

2001/EØS/31/29

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⁽¹⁾,

under henvisning til uttalelse fra Den økonomiske og sosiale komité⁽²⁾,

under henvisning til uttalelse fra Regionkomiteen⁽³⁾,

etter framgangsmåten fastsatt i traktatens artikkel 251⁽⁴⁾ og

ut fra følgende betraktninger:

- 1) 16. april 1997 framla Kommisjonen for Europaparlamentet, Rådet, Den økonomiske og sosiale komité og Regionkomiteen en melding om et europeisk initiativ innenfor elektronisk handel.
- 2) 8. oktober 1997 framla Kommisjonen for Europaparlamentet, Rådet, Den økonomiske og sosiale komité og Regionkomiteen en melding med tittelen «Sikkerhet og tillit i elektronisk kommunikasjon – mot en europeisk ramme for digitale underskrifter og kryptering».
- 3) 1. desember 1997 anmodet Rådet Kommisjonen 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 og for 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 tilliten til den nye teknologien og den allmenne anerkjennelsen av den. Medlemsstatenes lovgivning bør ikke hindre fri bevegelighet for varer og tjenester i det indre marked.
- 5) Elektronisk-signatur-produkters samvirkingsevne bør fremmes. I henhold til traktatens artikkel 14 omfatter det indre marked et område uten indre grenser med fri bevegelighet for varer. Grunnleggende særskilte krav til elektronisk-signatur-produkter må overholdes for å sikre fri bevegelighet i det indre marked og for å skape tillit til elektroniske signaturer, med forbehold for rådsforordning (EF) nr. 3381/94 av 19. desember 1994 om opprettelse av en fellesskapsordning for kontroll med eksport av varer av flerbrukskarakter⁽⁵⁾ og rådsbeslutning 94/942/FUSP av 19. desember 1994 om en felles aksjon vedtatt av Rådet vedrørende kontroll med eksport av varer av flerbrukskarakter⁽⁶⁾.
- 6) Dette direktiv harmoniserer ikke tjenesteyting med hensyn til opplysningenes fortrolighet når tjenesteytingen omfattes av nasjonale bestemmelser om offentlig orden (ordre public) eller offentlig sikkerhet.
- 7) Det indre marked sikrer fri bevegelighet for personer, med det resultatet at unionsborgere og andre som er bosatt i Den europeiske union, stadig oftere må ha kontakt med myndighetene i andre medlemsstater enn den de er bosatt i. Elektronisk kommunikasjon vil kunne bli til stor nytte i den forbindelse.
- 8) Den raske teknologiske utviklingen og Internetts globale karakter gjør det nødvendig å velge en framgangsmåte som åpner for forskjellig teknologi og forskjellige tjenester som muliggjør elektronisk autentisering av data.
- 9) Elektroniske signaturer vil få anvendelse i en rekke forskjellige situasjoner og på en rekke forskjellige bruksområder, noe som vil føre til et bredt spekter av nye tjenester og produkter i tilknytning til eller basert på bruk av 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 støtter elektroniske signaturer, som registreringstjenester, tidsstempeling, katalogtjenester, databehandlingstjenester eller rådgivningstjenester i forbindelse med elektroniske signaturer.

(*) Denne fellesskapsrettsakten, kunngjort i EFT L 13 av 19.1.2000, s. 12, er omhandlet i EØS-komiteens beslutning nr. 66/2000 av 2. august 2000 om endring av EØS-avtalens vedlegg XI (Telekommunikasjonstjenester), se EØS-tillegget til De Europaiske Fellesskaps Tidende nr. 44 av 5.10.2000, s. 2.

⁽¹⁾ EFT C 325 av 23.10.1998, s. 5.

⁽²⁾ EFT C 40 av 15.2.1999, s. 29.

⁽³⁾ EFT C 93 av 6.4.1999, s. 33.

⁽⁴⁾ Europaparlamentsuttalelse av 13. januar 1999 (EFT C 104 av 14.4.1999, s. 49), Rådets felles holdning av 28. juni 1999 (EFT C 243 av 27.8.1999, s. 33) og europaparlamentsbeslutning av 27. oktober 1999 (ennå ikke offentliggjort i EFT). Rådsbeslutning av 30. november 1999.

⁽⁵⁾ 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).

⁽⁶⁾ 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).

