



DET KONGELEGE
UTANRIKSDEPARTEMENT

St.prp. nr. 86

(1999-2000)

**Om samtykke til godkjenning av
avgjerd i EØS-komiteen nr. 66/2000 av
31. juli 2000 om endring av vedlegg XI til
EØS-avtala (telekommunika-
sjonstenester)**

*Tilråding frå Utanriksdepartementet av 8. september 2000,
godkjend i statsråd same dagen.*

1 Bakgrunn

EØS-komiteen tok 31. juli 2000 avgjerd om å innlemme europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer i vedlegg XI til EØS-avtala (telekommunikasjonstenester).

Bakgrunnen for direktivet er at utviklinga av elektronisk handel over opne globale nett gjer det naudsynt med autentisering av elektroniske signaturar. Ulike regelverk om rettsleg godkjenning av elektroniske signaturar og akkreditering av sertifikatutferdarar kan skape hindringar for elektronisk handel og hindre utviklinga av den indre marknaden. Difor trengst det eit harmonisert rammeverk for bruk av elektroniske signaturar.

Avgjerda i EØS-komiteen om å innlemme europaparlaments- og rådsdirektiv 1999/93/EF i EØS-avtala vart frå norsk side teken med atterhald om samtykke frå Stortinget, ettersom gjennomføringa i norsk rett gjer det naudsynt med lovendring, jf. Grl. § 26 andre leddet. Gjennom denne proposisjonen vart Stortinget oppmoda om å gje samtykke til godkjenning av avgjerd nr. 66/2000 i EØS-komiteen. Nærings- og handelsdepartementet vil fremje ein eigen odelstingsproposisjon med framlegg til ei ny lov som vil gjennomføre direktivet norsk rett.

Avgjerda i EØS-komiteen og direktivet i uoffisiell norsk omsetjing følger som trykte vedlegg til proposisjonen.

2 Nærmare om direktivet

Føremålet med europaparlaments- og rådsdirektiv 1999/93/EF er å sikre like reglar for rettsleg godkjenning av elektroniske signaturar og for akkreditering av sertifikatutferdarar i medlemsstatane.

Etter direktivet er ein elektronisk signatur ein kommunisert elektronisk signatur som identifiserer kven som sender ei elektronisk melding, på same måte som ein handskriven signatur identifiserer avsendaren ved papirbasert kommunikasjon. Signaturen vert utferda saman med eit sertifikat som knyter underteiknaren sin identitet til signaturen. Utferdaren av sertifikatet går god for koplinga mellom signaturen og ein fastsett identitet. Europaparlaments- og rådsdirektiv 1999/93/EF regulerer i første rekkje verksemda til slike utferdarar av sertifikattenester. Statane må ikkje førehandsgodkjenne slike tilbydarar, men skal skipe eit system som gjer det mogleg å føre tilsyn med verksemda deira.

Det går fram av direktivet at tilbydarane si innsamling av persondata skal avgrensast til det som er naudsynt for utferding av sertifikat. Bakgrunnen for denne regelen er omsynet til personvernet til brukarane. Det går òg fram av direktivet at tilbydarar av sertifikattenester har erstatningsansvar m.a. for skade som følgje av at nokon lit på at sertifikatet er riktig. Føremålet med denne føresegna er å skape tillit til dei elektroniske signaturane.

Vidare inneheld direktivet reglar om rettsverknadene av dei elektroniske signaturane. Dei elektroniske signaturane som stettar tryggleikskrava i direktivet, dei såkalla kvalifiserte signaturane, skal godkjennast på lik linje med handskrivne signaturar, og skal kunne leggjast fram som prov i retten på same måte som handskrivne signaturar.

Direktivet seier òg at sertifikat som vert utferda til ålmenta som kvalifiserte sertifikat av tilbydarar av sertifikattenester som er etablerte i ein tredjestat, vert rekna som rettsleg jamstilte med sertifikat som er utferda av tilbydarar av sertifikattenester som er etablerte innanfor Fellesskapet.

Direktivet stiller ikkje krav om at statane må tillate elektronisk kommunikasjon, men omfattar berre dei tilfella der nasjonal rett opnar for elektronisk kommunikasjon. Vidare regulerer ikkje direktivet elektroniske signaturar som berre vert nytta innanfor system som byggjer på frivillige avtaler mellom ei avgrensa mengd deltakarar, omtala som lukka nett, t.d. nettbankar.

I medhald av direktivet skal det oppnemast ein komité til å hjelpe Komisjonen i gjennomføringa av direktivet. Komiteen er ein såkalla artikkel 100-komité, der EFTA/EØS-statane er sikra deltaking.

3 Avgjerda i EØS-komiteen

Som eit ledd i samarbeidet i EØS vedtok EØS-komiteen 31. juli 2000 å endre vedlegg XI om telekommunikasjonstenester, slik at avtala òg omfattar europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer. Avgjerda inneheld ei innleiing og fire artiklar. I innleiinga vert det vist til EØS-avtala, og særleg til artikkel 98, som gjer det mogleg å endre vedlegga til avtala gjennom avgjerd i EØS-komiteen.

Artikkel 1 slår fast at i vedlegg XI til avtala etter nr. 5f (europaparlaments- og rådsdirektiv 97/66/EF) skal nytt nr. 5g lyde: «399 L 0 093: Europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer (EFT L 13 av 19.1 2000, s. 12).»

