KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 13.05.1998
KOM(1998) 297 endelig udg.

98/0191 (COD)

Forslag til
EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV
om en fælles ramme for elektroniske signaturer

(forelagt af Kommissionen)

BEGRUNDELSE

I. BAGGRUND

Åbne net som f.eks. Internet har voksende betydning for kommunikationen i hele verden. De giver mulighed for interaktiv kommunikation mellem parter, der ikke på forhånd har kendskab til hinanden. De giver nye forretningsmuligheder, idet de giver midler i hænde til styrkelse af produktiviteten og nesættelse af omkostningerne samt nye metoder til at skabe kontakt med kunderne. Nettene bliver brugt af virksomheder, som ønsker at udnytte nye forretningsmetoder og nye måder at arbejde på, som f.eks. fjernarbejde og fælles virtuelle omgivelser. Ministerier anvender også disse net i deres interaktion med virksomheder og borgere. Elektronisk handel giver Den Europæiske Union en glimrende mulighed for at bringe den økonomiske integration et skridt videre. For at få det bedste ud af disse muligheder må det imidlertid ske i sikre rammer.

For at kunne udnytte disse muligheder bedst muligt er der behov for et sikkert miljø for så vidt angår elektronisk autentifikation. Der findes flere forskellige metoder til at underskrive dokumenter elektronisk lige fra meget simple metoder (f.eks. indsættelse af et scannet billede af en håndskreven underskrift i et tekstbehandlingsdokument) til meget avancerede metoder (f.eks. elektroniske signaturer ved hjælp af "offentlig nøgle-kryptering"). Med elektroniske signaturer kan modtageren af elektronisk fremsendte data kontrollere disses oprindelse (*autentifikation af datakilden*) og undersøge, om data er fuldstændige og uændrede, og dermed værne deres integritet (*dataintegritet*).

Verifikation af datas autenticitet og integritet beviser ikke nødvendigvis identiteten på den underskriver, der har genereret de elektroniske signaturer. Hvordan kan modtageren af en meddelelse f.eks vide, at afsenderen rent faktisk er den, han udgiver sig for? Modtageren ønsker måske derfor at få mere pålidelige oplysninger om underskriverens identitet. Sådanne oplysninger kan gives af underskriveren selv ved at give modtageren tilfredsstillende bevis. En anden måde er at få identiteten bekræftet af tredjemand (dvs. en person eller institution, som begge parter har tillid til). I dette direktiv kaldes sådanne tredjeparter *certificeringstjenesteudbydere.*

I meddelelsen med titlen, Et europæisk initiativ inden for elektronisk handel[1], af 16. april 1997 til Europa-Parlamentet, Rådet, Det Økonomiske og Sociale Udvalg og Regionsudvalget anerkendte Kommissionen, at elektroniske signaturer er et væsentligt værktøj til at yde sikkerhed og udvikle tillid på åbne net. I erklæringen fra minister-konferencen i Bonn[2] peges der også på, at behovet for elektroniske signaturer er af afgørende betydning for elektronisk handel.

Som et første skridt forelagde Kommissionen en meddelelse med titlen, Sikkerhed og tillid i elektronisk kommunikation - Imod europæiske rammer for elektroniske signaturer og kryptering[3], for Europa-Parlamentet, Rådet, Det Økonomiske og Sociale Udvalg og Regionsudvalget, hvori behovet for en sammenhængende strategi på dette område

---

1 KOM(97) 157 endelig udg. af 16.4.97.

2 Europæisk ministerkonference: "Udnyttelse af mulighederne i forbindelse med globale informationsnet", Bonn den 6.-8. juli 1997.

3 KOM(97) 503 endelig udg. af 8.10.97.

skitseres. Den 1. december 1997 glædede Rådet sig over meddelelsen og opfordrede Kommissionen til at forelægge et forslag til Europa-Parlamentet og Rådets direktiv om elektroniske signaturer så hurtigt som muligt.

Efter offentliggørelsen af meddelelsen og som følge af møder med medlemsstater og repræsentanter for den private sektor, navnlig den europæiske krypteringsindustri, samt den internationale eksperthøring i København[4] har Kommissionen fået input fra de forskellige involverede parter. Der kan drages følgende konklusioner fra de indsamlede oplysninger:

1. Den voksende lovgivningsaktivitet på dette område i flere medlemsstater understreger det presserende behov for en harmoniseret retlig ramme på europæisk niveau, således at det undgås, at der opstår alvorlige hindringer for det indre marked.

2. Selv om der er en livlig debat om og arbejdes en hel del med elektronisk signaturteknologi, som anvender offentlig nøgle-kryptering, bør et direktiv på europæisk niveau være teknologineutralt og ikke blot fokusere på den slags signaturer. Da det kan forventes, at der bliver udviklet en række forskellige autentifikationssystemer, bør dette direktiv være bredt nok til at dække et bredt spektrum af elektroniske signaturer omfattende såvel sådanne, som er baseret på offentlig nøgle-kryptering, som andre midler til autentifikation af data.

