EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV 1999/93/EF
af 13. december 1999
om en fællesskabsramme for elektroniske signaturer

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 47, stk. 2, artikel 55 og 95,

under henvisning til forslag fra Kommissionen ([1]),

under henvisning til udtalelse fra Det Økonomiske og Sociale Udvalg ([2]),

under henvisning til udtalelse fra Regionsudvalget ([3]),

i henhold til fremgangsmåden i traktatens artikel 251 ([4]), og

ud fra følgende betragtninger:

(1) Kommissionen forelagde den 16. april 1997 Europa-Parlamentet, Rådet, Det Økonomiske og Sociale Udvalg og Regionsudvalget en meddelelse med titlen »Et europæisk initiativ inden for elektronisk handel«;

(2) Kommissionen forelagde den 8. oktober 1997 Europa-Parlamentet, Rådet, Det Økonomiske og Sociale Udvalg og Regionsudvalget en meddelelse med titlen »Sikkerhed og tillid i elektronisk kommunikation — Imod europæiske rammer for digitale signaturer og kryptering«;

(3) Rådet opfordrede den 1. december 1997 Kommissionen til snarest muligt at forelægge Europa-Parlamentet og Rådet et forslag til direktiv om digitale signaturer;

(4) elektronisk kommunikation og handel nødvendiggør elektroniske signaturer og dertil knyttede tjenesteydelser til autentifikation af data; forskellige regler for retlig anerkendelse af elektroniske signaturer og akkreditering af certificeringstjenesteudbydere i medlemsstaterne kan skabe betydelige hindringer for anvendelse af elektronisk kommunikation og elektronisk handel; en klar fællesskabsramme vedrørende betingelserne for elektroniske signaturer vil derimod styrke tilliden til og den generelle accept af de nye teknologier; medlemsstaternes lovgivning bør ikke udgøre en hindring for den frie bevægelighed for varer og tjenesteydelser i det indre marked;

(5) elektronisk signatur-produkters interoperabilitet bør fremmes; efter traktatens artikel 14 indebærer det indre marked et område med fri bevægelighed for varer; specifikke væsentlige krav til elektronisk signatur-produkter skal opfyldes for at sikre fri bevægelighed på det indre marked og opbygge tilliden til elektroniske signaturer, jf. dog Rådets forordning (EF) nr. 3381/94 af 19. december 1994 om en fællesskabsordning for kontrol med udførsel af varer med dobbelt anvendelse ([5]) og afgørelse 94/942/FUSP af 19. december 1994 om en fælles aktion vedtaget af Rådet vedrørende kontrol med udførslen af varer med dobbelt anvendelse ([6]);

(6) dette direktiv harmoniserer ikke levering af tjenesteydelser med hensyn til informationens fortrolige karakter, hvis disse ydelser er omfattet af nationale bestemmelser med »ordre public« eller offentlig sikkerhed;

(7) det indre marked sikrer den fri bevægelighed for personer, hvorfor unionsborgere og andre, der er bosat i EU, i stigende omfang har behov for kontakt med myndigheder i andre medlemsstater end den, hvori de er bosiddende; elektronisk kommunikation vil kunne blive til stor nytte i den forbindelse;

(8) den hastige teknologiske udvikling og Internettets globale karakter nødvendiggør, at den valgte metode er åben for forskellige teknologier og tjenester til elektronisk autentifikation af data;

(9) elektroniske signaturer vil blive anvendt i mange forskellige situationer og i forbindelse med meget forskellige applikationer, hvilket vil resultere i en lang række nye tjenesteydelser og produkter i relation til elektroniske signaturer; definitionen af sådanne produkter og tjenesteydelser bør ikke begrænses til udstedelse og forvaltning af certifikater, men bør også omfatte alle andre tjenesteydelser eller produkter, der anvender eller understøtter elektroniske signaturer, såsom registreringstjenester, tidsstempling, katalogtjenester, databehandlingstjenester eller konsulenttjenester i forbindelse med elektroniske signaturer;

(10) det indre marked giver certificeringstjenesteudbydere mulighed for at udvikle deres aktiviteter hen over grænserne med henblik på at øge deres konkurrenceevne og dermed tilbyde forbrugere og erhvervsliv nye muligheder for sikker elektronisk informationsudveksling og handel uden hensyn til grænser; certificeringstjenesteudbydere bør for at stimulere udbuddet af certificeringstjenesteydelser via åbne net i hele Fællesskabet frit kunne tilbyde deres tjenesteydelser uden forudgående autorisation; ved forudgående autorisation forstås ikke alene enhver