Vidare vert det i artikkel 1 slått fast at direktivet skal gjelde med visse tilpassingar for EFTA/EØS-statane: For det første slår artikkel 1 a) fast at det i artikkel 7 nr. 1 bokstav c) vert lagt til «eller mellom en EFTA-stat og tredjestatar eller internasjonale organisasjonar» etter «organisasjonar». Føresegna skal sikre at tilbydarar av sertifikattjenester som er etablerte i ein tredjestat på bakgrunn av ei avtale mellom ein EFTA-stat og ein tredjestat eller ein internasjonal organisasjon, skal jamstellast med sertifikat som er utferda av tilbydarar på bakgrunn av avtale mellom Fellesskapet og tredjestatar eller internasjonale organisasjonar. For det andre slår artikkel 1 b) fast at «i situasjonar som nevnt i artikkel 7 nr. 2 skal avtalepartene holde hverandre underrettet og, dersom det anmodes om det, holde samråd i EØS-komiteen». Føresegna skal sikre at EFTA-statane vert orienterte og ev. kan halde samråd i EØS-komiteen dersom Kommisjonen gjer framlegg med omsyn til den faktiske gjennomføringa av standardar for og internasjonale avtaler om sertifikattjenester, og ev. gjer framlegg for Rådet om føremålstenlege mandat for bilaterale og multilaterale avtaler med tredjestatar og internasjonale organisasjonar. For det tredje slår artikkel 1 c) fast at «når Fellesskapet forhandler med en tredjestat på grunnlag av artikkel 7 nr. 3 om markedsadgang for fellesskapsforetak, skal det søke å oppnå den samme behandling for foretak fra EFTA-statene». Føresegna skal sikre at føretak i EFTA-statene vert jamstilte med føretak i EU når Kommisjonen forhandlar med ein tredjestat om marknadstilgang i tredjestatar.

Artikkel 2 slår fast at europaparlaments- og rådsdirektivet skal gjelde på islandsk og norsk på lik linje med dei andre språka i medlemsstatane i Fellesskapet.

Artikkel 3 slår fast at avgjerda tek til å gjelde 1. august 2000, på det vilkåret at EØS-komiteen har motteke alle meldingar etter artikkel 103 nr. 1 i avtala.

Artikkel 4 slår fast at avgjerda i EØS-komiteen skal kunngjerast i EØS-avdelinga av og EØS-tillegget til *Tidend for Dei europeiske fellesskapa*.

Etter artikkel 103 nr. 1 jf. nr. 2 skal EFTA-statane innan seks månader frå det tidspunktet då avgjerda vart teken (som var 31. juli 2000), stadfeste overfor dei andre EØS-statane at dei forfatningsmessige krava er stetta, dvs. for Noreg sin del at det er henta inn samtykke frå Stortinget.

4 Tilhøvet til norsk rett

Det er i dag inga eiga regulering av bruken av elektroniske signaturar og tilhøyrande tenester i norsk rett. I fleire samanhengar har det likevel vore etterlyst lovregulering som skal leggje til rette for at elektronisk kommunikasjon og bruk av nett som infrastruktur for samhandling skal verte like akseptert, til-litsvekkjande og ha same juridiske truverd som tradisjonell skriftleg kommunikasjon og dokumentasjon, sjå m.a. St. meld. nr. 41 (1998-99) «Om elektronisk handel og forretningsdrift».

Delar av direktivet om elektroniske signaturar stiller absolutte krav overfor statane og som difor må gjennomførast i lov eller forskrift. Enkelte av føresegnene i direktivet står statane derimot fritt til å gjennomføre, t.d. regulering av ei frivillig akkrediteringsordning, eller «godkjenningsordning» av sertifikatutferdarar. Det er òg mogleg å sikre at verknadene av enkelte føresegner vert oppnådde på annan måte enn ved lovregulering dersom det er mest føremålstenleg, t.d. ved å oppmuntre til sjølvregulering av marknaden.

Til hausten vil Nærings- og handelsdepartementet fremje ein eigen odels-tingsproposisjon med framlegg til lov om elektroniske signaturar, som vil gjennomføre europaparlaments- og rådsdirektiv 1999/93/EF i norsk rett. Dette framlegget vil gjennomføre heile direktivet, men likevel slik at departementet rår til at føresegnene om ei frivillig akkrediteringsordning bør vurderast på eit seinare tidspunkt.

5 Vurdering

Ein reknar med at direktivet vil påverke den norske marknaden for sertifikatutferdarar og elektroniske signaturprodukt i positiv retning. Å regulere tilbodet av kvalifiserte sertifikat vil stimulere til bruk av sertifikat med eit særleg høgt tryggleiksnivå. Direktivet vil medverke til at tilliten til marknaden og tilliten til bruk av elektroniske signaturar i samfunnet aukar. Dette kan igjen medverke til at signaturteknologi vert teken i bruk på brei basis.

Direktivet krev at det vert skipa ei obligatorisk tilsynsordning for utferdarar av kvalifiserte sertifikat. Tilsynet må stette visse kriterium. Desse kriteria vert utarbeidde av Kommisjonen med medverknad frå den førnemnde komiteen der EFTA/EØS-statane har rett til å ta del. Det vert gjort framlegg om at Post- og teletilsynet vert utpeikt som tilsyn for Noreg.

I ein startfase vil det vere ein viss økonomisk risiko for sertifikatutferdarar i samband med med å gå inn i ein ny marknad. Denne risikoen vert forsterka dersom utferdarane vert møtte av økonomiske barrierar i form av høge registreringsgebyr, tilsynsavgifter og liknande. Nærings- og handelsdepartementet vil sjå nærmare på korleis desse problema kan avhjelpast i ein startfase.

Nærings- og handelsdepartementet rår til at avgjerda i EØS-komiteen om å ta direktivet om elektroniske signaturar inn i EØS-avtala vert godkjend. Utanriksdepartementet sluttar seg til dette.

Utanriksdepartementet

t i l r å r :

At Dykkar Majestet godkjenner og skriv under eit framlagt forslag til proposisjon til Stortinget om samtykke til godkjenning av avgjerd i EØS-komiteen nr. 66/2000 av 31. juli 2000 om endring av vedlegg XI til EØS-avtala (telekommunikasjonstenester).

Vi HARALD, Noregs Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjere vedtak om samtykke til godkjenning av avgjerd i EØS-komiteen nr. 66/2000 av 31. juli 2000 om endring av vedlegg XI til EØS-avtala (telekommunikasjonstenester), i samsvar med eit framlagt forslag.

Tilråding frå Utanriksdepartementet ligg ved.

