II

(Vorbereitende Rechtsakte)

KOMMISSION

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen

(98/C 325/04)

(Text von Bedeutung für den EWR)

KOM(1998) 297 endg. — 98/0191(COD)

(Von der Kommission vorgelegt am 16. Juni 1998)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 57 Absatz 2, die Artikel 66 und 100a,

auf Vorschlag der Kommission,

nach Stellungnahme des Wirtschafts- und Sozialausschusses,

nach Stellungnahme des Ausschusses der Regionen,

gemäß dem Verfahren in Artikel 189b EG-Vertrag,

in Erwägung nachstehender Gründe:

(1) Am 16. April 1997 legte die Kommission dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuß und dem Ausschuß der Regionen eine Mitteilung zu einer „Europäischen Initiative für den elektronischen Geschäftsverkehr" [1] vor.

(2) Am 8. Oktober 1997 unterbreitete die Kommission dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuß und dem Ausschuß der Regionen eine Mitteilung über „Sicherheit und Vertrauen in der elektronischen Kommunikation — Ein europäischer Rahmen für digitale Signaturen und Verschlüsselung" [2].

(3) Am 1. Dezember 1997 forderte der Rat die Kommission auf, so bald wie möglich einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über digitale Signaturen vorzulegen.

(4) Elektronische Kommunikation und elektronischer Geschäftsverkehr erfordern elektronische Signaturen und entsprechende Authentifizierungsdienste für Daten. Divergierende Regeln in den Mitgliedstaaten über die rechtliche Anerkennung elektronischer Signaturen und die Akkreditierung von Zertifizierungsdiensteanbietern können ein ernsthaftes Hindernis für die elektronische Kommunikation und den elektronischen Geschäftsverkehr darstellen und damit die Entwicklung des Binnenmarktes beeinträchtigen. Divergierende Aktivitäten in den Mitgliedstaaten sind ein Anzeichen für den Bedarf an Harmonisierung auf Gemeinschaftsebene.

(5) Die Interoperabilität von Produkten für elektronische Signaturen sind zu fördern. Gemäß Artikel 7a des Vertrages umfaßt der Binnenmarkt einen Raum ohne Binnengrenzen, in dem der freie Warenverkehr zu gewährleisten ist. Es sind grundlegende Anforderungen zu erfüllen, die für die von Zertifizierungsdiensteanbietern verwendeten elektronischen Signaturprodukte charakteristisch sind, um den freien Verkehr im Binnenmarkt und das Vertrauen in digitale Signaturen zu fördern.

(6) Die rasche technologische Entwicklung und der globale Charakter des Internet erfordern ein Konzept, das verschiedenen Technologien und Dienstleistungen im Bereich der elektronischen Authentifizierung offensteht. „Digitale Signaturen" auf der Basis eines Kryptographiesystems mit öffentlich bekanntem Schlüssel sind jedoch derzeit die anerkannteste Form der elektronischen Signatur.

---

[1] KOM(97) 157 endg.

[2] KOM(97) 503 endg.

(7) Der Binnenmarkt gestattet es Zertifizierungsdiensteanbietern, grenzüberschreitend tätig zu werden, um ihre Wettbewerbsfähigkeit zu steigern und damit Verbrauchern und Unternehmen neue Möglichkeiten des sicheren, grenzenlosen Informationsaustausches und elektronischen Geschäftsverkehrs zu eröffnen. Um das gemeinschaftsweite Anbieten von Zertifizierungsdiensten über offene Netze zu fördern, sollten Anbieter von Zertifizierungsdiensten diese in der Regel ungehindert ohne vorherige Genehmigung bereitstellen können. Es ist zur Zeit nicht erforderlich, den freien Verkehr von Zertifizierungsdiensten zu gewährleisten, indem begründete und verhältnismäßige einzelstaatliche Beschränkungen der Erbringung dieser Dienste vereinheitlicht werden.