3. For at sikre, at det indre marked kan fungere uhindret samt for at støtte en hurtig udvikling af markedet for så vidt angår brugerefterspørgsel og teknologisk innovation må forudgående autorisation undgås. Frivillige akkrediteringsordninger for certificeringstjenesteudbydere, der har til formål at skabe højere sikkerhedsniveauer, må anses for et nyttigt middel til at vinde forbrugernes tillid. For så vidt sådanne foranstaltninger kræves af markedet, kunne de yde certificeringstjenesteudbyderen og forbrugeren et klarere og mere forudsigeligt retligt sikkerhedsniveau.

4. Elektroniske signaturer, der anvendes inden for lukkede grupper, f.eks. hvor aftalemæssige forhold allerede eksisterer bør ikke automatisk være omfattet af dette direktiv. Aftalefriheden bør i denne forbindelse have forrang.

5. Sikring af retlig anerkendelse - navnlig på tværs af grænserne - af elektroniske signaturer og certificeringstjenester anses for at være det vigtigste spørgsmål på dette område. Dette indebærer klarlæggelse af væsentlige krav til certificeringstjenesteudbydere, herunder disses erstatningsansvar.

6. Det er erhvervslivets rolle sammen med standardiseringsorganer at tage initiativ til at udvikle internationalt anerkendte standarder for elektroniske signaturer. Disse standarder bør sigte mod at etablere et åbent miljø med interoperabilitet mellem produkter og tjenester. Kommissionens opgave er at støtte denne proces.

---

4 Den internationale høring i København den 23.-24.4.1998.

7. På internationalt niveau er mange aktiviteter og diskussioner i gang. De Forenede Nationers Kommission for international Handelsret (UNCITRAL) har vedtaget en modellov om elektronisk handel og igangsat yderligere arbejde med henblik på at forberede ensartede regler for elektroniske signaturer. Organisationen for Økonomisk Samarbejde og Udvikling (OECD) har også igangsat arbejde på dette område som opfølgning af dens retningslinjer for krypteringspolitik fra 1997. Andre internationale organisationer, herunder Verdenshandelsorganisationen (WTO), er også involveret i beslægtede spørgsmål. Der bør tages hensyn til denne løbende udvikling ved implementeringen af en retlig ramme på europæisk niveau.

II. HARMONISERINGSBEHOVET

Flere medlemsstater har allerede taget detaljerede lovgivningsinitiativer i forbindelse med elektroniske signaturer:

Medlemsstat	Lovgivningsinitiativernes udviklingstrin
Østrig	Forberedende arbejde
Belgien	• Telekommunikationslov: frivillig forudgående erklæringsordning for tjenesteudbydere; • Udkast til lov om certificeringstjenster i forbindelse med elektroniske signaturer; • Udkast til lov om ændringer inden for civilretten i forbindelse med elektroniske beviser; • Udkast til lov om anvendelse af elektroniske signaturer inden for social- og sundhedsvæsenet.
Danmark	Udkast til lov om sikker og effektiv anvendelse af elektronisk kommunikation.
Frankrig	• Telekommunikationslov (Autorisations- og undtagelsesdekreter): ⇒ udbud af elektroniske signatur-produkter og -tjenester, der er omfattet af krav om informationsprocedure; ⇒ fri anvendelse, import og eksport af elektroniske signatur-produkter og -tjenester. • Lovgivning om anvendelse af elektronisk signatur inden for social- og sundhedsvæsenet.
Finland	• Udkast til lov om elektroniske informationsudveksling i forvaltningen og forvaltningsretlige procedurer; • Udkast til lov om Det Centrale Folkeregisters stilling som certificeringstjenesteudbyder.
Tyskland	• Lov om elektronisk signatur og bekendtgørelse på plads: betingelser for, hvornår elektroniske signaturer anses for sikre; frivillig akkreditering af tjenesteudbydere; • Udkast til katalog over passende sikkerhedsforanstaltninger; • Offentlig høring om retlige aspekter ved elektroniske signaturer og elektronisk signerede elektroniske dokumenter i gang for tiden.

Italien	• Generel lov om reform af den offentlige forvaltning og administrativ forenkling: princip om retlig anerkendelse af elektroniske dokumenter; • Dekret om skabelse, arkivering og overførsel af elektroniske dokumenter og kontrakter; • Dekret om krav til produkter og tjenesteydelser under forberedelse; • Dekret om fiskale forpligtelser, der hidrører fra elektroniske dokumenter.
Nederlandene	• Frivillig akkrediteringsordning for tjenesteudbydere under forberedelse; • Skattelov, der åbner mulighed for elektronisk indsendelse af selvangivelse; • Udkast til lov om ændringer inden for civilretten.
Spanien	• Cirkulærer fra Toldstyrelsen om brug af elektroniske signaturer; • Beslutning på den sociale sikrings område om brugen af elektroniske midler; • Love og cirkulærer inden for pant, beskatning, finansielle tjenesteydelser og registrering af virksomheder, der tillader brugen af elektroniske procedurer; • Budgetlov 1998, der bemyndiger Mønten til at optræde som certificeringsudbyder.
Sverige	Forberedende arbejde
Det Forenede Kongerige	Udkast til lovgivning om frivillig autorisation af certificeringstjenesteudbydere og retlig anerkendelse af elektroniske signaturer.

