

Innst. O. nr. 41

(2000-2001)

Innstilling fra næringskomiteen om lov om elektronisk signatur

Ot.prp. nr. 82 (1999-2000)

Til Odelstinget

1. PROPOSISJONENS HOVEDINNHOOLD

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

For å sikre tillit mellom avsender og mottaker utstedes signaturen sammen med et tilhørende elektronisk sertifikat av en tredje part, i loven omtalt som sertifikatutsteder. Sertifikatutstederen skal bl.a. kontrollere identiteten til den som signerer. 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. 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 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. En har valgt å være så nøytral som mulig i forhold til valg av tekniske løsninger.

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

2. BAKGRUNNEN FOR LOVFORSLAGET

Bakgrunnen for EU-direktivet er at utviklingen av elektronisk handel over åpne globale nett nødvendigvis gjør elektroniske signaturer med tilhørende tjenester som sørger for autentisering. Ulike regelverk hva angår rettslig anerkjennelse av elektroniske signaturer og akkreditering av sertifikatutstedere, kan skape bar-

rierer for elektronisk handel og hindre utviklingen av det indre marked. Det er derfor behov for et harmonisert rammeverk for bruk av elektronisk signatur.

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. Departementet mener derfor at EU-direktivet bør implementeres i en ny lov med tilhørende forskrifter. Implementeringen i Norge skjer da på en tilnærmet identisk måte som i de øvrige nordiske land.

Høringsinstansene stiller seg 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. Høringsinstansene er videre generelt positive til at det legges opp til en minimumsregulering og en enkel modell for tilsyn.

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 anbefales bruk av de ordninger for sertifisering av IT-sikkerhet som allerede er etablert eller under etablering. På det nåværende tidspunkt vil det derfor være opp til markedet hvorvidt de vil opprette frivillige sertifiserings-/akkrediteringsordninger.

3. NÆRMERE OM LOVFORSLAGET

Definisjoner og virkeområde

Definisjonene som brukes i loven er i hovedsak en oversettelse og bearbeidelse av definisjonene i direktivet. Målet er å bruke definisjoner som beskriver et produkt, en virksomhet m.v. i forhold til en teknologi-

nøytral elektronisk signatur. Departementet ønsker videre å beholde definisjonene nærmest mulig opp til de tilsvarende nordiske definisjonene.

Lovforslaget åpner for at også 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. 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.

Sertifikatutsteder

Lovforslaget regulerer virksomheten til fysiske eller juridiske personer som utsteder kvalifiserte sertifikater eller tilbyr andre tjenester relatert til elektronisk signatur. Til en viss grad regulerer lovforslaget også tilbydere som går god for kvalifiserte sertifikater tilbudt av en annen. I lovforslaget anvendes begrepet sertifikatutsteder om tilbyder av sertifikattjenester. Vi får med dette en tilnærmet felles nordisk definisjon på det som kan kalles direktivets kjernebegrep.

Krav til sertifikatutsteder i lovens kap. III

Loven stiller krav til sertifikatutsteder som utsteder kvalifiserte sertifikater og til tjenestene de tilbyr. Det stilles 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. Utsteder av andre sertifikater enn kvalifiserte reguleres ikke. Departementet mener at det ikke er aktuelt å stille krav om interoperabilitet, men er positive til at utstederne selv inngår slike avtaler.

Kvalifiserte elektroniske sertifikater

Direktivet har visse minimumskrav til hva en bestemt type sertifikater med et høyt sikkerhetsnivå skal inneholde og krav til utsteder av slike sertifikater. Disse sertifikatene kalles «kvalifiserte sertifikater». Kravene til kvalifiserte sertifikater er implementert i lovforslaget, men vil også utdypes nærmere i forskrift. Til 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.

Pseudonym

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. En avansert elek-

tronisk signatur stiller krav om at den er entydig knyttet til undertegneren. Dersom man ønsker at en annen skal bruke det aktuelle pseudonymet, må sertifikatet trekkes tilbake og et nytt utstedes.