(8) Freiwillige Akkreditierungssysteme, die auf die Bereitstellung hochwertiger Dienste abzielen, können Zertifizierungsdiensteanbietern den geeigneten Rahmen für die Weiterentwicklung ihrer Dienste bieten, um das auf dem sich entwickelnden Markt geforderte Maß an Vertrauen, Sicherheit und Qualität zu erreichen. Diese Systeme sollten die Entwicklung bester Praktiken durch Zertifizierungsdiensteanbieter fördern. Zertifizierungsdiensteanbietern sollte es freistehen, sich akkreditieren zu lassen, um von der Akkreditierung zu profitieren. Die Mitgliedstaaten sollen es Anbietern von Zertifizierungsdiensten nicht untersagen, auch ohne Akkreditierung tätig zu sein. Es ist darauf zu achten, daß Akkreditierungssysteme den Wettbewerb im Bereich der Zertifizierungsdienste nicht einschränken. Es ist wichtig, ein ausgewogenes Verhältnis zwischen den Bedürfnissen der Verbraucher und der Unternehmen herzustellen.

(9) Diese Richtlinie soll daher zur Verwendung und zur rechtlichen Anerkennung elektronischer Signaturen in der Gemeinschaft beitragen. Es bedarf keiner rechtlichen Rahmenbedingungen für elektronische Signaturen, die ausschließlich in geschlossenen Systemen verwendet werden. Die Freiheit der Parteien, die Bedingungen zu vereinbaren, unter denen sie elektronisch signierte Daten akzeptieren, sollte respektiert werden, soweit dies im Rahmen des innerstaatlichen Rechts möglich ist. Diese Richtlinie zielt nicht darauf ab, nationales Vertragsrecht, insbesondere betreffend die Ausgestaltung und Erfüllung von Verträgen oder andere außervertragliche Formvorschriften, die Unterschriften erfordern, zu harmonisieren. Deshalb sollten die Regelungen über die rechtliche Anerkennung elektronischer Signaturen unbeschadet von nationalen gesetzlichen Vorschriften über die Form beim Abschluß von Verträgen oder die Festlegung des Ortes eines Vertragsabschlusses gelten.

(10) Um die allgemeine Akzeptanz elektronischer Signaturen zu fördern, darf einer elektronischen Signatur nicht die Rechtsgültigkeit mit der allgemeinen Begründung abgesprochen werden, daß sie in elektronischer Form vorliegt, nicht auf einem qualifizierten oder nicht auf von einem akkreditierten Diensteanbieter ausgestellten Zertifikat basiert oder der Diensteanbieter, der das Zertifikat ausgestellt hat, aus einem anderen Mitgliedstaat stammt. Elektronische Signaturen, die von einem vertrauenswürdigen, die grundlegenden Anforderungen erfüllenden Diensteanbieter zertifiziert werden, sollten die gleiche Rechtswirkung haben wie handschriftliche Unterschriften. Es muß gewährleistet sein, daß elektronische Signaturen in allen Mitgliedstaaten bei Gerichtsverfahren als Beweismittel anerkannt werden. Die rechtliche Anerkennung elektronischer Signaturen sollte auf objektiven Kriterien beruhen und nicht mit einer Genehmigung für den betreffenden Diensteanbieter verknüpft sein. Durch eine harmonisierte Regelung der rechtlichen Wirkung elektronischer Signaturen läßt sich gemeinschaftsweit ein kohärenter Rechtsrahmen aufrechterhalten.

(11) Diensteanbieter, die ihre Zertifizierungsdienste öffentlich anbieten, unterliegen den einzelstaatlichen Haftungsregelungen. Unterschiede bezüglich der Reichweite und des Inhalts dieser Regelungen können zu Rechtsunsicherheit führen, insbesondere bei Dritten, die sich auf diese Dienste verlassen. Diese Unsicherheit wirkt sich nachteilig auf die Entwicklung des grenzüberschreitenden Handels aus und behindert das Funktionieren des Binnenmarktes. Harmonisierte Haftungsregelungen schaffen Rechtssicherheit und Berechenbarkeit für Zertifizierungsdiensteanbieter und Verbraucher. Diese Regelungen würden zur generellen Akzeptanz und rechtlichen Anerkennung elektronischer Signaturen in der Gemeinschaft beitragen und sich damit positiv auf das Funktionieren des Binnenmarktes auswirken.