([1]) EFT C 325 af 23.10.1998, s. 5.
([2]) EFT C 40 af 15.2.1999, s. 29.
([3]) EFT C 93 af 6.4.1999, s. 33.
([4]) Europa-Parlamentets udtalelse af 13. januar 1999 (EFT C 104 af 14.4.1999, s. 49), Rådets fælles holdning af 28. juni 1999 (EFT C 243 af 27.8.1999, s. 33), Europa-Parlamentets afgørelse af 27. oktober 1999 (endnu ikke offentliggjort i EFT) og Rådets afgørelse af 30. november 1999 (endnu ikke offentliggjort i EFT).

([5]) EFT L 367 af 31.12.1994, s. 1. Forordningen er ændret ved forordning (EF) nr. 837/95 (EFT L 90 af 21.4.1995, s. 1).
([6]) EFT L 367 af 31.12.1994, s. 8. Afgørelsen er senest ændret ved afgørelse 1999/193/FUSP (EFT L 73 af 19.3.1999, s. 1).

tilladelse, hvis udstedelse forudsætter, at de nationale myndigheder træffer en afgørelse, inden certificeringstjenesteudbyderen kan udbyde sine certificeringstjenester, men også enhver anden foranstaltning med samme virkning;

(11) frivillige akkrediteringsordninger, hvis sigte er et tjenesteydelsesudbud på et mere avanceret niveau, kunne være den rette ramme for certificeringstjenesteudbyderne til at udvikle deres tjenester yderligere i retning af det tillids-, sikkerheds- og kvalitetsniveau, som et marked i hastig udvikling kræver; sådanne ordninger bør anspore udviklingen af optimal praksis blandt certificeringstjenesteudbydere; det bør stå certificeringstjenesteudbydere frit for, om de ønsker at tilslutte sig og nyde godt af sådanne ordninger;

(12) certificeringstjenesterne bør kunne udbydes enten af et offentligt organ eller en fysisk eller juridisk person oprettet i overensstemmelse med national ret; medlemsstaterne bør ikke forhindre certificeringstjenesteudbydere i at holde sig uden for sådanne akkrediteringsordninger; det bør sikres, at frivillige akkrediteringsordninger ikke svækker konkurrencen blandt certificeringstjenester;

(13) medlemsstaterne kan selv fastsætte, hvordan de vil sikre overvågningen af overholdelsen af direktivets bestemmelser; dette direktiv er ikke til hinder for indførelsen af overvågningssystemer, der baseres på den private sektor; direktivet forpligter ikke certificeringstjenesteudbyderne til at ansøge om at blive overvåget i henhold til en gældende akkrediteringsordning;

(14) det er vigtigt at finde den rigtige balance mellem forbrugernes og erhvervslivets behov;

(15) bilag III omfatter krav til sikre signaturgenereringssystemer med henblik på at sikre, at avancerede elektroniske signaturer fungerer hensigtsmæssigt; det omfatter ikke det samlede omgivende miljø, som systemerne opererer i; for at det indre marked kan fungere efter hensigten, er det påkrævet, at Kommissionen og medlemsstatene handler hurtigt med henblik på at muliggøre udpegelsen af de organer, der skal foretage overensstemmelsesvurderingen af sikre signatursystemer, jf. bilag III; for at imødekomme markedets behov bør overensstemmelsesvurderingen være rettidig og effektiv;

(16) dette direktiv bidrager til anvendelse og retlig anerkendelse af elektroniske signaturer i Fællesskabet; der er ikke behov for lovfæstede rammeforskrifter for elektroniske signaturer, der udelukkende anvendes inden for systemer, som er baseret på frivillige privatretlige aftaler mellem et afgrænset antal deltagere; parternes frihed til indbyrdes at aftale, på hvilke betingelser de vil acceptere elektronisk signerede data, bør respekteres i det omfang, national ret tillader det; elektroniske signaturer, der anvendes i sådanne systemer, bør ikke nægtes retlig gyldighed og anerkendelse som bevis under retssager;

