikatutstedere. Utvalget skal avgi sin innstilling den 31. desember 2000.

4.6 Nordisk samarbeid

Nærings- og handelsdepartementet har deltatt i et uformelt samarbeid mellom de relevante myndigheter i Danmark, Sverige, Finland og Island for å utveksle erfaringer og i størst mulig grad komme frem til et felles rettslig rammeverk for bruk av elektronisk signatur. En likest mulig lovgivning innen Norden kan fjerne unødvendige hindringer for elektronisk kommunikasjon og elektronisk handel på tvers av landegrensene. Det er tatt initiativ for å videreføre det nor-

10) United Nations Commission on International Trade law.

11) Mer informasjon vedrørende forvaltningsnettssamarbeidet finnes på http://forvaltningsnett.dep.no/.

12) Om PKI, se kapittel 3.1.

diske samarbeidet mellom tilsynsmyndighetene ved utformingen av forskrifter og valg av standarder.

I Danmark og Sverige har lovgivningsarbeidet kommet lenger enn i Norge, deres lovforslag er allerede vedtatt, men har ikke trådt i kraft. Lovene er langt på vei like. Den største forskjellen er valg av tilsynsmodell. I Danmark har de valgt en «IT revisjons-modell», se kapittel 6.2, mens den svenske modellen er tilnærmet identisk med det norske lovforslaget. Finland og Island forventes å legge frem lovforslag innen kort tid. Også disse ser ut til å bli langt på vei like de øvrige nordiske forslagene.

5 EU-direktivet om elektronisk signatur

EU-direktivet legger opp til å være teknologinøytralt, men omhandler i realiteten digitale signaturer som anvendes ved hjelp av offentlig nøkkel infrastruktur, PKI [13] . Dette er en følge av det faktum at det per i dag synes som om løsninger basert på digitale signaturer og offentlig nøkkel infrastruktur, med tilhørende tjenester fra en sertifikatutsteder, er mest aktuelt. En mulig trend er at andre (biometriske) løsninger i større grad vil bli brukt i kombinasjon med digital signatur.

Direktivet omhandler flere områder:

Markedsadgang: Landene må ikke stille krav om at sertifikatutstedere skal godkjennes forut for oppstart av virksomheten, men kan introdusere frivillige akkrediteringsordninger, med sikte på å etablere sertifikattjenester på «avansert nivå». Landene skal også sikre at det opprettes et system for å øve tilsyn med sertifikatutstedere som utsteder kvalifiserte sertifikater. Landene kan dessuten stille tilleggskrav til elektroniske signaturer i offentlig sektor.

Indre marked: Sertifikatutstedere etablert i EØS-området skal kunne tilby sine tjenester i et annet medlemsland. Landene skal også sikre at elektroniske signaturprodukter som er i samsvar med direktivet, kan sirkulere fritt i det indre markedet.

Rettsvirkning: Landene skal sikre at en kvalifisert elektronisk signatur [14] anerkjennes på linje med håndskrevne signaturer og kan legges frem som bevis i retten på samme måte som for håndskrevne signaturer, så fremt lover og forskrifter åpner for at signeringen kan skje elektronisk.

Landene skal dessuten sikre at elektronisk signatur på et annet nivå ikke fratas rettsvirkning bare fordi signaturen er i elektronisk form, ikke er basert på et kvalifisert sertifikat utstedt av en akkreditert tjenesteleverandør, eller ikke er laget av et sikkert signaturfremstillingssystem.

Ansvar: For å skape tillit hos de som baserer seg på sertifikatene har direktivet regler om erstatningsansvar for sertifikatutstedere. Landene skal sikre at utstedere av kvalifiserte sertifikater er ansvarlige for at informasjon angitt i sertifikatet er korrekt, i overensstemmelse med direktivets krav, og at personen som er identifisert i sertifikatet var i besittelse av korrekt signaturfremstillingsdata på det tidspunktet da sertifikatet ble utstedt. Imidlertid er sertifikatutstederen ikke ansvarlig dersom hun kan vise at hun ikke har vært uaktsom. Sertifikatutstederen er heller ikke ansvarlig når en kvalifisert signatur blir brukt utover de beløps- eller områdebegrensninger som er tydelig angitt i sertifikatet.

Internasjonale forhold: Landene skal sikre at kvalifiserte sertifikater utstedt i et tredjeland anerkjennes som rettslig likeverdige med kvalifiserte sertifikater utstedt innen EU, dersom sertifikatutstederen er akkreditert i et medlemsland. Likedan skal kvalifiserte sertifikater anerkjennes dersom en utsteder i et medlemsland som fyller kravene som er angitt i vedlegg II til

---

[13] PKI - Public Key Infrastructure - offentlig nøkkel infrastruktur, se kapittel 3.1.

[14] En kvalifisert signatur er en avansert elektronisk signatur som er basert på et kvalifisert sertifikat og som er fremstilt av et sikkert signaturfremstillingssystem.

direktivet, garanterer for sertifikatet i samme utstrekning som sitt eget, eller dersom utstederen er anerkjent under et regime etablert ved bi- eller multilateral avtale.

Personvern: Landene skal sikre at virksomheten til sertifikatutsteder er i overensstemmelse med personverndirektivet [15] . Sertifikatutstederens innsamling av persondata skal begrenses til det som er nødvendig for sertifikatutstedelse og skal skje direkte fra datasubjektet. Slike data kan ikke brukes til andre formål uten samtykke fra datasubjektet. Dersom underskriveren ønsker det, skal pseudonym nyttes i sertifikatet i stedet for underskriverens navn.

Dersom det er krav til, iht. nevnte direktiv eller nasjonal rett, å sende informasjon vedrørende innehaverens identitet til en offentlig myndighet (i) på grunn av etterforskning av straffbar handling som relateres til bruk av elektronisk signatur med pseudonymsertifikat eller (ii) som er påkrevet for å kunne fremme krav relatert til bruk av elektronisk signatur med pseudonymsertifikat, skal slik overføring logges og «datasubjektet» skal bli informert.

Komité: Det skal ifølge artikkel 9 og 10 i direktivet etableres en komite til å bistå Europakommisjonen med å gjennomføre direktivet. Komiteen skal bl.a. avklare uklarheter vedrørende krav som stilles i direktivets vedlegg og krav vedrørende sikre signaturfremstillingssystem. EFTA-land deltar fullt ut i komiteen med unntak av stemmerett.

*Underrettelse:*Landene skal informere Europakommisjonen om nasjonale akkrediteringsordninger, navn og adresse på nasjonale tilsynsorganer og organ som godkjenner sikre signaturfremstillingssystem og akkrediterte tjenesteleverandører.

Evaluering av direktivet: Direktivet og praktiseringen av det skal gjennomgås, blant annet med henblikk på om direktivets rekkevidde skal endres i lys av utviklingen. Kommisjonen skal legge frem en rapport for Europaparlamentet og Rådet senest tre og et halvt år etter at direktivet har trådt i kraft.

Implementering: Implementering av direktivet skal skje innen 18 måneder etter at det blitt publisert i EF-Tidende [16] . Den samme tidsfristen gjelder for EØS-landene.

---

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[16] EU-direktivet ble publisert i De Europeiske Fellesskaps Tidende (EF-Tidende) den 19. januar 2000.

6 Lovgivningen i de andre nordiske land

6.1 Sverige

Den svenske regjeringen fremsatte forslag til «lag om kvalificerade elektroniska signaturer m.m.» for den svenske riksdagen den 18. mai 2000, Prop. 1999/2000:117. Det tas sikte på at loven skal tre i kraft den 1. januar 2001.

I loven utpekes Post- och telestyrelsen som tilsynsmyndighet. Det legges opp til at tilbydere skal sende inn en registreringsmelding til tilsynet før de kan utstede kvalifiserte sertifikater. Tilsynet skal på begjæring få alle de opplysninger og dokumenter de trenger for å kunne utføre tilsynet.

Sertifikatutsteder omtales i den svenske loven som «certifikatutfärdare» og defineres som den som utsteder sertifikater eller som garanterer at noen annens sertifikat oppfyller visse krav.

I loven innføres en definisjon av kvalifiserte elektroniske signaturer og bestemmelsen om disse kvalifiserte signaturenes rettsvirkninger er tilnærmet identisk med den norske.

6.2 Danmark

Allerede i 1998 ble det fremmet et lovforslag om regulering av sertifikatutstedere i Danmark. Forslaget innebar bl.a. at alle typer elektroniske signaturer skulle gis rettsvirkninger. En konsekvens av dette forslaget ville være at offentlige myndigheter måtte investere i nye og dyre systemer for å kunne håndtere alle elektroniske signaturer. På denne bakgrunn, og også fordi EU hadde begynt å arbeide med et direktiv om elektroniske signaturer, ble lovforslaget trukket tilbake.

Det er nå utarbeidet en ny lov som ble fremsatt for Folketinget av den danske forskningsministeren den 22. mars 2000, lovforslag nr L 229. Denne loven vil tre i kraft den 1. oktober 2000.

Loven regulerer sertifikatutstedere, som omtales som «nøglecenter» og som defineres som en fysisk eller juridisk person som utsteder sertifikater.

I tidligere lovforslag ble ikke direktivets artikkel 5 vedrørende elektroniske signaturers retts- og bevisvirkning regulert. Det ble i stedet nedsatt et utvalg som skulle foreslå hvordan artikkel 5 skulle implementeres i dansk rett. Utvalget ser også nærmere på behovet for å lovregulere i hvilket omfang elektroniske meldinger skal kunne brukes på områder hvor det oppstilles formkrav og rettsvirkningene mellom avsender og mottaker i visse nærmere avgrensede situasjoner. Utvalgets arbeid ledes av Justisministeriet og er ennå ikke avsluttet. Bestemmelsen om rettsvirkninger er nå innarbeidet i loven om elektroniske signaturer. Bestemmelsen er tilnærmet lik tilsvarende bestemmelse i det norske og svenske lovforslaget.

Tilsynsmyndighet skal i henhold til loven være Telestyrelsen. Før en sertifikatutsteder kan markedsføre eller utstede kvalifiserte sertifikater, skal utstederen sende inn en registreringsmelding til tilsynet.

I Danmark har de valgt en «IT revisjons-modell» som tilsynsmodell. Sertifikatutstederne skal ved registrering, og deretter årlig, levere en rapport til tilsynet med en beskrivelse av virksomheten og de systemer som anvendes samt en erklæring fra ledelsen og valgte IT-revisor.

6.3 Finland

I desember 1999 ble loven om elektronisk dokumenthåndtering innen forvaltningen og lov om borgerkort vedtatt. I Finland arbeides det nå med gjennomføringen av EU-direktivet i finsk rett i et forslag til en ny lov om elektronisk signatur. I henhold til dette lovforslaget vil tilsynsmyndighet bli det finske Teletilsynet. Det er allerede konstatert at den nye loven vil erstatte deler av de bestemmelser som nå finnes i loven om elektronisk dokumenthåndtering.

6.4 Island

På Island arbeides det også for tiden med et forslag til en lov om elektronisk signatur. Det ser ut til at dette forslaget vil ligge nært opp til det norske forslaget. Forslaget vil bli fremsatt for det Islandske parlamentet til høsten. Tilsynsmyndighet vil bli Löggildingarstofa som ligger under Næringsdepartemetet.

7 Reglenes virkeområd

7.1 Geografisk virkeområde

I høringsnotatet foreslås det at loven skal gjelde for sertifikatutstedere som er etablert i Norge. Utenfor reguleringen faller i utgangspunktet utstedere som ikke er etablert i Norge, selv om sertifikatene utstedes for bruk i Norge. Det vil si at reglene om tilsyn og erstatningsreglene i dette lovforslaget gjelder sertifikatutstedere etablert i Norge. Lovforslaget bygger på at kvalifiserte sertifikater fra utstedere etablert innen EØS-området gis rettslig anerkjennelse på lik linje med tilsvarende sertifikater fra utstedere etablert i Norge. Videre har forslaget regler om rettslig anerkjennelse av kvalifiserte sertifikater fra utstedere etablert utenfor EØS-området, se kapittel 10.

Med «etablert» menes at det faktisk utøves aktiviteter innenfor en forholdsvis fast struktur. Strukturens rettslige status, f.eks. hvilken sammenslutningsform som er nyttet, er ikke avgjørende. Avgjørende er om sertifikatutstederen har tilstrekkelig tilknytning til Norge til å anses som etablert her. Dersom et utenlandsk selskap har et datterselskap i Norge som utsteder sertifikater her, er tilknytningskravet åpenbart oppfylt. Det samme gjelder utenlandske selskapers filialer i Norge. Den nærmere grensedragningen må finne sted i praksis.

7.2 Saklig virkeområde

7.2.1 Høringsnotatet

Høringsnotatet oppstilte et forslag om at loven kun skal regulere dem som utsteder sertifikater til allmennheten. Forslaget ville således ikke få direkte anvendelse på elektronisk signatur som bare brukes innenfor systemer som er basert på frivillige avtaler mellom et begrenset antall deltagere, omtalt som «lukkede nett». [17] Grensene for hva som skal regnes for lukkede nett er ikke helt klar. Eksempler kan være signaturer som brukes mellom ansatte innen en bedrift eller som brukes innen en begrenset medlemsmasse. Den nærmere grensedragningen vedrørende lukkede systemer ville måtte finne sted i praksis. Avgjørende for vurderingen ville altså være at signaturen kun skulle brukes mellom et begrenset antall deltakere hvor deltakelsen bygget på en frivillig privatrettslig avtale.

Direktivet legger ikke hindringer for at alle eller deler av bestemmelsene også kan gjelde for lukkede nett. Det følger av direktivets fortale at elektroniske signaturer som brukes innen lukkede nett ikke bør nektes rettslig gyldighet. Det er ikke behov for å regulere at elektroniske signaturer - i åpne eller lukkede nett - ikke skal fratas rettsvirkning eller gyldighet som bevis bare på

[17] I punktnr. 16 i direktivets fortale står følgende: «... a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants...»

grunnlag av at signaturen er i elektronisk form. Dette er allerede i samsvar med gjeldende rett (jf. kapittel 8.10.2).

Høringsnotatet hadde som utgangspunkt at det for dagens marked ikke er behov for å regulere bruken av elektronisk signatur i lukkede nett. Partene innen lukkede nett skal fritt kunne avtale på hvilke betingelser de vil akseptere elektroniske signaturer. Dette betyr bl.a. at bestemmelsene om erstatning og rettsvirkning i loven ikke vil få direkte anvendelse på elektroniske signaturer brukt innenfor et lukket nett. På den annen side må partene fritt kunne avtale at lovens regler skal kunne komme til anvendelse.

Direktivet får ikke innvirkning på nasjonal retts bestemmelser om formkrav, for eksempel krav til håndskreven underskrift, krav til bestemte dokumenttyper, krav til at avtaler skal inngås skriftlig mv. I fortalen til direktivet står bl.a. at direktivet ikke søker å harmonisere nasjonale regler vedrørende kontraktsrett, herunder særlig opprettelse og gjennomføring av avtaler. Videre står det at bestemmelsene i direktivet om rettsvirkninger ved bruk av elektronisk signatur ikke skal påvirke nasjonalt formkrav for at en avtale skal være inngått. Dette betyr at hver stat har mulighet til å hindre bruk av elektronisk signatur innenfor de områder den ikke finner slik bruk hensiktsmessig. Imidlertid, dersom nasjonalt regelverk åpner for elektronisk kommunikasjon, vil bestemmelsene i direktivet gjelde fullt ut. Dette prinsippet er blitt overført til lovforslaget, jf. lovforslag § 6. Samtidig skal det nevnes at det pågår et prosjekt i Norge der man ønsker å fjerne unødige hindringer for elektronisk kommunikasjon, jf. kapittel 4.3.

Selv om forslaget i høringsnotatet i utgangspunktet omfattet alle som utsteder sertifikater til allmennheten, ville de aller fleste bestemmelsene i lovutkastet kun omfatte utstedere av kvalifiserte sertifikater. Loven ville da i realiteten regulere utstedere av kvalifiserte sertifikater med to unntak: bestemmelsen i § 6 første ledd siste punktum om rettsvirkning og bestemmelsen i § 7 om innsamling og bruk av personopplysninger som gjelder *alle*sertifikatutstedere. Disse to bestemmelsene gjelder alle typer av sertifikater og alle sertifikatutstedere.

7.2.2 Høringsinstansenes syn

Telenor uttaler at de ideelt sett skulle ønske et klarere definert saklig virkeområde for loven, men at de har forståelse for at grensedragningen er vanskelig og derfor er enige i at den bør skje gjennom praktisering av regelverket.

NHO støtter forslaget i høringsnotatet om at loven kun skal gjelde for elektroniske signaturer som benyttes i åpne systemer. De påpeker at bruk av elektronisk signatur i lukkede systemer bør «system-eierne» selv ha adgang til å regulere gjennom eget avtaleverk.

Andre høringsinstanser er mer skeptisk til skillet mellom åpne og lukkede nett. *Næringslivets Sikkerhetsorganisasjon (NSO)* er i tvil om loven bør skille mellom lukkede/åpne nett da brukere erfaringsmessig har vanskelig for å skille disse, og fordi det vil eksistere glidende overganger.

Arbeids- og administrasjonsdepartementet mener at skillet er noe underlig, og at kvalifiserte sertifikater som sådanne bør kunne utstedes også til andre enn publikum. Videre forslår de at det innføres en klar virkeparagraf i loven

slik at det tydelig fremgår at kun §§ 6 og 7 gjelder utstedere av andre sertifikater enn de kvalifiserte.

Også *Norsk EDIPRO* påpeker at det lett kan oppstå tolkningstvil i forhold til hva det ligger i å utstede sertifikater til allmennheten i motsetning til å tilby sertifikater til en definert gruppe.

Norsk EDIPRO er av den oppfatning at loven i utgangspunktet burde få generell anvendelse, men at man burde gi anledning til å fravike loven ved avtale dersom sertifikatene kun skal tilbys til en klart definert brukergruppe.

*FNH*og *Sparebankforeningen* påpeker at hvis f.eks. en bank tilbyr sertifikater til alle sine kunder for bruk til autentisering mellom kunde og bank, taler hensynet til kundene for å la sertifikatutstedelsen omfattes av loven og at lukkede systemer og begrepet «allmenheten» i lovutkastet bør tolkes i forhold til dette.

Statskonsult savner at det sies noe om *hva loven ikke regulerer* i lovens bestemmelse om virkeområde.

Justisdepartementet foreslår et tillegg i lovteksten slik at lovens virkeområde også omfatter brukere av sertifikattjenester.

7.2.3 Departementets vurdering

Departementet har, på bakgrunn av høringsuttalelsene, nærmere vurdert behovet for å utvide lovens virkeområde til også å gjelde innenfor systemer som er basert på frivillige avtaler mellom et begrenset antall deltagere, såkalte lukkede systemer.

Lovens formål er å legge til rette for en sikker bruk av elektronisk signatur og bør således i størst mulig utstrekning legge til rette for at kvalifiserte elektroniske signaturer blir tatt i bruk. For å sikre forutberegnelighet ved bruk av elektroniske signaturer er det ønskelig at flest mulig signaturer oppfyller kravene til kvalifiserte signaturer og dermed omfattes av denne lovreguleringen. Videre vil det sikre bruken av signaturer at de omfattes av det tilsynsregimet som loven oppstiller. Grensegangen mellom lukkede og åpne nett synes dessuten å være noe uklar, og det vil ta tid før den nærmere grensegangen er avklart gjennom praksis. På denne bakgrunn har departementet kommet til at loven bør åpne opp for at alle sertifikatutstedere som ønsker å falle inn under denne lovreguleringen omfattes.

Lovforslaget åpner etter dette for at sertifikatutstedere som utsteder kvalifiserte sertifikater innen lukkede systemer skal omfattes av loven. Lovens virkeområde blir dermed alle utstedere av kvalifiserte sertifikater etablert i Norge.

For å falle inn under loven må sertifikatutsteder kalle sertifikatene for kvalifiserte og registrere seg hos tilsynet etter lovforslaget § 18. Sertifikatene som utstedes må oppfylle alle krav loven oppstiller til kvalifiserte sertifikater. Alle bestemmelsene i loven vil altså komme til anvendelse etter at sertifikatutsteder har registrert seg hos tilsynet.

Det vil altså være opp til den enkelte sertifikatutsteder hvorvidt han/hun vil utstede kvalifiserte sertifikater og dermed falle inn under denne lovreguleringen og det tilsynsregimet loven oppstiller, uavhengig av om sertifikatutstederen opererer innen åpne eller lukkede systemer. Enhver tilbyder av kvalifi-

serte sertifikater må registrere seg hos tilsynet for å kunne utstede kvalifiserte sertifikater.

Departementet går videre inn for at bestemmelsen om lovens virkeområde endres slik at det tydelig fremgår at § 6 annet punktum og § 7 gjelder alle signaturer med tilhørende sertifikater, og ikke bare de kvalifiserte.

8 Lovforslagets hovedinnhold

8.1 Definisjoner

8.1.1 Høringsnotatet

Definisjonene som brukes i loven er i hovedsak en oversettelse og bearbeidelse av definisjonene i direktivet og er for dagens marked nye. Målet er å bruke definisjoner som beskriver et produkt, en virksomhet m.v. i forhold til en teknologinøytral elektronisk signatur. Sannsynligvis hadde loven blitt enklere å forstå dersom man hadde benyttet seg av «privat nøkkel» i stedet for «signaturfremstillingssdata», «offentlig nøkkel» i stedet for «signaturverifikasjonsdata» eller «digital signatur» i stedet for «avansert elektronisk signatur» (jf. kapittel 3.1). Problemet er imidlertid at disse definisjonene ikke er teknologinøytrale, men kun relaterer seg til digital signatur. Ved å bruke teknologinøytrale definisjoner så langt det er mulig, håper man at det ikke skal bli nødvendig å måtte endre definisjonen når ny teknologi kommer på markedet. Dessuten er det usikkert om direktivet vil være fullt ut implementert, dersom loven kun regulerer digitale signaturer.

I høringsnotatet foreslås det i tillegg til direktivets definisjoner i artikkel 2, en definisjon av kvalifisert elektronisk signatur og en definisjon av elektronisk dokument. Definisjonen av kvalifisert elektronisk signatur er lagt til av hensyn til at bestemmelsen om elektroniske signaturers rettsvirkninger i § 6 (i tidligere utkast § 5) skal bli mer leservennlig. Alternativet ville være å la innholdet av definisjonen stå i bestemmelsen om rettsvirkninger. Definisjonen av elektronisk dokument ble lagt til av pedagogiske hensyn og viser til hva man signerer.

Definisjonen av elektronisk signaturprodukt blir ikke brukt i lovforslaget og er av den grunn utelatt fra definisjonslisten i forhold til direktivets definisjoner. Definisjonen av frivillig akkreditering er også utelatt i forhold til direktivets definisjonsliste da lovforslaget ikke regulerer noe frivillig akkrediteringssystem.

En av forslagets mest sentrale definisjoner, «tilbyder av sertifikattjenester» (nå endret til «sertifikatutsteder»), omtales nærmere under kapittel 8.2, mens «kvalifisert elektronisk sertifikat», som defineres i en egen paragraf, omtales under kapittel 8.4.

8.1.2 Høringsinstansenes syn

Mange høringsinstanser har kommet med innspill til utformingen av definisjonene.

Justisdepartementet kommer med innspill til endring av signaturfremstillingsprodukt til signaturfremstillingssystem. Flere av høringsinstansene har uttrykt at definisjonen av elektronisk dokument er uklar, både i forhold til hva den omfatter og i forhold til ulike dokumentbegreper i annen lovgivning. Øvrige kommentarer gjelder i hovedsak de tre definisjonene av signaturer.

Statskonsult uttaler at det kan være bedre å fokusere direkte på «data» eller «opplysninger» eller tilsvarende begrep, som ikke oppfattes å være mest aktuelt i papirverdenen, i stedet for dokument i definisjonen av elektronisk signatur. Statskonsult slutter seg ellers til innføringen av «kvalifisert elektronisk signatur» som en ny definisjon, og som etter deres mening har en nyttig funksjon.

Advokatforeningen og *eforum* uttaler at det bør vurderes om uttrykket «signatur» skal erstattes av «underskrift» da signatur har et bestemt meningsinnhold i andre sammenhenger som i selskapsretten der det med signatur siktes til rett til å tegne for et firma eller en annen juridisk person.

*NHO, FNH*og *Sparebankforeningen* påpeker bl.a. at begrepet autentiseringsmetode i definisjonen av elektronisk signatur bør gjøres mer tilgjengelig.

