RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 13. Dezember 1999
über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 47 Absatz 2, Artikel 55 und 95,

auf Vorschlag der Kommission [1],

nach Stellungnahme des Wirtschafts- und Sozialausschusses [2],

nach Stellungnahme des Ausschusses der Regionen [3],

gemäß dem Verfahren des Artikels 251 des Vertrags [4],

in Erwägung nachstehender Gründe:

(1) Am 16. April 1997 hat die Kommission dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuß und dem Ausschuß der Regionen eine Mitteilung mit dem Titel „Europäische Initiative für den elektronischen Geschäftsverkehr" vorgelegt.

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

(3) Am 1. Dezember 1997 hat der Rat die Kommission aufgefordert, 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 über die rechtliche Anerkennung elektronischer Signaturen und die Akkreditierung von Zertifizierungsdiensteanbietern in den Mitgliedstaaten können ein ernsthaftes Hindernis für die elektronische Kommunikation und den elektronischen Geschäftsverkehr darstellen. Klare gemeinschaftliche Rahmenbedingungen für elektronische Signaturen stärken demgegenüber das Vertrauen und die allgemeine Akzeptanz hinsichtlich der neuen Technologien. Die Rechtsvorschriften der Mitgliedstaaten sollten den freien Waren- und Dienstleistungsverkehr im Binnenmarkt nicht behindern.

(5) Die Interoperabilität von Produkten für elektronische Signaturen sollte gefördert werden. Gemäß Artikel 14 des Vertrags umfaßt der Binnenmarkt einen Raum ohne Binnengrenzen, in dem der freie Warenverkehr gewährleistet ist. Es sind grundlegende Anforderungen zu erfüllen, die speziell für Produkte für elektronische Signaturen gelten, um so den freien Verkehr im Binnenmarkt zu gewährleisten und das Vertrauen in digitale Signaturen zu fördern, wobei die Verordnung (EG) Nr. 3381/94 des Rates vom 19. Dezember 1994 über eine Gemeinschaftsregelung der Ausfuhrkontrolle von Gütern mit doppeltem Verwendungszweck [5] und der Beschluß 94/942/GASP des Rates vom 19. Dezember 1994 über die vom Rat angenommene gemeinsame Aktion zur Ausfuhrkontrolle von Gütern mit doppeltem Verwendungszweck [6] unberührt bleiben.

(6) Mit der vorliegenden Richtlinie wird die Erbringung von Dienstleistungen im Bereich der Vertraulichkeit von Informationen nicht harmonisiert, wenn für derartige Dienstleistungen einzelstaatliche Vorschriften hinsichtlich der öffentlichen Ordnung oder Sicherheit gelten.

(7) Der Binnenmarkt gewährleistet die Freizügigkeit von Personen, wodurch Bürger und Gebietsansässige der Europäischen Union zunehmend mit Stellen in anderen Mitgliedstaaten als demjenigen ihres Wohnsitzes in Verbindung treten müssen. Die Möglichkeit der elektronischen Kommunikation könnte in dieser Hinsicht von großem Nutzen sein.

(8) Die rasche technologische Entwicklung und der globale Charakter des Internet erfordern ein Konzept, das verschiedenen Technologien und Dienstleistungen im Bereich der elektronischen Authentifizierung offensteht.

(9) Elektronische Signaturen werden bei einer Vielzahl von Gegebenheiten und Anwendungen genutzt, die zu einem großen Spektrum neuer Dienste und Produkte im Zusammenhang mit oder unter Verwendung von elektronischen Signaturen führen. Die Definition solcher Produkte und Dienste sollte sich nicht auf die Ausstellung und Verwaltung von Zertifikaten beschränken, sondern sollte auch alle sonstigen Dienste und Produkte einschließen, die elektronische Signaturen verwenden oder mit ihnen zusammenhängen, wie Registrierungsdienste, Zeitstempel, Verzeichnisdienste, Rechnerdienste oder Beratungsdienste in Verbindung mit elektronischen Signaturen.

(10) Der Binnenmarkt ermöglicht es Zertifizierungsdiensteanbietern, grenzüberschreitend tätig zu werden, um ihre Wettbewerbsfähigkeit zu steigern und damit Verbrauchern und Unternehmen ohne Rücksicht auf Grenzen neue Möglichkeiten des sicheren Informationsaustausches und elektronischen Geschäftsverkehrs zu eröffnen. Um das gemeinschaftsweite Anbieten von Zertifizierungsdiensten über offene Netze zu fördern, sollten Anbieter von Zertifizierungsdiensten diese ungehindert ohne vorherige Genehmigung bereitstellen können.