(17) det er ikke dette direktivs mål at harmonisere national aftaleret, herunder især regler om kontraktindgåelse og -opfyldelse eller andre ikke-aftaleretlige formkrav vedrørende underskrifter: derfor bør bestemmelserne om elektroniske signaturers retsvirkninger ikke bevare formkrav til indgåelse af kontrakter eller regler til bestemmelse af, hvor en kontrakt er indgået, som er fastsat i national ret;

(18) opbevaring og kopiering af signaturgenereringsdata vil kunne udgøre en alvorlig trussel mod elektroniske signaturers juridiske gyldighed;

(19) elektroniske signaturer vil blive anvendt i den offentlige sektor inden for nationale forvaltninger og fællesskabsforvaltninger samt i kommunikationen mellem disse og med borgere og erhvervslivet, for eksempel i forbindelse med offentlige indkøb, beskatning, social sikkerhed, sundheds- og retsvæsenet;

(20) harmoniserede kriterier vedrørende retsvirkningen af elektroniske signaturer vil gøre det muligt at bevare en sammenhængende retlig ramme i hele Fællesskabet; der er i de nationale lovgivninger fastlagt forskellige krav for at anse håndskrevne underskrifter for juridisk gyldige; certifikater kan anvendes til at certificere identiteten af en person, der underskriver elektronisk; avancerede elektroniske signaturer, som er baseret på kvalificerede certifikater, tilsigter at skabe et højt sikkerhedsniveau; avancerede elektroniske signaturer, som er baseret på kvalificerede certifikater, og som er genereret af et sikkert signaturgenereringssystem, kan kun betragtes som retligt ligestillede med håndskrevne underskrifter, hvis kravene til håndskrevne underskifter er opfyldt;

(21) for at bidrage til at gøre elektroniske certificeringsmetoder almindeligt accepteret bør det sikres, at elektroniske signaturer kan anvendes som bevis ved retshandlinger i alle medlemsstater; den retlige anerkendelse af elektroniske signaturer bør hvile på objektive kriterier og ikke afhænge af den berørte certificeringstjenesteudbyders eventuelle akkreditering; fastlæggelsen af de retsområder, hvor der kan anvendes elektroniske dokumenter og elektroniske signaturer, reguleres i national lovgivning; dette direktiv indskrænker ikke nationale domstoles kompetence til at træffe afgørelse om, hvorvidt kravene i dette direktiv er overholdt, og berører ikke nationale bestemmelser om domstolenes fri bevisbedømmelse;

(22) certificeringstjenesteudbydere, der udbyder certificeringstjenester til offentligheden, er underkastet nationale erstatningsansvarsregler;

(23) udviklingen i international elektronisk handel kræver grænseoverskridende ordninger, der involverer tredjelande; for at sikre global interoperabilitet kan det være hensigtsmæssigt at indgå aftaler med tredjelande om multilaterale regler for gensidig anerkendelse af certificeringstjenester;

(24) med henblik på at øge brugernes tillid til elektronisk kommunikation og elektronisk handel skal certificeringstjenesteudbyderne overholde lovgivningen om databeskyttelse og privatlivets fred;

(25) bestemmelserne om brug af pseudonymer i certifikater bør ikke være til hinder for, at medlemsstaterne kan håndhæve krav om identifikation af personer i henhold til Fællesskabets lovgivning eller national lovgivning;

(26) de nødvendige gennemførelsesforanstaltninger til dette direktiv vedtages i overensstemmelse med Rådets afgørelse 1999/468/EF af 28. juni 1999 om fastsættelse af de nærmere vilkår for udøvelsen af de gennemførelsesbeføjelser, der tillægges Kommissionen [1];

(27) Kommissionen bør foretage en vurdering af dette direktiv to år efter dets gennemførelse bl.a. med henblik på at sikre, at hverken den teknologiske udvikling eller juridiske ændringer bliver til hinder for opfyldelsen af målene i dette direktiv; Kommissionen bør undersøge virkningerne af beslægtede tekniske områder og forelægge Europa-Parlamentet og Rådet en rapport herom;

(28) målsætningen om at skabe en harmoniseret retlig ramme for udbud af elektroniske signaturer og beslægtede tjenester kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne og kan derfor i overensstemmelse med subsidiaritets- og proportionalitetsprincipperne som omhandlet i traktatens artikel 5 bedre gennemføres af Fællesskabet; dette direktiv går ikke ud over, hvad der er nødvendigt for at nå dette mål —

UDSTEDT FØLGENDE DIREKTIV:

Artikel 1

Anvendelsesområde

Formålet med dette direktiv er at lette brugen af elektroniske signaturer og bidrage til disses retlige anerkendelse. Det fastlægger en retlig ramme for elektroniske signaturer og visse certificeringstjenester, for at det indre marked kan fungere efter hensigten.