- 10) Det indre marked gjør det mulig for tilbydere av sertifikattjenester å utvikle sin virksomhet over landegrensene med sikte på å øke sin konkurransedyktighet og på den måten tilby forbrukere og industri 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 ytingen av sertifikattjenester over åpne nett i hele Fellesskapet. 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 tilbydere av sertifikattjenester den riktige rammen for å utvikle sine tjenester ytterligere i retning av det tillits-, sikkerhets- og kvalitetsnivå som et marked i utvikling krever. Slike ordninger bør fremme utviklingen av optimal praksis blant tilbydere av sertifikattjenester. Tilbydere av sertifikattjenester bør fritt kunne slutte seg til slike akkrediteringsordninger og dra nytte av dem.
- 12) Sertifikattjenestene bør kunne 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 drive virksomhet utenfor slike frivillige akkrediteringsordninger. Det bør sikres at akkrediteringsordningene ikke svekker konkurransen på området sertifikattjenester.
- 13) Medlemsstatene kan selv avgjøre hvordan de vil føre tilsyn med overholdelsen av bestemmelsene fastsatt i dette direktiv. Dette direktiv er ikke til hinder for opprettelse av tilsynsordninger basert på privat sektor. Dette direktiv gir ikke tilbydere av sertifikattjenester pålegg om å søke om å bli undergitt tilsyn i henhold til en gjeldende akkrediteringsordning.
- 14) Det er viktig å finne den riktige balansen mellom forbrukernes og næringslivets behov.
- 15) Vedlegg III omfatter krav til sikre signaturframstillings-systemer for å sikre at avanserte elektroniske signaturer fungerer på en hensiktsmessig måte. Det omfatter ikke det totale miljøet disse systemene opererer i. For at det indre marked skal virke på en tilfredsstillende måte, må Kommisjonen og medlemsstatene handle raskt for å gjøre det mulig å utpeke de organer som skal foreta samsvars-vurderingen av de sikre signaturframstillingssystemene i henhold til vedlegg III. For å oppfylle markedets behov må samsvars-vurderingen utføres effektivt og til rett tid.
- 16) Dette direktiv bidrar til bruk og rettslig anerkjennelse av elektroniske signaturer i Fellesskapet. Det er ikke behov for rammeregler for elektroniske signaturer som brukes utelukkende i systemer basert på 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 rett 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 formkrav i forbindelse med underskrifter. Bestemmelsene om elektroniske signaturers rettsvirkninger bør ikke berøre formkrav fastsatt ved nasjonal lovgivning med hensyn til kontraktsinngåelse eller regler til avgjørelse av hvor en kontrakt er inngått.
- 18) Oppbevaring og kopiering av signaturframstillingsdata vil 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 i forbindelse med offentlige innkjøp, beskatning og trygd-, helse- og rettsystemet.
- 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 underskrifters rettslige gyldighet. Sertifikater kan brukes til å identifisere en person som underskriver elektronisk. Målet med avanserte elektroniske signaturer som er basert på kvalifiserte sertifikater, er å skape et høyere sikkerhetsnivå. Avanserte elektroniske signaturer som er basert på et kvalifisert sertifikat, og som er laget ved hjelp av et sikkert signaturframstillingssystem, kan i rettslig sammenheng anses for å tilsvare håndskrevne underskrifter bare dersom kriteriene for håndskrevne underskrifter 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 bygge på objektive kriterier og ikke avhenge av godkjenning av den berørte tilbyderen av sertifikattjenester. Nasjonal lovgivning avgjør hvilke rettsområder som elektroniske dokumenter og elektroniske signaturer kan anvendes på. Dette direktiv berører ikke en nasjonal domstols kompetanse til å avgjøre om kravene i dette direktiv er overholdt, og heller ikke nasjonale regler om domstolens frie bevisbedømmelse.
- 22) Tilbydere av sertifikattjenester som tilbyr sertifikat-tjenester til offentligheten, er underlagt nasjonale regler for erstatningsansvar.

- 23) Utviklingen innen internasjonal elektronisk handel krever internasjonale avtaler som involverer tredjestater. For å sikre samvirkningsevne på globalt plan kan det være hensiktsmessig å inngå avtaler med tredjestater om multilaterale regler for gjensidig anerkjennelse av 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 i sertifikater skal ikke hindre medlemsstatene i å kreve at personer identifiserer seg i henhold til fællesskapsrett eller nasjonal lovgivning.
- 26) De tiltak som er nødvendige for å gjennomføre 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⁽¹⁾.
- 27) Kommisjonen skal to år etter gjennomføringen av dette direktiv foreta en gjennomgang av direktivet, blant annet for å sikre at tekniske framskritt eller juridiske endringer ikke har lagt hindringer i veien for virkeliggjøringen av målene nedfelt i direktivet. Kommisjonen bør undersøke virkningene av beslektede tekniske områder og framlegge rapport om dette for Europaparlamentet og Rådet.
- 28) Målet som går ut på å skape en harmonisert rettslig ramme for elektroniske signaturer og tilknyttede tjenester, kan ikke i tilstrekkelig grad virkeliggjøres av medlemsstatene, og kan derfor i samsvar med nærhets- og forholdsmessighetsprinsippet omhandlet i traktatens artikkel 5 bedre virkeliggjøres av Fællesskapet. Dette direktiv går ikke lenger enn det som er nødvendig for å nå dette målet –