[1] ABl. C 325 vom 23.10.1998, S. 5.
[2] ABl. C 40 vom 15.2.1999, S. 29.
[3] ABl. C 93 vom 6.4.1999, S. 33.
[4] Stellungnahme des Europäischen Parlaments vom 13. Januar 1999 (ABl. C 104 vom 14.4.1999, S. 49). Gemeinsamer Standpunkt des Rates vom 28. Juni 1999 (ABl. C 243 vom 27.8.1999, S. 33) und Beschluß des Europäischen Parlaments vom 27. Oktober 1999 (noch nicht im Amtsblatt veröffentlicht). Beschluß des Rates vom 30. November 1999.

[5] ABl. L 367 vom 31.12.1994, S. 1. Verordnung geändert durch die Verordnung (EG) Nr. 837/95 (ABl. L 90 vom 21.4.1995, S. 1).
[6] ABl. L 367 vom 31.12.1994, S. 8. Beschluß zuletzt geändert durch den Beschluß 1999/193/GASP (ABl. L 73 vom 19.3.1999, S. 1).

Vorherige Genehmigung bedeutet nicht nur eine Erlaubnis, wonach der betreffende Zertifizierungsdiensteanbieter einen Bescheid der einzelstaatlichen Stellen einholen muß, bevor er seine Zertifizierungsdienste erbringen kann, sondern auch alle sonstigen Maßnahmen mit der gleichen Wirkung.

(11) Freiwillige Akkreditierungssysteme, die auf eine Steigerung des Niveaus der erbrachten 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 und Akkreditierungssysteme zu nutzen.

(12) Zertifizierungsdienste sollten entweder von einer öffentlichen Stelle oder einer juristischen oder natürlichen Person angeboten werden können, sofern diese im Einklang mit den einzelstaatlichen Rechtsvorschriften niedergelassen ist. Die Mitgliedstaaten sollten es Anbietern von Zertifizierungsdiensten nicht untersagen, auch ohne freiwillige Akkreditierung tätig zu sein. Es ist darauf zu achten, daß Akkreditierungssysteme den Wettbewerb im Bereich der Zertifizierungsdienste nicht einschränken.

(13) Die Mitgliedstaaten können entscheiden, wie sie die Überwachung der Einhaltung der Bestimmungen dieser Richtlinie gewährleisten. Diese Richtlinie schließt nicht aus, daß privatwirtschaftliche Überwachungssysteme geschaffen werden. Diese Richtlinie verpflichtet die Zertifizierungsdiensteanbieter nicht, eine Überwachung im Rahmen eines geltenden Akkreditierungssystems zu beantragen.

(14) Es ist wichtig, ein ausgewogenes Verhältnis zwischen den Bedürfnissen der Verbraucher und der Unternehmen herzustellen.

(15) Anhang III enthält die Anforderungen für sichere Signaturerstellungseinheiten zur Gewährleistung der Funktionalität fortgeschrittener elektronischer Signaturen. Er deckt nicht die gesamte Systemumgebung ab, in der die Einheit betrieben wird. Das Funktionieren des Binnenmarktes verlangt von der Kommission und den Mitgliedstaaten, rasch zu handeln, damit die Stellen benannt werden können, die für die Bewertung der Übereinstimmung von sicheren Signaturerstellungseinheiten mit den Anforderungen des Anhangs III zuständig sind. Um den Markterfordernissen zu entsprechen, muß die Bewertung der Übereinstimmung rechtzeitig und effizient erfolgen.

(16) Diese Richtlinie leistet einen Beitrag zur Verwendung und rechtlichen Anerkennung elektronischer Signaturen in der Gemeinschaft. Es bedarf keiner gesetzlichen Rahmenbedingungen für elektronische Signaturen, die ausschließlich in Systemen verwendet werden, die auf freiwilligen privatrechtlichen Vereinbarungen zwischen einer bestimmten Anzahl von Teilnehmern beruhen. 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. Elektronischen Signaturen, die in solchen Systemen verwendet werden, sollte die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht abgesprochen werden.

(17) Diese Richtlinie zielt nicht darauf ab, nationales Vertragsrecht, insbesondere betreffend den Abschluß und die Erfüllung von Verträgen, oder andere, außervertragliche Formvorschriften bezüglich der Unterschriften zu harmonisieren. Deshalb sollten die Regelungen über die rechtliche Wirksamkeit elektronischer Signaturen unbeschadet einzelstaatlicher Formvorschriften gelten, die den Abschluß von Verträgen oder die Festlegung des Ortes eines Vertragsabschlusses betreffen.