Vedlegg 1

EØS-komiteens beslutning nr. 66/2000 av 31. juli 2000 om endring av EØS-avtalens vedlegg XI (Telekommunikasjonstjenester)

EØS-KOMITEEN HAR -

under henvisning til avtalen om Det europeiske økonomiske samarbeidsområde, justert ved protokollen om justering av avtalen om Det europeiske økonomiske samarbeidsområde, heretter kalt «avtalen», særlig artikkel 98, og på følgende bakgrunn:

1. Avtalens vedlegg XI er endret ved EØS-komiteens beslutning nr. 175/1999 av 17. desember 1999.¹⁾
2. Europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer²⁾ skal innlemmes i avtalen.
3. Bestemmelsene om internasjonale aspekter i direktiv 1999/93/EF må tilpasses for avtalens formål -

BESLUTTET FØLGENDE:

Artikkel 1

I avtalens vedlegg XI etter nr. 5f (europaparlaments- og rådsdirektiv 97/66/EF) skal nytt nr. 5g lyde:

«5g.	399 L 0 093: Europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer (EFT L 13 av 19.1 2000, s. 12).
------	--

Direktivets bestemmelser skal for denne avtales formål gjelde med følgende tilpasning:

- a) I artikkel 7 nr. 1 bokstav c) tilføyes «eller mellom en EFTA-stat og tredjestater eller internasjonale organisasjoner» etter «organisasjoner».
- b) I situasjoner som nevnt i artikkel 7 nr. 2 skal avtalepartene holde hverandre underrettet og, dersom det anmodes om det, holde samråd i EØS-komiteen.
- c) Når Fellesskapet forhandler med en tredjestat på grunnlag av artikkel 7 nr. 3 om markedsadgang for fellesskapsforetak, skal det søke å oppnå den samme behandling for foretak fra EFTA-statene.»

Artikkel 2

Teksten til europaparlaments- og rådsdirektiv 1999/93/EF på islandsk og norsk, som vil bli kunngjort i EØS-tillegget til *De Europeiske Fellesskaps Tidende*, skal gis gyldighet.

¹⁾ Ennå ikke kunngjort.

²⁾ EFT L 13 av 19.1 2000, s. 12.

Artikkel 3

Denne beslutning trer i kraft 1. august 2000, forutsatt at EØS-komiteen har mottatt alle meddelelser etter avtalens artikkel 103 nr. 1 ³⁾.

Artikkel 4

Denne beslutning skal kunngjøres i EØS-avdelingen av og EØS-tillegget til *De Europeiske Fellesskaps Tidende*.

Utferdiget i Brussel, 31. juli 2000.

For EØS-komiteen	
Formann	
G.S. Gunnarsson	
EØS-komiteens sekretærer	
G. Vik	E. Gerner

³⁾ Forfatningsrettslige krav angitt.

Vedlegg 2**Europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer**

EUROPAPARLAMENTET OG RÅDET FOR DEN EUROPEISKE UNION HAR —

under henvisning til traktaten om opprettelse av Det europeiske fellesskap, særlig artikkel 47 nr. 2 og artikkel 55 og 95, under henvisning til forslag fra Kommisjonen ⁴⁾, under henvisning til uttalelse fra Den økonomiske og sosiale komité ⁵⁾, under henvisning til uttalelse fra Regionskomiteen ⁶⁾, etter framgangsmåten fastsatt i traktatens artikkel 251 ⁷⁾

og

ut fra følgende betraktninger:

1. Kommisjonen framla for Europaparlamentet, Rådet, Den økonomiske og sosiale komité og Regionskomiteen 16. april 1997 en melding om et europeisk initiativ innenfor elektronisk handel.
2. Kommisjonen framla for Europaparlamentet, Rådet, Den økonomiske og sosiale komité og Regionskomiteen 8. oktober 1997 en melding med tittelen «Sikkerhet og tillit innenfor elektronisk kommunikasjon — mot en europeisk ramme for digitale underskrifter og kryptering».
3. Rådet anmodet Kommisjonen 1. desember 1997 om så snart som mulig å framlegge et forslag til europaparlaments- og rådsdirektiv om elektroniske signaturer.
4. Elektronisk kommunikasjon og elektronisk handel gjør det nødvendig med «elektroniske signaturer» og tilknyttede tjenester som muliggjør autentisering av data. Forskjellige regler for rettslig anerkjennelse av elektroniske signaturer samt akkreditering av tilbydere av sertifikattjenester i medlemsstatene kan skape betydelige hindringer for bruken av elektronisk kommunikasjon og for elektronisk handel. På den annen side vil en klar fellesskapsramme for vilkårene for elektroniske signaturer styrke tiltroen til og den allmenne anerkjennelsen av de nye teknologiene. Medlemsstatenes lovgivning skal ikke hindre fri bevegelse av varer og tjenester i det indre marked.
5. Samspillet mellom elektronisk-signatur-produkter bør fremmes. I henhold til traktatens artikkel 14 omfatter det indre marked et område uten indre grenser med fri bevegelse av varer. Grunnleggende særskilte krav for elektronisk-signatur-produkter må overholdes for å sikre fri bevegelse i det indre marked og for å skape tillit til elektroniske signaturer, med forbehold for rådsdirektiv (EF) nr. 3 381/94 av 19. desember 1994 om opprettelse av en fellesskapsordning for kontroll av eksport av varer med dobbelt anvendelse ⁸⁾

⁴⁾ EFT C 325 av 23.10 1998, s. 5.

⁵⁾ EFT C 40 av 15.2 1999, s. 29.

⁶⁾ EFT C 93 av 6.4 1999, s. 33.

⁷⁾ Europaparlamentsuttalelse av 13. januar 1999 (EFT L 104 av 14.4 1999, s. 49), Rådets felles holdning av 28. juni 1999 (EFT L 243 av 27.8 1999, s. 33) og Europaparlamentsbeslutning av 27. oktober 1999 (ennå ikke offentliggjort i EFT). Rådsbeslutning av 30. november 1999.

og rådsbeslutning 94/942/FUSP av 19. desember 1994 om den felles handling vedtatt av Rådet om kontroll av eksport av varer med dobbelt anvendelse ⁹⁾