Registrering av sertifikatutsteder

I henhold til direktivet kan landene ikke stille krav om forhåndsgodkjenning av sertifikatutsteder. Det er imidlertid ikke noe til hinder for å kreve at sertifikatutsteder skal registrere seg før de begynner virksomheten, så fremt det ikke stilles andre krav enn at meldingen sendes inn. I proposisjonen foreslås at sertifikatutsteder skal sende inn registreringsmelding til tilsynsmyndigheten 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.

Tilsyn

Direktivet stiller krav om at det skal føres tilsyn med utsteder av kvalifiserte sertifikater som tilbyr slike og tilhørende tjenester til allmennheten. For å oppfylle kravet om tilsyn kreves at de sertifikatutstederne det skal føres tilsyn med, registreres i et offentlig register.

Selvdeklarasjonsmodellen er foreslått som tilsynsmodell. Modellen oppfyller de krav om tilsyn som stilles i direktivet, og vil gi et reelt og funksjonelt tilsyn som vil gi den nødvendige tillit i markedet. Det kan ikke utelukkes at modellen vil måtte justeres og kompletteres når markedet er mer modent. Utviklingen i markedet må derfor følges nøye fremover. Samtidig er det en modell som i liten grad detaljregulerer markedet.

Direktivet legger opp til at tilsynet kan være et offentlig eller privat organ. Departementet har kommet til at det bør velges et offentlig tilsynsorgan. bl.a. ut fra antagelsen om at et offentlig tilsynsorgan har størst tillit i markedet. På bakgrunn av Post- og teletilsynets erfaring med liknende oppgaver foreslås det at tilsynsoppgavene legges til Post- og teletilsynet. Departementet mener videre at det bør følge av loven at Kongen utpeker tilsynet og at dette ikke gjøres direkte i lovteksten.

Kravene loven stiller til utsteder av kvalifiserte sertifikater vil bli nærmere presisert i forskrifter. En av tilsynets hovedoppgaver vil være å utdype disse kravene ved å ta stilling til hvilken policy og praksis som oppfyller lovens krav. Tilsynet må kommunisere disse til sertifikatutsteder som ønsker å tilby kvalifiserte sertifikater, og se til at sertifikatutstederens virksomhet er i overensstemmelse med de presiserte krav.

Lovforslaget utpeker ikke klageorgan for Post- og teletilsynets avgjørelser, men gir Kongen hjemmel til å utpeke et slikt organ. Det legges ikke opp til at klageadgangen skal være videre enn hva som følger av forvaltningslovens regler.

Sikre signaturfremstillingssystem

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. 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.

Erstatningsbestemmelser

Departementet har kommet til at Norge bør gjennomføre en minimumsregulering av sertifikatutstede- ders erstatningsansvar i samsvar med direktivet. Sertifikatutsteder er erstatningsansvarlig i henhold til lovforslagets § 22 så sant utstederen ikke kan bevise at han/hun ikke handlet uaktsomt. Slik omvendt bevisbyrde innebærer en tyngre bevisbyrde for utsteder og er det eneste unntaket fra den alminnelige erstatningsrett. Et skjerpet krav om bevisbyrde skal være med på å sikre den nødvendige tillit og dermed øket anvendelse av kvalifiserte sertifikater. Erstatningsansvar for en utsteder som ikke utsteder kvalifiserte sertifikater reguleres i henhold til den alminnelige erstatningsretten. 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 sertifikatutstede- ders erstatningsansvar.

Rettsvirkning ved bruk av elektronisk signatur

Direktivets bestemmelse innebærer 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.