(18) Das Speichern und Kopieren von Signaturerstellungsdaten könnte die Rechtsgültigkeit elektronischer Signaturen gefährden.

(19) Elektronische Signaturen werden im öffentlichen Bereich innerhalb der staatlichen und gemeinschaftlichen Verwaltungen und im Kommunikationsverkehr zwischen diesen Verwaltungen sowie zwischen diesen und den Bürgern und Wirtschaftsteilnehmern eingesetzt, z. B. in den Bereichen öffentliche Auftragsvergabe, Steuern, soziale Sicherheit, Gesundheit und Justiz.

(20) Durch harmonisierte Kriterien im Zusammenhang mit der Rechtswirkung elektronischer Signaturen läßt sich gemeinschaftsweit ein kohärenter Rechtsrahmen aufrechterhalten. In den einzelstaatlichen Rechtsvorschriften sind verschiedene Anforderungen für die Rechtsgültigkeit handschriftlicher Unterschriften niedergelegt. Zertifikate können dazu dienen, die Identität einer elektronisch signierenden Person zu bestätigen. Auf qualifizierten Zertifikaten beruhende fortgeschrittene elektronische Signaturen zielen auf einen höheren Sicherheitsstandard. Fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und von einer sicheren Signaturerstellungseinheit erstellt werden, können nur dann gegenüber handschriftlichen Unterschriften als rechtlich gleichwertig angesehen werden, wenn die Anforderungen für handschriftliche Unterschriften erfüllt sind.

(21) Um die allgemeine Akzeptanz elektronischer Authentifizierungsmethoden zu fördern, ist zu gewährleisten, daß elektronische Signaturen in allen Mitgliedstaaten in Gerichtsverfahren als Beweismittel verwendet werden können. Die rechtliche Anerkennung elektronischer Signaturen sollte auf objektiven Kriterien beruhen und nicht mit einer Genehmigung für den betreffenden Zertifizierungsdiensteanbieter verknüpft sein. Die Festlegung der Rechtsgebiete, in denen elektronische Dokumente und elektronische Signaturen verwendet werden können, unterliegt einzelstaatlichem Recht. Diese Richtlinie läßt die Befugnis der einzelstaatlichen Gerichte, über die Übereinstimmung mit den Anforderungen dieser Richtlinie zu befinden, unberührt; sie berührt auch nicht die einzelstaatlichen Vorschriften über die freie gerichtliche Würdigung von Beweismitteln.

(22) Diensteanbieter, die ihre Zertifizierungsdienste öffentlich anbieten, unterliegen den einzelstaatlichen Haftungsregelungen.

(23) Die Entwicklung des internationalen elektronischen Geschäftsverkehrs erfordert grenzüberschreitende Vereinbarungen unter Beteiligung von Drittländern. Um die weltweite Interoperabilität zu gewährleisten, könnten Vereinbarungen mit Drittländern über multilaterale Regeln betreffend die gegenseitige Anerkennung der Zertifizierungsdienste nützlich sein.

(24) Zur Stärkung des Vertrauens der Nutzer in die elektronische Kommunikation und den elektronischen Geschäftsverkehr müssen die Zertifizierungsdiensteanbieter die Vorschriften über den Datenschutz und den Schutz der Privatsphäre achten.

(25) Die Bestimmungen über die Nutzung von Pseudonymen in Zertifikaten hindern die Mitgliedstaaten nicht daran, eine Identifizierung der Personen nach Gemeinschaftsrecht oder einzelstaatlichem Recht zu verlangen.

(26) Die zur Durchführung dieser Richtlinie erforderlichen Maßnahmen sind gemäß Artikel 2 des Beschlusses 1999/468/EG des Rates vom 28. Juni 1999 zur Festlegung der Modalitäten für die Ausübung der der Kommission übertragenen Durchführungsbefugnisse [1] zu erlassen.

(27) Die Kommission nimmt zwei Jahre nach der Umsetzung dieser Richtlinie eine Überprüfung vor, um unter anderem sicherzustellen, daß der technologische Fortschritt oder Änderungen des rechtlichen Umfelds keine Hindernisse für die Realisierung der erklärten Ziele dieser Richtlinie mit sich gebracht haben. Sie sollte die Auswirkungen verwandter technischer Bereiche prüfen und dem Europäischen Parlament und dem Rat hierüber einen Bericht vorlegen.