Det omfatter ikke aspekter i forbindelse med kontrakters indgåelse og gyldighed eller andre retlige forpligtelser, som ifølge national ret eller fællesskabsret er undergivet formkrav, og det berører heller ikke de regler og begrænsninger, der efter national ret eller fællesskabsret gælder for anvendelsen af dokumenter.

Artikel 2

Definitioner

I dette direktiv forstås ved:

1) »elektronisk signatur«: data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre elektroniske data, og som anvendes som en autentifikationsmetode

2) »avanceret elektronisk signatur«: en elektronisk signatur, som opfylder følgende krav:

   a) den er entydigt knyttet til underskriveren

   b) den kan identificere underskriveren

   c) den genereres med midler, som underskriveren kan bevare den fulde kontrol med, og

   d) den er knyttet til de data, som den vedrører, på en sådan måde, at en hvilken som helst senere ændring af disse data kan opdages

3) »underskriver«: en person, der besidder et signaturgenereringssystem og handler på egne vegne eller på vegne af den fysiske eller juridiske person eller det organ, som vedkommende repræsenterer

4) »signaturgenereringsdata«: unikke data, som f.eks. koder eller private krypteringsnøgler, som anvendes af underskriveren til generering af en elektronisk signatur

5) »signaturgenereringssystem«: konfigureret software eller hardware til behandling af signaturgenereringsdata

6) »sikkert signaturgenereringssystem«: et signaturgenereringssystem, der opfylder kravene i bilag III

7) »signaturverificeringsdata«: data, som f.eks. koder eller offentlige krypteringsnøgler, der anvendes til kontrol af den elektroniske signatur

8) »signaturverificeringssystem«: konfigureret software eller hardware til behandling af signaturverificeringsdata

9) »certifikat«: en elektronisk attestering, som knytter signaturverificeringsdata til en person og bekræfter denne persons identitet

10) »kvalificeret certifikat«: et certifikat, som opfylder kravene i bilag I og leveres af en certificeringstjenesteudbyder, som opfylder kravene i bilag II

11) »certificeringstjenesteudbyder«: et organ eller en fysisk eller juridisk person, der udsteder certifikater eller leverer andre tjenesteydelser i forbindelse med elektroniske signaturer

12) »elektronisk signatur-produkt«: hardware eller software eller relevante komponenter heraf, som er beregnet til at blive brugt af en certificeringstjenesteudbyder til levering af tjenesteydelser i forbindelse med elektronisk signatur eller beregnet til at blive brugt i forbindelse med generering eller verificering af elektroniske signaturer

13) »frivillig akkreditering«: enhver tilladelse, der fastsætter rettigheder og forpligtelser, der er særlige for certificeringstjenester, og som efter anmodning fra den pågældende certificeringstjenesteudbyder tildeles denne af det offentlige eller private organ, der har til opgave at udarbejde og føre tilsyn med overholdelsen af sådanne rettigheder og forpligtelser, og hvor certificeringstjenesteudbyderen ikke er berettiget til at udøve de rettigheder, som tilladelsen giver, før denne har modtaget organets afgørelse.

[1] EFT L 184 af 17.7.1999, s. 23.

Artikel 3

Markedsadgang

1. Medlemsstaterne må ikke gøre udbud af certificeringstjenesteydelser afhængigt af forudgående autorisation.

2. Med forbehold af stk. 1 kan medlemsstaterne indføre eller opretholde frivillige akkrediteringsordninger med henblik på at højne niveauet for ydelse af certificeringstjenester. Alle vilkår i forbindelse med sådanne ordninger skal være objektive, gennemsigtige, forholdsmæssige og ikke-diskriminerende. Medlemsstaterne kan ikke af årsager, der falder ind under dette direktivs anvendelsesområde, begrænse antallet af akkrediterede certificeringstjenesteudbydere.

3. Medlemsstaterne sikrer, at der indføres et passende system til kontrol af certificeringstjenesteudbydere, der er etableret på deres område, og som udbyder kvalificerede certifikater til offentligheden.

