EUROPÄISCHE KOMMISSION

KOM(1998)297end

13.05.98

MITTEILUNG DER KOMMISSION AN DEN RAT, DAS EUROPÄISCHE PARLAMENT, DEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

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

(Text von Bedeutung für den EWR)

BEGRÜNDUNG

I. VORGESCHICHTE

Offene Netze wie das Internet gewinnen für die weltweite Kommunikation immer mehr an Bedeutung. Sie ermöglichen die interaktive Kommunikation zwischen Parteien, die vorher in keiner Beziehung zueinander standen. Darüber hinaus ermöglichen sie das Schaffen neuer Geschäftszweige, neuer Methoden zur Produktivitätssteigerung und Kostensenkung sowie neuer Möglichkeiten, Kunden zu erreichen. Netze werden von Unternehmen in Anspruch genommen, die von neuen Arbeitsformen wie Telearbeit und gemeinsam genutzten virtuellen Umgebungen profitieren möchten. Auch Behörden bedienen sich ihrer bei ihrem Dialog mit Unternehmen und Bürgern. Der elektronische Geschäftsverkehr bietet der Europäischen Union eine ausgezeichnete Chance, ihre wirtschaftliche Integration voranzutreiben.

Um diese Möglichkeiten sinnvoll zu nutzen, bedarf es eines sicheren Rahmens für die elektronische Authentifizierung. Es gibt verschiedene Methoden zur elektronischen Unterzeichnung von Dokumenten, angefangen von einfachen Methoden (z.B. durch Einfügung einer mit Scanner eingelesenen handschriftlichen Unterschrift in ein Textverarbeitungsdokument) bis hin zu sehr fortschrittlichen Methoden (z.B. digitale Signaturen auf der Basis kryptographischer Systeme mit öffentlich bekanntem Schlüssel). Elektronische Signaturen ermöglichen dem Empfänger elektronischer versendeter Daten die Herkunft der Daten zu überprüfen (*Authentizität des Ursprungs der Daten*) und festzustellen, ob die Daten vollständig und unverändert sind (*Integrität der Daten*).

Die Überprüfung der Authentizität und Integrität der Daten beweisen nicht notwendigerweise die Identität des Unterzeichners, der die elektronische Signatur erstellt. Wie kann z.B. der Empfänger einer Nachricht feststellen, ob der Sender wirklich derjenige ist, für den er sich ausgibt? Der Empfänger möchte deshalb zuverlässigere Informationen über die Identität des Unterzeichners haben. Solche Informationen kann zunächst der Unterzeichner selbst liefern, indem er dem Empfänger mit ausreichenden Nachweisen versorgt. Eine andere Möglichkeit ist die Bestätigung durch eine dritte Stelle (z.B. eine Person oder Einrichtung der beide Seiten vertrauen). Im Zusammenhang mit dieser Richtlinie werden solche dritten Stellen als *Zertifizierungsdiensteanbieter* bezeichnet.

In der Mitteilung vom 16. April 1997 an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen über eine „Europäische Initiative für den elektronischen Geschäftsverkehr"[1] betrachtete die Kommission digitale Signaturen als wesentliches Element zur Gewährleistung der Sicherheit und des Vertrauens in offene Netze. Auch in der Bonner Ministererklärung[2] wurde auf die zentrale Bedeutung der digitalen Signatur für den elektronischen Geschäftsverkehr hingewiesen.

In einem ersten Schritt unterbreitete 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

---

1 KOM (97) 157 endgültig vom 16.04.1997

2 Europäische Ministerkonferenz zum Thema "Globale Informationsnetze: Nutzung neuer Chancen", Bonn 6.-8.07.1997

europäischer Rahmen für digitale Signaturen und Verschlüsselung"[3], in der sie auf den Bedarf an einem kohärenten Konzept für diesen Bereich hinwies. Am 1. Dezember 1997 begrüßte der Rat die Mitteilung und forderte die Kommission auf, so bald wie möglich einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über digitale Signaturen vorzulegen.

Im Anschluß an die Veröffentlichung der Mitteilung und als Ergebnis von Gesprächen mit den Mitgliedstaaten und Vertretern des Privatsektors, insbesondere der europäischen kryptographischen Industrie, sowie im Rahmen der internationalen Expertenanhörung in Kopenhagen[4] erhielt die Kommission Anregungen von den beteiligten Parteien. Daraus lassen sich folgende Schlüsse ziehen:

1. Die zunehmenden Rechtsetzungstätigkeiten in verschiedenen Mitgliedstaaten erfordern dringend harmonisierte Rahmenbedingungen auf europäischer Ebene, um ernsthafte Hindernisse für das Funktionieren des Binnenmarktes zu vermeiden.

2. Es wird zwar viel über Technologien für digitale Signaturen, die ein sog. kryptographisches System mit öffentlich bekanntem Schlüssel verwenden, diskutiert und intensiv daran gearbeitet, jedoch sollte eine europäische Richtlinie technologieunabhängig sein und sich nicht auf Signaturen dieser Art beschränken. Da mit einer Vielzahl von Authentifizierungsverfahren zu rechnen ist, sollte der Geltungsbereich der Richtlinie weit genug gefaßt sein, um ein ganzes Spektrum „elektronischer Signaturen" abzudecken, welches sowohl digitale Signaturen auf der Basis kryptographischer Systeme mit öffentlich bekanntem Schlüssel als auch Authentifizierungsverfahren anderer Art umfaßt.