(12) Die Entwicklung des internationalen elektronischen Geschäftsverkehrs erfordert grenzüberschreitende Mechanismen, in die Drittländer einbezogen werden und die auf kommerzieller Ebene entwickelt werden sollten. Um die weltweite Interoperabilität zu gewährleisten, könnten Vereinbarungen mit Drittländern über multilaterale Regelungen und die gegenseitige Anerkennung von Zertifizierungsdiensten von Vorteil sein.

(13) Elektronische Kommunikation und elektronischer Geschäftsverkehr können gefördert werden, wenn Vertrauen auf seiten der Nutzer hergestellt wird. Daher müssen die Mitgliedstaaten Zertifizierungsdiensteanbieter verpflichten, das Datenschutzrecht und den Schutz der Privatsphäre zu beachten. Zertifizierungsdiensteanbieter sollten, auf Wunsch des

Unterzeichners, Zertifizierungsdienste auch bei Verwendung von Pseudonymen anbieten. Im nationalen Recht sollte festgelegt werden, ob und unter welchen Voraussetzungen Daten, die die Identität der betroffenen Person zur Aufklärung von Straftaten betreffen, aufgedeckt werden müssen. Zertifizierungsdiensteanbieter sollten die Benutzer im voraus schriftlich, in klar verständlicher Sprache und über ein dauerhaftes Kommunikationsmittel über ihre Geschäftsbedingungen informieren, vor allem über die genaue Verwendung ihrer Zertifikate und über Haftungsbeschränkungen.

(14) Bei der Anwendung dieser Richtlinie sollte die Kommission von einem Ausschuß mit beratender Funktion unterstützt werden.

(15) Entsprechend dem in Artikel 3b EG-Vertrag niedergelegten Subsidiaritäts- und Verhältnismäßigkeitsprinzip kann das Ziel dieser Richtlinie, nämlich die Schaffung harmonisierter rechtlicher Rahmenbedingungen für die Bereitstellung elektronischer Signaturen, auf der Ebene der Mitgliedstaaten nicht ausreichend erreicht werden und läßt sich daher besser auf Gemeinschaftsebene verwirklichen. Diese Richtlinie beschränkt sich auf die zur Erreichung dieses Ziels notwendige Mindestmaß und geht nicht über das dazu Erforderliche hinaus —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1

Geltungsbereich

Mit dieser Richtlinie wird die rechtliche Anerkennung elektronischer Signaturen gewährleistet.

Sie erstreckt sich nicht auf andere Aspekte im Zusammenhang mit dem Abschluß und der Geltung von Verträgen oder mit anderen außervertraglichen Formvorschriften, die Unterschriften voraussetzen.

Sie enthält rechtliche Rahmenbedingungen für bestimmte, öffentlich angebotene Zertifizierungsdienste.

Artikel 2

Begriffsbestimmungen

Im Sinne dieser Richtlinie bedeutet:

1. „elektronische Signatur“: eine Signatur in digitaler Form, die in Daten enthalten ist, Daten beigefügt wird oder logisch mit ihnen verknüpft ist und von einem Unterzeichner verwendet wird, um zu bestätigen, daß er den Inhalt dieser Daten billigt. Die elektronische Signatur muß folgende Anforderungen erfüllen:

   a) Sie ist ausschließlich dem Unterzeichner zugewiesen.

   b) Sie kann den Unterzeichner identifizieren.

   c) Sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann.

   d) Sie ist so mit den Daten verknüpft, daß eine nachträgliche Veränderung der Daten offenkundig wird.

2. „Unterzeichner“: eine Person, die eine elektronische Signatur erstellt.

3. „Signaturerstellungseinheit“: einmalige Daten wie Codes oder private kryptographische Schlüssel oder ein einmalig konfiguriertes physisches Werkzeug, das vom Unterzeichner verwendet wird, um eine Signatur zu erstellen.

4. „Signaturprüfeinheit“: einmalige Daten wie Codes oder öffentliche kryptographische Schlüssel oder ein einmalig konfiguriertes physisches Werkzeug, das verwendet wird, um die elektronische Signatur zu überprüfen.

5. „Qualifiziertes Zertifikat“: eine Bescheinigung in digitaler Form, die eine Signaturprüfeinheit einer Person zuordnet, die Identität dieser Person bestätigt und den Anforderungen in Anhang I entspricht.