6. Dette direktiv harmoniserer ikke leveringen av tjenester når det gjelder fortrolige opplysninger når disse omfattes av nasjonale bestemmelser om offentlig orden eller offentlig sikkerhet.
7. Det indre marked sikrer fri bevegelse av personer, med det resultatet at borgere og personer bosatt i Den europeiske union stadig oftere må ha kontakt med myndighetene i andre medlemsstater enn den de er bosatt i. Muligheten for elektronisk kommunikasjon kunne komme til stor nytte i så henseende.
8. Med den raske teknologiske utviklingen og Internetts globale karakter er det nødvendig med en framgangsmåte som åpner for forskjellige teknologier og tjenester som muliggjør elektronisk autentisering av data.
9. Elektroniske signaturer vil få anvendelse i en rekke forskjellige situasjoner og bruksområder, som fører til en rekke nye tjenester og produkter i tilknytning til eller som bruker elektroniske signaturer. Slike produkter og tjenester bør ikke være begrenset til utstedelse og forvaltning av sertifikater, men bør også omfatte enhver annen tjeneste og ethvert annet produkt som bruker eller er tilknyttet elektroniske signaturer, som registreringstjenester, tidsstempling, katalogtjenester, databehandlingstjenester eller rådgivningstjenester i forbindelse med elektroniske signaturer.
10. Det indre marked gjør det mulig for tilbydere av sertifikattjenester å utvikle sin virksomhet over landegrensene, med henblikk på å øke sin konkurransedyktighet og på den måten tilby forbrukerne og industrien nye muligheter for sikker elektronisk informasjonsutveksling og elektronisk handel uavhengig av grenser. Tilbydere av sertifikattjenester bør kunne yte sine tjenester fritt uten forhåndsgodkjenning, for å stimulere leveringen av sertifikattjenester over åpne nett på fellelesskapsplan. Med «forhåndsgodkjenning» menes ikke bare enhver tillatelse hvis utstedelse forutsetter at nasjonale myndigheter treffer en beslutning før den berørte tilbyderen av sertifikattjenester kan yte sine sertifikattjenester, men også ethvert annet tiltak med samme virkning.
11. Frivillige akkrediteringsordninger med sikte på bedre tjenesteyting kan gi ytere av sertifikattjenester den riktige rammen for å forbedre sine tjenester og dermed oppnå den tillit, sikkerhet og kvalitet som et marked i utvikling krever. Slike ordninger bør fremme utviklingen av den beste praksis blant ytere av sertifikattjenester. Ytere av sertifikattjenester bør fritt kunne slutte seg til og dra nytte av slike akkrediteringsordninger.
12. Sertifikattjenestene kan tilbys av enten et offentlig organ eller en juridisk eller fysisk person når de er etablert i samsvar med nasjonal lovgivning. Medlemsstatene bør ikke hindre tilbydere av sertifikattjenester i å virke utenfor slike frivillige akkrediteringsordninger. Det bør sikres at akkrediteringsordningene ikke svekker konkurransen på området for sertifikattjenester.
13. Medlemsstatene kan selv fastsette hvordan de vil føre tilsyn med at

⁸⁾ EFT L 367 av 31.12 1994, s. 1. Forordningen sist endret ved forordning (EF) nr. 837/95 (EFT L 90 av 21.4 1995, s. 1).

⁹⁾ EFT L 367 av 31.12 1994, s. 8. Beslutningen sist endret ved beslutning 99/193/FUSP (EFT L 73 av 19.3 1999, s. 1).

bestemmelsene fastsatt i dette direktiv etterkommes. Dette direktiv hindrer ikke opprettelse av tilsynsordninger i privat sektor. Dette direktiv gir ikke ytere av sertifikattjenester pålegg om å søke om å bli ført tilsyn med i henhold til en gjeldende akkrediteringsordning.

14. Det er viktig å finne den riktige balansen mellom forbrukernes og foretakenes behov.
15. Vedlegg III omfatter kravene til sikre signaturframstillingsprodukter, for å sikre at avanserte elektroniske signaturer fungerer hensiktsmessig. Det omfatter ikke hele anvendelsesområdet til disse produktene. For at det indre marked skal fungere godt, må Kommisjonen og medlemsstatene handle raskt slik at det er mulig å utpeke de organer som er pålagt å foreta en samsvarsvurdering av de sikre signaturframstillingsproduktene i henhold til vedlegg III. For å oppfylle markedets behov må samsvarsvurderingen utføres effektivt og til rett tid.
16. Dette direktiv bidrar til bruk og rettslig anerkjennelse av elektroniske signaturer i Fellesskapet. Det er ikke nødvendig med rammeregler for elektroniske signaturer som brukes utelukkende i systemer som er opprettet på grunnlag av privatrettslige frivillige avtaler mellom et bestemt antall deltakere. Partenes frihet til innbyrdes å avtale de vilkår de vil akseptere elektronisk signerte data på, bør respekteres i den grad nasjonal lovgivning tillater det. Elektroniske signaturer som brukes i slike systemer bør ha rettslig gyldighet og bør kunne godkjennes som bevis under rettergang.
17. Dette direktiv har ikke som mål å harmonisere nasjonale regler for avtalerett, særlig inngåelse og oppfyllelse av kontrakter, eller andre ikke-avtalerettslige formaliteter i forbindelse med signaturer. Bestemmelsene om elektroniske signaturers rettsvirkning bør ikke berøre formkrav fastsatt ved nasjonal lovgivning eller regler som fastsetter kontraktsinngåelse eller hvor en kontrakt er inngått.
18. Oppbevaring og kopiering av signaturframstillingsdata kan kunne utgjøre en trussel mot elektroniske signaturers rettslige gyldighet.
19. Elektroniske signaturer vil bli brukt i offentlig sektor innenfor nasjonale forvaltninger og fellesskapsforvaltninger og i kommunikasjonen mellom disse forvaltningene og med borgere og markedsdeltakere, for eksempel innenfor offentlig innkjøp, skatt-, trygd-, helse- og rettssystemet.
20. Harmoniserte kriterier i forbindelse med elektroniske signaturers rettsvirkning vil gjøre det mulig å bevare en sammenhengende rettslig ramme i hele Fellesskapet. Nasjonal lovgivning fastsetter forskjellige krav til håndskrevne signaturers rettslige gyldighet. Sertifikater kan brukes til å identifisere en person som underskriver elektronisk. Målet med avanserte elektroniske signaturer på grunnlag av godkjente sertifikater er et høyere sikkerhetsnivå. Avanserte elektroniske signaturer på grunnlag av et kvalifisert sertifikat, som er laget ved hjelp av et sikkert signaturframstillingsprodukt, kan anses for rettslig å tilsvare håndskrevne signaturer bare dersom kriteriene for håndskrevne signaturer er oppfylt.
21. For å bidra til at elektronisk autentisering blir allment akseptert, må det sikres at elektroniske signaturer kan brukes som bevis under rettergang i alle medlemsstatene. Rettslig anerkjennelse av elektroniske signaturer bør hvile på objektive kriterier og ikke avhenge av godkjenning av den berørte tilbydereren av sertifikattjenester. Hvilke juridiske områder som elektroniske dokumenter og elektroniske signaturer kan anvendes på, reguleres av nasjonal lovgivning. Dette direktiv berører ikke en nasjonal