Denne oversigt viser, at de forskellige initiativer i medlemsstaterne fører til afvigende retlige forhold. Selv om medlemsstaterne synes at rette opmærksomheden mod de samme spørgsmål, navnlig kravene til tjenesteudbydere og produkter, betingelserne for, at der kan støttes ret på elektroniske signaturer samt akkrediteringsordningers struktur, er det indlysende, at de relevante reguleringer, eller manglen på samme, vil afvige fra hinanden i en sådan grad, at der er fare for, at det indre marked, for så vidt angår elektronisk signatur, ikke vil fungere, som det skal. Afvigende regler for, hvilke retsvirkninger der tillægges en elektronisk signatur, er til overordentlig stor skade for den videre udvikling af elektronisk handel, og dermed for den økonomisk vækst og beskæftigelsen i Fællesskabet. Forskellige regler for erstatningsansvar og risiko for usikkerhed om værneting i sager om hæftelse, når tjenesterne ydes mellem forskellige medlemsstater, giver yderligere usikkerhed. Det ser også ud til, at medlemsstaterne vil opstille forskellige betingelser for, hvornår elektroniske signaturer vil blive anset for sikre.

Disse afvigende forhold kunne skabe en alvorlig hindring for kommunikation og forretninger via åbne net i hele Det Europæiske Fællesskab ved at hæmme fri brug og frit udbud af tjenester i forbindelse med elektronisk signatur samt ved at begrænse udviklingen af nye økonomiske aktiviteter i forbindelse med elektronisk handel. Målet med vedlagte forslag til direktiv er at fjerne hindringer, navnlig forskelle vedrørende den retlige anerkendelse af elektroniske signaturer og begrænsninger i den frie udveksling af certificeringstjenester og -produkter mellem medlemsstaterne. Under hensyn til de mål, der forfølges, falder den planlagte foranstaltning ind under Fællesskabets enekompetence.

Direktivforslaget tilsigter at gøre brugen af elektroniske signaturer mulig inden for et område uden indre grænser ved at fokusere på væsentlige krav til certificeringstjenester og overlader de detaljerede gennemførelsesbestemmelser til medlemsstaterne. Dette er i overensstemmelse med Kommissionens lovgivningspraksis for så vidt angår subsidiaritet, proportionalitet og forenkling af love og administrative bestemmelser.

Derfor foreslår Kommissionen artikel 57, stk. 2, artikel 66 og artikel 100 A som hjemmel for dette forslag. Af proportionalitetsårsager finder Kommissionen, at et direktiv vil være det korrekte retlige instrument.

III. DIREKTIVETS MÅL OG ANVENDELSESOMRÅDE

1. Dette direktivs mål er at sikre, at det indre marked for så vidt angår elektroniske signaturer kan fungere korrekt, idet der skabes en harmoniseret og hensigtsmæssig retlig ramme for brugen af elektroniske signaturer i Det Europæiske Fællesskab og opstilles en række kriterier som grundlag for retlig anerkendelse af elektroniske signaturer.

2. Global elektronisk kommunikation og handel er afhængige af løbende tilpasning af nationale og internationale love til en teknologisk infrastruktur i hastig udvikling. Skønt analogier til eksisterende regler i mange situationer kunne give tilfredsstillende resultater, kan tilpasninger af disse eksisterende love i lyset af ny teknologi være påkrævet for at undgå uhensigtsmæssige og uønskede virkninger. Skønt elektroniske signaturer, der genereres under anvendelse af krypteringsteknikker, på nuværende tidspunkt anses for at være en vigtig type elektronisk signatur, må en europæisk regulatorisk ramme være fleksibel nok til at omfatte andre teknikker, som måtte blive anvendt til autentifikation.

3. Der er åbenbare anvendelser for elektronisk signatur-teknologi i lukkede miljøer, f.eks. en virksomheds lokalnet eller et banksystem. Certifikater og elektroniske signaturer anvendes også til bemyndigelsesformål, f.eks. adgang til private konti. Inden for den nationale lovs begrænsninger giver princippet om aftalefrihed kontraherende parter mulighed for indbyrdes at aftale deres forretningsvilkår, f.eks. accept af elektronisk signatur. På disse områder er der ikke noget indlysende behov for regulering.

4. I betragtning af antallet af forskellige tjenesteydelser og anvendelsesmuligheder bør certificeringstjensteudbydere kunne udbyde deres tjenester uden krav om forudgående autorisation. Det kunne imidlertid tænkes, at tjenesteudbydere gerne ville nyde godt af de dertil knyttede elektroniske signaturers retsgyldighed gennem en frivillig autorisationsordning i forbindelse med fælles krav. Akkreditering skal ses som en offentlig tjenesteydelse til certificeringstjenesteudbydere, som ønsker at udbyde avancerede tjenesteydelser. Dette indebærer på ingen måde, at ikke-akkrediterede tjenester automatisk er mindre sikre.