6. „Zertifizierungsdiensteanbieter“: eine Person oder Stelle, die Zertifikate erteilt oder anderweitige elektronische Signaturdienste öffentlich anbietet.

7. „Elektronisches Signaturprodukt“: Hard- oder Software bzw. Komponenten davon, die ein Zertifizierungsdiensteanbieter für die Bereitstellung von elektronischen Signaturdiensten verwendet.

Artikel 3

Marktzugang

(1) Die Mitgliedstaaten machen die Bereitstellung von Zertifizierungsdiensten nicht von einer vorherigen Genehmigung abhängig.

(2) Unbeschadet des Absatzes 1 können die Mitgliedstaaten freiwillige Akkreditierungssysteme einführen bzw. beibehalten, die auf höherwertige Zertifizierungsdienste abzielen. Alle mit diesen Systemen verknüpften Anforderungen müssen objektiv, transparent, verhältnismäßig und nichtdiskriminierend sein. Die Mitgliedstaaten dürfen die Zahl der Zertifizierungsdiensteanbieter nicht aus Gründen einschränken, die in den Geltungsbereich dieser Richtlinie fallen.

(3) Die Kommission kann gemäß Artikel 9 Referenznummern für allgemein anerkannte Normen für elektronische Signaturprodukte festlegen und im *Amtsblatt der Europäischen Gemeinschaften* veröffentlichen. Die Mitgliedstaaten gehen davon aus, daß die Anforderungen in Anhang II Buchstabe e) erfüllt sind, wenn ein elektronisches Signaturprodukt diesen Normen entspricht.

(4) Die Mitgliedstaaten können den Einsatz elektronischer Signaturen im öffentlichen Bereich zusätzlichen Anforderungen unterwerfen. Diese Auflagen müssen objektiv, transparent, verhältnismäßig und nichtdiskriminierend sein und dürfen sich nur auf die spezifischen Merkmale des betreffenden Verwendungszwecks beziehen.

Artikel 4

Binnenmarktgrundsätze

(1) Jeder Mitgliedstaat wendet die Bestimmungen, die er aufgrund dieser Richtlinie verabschiedet, auf die in seinem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter und deren Dienste an. Die Mitgliedstaaten dürfen die Bereitstellung von Zertifizierungsdiensten durch Diensteanbieter aus anderen Mitgliedstaaten in den unter diese Richtlinie fallenden Bereichen nicht einschränken.

(2) Die Mitgliedstaaten sorgen dafür, daß elektronische Signaturprodukte, die den Anforderungen dieser Richtlinie entsprechen, frei im Binnenmarkt vertrieben werden können.

Artikel 5

Rechtsgültigkeit

(1) Die Mitgliedstaaten sorgen dafür, daß einer elektronischen Signatur die Rechtsgültigkeit nicht allein deshalb abgesprochen wird, weil sie in elektronischer Form vorliegt oder nicht auf einem qualifizierten oder von einem akkreditierten Diensteanbieter ausgestellten Zertifikat basiert.

(2) Die Mitgliedstaaten stellen sicher, daß elektronische Signaturen, die auf einem qualifizierten Zertifikat basieren, welches von einem Zertifizierungsdiensteanbieter erteilt wurde, der den Anforderungen in Anhang II genügt, zur Erfüllung des rechtlichen Erfordernisses einer handschriftlichen Unterschrift anerkannt werden und in Gerichtsverfahren in gleicher Weise wie handschriftliche Unterschriften als Beweismittel zugelassen sind.

Artikel 6

Haftung

(1) Die Mitgliedstaaten sorgen dafür, daß ein Diensteanbieter, der ein qualifiziertes Zertifikat ausstellt, gegenüber jeder Person, die vernünftigerweise auf das Zertifikat vertraut, dafür haftet, daß

a) alle Informationen im qualifizierten Zertifikat zum Zeitpunkt seiner Ausstellung richtig sind, soweit der Diensteanbieter im Zertifikat nichts Gegenteiliges angegeben hat;

b) alle Anforderungen dieser Richtlinie bei der Ausstellung des qualifizierten Zertifikats eingehalten wurden;

c) die im qualifizierten Zertifikat angegebene Person zum Zeitpunkt der Ausstellung des Zertifikats im Besitz der Signaturerstellungseinheit ist, die der im Zertifikat angegebenen bzw. identifizierten Signaturprüfeinheit entspricht;

d) in Fällen, in denen der Zertifizierungsdiensteanbieter sowohl die Signaturerstellungseinheit als auch die Signaturprüfeinheit erzeugt, beide Komponenten in komplementärer Weise funktionieren.