NTNU uttaler at utrykket «avansert elektronisk signatur» bør endres til «sterk elektronisk signatur» som er mer i tråd med kryptologisk terminologi. Dessuten savner de et punkt i definisjonen som sier at det skal være praktisk umulig å forfalske signaturen.

FO/S påpeker at definisjonen av avansert elektronisk signatur, punkt d) bør endres slik at det presiseres at det lar seg gjøre å oppdage *at* dokumentet er endret, men at teknologien gjør det umulig å finne *hva* i dokumentet som er endret. Videre har de forslag til endringer i definisjonene av signaturfremstillingsdata og signaturverifikasjonsdata ved at man fjerner «koder» og endrer «krypteringsnøkler» til «signeringsnøkler».

Arbeids- og administrasjonsdepartementet mener at en begrensning der undertegner kun er en fysisk person er for snever og at dette vil stenge for anvendelser der en server signerer meldinger på vegne av virksomheten, mens *NHO* ønsker at det klart skal fremgå av loven at elektroniske signaturer forbeholdes fysiske personer.

NHO, FNH og Sparebankforeningen etterlyser en definisjon av signaturmottaker.

Norsk EDIPRO uttaler generelt at definisjonene i § 3 til dels er uklare og uforståelige.

8.1.3 Departementets vurdering

Innspillene fra Justisdepartementet, Statskonsult, NHO, FNH og Sparebankforeningen og FO/S til utformingen av enkelte definisjoner er i hovedsak tatt til følge. Det kan f.eks. nevnes at i definisjonen av elektronisk signatur er autentiseringsmetode endret slik at innholdet blir lettere tilgjengelig, jf. merknadene til de enkelte bestemmelsene i kapittel 15.

Enkelte høringsuttalelser er ikke tatt til følge, da særlig av den grunn at *departementet* ønsker å beholde definisjonene nærmest mulig opp til de tilsvarende nordiske definisjonene, og i tråd med direktivets formuleringer der disse ikke kan forenkles uten at meningsinnholdet går tapt.

Definisjonen av elektronisk dokument er fjernet da departementet har kommet til at den er unødvendig. Videre inneholder forskjellig lovgivning ulike dokumentbegreper, og enda et nytt dokumentbegrep kan føre til større usikkerhet enn avklaringer. Det har dessuten vist seg vanskelig å komme frem til et dokumentbegrep som i denne forbindelse både er tilstrekkelig omfattende, og samtidig klart avgrenset. Det er på det rene at all informasjon

i digital form kan signeres og at dette omfatter både tekst, lyd og bilde. På denne bakgrunn slutter departementet seg også til forslaget om å anvende «data» fremfor «dokument» i øvrige definisjoner.

Departementet har dessuten sett det som et mål i seg selv å ha med færrest mulig definisjoner da en omfattende definisjonsliste ikke er i tråd med norsk rettstradisjon. Departementet har derfor ikke fulgt forslaget om å tilføre en definisjon av «signaturmottaker».

8.2 Sertifikatutsteder

8.2.1 Høringsnotatet

Lovforslaget regulerer virksomheten til fysiske eller juridiske personer som utsteder kvalifiserte sertifikater eller tilbyr andre tjenester relatert til elektronisk signatur. I direktivet omtales denne aktøren som «certification-service-provider» (CSP). I høringsnotatet er dette oversatt til «tilbyder av sertifikattjenester». Til en viss grad regulerer lovforslaget også tilbydere som går god for kvalifiserte sertifikater tilbudt av en annen.

En tilbyder av sertifikattjenesters virksomhet innebærer i hovedsak tilbud om og utstedelse av sertifikater for elektroniske signaturer. En tilbyder kan også selv eller i samarbeid med andre håndtere andre tjenester som identitetskontroll, tildeling av entydig navn, katalog- og tilbaketrekkingstjenester, herunder vedlikehold av tilbaketrekkingsliste, arkivering, tidsstempling, utstedelse av elektroniske sertifikater og konsulenttjenester i forbindelse med elektronisk signatur. Konsulenttjenestene kan bl.a. innebære rådgivning i forhold til mottakelse av signaturer fra «ukjente» sertifikatutstedere. For hver av disse funksjonene kan det være samarbeidspartnere eller underleverandører. Kvalifiserte sertifikater må være signert med tilbyderens avanserte elektroniske signatur, jf. § 4. Rapporten «Elektroniske signaturer - Myndighetsroller og regulering av tilbyder av sertifikattjenester» inneholder en del informasjon om tilbyder av sertifikattjenester, se særlig vedlegg 4 i rapporten.

8.2.2 Høringsinstansenes syn

Telenor er enig i at kjernefunksjonen for tilbydere av sertifikattjenester er å garantere koblingen mellom undertegner og opplysningene i sertifikatet, samt å tilby katalog- og tilbaketrekkingstjenester. De er av den oppfatning at formuleringen «andre tjenester relatert til elektronisk signatur» favner vidt og muligens kan skape usikkerhet, samtidig som de ser behov for et dynamisk begrep.

Norsk EDIPRO påpeker at det er uklart hvem som omfattes av definisjonen når det gjelder en fysisk eller juridisk person som «tilbyr andre tjenester relatert til elektronisk signatur». De stiller spørsmål ved om f.eks. en kortprodusent eller datakommunikasjonsleverandør vil være omfattet.

8.2.3 Departementets vurdering

Direktivets begrep «certification-service-provider» omfatter som nevnt ikke bare de som utsteder sertifikater, men også de som tilbyr andre tjenester som har tilknytning til elektroniske signaturer. Kjernefunksjonen er imidlertid å

garantere sammenhengen mellom undertegner og opplysningene i sertifikatet. Dette gjøres ved at utstederen av sertifikatet signerer sertifikatet med sin egen avanserte signatur før det utstedes.

Det vil etter *departementets* mening være tilfredsstillende å bruke begrepet «sertifikatutsteder» i denne sammenheng. Inn under begrepet omfattes også andre tjenester enn det å utstede sertifikater, jf. definisjonen § 3 nr. 10.

Ved å benytte «sertifikatutsteder» i stedet for «tilbydere av sertifikattjenester» unngår man forvekslingen av «sertifikat» og «sertifisering». Likedan unngår man problemet som Skattedirektoratet nevner med at man vanligvis kaller den som leverer tilbud som «tilbyder» og den som leverer produkter og tjenester for «leverandør».

Departementet går inn for at begrepet sertifikatutsteder skal anvendes. Dette begrepet er derfor innarbeidet i lovforslaget, jf. lovforslaget § 3 nr. 10, og anvendes i proposisjonen for øvrig.

Lovforslaget regulerer det å tilby kvalifiserte sertifikater og relaterte tjenester og til en viss grad at man går god for kvalifiserte sertifikater tilbudt av en annen. Lovforslaget stiller krav til virksomheten og regulerer erstatningsansvar for den som utsteder kvalifiserte sertifikater. Hvilken sertifikatutsteder som har utstedt det enkelte sertifikatet vil fremgå av utsteders elektroniske signatur som er påført i sertifikatet til den kvalifiserte signaturen, jf. lovforslaget § 4 annet ledd bokstav h). Vanlige regler om regressansvar kommer til anvendelse mellom utsteder og eventuelle samarbeidspartnere.

De andre tjenestene som f.eks. identitetskontroll, katalog- og tilbaketrekkingstjenester eller tidsstempling, kan den som utsteder sertifikatene velge å utføre selv eller i samarbeid med andre. Det følger av lovforslagets §§ 12-14 at sertifikatutsteder plikter å sørge for hurtig og sikker katalog- og tilbakekallelsestjeneste, identitetskontroll av undertegner og at relevante opplysninger om sertifikatene lagres. Som nevnt kan disse tjenestene settes bort til andre. De som utfører tjenester på vegne av sertifikatutsteder, må oppfylle de kravene loven oppstiller til den aktuelle tjenesten. Sertifikatutsteder er også ansvarlig for disse tjenestene overfor den som stoler på sertifikatet, jf. § 22.

Det følger av definisjonen at begrepet sertifikatutsteder omfatter det å tilby «andre tjenester relatert til elektronisk signatur». Definisjonen skal i størst mulig grad være teknologinøytral, og det er derfor ikke hensiktsmessig å avgrense begrepet nærmere. Videre ser man for seg at elektroniske signaturer vil bli brukt i mange forskjellige situasjoner og i forbindelse med forskjellige applikasjoner. Dette kan føre til en lang rekke nye tjenesteytelser og produkter relatert til elektroniske signaturer som vi ikke kjenner i dag. Også av denne grunn bør det i lovteksten benyttes et dynamisk begrep som ikke begrenses til å omfatte det å utstede og forvalte sertifikater, men som også åpner for at nye tjenester kan omfattes. På den annen side er ikke begrepet altomfattende, og enkelte sider ved bruk av elektroniske signaturer vil falle utenfor. Departementet mener at begrepet skal forstås slik at det f.eks. ikke omfatter nettverksleverandørene. Oppramsingen av eksempler vil være veiledende for avgrensningen av begrepet.

Lovforslaget har blitt utarbeidet i samarbeid med de øvrige nordiske land med det mål å oppnå nordisk rettsenhet på området. Det er nå på det rene at i den svenske loven og i det finske lovutkastet anvendes begrepet «certifikatut-

färdare», mens den danske loven bruker «nøglecenter». Når også det norske lovforslaget anvender begrepet sertifikatutsteder, får vi tilnærmet en felles nordisk definisjon på det som kan kalles direktivets kjernebegrep. Også det tidligere foreslåtte uttrykket «tilbyder av sertifikattjenester» var nytt for det norske markedet.

8.3 Krav til sertifikatutsteder i lovens kapittel III

8.3.1 Høringsnotatet

Lovens kapittel III stiller krav til sertifikatutstedere som utsteder kvalifiserte sertifikater og tjenestene de tilbyr. Det stilles altså krav til både den som utsteder det kvalifiserte sertifikatet og til de som eventuelt oppfyller andre oppgaver i forbindelse med håndteringen av de kvalifiserte sertifikatene på vegne av utsteder. Utstedere av andre sertifikater enn kvalifiserte reguleres ikke av dette kapittelet.

8.3.2 Høringsinstansenes syn

Lovforslaget § 10

Norges Rederiforbund støtter en forsikringsplikt eller annen form for økonomisk garanti for sertifikatutstedere og uttaler videre at det bør vurderes i relasjon til alle utstedere - både av kvalifiserte og ikke kvalifiserte sertifikater.

Lovforslaget § 11

Statskonsult påpeker at regler/formuleringer i annet ledd om godkjennelse av produkter og systemer er uklare i forhold til hvordan de skal godkjennes.

eforum antar at sertifikatutstedere vil ha plikt til å oppdatere de aktuelle systemer og produkter etter hvert som den teknologiske utviklingen fører til at påliteligheten reduseres, f.eks. ved at de opprinnelige benyttede systemer og/eller produkter som følge av ny teknologi eksponeres for manipulering fra utenforstående. eforum foreslår derfor at en slik oppdateringsplikt innarbeides i lovteksten ved at tillegget «til en hver tid» inntas i bestemmelsens første ledd.

Lovforslaget § 12

NHO og *Forsvarsdepartementet* etterlyser en nærmere definisjon av begrepene katalog- og tilbaketrekkingstjeneste. Videre foreslår Forsvarsdepartementet at forslagets annet ledd om at tjenesten skal kunne gi opplysninger om eventuelle begrensninger etter § 4 bokstav i) og j) utgår da slike funksjonaliteter normalt ikke er en del av tilbaketrekkingsteknikker.

Lovforslaget § 13

NHO uttaler at bestemmelsen regulerer overraskende lite identitetskontroll av undertegner og at nettopp kontroll av sertifikatholders identitet og utlevering av sertifikat til denne er helt avgjørende for kvaliteten og tilliten til signaturtjenesten. Brukerne er ifølge NHO i liten grad i stand til å vurdere denne

del av tjenesten selv. NHO stiller også spørsmål om det ikke er naturlig at også ikke-kvalifiserte sertifikater bør omfattes av bestemmelsen.

Brønnøysundregistrene uttaler at det vil være riktig å basere seg på Enhetsregisteret og Foretaksregisteret når det skal angis identifikatorer, navn og juridiske roller i forbindelse med elektroniske underskrifter.

Advokatforeningen foreslår at det tas inn en forskriftshjemmel til § 13 som gir departementet mulighet til å sette krav til hvilke opplysninger som skal kontrolleres.

Lovforslaget § 14

KITH og *Rikstrygdeverket* påpeker at en oppbevaringstid på 10 år i mange sammenhenger er for kort, jf. f.eks. journalforskriftens krav om oppbevaring i ubegrenset tid og saker vedrørende krigspensjonering. KITH mener at en deponeringsordning for sertifikater som ikke lenger er tilgjengelig for utsteder bør vurderes.

Riksarkivet uttaler at teknisk sett tyder alt på at et dokument som er arkivert med påført digital signatur i beste fall lar seg verifisere i 10-15 år.

NTNU uttaler at det på grunn av risikoen for at det kan produseres falske tilbakedaterte dokumenter med signaturfremstillingsdata knyttet til foreldede/tilbaketrukkede sertifikater, ikke bør brukes elektroniske signaturer på dokumenter som skal være gyldige i mer enn 10 år.

Datatilsynet uttaler at det neppe er grunnlag for å lovfeste en eksplisitt minimumsfrist for lagring av opplysninger og foreslår at punktet fjernes. De er av den oppfatning at lagringstiden må vurderes konkret i forhold til sertifikat og brukertype.

Justisdepartementet presiserer at kravene til lagring av opplysninger i § 14 må ses i sammenheng med personopplysningsloven § 28, der det heter at personopplysninger ikke lagres lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen.

NTNU uttaler at det er viktig at det er interoperabilitet[18)] mellom forskjellige utstederes sertifikater. Dette betyr i realiteten at samtlige utstedere ideelt sett bør benytte seg av samme sertifikatformat. Interoperabilitet er nødvendig for at undertegner selv skal kunne velge hvilken sertifikatutsteder han/hun ønsker å bruke. Undertegner bør ikke tvinges f.eks. av sin bank til å bruke sertifikater fra en bestemt utsteder.

Ellers kommer *NTNU* med flere konkrete forslag til endringer i lovteksten for å øke sikkerheten, f.eks. at det skal tilføres et punkt i § 14 om lagring av opplysninger som sikrer at det skal være praktisk umulig å forfalske signaturer med foreldede eller tilbaketrukkede signaturfremstillingsdata uten å bli avslørt umiddelbart. Videre savner de et krav i forhold til direktivet om kompetent personale til å drive det tekniske utstyret hos tilbyder for å gjøre det enklere å unngå useriøse aktører.

[18)] Med interoperabilitet menes den egenskap at flere metoder, produkter, standarder eller liknende har teknisk evne til å virke sammen.

Lovforslaget § 15

NHO uttaler at bestemmelsen om at opplysninger kan sendes elektronisk «dersom det skjer i en for motparten umiddelbart lesbar form» er upresis og uheldig.

8.3.3 Departementets vurdering

Departementet har tatt til følge de forslagene som har kommet til forenklinger i lovteksten for å gjøre loven mest mulig leservennlig. Det er følgelig gjort enkelte endringer etter høringsrunden for å gjøre lovteksten mer klar og presis.

Når det gjelder forslag som går på mer konkretisering av tekniske forhold vil disse innspillene tas i betraktning ved utformingen av forskrifter, jf. forskriftshjemmelen i § 16.

Departementet har tatt innspillene vedrørende lagringstid i betraktning og har kommet til at forslaget om en pliktig lagringstid på 10 år opprettholdes. Departementet vil presisere at dette er et minimumskrav, og at det må vurderes konkret hvorvidt opplysningens skal lagres lenger, også i forhold til personopplysningsloven. Det skal ellers bemerkes at den danske loven oppstiller et krav om lagring av opplysningene i minst 6 år og at den svenske loven ikke krever noen minimum lagringstid.

Departementet mener at det ikke er aktuelt å stille krav om interoperabilitet, men er positive til at utstederne selv - etter krav fra brukerne - inngår slike avtaler.

8.4 Kvalifiserte elektroniske sertifikater

8.4.1 Generelt om kvalifiserte elektroniske sertifikater

Det finnes i dag forskjellige standarder for elektroniske sertifikater, noe som leder til problemer vedrørende samhandling/interoperabilitet mellom sertifikatutstedere. Elektroniske sertifikater kan inneholde vidt forskjellig informasjon og bygge på ulikt sikkerhetsnivå. På bakgrunn av dette oppstiller direktivet visse minimumskrav til hva en bestemt type sertifikater med et høyt sikkerhetsnivå skal inneholde og krav til utstedere av slike sertifikater. Disse sertifikatene kalles «kvalifiserte sertifikater». Kravene til kvalifiserte sertifikater er implementert i lovforslaget, men vil også utdypes nærmere i forskrift.

Til disse sertifikatene er det knyttet bestemmelser om tilsyn, erstatning og rettsvirkninger. De rettslige rammene for kvalifiserte sertifikater skal gi tillit til kvalifiserte elektroniske signaturer og dermed også legge til rette for bruken av dem.

Det må fremgå av sertifikatet at det er et kvalifisert sertifikat og betegnelsen «kvalifisert sertifikat» skal benyttes. Dersom sertifikatet benevnes som noe annet, f.eks. et «super sertifikat» vil det falle utenfor denne reguleringen. Et unntak her er erstatningsbestemmelsen som også oppstiller ansvar for sertifikatutstedere som utsteder sertifikater som gir inntrykk av at de er kvalifiserte uten å være det. Slike «liksom-kvalifiserte sertifikater» kan også falle inn under markedsføringslovens regler om villedende forretningsmetoder.

Betegnelsen «kvalifisert sertifikat» skal videre kun brukes av de som utsteder kvalifiserte sertifikater, som oppfyller kravene i loven og er registrert hos tilsynet.

8.4.2 Høringsnotatet

I høringsnotatet foreslås det i § 4 en bestemmelse om kravene til kvalifiserte sertifikater, herunder hvilken informasjon et kvalifisert sertifikat skal inneholde. Forslaget i høringsnotatet regulerer ikke i detalj de tekniske kravene for et kvalifisert sertifikat. Kravene kan utfylles ved forskrift og gjennom arbeidet i komitèen som skal etableres iht. direktivet, se kapittel 5.

I direktivets vedlegg II bokstav l), står det at kun bemyndigede personer skal kunne gjøre tillegg og endringer i sertifikater. Denne bestemmelsen er ikke implementert i høringsnotatet da den ikke antas å være relevant i forhold til den offentlige nøkkel infrastrukturteknikk (PKI) som brukes i dag. Dersom det er gjort endringer i et sertifikat etter at det er utstedt og signert med utsteders nøkkel, vil dette enkelt kunne oppdages. Et sertifikat hvor det har blitt gjort endringer er ikke lenger gyldig da man ikke lenger har grunn til å tro at opplysningene i det er korrekt. Dersom det er behov for å gjøre endringer i sertifikatet, må det derfor kalles tilbake og et nytt utstedes.

8.4.3 Høringsinstansenes syn

Telenor, FNH og Sparebankforeningen påpeker at § 4 annet ledd bokstav e) er justert i forhold til direktivet ved at det er spesifisert at de signaturfremstillingsdata som *ved utstedelsestidspunktet*var under undertegnerens kontroll, skal svare til signaturfremstillingsdata.

*Telenor*uttaler at de ser visse tekniske problemer knyttet til at eventuelle begrensninger skal fremgå *direkte*av sertifikatet, jf. § 4 annet ledd bokstavene i) og j). De uttaler videre at:

> «slike krav vil, før standardene og standardproduktene er tilpasset, kunne medføre betydelige kostnader for leverandørene og vil kunne ha begrenset verdi for brukerne (for eksempel vil trolig en rekke klientapplikasjoner ikke klare å håndtere feltet). En mulighet fram til standardene og standardproduktene er tilpasset, er å henvise ved hjelp av standard policyindikator».

Telenor påpeker at loven ikke implementerer kravet i direktivet om at kun bemyndigede personer skal kunne foreta tilføyelser og endringer i sertifikatet. Dette begrunnes med at det ikke er mulig i forhold til gjeldende teknologi. Telenor mener det likevel bør vurderes om kravet skal implementeres for å ta høyde for teknologisk utvikling.

Posten SDS uttaler at det er uheldig at annet ledd a), som krever at sertifikatet skal angi om sertifikatet er kvalifisert eller ikke, ikke er tilfredsstilt i dagens tekniske standarder for sertifikater, og heller ikke er støttet i dagens signaturfremstillingssystem eller signaturverifikasjonssystem. Posten SDS ber departementet vurdere å overlate til en tilsynsmyndighet å bestemme i detalj hva et kvalifisert sertifikat skal inneholde, etter hvert som teknologien utvikles og anvendes.

Samferdselsdepartementet mener det er uklart hvorvidt bestemmelsen også gjelder sertifikater som benytter liknende betegnelser til kvalifisert.

8.4.4 Departementets vurdering

Paragrafens første ledd er forenklet noe i forhold til høringsnotatet. Etter innspill fra Telenor m.fl. er spesifiseringen til *utstedelsestidspunktet* tatt ut av lovteksten da dette kan være egnet til å forvirre. Spesifiseringen var gjort i forhold til erstatningsbestemmelsen som oppstiller ansvar for at undertegner disponerte korrekt signaturfremstillingsdata på tidspunktet da sertifikatet ble utstedt. Denne endringen har ikke noen betydning for realitetsinnholdet i § 4.

Departementet mener at bestemmelsen i direktivet om at kun bemyndigede personer skal kunne foreta tilføyelse og endringer i sertifikatet er misvisende. Sertifikatutstederen skal gå god for innholdet i sertifikatet ved å signere det med sin egen avanserte signatur. Dersom sertifikatet har blitt endret etter signering vil det ikke lenger være gyldig. Det vil derfor, etter departementets mening, være misvisende å regulere hvem som kan endre sertifikatet da dette tilsynelatende bygger på en forutsetning om at det kan gjøres endringer. Departementet foreslår derfor at bestemmelsen på det nåværende tidspunkt ikke tas inn i loven.

Ifølge kravene i direktivet må eventuelle begrensninger fremgå direkte av sertifikatet. Det er således ikke mulig, eller tilstrekkelig, slik Telenor ønsker, å i sertifikatet vise til et annet dokument der disse begrensningene kan leses.

8.5 Pseudonym

8.5.1 Generelt om pseudonym

Uansett hvor teknisk sikkert det elektroniske signatursystemet er, vil det ha avgjørende betydning at mottakeren kan stole på at undertegner er den han utgir seg for å være. Ingen kjede er sterkere enn det svakeste ledd, og i dette tilfellet korrekt identifisering og registrering av innehaver av sertifikatet. Hvis det er mulig for hvem som helst å få utstedt et sertifikat med navnet Ola Normann, gir det begrenset sikkerhet for mottakeren som ikke vil vite om han har fått informasjonen fra en person ved dette navnet, eller om det er et pseudonym for en annen.

Direktivet legger opp til at det skal kunne brukes sertifikater med pseudonymer. Det må imidlertid fremgå av sertifikatet at et pseudonym er benyttet. Dette er innarbeidet i lovforslaget, jf. § 4. For mer informasjon om pseudonymsertifikater og andre typer sertifikater, se kapittel 3.3.

8.5.2 Høringsnotatet

I høringsnotatet fremgår det at det skal være mulig å få utstedt et sertifikat med et pseudonym, men da må det fremgå av sertifikatet at et pseudonym er brukt. I praksis er spørsmålet hvor stor anvendelse et slikt sertifikat kan ha. Kan man bruke slike sertifikater for å treffe bindende avtale eller til å sende inn selvangivelse? Dette drøftes ikke nærmere i høringsnotatet.

Ifølge direktivets fortale punkt 25 skal bruk av pseudonymer i sertifikater ikke hindre stater fra å kunne stille krav om identifisering av person i henhold til fellesskapsrett eller nasjonal rett.

8.5.3 Høringsinstansenes syn

NHO anbefaler at loven ikke åpner for pseudonymsertifikater, og de ønsker at det klart skal fremgå at elektroniske signaturer forbeholdes fysiske personer. NHO er av den oppfatning at slike pseudonymsertifikater verken er forenlig med norsk rettstradisjon eller de behov slike sertifikater og signaturer antas å skulle tjene.

Toll- og avgiftsdirektoratet uttaler at det bør vurderes om det bør gå frem av loven at et pseudonym alltid bør peke på en konkret person. Videre uttaler de at en fra/til dato bør knyttes til den pseudonymet peker på, slik at man i ettertid har oversikt over hvem som til enhver tid «eide» pseudonymet. Dette kan være aktuelt f.eks. ved et senere erstatningsansvar.