5. En certificeringstjenesteudbyder kan tilbyde en bred vifte af tjenesteydelser. Dette direktiv fokuserer navnlig på certificeringstjenester i forbindelse med elektroniske signaturer. Certifikater kan have en lang række funktioner og indeholde forskellige informationer. Det kan f.eks. være almindelige identifikatorer som

navn, adresse, registreringsnummer eller personnummer, moms- eller skatteregistreringsnummer, eller særlige forhold i forbindelse med underskriveren, f.eks. dennes prokura, kreditværdighed, eventuelle betalingsgarantier eller besiddelse af bestemte tilladelser og bemyndigelser. Derfor kan der forudses en række forskellige certifikater til en vifte af anvendelser. Der er imidlertid i første række behov for en retlig ramme for certifikater, for at en underskrivers elektroniske signatur skal kunne autenticificeres. Dette direktiv fokuserer derfor på et certifikats (benævnt autoriseret certifikat) funktion som forbindelse til en persons civile identitet eller rolle.

6. Elektroniske signaturers retsvirkninger er en nøglefaktor i et åbent men tillidsvækkende system for elektroniske signaturer. Anvendelsen af dette direktiv skal også bidrage til en harmoniseret retlig ramme i Fællesskabet ved at sikre, at en elektronisk signatur ikke nægtes retsgyldighed, -virkninger eller eksekutionskraft udelukkende med den begrundelse, at den foreligger i form af elektroniske data, ikke er baseret på et autoriseret certifikat eller på et certifikat udstedt af en akkrediteret tjenesteudbyder, samt at elektroniske signaturer anerkendes retligt på linje med håndskrevne underskrifter. Endvidere bør de nationale bevisregler åbnes for anerkendelse af brugen af elektroniske signaturer.

7. Retlig anerkendelse af elektroniske signaturer bør baseres på objektive, gennemsigtige, ikke-diskriminerende og rimelige kriterier og ikke på nogen måde være knyttet til den pågældende tjenesteudbyders eventuelle akkreditering. Fælles krav til certificeringstjenesteudbydere ville være et godt bidrag til anerkendelse på tværs af grænserne af signaturer og certifikater i Det Europæiske Fællesskab. Listen over krav skal finde anvendelse på certificeringstjenesteudbydere uafhængigt af den enkelte medlemsstats akkrediteringsmodel. Da den fremtidige teknologi- og markedsudvikling kan kræve tilpasninger, kan der være behov for at revidere kravene fra tid til anden. Kommissionen kan derfor tænkes at foreslå ændrede krav i fremtiden på grundlag af modtagne råd.

8. Fælles regler for erstatningsansvar ville bidrage til skabelsen af tillid både hos forbrugere, virksomheder, der forlader sig på certifikaterne, og hos tjenesteudbyderne, og ville dermed fremme en bred accept af elektroniske signaturer.

9. Samarbejdsordninger med tredjelande til støtte for anerkendelse af signaturer og certifikater på tværs af grænserne er vigtige for udviklingen af den internationale elektroniske handel. Navnlig hvis tjenesteudbydere i Det Europæiske Fællesskab blev sat i stand til at stå inde for tredjelandscertifikater i samme udstrækning som for deres egne, kunne det lette udvekslingen af tjenesteydelser på tværs af grænserne på en enkel men effektiv måde.

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV

om en fælles ramme for
elektroniske signaturer

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR -

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 57, stk.2, artikel 66 og artikel 100 A,

under henvisning til forslag fra Kommissionen[5],

under henvisning til udtalelse fra Det Økonomiske og Sociale Udvalg[6],

under henvisning til udtalelse fra Regionsudvalget[7],

i henhold til fremgangsmåden i traktatens artikel 189 B[8], 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[9];

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 elektroniske signaturer og kryptering[10];

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

4. elektronisk kommunikation og handel kræver elektroniske signaturer og dertil knyttede tjenesteydelser til autentifikation af data; afvigende regler for retlig anerkendelse af elektroniske signaturer og akkreditering af certificeringstjeneste-udbydere i medlemsstaterne kan skabe betydelige hindringer for elektronisk

---

5 EFT C

6 EFT C

7 EFT C

8 EFT C

9 KOM(97) 157 endelig udg.

10 KOM(97) 503 endelig udg.

kommunikation og handel og dermed hæmme det indre markeds udvikling; initiativer i medlemsstaterne, der peger i forskellig retning, viser, at der er behov for harmonisering på fællesskabsniveau;

5. elektronisk signatur-produkters interoperabilitet skal fremmes; ifølge traktatens artikel 7 A indebærer det indre marked et område med fri bevægelighed for varer; væsentlige krav, der er specifikke for elektronisk signatur-produkter, der anvendes af certificeringstjenesteudbydere, skal opfyldes for at sikre fri bevægelighed inden for det indre marked og opbygge tilliden til elektroniske signaturer;

6. den hastige teknologiske udvikling og Internettets globale karakter kræver, at den valgte metode er åben for forskellige teknologier og tjenester til elektronisk autentifikation af data; digitale signaturer baseret på offentlig nøgle-kryptering er på nuværende tidspunkt den mest anerkendte form for elektronisk signatur;