- domstols rett til å bestemme om kravene i dette direktiv overholdes, og heller ikke nasjonale regler for fri rettslig vurdering av beviser.
22. Tilbydere av sertifikattjenester som tilbyr sertifikattjenester til offentligheten er underlagt nasjonale regler for erstatningsansvar.
 23. Utviklingen innen internasjonal elektronisk handel krever ordninger over landegrensene, som involverer tredjestater. For å sikre samfunksjonsevnen på globalt plan kan det være hensiktsmessig å inngå avtaler med tredjestater om multilaterale regler for sertifikattjenester.
 24. For å øke brukernes tillit til elektronisk kommunikasjon og elektronisk handel må tilbyderne av sertifikattjenester overholde lovgivningen om datasikring og privatlivets fred.
 25. Bestemmelser om bruk av pseudonymer på sertifikater skal ikke hindre medlemsstatene i å kreve at personer identifiserer seg i henhold til fellesskapsrett eller nasjonale regler.
 26. De tiltak som er nødvendige for gjennomføringen av dette direktiv, skal vedtas i samsvar med rådsbeslutning 1999/468/EF av 28. juni 1999 om fastsettelse av nærmere regler for utøvelsen av den gjennomføringsmyndighet som er tillagt Kommisjonen ¹⁰⁾
 27. Kommisjonen skal to år etter iverksettelsen av dette direktiv, foreta en gjennomgang av det, blant annet for å sikre at tekniske fremskritt eller juridiske endringer ikke hindrer at målene i direktivet kan nås. Kommisjonen bør undersøke virkningene på tilknyttede tekniske områder og framlegge for Europaparlamentet og Rådet en rapport om dette.
 28. Målet om å skape en harmonisert rettslig ramme for elektroniske signaturer og tilknyttede tjenester kan ikke i stor nok grad oppnås av medlemsstatene, og kan derfor i samsvar med nærhets- og forholdsmessighetsprinsippet omhandlet i traktatens artikkel 5 bedre nås av Fellesskapet. Dette direktiv går ikke lenger enn det som er nødvendig for å nå dette målet —

VEDTATT DETTE DIREKTIV:

Artikkel 1

Virkeområde

Målet med dette direktiv er å gjøre det enklere å bruke elektroniske signaturer og bidra til rettslig anerkjennelse av dem. Det oppretter en rettslig ramme for elektroniske signaturer og visse sertifikattjenester for å sikre at det indre marked fungerer hensiktsmessig.

Det omfatter ikke aspekter i forbindelse med inngåelse av kontrakter og kontraktens gyldighet eller andre juridiske forpliktelser som i henhold til nasjonal lovgivning eller fellesskapsrett er underlagt formkrav. Det berører heller ikke regler eller begrensninger som i henhold til nasjonal lovgivning eller fellesskapsrett gjelder for anvendelsen av dokumenter.

¹⁰⁾ EFT L 184 av 17.7 1999, s. 23.

Artikkel 2

Definisjoner

I dette direktiv menes med

1. «elektronisk signatur»: data i elektronisk form som er tilknyttet eller logisk forbundet med andre elektroniske data og som fungerer som autentiseringsmetode,
2. «avansert elektronisk signatur»: en elektronisk signatur som oppfyller følgende krav:
 - a) den er entydig knyttet til underskriveren,
 - b) den kan identifisere underskriveren,
 - c) den er opprettet ved hjelp av midler som underskriveren alene har kontroll over, og
 - d) den er tilknyttet dataene som den vedrører på en slik måte at enhver senere endring kan oppdages,
3. «underskriver»: enhver person som har et signaturframstillingsprodukt, og som handler på egne vegne eller på vegne av den fysiske eller juridiske person eller det organ som vedkommende representerer,
4. «signaturframstillingsdata»: unike data, som koder eller private kryptonøkler, som underskriveren bruker for å opprette en elektronisk signatur,
5. «signaturframstillingsprodukt»: konfigurert programvare eller maskinvare for behandling av signaturframstillingsdata,
6. «sikkert signaturframstillingsprodukt»: et signaturframstillingsprodukt som oppfyller kravene fastsatt i vedlegg III,
7. «signaturverifikasjonsdata»: data, som koder eller offentlige kryptonøkler, som brukes for å verifisere en elektronisk signatur,
8. «signaturverifikasjonssystem»: konfigurert programvare eller maskinvare som brukes til behandling av signaturverifikasjonsdata,
9. «sertifikat»: en elektronisk attestering som knytter signaturverifikasjonsdata til en person og bekrefter personens identitet,
10. «kvalifisert sertifikat»: et sertifikat som oppfyller kravene omhandlet i vedlegg II,
11. «tilbyder av sertifikattjenester»: et organ eller en fysisk eller juridisk person som utsteder sertifikater eller tilbyr andre tjenester i tilknytning til elektroniske signaturer,
12. «elektronisk-signatur-produkt»: maskinvare eller programvare eller en særskilt tilknyttet komponent som er beregnet på å brukes av en tilbyder av sertifikattjenester for å tilby sertifikattjenester, eller som er beregnet på å brukes for å opprette eller verifisere elektroniske signaturer,
13. «frivillig akkreditering»: enhver tillatelse som fastsetter rettigheter og forpliktelser for ytelse av sertifikattjenester, som skal utstedes på anmodning fra den berørte tilbyder av sertifikattjenester av det offentlige eller private organ som er pålagt å utarbeide og føre tilsyn med overholdelse av slike rettigheter og forpliktelser, og der tilbyderen av sertifikattjenester ikke er berettiget til å utøve de rettighetene som tillatelsen gir før vedkommende har mottatt organets beslutning.