(2) Die Mitgliedstaaten sorgen dafür, daß der Zertifizierungsdiensteanbieter für Fehler im qualifizierten Zertifikat, die auf Informationen beruhen, die er von der Person erhält, für die das Zertifikat ausgestellt wird, nicht haftet, wenn er nachweisen kann, daß er alle zumutbaren Schritte unternommen hat, um diese Informationen zu überprüfen.

(3) Die Mitgliedstaaten sorgen dafür, daß Zertifizierungsdiensteanbieter im qualifizierten Zertifikat Beschränkungen des Anwendungsbereichs des Zertifikats vorgeben können. Der Zertifizierungsdiensteanbieter haftet nicht für Schäden, die sich aus einer über den Anwendungsbereich hinausgehenden Nutzung des qualifizierten Zertifikats ergeben.

(4) Die Mitgliedstaaten sorgen dafür, daß Zertifizierungsdiensteanbieter im qualifizierten Zertifikat den Wert der Transaktionen begrenzen können, für die das Zertifikat gültig ist. Der Zertifizierungsdiensteanbieter haftet nicht für Schäden, die sich aus der Überschreitung dieser Höchstgrenze ergeben.

(5) Die Absätze 1 bis 4 gelten unbeschadet der Richtlinie 93/13/EWG des Rates [1].

[1] ABl. L 95 vom 21.4.1993, S. 29.

Artikel 7

Internationale Aspekte

(1) Die Mitgliedstaaten sorgen dafür, daß Zertifikate, die von einem Zertifizierungsdiensteanbieter eines Drittlandes ausgestellt werden, den von einem in der Gemeinschaft niedergelassenen Diensteanbieter ausgestellten Zertifikaten rechtlich gleichgestellt werden, wenn

a) der Zertifizierungsdiensteanbieter die Anforderungen dieser Richtlinie erfüllt und unter einem freiwilligen Akkreditierungssystem eines Mitgliedstaats akkreditiert ist oder

b) ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen gemäß Anhang II erfüllt, für das Zertifikat in gleichem Umfang einsteht wie für seine eigenen Zertifikate oder

c) das Zertifikat oder der Zertifizierungsdiensteanbieter im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Gemeinschaft und Drittländern oder internationalen Organisationen anerkannt ist.

(2) Die Kommission kann Maßnahmen ergreifen, um grenzüberschreitende Zertifizierungsdienste mit Drittländern und die rechtliche Anerkennung elektronischer Signaturen, die aus Drittländern stammen, zu erleichtern. Hierzu kann sie Vorschläge unterbreiten, um die effiziente Umsetzung von Normen und internationalen Vereinbarungen über Zertifizierungsdienste zu gewährleisten. Insbesondere kann sie dem Rat bei Bedarf Vorschläge zur Erteilung von Mandaten zur Aushandlung bilateraler und multilateraler Vereinbarungen mit Drittländern und internationalen Organisationen vorlegen. Der Rat beschließt mit qualifizierter Mehrheit.

Artikel 8

Datenschutz

(1) Die Mitgliedstaaten sorgen dafür, daß Zertifizierungsdiensteanbieter und die für die Akkreditierung und Aufsicht zuständigen nationalen Stellen die nationalen Vorschriften zur Umsetzung der Richtlinien 95/46/EG [1] und 97/66/EG [2] des Europäischen Parlaments und des Rates einhalten.

(2) Die Mitgliedstaaten sorgen dafür, daß Zertifizierungsdiensteanbieter personenbezogene Daten nur unmittelbar von der betroffenen Person einholen können und nur insoweit, als dies zur Ausstellung eines Zertifikats erforderlich ist. Die Daten dürfen ohne Zustimmung der betroffenen Person nicht für anderweitige Zwecke erfaßt oder verarbeitet werden.