VEDTATT DETTE DIREKTIV:

Artikkel 1

Virkeområde

Formålet med dette direktiv er å gjøre det enklere å bruke elektroniske signaturer og bidra til rettslig anerkjennelse av dem. Det fastlegger en rettslig ramme for elektroniske signaturer og visse sertifikattjenester for å sikre at det indre marked virker på en tilfredsstillende måte.

Det omfatter ikke aspekter i forbindelse med inngåelse av kontrakter og kontraktens gyldighet eller andre rettslige forpliktelser som i henhold til nasjonal lovgivning eller Fællesskapets regelverk er underlagt formkrav; det berører

heller ikke regler eller begrensninger som i henhold til nasjonal lovgivning eller Fællesskapets regelverk gjelder for anvendelse av dokumenter.

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 laget ved hjelp av midler som bare underskriveren kan bevare kontroll over, og
 - d) den er knyttet til dataene som den vedrører på en slik måte at enhver senere endring kan oppdages,
- 3) «underskriver», enhver person som disponerer et signaturframstillingssystem, og som handler enten på vegne av seg selv eller på vegne av den fysiske eller juridiske person eller det organ vedkommende representerer,
- 4) «signaturframstillingsdata», unike data, som koder eller private kryptonøkler, som underskriveren benytter for å framstille en elektronisk signatur,
- 5) «signaturframstillingssystem», konfigurert programvare eller maskinvare for behandling av signaturframstillingsdata,
- 6) «sikkert signaturframstillingssystem», et signaturframstillingssystem som oppfyller kravene fastsatt i vedlegg III,
- 7) «signaturverifikasjonsdata», data, som koder eller offentlige kryptonøkler, som benyttes til å verifisere en elektronisk signatur,
- 8) «signaturverifikasjonssystem», konfigurert programvare eller maskinvare som benyttes til behandling av signaturverifikasjonsdata,
- 9) «sertifikat», en elektronisk attestasjon som knytter signaturverifikasjonsdata til en person og bekrefter personens identitet,
- 10) «kvalifisert sertifikat», et sertifikat som oppfyller kravene i vedlegg I, og som leveres av en tilbyder av sertifikattjenester som oppfyller kravene 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 benyttes av en tilbyder av sertifikattjenester for å tilby sertifikattjenester, eller som

⁽¹⁾ EFT L 184 av 17.7.1999, s. 23.

er beregnet på å benyttes til å framstille eller verifisere elektroniske signaturer,

- 13) «frivillig akkreditering», enhver tillatelse som fastsetter rettigheter og forpliktelser for yting 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 overholdelsen 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 gjøre tilbudet om sertifikattjenester avhengig av forhåndsgodkjenning.

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 og forholdsmessige og sikre likebehandling. 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 sikre signaturframstillings-systemer oppfyller kravene 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 de avgjørelser som organene nevnt i første ledd treffer med hensyn til oppfyllelse av kravene i vedlegg III.

5. I samsvar med framgangsmåten fastsatt i artikkel 9 kan Kommisjonen opprette og offentliggjøre i *De Europaiske 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 i vedlegg II bokstav f) og i vedlegg III.

6. Medlemsstatene og Kommisjonen skal samarbeide for å fremme utviklingen og bruken av signaturverifikasjons-systemer i lys av anbefalingene om sikker signaturverifikasjon i vedlegg IV og for å ivareta forbrukerens interesser.

7. Medlemsstatene kan bruke elektroniske signaturer i offentlig sektor, forutsatt at eventuelle tilleggskrav oppfylles. Slike krav skal være objektive, klare og forholdsmessige og sikre likebehandling, og skal bare gjelde den aktuelle anvendelsens særskilte kjennetegn. Slike krav skal ikke utgjøre noen hindring for yting av tjenester over landegrensene til borgerne.

Artikkel 4

Prinsipper for det indre marked

1. Medlemsstatene 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 disse tilbyr. Medlemsstatene kan ikke begrense ytingen av sertifikattjenester med opprinnelse i en annen medlemsstat på områder som omfattes av dette direktiv.