7. det indre marked giver certificeringstjenesteudbydere mulighed for med henblik på øget konkurrenceevne at udvikle deres aktiviteter hen over grænserne og dermed tilbyde forbrugere og erhvervsliv nye muligheder for sikker elektronisk informationsudveksling og handel uden hensyn til grænser; certificerings-tjenesteudbydere bør for at stimulere udbuddet af certificeringstjenesteydelser via åbne net i hele Fællesskabet i almindelighed frit kunne tilbyde deres tjenesteydelser uden forudgående autorisation; der er ikke noget umiddelbart behov for at sikre fri udveksling af certificeringstjenester ved at harmonisere berettigede og rimelige nationale begrænsninger i det frie udbud af sådanne tjenester;

8. 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 kunne anspore udviklingen af bedste praksis blandt certificeringstjeneste-udbydere; det bør stå certificeringstjenesteudbydere frit, om de ønsker at tilslutte sig og nyde godt af sådanne ordninger; medlemsstaterne bør ikke forhindre certificeringstjenesteudbydere i at holde sig uden for sådanne akkrediterings-ordninger; det bør sikres, at akkrediteringsordninger ikke svækker konkurrencen blandt certificeringstjenester; det er vigtigt at finde den rigtige balance mellem forbrugernes og erhvervslivets behov;

9. dette direktiv bør bidrage til anvendelse og retlig anerkendelse af elektroniske signaturer i Fællesskabet; der er ikke behov for en regulatorisk ramme for elektroniske signaturer, der udelukkende anvendes inden for lukkede systemer; parternes frihed til selv indbyrdes at aftale, på hvilke betingelser, de vil acceptere elektronisk signerede data, bør respekteres i det omfang national ret tillader det; dette direktiv har ikke til formål at harmonisere national aftaleret, som vedrørende f.eks. kontraktindgåelse og -opfyldelse, eller andre ikke-kontraktlige formaliteter, hvor underskrift er påkrævet; bestemmelserne om elektroniske signaturers retsvirkninger bør ikke berøre nationale retlige formkrav med hensyn til indgåelse af kontrakter eller regler til bestemmelse af, hvor en kontrakt er indgået;

10. for at bidrage til generel accept af elektroniske signaturer, bør en elektronisk signatur ikke nægtes gyldighed alene med den begrundelse, at underskriften har form af elektroniske data, ikke er baseret på et autoriseret certifikat eller på et certifikat, der er udstedt af en akkrediteret certificeringstjenesteudbyder, eller at tjenesteudbyderen, der har udstedt det pågældende certifikat, er fra en anden medlemsstat; elektroniske signaturer, der støttes på en pålidelig certificeringstjenesteudbyder, som overholder de væsentlige krav, bør have samme retsvirkninger som håndskrevne underskrifter; det må sikres, at elektroniske signaturer kan anvendes som bevis ved retshandlinger i alle medlemsstater; det retlige anerkendelse af elektroniske signaturer bør hvile på objektive kriterier og ikke være knyttet til den berørte tjenesteudbyders eventuelle autorisation; harmoniserede regler for elektroniske signaturers retsvirkninger vil bevare en sammenhængende retlig ramme i hele Fællesskabet;

11. certificeringstjenesteudbydere, der udbyder certificeringstjenester til offentligheden, er underkastet nationale erstatningsansvarsregler; forskelle i sådanne erstatningsansvarsreglers rækkevidde og indhold kan forårsage retlig usikkerhed, navnlig for tredjemand, som forlader sig på deres tjenester; sådan usikkerhed vil skade udviklingen af handel på tværs af grænserne og være en hæmsko for, at det indre marked kan fungere, som det skal; harmoniserede erstatningsansvarsregler giver både certificeringstjenesteudbydere og forbrugere retssikkerhed og forudsigelighed; sådanne regler ville bidrage til generel accept og anerkendelse af elektroniske signaturer i Fællesskabet og dermed have en gunstig virkning på det indre marked;

12. udviklingen international elektronisk handel kræver grænseoverskridende systemer, der involverer tredjelande; sådanne systemer bør udvikles i erhvervslivet; aftaler med tredjelande om multilaterale regler for anerkendelse af certificeringstjenester kunne være gavnlige med henblik på sikring af interoperabilitet på globalt niveau;

13. med henblik på at stimulere elektronisk kommunikation og elektronisk handel gennem sikring af brugernes tillid skal medlemsstaterne forpligte certificeringstjenesteudbyderne til at overholde retsregler om databeskyttelse og privatlivets fred; det bør pålægges certificeringstjenesteudbyderne på underskrivers anmodning også at yde certificeringstjenester for pseudonymer; det bør i national ret fastsættes, om, og under hvilke omstændigheder data vedrørende en registrerets identitet skal overføres med henblik på kriminalefterforskning; certificeringstjenesteudbydere bør på forhånd skriftligt og i et umiddelbart forståeligt sprog samt under anvendelse af et bestandigt kommunikationsmedium underrette deres brugere om deres forretningsbetingelser, navnlig om den præcise brug af deres certifikater og begrænsninger i deres erstatningsansvar;

14. med henblik på anvendelsen af dette direktiv bør Kommissionen bistås af et rådgivende udvalg;

15. målet 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 subsidiaritetsprincippet, jf. traktatens

artikel 3 B, bedre gennemføres på fællesskabsplan; dette direktiv er i overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, begrænset til de minimumsforskrifter, der er nødvendige for at nå dette mål -

UDSTEDT FØLGENDE DIREKTIV:

Artikel 1
Anvendelsesområde

Dette direktiv vedrører den retlige anvendelse af elektroniske signaturer.