(3) Die Mitgliedstaaten sorgen dafür, daß der Zertifizierungsdiensteanbieter auf Verlangen des Unterzeichners im Zertifikat ein Pseudonym anstelle des Namens des Unterzeichners angibt.

(4) Die Mitgliedstaaten sorgen dafür, daß Zertifizierungsdiensteanbieter Daten über die Identität von Personen, die Pseudonyme verwenden, mit Zustimmung der betroffenen Person an Behörden auf deren Anforderung weitergeben. Wenn nach nationalem Recht die Weitergabe der Daten über die Identität der betroffenen Person zur Aufklärung von Straftaten, im Zusammenhang mit dem Einsatz elektronischer Signaturen unter einem Pseudonym, erforderlich ist, ist die Weitergabe zu registrieren und die betroffene Person nach Abschluß der Ermittlungen so bald wie möglich über die Weitergabe ihrer Daten zu unterrichten.

Artikel 9

Ausschuß

Die Kommission wird von einem Ausschuß mit beratender Funktion, dem „Ausschuß für elektronische Signaturen" (im folgenden „Ausschuß" genannt), unterstützt, der sich aus Vertretern der Mitgliedstaaten zusammensetzt und in dem der Vertreter der Kommission den Vorsitz führt.

Der Vertreter der Kommission unterbreitet dem Ausschuß einen Entwurf der zu treffenden Maßnahmen. Der Ausschuß gibt — gegebenenfalls nach Abstimmung — seine Stellungnahme zu diesem Entwurf innerhalb einer Frist ab, die der Vorsitzende unter Berücksichtigung der Dringlichkeit der betreffenden Frage festsetzen kann.

Die Stellungnahme wird in das Protokoll aufgenommen; darüber hinaus hat jeder Mitgliedstaat das Recht zu verlangen, daß sein Standpunkt im Protokoll festgehalten wird.

Die Kommission berücksichtigt so weit wie möglich die Stellungnahme des Ausschusses. Sie unterrichtet den Ausschuß darüber, inwieweit sie seine Stellungnahme berücksichtigt hat.

Artikel 10

Konsultation des Ausschusses

Der Ausschuß ist bei Bedarf zu den in Anhang II aufgeführten Anforderungen an Zertifizierungsdiensteanbieter sowie zu allgemein anerkannten Normen für elektronische Signaturprodukte gemäß Artikel 3 Absatz 3 zu konsultieren.

---

[1] ABl. L 281 vom 23.11.1995, S. 31.

[2] ABl. L 24 vom 30.1.1998, S. 1.

Artikel 11

Notifizierung

(1) Die Mitgliedstaaten übermitteln der Kommission folgende Informationen:

a) Angaben zu freiwilligen nationalen Akkreditierungssystemen einschließlich zusätzlicher Anforderungen gemäß Artikel 3 Absatz 4,

b) Namen und Anschriften der für Akkreditierung und Aufsicht zuständigen nationalen Stellen sowie

c) Namen und Anschriften der akkreditierten nationalen Zertifizierungsdiensteanbieter.

(2) Die auf der Grundlage von Absatz 1 gelieferten Informationen und diesbezügliche Änderungen sind von den Mitgliedstaaten so schnell wie möglich zu übermitteln.

Artikel 12

Überprüfungen

(1) Die Kommission überprüft die Durchführung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat spätestens zum 31. Dezember 2002 darüber Bericht.

(2) Bei der Überprüfung ist unter anderem festzustellen, ob der Geltungsbereich der Richtlinie angesichts der technologischen und rechtlichen Entwicklungen zu ändern ist. Der Bericht umfaßt insbesondere eine Bewertung der Harmonisierungsaspekte auf der Grundlage der gesammelten Erfahrungen. Gegebenenfalls sind Änderungsvorschläge beizufügen.

Artikel 13

Umsetzung

(1) Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie spätestens am 31. Dezember 2000 nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Bei dem Erlaß dieser Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Die Mitgliedstaaten teilen der Kommission alle innerstaatlichen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden oder einem angrenzendem Gebiet erlassen, zusammen mit einer Übereinstimmungstabelle zwischen dieser Richtlinie und den nationalen Bestimmungen.