Artikkel 3

Markedsadgang

1. Medlemsstatene skal ikke tilby sertifikattjenester som er underlagt forhåndstillatelse.
2. Med forbehold for bestemmelsene i nr. 1 kan medlemsstatene innføre eller opprettholde frivillige akkrediteringsordninger med sikte på å tilby bedre sertifikattjenester. Alle vilkår i forbindelse med slike ordninger skal være objektive, klare, forholdsmessige og ikke-diskriminerende. Medlemsstatene kan ikke begrense antallet akkrediterte tilbydere av sertifikattjenester av årsaker som omfattes av dette direktivs virkeområde.
3. Hver enkelt medlemsstat skal sikre at det opprettes et egnet system som gjør det mulig å føre tilsyn med tilbydere av sertifikattjenester som er etablert på deres territorium, og som utsteder kvalifiserte sertifikater til offentligheten.
4. Egnede offentlige eller private organer som utpekes av medlemsstatene skal avgjøre om de sikre signaturframstillingsproduktene er i samsvar med kravene omhandlet i vedlegg III. Kommisjonen skal etter framgangsmåten omhandlet i artikkel 9 fastsette kriterier slik at medlemsstatene kan bestemme om et organ skal utpekes eller ikke. Alle medlemsstatene skal anerkjenne avgjørelsen til organene nevnt i første ledd om at kravene i vedlegg III er oppfylt.
5. I samsvar med framgangsmåten fastsatt i artikkel 9 kan Kommisjonen opprette og offentliggjøre i De Europeiske Fellesskaps Tidende referansenumre for allment anerkjente standarder for elektronisk-signatur-produkter. Når et elektronisk-signatur-produkt oppfyller disse standardene, skal medlemsstatene gå ut fra at det oppfyller kravene omhandlet i vedlegg II, bokstav f) og i vedlegg III.
6. Medlemsstatene og Kommisjonen skal samarbeide for å fremme utviklingen og bruken av signaturverifikasjonssystemer i lys av anbefalingene om sikker signaturverifikasjon i vedlegg IV og av hensyn til forbrukerens interesser.
7. Medlemsstatene kan bruke elektroniske signaturer i offentlig sektor, forutsatt at eventuelle tilleggskrav oppfylles. Slike krav skal være objektive, klare, forholdsmessige og ikke-diskriminerende, og skal bare gjelde den aktuelle anvendelsens særskilte kjennetegn. Slike krav skal ikke utgjøre noen hindring for tjenester over landegrensene til borgerne.

Artikkel 4

Prinsipper for det indre marked

1. Hver enkelt medlemsstat skal anvende de nasjonale reglene de vedtar i henhold til dette direktiv, på tilbydere av sertifikattjenester som er etablert på deres territorium og på de tjenestene de tilbyr. Medlemsstatene kan ikke begrense leveringen av sertifikattjenester med opprinnelse i en annen medlemsstat på områder som omfattes av dette direktiv.
2. Medlemsstatene skal sikre fri bevegelse i det indre marked av elektronisk-signatur-produkter som etterkommer dette direktiv.

Artikkel 5

Elektroniske signaturers rettsvirkninger

1. Medlemsstatene skal sikre at avanserte elektroniske signaturer opprettet på grunnlag av et kvalifisert sertifikat, og som er opprettet ved hjelp av et signaturframstillingsprodukt,
 - a) oppfyller lovfestede krav til en signatur i forbindelse med data i elektronisk form, på samme måte som en håndskrevet signatur oppfyller disse kravene i forbindelse med data på papir, og
 - b) godtas som bevis under rettergang.
2. Medlemsstatene skal sikre at en elektronisk signatur ikke nektes rettslig gyldighet eller ikke godtas som bevis under rettergang utelukkende fordi den er
 - i elektronisk form,
 - ikke er dannet på grunnlag av et kvalifisert sertifikat,
 - ikke er dannet på grunnlag av et kvalifisert sertifikat utstedt av en akkreditert tilbyder av sertifikattjenester eller
 - ikke er opprettet av et sikkert signaturframstillingsprodukt.

Artikkel 6

Erstatningsansvar

1. Medlemsstatene skal som et minimum sikre at når en tilbyder av sertifikattjenester utsteder et sertifikat til offentligheten som et kvalifisert sertifikat, eller som garanterer et slikt sertifikat overfor offentligheten, har erstatningsansvaret for skade forvoldt ethvert organ eller enhver fysisk eller juridisk person som med rimelighet stoler på dette sertifikatet når det gjelder
 - a) at alle opplysningene på det kvalifiserte sertifikatet er korrekte på utstedelsestidspunktet, og at sertifikatet inneholder alle detaljer som et kvalifisert sertifikat skal inneholde,
 - b) vissheten om at underskriveren som er identifisert på det kvalifiserte sertifikatet på utstedelsestidspunktet for sertifikatet hadde de signaturframstillingsdataene som tilsvarte signaturverifikasjonsdataene som var angitt eller identifisert på sertifikatet,
 - c) vissheten om at signaturframstillingsdataene og signaturverifikasjonsdataene kan utfylle hverandre i tilfeller der tilbyderen av sertifikattjenester genererer begge, med mindre tilbyderen av sertifikattjenester kan bevise at han eller hun ikke har handlet uaktsomt.
2. Medlemsstatene skal som et minimum sikre at en tilbyder av sertifikattjenester, som har utstedt et sertifikat til offentligheten som et kvalifisert sertifikat, har erstatningsansvaret for skade forvoldt ethvert organ eller enhver fysisk eller juridisk person som med rimelighet stoler på sertifikatet når det gjelder manglende registrering av tilbakekalling av sertifikatet, med mindre tilbyderen av sertifikattjenester kan bevise at han eller hun ikke har handlet uaktsomt.
3. Medlemsstatene skal sikre at en tilbyder av sertifikattjenester på et kvalifisert sertifikat kan angi de fastsatte begrensninger for bruken av sertifika-

tet, forutsatt at begrensningene er tydelige for tredjeparter. Tilbyderen av sertifikattjenester skal ikke ha erstatningsansvar for skade som følge av at bruken av et kvalifisert sertifikat overskrider begrensningene for sertifikatet.