4. Egnede offentlige eller private organer, som udpeges af medlemsstaterne, afgør, om sikre signaturgenereringssystemer opfylder kravene i bilag III. Kommissionen fastlægger efter proceduren i artikel 9 kriterier, ud fra hvilke medlemsstaterne afgør, om et organ er egnet til at blive udpeget.

Medlemsstaterne anerkender de afgørelser, som de organer, der er nævnt i første afsnit, træffer for så vidt angår opfyldelsen af kravene i bilag III.

5. Kommissionen kan efter proceduren i artikel 9 fastsætte og i *De Europæiske Fællesskabers Tidende* offentliggøre referencenumre på almindeligt anerkendte standarder for elektroniske signatur-produkter. Medlemsstaterne formoder, at et elektronisk signatur-produkt overholder kravene i bilag II, litra f), og bilag III, hvis det overholder sådanne standarder.

6. Medlemsstaterne og Kommissionen samarbejder med henblik på at fremme udviklingen og brugen af signaturverificeringssystemer på baggrund af anbefalingerne vedrørende signaturverificering i bilag IV og under hensyn til forbrugernes interesser.

7. Medlemsstaterne kan gøre anvendelse af elektroniske signaturer i den offentlige sektor afhængig af opfyldelsen af eventuelle supplerende krav. Sådanne krav skal være objektive, gennemsigtige, forholdsmæssige og ikke-diskriminerende, og må kun være affødt af den pågældende anvendelses særlige karakter. Kravene må ikke hindre grænseoverskridende tjenesteydelser til borgerne.

Artikel 4

Principper vedrørende det indre marked

1. Medlemsstaterne anvender de nationale bestemmelser, som de vedtager i henhold til dette direktiv, på certificeringstjenesteudbydere, der er etableret på deres område, og på disses tjenesteydelser. Medlemsstaterne kan ikke på områder, der er omfattet af dette direktiv, pålægge ydelse af certificeringstjenester med oprindelse i en anden medlemsstat begrænsninger.

2. Medlemsstaterne sikrer fri bevægelighed inden for det indre marked for elektroniske signatur-produkter, der overholder bestemmelserne i dette direktiv.

Artikel 5

Retsvirkninger af elektroniske signaturer

1. Medlemsstaterne sikrer, at avancerede elektroniske signaturer, der er baseret på et kvalificeret certifikat, og som er genereret af et sikkert signaturgenereringssystem,

a) opfylder retskravene til en signatur i forbindelse med data i elektronisk form, på samme måde som en håndskreven underskrift opfylder disse krav i forbindelse med papirbaserede data, og

b) kan godtages som bevismateriale under retssager.

2. Medlemsstaterne sikrer, at en elektronisk signatur ikke nægtes retlig gyldighed og anerkendelse som bevis under retssager alene af den grund, at den

— er i elektronisk form, eller

— ikke er baseret på et kvalificeret certifikat, eller

— ikke er baseret på et kvalificeret certifikat udstedt af en akkrediteret certificeringstjenesteudbyder, eller

— ikke er genereret af et sikkert signaturgenereringssystem.

Artikel 6

Erstatningsansvar

1. Medlemsstaterne sikrer som et minimum, at en certificeringstjenesteudbyder, der udsteder et certifikat som kvalificeret certifikat til offentligheden, eller som garanterer et sådant certifikat over for offentligheden, ifalder erstatningsansvar for tab, der påføres ethvert organ eller enhver fysisk eller juridisk person, som med rimelighed forlader sig på certifikatet for så vidt angår:

a) korrektheden af alle oplysningerne i det kvalificerede certifikat på udstedelsestidspunktet og certifikatets indhold af alle de for et kvalificeret certifikat foreskrevne angivelser

b) sikkerhed for, at den i det kvalificerede certifikat identificerede underskriver på udstedelsestidspunktet var i besiddelse af de signaturgenereringsdata, der svarer til de i certifikatet indeholdte eller omhandlede signaturverificeringsdata

c) sikkerhed for, at signaturgenererings- og signaturverificeringsdataene kan anvendes komplementært med hinanden i de tilfælde, hvor det er certificeringstjenesteudbyderen, der genererer begge datasæt,

medmindre certificeringstjenesteudbyderen kan bevise, at han ikke har handlet uagtsomt.