Det vedrører ikke andre aspekter i forbindelse med kontrakters indgåelse og gyldighed eller andre ikke-kontraktige formaliteter, hvor underskrift er påkrævet.

Det etablerer en retlige ramme for visse certificeringstjenester, som offentligheden kan anvende.

Artikel 2
Definitioner

I dette direktiv forstås ved:

1) "elektronisk signatur" en underskrift i digital form i, vedføjet eller logisk tilknyttet data og brugt af en underskriver til at angive underskriverens vedkendelse af indholdet i disse data, og som opfylder følgende krav:

   (a) den er entydig knyttet til underskriveren

   (b) den kan identificere underskriveren

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

   (d) den er knyttet til de data, den vedrører, på en sådan måde, at enhver efterfølgende ændring af disse data afsløres.

2) "underskriver" en person, der afgiver en elektronisk signatur.

3) "signaturgenereringssystem" unikke data, som f.eks.. koder eller private krypteringsnøgler eller et unikt konfigureret fysisk system, som anvendes af underskriveren til generering af en elektronisk signatur.

4) "signaturkontrolsystem" unikke data, som f.eks. koder eller offentlige krypteringsnøgler eller et unikt konfigureret fysisk system, som anvendes til kontrol af den elektroniske signatur.

5) "autoriseret certifikat" en digital attestering, som knytter et signaturkontrolsystem til en person, bekræfter denne persons identitet og opfylder kravene i bilag I.

6) "certificeringstjenesteudbyder" person eller organ, der udsteder certifikater eller leverer andre tjenesteydelser i forbindelse med elektronisk signatur til offentligheden.

7) "elektronisk signatur-produkt" hardware eller software eller relevante komponenter heri, som er beregnet til at blive brugt af en certificeringstjenesteudbyder til tjenesteydelser i forbindelse med elektronisk underskrift.

Artikel 3
Markedsadgang

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

2. Uanset bestemmelserne i stk. 1 kan medlemsstaterne indføre eller opretholde frivillige akkrediteringsordninger med henblik på ydelse af certificeringstjenester på avanceret niveau. Alle vilkår i forbindelse med sådanne ordninger skal være objektive, gennemsigtige, rimelige og ikke-diskriminerende. Medlemsstaterne kan ikke af årsager, der falder ind under dette direktivs anvendelsesområde begrænse antallet af certificeringstjenesteudbydere.

3. Kommissionen kan efter proceduren i artikel 9 fastsætte og i De Europæiske Fællesskabers Tidende offentliggøre referencenumre på almindeligt anerkendte standarder for elektronisk signatur-produkter. Medlemsstaterne anser et elektronisk signatur-produkt for at overholde kravene i bilag II, litra e), hvis det overholder sådanne standarder.

4. Medlemsstaterne kan gøre anvendelse af elektroniske signaturer i den offentlige sektor afhængig af opfyldelsen af supplerende krav. Sådanne krav skal være objektive, gennemsigtige, rimelige og ikke-diskriminerende, og må kun være affødt af den pågældende anvendelses særlige karakter.

Artikel 4
Principper vedrørende det indre marked

1. Alle medlemsstater anvender de nationale bestemmelser, 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 elektronisk signatur-produkter, der overholder bestemmelserne i dette direktiv.

Artikel 5
Retsvirkninger

1. Medlemsstaterne sikrer, at en elektronisk signatur ikke nægtes retsvirkning, gyldighed og eksekutionskraft alene med den begrundelse, at underskriften er i

elektronisk form, ikke er baseret på et autoriseret certifikat eller ikke er baseret på et certifikat, der er udstedt af en akkrediteret certificeringstjenesteudbyder.

2. Medlemsstaterne sikrer, at elektroniske signaturer, der er baseret på et autoriseret certifikat, der er udstedt af en certificeringstjenesteudbyder, der opfylder kravene i bilag II, dels anerkendes som opfyldende de retlige krav vedrørende en håndskreven underskrift, dels kan godtages som bevis ved retshandlinger på samme måde som håndskrevne underskrifter.

Artikel 6

Erstatningsansvar

1. Medlemsstaterne sikrer, at en certificeringstjenesteudbyder ved at udstede et autoriseret certifikat ifalder erstatningsansvar over for enhver person, som med rimelighed forlader sig på certifikatet for så vidt angår:

(a) korrektheden af alle oplysningerne i det autoriserede certifikat regnet fra udstedelsesdagen, medmindre certificeringstjenesteudbyderen i certifikatet har erklæret noget andet

(b) overholdelsen af alle dette direktivs krav med hensyn til udstedelsen af et autoriseret certifikat

(c) sikkerhed for, at den i det autoriserede certifikat identificerede person på udstedelsesdagen var i besiddelse af det signaturgenereringssystem, der svarer til det i certifikatet indeholdte eller omhandlede signaturkontrolsystem

(d) sikkerhed for at signaturgenereringssystemet og signaturkontrolsystemet fungerer komplementært med hinanden i de tilfælde, hvor det er certificeringstjenesteudbyderen, der genererer de to systemer.