8.5.4 Departementets vurdering

Departementet har kommet til at loven må åpne for at pseudonym skal kunne anvendes i et kvalifisert sertifikat for at EU-direktivet skal være implementert i sin helhet. EU-direktivet oppstiller i vedlegg I krav om at et kvalifisert sertifikat skal kunne inneholde et pseudonym, men at det må fremgå at det er et pseudonym. Dette følger også av definisjonen av en avansert elektronisk signatur, som sier at denne entydig skal være knyttet til undertegner. Departementet er videre av den oppfatning at det kan være et faktisk behov i markedet for å anvende pseudonym også i kvalifiserte sertifikater.

En kvalifisert elektronisk signatur er en avansert elektronisk signatur som er basert på et kvalifisert sertifikat og fremstilt av et godkjent sikkert signaturfremstillingssystem, jf. § 3 nr. 3. En avansert elektronisk signatur stiller krav om at den er entydig knyttet til undertegneren. Dette betyr at signaturen ikke kan benyttes av flere personer. Dersom man ønsker at en annen skal bruke det aktuelle pseudonymet, må sertifikatet trekkes tilbake og et nytt utstedes. Således vil det ikke være behov for å koble pseudonymet til en dato som Toll- og avgiftsdirektoratet ønsker.

8.6 Registrering av sertifikatutsteder

8.6.1 Generelt om registrering av sertifikatutsteder

I henhold til direktivet må landene ikke stille krav om forhåndsgodkjennelse av sertifikatutstedere, jf. artikkel 3 nr. 1. Dette er utdypet i punkt 10 i fortalen til direktivet til å også gjelde «...enhver annen foranstaltning med samme virkning...». Det er imidlertid ikke noe til hinder for å kreve at sertifikatutstedere skal registrere seg før de begynner virksomheten, så fremt det ikke stilles andre krav enn at meldingen sendes inn.

8.6.2 Høringsnotatet

I høringsnotatet foreslås det at sertifikatutsteder skal sende inn registreringsmelding til tilsynsmyndigheten (Post- og teletilsynet) senest samtidig med at utstederen begynner å utstede kvalifiserte sertifikater. Sertifikatutstederen er deretter pålagt å sende inn melding om alle eventuelle endringer av registrerte opplysninger.

8.6.3 Høringsinstansenes syn

Ingen av høringsinstansene kommenterer direkte forslaget om registreringsordning, se kapittel 8.7.2.2. om høringsinstansenes generelle kommentarer til valg av tilsynsmodell.

8.6.4 Departementets vurdering

Selv om det er mulig å kreve at utstedere skal sende inn registreringsmelding før de begynner å utstede kvalifiserte sertifikater, er *departementet* av den oppfatning at det er tilstrekkelig at melding sendes inn senest samtidig med utstedelse av det første kvalifiserte sertifikatet. Sannsynligvis vil registrering skje langt tidligere enn dette tidspunktet. Sertifikatutstederne ønsker neppe å havne i den situasjonen at de sertifikater som tilbys på markedet ikke godkjennes av tilsynet som kvalifiserte, slik at sertifikatene må trekkes tilbake og nye utstedes. En slik situasjon vil høyst sannsynligvis påvirke utstederens tillit i markedet negativt.

8.7 Tilsyn

8.7.1 Krav om tilsyn

Ifølge direktivet stilles det krav om at det skal føres tilsyn med de utstedere av kvalifiserte sertifikater som tilbyr sertifikatene og tilhørende tjenester til allmenheten. Direktivet er ikke til hinder for at tilsynet også kan omfatte utstedelse av sertifikater på et annet nivå enn kvalifisert. For å oppfylle kravet om tilsyn er det hensiktsmessig å kreve at de sertifikatutstederne det skal føres tilsyn med registreres i et offentlig register. Krav om registrering i et slikt register vil ikke være i strid med direktivets forbud mot forhåndsgodkjenning, heller ikke dersom registrering skal skje før utstederne begynner sin virksomhet.

8.7.2 Tilsynsmodell

8.7.2.1 Høringsnotatet

I rapporten «Elektroniske signaturer - Myndighetsroller og regulering av tilbyder av sertifikattjenester» (jf. kapittel 4.2) presenteres flere mulige modeller for regulering av sertifikatutstedelse og tilhørende tjenester. Disse forskjellige modellene vil ikke bli nærmere drøftet her. I rapporten anbefaler utvalget at man bør velge en modell som kalles selvdeklarasjonsmodellen. I rapportens kapittel 6 er modellen beskrevet på følgende måte (CSP (certification-service-provider) er det samme som sertifikatutsteder):

> «... modellen bygger på at CSPene er avhengige av at markedet har tillit til sertifikatene, og at markedet derfor i stor grad vil regulere seg selv. Samtidig kan det av hensyn til tilliten til systemet i sin helhet være verdifullt med et tilsyn som kan gripe inn. Tilsynet bør være så markedsorientert som mulig, slik at man ikke legger unødvendige administrative byrder, og derved kostnader på CSPene.
>
> Tilsynet er en eksisterende offentlig virksomhet, f.eks. PT [Post- og teletilsynet]. CSPer som skal utstede kvalifiserte sertifikater i Norge må melde denne virksomheten inn til tilsynsmyndigheten. Denne meldingen skal være en deklarasjon om at CSPen oppfyller kravene til

kvalifisert sertifikat, herunder opplyse om hvilken sertifikatpolicy de følger og hvordan deres sertifikatutstedelsespraksis er. Tilsynet kan vise til hvilke policy og praksis som oppfyller kravene. Hva som skal rapporteres inn besluttes i forskrift av tilsynet. Virksomheten blir registrert i et eget register med oversikt over CSP-er.

Deklarasjonen sendes kun inn ved oppstart av virksomheten, og dersom det skjer endringer som gjør at de registrerte opplysningene ikke lenger er korrekte.

Tilsynsmyndighetene kan imidlertid kreve å få alle de opplysninger som de ønsker for å sikre at CSPer som tilbyr kvalifiserte sertifikater oppfyller kravene i loven. Slik kontroll kan skje dersom tilsynet mener det er nødvendig, eller etter 'krav' fra brukere eller andre aktører.»

Når det gjelder fordeler og ulemper med modellen står det følgende i rapporten:

«Sammenlignet med revisjonsmodellen må CSPene i selvdeklarasjonsmodellen ikke sende inn årlige rapporter om foretatt IT-revisjon til tilsynet. I Sverige har man kommet frem til at revisjonsmodellen vil være et tungrodd og kostbart apparat. Man ønsker ikke en utvikling der CSPer, kun for å unngå et kostbart tilsyn, ikke kaller sine sertifikater for kvalifiserte selv om de oppfyller kravene.

Ved å velge selvdeklarasjonsmodellen vil det heller ikke være behov for å regulere hvem som kan være IT-revisor.

Til forskjell fra kontrollmodellen må CSPen ikke sende inn jevnlige rapporter til tilsynet.

Deklarasjonen som skal sendes tilsynet kan være relativt kort og bør blant annet inneholde garantier vedrørende personvern, økonomi og overholdelse av kravene i anneksene til direktivet...

Modellen krever en viss kompetanse innen IT-revisjon hos tilsynet, men tilsynsformen utelukker ikke at man innhenter privat ekspertise i forbindelse med enkelte kontroller.»

I sine konklusjoner, kapittel 7, skriver utvalget bl.a. følgende:

«Ut i fra kunnskapene om at en omfattende tilsynsordning med sterk kontroll er dyrt, at markedet er i utvikling, at kundene er få og etterspør billige løsninger, anbefaler utvalget at myndighetene viser varsomhet vedrørende regulering av CSP-virksomhet. Utvalget konkluderer derfor med å velge selvdeklarasjonsmodellen.»

Det er vanskelig å velge den mest hensiktsmessige tilsynsmodellen for et marked som er så ungt. Det er derfor viktig å ikke detaljregulere dette markedet på en slik måte at markedet hindres i å utvikle seg på en mest mulig optimal måte. Her bør partene i markedet så langt det er mulig selv få «regulere» sin virksomhet og sikre at de følger de kravene som står i loven. Dessuten er det viktig at man ikke fra norsk side utformer en lov som stiller norske sertifikatutstedere i en dårligere stilling konkurransemessig enn utstedere etablert i andre land.

I høringsnotatet foreslås selvdeklarasjonsmodellen som tilsynsmodell. Denne modellen er en av de minst inngripende modellene som er presentert i utvalgets rapport. Likevel oppfyller modellen de krav om tilsyn som stilles i direktivet, og modellen vil gi et reelt og funksjonelt tilsyn, som vil gi den nødvendige tilliten i markedet. Det svenske lovforslaget innebærer en tilnærmet identisk tilsynsmodell. Det kan imidlertid ikke utelukkes at modellen vil måtte

justeres og kompletteres når markedet er mer modent. Utviklingen i markedet må derfor følges nøye fremover.

8.7.2.2 Høringsinstansenes syn

EDIPRO, Telenor, Advokatforeningen, eforum, Norges Eksportråd og *Euro Info* uttaler at de er positive til at departementet har valgt den tilsynsmodellen som er minst inngripende bl.a. fordi denne modellen er best egnet ut fra det syn at markedet er ungt og at norske aktører ikke bør stille konkurransemessig dårligere enn sertifikatutstedere etablert i andre land. Også *NORTIB, FNH og Sparebankforeningen*støtter valget av tilsynsordning. *Norges Bedriftsforbund* bemerker at registreringskostnader og tilsynsavgifter bør være lave for utstedere i etableringsfasen.

Posten SDS aksepterer valget av selvdeklareringsmodellen, men mener imidlertid at «revisjonsmodellen» vil gi bedre sertifikattjenester. Posten SDS uttaler at de har funnet av egne erfaringer at kvaliteten på tjenestene styrkes ved at de har hatt en fullstendig revisjon av sertifikattjenesten foretatt av ekstern instans. De er litt usikre på om leverandører som ikke har foretatt en slik uhildet revisjon klarer å lage noe som kvalifiserer til betegnelsen kvalifiserte sertifikater.

NTNU uttaler at det er lagt opp til et utilstrekkelig tilsyn med utstedere av kvalifiserte sertifikater. NTNU mener at evaluering og akkreditering er nødvendig for å hindre utglidning i bransjen. Dette er også nødvendig for at forbrukerne skal kunne ha tillit til ukjente aktører i bransjen. NTNU peker bl.a. på at man ikke kan få et sikkert system basert på at bestanddelene hver for seg regnes som sikre, men at systemet må evalueres og sertifiseres som en helhet.

Justervesenet uttaler at dersom det er behov for anerkjennelse av elektroniske signaturer over landegrensene er det verdt å vurdere og etablere en mer spesifikk frivillig ordning basert på akkreditering. Justervesenet mener at det ligger vel til rette for å gjøre nytte av den infrastrukturen som allerede er etablert gjennom, bl.a. European Cooperation for Accreditation, for å skape internasjonal tillit til utstedere av kvalifiserte sertifikater på en rasjonell og effektiv måte.

8.7.2.3 Departementets vurdering

Departementet mener at det på det nåværende tidspunkt er avgjørende at man ikke overregulerer markedet slik at den tekniske utviklingen hindres. På den annen side er det klart at innholdet i tilsynsvirksomheten ikke er helt klartlagt før forskriftene er på plass. Disse forskriftene skal tre i kraft samtidig med loven.

Departementet ser positivt på mulige fremtidige initiativ i markedet til frivillige sertifiserings- / akkrediteringsordninger. Departementet antar at aktualiteten av slike ordninger vil vurderes når utviklingen i andre europeiske land er klarere og standardiseringsarbeidet har kommet lenger.

8.7.3 Tilsynsorgan

8.7.3.1 Høringsnotatet

Direktivet legger opp til at tilsynet kan være et offentlig eller privat organ. Når det gjelder spørsmålet om det skal utpekes et offentlig eller privat organ har departementet kommet til at det bør velges et offentlig tilsynsorgan. Departementets konklusjon bygger bl.a. på antagelsen om at et offentlig tilsynsorgan har størst tillit i markedet. Videre er denne typen tilsynsvirksomhet et av det offentliges kjerneoppgaver da det regulerer borgernes rettigheter og plikter, i dette tilfellet i tillegg på et område hvor brukerne har liten kompetanse.

Utredningen «Elektroniske signaturer - Myndighetsroller og regulering av tilbyder av sertifikattjenester» tar for seg spørsmål om myndighetsroller, godkjenningsordning og krav til utstedere burde utredes nærmere. Herunder kommer de med forslag til valg av tilsynsorgan. I rapporten foreslås det at tilsynet bør legges til Post- og teletilsynet. Konklusjonene i høringsnotatet bygger på denne rapporten. I valget av tilsyn har utvalget vektlagt følgende:

- Post- og teletilsynet (PT) har allerede ansvar for å føre tilsyn med aktørene på post- og teleområdet. PT forvalter i dag et større antall forskrifter og utøver tilsyn på mange områder.
- PT fører allerede register over aktørene på post- og teleområdet.
- PT har bred kompetanse både på det juridiske, økonomiske og teknologiske området, og er i sin virksomhet vant til å arbeide i grensefeltet mellom disse områdene.
- Med dereguleringen av telemarkedet har PT, i forbindelse med opprettelse og forståelse av samtrafikkavtaler mellom Telenor og de nye aktørene i telemarkedet, hatt rollen som mekler mellom partene.
- Sverige og Danmark har valgt sine Post- og teletilsyn som tilsynsmyndighet.

Valget av tilsyn begrunnes på følgende måte i rapporten:

> «PT har også et bredt og omfattende internasjonalt kontaktnett og arbeider aktivt med internasjonale spørsmål. For flere av aktørene vil også PT være en kjent organisasjon å forholde seg til. PT vil derfor være et godt egnet sted å plassere tilsynet. PT er også en relativt stor organisasjon med ca 200 ansatte som lettere vil kunne innpasse nye områder i sitt arbeidsfelt. Datatilsynet har på sin side kun 22 tilsatte.
>
> I valget mellom disse to eksisterende tilsyn [PT eller Datatilsynet] konkluderer utvalget med å anbefale Post- og teletilsynet. Det legges særlig vekt på hva som er disse institusjonenes hovedformål. Post- og teletilsynets generelle formål er å sikre rimelige og gode post- og teletjenester. Å føre tilsyn med CSPer [sertifikatutstedere] kan ses på som en del av dette.»

Departementet støtter utvalgets konklusjon i valg av tilsynsorgan. På bakgrunn av Post- og teletilsynets erfaring med liknende oppgaver foreslås det i høringsnotatet at tilsynsoppgavene legges til Post- og teletilsynet.

8.7.3.2 Høringsinstansenes syn

Justervesenet, Brønnøysundregistrene, Samferdselsdepartementet, Norsk Bedriftsforbund og *NORTIB*uttaler at de støtter valget av Post- og teletilsynet utfra kompetanse og ansvarsområde. Ingen av høringsinstansene er negative

til valg av Post- og teletilsynet som tilsynsorgan. Flere høringsinstanser mener at tilsynet bør utpekes i lovteksten.

Datatilsynet uttaler at de har ingen vesentlige innvendinger mot forslaget om å legge tilsynsfunksjonen til Post- og teletilsynet. Imidlertid er de av den oppfatning at tilsyn i tilknytning til personvernrelaterte spørsmål, herunder sikring av personopplysninger, fortsatt tilligger Datatilsynet i henhold til den nye personopplysningsloven.

Post- og teletilsynet stiller seg positive til å påta seg tilsynsoppgaven.

8.7.3.3 Departementets vurdering

Departementet opprettholder forslaget til valg av Post- og teletilsynet som tilsynsorgan med virksomheten til utstedere av kvalifiserte sertifikater. Dette forslaget støttes av samtlige høringsinstanser. Det er selvsagt også et viktig moment at Post- og teletilsynet stiller seg positive til å påta seg tilsynsoppgaven.

Departementet har kommet til at det bør følge av loven at Kongen utpeker tilsynet og at dette ikke gjøres direkte i lovteksten.

Når det gjelder lovforslaget § 7 om innsamling og bruk av personopplysninger, er departementet imidlertid enig i uttalelsene fra Datatilsynet om at tilsyn i tilknytning til personvernrelaterte spørsmål bør ligge hos Datatilsynet. Denne bestemmelsen ligger i innhold nært opptil personopplysningslovens regler som håndheves av Datatilsynet. Videre skal bestemmelsen gjelde alle sertifikatutstedere, også de som ikke utsteder kvalifiserte sertifikater. De tilsynsoppgavene som tillegges Post- og teletilsynet vil kun gjelde utstedere av kvalifiserte sertifikater. Dette kan oppsummeres slik at Post- og teletilsynet utpekes som tilsyn iht. lovforslaget, med unntak av § 7 hvor tilsynet legges til Datatilsynet. Se mer om dette under kapittel 11.

8.7.4 Tilsynets oppgaver

8.7.4.1 Høringsnotatet

Kravene loven stiller til utstedere av kvalifiserte sertifikater vil bli nærmere presisert i forskrifter. En av tilsynets hovedoppgaver vil være å utdype disse kravene ved å ta stilling til hvilke policy og praksis som oppfyller lovens krav, herunder må tilsynet vurdere hvorvidt eventuelle frivillige sertifiseringer (se kapittel 9) og rapporter fra IT-revisjonsfirmaer kan «erstatte» deler av tilsynets eget arbeid.

For det andre må tilsynet kommunisere disse presiserte kravene til sertifikatutstedere som ønsker å tilby kvalifiserte sertifikater. Tilsynet kan f.eks. legge ut en liste på en egen hjemmeside over hvilke policy og praksis som oppfyller kravene.

For det tredje må tilsynet se til at sertifikatutstedernes virksomhet er i overensstemmelse med de presiserte kravene. På bakgrunn av meldingene fra utstedere av kvalifiserte sertifikater skal tilsynet vurdere om kravene som stilles i loven med forskrifter er oppfylt. Tilsynet har anledning til å etterspørre ytterligere informasjon og dokumenter som er nødvendige for at tilsynet skal kunne utføre sine oppgaver. Bl.a. må tilsynet vurdere utstedernes sertifikatpo-

licy, hvorvidt sertifikatutstedelsespraksis er i samsvar med policy og om den faktiske gjennomføringen er i samsvar med praksis.

Tilsynet bør legge ut en liste over alle registrerte sertifikatutstedere, eventuelt kan dette gjøres på egen hjemmeside. Hvilken informasjon som for øvrig bør legges ut, kan vurderes på et senere tidspunkt. På den måten vil det være mulig for de som ønsker å skaffe seg en elektronisk signatur og for de som stoler på sertifikater, å se hvilke utstedere som oppfyller kravene i loven med forskrifter og omfattes av tilsynet.

Det presiseres at tilsynets oppgaver vil konkretiseres i forskrifter, mens lovforslaget inneholder mer overordnede prinsipper som bygger på EU-direktivet.

8.7.4.2 Departementets vurdering

Tilsynets oppgaver vil bli nærmere fastlagt i forskrift. Disse forskriftene vil tre i kraft samtidig med lovforslaget.

8.7.5 Klageadgang for tilsynets avgjørelser

8.7.5.1 Høringsnotatet

De vedtak tilsynet vil treffe i medhold av denne loven vil i hovedsak omhandle driftsmessige og tekniske forhold relatert til den virksomhet som sertifikatutstederne kan drive. En ankeinstans må derfor ha inngående teknisk kjennskap til elektroniske signaturer og utstedernes virksomhet for å være i stand til å vurdere tilsynets avgjørelser. Ankeinstansen vil sannsynligvis kun treffe avgjørelser i et lite antall saker. Det tas i høringsnotatet ikke stilling til hvem som skal utpekes som klageinstans, jf. § 23.

8.7.5.2 Høringsinstansenes syn

Når det gjelder klageadgang uttaler *Post- og teletilsynet* at det i rapporten legges opp til at klager behandles av de samme organer som behandler øvrige klager på deres vedtak. I kommentarene til lovforslaget er det påpekt at klageinstansen må ha inngående kjennskap til elektroniske signaturer og tilbydernes virksomhet. Etter Post- og teletilsynets oppfatning er det tvilsomt om dagens klageinstanser besitter slik kompetanse. Post- og teletilsynet mener at det trolig kan være hensiktsmessig at Nærings- og handelsdepartementet, som ansvarlig departement for loven med tilhørende forskrifter, kan være klageinstans. Departementet kan etter deres mening på denne måten skaffe seg erfaring med loven, som kan være nyttig med tanke på eventuelle revisjoner av loven og forskrifter.

Samferdselsdepartementet uttaler at det ved utpekingen av klageorgan bør legges vekt på å ikke komplisere klageordningen på teleområdet ytterligere. Utpekingen bør etter deres mening skje i samråd med Samferdselsdepartementet, og de forutsetter at klageorganet blir tilført nødvendig kompetanse.

8.7.5.3 Departementets vurdering

Lovforslaget utpeker ikke klageorgan for Post- og teletilsynets avgjørelser, men gir Kongen hjemmel til å utpeke et slikt organ. Dette organet vil være

overordnet forvaltningsorgan i forhold til reglene om klageadgang i forvaltningsloven §§ 28 flg. Forvaltningslovens klageregler kommer ellers til anvendelse.

Departementet legger ikke opp til at klageadgangen skal være videre enn hva som følger av forvaltningslovens regler. For å kunne klage på tilsynets avgjørelser må man således ha rettslig klageinteresse. Det legges dermed ikke opp til noen formell klageadgang for forbrukerne tilsvarende den utvidede klageadgangen på områdene som dekkes av lov om telekommunikasjon.

Avgjørelser fra tilsynet som kan påklages vil f.eks. være pålegg om å gi opplysninger, jf. § 17 annet ledd, krav om IT-revisjon, jf. § 17 fjerde ledd, vedtak om å frata sertifikatutsteder retten til å anvende begrepet kvalifisert sertifikat, jf. § 17 femte ledd, beslutning om å fremme granskningsforretning, jf. § 19 og feil i registeret fra tilsynets side, jf. § 18.

Ved utpekelsen av klageorganet vil det legges vekt på at det utpekte organet skal ha tilstrekkelig kompetanse og klare ansvarslinjer i forhold til Post- og teletilsynets avgjørelser.

8.8 Sikre signaturfremstillingssystem

8.8.1 Høringsnotatet

Det følger av den foreslåtte definisjonen av kvalifisert elektronisk signatur at dette er en avansert elektronisk signatur basert på et kvalifisert sertifikat som er fremstilt av et sikkert signaturfremstillingssystem. Dette betyr at det må brukes et sikkert signaturfremstillingssystem for å oppnå rettsvirkninger i henhold til § 6. Sikre signaturfremstillingssystem kan først tas i bruk når de er i samsvar med standarder fastsatt av Europakommisjonen eller godkjent av et oppnevnt nasjonalt organ, se nedenfor. Kravene til sikre signaturfremstillingssystem oppstilles i § 8.

I henhold til § 9 første ledd kan medlemslandene utpeke et egnet offentlig eller privat organ som skal avgjøre om et signaturfremstillingssystem oppfyller kravene i § 8.

Dessuten kan Europakommisjonen fastsette, og i EF-Tidende offentliggjøre, referansenummer på generelt anerkjente standarder for elektroniske signaturprodukter, jf. loven § 9 tredje ledd. Kravene til et sikkert signaturfremstillingssystem er oppfylte når maskin- eller programvare som benyttes er i overensstemmelse med slike standarder.

I Norge er Forsvarets Overkommando/Sikkerhetsstaben (FO/S) utøvende myndighet for sertifisering av IT-sikkerhet i produkter og systemer. Det er altså FO/S som utsteder sertifikater til de produkter som har vært gjenstand for evaluering av et evalueringsorgan. Evalueringsorgan blir akkreditert av Norsk Akkreditering som teknisk laboratorium etter standardene EN 45001 eller ISO Guide 25.

FO/S sertifiserer i henhold til Common Criteria. Common Criteria ble utviklet med det mål å etablere felles internasjonalt harmoniserte kriterier for sikkerhetsevaluering, og er basert på kravene i de europeiske (ITSEC), de amerikanske (TCSEC) og de kanadiske (CTCPEC) kriteriene.

Det er per i dag ikke sikkert om det vil være behov for å opprette et slikt organ i Norge. Imidlertid, dersom dette skal skje, bør det velges et allerede

eksisterende organ. Den mest nærliggende løsningen er da at FO/S utpekes som det organ som skal avgjøre om et signaturfremstillingssystem er sikkert. Men det er for tidlig å ta noen endelig avgjørelse vedrørende dette nå. Komiteen nedsatt iht. direktivet har arbeidet frem de kriterier som skal stilles ved valg av det nasjonale organet.