2. Medlemsstatene skal sikre fri bevegelighet i det indre marked for elektronisk-signatur-produkter som etterkommer dette direktiv.

Artikkel 5

Elektroniske signaturers rettsvirkninger

1. Medlemsstatene skal sikre at avanserte elektroniske signaturer som er basert på et kvalifisert sertifikat, og som er framstilt ved hjelp av et sikkert signaturframstillingssystem,

a) oppfyller lovfestede krav til en signatur i forbindelse med data i elektronisk form, på samme måte som en håndskrevet underskrift oppfyller disse kravene i forbindelse med data på papir, og

b) kan 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 basert på et kvalifisert sertifikat,

– ikke er basert på et kvalifisert sertifikat utstedt av en akkreditert tilbyder av sertifikattjenester eller

– ikke er framstilt av et sikkert signaturframstillingssystem.

Artikkel 6

Erstatningsansvar

1. Medlemsstatene skal som et minimum sikre at en tilbyder av sertifikattjenester som utsteder et sertifikat til offentligheten som et kvalifisert sertifikat, eller som garanterer et slikt sertifikat overfor offentligheten, har erstatningsansvar for skade påført ethvert organ eller enhver fysisk eller juridisk person som med rimelighet stoler på dette sertifikatet når det gjelder

- a) at alle opplysningene i 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 i det kvalifiserte sertifikatet, på utstedelsestidspunktet for sertifikatet var i besittelse av signaturframstillingsdataene som tilsvarer signaturverifikasjonsdataene som er angitt eller identifisert i 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 erstatningsansvar for skade påført ethvert organ eller enhver fysisk eller juridisk person som med rimelighet stoler på sertifikatet, med hensyn til 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 i et kvalifisert sertifikat kan angi begrensninger for bruken av sertifikatet, 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 sertifikatets begrensninger.

4. Medlemsstatene skal sikre at en tilbyder av sertifikattjenester i et kvalifisert sertifikat kan angi en beløpsgrense for de transaksjoner sertifikatet kan brukes til, forutsatt at denne beløpsgrensen er tydelig for tredjeparter.

Tilbyderen av sertifikattjenester skal ikke ha erstatningsansvar for skade som følge av at beløpsgrensen overstiges.

5. Bestemmelsene i nr. 1 til 4 berører ikke anvendelsen av rådsdirektiv 93/13/EØF av 5. april 1993 om urimelige vilkår i forbrukeravtaler⁽¹⁾.

Artikkel 7

Internasjonale aspekter

1. Medlemsstatene skal sikre at sertifikater utstedt 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 Fællesskapet,

- 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 som er etablert innenfor Fællesskapet, og 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 Fællesskapet og tredjestater eller internasjonale organisasjoner.

2. For å lette ytingen av sertifikattjenester over landegrensene med tredjestater og rettslig anerkjennelse av avanserte elektroniske signaturer med opprinnelse i tredjestater, skal Kommisjonen eventuelt framsette forslag med hensyn til den faktiske gjennomføringen av standarder og internasjonale avtaler som får anvendelse på sertifikattjenester. Dersom det er nødvendig, skal den særlig framlegge for Rådet forslag til egnede mandater for å framforhandle bilaterale og multilaterale avtaler med tredjestater og internasjonale organisasjoner. Rådet skal treffe sin beslutning med kvalifisert flertall.

3. Når Kommisjonen underrettes om vanskeligheter som fællesskapsforetak møter med hensyn til markedsadgang i tredjestater, kan den om nødvendig framlegge for Rådet forslag til et egnet mandat for å framforhandle tilsvarende rettigheter for fællesskapsforetak i disse tredjestatene. Rådet skal treffe sin beslutning med kvalifisert flertall.

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

Artikkel 8

Datasikring

1. Medlemsstatene skal sikre at tilbydere av sertifikattjenester og nasjonale akkrediterings- og tilsynsorganer oppfyller kravene 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⁽²⁾.

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 uttrykkelige samtykke, og bare i den grad det er nødvendig for å utstede og opprettholde et sertifikat. Data 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 medlemsstatene ikke hindre tilbydere av sertifikattjenester i å oppgi et pseudonym i sertifikatet i stedet for underskriverens navn.

⁽¹⁾ EFT L 95 av 21.4.1993, s. 29.

⁽²⁾ EFT L 281 av 23.11.1995, s. 31.

*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, idet det tas hensyn til bestemmelsene i beslutningens artikkel 8.

Tidsrommet nevnt i artikkel 4 nr. 3 i beslutning 1999/468/EF fastsettes til tre måneder.