(28) Nach den in Artikel 5 des Vertrags niedergelegten Grundsätzen der Subsidiarität und der Verhältnismäßigkeit kann das Ziel der Schaffung harmonisierter rechtlicher Rahmenbedingungen für die Bereitstellung elektronischer Signaturen und entsprechender Dienste von den Mitgliedstaaten nicht ausreichend erreicht werden und läßt sich daher besser durch die Gemeinschaft verwirklichen. Diese Richtlinie geht nicht über das zur Erreichung dieses Ziels erforderliche Maß hinaus —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1

Anwendungsbereich

Diese Richtlinie soll die Verwendung elektronischer Signaturen erleichtern und zu ihrer rechtlichen Anerkennung beitragen. Sie legt rechtliche Rahmenbedingungen für elektronische Signaturen und für bestimmte Zertifizierungsdienste fest, damit das reibungslose Funktionieren des Binnenmarktes gewährleistet ist.

Es werden weder Aspekte im Zusammenhang mit dem Abschluß und der Gültigkeit von Verträgen oder anderen rechtlichen Verpflichtungen, für die nach einzelstaatlichem Recht oder Gemeinschaftsrecht Formvorschriften zu erfüllen sind, erfaßt, noch werden im einzelstaatlichen Recht oder im Gemeinschaftsrecht vorgesehene Regeln und Beschränkungen für die Verwendung von Dokumenten berührt.

Artikel 2

Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

1. „elektronische Signatur“ Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen;
2. „fortgeschrittene elektronische Signatur“ eine elektronische Signatur, die folgende Anforderungen erfüllt:
   a) Sie ist ausschließlich dem Unterzeichner zugeordnet;
   b) sie ermöglicht die Identifizierung des Unterzeichners;
   c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;
   d) sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, daß eine nachträgliche Veränderung der Daten erkannt werden kann;
3. „Unterzeichner“ eine Person, die eine Signaturerstellungseinheit besitzt und die entweder im eigenen Namen oder im Namen der von ihr vertretenen Stelle oder juristischen oder natürlichen Person handelt;
4. „Signaturerstellungsdaten“ einmalige Daten wie Codes oder private kryptographische Schlüssel, die vom Unterzeichner zur Erstellung einer elektronischen Signatur verwendet werden;
5. „Signaturerstellungseinheit“ eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturerstellungsdaten verwendet wird;
6. „sichere Signaturerstellungseinheit“ eine Signaturerstellungseinheit, die die Anforderungen des Anhangs III erfüllt;
7. „Signaturprüfdaten“ Daten wie Codes oder öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden;
8. „Signaturprüfeinheit“ eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturprüfdaten verwendet wird;
9. „Zertifikat“ eine elektronische Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und die Identität dieser Person bestätigt wird;
10. „qualifiziertes Zertifikat“ ein Zertifikat, das die Anforderungen des Anhangs I erfüllt und von einem Zertifizierungsdiensteanbieter bereitgestellt wird, der die Anforderungen des Anhangs II erfüllt;
11. „Zertifizierungsdiensteanbieter“ eine Stelle oder eine juristische oder natürliche Person, die Zertifikate ausstellt oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellt;
12. „Produkt für elektronische Signaturen“ Hard- oder Software bzw. deren spezifische Komponenten, die von einem Zertifizierungsdiensteanbieter für die Bereitstellung von Diensten für elektronische Signaturen verwendet werden sollen oder die für die Erstellung und Überprüfung elektronischer Signaturen verwendet werden sollen;
13. „freiwillige Akkreditierung“ eine Erlaubnis, mit der die Rechte und Pflichten für die Erbringung von Zertifizierungsdiensten festgelegt werden und die auf Antrag des betreffenden Zertifizierungsdiensteanbieters von der öffentlichen oder privaten Stelle, die für die Festlegung dieser Rechte und Pflichten sowie für die Überwachung ihrer Einhaltung zuständig ist, erteilt wird, wenn der Zertifizierungsdiensteanbieter die sich aus der Erlaubnis ergebenden Rechte nicht ausüben darf, bevor er den Bescheid der Stelle erhalten hat.

[1] ABl. L 184 vom 17.7.1999, S. 23.

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 die Steigerung des Niveaus der erbrachten Zertifizierungsdienste abzielen. Alle mit diesen Systemen verknüpften Anforderungen müssen objektiv, transparent, verhältnismäßig und nichtdiskriminierend sein. Die Mitgliedstaaten dürfen die Zahl der akkreditierten Zertifizierungsdiensteanbieter nicht aus Gründen einschränken, die in den Geltungsbereich dieser Richtlinie fallen.