Videre krever direktivet at det må sikres at kvalifiserte elektroniske signaturer kan legges frem som bevis ved domstolene og at elektronisk signatur, på annet nivå enn kvalifisert, ikke skal fratras 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 signaturfremstillingssystem. Disse bestemmelsene behøver ikke tas inn i loven da de allerede er i samsvar med gjeldende rett. Ettersom bestemmelsen om rettsvirkninger er en sentral del av direktivet som implementeres ved denne lov, bør imidlertid også dette reguleres i loven.

Kongen gis i forslaget hjemmel til å regulere bruk av elektroniske signaturer ved kommunikasjon med og i offentlig sektor. 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.

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

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

5. KOMITEENS MERKNADER

Komiteen, medlemmene fra Arbeiderpartiet, Erling Brandsnes, Gunnar Breimo, Mimmi Bæivi, Karin Kjølmoen, Kjell Opseth og Rita Tveiten, fra Fremskrittspartiet, Øystein Hedstrøm og Terje Knudsen, fra Kristelig Folkeparti, Randi Karlstrøm og Jon Lilletun, fra Høyre, Ansgar Gabrielsen og Ivar Kristiansen, fra Senterpartiet, lederen Morten Lund, og fra Venstre, Leif Helge Kongshaug, mener det er viktig at elektronisk kommunikasjon og bruk av nett for samhandling skal bli like akseptert, tillitvekkende og ha samme juridiske holdbarhet som tradisjonell skriftlig kommunikasjon og dokumentasjon.

Komiteen har merket seg at EØS-komiteen den 31. juli 2000 vedtok å innlemme europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999, om en fellesskapsramme for elektroniske signaturer i vedlegg XI til EØS-avtalen. Direktivet stiller i noen deler absolutte krav overfor statene, mens andre bestemmelser står statene fritt å implementere.

Komiteen merker seg at loven skal gjelde for sertifikatutstedere som er etablert i Norge. For å falle inn under loven må sertifikatutsteder kalle sertifikate- ne for kvalifiserte og registrere seg hos tilsynet, slik det er foreslått i §18. Komiteen legger merke til at det er sertifikatutstederen som må avgjøre om han/hun vil utstede kvalifiserte sertifikater eller ikke. Utsteder av ikke-kvalifiserte signaturer faller inn under lovens §§ 6 og 7, der § 7 omhandler innsamling av personopplysninger. Ettersom det er knyttet særlige bestem-

melser om tilsyn, erstatning og rettsvirkninger til kvalifiserte elektroniske signaturer, mener komiteen at det vil gi høy tillit til kvalifiserte signaturer og at det dermed er lagt til rette for bruk av slike signaturer. Komiteen har også merket seg at ikke kvalifiserte signaturer også kan gis rettsvirkning.

Komiteen merker seg at loven åpner for bruk av pseudonym i et kvalifisert sertifikat og at det i høringen er kommet fram betenkeligheter mot bruk av pseudonymer. Komiteen viser til brev fra Nærings- og handelsdepartementet av 6. desember 2000 (vedlagt), der det pekes på at bruk av pseudonym er tatt direkte ut fra direktivet, og at dette må tas med i loven for å oppfylle våre internasjonale forpliktelser.

Komiteen viser til at lovforslaget har bestemte krav til systemer for signaturframstilling og til utstedere av kvalifiserte sertifikater. Komiteen mener det er viktig at en elektronisk signatur er tilfredsstillende beskyttet mot forfalskning og at et sikkert signaturframstillingssystem skal godkjennes av et organ Kongen har utpekt.

Komiteen er enig i at det må stilles strenge krav til utstedere av kvalifiserte sertifikater, slik at virksomheten kan tilby sikre, pålitelige og velfungerende sertifikattjenester.

Komiteen er enig i at det skal føres tilsyn med de som utsteder kvalifiserte sertifikater og som tilbyr sertifikatene og tilhørende tjenester til allmennheten. Komiteen er enig i at det kan være naturlig at Post- og teletilsynet får dette tilsynsansvaret idet Post- og teletilsynet allerede i dag har god og bred kompetanse innenfor beslektede områder.