2. Medlemsstaterne sikrer som et minimum, at en certificeringstjenesteudbyder, der har udstedt et certifikat som et kvalificeret certifikat til offentligheden, er erstatningsansvarlig for tab, der påføres ethvert organ eller enhver fysisk eller juridisk person, som med rimelighed forlader sig på certifikatet, for så vidt angår manglende registrering af tilbagekaldelse af certifikatet, medmindre certificeringstjenesteudbyderen kan bevise, at han ikke har handlet uagtsomt.

3. Medlemsstaterne sikrer, at en certificeringstjenesteudbyder i et kvalificeret certifikat kan anføre begrænsninger i dette certifikats anvendelsesområde, idet disse begrænsninger skal være tydelige for tredjeparter. Certificeringstjenesteudbyderen hæfter ikke for tab, der skyldes brug af et kvalificeret certifikat, som overskrider begrænsningerne i dets anvendelsesområde.

4. Medlemsstaterne sikrer, at certificeringstjenesteudbyderen i et kvalificeret certifikat kan sætte en beløbsgrænse for de transaktioner, som certifikatet kan anvendes til, og at denne beløbsgrænse er tydelig for tredjeparter.

Certificeringstjenesteudbyderen hæfter ikke for tab, der skyldes en overskridelse af denne beløbsgrænse.

5. Stk. 1-4 berører ikke Rådets direktiv 93/13/EØF af 5. april 1993 om urimelige kontraktvilkår i forbrugeraftaler ([1]).

Artikel 7

Internationale aspekter

1. Medlemsstaterne sikrer, at certifikater, der er udstedt som kvalificerede certifikater til offentligheden af en certificeringstjenesteudbyder, der er etableret i et tredjeland, anses for at være retligt ligestillede med certifikater, der er udstedt af en certificeringstjenesteudbyder, der er etableret inden for Fællesskabet:

a) hvis certificeringstjenesteudbyderen opfylder kravene i dette direktiv og er akkrediteret under en frivillig akkrediteringsordning i en medlemsstat, eller

b) hvis en certificeringstjenesteudbyder, der er etableret inden for Fællesskabet, og som opfylder kravene i dette direktiv, garanterer certifikatet, eller

c) hvis certifikatet eller certificeringstjenesteudbyderen er anerkendt i henhold til en bilateral eller multilateral aftale mellem Fællesskabet og tredjelande eller internationale organisationer.

2. For at lette grænseoverskridende certificeringstjenester med tredjelande og retlig anerkendelse af avancerede elektroniske signaturer med oprindelse i tredjelande fremsætter Kommissionen i givet fald forslag med henblik på den faktiske implementering af standarder og internationale aftaler om certificeringstjenester. Kommissionen forelægger, hvis det er nødvendigt, Rådet forslag til passende mandater til forhandling af bilaterale og multilaterale aftaler med tredjelande og internationale organisationer. Rådet træffer afgørelse med kvalificeret flertal.

3. Når Kommissionen underrettes om vanskeligheder, som EF-virksomheder støder på ved markedsføringen i tredjelande, kan den om nødvendigt forelægge forslag til Rådet til et passende mandat med henblik på forhandling af tilsvarende rettigheder for EF-virksomheder i disse tredjelande. Rådet træffer afgørelse med kvalificeret flertal.

Foranstaltninger, der træffes i henhold til dette stykke, berører ikke Fællesskabets og medlemsstaternes forpligtelser i henhold til relevante internationale aftaler.

Artikel 8

Databeskyttelse

1. Medlemsstaterne sikrer, at certificeringstjenesteudbyderne og de nationale akkrediterings- og tilsynsorganer opfylder kravene i Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ([2]).

2. Medlemsstaterne sikrer, at den certificeringstjenesteudbyder, der udsteder certifikatet til offentligheden, kun har tilladelse til at opnå persondata direkte fra den registrerede eller med den registreredes udtrykkelige tilladelse og kun i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat. Data må ikke indsamles eller behandles til noget andet formål uden den registreredes udtrykkelige samtykke.

3. Uden at den retsvirkning, der tillægges pseudonymer i henhold til den nationale lovgivning dermed foregribes, må medlemsstaterne ikke forhindre, at certificeringstjenesteudbyderen på certifikatet anfører et pseudonym i stedet for underskriverens navn.

Artikel 9

Udvalg

1. Kommissionen bistås af et elektronisk signatur-udvalg, i det følgende benævnt »udvalget«.

2. Når der henvises til dette stykke, anvendes artikel 4 og 7 i afgørelse 1999/468/EF under overholdelse af bestemmelserne i afgørelsens artikel 8.