2. Medlemsstaterne sikrer, at certificeringstjenesteudbyderen ikke ifalder erstatningsansvar for fejl i oplysninger i det autoriserede certifikat, som er afgivet af den person, til hvem certifikatet er udstedt, hvis certificeringstjenesteudbyderen kan godtgøre, at der er taget alle rimelige skridt til at kontrollere disse oplysninger.

3. Medlemsstaterne sikrer, at en certificeringstjenesteudbyder i et autoriseret certifikat kan anføre begrænsninger i et bestemt certifikats anvendelsesområde. Certificeringstjenesteudbyderen hæfter ikke for tab, der skyldes brug, der går ud over anvendelsesområdet for et autoriseret certifikat med begrænsninger i sit anvendelsesområde.

4. Medlemsstaterne sikrer, at certificeringstjenesteudbyderen i et autoriseret certifikat kan sætte en beløbsgrænse for de transaktioner, som certifikatet er gyldigt for. Certificeringstjenesteudbyderen ifalder ikke erstatningspligt, der overstiger denne beløbsgrænse.

5. Stk. 1-4 berører ikke Rådets direktiv 93/13/ØF[11].

Artikel 7
Internationale aspekter

1. Medlemsstaterne sikrer, at certifikater, der er udstedt af en certificeringstjenesteudbyder, der er etableret i et tredjeland, anses 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 i forbindelse med en frivillig akkrediteringsordning, der er fastsat af en medlemsstat, eller

   (b) hvis en certificeringstjenesteudbyder, der er etableret inden for Fællesskabet, og som opfylder kravene i bilag II, står inde for certifikatet i samme udstrækning som for sine egne certifikater, eller

   (c) hvis certifikatet eller certificeringstjenesteudbyderen er anerkendt i henhold til ordningen for bilaterale eller multilaterale aftaler mellem Fællesskabet og tredjelande eller internationale organisationer.

2. For at lette certificering på tværs af grænserne med tredjelande og retlig anerkendelse af 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, og navnlig, om fornødent, forelægge Rådet forslag til de nødvendige mandater til forhandling af bilaterale og multilaterale aftaler med tredjelande og internationale organisationer. Rådet træffer afgørelse med kvalificeret flertal.

Artikel 8
Databeskyttelse

1. Medlemsstaterne sikrer, at certificeringstjenesteudbyderne og de nationale akkrediterings- og tilsynsorganer opfylder kravene i de nationale bestemmelser til gennemførelse af Europa-Parlamentets og Rådets direktiv 95/46/EF[12] og 97/66/EF[13].

2. Medlemsstaterne sikrer, at certificeringstjenesteudbyderen kun har tilladelse til at få persondata direkte fra den registrerede og kun i det omfang, det er nødvendigt for udstedelsen af et certifikat. Data må ikke indsamles eller behandles med andre formål uden den registreredes samtykke.

---

[11] EFT L 95 af 21.4.1993, s. 29.
[12] EFT L 281 af 23.11.1995, s. 31.
[13] EFT L 24 af 30.1.1998, s. 1.

3. Medlemsstaterne sikrer, at certificeringstjenesteudbyderen, når underskriveren anmoder herom, på certifikatet anfører et pseudonym i stedet for underskriverens navn.

4. Medlemsstaterne sikrer, at certificeringstjenesteudbyderen i tilfælde, hvor personer anvender pseudonym, er forpligtet til på anmodning og med den registreredes samtykke at overføre data om sådanne personers identitet til offentlige myndigheder. Når det i henhold til national ret af hensyn til efterforskning i en kriminalsag i forbindelse med brugen af elektronisk signatur under pseudonym er nødvendigt at overføre data, der afslører en registrerets identitet, skal overførslen registreres og den registrerede underrettes om overførslen snarest muligt efter efterforskningens afslutning.

Artikel 9
Udvalg

Kommissionen bistås af et rådgivende udvalg, benævnt Elektronisk Signatur-Udvalget (herefter benævnt udvalget), der består af repræsentanter for medlemsstaterne, og som har Kommissionens repræsentant som formand.

Kommissionens repræsentant forelægger udvalget et udkast til de foranstaltninger, der skal træffes. Udvalget afgiver en udtalelse om dette udkast inden for en frist, som formanden kan fastsætte under hensyn til, hvor meget det pågældende spørgsmål haster, i givet fald ved afstemning.

Udtalelsen optages i mødeprotokollen; derudover har hver medlemsstat ret til at anmode om, at dens holdning indføres i mødeprotokollen.

Kommissionen tager størst muligt hensyn til udvalgets udtalelse. Den underretter udvalget om, hvorledes den har taget hensyn til dets udtalelse.