8.8.2 Høringsinstansenes syn

NHO, Statskonsult, FNH og Sparebankforeningen påpeker at det er uklart hvorvidt sikre signaturfremstillingssystem kan godkjennes på en eller to ulike måter i henhold til bestemmelsen. *Justisdepartementet* kommer med konkrete forslag til forenkling av lovteksten.

8.8.3 Departementets vurdering

Bestemmelsen om godkjennelse er endret slik at det kommer tydeligere frem at sikre signaturfremstillingssystem kan godkjennes på to måter. De skal være i samsvar med standarder fastsatt av EU-kommisjonen eller godkjent av et oppnevnt nasjonalt organ. Videre er bestemmelsen endret i tråd med forslag fra Justisdepartementet.

Når et signaturfremstillingssystem er godkjent av et annet nasjonalt organ innenfor EØS-området, må denne godkjennelsen aksepteres av det norske tilsynet. En sertifikatutsteder som omfattes av det norske tilsynet kan altså bruke dette systemet uten å måtte innhente en ny godkjennelse i Norge. Dette følger av lovforslaget § 9 annet ledd.

Komiteen, etablert i henhold til EU-direktivet artikkel 9 og 10, har utarbeidet kriterier for utpeking av det nasjonale godkjennelsesorganet.

8.9 Erstatningsbestemmelser

8.9.1 Generelt om lovens erstatningsregler

Lovens § 22 regulerer erstatningsansvar for utstedere av kvalifiserte sertifikater og sertifikatutstedere som garanterer for slike sertifikater utstedt av andre. Når en sertifikatutsteder garanterer for en annen sertifikatutsteder omtales dette gjerne som kryssertifisering.

Det følger av § 2 om lovens virkeområde at erstatningsbestemmelsen gjelder de som utsteder kvalifiserte sertifikater. I § 22 presiseres det at sertifikater som utgis for å være kvalifiserte, selv om kravene ikke er oppfylte, også omfattes av erstatningsbestemmelsen. Presiseringen er ment å forebygge at sertifikatutstedere tilbyr sertifikater som brukerne får inntrykk av at omfattes av lovverket, uten at utstederen har det erstatningsansvaret som følger av loven. For andre sertifikater gjelder de alminnelige erstatningsreglene.

Direktivets erstatningsbestemmelse er en minimumsbestemmelse. Dette innbærer at EØS-landene kan velge å pålegge et strengere ansvar enn direktivets ordlyd. Departementet har vurdert å gå lenger enn direktivet ved å gi erstatningsregler som skal gjelde for alle sertifikater og ikke bare de kvalifiserte. Som argument for en utvidelse av ansvaret kan det anføres at det etter alminnelig erstatningsrett kan være usikkert hvilket ansvar som gjelder, særlig der det ikke foreligger et kontraktsforhold mellom partene. Denne usikker-

heten taler for å utvide ansvaret. Videre er det usikkert hvorvidt markedet i fremtiden vil anvende seg av kvalifiserte sertifikater eller andre sertifikater som ikke er kvalifiserte i henhold til direktivet. Også ved bruk av andre sertifikater kan det være et behov for særlige erstatningsregler.

På den annen side bør det påpekes at dersom sertifikatutstederne pålegges et særlig strengt ansvar vil dette kunne medføre at prisene på tjenestene blir høye, og at norske sertifikatutstedere vanskelig vil kunne konkurrere med sertifikatutstedere fra andre EØS-land. Videre er noe av formålet med direktivet å skape en felles ramme for betingelser for bruk av elektronisk signatur, bl.a. for å styrke tilliten til den nye teknologien ved å gi de kvalifiserte sertifikatene en særstilling. Det er dessuten et mål i seg selv at direktivet gjennomføres likest mulig, slik at det i størst mulig grad legges til rette for fri bevegelse av varer og tjenester på tvers av landegrensene. Det svenske og det danske lovforslaget går ikke lengre i å pålegge erstatningsansvar enn det direktivet krever. Hensynet til nordisk rettsenhet er et vektig argument i seg selv. Departementet har kommet til at Norge bør gjennomføre en minimumsregulering av sertifikatutsteders erstatningsansvar i samsvar med direktivet.

Forslaget innebærer en minimumsregulering, slik at det ikke vil være mulig å gjøre avtaler til ulempe for den som stoler på et sertifikat. Lovforslaget er med andre ord preseptorisk. Videre vil avtaleloven § 37 beskytte forbrukere som inngår standardavtaler med sertifikatutsteder.

8.9.2 Ansvarets omfang

Sertifikatutsteder er erstatningsansvarlig overfor fysiske eller juridiske personer som med rimelighet stolte på sertifikatet. Disse personene kan være undertegner, mottaker eller en tredjemann som stolte på sertifikatet. I forhold til tredjemann kan det nevnes at det foreligger tekniske løsninger som gjør det mulig å sende et signert dokument videre gjennom mange mellomledd med den samme opprinnelige signaturen. En signatur kan med andre ord verifiseres av flere tredjemenn.

Særlige problemer oppstår i forhold til undertegnerens ansvar ved tredjemanns urettmessige bruk av signaturen. Dette kan skje ved at en person tilegner seg PIN-kode og/eller smartkort, eller ved at sertifikatutsteder utleverer PIN-kode og/eller smartkort til feil person. Loven vil ikke regulere dette forholdet, men dette kan reguleres i generelle avtalebestemmelser og i avtalene mellom sertifikatutsteder og undertegner.

Sertifikatutsteder er erstatningsansvarlig i henhold til lovforslagets § 22 så sant utstederen ikke kan bevise at han/hun ikke handlet uaktsomt. Sertifikatutsteder har således et culpa-ansvar med omvendt bevisbyrde. Dette innebærer et unntak fra de alminnelige erstatningsrettslige prinsipper som sier at skadelidte har bevisbyrden for å påvise en sannsynlighetsovervekt for at skaden er voldt ved en uaktsom handling. Sertifikatutsteder må etter denne loven vise at skaden ikke skyldtes dennes uaktsomme handling. En lovfestning av den omvendte bevisbyrden innebærer at sertifikatutsteder må vise at sertifiseringspraksis, verifisering av sertifikater, opplysninger om eventuell sperring mv. er skjedd i overensstemmelse med gjeldende regler og forskrifter.

Culpa-ansvaret med omvendt bevisbyrde innebærer ikke direkte noe strengere erstatningsansvar i forhold til de alminnelige erstatningsreglene,

men en tyngre bevisbyrde for utsteder. I realiteten kan dette føre til et skjerpet ansvar for utsteder. Den omvendte bevisbyrden er det eneste unntaket fra den alminnelige erstatningsrett.

Culpa-ansvar med omvendt bevisbyrde er innført pga. områdets meget tekniske og kompliserte karakter. For den alminnelige bruker av elektroniske signaturer, uten særlig kjennskap til teknologien, vil det være vanskelig å påvise at sertifikatutsteder har begått feil eller forsømmelser som kan bedømmes som culpøse eller forsettlige. Videre skal et skjerpet krav om bevisbyrde være med på å sikre den nødvendige tillit og dermed øket anvendelse av kvalifiserte sertifikater.

Loven legger opp til at sertifikatet kan inneholde begrensninger i forhold til anvendelsesområde eller beløp, jf. lovens § 4 annet ledd bokstav i) og j). Disse begrensningene gjelder også i forhold til erstatningsreglene. Sertifikatutsteder vil altså ikke være erstatningsansvarlig for bruk av sertifikatet som er i strid med tydelige begrensninger i sertifikatets anvendelsesområde eller utover beløpsmessige begrensninger, jf. lovforslaget § 22 annet ledd.

8.9.3 Forholdet til alminnelig erstatningsrett

Erstatningsbestemmelsen regulerer kun enkelte sider ved erstatningsansvaret for en sertifikatutsteder som utsteder kvalifiserte sertifikater. I dette ligger det at alminnelig erstatningsrett vil supplere lovens erstatningsregler. Kravene om ansvarsgrunnlag, årsakssammenheng og adekvans skal f.eks. alltid oppfylles. Erstatningsansvar for en utsteder som ikke utsteder kvalifiserte sertifikater reguleres i henhold til den alminnelige erstatningsretten. Det kan her bemerkes at forholdet mellom utsteder og undertegner nok i stor grad vil reguleres gjennom avtaler, slike avtaler må imidlertid ikke være i strid med denne lovens bestemmelser. Denne loven er med andre ord preseptorisk.

8.9.4 Høringsnotatet

Høringsnotatet inneholder et forslag til lovtekst i tråd med de synspunkter som er nevnt ovenfor. Erstatningsbestemmelsen oppstiller et culpa-ansvar med omvendt bevisbyrde for utstedere av kvalifiserte sertifikater for nærmere angitte forhold. Forslaget åpner for at sertifikatutsteder og undertegner kan avtale begrensninger i sertifikatets anvendelsesområde og begrensninger for hvor store beløp som skal kunne overføres med signaturen. Slike begrensninger vil tilsvarende begrense sertifikatutstederes erstatningsansvar.

8.9.5 Høringsinstansenes syn

Norsk EDIPRO uttaler at unntaket i annet ledd for bruk av sertifikatet i strid med tydelige begrensninger i sertifikatets anvendelsesområder eller beløpsmessige begrensninger, kan danne grunnlag for en rekke rettslige tvister. Det foreligger etter deres skjønn en fare for at man her begrenser anvendelsesområdet for sertifikatet på en slik måte at det virker begrensende på utbredelsen. Lovgiver burde etter deres mening derfor legge føringer for hvilke begrensninger som kan aksepteres.

Bl.a. *NHO, Norges Eksportråd*og *Euro Info* uttaler at de støtter den løsning som er valgt, culpa med omvendt bevisbyrde, men med mulighet for utsteder til å redusere sin ansvars-eksponering etter de alminnelige erstatningsregler.

Det kan imidlertid vurderes om slik ansvarsbegrensning må fremkomme tydeligere fra utsteders side enn lovutkastet legger opp til.

Telenor uttaler at de er tilfreds med lovforslagets minimumsregulering. I den forbindelse peker de særlig på sammenhengen mellom ansvar og pris på tjenesten. Telenor mener kombinasjonen av culpa-ansvar med omvendt bevisbyrde, og *muligheten*for begrensninger i anvendelsesområde og beløpsmessige begrensninger som fremgår av sertifikatene, er en hensiktsmessig balansering av utsteders og brukernes interesser.

NHO, FNH og Sparebankforeningen savner en klarere angivelse av at sertifikatutsteder er erstatningsansvarlig etter bestemmelsen også dersom sertifikatet er utlevert til en annen person enn den hvis identitet fremgår av sertifikatet. De uttaler at å vise til § 13 om kontroll ved utlevering av sertifikat ikke nødvendigvis klargjør om utlevering til feil person faller inn under erstatningsregelen i § 22 og antar videre at dette kan presiseres i bokstav d). Videre uttaler de at utkastets bokstav e) bør formuleres noe mer presist i forhold til den situasjon som foranlediger ansvar, samt harmoniseres bedre med begrepsbruken i utkastets § 11.

Justisdepartementet påpeker at lovforslaget reiser enkelte problemstillinger i forhold til garantiansvaret som ikke er avklart i lovteksten eller i merknadene. Det er spørsmål om det skal gjelde et såkalt «dobbelt» skyldkrav i forhold til garantisten. Et dobbelt skyldkrav vil innebære at garantisten blir erstatningsansvarlig med mindre han kan bevise at verken han eller utstederen av sertifikatet handlet uaktsomt. Når bevisbyrden er snudd for skyldspørsmålet innebærer dobbelt skyldkrav at ansvaret blir enda strengere for garantisten, fordi det ikke er tilstrekkelig at han beviser at han selv ikke handlet uaktsomt - han må også bevise at utstederen ikke handlet uaktsomt for ikke å bli erstatningsansvarlig. Her er garantistens ansvar avledet av utsteders ansvar. På den annen side kan det sies at erstatningsansvaret ikke skal være strengere for garantisten enn for utstederen. Da vil det være tilstrekkelig at garantisten beviser at han selv ikke handlet uaksomt. Ut fra teksten i direktivet mener Justisdepartementet at det trolig er tilstrekkelig at garantisten ikke har handlet uaktsomt, men de anbefaler at man vurderer spørsmålet nærmere og foretar en avklaring i lovteksten og/eller i merknaden.

8.9.6 Departementets vurdering

Departementet opprettholder forslaget til en bestemmelse om at sertifikatutsteder ikke er erstatningsansvarlig dersom sertifikatet er brukt i strid med tydelige begrensninger i sertifikatets anvendelsesområde eller utover beløpsmessige begrensninger. Denne bestemmelsen er nå flyttet til tredje ledd. Det er etter departementets mening nødvendig å innta en slik bestemmelse i lovteksten for at EU-direktivet skal være korrekt implementert, jf. EU-direktivet artikkel 6 nr. 3 og 4. Departementet mener det ikke er hensiktsmessig å nærmere regulere hvilke typer av begrensninger som kan aksepteres. Dette må i utgangspunktet avtales mellom partene.

Bestemmelsen er endret noe slik at det følger av annet ledd at sertifikatutsteder er ansvarlig etter første ledd medmindre han godtgjør at han ikke handlet uaktsomt. Dette er tilnærmet identisk med ordlyden i det tidligere lovforslaget. Videre følger det av annet ledd at den som stiller garanti må godgjøre

at utstederen ikke handlet uaktsomt, eventuelt sammen med utstederen av sertifikatet. Garantisten vil ikke være ansvarlig så fremt det kan vises at verken utstederen eller garantisten handlet uaktsomt. Videre vil vanlige regler om regress kunne komme til anvendelse slik at garantisten kan få dekket eventuelle erstatningskrav av den som utstedte sertifikatet. Bakgrunnen for at departementet har valgt denne presiseringen av lovteksten, er at det skal være helt klart at den som stoler på sertifikatet skal stilles likt enten hun forholder seg til utstederen av sertifikatet eller til en som stiller garanti for sertifikatet på vegne av utstederen. Når noen har stilt garanti for et sertifikat skal brukeren for øvrig kun måtte forholde seg til garantisten.

I forhold til uttalelsene til NHO, FNH og Sparebankforeningen om at sertifikatutsteder er erstatningsansvarlig dersom sertifikatet er utlevert til en annen person enn den hvis identitet fremgår av sertifikatet, har departementet ikke funnet behov for å endre lovteksten. Det presiseres i kommentarene til lovteksten at sertifikatutsteder er erstatningsansvarlig også når sertifikatet er utlevert til feil person. Dette følger av § 22 bokstav d) som sier at sertifikatutsteder er ansvarlig for at undertegner disponerte korrekt signaturfremstillingsdata på tidspunktet da sertifikatet ble utstedt.

8.10 Rettsvirkning ved bruk av elektronisk signatur

8.10.1 Gjeldende rett

Et spørsmål som har blitt diskutert både i Norge og internasjonalt de siste årene er om en elektronisk signatur - dersom den oppfyller et visst sikkerhetsnivå - generelt skal gis samme rettsvirkning som en egenhendig underskrift.

I norsk rett er det relativt få rettsregler om at egenhendig underskrift eller lignende må brukes for at en rettslig disposisjonen skal anses gyldig. Når det gjelder forretningssituasjoner som avtale om kjøp av varer og tjenester m.m. finnes kun et begrenset antall situasjoner der norsk lovgivning krever avtale i skriftlig form undertegnet av partene. Konsekvensene av at dokumentet ikke er undertegnet vil være forskjellige. Skriftlighetskrav kan ha en informasjons- og en advarselsfunksjon. En avtale blir vanligvis ikke ugyldig om kravet ikke er oppfylt, men dette kan få betydning for rettsforholdet mellom partene. Manglende informasjon kan få betydning for partenes rettsstilling, og da slik at den som ikke har fått informasjon får en sterkere stilling. Men krav om skriftlighet kan være en gyldighetsbetingelse, f.eks. skal oppsigelse i arbeidsforhold være skriftlig og ha et nærmere angitt innhold. Oppsigelsen vil ikke kunne gjøres gjeldende mot den som er sagt opp dersom formkravene ikke er fulgt.

Selv om det ikke stilles krav om underskrift, vil et signert dokument ha en høy bevisverdi. En underskrift på et dokument kan brukes som bevis på at en person har godtatt vilkårene i dokumentet.

I et brev av 5. mai 1999 til Nærings- og handelsdepartementet vedrørende adgangen til å treffe avtaler elektronisk og beviskraften av elektroniske dokumenter, skriver Justisdepartementet følgende:

> «Vi viser til brev 23 mars 1999 fra Nærings- og handelsdepartementet der Nærings- og handelsdepartementet ber om en uttalelse om følgende spørsmål:
> 1. Er det adgang til å treffe avtale elektronisk?

2. Er det en forskjell i beviskraft mellom et elektronisk dokument og et papirdokument, selv om de har samme innhold?

Avtalefrihet, herunder formfrihet, er et sentralt prinsipp i norsk rett. Formfrihetsprinsippet innebærer at det normalt ikke gjelder formkrav for å inngå avtaler. Som utgangspunkt velger partene således selv i hvilken form de ønsker å inngå en bindende avtale, for eksempel muntlig, skriftlig eller elektronisk. Hvilken form partene velger, har i seg selv ikke betydning i forhold til at avtalen er bindende og skal holdes.

Det som særpreger en rettslig bindende avtale, er at den kan gjennomføres ved domstolenes hjelp. Hjelp til gjennomføring av en avtale fra domstolene forutsetter imidlertid at domstolen legger til grunn at en bindende avtale er inngått, noe som igjen avhenger av hva partene kan bevise for domstolene. Nettopp for å sikre bevis, velger mange å inngå avtaler på papir med underskrift fra begge parter. Et sentralt spørsmål i forhold til elektroniske avtaler er hvordan partene skal ivareta bevishensynet for disse avtalene, og dermed eventuelt sikre seg domstolenes hjelp til å få sine rettigheter etter avtalen.

Norsk sivilprosess bygger på prinsippet om fri bevisføring og fri bevisvurdering. Dette innebærer at partene i utgangspunktet kan føre ethvert bevis de finner hensiktsmessig, og at dommeren avgjør etter en samvittighetsfull prøvelse av hele saken hvilket faktum som ut fra en sannsynlighetsvurdering skal legges til grunn for pådømmelsen. Det er således ikke noe rettslig i veien for at elektroniske dokumenter legges frem som bevis for en norsk domstol. Spørsmålet er hvilken vekt domstolen vil tillegge slike dokumenter i sin bevisvurdering.

Spørsmålet om beviskraft er ikke mulig å besvare generelt ettersom den beror på den konkrete bevissituasjonen i den enkelte sak. Denne usikkerheten er imidlertid ikke særegen for elektroniske avtaler, men gjør seg også gjeldende i forhold til avtaler inngått i andre former. Beviskraften av et skriftlig dokument vil avhenge av mange forskjellige forhold, som for eksempel om det fremstår som ekte, og om det er sammenfallende eller motstridende med andre dokumenter eller bevis som finnes i saken. Det er ikke mulig å gi en uttømmende oppregning av de faktorer som spiller inn ved vurderingen av troverdigheten av et bevis. Poenget er at domstolene i en sivil sak som hovedregel skal legge til grunn det faktum som fremstår som mest sannsynlig.

I praksis vil partene i elektroniske avtaler antakelig normalt i sin bevisføring i første omgang legge frem utskrifter av de elektroniske dokumentene for domstolene. Dersom motparten ikke bestrider at utskriften gir uttrykk for et elektronisk dokument som har vært utvekslet mellom partene, er ytterligere bevisføring på dette punkt unødvendig. Dersom det skulle være behov for det, kan bevis for at tekniske sikkerhetsløsninger har vært benyttet, føres i form av f.eks. vitneutsagn eller muntlige eller skriftlige forklaringer fra sakkyndige som har foretatt en undersøkelse av dokumentet og systemet. Vi antar at utskrifter av elektroniske dokumenter i kombinasjon med sakkyndige erklæringer om at det er anvendt tekniske metoder med høy bevisverdi, vil ha stor overbevisningskraft.»

8.10.2 Implementering av direktivet

Sett i sammenheng med direktivets artikkel 1 innebærer artikkel 5 nr. 1 bokstav a) at et krav om signatur alltid vil være oppfylt av en kvalifisert elektronisk

signatur, på samme måte som en håndskreven signatur, såfremt lovgivningen åpner for at disposisjonen kan gjennomføres elektronisk. Ved å likestille kvalifisert elektronisk signatur med håndskreven underskrift skapes en felles standard for elektronisk signatur innenfor hele EØS-området.

I artikkel 5 nr. 1 bokstav b) krever direktivet at det må sikres at kvalifiserte elektroniske signaturer kan legges frem som bevis ved domstolene. I artikkel 5 nr. 2 i direktivet kreves også at elektronisk signatur, på annet nivå enn kvalifisert, ikke skal fratas rettsvirkning eller gyldighet som bevis bare på grunnlag av at signaturen er i elektronisk form, ikke er basert på et kvalifisert sertifikat, ikke er basert på et kvalifisert sertifikat utstedt av en akkreditert tilbyder eller ikke er fremstilt av et sikkert signaturfremstillingsystem. Disse bestemmelsene behøver ikke tas inn i loven da de allerede er i samsvar med gjeldende rett. Prinsippet om fri bevisføring og fri bevisvurdering innebærer at elektroniske signaturer, uansett om de er kvalifiserte eller ikke, kan legges frem som bevis for domstolene. Det forhold at signaturen ikke er kvalifisert vil antakelig ha betydning for signaturens beviskraft, men direktivet oppstiller ingen krav i forhold til beviskraften.

8.10.3 Høringsnotatet

Av informasjonshensyn nevnes det i tidligere § 5 (nå § 6 annet punktum) at også en elektronisk signatur som ikke er kvalifisert kan oppfylle eventuelle formkrav. Av første punktum følger det at om det oppstilles krav om signatur, og disposisjonen kan utføres elektronisk, vil en kvalifisert elektronisk signatur alltid oppfylle slike krav.

I henhold til det som er nevnt ovenfor er det ikke behov for å regulere at alle typer elektroniske signaturer kan legges frem som bevis. Selvfølgelig vil beviskraften være forskjellig i forhold til hvilken type elektronisk signatur som benyttes.

I høringsnotatets § 5 annet ledd (nå § 5 første ledd) gis hjemmel til å oppstille tilleggskrav ved kommunikasjon med og i offentlig sektor.

8.10.4 Høringsinstansenes syn

Statskonsult foreslår alternative formuleringer for å gjøre lovteksten mer pedagogisk. Bl.a. foreslår de et tillegg om at andre elektroniske signaturer også kan tilfredsstille krav om signatur «ut fra en konkret vurdering i det enkelte tilfelle, jf. prinsippet i norsk rett om fri bevisføring og fri bevisvurdering».

Videre etterlyser de krav om tidsstempling slik at man kan vise at signerte data ble mottatt eller at signaturen ble verifisert på et tidspunkt hvor sertifikatet stadig var gyldig. Videre uttaler de at langtidsgyldighet av elektroniske signaturer er et meget vanskelig tema, og at tidsstempling heller ikke løser alle problemer. De hevder at enhver løsning av dette problemet innebærer bruk av systemer alle parter har tiltro til, som på en eller annen måte oppbevarer spor av transaksjonen og av at partene på behørig måte har identifisert seg, f.eks. ved hjelp av kvalifiserte signaturer.

Oslo kommune anbefaler at man flytter bestemmelsen om rettsvirkninger til en egen lov i likhet med det tidligere danske forslaget.

8.10.5 Departementets vurdering

På bakgrunn av at bestemmelsen om rettsvirkninger er en sentral del av direktivet som implementeres ved denne lov, bør også dette reguleres i loven.

Departementet er enig i Statskonsults forståelse av bestemmelsen, men har kommet til at forslaget inneholder opplysninger som bør stå i kommentarer til lovteksten og ikke i selve loven, slik at denne lovteknisk blir best mulig.

Det finnes flere begrunnelser for hvorfor det ikke stilles krav om tidsstempling i forhold til elektroniske signaturers rettsvirkning. For det første er det ønskelig at loven skal være teknologinøytral. Krav om bl.a. tidsstempling vil ikke være teknologinøytralt. For det andre bør loven, i tråd med nordisk rettstradisjon, være tilnærmet lik de andre nordiske landenes lover. Verken den danske eller den svenske loven stiller krav om tidsstempling. For det tredje vil det i utgangspunktet ikke være mulig å stille tilleggskrav for en kvalifisert elektronisk signatur utover det som allerede er regulert i direktivet og ev. utdypet i forskrifter. Det eneste unntaket fra dette er at det kan stilles tilleggskrav ved kommunikasjon med offentlig sektor etter § 5. Det er derfor usikkert om det overhodet er mulig å oppstille et krav om tidsstempling i forhold til kvalifiserte elektroniske signaturers rettsvirkning.