(3) Die Mitgliedstaaten tragen dafür Sorge, daß ein geeignetes System zur Überwachung der in ihrem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter, die öffentlich qualifizierte Zertifikate ausstellen, eingerichtet wird.

(4) Die Übereinstimmung sicherer Signaturerstellungseinheiten mit den Anforderungen nach Anhang III wird von geeigneten öffentlichen oder privaten Stellen festgestellt, die von den Mitgliedstaaten benannt werden. Die Kommission legt nach dem Verfahren des Artikels 9 Kriterien fest, anhand deren die Mitgliedstaaten bestimmen, ob eine Stelle zur Benennung geeignet ist.

Die von den in Unterabsatz 1 genannten Stellen vorgenommene Feststellung der Übereinstimmung mit den Anforderungen des Anhangs III wird von allen Mitgliedstaaten anerkannt.

(5) Die Kommission kann nach dem Verfahren des Artikels 9 Referenznummern für allgemein anerkannte Normen für Produkte für elektronische Signaturen festlegen und im *Amtsblatt der Europäischen Gemeinschaften* veröffentlichen. Die Mitgliedstaaten gehen davon aus, daß die Anforderungen nach Anhang II Buchstabe f) und Anhang III erfüllt sind, wenn ein Produkt für elektronische Signaturen diesen Normen entspricht.

(6) Die Mitgliedstaaten und die Kommission arbeiten unter Berücksichtigung der Empfehlungen für die sichere Signaturprüfung in Anhang IV und im Interesse des Verbrauchers zusammen, um die Entwicklung und die Nutzung von Signaturprüfeinheiten zu fördern.

(7) Die Mitgliedstaaten können den Einsatz elektronischer Signaturen im öffentlichen Bereich möglichen zusätzlichen Anforderungen unterwerfen. Diese Anforderungen müssen objektiv, transparent, verhältnismäßig und nichtdiskriminierend sein und dürfen sich nur auf die spezifischen Merkmale der betreffenden Anwendung beziehen. Diese Anforderungen dürfen für grenzüberschreitende Dienste für den Bürger kein Hindernis darstellen.

Artikel 4

Binnenmarktgrundsätze

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

(2) Die Mitgliedstaaten tragen dafür Sorge, daß Produkte für elektronische Signaturen, die den Anforderungen dieser Richtlinie entsprechen, frei im Binnenmarkt verkehren können.

Artikel 5

Rechtswirkung elektronischer Signaturen

(1) Die Mitgliedstaaten tragen dafür Sorge, daß fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und die von einer sicheren Signaturerstellungseinheit erstellt werden,

a) die rechtlichen Anforderungen an eine Unterschrift in bezug auf in elektronischer Form vorliegende Daten in gleicher Weise erfüllen wie handschriftliche Unterschriften in bezug auf Daten, die auf Papier vorliegen, und

b) in Gerichtsverfahren als Beweismittel zugelassen sind.

(2) Die Mitgliedstaaten tragen dafür Sorge, daß einer elektronischen Signatur die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen wird,

— weil sie in elektronischer Form vorliegt oder

— nicht auf einem qualifizierten Zertifikat beruht oder

— nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder

— nicht von einer sicheren Signaturerstellungseinheit erstellt wurde.

Artikel 6

Haftung

(1) Die Mitgliedstaaten gewährleisten als Mindestregelung, daß ein Zertifizierungsdiensteanbieter, der ein Zertifikat als qualifiziertes Zertifikat öffentlich ausstellt oder für ein derartiges Zertifikat öffentlich einsteht, in bezug auf Schäden gegenüber einer Stelle oder einer juristischen oder natürlichen Person, die vernünftigerweise auf das Zertifikat vertraut, dafür haftet, daß

a) alle Informationen in dem qualifizierten Zertifikat zum Zeitpunkt seiner Ausstellung richtig sind und das Zertifikat alle für ein qualifiziertes Zertifikat vorgeschriebenen Angaben enthält,

b) der in dem qualifizierten Zertifikat angegebene Unterzeichner zum Zeitpunkt der Ausstellung des Zertifikats im Besitz der Signaturerstellungsdaten war, die den im Zertifikat angegebenen bzw. identifizierten Signaturprüfdaten entsprechen,

c) in Fällen, in denen der Zertifizierungsdiensteanbieter sowohl die Signaturerstellungsdaten als auch die Signaturprüfdaten erzeugt, beide Komponenten in komplementärer Weise genutzt werden können,

es sei denn, der Zertifizierungsdiensteanbieter weist nach, daß er nicht fahrlässig gehandelt hat.