6. KOMITEENS TILRÅDING

Komiteen har for øvrig ingen merknader, viser til proposisjonen og rår Odelstinget til å gjøre slikt

vedtak 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 signaturframstillingssystemer.

§ 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 signaturframstillingssystem,
4. *undertegner*: den som disponerer et signaturframstillingssystem og som handler på vegne av seg selv eller på vegne av en annen fysisk eller juridisk person,
5. *signaturframstillingssdata*: unike data, som for eksempel koder eller private nøkler, som undertegneren benytter for å fremstille en elektronisk signatur,
6. *signaturframstillingssystem*: programvare eller maskinvare som benyttes til å fremstille elektronisk signatur ved hjelp av signaturframstillingsdata,
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 for-

falskning. 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 utpeker. 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 falskning av sertifikatene. Dersom sertifikatutsteder fremstiller signaturfremstillingsdata, skal utstederen garantere fortroligheten av disse dataene under fremstillingsprosessen.

§ 12 *Krav om katalog- og tilbaketrekkingsstjeneste*

Utstedere av kvalifiserte sertifikater skal sørge for en hurtig og sikker katalog- og tilbaketrekkingsstjeneste 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

- opplysningens ekthet kan kontrolleres,
- sertifikatene kun er offentlig tilgjengelige i de tilfellene der innehaveren har gitt sitt samtykke, og
- 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

- vilkårene og begrensningene for bruken av sertifikatet,
- opplysninger om eventuelle frivillige akkrediterings- eller sertifiseringsordninger, og
- 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 registreres, 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

- unnlater å registrere/sende melding etter § 18,
- unnlater å gi opplysninger etter § 17,
- behandler personopplysninger i strid med §§ 7 og 14, eller
- 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:

- informasjonen angitt i sertifikatet var korrekt på utstedelsestidspunktet,
- sertifikatet inneholder alle opplysninger som kreves i henhold til § 4,
- signaturfremstillingsdata og signaturverifikasjonsdata hører sammen på en unik måte dersom sertifikatutstederen fremstiller begge,
- undertegner disponerte korrekt signaturfremstillingsdata på tidspunktet da sertifikatet ble utstedt, eller
- 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:

- utstederen oppfyller kravene i denne lov og har blitt godkjent iht. en frivillig godkjenningsordning i et medlemsland,
- en sertifikatutsteder som er etablert innen EØS-området, og som oppfyller kravene i denne loven, garanterer for utstederen, eller
- 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.

Oslo, i næringskomiteen, den 12. desember 2000

Morten Lund

leder

Erling Brandsnes

ordfører

Kjell Opseth

sekretær

Vedlegg

Brev fra Nærings- og handelsdepartementet v/statsråd Grete Knudsen til Arbeiderpartiets stortingsgruppe v/Erling Brandsnes, datert 6. desember 2000

Ot.prp. nr. 82 – Lov om elektroniske signaturer

Vi viser til Deres to brev av 27. november 2000. I brevet fremlegges synspunkter fra NHO og eforum om endringer av lovteksten i forslaget til lov om elektronisk signatur. Nærings- og handelsdepartementet bes om å kommentere disse forslagene.

§ 4 om kvalifiserte sertifikater

Det foreslås at denne bestemmelsen blir tillagt en forskriftshjemmel som åpner for at man kan spesifisere reguleringen vedrørende pseudonymsertifikater.

Lovforslagets § 4 er tatt direkte ut fra direktivet. I vedlegg I (c) i direktivet står at et kvalifisert sertifikat skal inneholde «... the name of the signatory or a pseudonym, which shall be identified as such.» Således stiller direktivet krav om at man åpner for pseudonymsertifikater. Det skal også bemerkes at både den danske loven som allerede har trådt i kraft og det svenske lovforslaget som skal tre i kraft 1. januar 2001, åpner for pseudonymsertifikater.