Departementet vil ellers påpeke at bestemmelsen må ses i forhold til hvorvidt det generelt er adgang til å kommunisere elektronisk innen det enkelte rettsområde. Det tidligere omtalte «Kartleggingsprosjektet», se kapittel 4.3, innebærer en gjennomgang av rettslige hindringer for elektronisk kommunikasjon. Det vil bli fremsatt forslag til løsninger på de hindringene som avdekkes i regi av prosjektet. Det er derfor ikke naturlig å oppstille en særskilt gjennomgang av dette her.

Departementet vil presisere følgende angående forholdet mellom begrensninger i sertifikatets anvendelsesområde og signaturenes rettsvirkninger: Et kvalifisert sertifikat kan være begrenset i forhold til beløp eller type transaksjon, jf. § 4 annet ledd bokstav i) og j). Normalt vil disse begrensningene oppstilles der undertegner handler på vegne av en annen, f.eks. som ansatt i et selskap. Selve signaturens rettsvirkning vil ikke påvirkes av at undertegner har gått utover disse begrensningene. Det kan ikke bestrides at dokumentet er blitt signert av undertegner. Derimot kan bl.a. fullmaktsbestemmelsene i avtaleloven være aktuelle. Av disse bestemmelsene følger det bl.a. at dersom en fullmektig har handlet utenfor fullmakten vil fullmaktsgiver ikke være bundet av kontrakten. Fullmektigen må imidlertid holde tredjemann skadesløs.

Bestemmelsen er flyttet til § 6, mens hjemmelen til å oppstille tilleggskrav ved kommunikasjon med og i offentlig sektor står i § 5.

8.11 Tilleggskrav ved kommunikasjon med og i offentlig sektor

8.11.1 Innledning

Kongen gis i forslaget hjemmel til å regulere bruk av elektroniske signaturer ved kommunikasjon med og i offentlig sektor. Bestemmelsen bygger på direktivets artikkel 3 nr. 7 som sier at det kan stilles supplerende krav til elektroniske signaturer som skal brukes ved kommunikasjon med og i offentlig sektor. Videre stiller direktivet krav til at innholdet i disse tilleggskravene skal

være objektive, klare, forholdsmessige, ikke-diskriminerende og at de skal stilles i forhold til det aktuelle anvendelsesområdet og de spesielle behov som her gjør seg gjeldende.

Regjeringen har oppnevnt et utvalg som skal utrede forslag til policy for bruk av digital signatur med tilhørende infrastruktur i offentlig sektor. Utvalgets forslag skal danne grunnlag for slik fremtidig regulering, jf. kapittel 4.5.

En forskrift om elektronisk kommunikasjon med forvaltningen kan tenkes forankret i forvaltningsloven. Den aktuelle hjemmelen i lov om elektroniske signaturer kan, innenfor rammen av en slik forskrift, brukes til å gi nærmere bestemmelser om hvilke typer av elektroniske signaturer som skal benyttes innen offentlig sektor og i kommunikasjon mellom offentlig sektor og brukere. Hjemmelen omfatter krav som kan stilles til den elektroniske signaturen, sertifikatutsteder og de produkter og systemer som skal benyttes.

8.11.2 Høringsnotatet

I høringsnotatet er hjemmelen utformet som et annet ledd i den tidligere § 5 om rettsvirkninger.

8.11.3 Høringsinstansenes syn

Arbeids- og administrasjonsdepartementet uttaler i høringsuttalelsen at hjemmelen er plassert feil i loven og at den også har en feil i ordlyden. Videre uttaler Arbeids- og administrasjonsdepartementet:

> «Det finnes imidlertid behov for regulering av elektronisk kommunikasjon med forvaltningen, der det kan oppstilles nærmere regler for hvordan slik kommunikasjon skal foregå, for å kunne godtas som gyldig henvendelsesmåte til og fra forvaltningen i ulike saker. Dette kan omfatte forhold som signering, autentisering, tidfesting, kunngjøring av vedtak, frister og deres etterlevelse mv. Bruk av elektroniske signaturer hører hjemme her. Krav til sertifikatutstedere hører derimot hjemme i Lov om elektroniske signaturer.»

Statskonsult uttaler at slik lovutkastet er formulert i høringsnotatet, ser det ut som det er fritt frem til å gi generelle regler på et meget bredt område, mens det i direktivets artikkel 3 nr. 7 er presisert bedre og gjort avhengig av at de nevnte kriteriene må følges. Videre mener de at utkastets formulering «med og i offentlig sektor» bør revurderes i forhold til direktivets «in the public sector», som virker som en snevrere formulering. Videre uttaler Statskonsult at det kunne være mer naturlig å plassere en ev. slik hjemmel i forvaltningsloven.

I sin høringsuttalelse viser *Rikstrygdeverket* til særlige behov for sikkerhet ved samhandling med Trygdeetaten som følge av at de forvalter store midler og mange sensitive opplysninger. Dette er forhold som naturlig bør vurderes ved en eventuell anvendelse av forskriftshjemmelen.

Norges Rederiforbund uttaler at adgangen til å bruke elektronisk signatur bør være så vid og generell som mulig og at kommunikasjon mellom det offentlige og private bør behandles på samme måte som kommunikasjon mellom private. Videre ser de at det på enkelte områder foreligger særlige hensyn som krever en annen sikkerhetsgrad. Norges Rederiforbund forutsetter at slike unntak kun innføres på områder der det er et sterkt behov og at unntakene begrunnes særskilt.

Skattedirektoratet peker på behovet for utarbeidelse av et lite antall sertifikatpolicies som kan møte ulike behov for sikkerhet. De viser til at dette er viktig for å få ivaretatt nødvendige samordningsbehov, som etatenes behov for frihet til å velge de rimeligste, tilstrekkelig sikre, løsninger.

8.11.4 Departementets vurdering

Departementet har tatt Arbeids- og administrasjonsdepartementets synspunkt om at forskriftshjemmelen bør flyttes til følge. Bestemmelsen regulerer kommunikasjon med og i offentlig forvaltning som ikke behandles i noen andre bestemmelser i loven. Departementet finner det derfor mest naturlig at hjemmelen reguleres i en egen paragraf, i nær tilknytning til bestemmelsen som oppstiller krav til kvalifiserte signaturer og bestemmelsen om rettsvirkninger. Forskriftshjemmelen gis i en ny § 5.

Departementet er ikke enig i Arbeids- og administrasjonsdepartementets vurdering om at innholdet i bestemmelsen bør endres, da hjemmelen ikke bare gir adgang til at man kan oppstille andre krav til sertifikatutstedere, men generelt andre krav til signaturen. Videre er departementet ikke enig i Statskonsults uttalelse om at hjemmelen bør plasseres i forvaltningsloven. Bestemmelsen gir anledning til å stille tilleggskrav i forhold til øvrige bestemmelser regulert av loven her. Det er dermed mer oversiktlig og gir større forutberegnelighet for sertifikatutstederne at hjemmelen står i loven som regulerer rammevilkårene for sertifikatutstedernes virksomhet for øvrig.

Departementet slutter seg til Statskonsults uttalelse om at direktivet legger føringer for hvordan tilleggskravene skal utformes. Kravene som oppstilles i direktivet må gjelde tilsvarende, slik at eventuelle tilleggskrav må være objektive, klare, forholdsmessige og ikke-diskriminerende, og de skal stilles i forhold til det aktuelle anvendelsesområde og de spesielle behov som her gjør seg gjeldende. Det må altså vurderes særskilt i forhold til det aktuelle anvendelsesområde hvorvidt det er nødvendig med tilleggskrav, ut fra særlige behov som der gjør seg gjeldende.

8.12 Straff

8.12.1 Høringsnotatet

Høringsnotatet inneholder et forslag til en bestemmelse om straffeansvar for overtredelse av nærmere angitte bestemmelser når overtredelsen er forsettelig eller grovt uaktsom. Bestemmelsen suppleres av alminnelige strafferettslige prinsipper. I høringsnotatet er det foreslått at medvirkning straffes på samme måte, og dessuten at Kongen i forskrift kan fastsette at overtredelser i eller i medhold av loven kan straffes med bøter.

8.12.2 Høringsinstansenes syn

NHO, FNH, Sparebankforeningen og *Justisdepartementet* uttaler at hvilke bestemmelser som er straffesanksjonerte bør fremgå av lovteksten.

Justisdepartementet påpeker at forskriftshjemmelen i tredje ledd kan komme i konflikt med Grunnloven § 96 da utgangspunktet er at straff krever hjemmel i formell lov, mens angivelsen av gjerningsinnholdet *kan* reguleres

i forskrift. I utgangspunktet vil da bestemmelsen i tredje ledd være i strid med Grunnloven § 96. Justisdepartementet påpeker at et unntak fra dette følger av straffeloven § 339 nr. 2, hvoretter overtredelse av bestemmelser i en forskrift kan straffes med bøter når hjemmelen for å straffe følger av forskriften. Imidlertid ser ikke Justisdepartementet noen praktiske grunner som tilsier en slik ordning.

NTNU uttaler at det bør gjøres straffbart å unnlate å følge opp offentliggjøring av rutiner som nevnt i § 13 annet ledd.

Barne- og familiedepartementet gjør oppmerksom på at utstedere av kvalifiserte sertifikater, som i virkeligheten ikke er kvalifiserte, vil kunne rammes av markedsføringslovens sanksjonsbestemmelser, jf. §§ 2 og 17.

8.12.3 Departementets vurdering

Departementet er enig i at det i loven bør tas stilling til hvilke bestemmelser som kan straffesanksjoneres og endrer lovforslaget i tråd med dette. Det følger av lovforslagets § 21 at forsettlig eller grovt uaktsom overtredelse av § 18 eller unnlatelse av å gi opplysninger etter § 17 kan straffes med bøter. Likedan kan behandling av personopplysninger i strid med §§ 7 og 14 og oppgivelse av uriktige eller villedende opplysninger til tilsynet straffes med bøter.

9 Akkreditering og sertifisering

9.1 Høringsnotatet

Det følger av direktivet at medlemsstatene kan innføre frivillige akkrediteringsordninger for sertifikatutstedere på et «høyere» nivå, dvs. for kvalifiserte sertifikater. Direktivet oppstiller en del generelle krav til utstedere av kvalifiserte sertifikater i vedlegg II. Det er i dag ikke utviklet standarder eller stabile operasjonelle kriterier som dekker alle de kravområder som vedlegg II angir. Det er derfor vanskelig å etablere en total ordning for akkreditering av utstedere av kvalifiserte sertifikater.

I rapporten «Elektroniske signaturer - Myndighetsroller og regulering av sertifikattjenester» anbefales det ikke at myndighetene tar initiativ til etablering av en akkreditert sertifiseringsordning nå, men det anbefales bruk av de ordningene for sertifisering av IT-sikkerhet som allerede er etablert eller under etablering. Departementet er enig i denne vurderingen og overlater det på det nåværende tidspunkt til markedet å vurdere hvorvidt det skal opprettes frivillige akkrediteringsordninger. På den annen side oppfatter departementet det som positivt dersom slike ordninger benyttes eller opprettes.

9.2 Høringsinstansenes syn

Justervesenet mener det er verdt å vurdere å etablere en mer spesifikk, frivillig ordning basert på akkreditering og å notifisere denne i henhold til direktivets artikkel 11 for anerkjennelse av elektroniske signaturer over landegrensene.

Arbeids- og administrasjonsdepartementet er uenig i konklusjonene fra rapporten fra «Elektroniske signaturer - Myndighetsroller og regulering av tilbyder av sertifikattjenester», der det ikke anbefales noen myndighetsinitiativ på området. De uttaler at de, ut fra et brukerperspektiv, ser nytten av og behovet for frivillige godkjenningsordninger for leverandører av digitale sertifikater, uavhengig av om de er kvalifiserte eller ikke. På nåværende tidspunkt mener de imidlertid at det ikke er formålstjenlig å anbefale opprettelsen av en akkreditert sertifiseringsordning for godkjenning av sertifikatutstedere. De ser imidlertid behov for en godkjenningsordning, som kan gi sertifikatutstederne et «stempel» som indikerer kvalitet på tjenesten som leveres uavhengig av «kvalifisert»-tankegangen.

9.3 Departementets vurdering

Departementet er langt på vei enig i uttalelsene fra Arbeids- og administrasjonsdepartementet. Departementet er av den oppfatning at det i forhold til dagens marked er for tidlig å ta initiativ til etablering av en akkreditert sertifiseringsordning fra myndighetenes side. På den annen side anbefaler departementet bruk av de ordningene for sertifisering av IT-sikkerhet som allerede er etablert eller under etablering. På det nåværende tidspunkt vil det således

være opp til markedet hvorvidt de vil opprette frivillige sertifiserings-/akkrediteringsordninger.

Departementet vil følge utviklingen på markedet nøye i forhold til hvorvidt det vil bli aktuelt med et fremtidig initiativ til opprettelse av frivillige sertifiserings-/akkrediteringsordninger. Se også kapittel 8.7.2 om valg av tilsynsmodell.

10 Internasjonale forhold

10.1 Innenfor EØS-området

Det følger av EU-direktivet at dersom det oppstilles krav om signatur vil en kvalifisert elektronisk signatur alltid oppfylle et slikt krav, så fremt disposisjonen kan gjennomføres elektronisk (jf. artikkel 5). Dette gjelder også når signaturen baseres på et sertifikat som er utstedt av en sertifikatutsteder fra et annet land innenfor EØS-området. Dette betyr at en nasjonal domstol skal behandle sertifikater og signaturer på samme måte, uansett om disse kommer fra en nasjonal sertifikatutsteder eller en utsteder innenfor EØS-området. I det enkelte medlemsland kan det offentlige likevel kreve at man bruker en signatur med høyere sikkerhet enn en kvalifisert elektronisk signatur.

EU-direktivet artikkel 4 om prinsipper vedrørende det indre marked skal sikre fri bevegelighet innen det indre marked og inneholder direktivets ikkediskrimineringsregel. Ifølge bestemmelsen kan det ikke stilles ytterligere krav til kvalifiserte sertifikater fra utstedere etablert i et annet EØS-land. Medlemslandene skal også sikre fri bevegelighet innen det indre marked for elektroniske signaturprodukter som overholder kravene i direktivet. En beslutning fra et organ i et medlemsland om å godkjenne et signaturfremstillingssystem som sikkert etter § 9, skal dermed automatisk godkjennes av samtlige medlemsland. Artikkel 4 nr. 1 er implementert i lovforslaget § 25 første ledd.

10.2 Utenfor EØS-området

I henhold til direktivets artikkel 7 skal kvalifiserte sertifikater utstedt av sertifikatutstedere etablert i land utenfor EØS-området gis rettslig anerkjennelse på lik linje med kvalifiserte sertifikater fra utstedere innen EØS-området, når disse i tillegg har en nærmere tilknytning. Denne tilknytningen oppfylles ved at sertifikatutstederen er sertifisert i et medlemsland, er kryssertifisert av en annen utsteder innen EØS-området som utsteder kvalifiserte sertifikater eller omfattes av en multi- eller bilateral avtale. Denne bestemmelsen er implementert i lovforslaget § 25 annet ledd.

11 Innsamling og bruk av personopplysninger

11.1 Innledning

Europaparlamentets og rådets direktiv 95/46/EG av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, vil bli implementert i norsk rett ved lov om behandling av personopplysninger (personopplysningsloven). Lovforslaget inneholder bestemmelser om når behandling av personopplysninger kan skje.

Ifølge personopplysningsloven kan personopplysninger bare behandles dersom den registrerte har gitt sitt samtykke til behandlingen, eller dersom behandlingen er nødvendig av nærmere angitte grunner. Personopplysninger som behandles må bare nyttes til uttrykkelige formål som er saklig begrunnet i den behandlingsansvarliges virksomhet, og må ikke brukes til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker. Behandlingsansvarlig skal dessuten sørge for at personopplysningene som behandles er tilstrekkelige og relevante for formålet med behandlingen.

Dette lovforslagets § 7 regulerer sertifikatutsteders innhenting av personopplysninger og utfylles av personopplysningslovens regler. Der lovforslaget ikke selv inneholder særregler for behandling av personopplysninger, vil personopplysningsloven komme til anvendelse. Således vil f.eks. personopplysningsloven § 31 om meldeplikt gjelde også her.

11.2 Høringsnotatet

I § 6 (nå § 7) i dette lovutkastet fastslås det at en sertifikatutsteder kun får innhente personopplysninger direkte fra den som opplysningene gjelder eller med dennes uttrykkelige samtykke, og bare i den utstrekning det er nødvendig for å utstede et sertifikat. Dette er en direkte implementering av artikkel 8 nr. 2 i direktivet, og oppstiller således noe strengere krav enn de som stilles i forslaget til personopplysningsloven.

Med samtykke menes en frivillig, uttrykkelig og informert erklæring fra undertegner om at han eller hun godtar behandling av opplysning om seg selv. Dette er i samsvar med hvordan «samtykke» defineres i forslaget til personopplysningsloven.

Det skal bemerkes at bestemmelsen i § 6 (nå § 7) omfatter alle som utsteder sertifikater. Bestemmelsen retter seg til alle sertifikatutstedere på lik linje, uavhengig av om de utsteder kvalifiserte sertifikater eller ei. Bestemmelsen ble i høringsnotatet omtalt som «databeskyttelse». Datatilsynet vil i henhold til forslaget til lov om personopplysninger få til oppgave å sikre at personopplysningsloven etterleves.

11.3 Høringsinstansenes syn

Arbeids- og administrasjonsdepartementet uttaler at dersom informasjon skal kreves direkte fra den det gjelder, vil dette skape problemer i forbindelse med masseutstedelse av sertifikater til ansatte. Videre uttaler de at ordlyden i bestemmelsen bør harmoniseres med den nye personopplysningsloven.

Sosial- og helsedepartementet uttaler at dersom det er Datatilsynet som skal føre tilsyn med at utstedere av ikke-kvalifiserte sertifikater etterlever § 7 bør dette komme tydeligere frem, enten i lovteksten eller i motivene.

Telenor uttaler at personvern og databeskyttelse etter deres syn er sentralt for å skape tillit til sertifikattjenester. En *streng*praktisering av bestemmelsen kan *muligens* gjøre utstedelse av sertifikater mer arbeidskrevende for brukerne. Dette er noe som kan bremse utbredelsen.

*Justisdepartementet, Datatilsynet*og *Statskonsult* foreslår at tittelen til lovbestemmelsen endres.

Post- og teletilsynet har oppfattet det dithen at tilsynet vil være myndighet også for lovens bestemmelse om personopplysninger hva angår utstedere av kvalifiserte sertifikater, men at Datatilsynet vil være tilsynsmyndighet mht. til de øvrige utstederne. Post- og teletilsynet mener det er behov for at denne kompetansedelingen presiseres, og at forholdet mellom de to tilsynene bør være gjenstand for nærmere regulering i § 7.

11.4 Departementets vurdering

Bestemmelsens tittel er endret til «Innsamling og bruk av personopplysninger«.

Departementet har vurdert valg av tilsyn med innhenting av personopplysinger etter lovforslagets § 7 og kommet til at det er lite hensiktsmessig å dele tilsynet mellom Post- og teletilsynet, hva angår utstedere av kvalifiserte sertifikater, og Datatilsynet, hva angår øvrige utstederne. En slik deling av tilsynsoppgavene vil være lite oversiktlig for markedet. Videre ser departementet det som uheldig om bestemmelsen skulle håndheves ulikt overfor utstedere av forskjellige sertifikater av den grunn at ulike organ førte tilsyn med virksomheten.

Departementet har kommet til at Datatilsynet bør være tilsyn i forhold til bestemmelsen om innsamling og bruk av personopplysninger. Datatilsynet fører kontroll med personopplysninger iht. personopplysningsloven. Innholdet i lovforslagets § 7 avviker i liten grad fra innholdet i personopplysningsloven. Videre må sertifikatutstederne ha konsesjon for opprettelse av personregistre av Datatilsynet. Datatilsynet vil således få oversikt over samtlige utstedere av sertifikater. En nærmere avgrensning av tilsynets oppgaver kan gjøres i forskrift med hjemmel i § 17 sjette ledd.

12 Melding til EFTAs overvåkingsorgan

Statene skal informere hverandre og EFTAs overvåkingsorgan om hvilket akkrediteringsystem (sertifiseringssystem) som brukes, navn på akkrediteringsorgan, tilsynsorgan og organ som avgjør hvorvidt sikre signaturfremstillingssystem oppfyller lovens krav, samt navn på samtlige akkrediterte sertifikatutstedere, jf. artikkel 11 i direktivet.

13 Behov for revisjon av loven

Loven regulerer et forholdsvis nytt teknisk område hvor utviklingen skjer raskt. Det kan antas at nye tjenester fortløpede vil bli presentert, basert på nye tekniske muligheter og i henhold til kundenes krav og behov. På denne bakgrunn vil det være behov for å revidere loven i takt med utviklingen på området. Dette gjelder bl.a. behovet for å se om kvalifiserte sertifikater blir tatt i bruk. Dersom markedet ikke ønsker kvalifiserte sertifikater, bør tilsynets virksomhet vurderes. Behovet for å revidere reguleringen er også blitt identifisert i direktivet. I artikkel 12 i direktivet står det at Kommisjonen skal vurdere behovet for å justere direktivet. En slik vurdering skal baseres på den tekniske utviklingen, endringer innenfor markedet og endrede rettslige rammebetingelser. Innen tre og et halvt år etter at direktivet har trådt i kraft skal Kommisjonen avgi rapport vedrørende dette til det Europeiske Parlamentet og Rådet.

14 Økonomiske og administrative konsekvenser

I henhold til lovforslaget skal det etableres en obligatorisk tilsynsordning for utstedere av kvalifiserte sertifikater. Post- og teletilsynet utpekes som tilsynsorgan.

Tilsynsordningen er nærmere beskrevet under kapittel 8.7 hvor det fremgår at det legges opp til en relativt lite inngripende tilsynsordning. Ordningen går ut på at tilbydere av kvalifiserte sertifikater skal registrere seg hos tilsynet og selv deklarere at de oppfyller kravene til kvalifiserte sertifikater. Tilsynet kan så kreve mer informasjon på eget initiativ eller etter «tips» fra andre.

De nye tilsynsoppgavene vil medføre økte kostnader for Post- og teletilsynet. De må bygge opp kompetanse på området og sannsynligvis ansette nytt personell for å utføre oppgavene. Post- og teletilsynet antar at tilsynsvirksomheten vil sysselsette to årsverk. Videre vil det være kostnader forbundet med å opprette et nytt register over de utstederne som omfattes av tilsynet. Post- og teletilsynet antar at de vil ha minimumskostnader på ca. kr 500 000,- uavhengig av om noen sertifikatutstedere skulle registrere seg eller ikke. Om man antar at 5 utstedere skulle registrere seg, anslår Post- og teletilsynet de årlige kostander til nærmere 2 mill. kr. Det er for øvrig vanskelig å anslå tilsynets kostnader før tilsynets oppgaver er nærmere fastlagt i forskrift.

Post- og teletilsynet er i dag selvfinansiert. I utgangspunktet bør tilsynet finansieres på samme måte som resten av virksomheten. Det å utstede sertifikater er imidlertid en ny type virksomhet i et helt nytt marked. Det vil da være en særlig økonomisk risiko forbundet med å tre inn i dette markedet. Denne risikoen blir forsterket dersom utstederne møtes av økonomiske barrierer i form av høye registreringsgebyrer, tilsynsavgifter og lignende. Regjeringen ønsker å avhjelpe disse problemene i en startfase for å bidra til mer utstrakt bruk av elektroniske signaturer. Dette kan gjøres ved at gebyrene suppleres med et tilskudd fra staten.

Ved å gi et slikt tilskudd i en overgangsfase antar departementet at gebyrene kan holdes på et stabilt nivå fremover slik at de første sertifikatutstederne ikke blir økonomisk straffet for å være tidlig ute. Videre vil tilskuddet bidra til å holde prisene på de elektroniske signaturene med tilhørende sertifikater på et moderat nivå, slik at tjenesten kan bli tatt i bruk av flere på et tidlig tidspunkt.

Regjeringen foreslår at det bevilges et tilskudd til Post- og teletilsynet til dekning av kostander forbundet med opprettelsen av tilsynet. Dette tilskuddet kan dekkes innenfor gjeldende budsjettrammer.

Datatilsynet vil ifølge forslaget håndheve lovens bestemmelse om personvern. Dette er i prinsippet ingen utvidelse av de arbeidsoppgaver Datatilsynet allerede har.