3. Komiteen vedtar selv sin 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 standardene for elektronisk-signatur-produkter som er utarbeidet og offentliggjort i henhold til artikkel 3 nr. 5.

*Artikkel 11***Underretning**

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

- a) opplysninger om frivillige nasjonale akkrediteringsordninger, herunder alle tilleggskrav i henhold til artikkel 3 nr. 7,
- b) navnet og adressen til nasjonale akkrediterings- og tilsynsorganer samt til organene nevnt i artikkel 3 nr. 4 og
- c) navnet og adressen til samtlige akkrediterte nasjonale tilbydere av sertifikatjenester.

2. Medlemsstatene skal så snart som mulig gi underretning om samtlige opplysninger som gis i henhold til nr. 1 samt om endringer i disse opplysningene.

*Artikkel 12***Gjennomgang**

1. Kommisjonen skal foreta en gjennomgang av måten dette direktiv virker på, og framlegge 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 om-handler.

*Artikkel 14***Ikrafttredelse**

Dette direktiv trer i kraft den dag det kunngjøres i *De Europeiske Fællesskaps Tidende*.

*Artikkel 15***Adressater**

Dette direktiv er rettet til medlemsstatene.

Utferdiget i Brussel, 13. desember 1999.

For Europaparlamentet

N. FONTAINE

President

For Rådet

S. HASSI

Formann

*VEDLEGG I***Krav til kvalifiserte sertifikater**

Kvalifiserte sertifikater skal inneholde

- a) angivelse av at sertifikatet er utstedt som et kvalifisert sertifikat,
- b) angivelse av identiteten til tilbyderen av sertifikattjenester og av den stat vedkommende er etablert i,
- c) underskriverens navn eller pseudonym; i det sistnevnte tilfellet skal det framgå at det er tale om et pseudonym,
- d) særskilte opplysninger om underskriveren som eventuelt skal tilføyes, avhengig av hva sertifikatet skal brukes til,
- e) signaturverifikasjonsdataene som tilsvarer signaturframstillingsdataene underskriveren har kontroll over,
- f) angivelse av sertifikatets ikrafttredelses- og utløpsdato,
- g) sertifikatets identitetskode,
- h) den avanserte elektroniske signaturen til tilbyderen av sertifikattjenester,
- i) eventuelle begrensninger i sertifikatets bruksområde, og
- j) eventuelle beløpmessige begrensninger med hensyn til transaksjoner 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 og i samsvar med nasjonal lovgivning verifisere identiteten og eventuelle særlige forhold i forbindelse med den personen sertifikatet er utstedt til,
- e) ansette personale som har den sakkunnskap og erfaring og de kvalifikasjoner som er nødvendige av hensyn til de tjenestene som ytes, særlig lederkompetanse, kompetanse innen teknologi for elektroniske signaturer og god kjennskap til korrekte sikkerhetsrutiner. De skal også bruke adekvate administrasjons- og driftsprosedyrer som overholder anerkjente standarder,
- f) bruke pålitelige systemer og produkter som er beskyttet mot endringer, og som garanterer den tekniske og kryptografiske sikkerheten i prosessene de støtter,
- g) treffe tiltak mot forfalskning av sertifikater og, når tilbyderen av sertifikattjenester genererer signaturframstillingsdata, garantere disse dataenes fortrolighet under genereringsprosessen,
- h) til enhver tid ha tilstrekkelige økonomiske midler for å drive virksomheten i samsvar med kravene fastsatt i dette direktiv, særlig for å bære erstatningsansvar, for eksempel ved å tegne en egnet forsikring,
- i) registrere alle viktige opplysninger om kvalifiserte sertifikater 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 ytt nøkkelforvaltningstjenester til,
- k) før de inngår et kontraktsforhold med en person som søker om 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 gis skriftlig og på et lett forståelig språk. Relevante deler av disse opplysningene skal også gjøres tilgjengelige på anmodning fra tredjeparter som stoler på sertifikatet,
- l) bruke pålitelige systemer til oppbevaring av sertifikater i en verifiserbar form slik
 - at bare autoriserte personer kan gjøre tilføyelser og endringer,
 - at opplysningenes autenticitet kan kontrolleres,
 - at sertifikatene er offentlig tilgjengelige bare når innehaveren av sertifikatet har gitt samtykke til det, og
 - at enhver teknisk endring som setter disse sikkerhetskrav i fare, er synlige for operatøren.

—

*VEDLEGG III***Krav til sikre signaturframstillingssystemer**

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

*VEDLEGG IV***Anbefalinger om sikker signaturverifikasjon**

I løpet av signaturverifikasjonsprosessen bør det med rimelig sikkerhet sørges for

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