Det kan virke motstridende å benytte pseudonymsertifikat når man ønsker å verifisere identiteten til en person, men disse sertifikater vil også kunne brukes ved disposisjoner der mottaker er uinteressert å vite hvem han kommuniserer med, men bare ønsker å sikre at han mottar den ytelsen som undertegner har lovet. For eksempel vil dette være relevant ved kjøp over Internett. En selger er normalt mer interessert i å sikre at han får betalt enn å vite med hvem han selger til. Til kjøpers sertifikat kan det tenkes være koblet en garanti fra en bank om at beløpet vil bli betalt. Selger vil da være sikret betaling, selv om kjøpers identitet forblir ukjent for ham.

Departementet mener at vi må implementere direktivets bestemmelser om pseudonymsertifikat for å oppfylle våre internasjonale forpliktelser. Vi mener derfor at bestemmelsen ikke skal endres.

§ 6 om rettsvirkninger

I lovforslaget § 6 står følgende;

- hvis det stilles krav om underskrift og disposisjonen kan gjøres elektronisk vil en kvalifisert elektronisk signatur oppfylle slikt krav, og
- at signaturer som ikke er kvalifiserte også kan oppfylle slikt krav.

eforum ønsker at man fjerner kravet om at «disposisjonen skal kunne gjennomføres elektronisk».

NHO og eforum ønsker videre at det skal settes inn en forskriftshjemmel som redegjør for i hvilke tilfeller «ikke-kvalifiserte» elektroniske sertifikater kan

oppfylle kravet om underskrift. eforum har følgende forslag til annet ledd: «Kongen kan ved forskrift bestemme unntak fra denne regelen der særlige hensyn tilsier dette.»

Det finnes typer av disposisjoner som man ikke ønsker skal kunne gjennomføres elektronisk. For eksempel ønsker man ikke i dag å åpne for elektroniske testamenter. På bakgrunn av dette vil det ikke være mulig å fjerne kravet om at bestemmelsen må åpne for elektronisk kommunikasjon, for at den aktuelle rettsvirkningen skal kunne tre inn. Hvis man ikke har denne begrensningen vil § 6 gå lengre enn hva som er ønskelig. Hovedregelen vil da være at elektronisk kommunikasjon alltid er en mulig kommunikasjonsform, så fremt det ikke står at disposisjonen ikke kan gjennomføres elektronisk. Denne typen generell regulering for å åpne for elektronisk kommunikasjon er blitt drøftet og avvist i e-regelprosjektet (tidligere «Kartleggingsprosjektet»), jf. kapittel 4.3 i Ot.prp-en til lovforslaget.

Utgangspunktet i bestemmelsen er at en kvalifisert elektronisk signatur skal likestilles med en håndskreven underskrift, og at det ikke er mulig å stille høyere krav. Det finnes imidlertid et unntak fra dette. I lovutkastet § 5 kan det fastsettes andre krav til kvalifiserte sertifikater som skal brukes ved kommunikasjon i og med offentlig forvaltning.

Slik paragrafens første ledd er utformet åpner den allerede for at en elektronisk signatur - på et «lavere nivå» enn en kvalifisert - kan gis samme rettsvirkning som en kvalifisert elektronisk signatur. Hovedregelen er at man ikke kan kreve mer enn en kvalifisert elektronisk signatur, men at det er mulig å benytte seg av andre signaturer for å få samme rettsvirkning. Bestemmelsen har et «tak» men ikke et «gulv». Det vil derfor ikke være riktig å i annet ledd innføre en bestemmelse om «unntak» fra første ledd. Alt under «tak» er allerede tillatt.

Hvis man ønsker å gi «ikke-kvalifiserte» signaturer rettsvirkning, må det normalt reguleres i den aktuelle bestemmelsen som kan være i en lov, forskrift eller instruks. Denne reguleringen vil ikke være hjemlet i lov om elektronisk signatur. Det vil derfor være uriktig å i annet ledd ha en forskriftshjemmel for «unntak».