Den frist, der er omhandlet i artikel 4, stk. 3, i afgørelse 1999/468/EF, fastsættes til tre måneder.

3. Udvalget vedtager selv sin forretningsorden.

Artikel 10

Udvalgets hverv

Udvalget skal efter proceduren i artikel 9, stk. 2, præcisere de krav, der er fastlagt i bilagene, de kriterier, som er omhandlet i artikel 3, stk. 4, samt de alment anerkendte standarder for elektroniske signatur-produkter, der er indført og offentliggjort i henhold til artikel 3, stk. 5.

([1]) EFT L 95 af 21.4.1993, s. 29.

([2]) EFT L 281 af 23.11.1995, s. 31.

Artikel 11

Meddelelse

1. Medlemsstaterne meddeler Kommissionen og de øvrige medlemsstater følgende:

a) oplysninger om frivillige nationale akkrediteringsordninger, herunder alle supplerende krav i henhold til artikel 3, stk. 7

b) navn og adresse på nationale akkrediterings- og tilsynsorganer og på de organer, som er omhandlet i artikel 3, stk. 4

c) navn og adresse på alle akkrediterede nationale certificeringstjenesteudbydere.

2. Medlemsstaterne meddeler alle oplysninger i henhold til stk. 1 samt ændringer heraf så hurtigt som muligt.

Artikel 12

Revision

1. Kommissionen foretager en vurdering af, hvordan dette direktiv fungerer, og aflægger rapport herom til Europa-Parlamentet og Rådet senest den 19. juli 2003.

2. I vurderingen tages der bl.a. stilling til, om direktivets anvendelsesområde bør ændres under hensyn til den teknologiske, markedsmæssige og retlige udvikling. Rapporten skal på grundlag af de indhøstede erfaringer navnlig omfatte en bedømmelse af harmoniseringsaspekterne. Rapporten ledsages om fornødent af forslag til retsforskrifter.

Artikel 13

Gennemførelse

1. Medlemsstaterne sætter de nødvendige love og administrative bestemmelser i kraft for at efterkomme dette direktiv inden den 19. juli 2001. De underretter straks Kommissionen herom.

Disse love og administrative bestemmelser skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for henvisningen fastlægges af medlemsstaterne.

2. Medlemsstaterne meddeler Kommissionen de væsentligste nationale retsforskrifter, som de udsteder på det område, der er omfattet af dette direktiv.

Artikel 14

Ikrafttræden

Dette direktiv træder i kraft på dagen for offentliggørelsen i *De Europæiske Fællesskabers Tidende*.

Artikel 15

Adressater

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den 13. december 1999.

På Europa-Parlamentets vegne	*På Rådets vegne*
N. FONTAINE	S. HASSI
Formand	*Formand*

BILAG I

Krav til kvalificerede certifikater

Kvalificerede certifikater skal indeholde:

a) angivelse af, at certifikatet er udstedt som et kvalificeret certifikat

b) den udstedende certificeringstjenesteudbyders identifikation og den stat som vedkommende er etableret i

c) underskriverens navn eller pseudonym; i sidstnævnte tilfælde skal det fremgå, at der er tale om et pseudonym

d) særlige oplysninger om underskriveren, der tilføjes, hvis det er relevant, afhængigt af formålet med certifikatet

e) de signaturverificeringsdata, som svarer til de signaturgenereringsdata, som er under underskriverens kontrol

f) certifikatets ikrafttrædelses- og udløbsdato

g) certifikatets identifikationskode

h) den udstedende certificeringstjenesteudbyders avancerede elektroniske signatur

i) eventuelle begrænsninger i certifikatets anvendelsesområde, og

j) eventuelle beløbsmæssige begrænsninger med hensyn til de transaktioner, for hvilke certifikatet kan anvendes.