(2) Die Mitgliedstaaten gewährleisten als Mindestregelung, daß ein Zertifizierungsdiensteanbieter, der ein Zertifikat als qualifiziertes Zertifikat öffentlich ausgestellt hat, in bezug auf Schäden gegenüber einer Stelle oder einer juristischen oder natürlichen Person, die vernünftigerweise auf das Zertifikat vertraut, für den Fall haftet, daß der Widerruf des Zertifikats nicht registriert worden ist, es sei denn, der Zertifizierungsdiensteanbieter weist nach, daß er nicht fahrlässig gehandelt hat.

(3) Die Mitgliedstaaten tragen dafür Sorge, daß Zertifizierungsdiensteanbieter in einem qualifizierten Zertifikat Beschränkungen für die Verwendung des Zertifikates angeben können; diese Beschränkungen müssen für Dritte erkennbar sein. Der Zertifizierungsdiensteanbieter haftet nicht für Schäden, die sich aus einer über diese Beschränkungen hinausgehenden Verwendung des qualifizierten Zertifikats ergeben.

(4) Die Mitgliedstaaten tragen dafür Sorge, daß Zertifizierungsdiensteanbieter in dem qualifizierten Zertifikat eine Grenze für den Wert der Transaktionen angeben können, für die das Zertifikat verwendet werden kann; diese Grenze muß für Dritte erkennbar sein.

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 vom 5. April 1993 über mißbräuchliche Klauseln in Verbraucherverträgen [1].

Artikel 7

Internationale Aspekte

(1) Die Mitgliedstaaten tragen dafür Sorge, daß Zertifikate, die von einem Zertifizierungsdiensteanbieter eines Drittlandes öffentlich als qualifizierte Zertifikate ausgestellt werden, den von einem in der Gemeinschaft niedergelassenen Zertifizierungsdiensteanbieter ausgestellten Zertifikaten rechtlich gleichgestellt werden, wenn

a) der Zertifizierungsdiensteanbieter die Anforderungen dieser Richtlinie erfüllt und im Rahmen eines freiwilligen Akkreditierungssystems eines Mitgliedstaats akkreditiert ist oder

b) ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen dieser Richtlinie erfüllt, für das Zertifikat einsteht 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) Um grenzüberschreitende Zertifizierungsdienste mit Drittländern und die rechtliche Anerkennung fortgeschrittener elektronischer Signaturen, die aus Drittländern stammen, zu erleichtern, unterbreitet die Kommission gegebenenfalls Vorschläge mit dem Ziel, die effiziente Umsetzung von Normen und internationalen Vereinbarungen über Zertifizierungsdienste zu erreichen. Insbesondere unterbreitet sie dem Rat bei Bedarf Vorschläge zur Erteilung von geeigneten Mandaten zur Aushandlung bilateraler und multilateraler Vereinbarungen mit Drittländern und internationalen Organisationen. Der Rat beschließt mit qualifizierter Mehrheit.

(3) Wird die Kommission über Schwierigkeiten unterrichtet, auf die Unternehmen der Gemeinschaft beim Marktzugang in Drittländern stoßen, so kann sie erforderlichenfalls dem Rat Vorschläge für ein geeignetes Mandat zur Aushandlung vergleichbarer Rechte für Unternehmen der Gemeinschaft in diesen Drittländern vorlegen. Der Rat beschließt mit qualifizierter Mehrheit.

Die gemäß diesem Absatz ergriffenen Maßnahmen lassen die Verpflichtungen der Gemeinschaft und der Mitgliedstaaten im Rahmen der einschlägigen internationalen Übereinkünfte unberührt.

Artikel 8

Datenschutz

(1) Die Mitgliedstaaten tragen dafür Sorge, daß Zertifizierungsdiensteanbieter und die für die Akkreditierung und Aufsicht zuständigen nationalen Stellen die Anforderungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [2] erfüllen.

(2) Die Mitgliedstaaten tragen dafür Sorge, daß Zertifizierungsdiensteanbieter, die öffentlich Zertifikate ausstellen, personenbezogene Daten nur unmittelbar von der betroffenen Person oder mit ausdrücklicher Zustimmung der betroffenen Person und nur insoweit einholen können, als dies zur Ausstellung und Aufrechterhaltung des Zertifikats erforderlich ist. Die Daten dürfen ohne ausdrückliche Zustimmung der betroffenen Person nicht für anderweitige Zwecke erfaßt oder verarbeitet werden.