15 Merknader til de enkelte bestemmelsene

Kapittel I Alminnelige regler

Til § 1 Lovens formål

Bestemmelsen fastsetter lovens formål og følger opp direktivets målsettinger om å fremme en sikker bruk av elektronisk signatur. Lovforslaget innebærer en minimumsregulering av krav som stilles til elektroniske sertifikater med et nærmere fastlagt sikkerhetsnivå som omtales som kvalifisert, til sertifikatutstedere og til sikre signaturfremstillingssystem. Lovforslaget skal dermed sikre at det på markedet er produkter og sertifikatutstedere som oppfyller en rekke krav som skal gjøre dem sikre å bruke.

Det ville ikke være hensiktsmessig å regulerer alle typer elektroniske signaturer og tilhørende sertifikater i denne loven. Det er derfor frivillig hvorvidt en sertifikatutsteder ønsker å tilby kvalifiserte sertifikater som reguleres av dette lovforslaget, eller om de vil tilby sertifikater på et annet sikkerhetsnivå og dermed falle utenfor dette regimet.

Til § 2 Lovens virkeområde

Bestemmelsen angir saklig og geografisk virkeområde for lovforslaget. Det følger av *første ledd* at loven gjelder sertifikatutstedere som er etablert i Norge. Det stilles ikke krav til utstedere som er etablert i andre land. Bestemmelsen gjennomfører dermed artikkel 4 i direktivet som bl.a. fastsetter at hvert medlemsland skal anvende nasjonale bestemmelser vedtatt i henhold til direktivet på utstedere etablert på deres territorium. Forholdet til sertifikater fra utstedere etablert i andre land reguleres i § 25.

Loven gjelder i hovedsak sertifikatutstedere som tilbyr kvalifiserte sertifikater. Sertifikatutstederne faller dermed utenfor lovens område ved å tilby sertifikater på et annet sikkerhetsnivå eller ved ikke å kalle sine sertifikater for kvalifiserte. Sertifikatutstedere kan ikke utstede kvalifiserte sertifikater før de har sendt registreringsmelding til tilsynet. For å falle inn under denne lovreguleringen må sertifikatutstederen altså registrere seg hos tilsynet etter lovforslaget § 18, slik at utstederen omfattes av tilsynet.

To av lovens bestemmelser gjelder alle elektroniske signaturer og elektroniske sertifikater. Dette er nærmere presisert i første ledd hvor det fremgår at § 6 annet punktum og § 7 gjelder alle elektroniske signaturer og sertifikatutstedere.

Annet ledd gir Kongen kompetanse til å bestemme at loven helt eller delvis skal gjelde for Svalbard og Jan Mayen.

Til § 3 Definisjoner

Bestemmelsen bygger på direktivets artikkel 2 og definerer en del begreper som er sentrale i lovforslaget. Kvalifisert sertifikat og sikkert signaturfremstillingssystem er definert i en egne paragrafer, henholdsvis §§ 4 og 8.

Nr. 1 definerer elektronisk signatur. Lovforslaget er basert på prinsippet om teknologinøytralitet. Elektronisk signatur skal omfatte alle former for elek-

troniske autentiseringsmetoder og er således et svært vidt begrep. Definisjonen stiller krav om at signaturen skal kunne bekrefte hvem som er undertegner. Denne funksjonen omtales som autentisering.

Den mest utbredte elektroniske signaturteknologien i dag er den såkalte digitale signaturen som er basert på et system med en privat og en offentlig signaturnøkkel (i direktivet benevnt som henholdsvis signaturfremstillingsdata og signaturverifikasjonsdata). Videre omfatter lovforslaget andre elektroniske systemer som er beregnet til identifikasjon av brukeren som f.eks. koder og biometriske verdier. Elektronisk og digital signatur er nærmere forklart i kapittel 3.1.

Nr. 2 definerer avansert elektronisk signatur. Definisjonen omfatter det man i dag kaller en digital signatur, jf. kapittel 3.1, men er i prinsippet noe videre slik at den også skal kunne omfatte andre fremtidige teknikker. Den avanserte elektroniske signaturen skal ifølge bokstavene a) og b) sikre autentisering av undertegner ved at avsender knyttes til meldingens innhold og at signaturen identifiserer undertegner. Dette bidrar dessuten til å sikre at avsender ikke senere kan nekte for å ha sendt dokumentet. Funksjonen kalles ikke-benekting. Uttrykket «kan identifisere undertegneren» i b) innebærer et krav om at den avanserte signaturen faktisk skal kunne identifisere undertegner. Dette er altså ikke å forstå som en valgfri mulighet. Det er ikke hensiktsmessig å spesifisere i lovteksten hva som kreves for at undertegner er identifisert. Dette vil kunne endre seg ved f.eks. at det kan åpnes for at personnummer kan brukes. Videre skal avsender ifølge bokstav c) kunne ha kontroll over midlene signaturen er laget ved hjelp av. Da reduseres faren for at en tredjemann skal kunne bruke signaturen urettmessig. Dessuten betyr dette at en avansert elektronisk signatur ikke skal anvendes av flere personer. Kravet i bokstav d) skal sikre dokumentets integritet, dvs. at man kan være sikker på at inneholdet i det signerte dokumentet ikke har blitt forandret på vei til mottaker.

*Nr. 3*definerer kvalifisert elektronisk signatur, som særlig er relevant for bestemmelsen om elektroniske signaturers rettsvirkninger, jf. § 6.

Nr. 4 definerer undertegner, som er den fysiske personen som signerer dokumentet elektronisk. «Undertegner» omfatter ikke en person som urettmessig har tilegnet seg et signaturfremstillingssystem, men den som i sertifikatet er utpekt som undertegner. Signaturen og nødvendige signaturfremstillingssystem og data kan imidlertid eies av noen andre, typisk en arbeidsgiver, men disponeres av undertegner. Undertegner kan således handle på vegne av andre fysiske eller juridiske personer. Her kommer vanlige regler om fullmakt mv. til anvendelse.

*Nr. 5*definerer hva som forstås med signaturfremstillingsdata. Signaturfremstillingsdata er de data som anvendes til å frembringe den elektroniske signaturen. I den digitale signaturteknologien kalles signaturfremstillingsdata for den private nøkkelen.

I *nr. 6*fastlegges hva som forstås med et signaturfremstillingssystem. Et signaturfremstillingssystem er det systemet som brukes til å lage den elektroniske signaturen. Signaturfremstillingssystemet anvender signaturfremstillingsdataene til å fremstille signaturen. Systemet kan være både programvare og maskinvare. En mulig maskinvareløsning er for eksempel signaturfremstil-

lingsdata lagret på et såkalt smartkort (en chip på et plastkort). En programvarebasert løsning vil typisk være en del av et elektronisk post-program i en datamaskin.

*Nr. 7*definerer signaturverifikasjonsdata. Dette er de data som brukes til å verifisere at meldingen fra avsender er «ekte», dvs. den offentlige delen av nøkkelparet jf. kapittel 3.1.

Nr. 8 fastsetter hva som forstås med et signaturverifikasjonssystem. Det er et produkt, programvare eller maskinvare, som brukes til å verifisere den elektroniske signaturen ved å anvende signaturverifikasjonsdata, eller den offentlige nøkkelen.

I *nr.9* defineres et sertifikat. Sertifikatet knytter signaturverifikasjonsdata til et entydig navn og er således en kopling mellom disse. Sertifikatet inneholder med andre ord opplysninger om hvem som er undertegner. Undertegneren er den personen som disponerer et signaturfremstillingssystem, jf. ovenfor, og som regel den som inngår en avtale med en sertifikatutsteder om utstedelse av et sertifikat. Se mer om dette i kapittel 3.3. I § 4 oppstilles kravene til et kvalifisert sertifikat.

I *nr. 10* defineres en sertifikatutsteder. Benevnelsen brukes om en rekke funksjoner som sertifikatutstederen kan oppfylle. Disse tjenestene kan imidlertid utstederen også helt eller delvis sette bort til andre, av den grunn står det i definisjonen «eller tilbyr...».

Kjernefunksjonen for en sertifikatutsteder er å garantere sammenhengen mellom undertegner og opplysningene i sertifikatet. Ved å bruke sikre rutiner ved innhenting av opplysninger og utstedelse av sertifikater sikres koplingen mellom person og opplysningene i sertifikatet. Denne garantien manifesteres ved at sertifikatet signeres av utstederen. Det vil på den måten fremgå av sertifikatet hvem som har utstedt det, og denne utstederen er ansvarlig i forhold til erstatningsbestemmelsen i § 22.

Andre sentrale tjenester en sertifikatutsteder kan tilby selv, eller sette ut til andre, er identitetskontroll, tildeling av navn, katalog- og tilbaketrekkingstjenester. Dersom andre utfører tjenester på vegne av sertifikatutsteder må også de oppfylle kravene loven stiller til den aktuelle tjenesten. Videre står utstederen fritt til å tilby en rekke relaterte tjenesteytelser, f.eks. valideringstjenester, tidsstempling, arkivering eller konsulenttjenester i forbindelse med elektroniske signaturer. Begrepet «tjenester relatert til elektronisk signatur» er et dynamisk begrep som skal tolkes i lys av utviklingen i markedet. Også av hensyn til at begrepet i størst mulig grad skal være teknologinøytralt er det ikke hensiktsmessig å avgrense begrepet nærmere.

Til § 4 Kvalifisert sertifikat

Bestemmelsen oppstiller krav til et sertifikat med et bestemt sikkerhetsnivå og bygger på direktivets definisjon av et kvalifisert sertifikat i artikkel 2 nr. 10 og vilkårene som oppstilles til slike sertifikater i direktivets vedlegg I. Det følger av lovforslagets system at det må anvendes et kvalifisert sertifikat for at reglene om erstatning og enkelte sider ved rettsvirkningene skal komme til anvendelse. Kravene til et kvalifisert sertifikat er dermed minimumskrav som må være oppfylt for at hoveddelen av bestemmelsene i denne lov skal komme til anvendelse. Dette fremgår av *første ledd*.

Det følger av *annet ledd bokstav a)* at det skal fremgå direkte av sertifikatet hvorvidt det er kvalifisert eller ikke. Det er ikke tilstrekkelig med en henvisning til et annet dokument, for eksempel en sertifikatpolicy, hvor dette fremgår.

Annet ledd bokstav b) slår fast at det skal fremgå av sertifikatet hvilken utsteder som har utstedt det. Det er denne sertifikatutstederen som er erstatningsansvarlig i henhold til § 22 så fremt ingen annen har garantert for sertifikatet.

Annet ledd bokstav c) oppstiller krav om at undertegners navn eller pseudonym skal fremgå av sertifikatet. Dersom et pseudonym er benyttet skal dette alltid fremgå av sertifikatet. Om bruk av pseudonym, se nærmere kapittel 8.5.

Annet ledd bokstav d) krever at sertifikatet inneholder ytterligere opplysninger om undertegneren. Hva som anses som relevante opplysninger avhenger av formålet med sertifikatet. Er det f.eks. tale om et sertifikat som bare skal brukes til kommunikasjon med et forsikringsselskap, kan det være hensiktsmessig å la sertifikatet inneholde undertegners polisenummer. I hovedsak vil disse ytterligere opplysningene være opplysninger som er nødvendige for å sikre en entydig identifikasjon av undertegner.

Annet ledd bokstav e) krever at det kvalifiserte sertifikatet inneholder de signaturverifiseringsdata som korresponderer med undertegnerens signaturfremstillingsdata. I den digitale signatur-teknologien innebærer dette at sertifikatet må inneholde den offentlige nøkkelen som korresponderer til undertegners private nøkkel. Ved å stille et slikt krav vil det være mulig for mottakere å kontrollere den elektroniske signaturen umiddelbart etter mottakelsen av dokumentet, så lenge mottaker har nødvendig teknisk utrustning. Mottaker slipper å måtte henvende seg til sertifikatutstederen eller noen andre for å få tilgang til signaturverifikasjonsdataene.

Ifølge *annet ledd bokstav f)* kreves det at et kvalifisert sertifikat inneholder ikrafttredelse- og utløpsdato. Det må imidlertid være opp til markedet å nærmere bestemme hvor lenge et sertifikat skal være gyldig. Det må bl.a. tas hensyn til den raske tekniske utviklingen på området.

Annet ledd bokstav g) krever at et kvalifisert sertifikat skal inneholde en unik identifikasjonskode, et såkalt referansenummer. Det skal således være mulig å identifisere sertifikatet entydig.

Annet ledd bokstav h) krever at sertifikatet er undertegnet med sertifikatutstederens avanserte elektroniske signatur. Av dette vil det fremgå hvilken sertifikatutsteder som utstedte det, og det sikres at sertifikatet ikke kan endres uten at det oppdages.

Annet ledd bokstav i) og j) gir sertifikatutsteder mulighet til å fastsette anvendelses- og beløpsmessige begrensninger for bruken av sertifikatet. Når en sertifikatutsteder fastsetter slike begrensninger for bruken av sertifikatet skal dette fremgå av sertifikatet. Eventuelle begrensninger i sertifikatets bruksområde må umiddelbart fremstå for en tredjemann dersom denne skal kunne ha tillit til den elektroniske signaturen. Det kreves derfor at slike begrensninger fremgår *direkte av sertifikatet.* Her må man imidlertid være klar over at hvordan programvaren er installert kan ha betydning for hvordan informasjonen fremgår, selv om informasjonen finnes i sertifikatet.

Bestemmelsen må ses i sammenheng med bestemmelsen om erstatningsansvar, hvor det fremgår at sertifikatutsteder ikke er ansvarlig for tap som oppstår som følge av anvendelse utenfor de fastsatte begrensningene, jf. § 22.

Tredje ledd gir Kongen kompetanse til å fastsette nærmere krav til hva et kvalifisert sertifikat skal inneholde.

Til § 5 Krav til kvalifiserte elektroniske signaturer brukt i kommunikasjon med og i offentlig sektor

Bestemmelsen gir Kongen hjemmel til å regulere bruken av kvalifiserte elektroniske signaturer ved kommunikasjon med og i offentlig sektor. Bakgrunnen for bestemmelsen er at direktivet åpner for at det kan stilles supplerende krav til bruk av elektroniske signaturer innen offentlig sektor, jf. direktivets artikkel 3 nr. 7. Disse supplerende kravene skal være objektive, klare, forholdsmessige og ikke-diskriminerende. Videre skal tilleggskravene kun stilles i forhold til det aktuelle anvendelsesområdet og de spesielle behov som her gjør seg gjeldende. Det må altså gjøres en konkret vurdering i forhold til det bestemte anvendelsesområde av hvorvidt tilleggskrav er nødvendig.

Til § 6 Rettsvirkningen av elektronisk signatur

Bestemmelsen bygger på direktivets bestemmelser om rettsvirkninger i artikkel 5 nr. 1 bokstav a) og artikkel 3 nr. 7. Artikkel 5 nr. 1 bokstav b) og nr. 2 er ikke implementert i loven, da de er i samsvar med gjeldende rett, jf. kapittel 8.10.1.

Et krav om underskrift eller signatur vil alltid være oppfylt av en kvalifisert elektronisk signatur, på samme måte som en håndskreven underskrift, såfremt lovgivningen åpner for at disposisjonen kan gjennomføres elektronisk. Uttrykket «disposisjonen kan gjennomføres elektronisk» viser til at det må være rettslig adgang til å kommunisere elektronisk innen det aktuelle rettsområdet og sier ikke noe om tekniske muligheter. Bestemmelsen likestiller under gitte forutsetninger rettsvirkningene av en kvalifisert elektronisk signatur med håndskreven underskrift. Andre elektroniske signaturer kan også anses å tilfredsstille slikt krav om underskrift, men da ut fra en konkret vurdering i det enkelte tilfelle, jf. prinsippet i norsk rett om fri bevisføring og fri bevisvurdering. Se nærmere om bestemmelsen om rettsvirkning i kapittel 8.10.

Til § 7 Innsamling og bruk av personopplysninger

Første ledd implementerer artikkel 8 nr. 2 i direktivet og stiller krav om hvordan en sertifikatutsteder kan innhente og behandle personopplysninger. Bestemmelsen stiller strengere krav enn personopplysningsloven og er nærmere omtalt i kapittel 11.

Det presiseres at bestemmelsen gjelder alle sertifikatutstedere, også de som ikke tilbyr kvalifiserte sertifikater. Dette følger av bestemmelsens første punktum som stiller krav til «en sertifikatutsteder».

I *annet ledd* utpekes Datatilsynet til å føre tilsyn med at personopplysninger samles inn og brukes i overensstemmelse med denne bestemmelsen.

Kapittel II Sikre signaturfremstillingssystem

Til § 8 Krav til sikre signaturfremstillingssystem

Bestemmelsen bygger på direktivets vedlegg III som stiller bestemte krav til et signaturfremstillingssystem, for at det skal ha et bestemt sikkerhetsnivå. Signaturfremstillingssystem med et slikt «høyere» sikkerhetsnivå må benyttes for at den elektroniske signaturen skal få rettsvirkninger etter § 6.

*Første ledd*stiller bl.a. krav til at signaturfremstillingssystemet skal beskytte signaturen mot forfalskning.

*Annet ledd*stiller krav om at signaturfremstillingssystemet ikke skal forandre dataene. Dette er bl.a. viktig for å sikre dataenes integritet. Videre er det viktig at undertegner kan se dataene ved undertegningen slik at hun kan være sikker på hva som har blitt undertegnet og sendt til mottaker. Her er det avgjørende at programvaren er installert på en slik måte at signeringen skjer korrekt, og at programvaren ikke er blitt modifisert slik at man signerer og sender noe annet enn det man ser. Dette er et sårbart punkt, og man må velge programvareløsninger man har tillit til at fungerer som forutsatt.

Til § 9 Godkjennelse av sikre signaturfremstillingssystem

Bestemmelsen bygger på direktivets artikkel 3 nr. 4 og nr. 5.

Kommisjonen skal fastsette kriterier for valg av nasjonalt organ som skal godkjenne sikre signaturfremstillingssystem etter *første ledd*, jf. direktivets artikkel 3 nr. 4. Kongen oppnevner et slikt organ, se kapittel 8.8.

Etter *annet ledd*skal en godkjennelse av et slik nasjonalt organ likestilles med en godkjennelse fra et organ utpekt etter tilsvarende regler i et annet EØS-land.

Det følger av *tredje ledd* at kravene i § 8 er oppfylt når signaturfremstillingssystemene er i samsvar med bestemte standarder som Europakommisjonen fastsetter. Dersom man oppfyller gitte standarder kreves ikke godkjennelse av utpekt organ etter første eller annet ledd. Se mer om fastsettelsen av standardene under kapittel 8.8.

Kapittel III Krav til utstedere av kvalifiserte sertifikater

Bestemmelsene i dette kapittelet bygger på direktivets vedlegg II. Kapittelet stiller krav til de sertifikattjenestene som benyttes ved utstedelse av kvalifiserte sertifikater. Det stilles altså krav både til den som utsteder det kvalifiserte sertifikatet og til de som på vegne av utsteder oppfyller andre oppgaver i forbindelse med håndteringen av de kvalifiserte sertifikatene. Utstedere av andre sertifikater enn kvalifiserte reguleres ikke av dette kapittelet. Se ellers om kvalifiserte sertifikater i kapittel 8.4. Om sertifikatutsteder og krav til sertifikatutsteder, se kapittel 8.2 og 8.3.

Til § 10 Krav til virksomheten

Bestemmelsen implementerer direktivets vedlegg II bokstav (a), (e) og (h).

Det følger av *første ledd* at utstedere av kvalifiserte sertifikater fortløpende skal treffe nødvendige juridiske, organisatoriske, tekniske, samt personal-, drifts-, og sikkerhetsmessige disposisjoner for å kunne tilby sikre og velfunge-

rende tjenester. Dette følger av formuleringen «utøve og administrere virksomheten på en forsvarlig måte». Hva som vil være nødvendige disposisjoner for å oppfylle kravene i første ledd, vurderes ut i fra hvilke tjenester som tilbys og til hvilke kundegrupper. Sertifikatutstederen må løpende vurdere disposisjonene dersom porteføljen av tilbudte tjenesteytelser utvides eller på annen måte endres.

I forhold til de tjenesteytelser som tilbys skal utstederen ha personale med nødvendig ekspertise, erfaring og kvalifikasjoner, særlig når det gjelder ledelse, teknikk og sikkerhet. Personalet skal ha sakkunnskap innenfor teknologien for elektroniske signaturer og inngående kjennskap til korrekte sikkerhetsprosedyrer. Kravet oppstilles for å sikre at risikoen for menneskelige feil minimaliseres. Personalet skal ha kjennskap til de systemer og produkter som anvendes for å unngå fare for sikkerhetsbrudd. Sertifikatutsteder skal følge anerkjente standarder innen administrative og ledelsesmessige prosedyrer.

Etter *annet ledd* skal utstedere av kvalifiserte sertifikater til enhver tid ha tilstrekkelige økonomiske ressurser til å kunne drive virksomheten i henhold til kravene i lovforslaget, herunder ha evne til å kunne bære et eventuelt erstatningsansvar. Hvorvidt en utsteder har tilstrekkelige økonomiske ressurser vil bl.a. avhenge av hvilke tjenester som tilbys og eventuelle begrensninger i sertifikatet, jf. § 4 annet ledd bokstav i) og j). Dette betyr at dersom utstederen tilbyr tjenesteytelser innenfor områder med store økonomiske konsekvenser for de involverte parter, skal den økonomiske beredskapen være tilsvarende høy. Utstederen må således opprettholde et balansert forhold mellom de økonomiske ressursene og omfanget og karakteren av de tjenester som tilbys. Kravet kan bl.a. oppfylles ved at sertifikatutsteder tegner en passende forsikring.

Til § 11 Krav til produkter og systemer

Bestemmelsen implementerer direktivets vedlegg 2 bokstav (f) og (g).

Første ledd stiller krav til utstedere av kvalifiserte sertifikater om å anvende sikre produkter og systemer i virksomheten. Sertifikatutsteder skal bl.a. benytte produkter og systemer som er beskyttet mot uautoriserte endringer.

Det er avgjørende for sikkerheten i infrastrukturen som bygges opp omkring de elektroniske signaturene at sertifikatutsteder, som nettopp skal stå som den troverdige tredjepart, anvender pålitelige produkter og systemer. Videre må produktene og systemene som anvendes være innrettet på en slik måte at sikkerheten omkring sertifikattjenestene virkelig er optimal.

Det følger av *annet ledd*at dersom sertifikatutsteder benytter seg av sikre signaturfremstillingssystemer godkjent av det organ Kongen utpeker eller tilsvarende organ i annen EØS-stat, eller standarder for produkter fastsatt av Europakommisjonen, jf. § 9, vil kravene i første ledd være oppfylt, se kapittel 8.8.

Tredje ledd pålegger sertifikatutsteder å treffe foranstaltninger og å etablere prosedyrer som imøtegår eventuelle muligheter for forfalskninger av sertifikatene. Bestemmelsen skal sikre at sertifikatet ikke forfalskes etter utstedelse. Et sertifikats integritet sikres bl.a. ved at sertifikatutsteder påfører sertifikatet sin egen avanserte elektroniske signatur. Dermed vil etterfølgende

forsøk på endringer i sertifikatet kunne oppdages. Dette forutsetter at sertifikatutsteders signatur ikke lett kan forfalskes.

Til § 12 Krav om katalog- og tilbaketrekkingstjeneste

Bestemmelsen er en implementering av direktivets vedlegg II bokstav (b) og (c) og pålegger utstedere av kvalifiserte sertifikater å sikre at det etableres en rask og sikker katalog- og tilbaketrekkingstjeneste.

Sertifikatutsteder skal fastlegge en prosedyre for utstedelse av sertifikater, sperring og tilbaketrekking, slik at det ved hjelp av denne prosedyren skal være mulig å fastslå dato og tidspunkt for ikrafttredelse og sperring eller tilbaketrekking. Dette kan være avgjørende ved eventuelle senere tvister.

En tilbaketrekkingsliste må inneholde opplysninger om hvilket sertifikat det gjelder og fra hvilket tidspunkt det er trukket tilbake. Bakgrunnen for tilbaketrekkingen av sertifikatet kan være at nøklene og tilhørende koder har kommet på avveie, har blitt misbrukt eller at sertifikatet inneholder feilaktige opplysninger. Sertifikatutsteder skal umiddelbart sperre et sertifikat når undertegneren ønsker det eller det ellers er behov for det. Det må kunne stilles krav til at undertegner opplyser om tap av nøkler og koder m.m. på samme måte som med et kredittkort. Det er en forutsetning for at markedet skal ha tillit til signaturene og sertifikatene at tilbaketrekkingslisten ajourføres på en sikker måte.