Avslutningsvis ser vi heller ikke noen grunn for at man skal akseptere ikke-kvalifiserte signaturer kun «der særlige hensyn taler for det». Utgangspunktet her må være at man ikke krever mer kompliserte og dyre tekniske løsninger enn hva som er nødvendig. Hvilke løsninger som skal aksepteres må skje ved en hel-

hetsvurdering av den aktuelle bestemmelsen. At man velger et annet nivå enn kvalifiserte elektroniske signaturer må kunne skje selv om ikke «særlige hensyn taler for det».

Departementet mener at bestemmelsen ikke bør endres.

§ 11 – Krav til produkter og systemer

I lovforslaget § 11 første ledd står: «Utsteder av kvalifiserte sertifikater skal bruke pålitelige produkter ...».

eforum ønsker at en i denne bestemmelsen skal tilføre «til en hver tid» foran «bruke».

Lovens krav om at produktet er pålitelig gjelder hele tiden det er i bruk. eforums tillegg medfører ikke noen realitetsendring. Departementet er derfor av den oppfatning at ovennevnte tillegg er overflødig, og at bestemmelsen ikke behøver endres.

§ 13 – Krav om kontroll av undertegners identitet

Paragrafens første ledd lyder:

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

NHO mener det er behov for å fastsette krav om hvilke opplysninger som minimum skal kontrolleres, for eksempel undertegners identitet med personnummer mv.

Bestemmelsen er utformet i tråd med direktivets tekst. Det pågår et arbeid i en nordisk arbeidsgruppe som ser på hvordan forskriftene til respektive nasjonale lover skal utformes. I forbindelse med dette arbeidet vil man bl.a. drøfte spørsmålet om kontroll av identitet. Det er bl.a. blitt diskutert om man skal kreve personlig fremmøte eller ikke. Man må imidlertid

være forsiktig med ev. tilleggskrav, slik at man ikke stiller krav som direktivet ikke åpner for.

Departementet vil ta dette innspillet med seg i den videre behandlingen av forskrifter knyttet til loven.

§ 17 – Tilsyn

NHO foreslår at det presiseres hvem som skal utføre tilsynet, på hvilken måte og i hvilke situasjoner.

I tråd med normal lovteknikk står i lovteksten «tilsynet» og ikke Post- og teletilsynet, som i lovutkastet er anbefalt som tilsynsmyndighet. Begrunnelsen for dette er bl.a. at man ikke må endre loven dersom man ønsker å utpeke et annet tilsyn eller om tilsynet endrer navn. Kongen vil ifølge lovforslaget utpeke tilsynsorgan.

Ifølge lovforslaget § 17 fjerde ledd kan tilsynet kreve at utstedere gjennomfører en «IT-revisjon». NHO ønsker at begrepet «IT-revisjon» defineres. eforum foreslår at en skal tilføre følgende som et siste punktum i tredje ledd: «...IT-revisjonen skal gjennomføres basert på sertifikatutstederens selvdeklarasjon».

Behovet for IT-revisjon er særlig stort der nettopp selvdeklarasjonen ikke er fullstendig eller på annen måte ikke god nok. Skulle tilsynet i disse situasjonene likevel være forpliktet til å basere seg på selvdeklarasjonen, vil IT-revisjonen miste mye av sin funksjon.

Begrepet «IT-revisjon» er et dynamisk begrep og vil bl.a. påvirkes av hvilken teknisk løsning som velges. I merknaden til bestemmelsen nevnes at «den vanligste formen for IT-revisjon er at et revisjonsbyrå gjennomgår sertifikatutsteders praksis for å se om praksis er i samsvar med beskrevet sertifikatutstedelsespraksis». Det er vanskelig å i lovteksten nærmere presisere hva som menes med IT-revisjon.

Departementet mener at paragrafen ikke bør endres.