BILAG II

Krav til certificeringstjenesteudbydere, der udsteder kvalificerede certifikater

Certificeringstjenesteudbydere

a) skal udvise den fornødne pålidelighed til at kunne udbyde certificeringstjenester

b) skal sørge for en hurtig og sikker katalog- og tilbagekaldelsestjeneste

c) skal sikre, at det er muligt at fastslå datoen og tidspunktet for udstedelsen eller tilbagekaldelsen af et certifikat

d) skal med hensigtsmæssige midler og i overensstemmelse med national ret kontrollere identiteten og eventuelt særlige forhold i forbindelse med de personer, til hvem der udstedes kvalificerede certifikater

e) skal beskæftige personale med den ekspertviden og de erfaringer og kvalifikationer, som de tilbudte tjenesteydelser kræver, navnlig ledelseskompetence, sagkundskab inden for elektronisk signaturteknologi og indgående kendskab til korrekte sikkerhedsprocedurer; de skal også anvende adækvate administrative og ledelsesmæssige procedurer, som overholder anerkendte standarder

f) skal anvende pålidelige systemer og produkter, som er beskyttet mod ændringer, og som garanterer de af disse systemer og produkter understøttede processers tekniske og kryptografiske sikkerhed

g) skal træffe foranstaltninger imod forfalskning af certifikater, og, hvis certificeringstjenesteyderen genererer signaturgenereringsdata, garantere disse datas fortrolighed under genereringsprocessen

h) skal til stadighed have tilstrækkelige økonomiske ressourcer til at drive virksomheden i overensstemmelse med dette direktivs krav, navnlig til at bære erstatningsansvaret, f.eks. ved at tegne en passende forsikring

i) skal registrere alle relevante oplysninger om kvalificerede certifikater i en rimelig periode, navnlig for at kunne fremlægge bevis for certificering, når det er påkrævet i retssager. Denne registrering kan ske elektronisk

j) må ikke opbevare eller kopiere de personers signaturgenereringsdata, som certificeringstjenesteyderen har tilbudt nøglehåndteringstjenester

k) skal, inden de indgår i et kontraktforhold med en person, der søger at opnå et certifikat fra dem til støtte for sin elektroniske signatur, gennem et bestandigt kommunikationsmedium underrette denne person om de nøjagtige vilkår for anvendelsen af certifikatet, herunder eventuelle begrænsninger i brugen heraf, eksistensen af en eventuel frivillig akkrediteringsordning og procedurer for klager og bilæggelse af tvister. Sådanne oplysninger, som kan sendes elektronisk, skal gives skriftligt og i et umiddelbart forståeligt sprog. De relevante dele af disse oplysninger skal efter anmodning også stilles til rådighed for tredjemand, der forlader sig på certifikatet

l) skal benytte pålidelige systemer til opbevaring af certifikater i verificerbar form, således at

— kun bemyndigede personer kan foretage tilføjelser og ændringer

— oplysningernes ægthed kan kontrolleres

— certifikaterne kun er offentligt tilgængelige i de tilfælde, hvor indehaveren har givet sit samtykke, og

— eventuelle tekniske ændringer, som bringer disse sikkerhedskrav i fare, er synlige for operatøren.

BILAG III

Krav til sikre elektroniske signaturgenereringssystemer

1. Sikre signaturgenereringssystemer skal ved hjælp af passende og tekniske og proceduremæssige midler i det mindste sikre, at:

   a) signaturgenereringsdata, der anvendes til signaturgenerering, i praksis kun kan fremtræde én gang, og at de med rimelig sikkerhed forbliver hemmelige

   b) signaturgenereringsdata, der anvendes til signaturgenerering, med rimelig sikkerhed ikke kan udledes, og at signaturen er beskyttet mod forfalskning under anvendelse af eksisterende teknologi

   c) signaturgenereringsdata, der anvendes til signaturgenerering, på pålidelig vis kan beskyttes af den retmæssige underskriver mod andres brug.

2. Sikre signaturgenereringssystemer må ikke ændre de data, som skal underskrives, eller hindre, at disse data vises for underskriveren forud for signaturprocessen.

BILAG IV

Anbefalinger vedrørende signaturverificering

I løbet af signaturverificeringsprocessen bør der skabes rimelig sikkerhed for, at:

a) de data, der anvendes til verificering af signaturen, svarer til de data, som vises kontrolløren

b) signaturen verificeres på pålidelig vis, og at resultatet af denne verificering vises korrekt

c) kontrolløren om nødvendigt på pålidelig vis kan fastslå indholdet af de underskrevne data

d) certifikatets ægthed og gyldighed, som kræves på tidspunktet for signaturverificeringen, verificeres på pålidelig vis

e) resultatet af verificeringen og underskriverens identitet vises på korrekt vis

f) anvendelsen af pseudonym klart fremgår

g) eventuelle sikkerhedsrelevante ændringer kan spores.