4. Medlemsstatene skal sikre at en tilbyder av sertifikattjenester på et kvalifisert sertifikat kan angi grenseverdien for de transaksjoner sertifikatet kan brukes til, forutsatt at denne grensen er tydelig for tredjeparter. Tilbyderen av sertifikattjenester skal ikke ha erstatningsansvar for skade som følge av at denne øvre grensen overstiges.
5. Bestemmelsene i nr. 1-4 berører ikke anvendelsen av rådsdirektiv 93/13/EØF av 5. april 1993 om urimelige vilkår i forbrukeravtaler ¹¹⁾

Artikkel 7

Internasjonale aspekter

1. Medlemsstatene skal sikre at sertifikater som utstedes til offentligheten som kvalifiserte sertifikater, av tilbydere av sertifikattjenester som er etablert i en tredjestat, anses som rettslig likestilte med sertifikater utstedt av tilbydere av sertifikattjenester som er etablert innenfor Fellesskapet,
 - a) dersom tilbyderen av sertifikattjenester oppfyller kravene fastsatt i dette direktiv, og er akkreditert i henhold til en frivillig akkrediteringsordning som er opprettet i en medlemsstat, eller
 - b) dersom en tilbyder av sertifikattjenester etablert innenfor Fellesskapet, som oppfyller kravene fastsatt i dette direktiv, garanterer sertifikatet, eller
 - c) dersom sertifikatet eller tilbyderen av sertifikattjenester er anerkjent i henhold til en bilateral eller multilateral avtale mellom Fellesskapet og tredjestater eller internasjonale organisasjoner.
2. For å lette sertifikattjenester over landegrensene med tredjestater og rettslig anerkjennelse av avanserte elektroniske signaturer med opprinnelse i tredjestater, skal Kommisjonen eventuelt fremsette forslag med hensyn til den faktiske gjennomføringen av standarder for og internasjonale avtaler om sertifikattjenester. Dersom det er nødvendig, skal den særlig framlegge for Rådet forslag om egnede mandater for bilaterale og multilaterale avtaler med tredjestater og internasjonale organisasjoner. Rådet skal treffe sin beslutning med kvalifisert flertall.
3. Når Kommisjonen underrettes om vanskeligheter som fellesskapsforetak møter på ved markedsadgang i tredjestater, kan den om nødvendig framlegge for Rådet forslag om egnede mandat til å forhandle om tilsvarende rettigheter for fellesskapsforetak i disse tredjestatene. Rådet skal treffe sin beslutning med kvalifisert flertall.

Tiltak som treffes i henhold til dette nummer, berører ikke Kommisjonens og medlemsstatenes forpliktelser i henhold til gjeldende internasjonale avtaler.

¹¹⁾ EFT L 95 av 21.4 1993, s. 29.

Artikkel 8

Datasikring

1. Medlemsstatene skal sikre at tilbydere av sertifikattjenester, og nasjonale organer som er ansvarlige for akkreditering eller tilsyn, etterkommer kravene fastsatt i europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger ¹²⁾
2. Medlemsstatene skal sikre at en tilbyder av sertifikattjenester som utsteder sertifikater til offentligheten kan innsamle personopplysninger bare direkte fra den registrerte, eller med den registrertes direkte samtykke, og bare i den grad det er nødvendig for å utstede og opprettholde sertifikatet. Dataene kan ikke innsamles eller behandles for andre formål uten den registrertes uttrykkelige samtykke.
3. Med forbehold for pseudonymers rettsvirkning i henhold til nasjonal lovgivning skal ikke medlemsstatene hindre tilbydere av sertifikattjenester i å oppgi et pseudonym på sertifikatet i stedet for underskriverens navn.

Artikkel 9

Komité

1. Kommisjonen skal bistås av en «komité for elektroniske signaturer», heretter kalt «komiteen».
2. Når det vises til dette nummer, får artikkel 4 og 7 i beslutning 1999/468/EF anvendelse, der bestemmelsene i beslutningens artikkel 8 skal overholdes.
Tidsrommet nevnt i artikkel 4 nr. 3 i beslutning 1999/468/EF skal fastsettes til tre måneder.
3. Komiteen skal vedta sin egen forretningsorden.

Artikkel 10

Komiteens oppgaver

Komiteen skal etter framgangsmåten omhandlet i artikkel 9 nr. 2 presisere kravene nevnt i vedleggene til dette direktiv, kriteriene nevnt i artikkel 3 nr. 4 og de allment anerkjente standarder for elektronisk-signatur-produkter opprettet og offentliggjort i henhold til artikkel 3 nr. 5.

Artikkel 11

Underretning

1. Medlemsstatene skal underrette Kommisjonen og de øvrige medlemsstatene om følgende:

¹²⁾ EFT L 281 av 23.11 1995, s. 31.

- a) opplysninger om frivillige nasjonale akkrediteringsordninger, herunder ethvert tilleggskrav i henhold til artikkel 3 nr. 7,
 - b) navnet og adressen til de nasjonale organer som er ansvarlige for akkreditering og tilsyn samt til organene nevnt i artikkel 3 nr. 4 og
 - c) navnet og adressen til samtlige akkrediterte nasjonale tilbydere av sertifikattjenester.
1. Medlemsstatene skal så snart som mulig underrette om samtlige opplysninger som gis i henhold til nr. 1.

Artikkel 12

Gjennomgang

1. Kommisjonen skal foreta en gjennomgang av anvendelsen av dette direktiv, og framlegge en rapport om dette for Europaparlamentet og Rådet innen 19. juli 2003.
2. I denne gjennomgangen skal det blant annet tas stilling til om direktivets virkeområde bør endres for å ta hensyn til teknologisk, markedsmessig og rettslig utvikling. Rapporten skal på grunnlag av oppnådd erfaring særlig omfatte en vurdering av harmoniseringsarbeidet. Rapporten skal eventuelt vedlegges forslag til nytt regelverk.

Artikkel 13

Gjennomføring

1. Medlemsstatene skal sette i kraft de lover og forskrifter som er nødvendige for å etterkomme dette direktiv, innen 19. juli 2001. De skal umiddelbart underrette Kommisjonen om dette.
Disse bestemmelsene skal, når de vedtas av medlemsstatene, inneholde en henvisning til dette direktiv, eller det skal vises til direktivet når de kunngjøres. Nærmere regler for henvisningen fastsettes av medlemsstatene.
2. Medlemsstatene skal oversende Kommisjonen teksten til de viktigste internrettslige bestemmelser som de vedtar på det området dette direktiv omhandler.

Artikkel 14

Ikrafttredelse

Dette direktiv trer i kraft den dagen det kunngjøres i De Europeiske Fellesskaps Tidende.