Direktivets ordlyd i vedlegg II bokstav c) sier «...the date and time when a certificate is issued...». Departementet har imidlertid funnet det mest hensiktsmessig å kreve at dato og tidspunkt for «ikrafttredelse», jf. § 4 annet ledd bokstav f), skal angis i stedet for «utstedelse». Det skal bemerkes at det er en forskjell mellom utstedelse og ikrafttredelse. Utstedelse er når sertifikatet de facto er blitt utstedt til undertegner, men ikrafttredelse er fra det tidspunktet som sertifikatet kan brukes. Sannsynligvis vil disse inntre samtidig, men det vil være mulig at ikrafttredelsestidspunktet inntrer ved et senere tidspunkt. Dette kan f.eks. være aktuelt dersom man utsteder et rollesertifikat for noen som ved utstedelsen ennå ikke har inntatt den aktuelle rollen.

Til § 13 Krav om kontroll av undertegners identitet

Bestemmelsen bygger på direktivets vedlegg 2 bokstav (d) og stiller i realiteten krav til hva sertifikatpolicyen skal inneholde vedrørende kontroll av undertegners identitet. Om sertifikatpolicy, se kapittel 3.4.

Etter *første ledd* er sertifikatutsteder ansvarlig for at undertegners identitet, eventuelle rolle og andre tilleggsopplysninger blir kontrollert og verifisert på en sikker måte. Dette er en tjeneste som sertifikatutsteder i praksis kan sette bort til en registreringsenhet.

Etter *annet ledd* skal rutinene for kontroll etter første ledd være offentlig tilgjengelige.

Til § 14 Krav til lagring av opplysninger

Bestemmelsen implementerer direktivets vedlegg 2 bokstav j) og fastsetter sertifikatutsteders plikt til å registrere relevant informasjon om et kvalifisert sertifikat og til å bruke pålitelige systemer for lagring av sertifikatet.

Hensikten bak kravet om registrering og lagring er at disse opplysningene skal kunne fremlegges som bevis hvis det er påkrevet. Registreringen skal skje elektronisk særlig for å kunne fremlegge bevis for sertifisering når dette er påkrevet i rettssaker og lignende. Imidlertid fastsetter lovforslaget et krav om å lagre opplysningene i minst 10 år etter at sertifikatet er registrert i tilbaketrekkingslisten. Dette minimumskravet er i samsvar med bl.a. regnskapslovens bestemmelser om lagring av registrerte opplysinger.

Hva som er en «rimelig periode», jf. *første ledd* avgjøres med hensyn til hvilken type sertifikat som tilbys. Andre relevante momenter kan være hvilke tekniske muligheter det er for lagring, hva som anses nødvendig i forhold til brukernes eller publikums behov for å få verifisert opplysningene i sertifikatet og hva leverandøren finner nødvendig.

Hva som er en rimelig periode må videre ses i sammenheng med personopplysningsloven § 28, der det heter at personopplysninger ikke lagres lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Dette innebærer at det etter utløpet av 10-års perioden må bero på en konkret vurdering om opplysningene fortsatt er av betydning for registreringsformålet. Opplysninger som etter 10 år ikke lenger er av betydning for registreringsformålet må slettes med hjemmel i personopplysningsloven § 28, dersom det ikke følger av arkivloven eller annen lovgivning at de likevel skal oppbevares.

I *annet ledd* kreves det at sertifikatutsteder skal benytte pålitelige systemer til oppbevaring av sertifikater i verifiserbar form. Kravet innebærer at det i etterkant skal være mulig å kontrollere ektheten av opplysningene, jf. *annet ledd bokstav a)*.

Annet ledd bokstav b) forbyr at et kvalifisert sertifikat oppføres i en offentlig tilgjengelig database eller på annen måte gjøres offentlig tilgjengelig, med mindre innehaveren har gitt sitt samtykke. Regelen er begrunnet utfra personvernhensyn. Dette forhindrer ikke at mottaker av en melding med elektronisk signatur får tilgang til undertegners sertifikat.

Bestemmelsen i *annet ledd bokstav c)* innebærer at sertifikatutstederen må sikre systemene ved å anvende den teknologi som til enhver tid er til rådighet.

Det er ifølge bestemmelsen i *tredje ledd* forbudt for en utsteder av kvalifiserte sertifikater å oppbevare eller kopiere signaturfremstillingsdata. Oppbevaring og kopiering av signaturfremstillingsdata vil kunne være en trussel mot den juridiske anerkjennelse av elektroniske signaturer. Det bør sikres at kun innehaveren av den elektroniske signaturen har adgang til signaturfremstillingsdataene, slik at kun innehaveren disponerer den elektroniske signatur. Dette er et absolutt forbud. Det er ikke mulig å avtale noe annet mellom sertifikatutsteder og innehaver. Dersom signaturfremstillingsdataene, dvs. den private nøkkelen, skulle bli ødelagte eller komme bort, innebærer det at man ikke lenger kan signere et dokument med disse dataene. Allerede signerte dokumenter vil imidlertid fortsatt kunne verifiseres.

Til § 15 Krav om informasjon om vilkår, begrensninger og lignende.

Bestemmelsen er en implementering av direktivets vedlegg 2 bokstav (k).

Etter *første ledd* pålegges utsteder av kvalifiserte sertifikater å gi nødvendige opplysninger til den som sertifikatet skal utstedes til, slik at hun settes i stand til å vurdere tjenesten. Opplysningene skal gis «skriftlig», dvs. i betydningen «ikke muntlig».

Etter *annet ledd* skal opplysningene kunne gis elektronisk, under forutsetning av at det skjer på en slik måte at mottakeren umiddelbart kan få tilgang til informasjonen. Å henvise til en hjemmeside under sertifikatutstederens kontroll, hvor denne fra tid til annen kan endre vilkårene, er ikke tilstrekkelig. Informasjonen skal også på begjæring stilles til rådighet for andre, f.eks. mottakeren av en signatur basert på sertifikatet. Dette betyr ikke at tredjemann har rett til innsyn i avtalen mellom sertifikatutsteder og undertegner.

Med «motparten» siktes det ikke bare til mottaker av sertifikatet, men dette kan også være f.eks. mottakerens arbeidsgiver som inngår avtaler på vegen av sine ansatte.

Til § 16 Utfyllende krav

Det åpnes for at det kan gis nærmere bestemmelser ved forskrift om hvilke krav som kan stilles til sertifikatutsteder som tilbyr kvalifiserte sertifikater.

Kapittel IV Tilsyn og sanksjoner

Loven oppstiller regler om at det skal føres tilsyn med utstedere av kvalifiserte sertifikater som er etablert i Norge.

Til § 17 Tilsyn med utstedere av kvalifiserte sertifikater

Bestemmelsene om tilsyn bygger på direktivets artikkel 3 nr. 3 om krav om tilsyn, i den forstand at tilsynet må gis rettigheter mv. for å kunne virke effektivt.

Første ledd slår fast at et tilsyn kan oppnevnes, og at tilsynets overordnede oppgave er å sikre at utstedere av kvalifiserte sertifikater som er etablert i Norge etterlever lovens bestemmelser og de forskrifter som er gitt i medhold av denne lov. Dette er også et absolutt krav i henhold til direktivets bestemmelser, jf. artikkel 3 nr. 3.

Tilsynet gis i *annet ledd* rett til å kreve alle de opplysninger og dokumenter det trenger for å utføre sine oppgaver i henhold til loven. Denne retten gjelder ikke bare overfor sertifikatutstedere som har sendt inn melding om registrering, men også sertifikatutstedere som påstår at de utsteder kvalifiserte sertifikater, men som ikke har sendt inn registreringsmelding til tilsynet. Det kan samtidig fastsettes en tidsfrist for innsendelse av opplysningene til tilsynet. Denne tidsfristen må settes slik at det vil være mulig for sertifikatutsteder å frembringe nødvendig informasjon og dokumentasjon, men samtidig må det sikres at sertifikatutstedere som ikke oppfyller kravene i loven snarest mulig slettes fra registeret.

Tredje ledd gir tilsynet hjemmel til å utferdige pålegg om at virksomhet i strid med loven skal opphøre, eller i stedet kreve retting av forholdene. Tilsy-

net vil med denne bestemmelsen få generell adgang til å gripe inn med pålegg overfor den som overtrer lovens regler. Tilsynet vil f.eks. kunne gripe inn overfor sertifikatutstedere som ikke oppfyller kravene for kvalifisert sertifikat eller overfor den utsteder som bruker personopplysninger til formål som er uforenlige med det formålet de opprinnelig ble innsamlet for. Pålegg kan også rettes mot offentlige organer i den grad konstitusjonelle grunner ikke er til hinder for dette. Bestemmelsen gir ikke adgang for tilsynet til å gi pålegg om strengere regulering enn det som følger av loven, og tilsynet kan bare sette vilkår som bringer behandlingen i samsvar med lovens øvrige regler. Siden flere av behandlingsreglene i lovforslaget inneholder skjønnsmessige begreper, vil tilsynet i praksis kunne gi pålegg og sette vilkår som presiserer lovtekstens nærmere innhold innenfor rammen av ordlyden i de ulike bestemmelsene. I valget mellom pålegg om opphør eller fastsetting av vilkår skal det tas hensyn til at førstnevnte reaksjon ofte vil være mest inngripende.

Tilsynet kan etter *fjerde ledd* kreve at sertifikatutsteder gjennomfører en IT-revisjon. Den vanligste formen for IT-revisjon er at et revisjonsbyrå gjennomgår sertifikatutstederens praksis for å se om praksis er i samsvar med beskrevet sertifikatutstedelsespraksis, se kapittel 3.4. Det kan være aktuelt å kreve IT-revisjon dersom tilsynet ikke finner å ha mottatt tilstrekkelig underlag for å kunne vurdere om sertifikatutsteder oppfyller kravene i loven. Det kan også være aktuelt dersom det finnes grunn til å tro at selskapet ikke lenger oppfyller lovens krav.

Etter *femte ledd* kan tilsynet i visse situasjoner frata en sertifikatutsteder retten til å anvende betegnelsen kvalifiserte sertifikater, jf. § 4. Denne bestemmelsen vil ikke bare gjelde overfor de som er blitt registrert etter bestemmelsene i § 18, men også andre som urettmessig bruker betegnelsen kvalifiserte sertifikater eller liknende betegnelser som gir uttrykk for at de er kvalifiserte. Å frata en sertifikatutsteder retten til å utstede kvalifiserte sertifikater er en inngripende beslutning. Derfor bør denne retten kun brukes dersom andre sanksjoner viser seg å være virkningsløse. Vedtaket kan kun omfatte den del av sertifikatutsteders virksomhet som omfattes av tilsynet. I vedtaket kan tilsynet også beslutte hvordan virksomheten skal avvikles.

Sjette ledd åpner for at det kan gis nærmere bestemmelser ved forskrift om tilsynets virksomhet. Forskriften vil være på plass samtidig med at loven trer i kraft.

Til § 18 Registrering av utstedere av kvalifiserte sertifikater

I henhold til direktivet kan ikke stater stille krav om forhåndsgodkjennelse av sertifikatutsteder, se kapittel 8.6. Lovforslaget innebærer derfor et forslag om at utstedere av kvalifiserte sertifikater skal sende registreringsmelding til tilsynet før de starter virksomheten. På denne måten får tilsynet oversikt over hvilke sertifikatutstedere de skal føre kontroll med.

Til § 19 Adgang til lokaler m.v.

I utgangspunktet kan tilsynet utføre tilsynsoppgavene basert på de dokumenter de får tilsendt. I en del saker vil dette dokumentinnsynet være nok, men i enkelte saker kan det være behov for å se på lokalene og faktiske installasjo-

ner hos sertifikatutsteder. Bestemmelsen gir tilsynet hjemmel til å foreta granskning.

Første ledd hjemler at tilsynet kan kreve adgang til sertifikatutstedernes lokaler.

Etter *annet ledd* kan tilsynet gjennomføre de kontroller de finner nødvendig og kreve bistand fra personalet.

Det følger av *tredje ledd* at bestemmelsen suppleres av reglene i forvaltningsloven § 15 om fremgangsmåten ved granskning o.l. Bestemmelsen setter krav til måten kontrollen skal gjennomføres på når den utføres andre steder enn offentlige kontorer og andre tjenestesteder. Etter § 15 fjerde ledd kan den som granskningsforretningen angår klage over beslutningen om å fremme forretningen. Slik klage kan rettes til klageorgan utnevnt i henhold til § 23.

Til § 20 Tvangsmulkt

Tilsynet gis i *første ledd* myndighet til å ilegge tvangsmulkt til sertifikatutsteder som ikke har oppfylt pålegg om å endre eller stanse en ulovlig handling. Tvangsmulkt kan fastsettes i vedtaket som inneholder det materielle pålegget, eller senere, typisk når pålegget er overtrådt.

Mulktens størrelse må bestemmes av tilsynet i lys av alminnelige forvaltningsrettslige prinsipper, herunder hensynet til rimelig forholdsmessighet mellom det målet som søkes oppnådd og de virkemidlene som benyttes. Momenter som vil kunne ha betydning ved fastsettelsen av mulktens størrelse vil bl.a. være hvor viktig og betydelig overtredelsen er, hvilke fordeler overtredelsen innebærer for den som gjør seg skyldig i den, hvilke ulemper overtredelsen medfører for bl.a. undertegner og for samfunnet for øvrig. Tvangsmulkt kan ikke begynne å løpe før det har vært mulig å oppfylle pålegget.

Etter *annet ledd* kan tvangsmulkten ikke begynne å løpe før klagefristen på tre uker er utløpt. Dersom vedtaket påklages løper tvangsmulkten fra det tidspunktet tilsynets klageinstans fastsetter etter å ha opprettholdt tilsynets vedtak.

Tilsynet kan frafalle påløpt tvangsmulkt, jf *tredje ledd*. Vedtak om tvangsmulkt er tvangsgrunnlag for utlegg, jf. tvangsfullbyrdelsesloven § 7-2 (d).

Til § 21 Straff

Første ledd hjemler straffansvar for overtredelse av nærmere angitte bestemmelser når overtredelsen er forsettelig eller grovt uaktsom. Bestemmelsen suppleres av alminnelige strafferettslige prinsipper.

Etter *annet ledd* kan medvirkning straffes tilsvarende.

Til § 22 Erstatning

Bestemmelsen bygger på EU-direktivet artikkel 6.

Forhold som ikke omfattes av erstatningsreglene i denne lov må bedømmes i henhold til den alminnelige erstatningsretten. Alminnelige erstatningsrettslige prinsipper supplerer bestemmelsen. Det kan finnes bestemmelser i andre lover og forskrifter som gir rett til erstatning for samme type disposisjoner.

Bestemmelsen er en minimumsregulering som hjemler erstatningsansvar for utstedere av kvalifiserte sertifikater, eller utstedere som garanterer for slike sertifikater. Erstatningsansvaret omfatter også sertifikater som ikke oppfyller lovens krav til kvalifiserte sertifikater, men som utgis for å være det eller gir et slikt inntrykk.

Det følger av *første ledd* at en sertifikatutsteder etablert i Norge kan garantere for at sertifikater fra en annen sertifikatutsteder, etablert i eller utenfor Norge, overholder reglene for utstedelse av kvalifiserte sertifikater. En slik garantistillelse innebærer at garantisten blir erstatningsansvarlig på linje med utsteder av sertifikatet.

Sertifikatutsteder er ansvarlig for tap hos den som hadde rimelig grunn til å ha tillit til sertifikatet. Erstatningsansvaret er ikke begrenset til bare å omfatte mottakeren av et sertifikat. Også en undertegner som har inngått en avtale med sertifikatutsteder kan lide tap pga. feil i sertifikatet. Videre kan en tredjemann lide tap som følge av at han hadde tillit til sertifikatet, noe som også omfattes av bestemmelsen.

Det følger av *første ledd bokstav a)* at sertifikatutsteder er ansvarlig for at all informasjon i sertifikatet var korrekt på det tidspunktet da sertifikatet ble utlevert.

Videre skal sertifikatet inneholde alle opplysninger som kreves i henhold til § 4, jf. § 22 *første ledd bokstav b)*. Dette er opplysninger sertifikatet må inneholde for at det skal være kvalifisert. Dersom noen av disse opplysningene mangler er dette altså en feil som kan medføre erstatningsansvar.

Første ledd bokstav c) gjelder kun når sertifikatutsteder har fremstilt begge typer data.

Første ledd bokstav d) sier at sertifikatutsteder er ansvarlig for at undertegneren var i besittelse av riktig signaturfremstillingsdata på det tidspunktet da sertifikatet ble utferdiget. Med korrekt signaturfremstillingsdata menes her de signaturfremstillingsdataene som svarer til signaturverifikasjonsdataene angitt i sertifikatet. I forhold til digital signatur-teknologi innebærer dette at utsteder er ansvarlig for at undertegner var i besittelse av den private nøkkelen som hører til den offentlige nøkkelen som fremgår i sertifikatet, på det tidspunktet da sertifikatet ble utstedt til undertegner. Videre følger det av § 13 at sertifikatutsteder må sørge for at den personen sertifikatet utstedes til er identifisert på en sikker måte. Sertifikatutsteder er ansvarlig for at signaturen med tilhørende sertifikat ble utstedt til undertegner. Dersom undertegnerens signaturfremstillingsdata ikke korresponderer med signaturverifikasjonsdataene i sertifikatet inneholder dessuten sertifikatet feilaktige opplysninger.

Bokstav e) sier at sertifikatutsteder er erstatningsansvarlig dersom et sertifikat ikke ble korrekt registrert i tilbaketrekkingslisten. En korrekt ajourføring av tilbaketrekkingslisten er nødvendig for at en tredjemann skal kunne stole på signaturen med tilhørende sertifikatet. Mottaker skal kunne kontrollere sertifikatet mot denne listen for å verifisere hvorvidt hun kan stole på at signaturen er gyldig.

Det følger av *annet ledd* at sertifikatutstederen ikke er erstatningsansvarlig dersom hun kan vise at skaden ikke skyldtes uaktsomhet. Sertifikatutsteder har således et culpa-ansvar med omvendt bevisbyrde.

En sertifikatutsteder som garantert for sertifikatene fra en annen sertifikatutsteder er også ansvarlig etter første ledd, medmindre garantisten godtgjør at verken hun eller utstederen av sertifikatet handlet uaktsomt. Sertifikatutsteder må dermed bevise at en utsteder som hun har garantert for, ikke handlet uaktsomt. Dette innebærer et strengere bevisbyrde for utstederen, og eventuelt den som stiller garanti, enn hva som følger av den alminnelige erstatningsretten. Unntaket er begrunnet utfra hensynet til forbrukerinteresser. Se mer om dette under kapittel 8.9.

Det følger av *tredje ledd* at sertifikatutstederen skal kunne begrense erstatningsansvaret ved at det i sertifikatet angis begrensninger i sertifikatets anvendelsesområde eller transaksjonsbeløp. Disse begrensningene må være tydelige for tredjemann. Dette innebærer at de må fremgå tydelig av sertifikatet, både for den sertifikatet er utferdiget til og, ikke minst, for den mottaker som skal stole på sertifikatet. Det bemerkes at programvaren må være korrekt installert og programvaren må kunne håndtere slik fremvisning, slik at all informasjon i sertifikatet fremgår for mottaker. Det er viktig at brukeren velger en programvare hun har tillit til at fungerer som forutsatt. Sertifikatutsteder er ikke erstatningsansvarlig for skade som skyldes at sertifikatet anvendes utover begrenset anvendelsesområde. Dessuten, dersom sertifikatet brukes utover angitt transaksjonsbeløp, er ikke sertifikatutsteder ansvarlig for beløp som overstiger begrensingen.

Lovens regler er som nevnt minimumsregler slik at det ikke skal kunne gjøres avtaler til ulempe for den som har tillit til sertifikatet.

I direktivet vises det til Rådets direktiv 93/13/EØS av 5. april 1993 om urimelige kontraktsvilkår i forbrukeravtaler. Erstatningsbestemmelsen skal ikke gripe inn i det vernet nevnte direktiv om kontraktsvilkår gir. Dette direktivet er implementert i avtaleloven § 37 om urimelige kontraktsvilkår i forbrukeravtaler som gjelder standardavtaler mellom en forbruker og en næringsdrivende.

Til § 23 Klageadgang

Ifølge forvaltningsloven § 28 første ledd første punktum, kan enkeltvedtak påklages til det forvaltningsorgan som er nærmest overordnet det forvaltningsorgan som har truffet vedtaket. Tilsynets vedtak i medhold av denne lov kan påklages til det organ som utpekes med hjemmel i § 23.

Klageinstansen skal utpekes av kongen etter innspill fra Nærings- og handelsdepartementet som ansvarlig departement for loven. Frist for klage reguleres av forvaltningslovens §§ 29 og 30.

Til § 24 Gebyr

Bestemmelsen hjemler adgang til å pålegge sertifikatutstedere gebyrer til finansiering av tilsynets virksomhet. Nærmere regulering vedrørende gebyr vil skje i forskrift med hjemmel i denne bestemmelsen. Når det gjelder økonomiske konsekvenser mv. for tilsynet og andre deler av loven vises det til kapittel 14. I en startfase foreslås det at tilsynets virksomhet helt eller delvis finansieres med statlige midler.

På sikt forutsettes det at tilsynets virksomhet vil kunne betales av utstederne av kvalifiserte sertifikater, helt eller delvis.

Til § 25 Rettslig anerkjennelse av kvalifiserte sertifikater fra utstedere etablert utenfor Norge

Første ledd bygger på EU-direktivet artikkel 4 nr. 1 som inneholder direktivets ikke-diskrimineringsbestemmelse. Direktivet sier at medlemsstatene ikke kan pålegge begrensninger i tjenester fra sertifikatutstedere etablert i et annet medlemsland på direktivets område.

Det følger av første ledd at et sertifikat som oppfyller kravene til å være kvalifisert i det EØS-landet hvor utstederen er etablert, skal godkjennes som kvalifisert i hele EØS-området

Annet ledd gjennomfører EU-direktivet artikkel 7 som stiller krav til medlemslandene om rettslig anerkjennelse av sertifikater fra sertifikatutstedere etablert utenfor EØS-området på nærmere fastsatte vilkår.

Til § 26 Ikrafttredelse

Det tas sikte på at loven skal tre i kraft den 1. juli 2001. Dette er innenfor implementeringstiden på 18 måneder fra direktivet er offentliggjort i EF-Tidende, se kapittel 2.2. Det forventes at forskriftene til loven vil være på plass og tre i kraft fra samme dato.

Til § 27 Overgangsregler

Det er på det rene at allerede før loven trer i kraft, kan det finnes sertifikatutstedere som driver slik virksomhet som reguleres i denne lov. Det er derfor behov for å gi disse utstederne tid til å innrette seg etter bestemmelsene i loven.

Det er ikke noe til hinder for at en sertifikatutsteder tilbyr «kvalifiserte sertifikater» før lovens bestemmelser trer i kraft. Før ikrafttredelsen er det sannsynligvis heller ikke noe til hinder for bruk av betegnelsen, selv om sertifikatet ikke oppfyller kravene for kvalifisert sertifikat som stilles i direktivet og loven. Etter at loven har trådt i kraft vil det være forbudt for en sertifikatutsteder å betegne sine sertifikater som kvalifiserte, såfremt ikke kravene i loven er oppfylt.

Etter at loven har trådt i kraft bør derfor sertifikatutstedere gis en viss tid til å melde seg til tilsynet eller til å opphøre med å betegne sertifikatet for «kvalifisert». Da denne typen av sertifikater bl.a. kan utløse et eksplisitt erstatningsansvar, bør fristen være relativt kort. Videre vil denne loven i nåværende situasjon rette seg mot et relativt lite antall tilbyder. På bakgrunn av dette settes fristen til 6 måneder.

Nærings- og handelsdepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om lov om elektronisk signatur.

Vi HARALD, Norges Konge,

s t a d f e s t e r:

Stortinget blir bedt om å gjøre vedtak til lov om elektronisk signatur i samsvar med et framlagt forslag.

Tilråding fra Nærings- og handelsdepartementet ligger ved.

Forslag til lov om elektronisk signatur

Kapittel I Alminnelige regler

§ 1 *Lovens formål*

Formålet med denne loven er å legge til rette for en sikker og effektiv bruk av elektronisk signatur ved å fastsette krav til kvalifiserte sertifikater, til utstederne av disse sertifikatene og til sikre signaturfremstillingssystemer.

§ 2 *Lovens virkeområde*

Loven gjelder for sertifikatutstedere som er etablert i Norge. Loven regulerer rammebetingelsene for bruk av kvalifiserte elektroniske signaturer, med unntak av § 6 annet punktum og § 7 som gjelder alle elektroniske signaturer.