(3) Unbeschadet der Rechtswirkungen, die Pseudonyme nach einzelstaatlichem Recht haben, hindern die Mitgliedstaaten Zertifizierungsdiensteanbieter nicht daran, im Zertifikat ein Pseudonym anstelle des Namens des Unterzeichners anzugeben.

Artikel 9

Ausschuß

(1) Die Kommission wird von einem „Ausschuß für elektronische Signaturen“ (im folgenden „Ausschuß“ genannt) unterstützt.

(2) Bei einer Bezugnahme auf diesen Absatz finden die Artikel 4 und 7 des Beschlusses 1999/468/EG Anwendung, wobei Artikel 8 desselben Beschlusses zu beachten ist.

Der Zeitraum nach Artikel 4 Absatz 3 des Beschlusses 1999/468/EG wird auf drei Monate festgesetzt.

(3) Der Ausschuß gibt sich eine Geschäftsordnung.

Artikel 10

Aufgaben des Ausschusses

Der Ausschuß präzisiert die in den Anhängen festgelegten Anforderungen, die Kriterien nach Artikel 3 Absatz 4 und die allgemein anerkannten Normen für Produkte für elektronische Signaturen, die gemäß Artikel 3 Absatz 5 festgelegt und veröffentlicht werden, nach dem Verfahren des Artikels 9 Absatz 2.

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

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

Artikel 11

Notifizierung

(1) Die Mitgliedstaaten übermitteln der Kommission und den übrigen Mitgliedstaaten folgende Informationen:

a) Angaben zu nationalen freiwilligen Akkreditierungssystemen einschließlich zusätzlicher Anforderungen gemäß Artikel 3 Absatz 7,

b) Namen und Anschriften der für Akkreditierung und Aufsicht zuständigen nationalen Stellen und der in Artikel 3 Absatz 4 genannten Stellen sowie

c) Namen und Anschriften aller akkreditierten nationalen Zertifizierungsdiensteanbieter.

(2) Die Informationen gemäß Absatz 1 und diesbezügliche Änderungen sind von den Mitgliedstaaten so bald wie möglich zu übermitteln.

Artikel 12

Überprüfung

(1) Die Kommission überprüft die Durchführung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat spätestens zum 19. Juli 2003 darüber Bericht.

(2) Bei der Überprüfung ist unter anderem festzustellen, ob der Anwendungsbereich dieser Richtlinie angesichts der technologischen und rechtlichen Entwicklungen und der Marktentwicklung geändert werden sollte. Der Bericht umfaßt insbesondere eine Bewertung der Harmonisierungsaspekte auf der Grundlage der gesammelten Erfahrungen. Gegebenenfalls sind dem Bericht Vorschläge für Rechtsvorschriften beizufügen.

Artikel 13

Durchführung

(1) Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie vor dem 19. Juli 2001 nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Wenn die Mitgliedstaaten diese Vorschriften erlassen, nehmen sie 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 den Wortlaut der wichtigsten innerstaatlichen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 14

Inkrafttreten

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

Artikel 15

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am 13. Dezember 1999.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*
N. FONTAINE	S. HASSI

ANHANG I

Anforderungen an qualifizierte Zertifikate

Qualifizierte Zertifikate müssen folgende Angaben enthalten:

a) Angabe, daß das Zertifikat als qualifiziertes Zertifikat ausgestellt wird;

b) Angabe des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist;

c) Name des Unterzeichners oder ein Pseudonym, das als solches zu identifizieren ist;

d) Platz für ein spezifisches Attribut des Unterzeichners, das gegebenenfalls je nach Bestimmungszweck des Zertifikats aufgenommen wird;

e) Signaturprüfdaten, die den vom Unterzeichner kontrollierten Signaturerstellungsdaten entsprechen;

f) Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikats;

g) Identitätscode des Zertifikats;

h) die fortgeschrittene elektronische Signatur des ausstellenden Zertifizierungsdiensteanbieters;

i) gegebenenfalls Beschränkungen des Geltungsbereichs des Zertifikats und

j) gegebenenfalls Begrenzungen des Wertes der Transaktionen, für die das Zertifikat verwendet werden kann.