Artikel 10
Høring

Udvalget høres i nødvendigt omfang om kravene til certificeringstjenesteudbydere i bilag II og om alment anerkendte standarder for elektronisk signatur-produkter jf. artikel 3, stk. 3.

Artikel 11
Underretning

1. Medlemsstaterne meddeler Kommissionen følgende oplysninger:

   (a) oplysninger om frivillige nationale akkrediteringsordninger, herunder alle supplerende krav i henhold til artikel 3, stk. 4

   (b) navn og adresse på nationale akkrediterings- og tilsynsorganer

   (c) navn og adresse på akkrediterede nationale certificeringstjenesteudbydere.

2. Alle oplysninger i henhold til stk. 1 samt ændringer heraf meddeles af medlemsstaterne snarest muligt.

Artikel 12
Revisionsprocedurer

1. Kommissionen foretager en vurdering af, hvordan dette direktiv fungerer og aflægger rapport herom til Europa-Parlamentet og Rådet senest den 31. december 2002.

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

Artikel 13
Gennemførelse

1. Medlemsstaterne sætter de nødvendige love og administrative bestemmelser i kraft for at efterkomme dette direktiv senest den 31. december 2000. De underretter straks Kommissionen herom.

Når medlemsstaterne vedtager disse love og administrative bestemmelser, skal de indeholde en henvisning til dette direktiv, eller de skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for denne henvisning fastsættes af medlemsstaterne.

2. Medlemsstaterne meddeler Kommissionen teksten til de nationale retsforskrifter, som de udsteder på det område, der er omfattet af dette direktiv og på beslægtede områder.

Artikel 14
Ikrafttrædelse

Dette direktiv træder i kraft på tyvendedagen efter offentliggørelsen i De Europæiske Fællesskabers Tidende.

Artikel 15
Adressater

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den

På Europa-Parlamentets vegne

Formand

På Rådets vegne

Formand

BILAG I
Krav til autoriserede certifikater

Autoriserede certifikater skal indeholde:

a) den udstedende certificeringstjenesteudbyders identifikator

b) indehaverens entydige navn eller entydige pseudonym; i sidstnævnte tilfælde skal det fremgå, at der er tale om et pseudonym

c) særlige oplysninger om indehaveren, som f.eks. vedkommendes adresse, prokura i en virksomhed, kreditværdighed, moms- eller skatteregistreringsnummer, eventuelle betalingsgarantier eller bestemte tilladelser eller fuldmagter

d) et signaturkontrolsystem, som svarer til signaturgenereringssystemet, som er under indehaverens kontrol

e) certifikatets ikrafttrædelses- og udløbsdato

f) certifikatets unikke identifikationskode

g) den udstedende certificeringstjenesteudbyders elektroniske signatur

h) eventuelle begrænsninger i certifikatets anvendelsesområde og

i) eventuelle begrænsninger i certificeringstjenesteudbyderens hæftelse og i værdien af de transaktioner, for hvilke certifikatet er gyldigt.

BILAG II
Krav til certificeringstjenesteudbydere

Certificeringstjenesteudbydere skal/må:

a) udvise den fornødne pålidelighed til at kunne udbyde certificeringstjenester

b) have en hurtig og sikker tilbagekaldelsesservice

c) med hensigtsmæssige midler kontrollere de personers identitet og bemyndigelser, til hvem der udstedes autoriserede certifikater

d) beskæftige personale med de(n) ekspertviden, erfaring og kvalifikationer, som de tilbudte tjenesteydelser kræver, navnlig ledelseskompetence, sagkundskab inden for elektronisk signatur-teknologi og indgående kendskab til korrekte sikkerheds-procedurer; de skal også anvende adækvate administrative og ledelsesmæssige procedurer og processer, som overholder anerkendte standarder

e) anvende pålidelige systemer og elektronisk signatur-produkter, som er sikret mod at blive ændret på en sådan måde, at de kan anvendes til andre end deres oprindelige formål; de skal også anvende elektronisk signatur-produkter, som garanterer de af disse produkter understøttede certificeringsprocessers tekniske og kryptografiske sikkerhed

f) træffe foranstaltninger imod forfalskning af certifikater, og, hvis certificerings-tjenesteyderen genererer private kryptografiske signaturnøgler, garantere fortrolighed under genereringsprocessen

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

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

i) ikke opbevare eller kopiere de personers private kryptografiske signaturnøgler, som certificeringstjenesteyderen har tilbudt nøglehåndteringstjenester, medmindre disse udtrykkelig anmoder herom

j) skriftligt informere forbrugere, der ønsker at indgå en aftale, i et umiddelbart forståeligt sprog og under anvendelse af et bestandigt kommunikationsmedium om de nøjagtige vilkår for anvendelsen af certifikatet, herunder eventuelle begræns-ninger i hæftelse, en eventuel frivillig akkreditering og procedurer for klager og bilæggelse af tvister.

ISSN 0254-1459

KOM(98) 297 endelig udg.

DOKUMENTER

DA **15 06 10 01**

Katalognummer : CB-CO-98-336-DA-C

ISBN 92-78-36437-1

Kontoret for De Europæiske Fællesskabers Officielle Publikationer

L-2985 Luxembourg