Artikkel 15

Mottakere

Dette direktiv er rettet til medlemsstatene.

Utferdiget i Brussel, 13. desember 1999.

<i>For Europaparlamentet</i>	<i>For Rådet</i>
N. FONTAINE	S. HASSI
<i>President</i>	<i>Formann</i>

Vedlegg I

Krav til kvalifiserte sertifikater

Kvalifiserte sertifikater skal inneholde

- a) angivelse av at sertifikatet er utstedt som et kvalifisert sertifikat,
- b) identiteten til tilbyderen av sertifikattjenester og staten vedkommende er etablert i,
- c) underskriverens navn eller pseudonym, der det skal framgå om det er et pseudonym,
- d) særskilte opplysninger om underskriveren som eventuelt skal tilføyes, avhengig av hva sertifikatet skal brukes til,
- e) signaturverifikasjonsdataene som tilsvarer signaturframstillingsdataene som underskriveren har kontroll over,
- f) angivelse av ikrafttredelses- og utløpsdato for sertifikatets gyldighetstid,
- g) sertifikatets identitetskode,
- h) den avanserte elektroniske signaturen til tilbyderen av sertifikattjenester,
- i) eventuelle begrensninger i sertifikatets bruksområde og
- j) eventuelle begrensninger i transaksjonsverdiene som sertifikatet kan brukes til.

Vedlegg II

Krav til tilbydere av sertifikattjenester som utsteder kvalifiserte sertifikater

Tilbydere av sertifikattjenester skal

- a) utvise den pålitelighet som er nødvendig for å tilby sertifikattjenester,
- b) sikre en hurtig og sikker katalogtjeneste og en sikker og øyeblikkelig tilbakekallingstjeneste,
- c) sørge for at det er mulig å fastslå nøyaktig dato og tidspunkt for sertifikatets utstedelse og tilbakekalling,
- d) med egnede midler i samsvar med nasjonal lovgivning verifisere identiteten og eventuelle særlige opplysninger om personen som sertifikatet er utstedt til,
- e) ansette personale som har den sakkunnskap, erfaring og de kvalifikasjoner som er nødvendige for de tjenestene som ytes, særlig lederkompetanse, kompetanse innenfor teknologien med elektroniske signaturer og god kjennskap til korrekte sikkerhetsrutiner. De skal også bruke adekvate forvaltnings- og driftsprosedyrer som overholder anerkjente standarder,
- f) bruke pålitelige systemer og produkter som er beskyttet mot endringer og som garanterer sikkerheten med hensyn til teknikk og kryptografi i pro-

- sessene de støtter,
- g) treffe tiltak mot forfalskning av sertifikater og, når tilbyderen av sertifikat-tjenester genererer signaturframstillingsdata, garanterer fortroligheten under genereringen av disse dataene,
 - h) opprettholde tilstrekkelige økonomiske midler for å drive virksomheten i samsvar med kravene fastsatt i dette direktiv, særlig for å påta seg erstatningsansvaret, for eksempel ved å tegne en egnet forsikring,
 - i) registrere alle viktige opplysninger om et kvalifisert sertifikat i en passende periode, særlig for å kunne framlegge bevis for sertifisering i en rettssak. Denne registreringen kan gjøres elektronisk,
 - j) ikke oppbevare eller kopiere signaturframstillingsdataene til en person som tilbyderen av sertifikattjenester har levert nøkkelforvaltningstjenester til,
 - k) før de inngår et kontraktsforhold med en person som søker om et sertifikat for sin elektroniske signatur, ved hjelp av et varig kommunikasjonsmiddel gi vedkommende opplysninger om de nøyaktige vilkår for bruken av sertifikatet, herunder begrensninger i bruken, eksistensen av en frivillig akkrediteringsordning og klage- og tvisteløsningsprosedyrer. Slike opplysninger, som kan overføres elektronisk, skal være skriftlige og på et lett forståelig språk. Viktige deler av disse opplysningene skal også gjøres tilgjengelige på anmodning fra tredjeparter som stoler på sertifikatet,
 - l) bruke pålitelige systemer til å oppbevare sertifikater i en verifiserbar form i slik at
 - bare autoriserte personer kan gjøre tilføyelser og endringer,
 - opplysningenes autentisitet kan kontrolleres,
 - sertifikatene er offentlig tilgjengelige bare når innehaveren av sertifikatet har gitt sitt samtykke til det, og
 - enhver teknisk endring som setter disse sikkerhetskravene i fare er synlige for operatøren.

Vedlegg III

Krav til sikre signaturframstillingsprodukter

1. De sikre signaturframstillingsproduktene skal ved hjelp av tekniske midler og egnede framgangsmåter minst sikre at
 - a) signaturframstillingsdataene som brukes ved signaturgenerering i praksis kan forekomme bare én gang, og at de med rimelig sikkerhet forblir hemmelige,
 - b) signaturframstillingsdataene som brukes ved signaturgenerering med rimelig sikkerhet ikke kan utledes, og at signaturen ved hjelp av tilgjengelig teknologi er beskyttet mot forfalskning,
 - c) den rettmessige underskriveren på en pålitelig måte sikrer at signaturframstillingsdataene som brukes ved signaturgenerering ikke brukes av andre.
2. De sikre signaturframstillingsproduktene skal ikke endre dataene som skal underskrives, eller hindre at disse dataene presenteres for underskriveren i forkant av signaturprosessen.

*Vedlegg IV***Anbefalinger om sikker signaturverifikasjon**

I løpet av signaturverifikasjonsprosessen bør det med rimelig sikkerhet sørges for at

- a) dataene som brukes for å verifisere signaturen tilsvarer dataene som forevises signaturkontrolløren,
- b) signaturen er pålitelig verifisert og at resultatet av verifikasjonen vises korrekt,
- c) signaturkontrolløren, om nødvendig, på en sikker måte kan fastslå innholdet i de signerte dataene,
- d) sertifikatets autentisitet og gyldighet som kreves på tidspunktet for signaturverifikasjonen er verifisert på en sikker måte,
- e) resultatet av verifikasjonen og underskriverens identitet vises korrekt,
- f) bruken av pseudonym kommer klart fram og
- g) enhver endring av sikkerhetsmessig betydning kan oppdages.