ANHANG II

Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen

Zertifizierungsdiensteanbieter

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

b) müssen den Betrieb eines schnellen und sicheren Verzeichnisdienstes und eines sicheren und unverzüglichen Widerrufsdienstes gewährleisten;

c) müssen gewährleisten, daß Datum und Uhrzeit der Ausstellung oder des Widerrufs eines Zertifikats genau bestimmt werden können;

d) müssen mit geeigneten Mitteln nach einzelstaatlichem Recht die Identität und gegebenenfalls die spezifischen Attribute der Person überprüfen, für die ein qualifiziertes Zertifikat ausgestellt wird;

e) müssen Personal mit den für die angebotenen Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen beschäftigen; dazu gehören insbesondere Managementkompetenzen, Kenntnisse der Technologie elektronischer Signaturen und Vertrautheit mit angemessenen Sicherheitsverfahren; sie müssen ferner geeignete Verwaltungs- und Managementverfahren einhalten, die anerkannten Normen entsprechen;

f) müssen vertrauenswürdige Systeme und Produkte einsetzen, die vor Veränderungen geschützt sind und die die technische und kryptographische Sicherheit der von ihnen unterstützten Verfahren gewährleisten;

g) müssen Maßnahmen gegen Fälschungen von Zertifikaten ergreifen und in den Fällen, in denen sie Signaturerstellungsdaten erzeugen, die Vertraulichkeit während der Erzeugung dieser Daten gewährleisten;

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

i) 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;

j) dürfen keine Signaturerstellungdaten von Personen speichern oder kopieren, denen Schlüsselmanagementdienste angeboten werden;

k) müssen, bevor sie in Vertragsbeziehungen mit einer Person eintreten, die von ihnen ein Zertifikat zur Unterstützung ihrer elektronischen Signatur wünscht, diese Person mit einem dauerhaften Kommunikationsmittel über die genauen Bedingungen für die Verwendung des Zertifikats informieren, wozu unter anderem Nutzungsbeschränkungen für das Zertifikat, die Existenz eines freiwilligen Akkreditierungssystems und das Vorgehen in Beschwerde- und Schlichtungsverfahren gehören. Diese Angaben müssen schriftlich — gegebenenfalls elektronisch übermittelt — in klar verständlicher Sprache vorliegen. Wichtige Teilinformationen werden auf Antrag auch Dritten zur Verfügung gestellt, die auf das Zertifikat vertrauen;

l) müssen vertrauenswürdige Systeme für die Speicherung von Zertifikaten in einer überprüfbaren Form verwenden, so daß

— nur befugte Personen Daten eingeben und ändern können;

— die Angaben auf ihre Echtheit hin überprüft werden können;

— Zertifikate nur in den Fällen öffentlich abrufbar sind, für die die Zustimmung des Inhabers des Zertifikats eingeholt wurde;

— technische Veränderungen, die die Einhaltung dieser Sicherheitsanforderungen beeinträchtigen, für den Betreiber klar ersichtlich sind.

ANHANG III

Anforderungen an sichere Signaturerstellungseinheiten

1. Sichere Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, daß
   a) die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten praktisch nur einmal auftreten können und daß ihre Geheimhaltung hinreichend gewährleistet ist;
   b) die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die Signatur vor Fälschungen bei Verwendung der jeweils verfügbaren Technologie geschützt ist;
   c) die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten von dem rechtmäßigen Unterzeichner vor der Verwendung durch andere verläßlich geschützt werden können.
2. Sichere Signaturerstellungseinheiten verändern die zu unterzeichnenden Daten nicht und verhindern nicht, daß diese Daten dem Unterzeichner vor dem Signaturvorgang dargestellt werden.

ANHANG IV

Empfehlungen für die sichere Signaturprüfung

Während des Signaturprüfungsvorgangs ist mit hinreichender Sicherheit zu gewährleisten, daß

a) die zur Überprüfung der Signatur verwendeten Daten den Daten entsprechen, die dem Überprüfer angezeigt werden,
b) die Signatur zuverlässig überprüft wird und das Ergebnis dieser Überprüfung korrekt angezeigt wird,
c) der Überprüfer bei Bedarf den Inhalt der unterzeichneten Daten zuverlässig feststellen kann,
d) die Echtheit und die Gültigkeit des zum Zeitpunkt der Überprüfung der Signatur verlangten Zertifikats zuverlässig überprüft werden,
e) das Ergebnis der Überprüfung sowie die Identität des Unterzeichners korrekt angezeigt werden,
f) die Verwendung eines Pseudonyms eindeutig angegeben wird, und
g) sicherheitsrelevante Veränderungen erkannt werden können.