Kongen kan i forskrift bestemme at loven skal gjelde for Svalbard og Jan Mayen.

§ 3 *Definisjoner*

I denne loven menes med:

–1. *elektronisk signatur*: data i elektronisk form som er knyttet til andre elektroniske data og som brukes til å kontrollere at disse stammer fra den som fremstår som undertegner,

–2. *avansert elektronisk signatur*: en elektronisk signatur som

–a) er entydig knyttet til undertegneren,

–b) kan identifisere undertegneren,

–c) er laget ved hjelp av midler som bare undertegneren har kontroll over, og

–d) er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering,

–3. *kvalifisert elektronisk signatur*: en avansert elektronisk signatur som er basert på et kvalifisert sertifikat og fremstilt av et godkjent sikkert signaturfremstillingssystem,

–4. *undertegner*: den som disponerer et signaturfremstillingssystem og som handler på vegne av seg selv eller på vegne av en annen fysisk eller juridisk person,

–5. *signaturfremstillingssdata*: unike data, som for eksempel koder eller private nøkler, som undertegneren benytter for å fremstille en elektronisk signatur,

–6. *signaturfremstillingssystem*: programvare eller maskinvare som benyttes til å fremstille elektronisk signatur ved hjelp av signaturfremstillingsdata,

–7. *signaturverifikasjonsdata*: unike data, som for eksempel koder eller offentlige nøkler, som benyttes til å verifisere en elektronisk signatur,

–8. *signaturverifikasjonssystem*: programvare eller maskinvare som benyttes for å verifisere elektronisk signatur ved hjelp av signaturverifikasjonsdata,

–9. *sertifikat*: en kopling mellom signaturverifikasjonsdata og undertegner

som bekrefter undertegners identitet og er signert av sertifikatutsteder,

–10. *sertifikatutsteder*: en fysisk eller juridisk person som utsteder sertifikater eller tilbyr andre tjenester relatert til elektronisk signatur.

§ 4 *Kvalifisert sertifikat*

Betegnelsen kvalifisert sertifikat skal kun brukes om sertifikater som oppfyller kravene i denne paragrafen og utstedes for en begrenset periode av en sertifikatutsteder som oppfyller kravene i §§ 10 - 15.

Et kvalifisert sertifikat skal inneholde følgende informasjon:

–a) en angivelse av at sertifikatet er utstedt som et kvalifisert sertifikat,
–b) sertifikatutstederens identitet og den stat den er etablert i,
–c) undertegnerens navn eller pseudonym med opplysning om at det er et pseudonym,
–d) eventuelt ytterligere opplysninger om undertegneren, dersom de er relevante for bruken av sertifikatet,
–e) de signaturverifikasjonsdata, som svarer til de signaturfremstillingsdata som er under undertegnerens kontroll,
–f) sertifikatets ikrafttredelses- og utløpsdato,
–g) sertifikatets identifikasjonskode,
–h) sertifikatutstederens avanserte elektroniske signatur,
–i) eventuelle begrensninger i sertifikatets anvendelsesområde, og
–j) eventuelle beløpsmessige begrensninger i sertifikatet med hensyn til hvilke transaksjoner sertifikatet kan brukes til.

Kongen kan i forskrift regulere hva det kvalifiserte sertifikatet nærmere skal inneholde.

§ 5 *Krav til kvalifiserte elektroniske signaturer brukt i kommunikasjon med og i offentlig sektor*

Kongen kan fastsette nærmere regler om hvilke krav som skal stilles til kvalifiserte elektroniske signaturer som skal brukes ved kommunikasjon med og i offentlig sektor.

§ 6 *Rettsvirkninger av elektronisk signatur*

Dersom det i lov, forskrift eller på annen måte er oppstilt krav om underskrift for å få en bestemt rettsvirkning og disposisjonen kan gjennomføres elektronisk, oppfyller en kvalifisert elektronisk signatur alltid et slikt krav. En elektronisk signatur som ikke er kvalifisert, kan oppfylle et slikt krav.

§ 7 *Innsamling og bruk av personopplysninger*

En sertifikatutsteder får kun 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.

Datatilsynet skal føre tilsyn med at denne bestemmelsen overholdes.

Kapittel II Sikre signaturfremstillingssystemer

§ 8 *Krav til sikre signaturfremstillingssystemer*

Et sikkert signaturfremstillingssystem skal sikre at signaturen er tilfredsstillende beskyttet mot forfalskning. Videre skal et sikkert signaturfremstillingssystem sikre at signaturfremstillingsdata:

–a) i praksis kun kan fremtre én gang og med rimelig grad av sikkerhet forblir hemmeligholdt,
–b) i rimelig utstrekning ikke kan utledes, og
–c) på pålitelig vis kan beskyttes av rette undertegner mot andres bruk.

Et sikkert signaturfremstillingssystem må ikke forandre data i elektronisk form som skal signeres, eller hindre at dataene vises for undertegner før det signeres.

§ 9 *Godkjennelse av sikre signaturfremstillingssystem*

Godkjennelse som et sikkert signaturfremstillingssystem, jf. § 8, gis av det organ som Kongen utpeket. Kongen kan i forskrift gi nærmere bestemmelser om organet og om krav til sikre signaturfremstillingssystem.

Likestilt med godkjennelse etter første ledd er godkjennelse fra et tilsvarende organ i en annen stat som er part i EØS-avtalen.

Kravene i § 8 skal anses oppfylt når den maskin- eller programvaren som benyttes, er i samsvar med de standarder for elektroniske signaturprodukter som Europakommisjonen fastsetter og som offentliggjøres i De Europeiske Fellesskaps Tidende.

Kapittel III Krav til utstedere av kvalifiserte sertifikater

§ 10 *Krav til virksomheten*

Utstedere av kvalifiserte sertifikater skal utøve og administrere virksomheten på en forsvarlig måte slik at den kan tilby sikre, pålitelige og velfungerende sertifikattjenester.

Sertifikatutstederen skal til enhver tid ha tilstrekkelige økonomiske ressurser til å kunne drive virksomheten i henhold til kravene som er stilt i eller i medhold av denne lov.

§ 11 *Krav til produkter og systemer*

Utstedere av kvalifiserte sertifikater skal bruke pålitelige produkter og systemer som er beskyttet mot endringer, og som gir teknisk og kryptografisk sikkerhet i understøttende prosesser.

Kravene i første ledd skal anses oppfylte dersom sertifikatutsteder benytter seg av produkter og systemer som er godkjent av et organ i henhold til § 9 første og annet ledd, eller er i samsvar med standarder fastsatt av Europakommisjonen etter § 9 tredje ledd.

Sertifikatutsteder skal iverksette tiltak mot forfalskning av sertifikatene. Dersom sertifikatutsteder fremstiller signaturfremstillingsdata, skal utstederen garantere fortroligheten av disse dataene under fremstillingsprosessen.

§ 12 *Krav om katalog- og tilbaketrekkingstjeneste*

Utstedere av kvalifiserte sertifikater skal sørge for en hurtig og sikker katalog- og tilbaketrekkingstjeneste og skal sikre at det er mulig å fastslå dato og tidspunkt for ikrafttredelse eller tilbaketrekking av et sertifikat.

§ 13 *Krav om kontroll av undertegners identitet*

Utstedere av kvalifiserte sertifikater er ansvarlige for at identiteten til undertegner og ytterligere relevante opplysninger om vedkommende blir kontrollert gjennom sikre rutiner.

Opplysninger om rutinene som nevnt i første ledd skal være offentlig tilgjengelige.

§ 14 *Krav til lagring av opplysninger*

Utstedere 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.

Sertifikatutsteder skal benytte pålitelige systemer til oppbevaring av sertifikater i verifiserbar form, slik at

–a) opplysningens ekthet kan kontrolleres,
–b) sertifikatene kun er offentlig tilgjengelige i de tilfellene der innehaveren har gitt sitt samtykke, og
–c) eventuelle tekniske endringer, som bringer disse sikkerhetskravene i fare, er synlige for operatøren.

Utstedere av kvalifiserte sertifikater må ikke oppbevare eller kopiere undertegners signaturfremstillingsdata.

§ 15 *Krav om informasjon om vilkår, begrensninger og lignende*

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

–a) vilkårene og begrensningene for bruken av sertifikatet,
–b) opplysninger om eventuelle frivillige akkrediterings- eller sertifiseringsordninger, og
–c) prosedyrer for klage og avgjørelse av tvister.

Opplysninger i henhold til første ledd kan sendes elektronisk, dersom det skjer i en for motparten umiddelbart lesbar form. Disse opplysningene skal også kunne kontrolleres av signaturmottakeren.

§ 16 *Utfyllende krav*

Kongen kan i forskrift fastsette nærmere regler om hvilke krav som kan stilles til utstedere av kvalifiserte sertifikater for å oppfylle bestemmelsene i §§ 10 - 15.

Kapittel IV Tilsyn og sanksjoner

§ 17 *Tilsyn med utstedere av kvalifiserte sertifikater*

Kongen kan utpeke et organ som skal føre tilsyn med at denne lov med forskrifter etterleves.

Tilsynet kan kreve de opplysninger og dokumenter som er nødvendige for å utføre sine oppgaver, og fastsette en tidsfrist for å sende dem inn.

Tilsynet kan gi påbud om at forhold som er i strid med bestemmelser som er gitt i eller i medhold av denne loven, skal opphøre og stille vilkår som må oppfylles for at virksomheten skal være i samsvar med loven.

Tilsynet kan kreve at det gjennomføres IT-revisjon hos utstedere av kvalifiserte sertifikater og utpeke en revisor til å utføre IT-revisjonen. Sertifikatutsteder kan pålegges å betale for revisjonen.

Tilsynet kan frata en sertifikatutsteder retten til å anvende betegnelsen kvalifisert sertifikat, dersom sertifikatutstederen grovt eller gjentatte ganger ikke overholder lovens regler.

Kongen kan gi nærmere forskrifter om tilsynets virksomhet.

§ 18 *Registrering av utstedere av kvalifiserte sertifikater*

En sertifikatutsteder kan ikke utstede kvalifiserte sertifikater før registreringsmelding er sendt til tilsynet. Endringer i allerede registrerte opplysninger og nye opplysninger som skal registeres, skal meldes til tilsynet uten ugrunnet opphold.

§ 19 *Adgang til lokaler m.v.*

Tilsynet kan som ledd i sin kontroll, kreve adgang til steder der det drives virksomhet som står under tilsyn.

Tilsynet kan gjennomføre de kontroller det finner nødvendig, og kreve bistand fra personalet på stedet i den grad dette må til for å få utført kontrollen.

Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker § 15 om fremgangsmåten ved granskning, kommer til anvendelse.

§ 20 *Tvangsmulkt*

For å sikre at bestemmelser som er gitt i eller i medhold av denne lov overholdes, kan tilsynet bestemme at sertifikatutsteder skal betale en daglig løpende mulkt til staten inntil lovstridig virksomhet er opphørt eller pålegg og vilkår gitt med hjemmel i denne lov er etterkommet.

Mulkten løper ikke før klagefristen er ute. Påklages vedtaket om tvangsmulkt, løper ingen tvangsmulkt før klagesaken er avgjort med mindre klageorganet bestemmer annerledes.

Tilsynet kan frafalle påløpt tvangsmulkt.

§ 21 *Straff*

Med bøter straffes den som forsettlig eller grovt uaktsomt

–a) unnlater å registrere/sende melding etter § 18,

–b) unnlater å gi opplysninger etter § 17,
–c) behandler personopplysninger i strid med §§ 7 og 14, eller
–d) gir uriktige eller villedende opplysninger til tilsynet.

Medvirkning straffes på samme måte.

§ 22 *Erstatning*

En sertifikatutsteder som utsteder sertifikater som utgis for å være kvalifiserte, eller som garanterer for slike sertifikater utgitt av en annen, er erstatningsansvarlig for tap hos en fysisk eller juridisk person som følge av at denne hadde hatt rimelig grunn til å ha tillit til at:
–a) informasjonen angitt i sertifikatet var korrekt på utstedelsestidspunktet,
–b) sertifikatet inneholder alle opplysninger som kreves i henhold til § 4,
–c) signaturfremstillingsdata og signaturverifikasjonsdata hører sammen på en unik måte dersom sertifikatutstederen fremstiller begge,
–d) undertegner disponerte korrekt signaturfremstillingsdata på tidspunktet da sertifikatet ble utstedt, eller
–e) sertifikatet blir registrert i tilbaketrekkingslisten, jf. § 12.

Sertifikatutsteder er ansvarlig etter første ledd medmindre han godtgjør at han, eller den han garanterer for, ikke handlet uaktsomt.

Sertifikatutsteder er ikke erstatningsansvarlig for skade som skyldes at sertifikatet har blitt brukt i strid med tydelige begrensninger i sertifikatets anvendelsesområde eller utover beløpsmessige begrensninger.

§ 23 *Klageadgang*

Tilsynets avgjørelser etter bestemmelser som er gitt i eller i medhold av denne loven, kan påklages til det organ Kongen utpeker.

§ 24 *Gebyr*

Kongen kan i forskrift bestemme at sertifikatutstedere som er registreringspliktige etter § 18, skal betale gebyr. Gebyrene må ikke overstige kostnadene ved tilsynets virksomhet.

Kapittel V Internasjonale forhold

§ 25 *Rettslig anerkjennelse av kvalifiserte sertifikater fra utstedere etablert utenfor Norge*

Sertifikater fra sertifikatutstedere som er etablert innen EØS-området, anses som kvalifiserte sertifikater i henhold til denne lov dersom de oppfyller kravene til et kvalifisert sertifikat i det landet der utstederen er etablert.

Kvalifiserte sertifikater fra sertifikatutstedere som er etablert i land utenfor EØS-området, skal gis rettslig anerkjennelse på lik linje med kvalifiserte sertifikater fra sertifikatutstedere innen EØS-området dersom:
–a) utstederen oppfyller kravene i denne lov og har blitt godkjent iht. en frivillig godkjenningsordning i et medlemsland,
–b) en sertifikatutsteder som er etablert innen EØS-området, og som oppfyller kravene i denne loven, garanterer for utstederen, eller

–c) sertifikatet eller utstederen er anerkjent i henhold til multilaterale eller bilaterale avtaler med Norge, EU, tredjeland eller internasjonale organisasjoner.

Kapittel VI Ikrafttredelse og overgangsregler

§ 26 *Ikrafttredelse*

Loven trer i kraft fra den tid Kongen bestemmer.

§ 27 *Overgangsregler*

Utstedere av kvalifiserte sertifikater skal innen 6 måneder etter at loven har trådt i kraft registrere seg i henhold til § 18 eller innenfor samme frist opphøre med å kalle sertifikatene for kvalifiserte eller bruke betegnelse som gir inntrykk av at de er kvalifiserte.

Vedlegg 1

Directive 1999193/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,

Having regard to the proposal from the Commission [19],

Having regard to the opinion of the Economic and Social Committee [20],

Having regard to the opinion of the Committee of the Regions [21],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [22],

Whereas:

(1) On 16 April 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on a European Initiative in Electronic Commerce;

(2) On 8 October 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on ensuring security and trust in electronic communicationb - towards a European framework for digital signatures and encryption;

(3) On 1 December 1997 the Council invited the Commission to submit as soon as possible a proposal for a Directive of the European Parliament and of the Council on digital signatures;

(4) Electronic communication and commerce necessitate' electronic signatures' and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the rule of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market;

(5) The interoperability of electronic-signature products should be promoted; in accordance with Article 14 of the Treaty, the internal urarket comprises an area without internal frontiers in which the free movement of goods is ensured; essential requirements specific to electronic-signature products

---

[19] OJ C 325, 23.10.1998, p. 5.

[20] OJ C 40, 15.2.1999, p. 29.

[21] OJ C 93, 6.4.1999, p. 33.

[22] Opinion of the European Parliament of 13 January 1999 (OJ C 104, 14.4.1999, p. 49), Council Common Position of 28 June 1999 (OJ C 243 27.8.1999, p. 33) and Decision of the European Parlia ment of 27 October 1999 (not yet published in the Official journal). Council Decision of 30 November 1999.

must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods [23] and Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use goods [24] ;

(6) This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security;

(7) The internal market ensures the free movement of persons, as a result of which citizens and residents of the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; the availability of electronic communication could be of great service in this respect;

(8) Rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically;

(9) Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time–stamping services, directory services, computing services or consultancy services related to electronic signatures;

(10) The internal market enables certification-service-providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and businesses new opportunities to exchange information and trade electronically in a secure way, regardless of frontiers; in order to stimulate the Community-wide provision of certification services over open networks, certification-service-providers should be free to provide their services without prior authorisation; prior authorisation means not only any permission whereby the certification-service-provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect;

(11) Voluntary accreditation schemes aiming at an enhanced level of service-provision may offer certification-service-providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among certification-service-providers; certification-service-providers should be left free to adhere to and benefit from such accreditation schemes;

(12) Certification services can be offered either by a public entity or a legal or natural person, when it is established in accordance with the national law;

---

[23] OJ L 367 31.12.1994, p. 1. Regulation as amended by Regulation (EC) No 83795 (OJ L 90, 21.4.1995, p. 1).

[24] OJ L 367 31 12.1994, p. 8. Decision as last amended by Decision 991193/CFSP (OJ L 73, 19.3.1999. p. 1).

whereas Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; it should be ensured that such accreditation schemes do not reduce competition for certification services; (20)

(13) Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme;

(14) It is important to strike a balance between consumer and business needs;

(15) Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate; the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; in order to meet market needs conformity assessment must be timely and efficient;

(16) This Directive contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised;

(17) This Directive does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, or other formalities of a non-contractual nature concerning signatures; for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded;

(18) The storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures;

(19) Electronic signatures will be used in the public sector within national and Community administrations and in communications between such administrations and with citizens and economic operators, for example in the public procurement, taxation, social security, health and justice systems;

(20) Harmonised criteria relating to the legal effects of electronic signatures vill preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of handwritten signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signa-

ture-creation device can be regarded as legally equivalent to handwritten signaturel only if the requirements for handwritten signaturel are fulfilled;

(21) In order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the certification-service-provider involved; national law governs the legal spheres in which electronic documents and electronic signatures may be used; this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence;

(22) Certification-service-providers providing certefication-services to the public are subject to national rules regarding liability;

(23) The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial;

(24) In order to increase user confidence in electronic communication and electronic commerce, certification-service-providers must observe data protection legislation and individual privacy;

(25) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law;

(26) The measures necessary for the implementation of this Directive are to be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission [25)] ;

(27) Two years after its implementation the Commission will carry out a review of this Directive so as, inter alia, to ensure that the advance of technology or changes in the legal environment have not created barriers to achieving the aims stated in this Directive; it should examine the implications of associated technical areas and submit a report to the European Parliament and the Council on this subject;

(28) In accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty, the objective of creating a harmonised legal framework for the provision of electronic signatures and related services cannot be sufficiently achieved by the Member States and can therefore be better achieved by the Community; this Directive does not go beyond what is necessary to achieve that objective,

HAVE ADOPTED THIS DIRECTIVE:

[25)] OJ L 184, 17.7.1999, p. 23.

Article 1

Scope

The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market.

It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

Article 2

Definitions

For the purpose of this Directive:

1. 'electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

2. 'advanced electronic signature' means an electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;
b) it is capable of identifying the signatory;
c) it is created using means that the signatory can maintain under his sole control; and
d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

3. 'signatory' means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;

4. 'signature-creation data' means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

5. 'signature-creation device' means configured software or hardware used to implement the signature-creation data;

6. 'secure-signature-creation device' means a signature-creation device which meets the requirements laid down in Annex III;

7. 'signature-verification-data' means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;

8. 'signature-verification device' means configured software or hardware used to implement the signature-verificationdata;

9. 'certificate' means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;

10. 'qualified certificate' means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;

11. 'certification-service-provider' means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;

12. 'electronic-signature product' means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;

13. 'voluntary accreditation' means any permission, setting out rights and obligations specific to the provisjon of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervisjon of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

Article 3

Market access

1. Member States shall not make the provision of certification services subject to prior authorisation.

2. Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-proveders for reasons which fall within the scope of this Directive.

3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.

4. The conformity of secure signature-creation-devices with the requirements laid down in Annex Ill shall be determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated.

A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States.

5. The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the *Official Journal of the European Communities.*Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.

6. Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer.

7. Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.

Article 4

Internal market principles

1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certificationservice-proveders established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.

2. Member States shall ensure that electronic-signature products which comply with this Directive are permitted to circulate freely in the internal market.

Article 5

Legal effects of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualifeed certificate and which are created by a secure-signature-creation device:

a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

– in electronic form, or
– not based upon a qualified certificate, or
– not based upon a qualified certificate issued by an accredited certification-service-provider, or
– not created by a secure signature-creation device.

Article 6

Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;

unless the certification-service-provider proves that he has not acted negligently.

2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.

3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate. provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.

4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties.

The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.

5. The provisions of paragraphs 1 to 4 shall be without prejudice to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [26)].

[26)] Oj L 95, 21.4.1993, p. 29.

Article 7

International aspects

1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:

a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or
b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or
c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

2. In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organisations. The Council shall decide by qualified majority.

3. Whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority.

Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements.

Article 8

Data protection

1. Member States shall ensure that certification-service-providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on tile protection of individuals with regard to the processing of personal data and on the free movement of such data [27)] .

2. Member States shall ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate.

[27)] OJ L 281, 23.11.1995, p. 31.

The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

Article 9

Committee

1. The Commission shall be assisted by an 'Electronic-Signature Committee', hereinafter referred to as 'the committee'.

2. Where reference is made to this paragraph, Articles 4 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

The period laid down in Article 4(3) of Decision 1999/468/EC shall be set at three months.

3. The Committee shall adopt its own rules of procedure.

Article 10

Tasks of the committee

The committee shall clarify the requirements laid down in the Annexes of this Directive, the criteria referred to in Article 3(4) and the generally recognised standards for electronic signature products established and published pursuant to Article 3(5), in accordance with the procedure laid down in Article 9(2).

Article 11

Notification

1. Member States shall notify to the Commission and the other Member States the following:

a) information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);
b) the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4);
c) the names and addresses of all accredited national certification service providers.

2. Any information supplied under paragraph 1 and changes in respect of that information shall be notified by the Member States as soon as possible.

Article 12

Review

1. The Commission shall review the operation of this Directive and report thereon to the European Parliament and to the Council by 19 July 2003 at the latest.

2. The review shall inter alia assess whether the scope of this Directive should be modified, taking account of technological, market and legal developments. The report shall in particular include an assessment, on the basis of experience gained, of aspects of harmonisation. The report shall be accompanied, where appropriate, by legislative proposals.

Article 13

Implementation

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 19 July 2001. They shall forthwith inform the Commission thereof.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the main provisions of domestic law which they adopt in the field governed by this Directive.

Article 14

Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities

Article 15

Addressees

This Directive is addressed to the Member States.

Done at Brussels, 13 December 1999.

For the European Parliament

The President

N. FONTAINE

For the Council

The President

S. HASSI

Annex I

Requirements for qualified certificates

Qualified certificates must contain:
a) an indication that the certificate is issued as a qualified certificate;
b) the identification of the certification-service-provider and the State in which it is established;
c) the name of the signatory or a pseudonym, which shall be identified as such;
d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
e) signature-verification data which correspond to signature-creation data under the control of the signatory;
f) an indication of the beginning and end of the period of validity of the certificate;
g) the identity code of the certificate;
h) the advanced electronic signature of the certification-service-provider issuing it;
i) limitations on the scope of use of the certificate, if applicable; and
j) limits on the value of transactions for which the certificate can be used, if applicable.

Annex II

Requirements for certification-service-providers issuing quaffied certificates

Certification-service-providers must:
a) demonstrate the reliability necessary for providing certification services;
b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;
d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature techology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;
f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;
h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of lia-

bility for damages, for example, by obtaining appropriate insurance;
i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in redily understandable language. Relevant parts of this information must also be made available on request to third parties relying on the certificate;
l) use trustworthy systems to store certificates in a verifiable form so that:

– only authorised persons can make entries and changes,
– information can be checked for authenticity,
– certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
– any technical changes compromising these security requirements are apparent to the operator.

Annex III

Requirements for secure signature-creation devices

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

Annex IV

Recommendations for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that:
a) the data used for verifying the signature correspond to the data displayed to the verifier;

b) the signature is reliably verified and the result of that verification is correcdy displayed;
c) the verifier can, as necessary, reliably establish the contents of the signed data;
d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;
e) the result of verification and the signatory's identity are correctly displayed;
f) the use of a pseudonym is clearly indicated; and
g) any security-relevant changes can be detected.