Artikel 14

Inkrafttreten

Diese Richtlinie tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Gemeinschaften* in Kraft.

Artikel 15

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

ANHANG I

ANFORDERUNGEN AN QUALIFIZIERTE ZERTIFIKATE

Qualifizierte Zertifikate müssen folgende Angaben enthalten:

a) die Kennung des Diensteanbieters, der das Zertifikat erteilt;

b) den unverwechselbaren Namen des Inhabers oder ein unverwechselbares Pseudonym, das als solches zu identifizieren ist;

c) ein spezifisches Attribut des Inhabers (z. B. die Adresse, die Vertretungsbefugnis für ein Unternehmen, Kreditwürdigkeit, (Mehrwert-)Steuernummer, Zahlungsgarantien oder spezielle Genehmigungen bzw. Lizenzen);

d) eine Signaturprüfeinheit, die einer vom Inhaber kontrollierten Signaturerstellungseinheit entspricht;

e) Beginn und Ende der Laufzeit des Zertifikats;

f) den eindeutigen Identitätscode des Zertifikats;

g) die elektronische Signatur des ausstellenden Diensteanbieters;

h) gegebenenfalls Beschränkungen des Anwendungsbereichs des Zertifikats und

i) gegebenenfalls Begrenzungen der Haftung des Zertifizierungsdiensteanbieters oder des Wertes der Transaktionen, für die das Zertifikat gilt.

ANHANG II

ANFORDERUNGEN AN ZERTIFIZIERUNGSDIENSTEANBIETER

Zertifizierungsdiensteanbieter

a) müssen die erforderliche Zuverlässigkeit für die Bereitstellung von Zertifizierungsdiensten besitzen;

b) müssen einen schnellen und sicheren Widerrufsdienst anbieten;

c) müssen mit geeigneten Mitteln die Identität und Vertretungsbefugnis der Person überprüfen, der ein qualifiziertes Zertifikat ausgestellt wird;

d) müssen Personal mit den für die angebotenen Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen beschäftigen. Dazu gehören vor allem Managementkompetenzen, Kenntnisse der Technologie elektronischer Signaturen und Vertrautheit mit angemessenen Sicherheitsverfahren. Sie müssen ferner geeignete Verwaltungs- und Managementverfahren einhalten, die anerkannten Normen entsprechen;

e) müssen vertrauenswürdige Systeme und elektronische Signaturprodukte einsetzen, die Schutz gegen unbefugte Veränderungen der Produkte gewährleisten und ausschließen, daß sie für andere Zwecke verwendet werden als die, für die sie bestimmt sind. Sie müssen ferner elektronische Signaturprodukte verwenden, die die technische und kryptographische Sicherheit der unterstützten Zertifizierungsverfahren gewährleisten;

f) müssen Maßnahmen gegen Fälschungen von Zertifikaten ergreifen und bei Erstellung privater kryptographischer Signaturschlüssel die Vertraulichkeit während der Erstellung gewährleisten;

g) müssen über ausreichende Finanzmittel verfügen, um den Anforderungen dieser Richtlinie entsprechend arbeiten zu können. Sie müssen vor allem in der Lage sein, das Haftungsrisiko für Schäden zu tragen, zum Beispiel durch Abschluß einer entsprechenden Versicherung;

h) müssen alle einschlägigen Informationen über ein qualifiziertes Zertifikat über einen angemessenen Zeitraum aufzeichnen, um insbesondere für Gerichtsverfahren die Zertifizierung nachweisen zu können. Die Aufzeichnungen können in elektronischer Form erfolgen;

i) dürfen keine privaten kryptographischen Signaturschlüssel von Personen speichern oder kopieren, denen Schlüsselmanagementdienste angeboten werden, sofern diese nicht ausdrücklich darum ersuchen;

j) müssen die Verbraucher vor Abschluß eines Vertrages schriftlich, in klar verständlicher Sprache und mit einem dauerhaften Kommunikationsmittel über die genauen Bedingungen für die Verwendung des Zertifikats informieren. Dazu gehören u. a. Haftungsbeschränkungen, die Existenz eines freiwilligen Akkreditierungssystems sowie das Vorgehen in Beschwerde- und Schlichtungsverfahren.