3. Um das Funktionieren des Binnenmarktes zu gewährleisten und die rasche Marktentwicklung im Hinblick auf Nachfrage und technologische Innovation zu unterstützen, sind Verfahren, die die vorherige Erteilung einer Genehmigung voraussetzen, zu vermeiden. Um das Vertrauen der Verbraucher zu gewinnen, werden freiwillige Akkreditierungssysteme für solche Zertifizierungsdiensteanbieter für sinnvoll gehalten, die ein höheres Sicherheitsniveau anstreben. Soweit solche Maßnahmen vom Markt gefordert werden, könnten sie zu einem höheren Maß an rechtlicher Sicherheit für Zertifizierungsdiensteanbieter und Verbraucher beitragen.

4. Elektronische Signaturen, die in geschlossenen Systemen verwendet werden, in denen zum Beispiel bereits vertragliche Beziehungen bestehen, sollten nicht automatisch in den Geltungsbereich dieser Richtlinie fallen. Hier sollte die Vertragsfreiheit vorherrschen.

5. Die Sicherstellung der - insbesondere grenzüberschreitenden - rechtlichen Anerkennung elektronischer Signaturen und von Zertifizierungsdiensten gilt als die wichtigste Aufgabe in diesem Bereich. Hierfür sind die wesentlichen Anforderungen an Zertfizierungsdiensteanbieter sowie Haftungsfragen zu klären.

6. Es ist davon auszugehen, daß die Industrie in Zusammenarbeit mit Normungsgremien die Vorreiterrolle bei der Entwicklung international abgestimmter Normen für elektronische Signaturen übernehmen wird. Dabei sollte der Schwerpunkt auf der

---

3 KOM (97) 503 endgültig vom 08.10.97;

4 Internationale öffentliche Anhörung, Kopenhagen, 23-24.04.1998

Schaffung einer offenen Umgebung für interoperable Produkte und Dienste liegen. Die Kommission wird diesen Prozeß unterstützen.

7. Auf internationaler Ebene gibt es zahlreiche Aktivitäten und Diskussionen. Die UN-Kommission für internationales Handelsrecht (UNCITRAL) hat ein Modellgesetz für den elektronischen Geschäftsverkehr beschlossen und, darauf basierend, Arbeiten zur Entwicklung einheitlicher Regeln für digitale Signaturen aufgenommen. Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ist ebenfalls in diesem Bereich aktiv und stützt sich dabei auf die Leitlinien für die Kryptographiepolitik von 1997. Weitere internationale Organisationen, darunter die Welthandelsorganisation (WTO), befassen sich ebenfalls mit diesen Themen. Diese laufenden Entwicklungen sind bei der Einführung rechtlicher Rahmenbedingungen auf europäischer Ebene zu berücksichtigen.

II. BEDARF AN HARMONISIERUNG

Mehrere Mitgliedstaaten haben bereits detaillierte Gesetzgebungsmaßnahmen im Bereich elektronischer Signaturen eingeleitet:

Mitgliedstaat	Stand der Gesetzgebungsmaßnahmen
Österreich	Vorarbeiten
Belgien	• Telekommunikationsrecht: freiwilliges System mit vorheriger Anzeige für Diensteanbieter • Gesetzentwurf zu Zertifizierungsdiensten für digitale Signaturen • Gesetzentwurf zur Änderung des Bürgerlichen Gesetzbuchs in bezug auf elektronische Beweismittel • Gesetzentwurf zum Einsatz digitaler Signaturen in der Sozialversicherung und im öffentlichen Gesundheitswesen
Dänemark	• Gesetzentwurf zur sicheren und effizienten Nutzung der digitalen Kommunikation
Frankreich	• Telekommunikationsrecht (Erlasse über Genehmigungen und Ausnahmen): ⇒ Bereitstellung elektronischer Signaturprodukte und -dienste auf der Grundlage eines Anzeigeverfahrens ⇒ Ungehinderte Nutzung und Ein-/Ausfuhr elektronischer Signaturprodukte und –dienste • Gesetz über den Einsatz digitaler Signaturen in der Sozialversicherung und im öffentlichen Gesundheitswesen
Finnland	• Gesetzentwurf zum elektronischen Informationsaustausch in Verwaltungen und verwaltungsgerichtlichen Verfahren • Gesetzentwurf zum Status des zentralen Bevölkerungsregisters als Zertifizierungsdiensteanbieter
Deutschland	• Gesetz und Verordnung über digitale Signaturen in Kraft: Bedingungen, unter denen digitale Signaturen als sicher zu betrachten sind; freiwillige Akkreditierung von Diensteanbietern

	• Entwurf eines Katalogs geeigneter Sicherheitsmaßnahmen • Öffentliche Anhörung zu rechtlichen Aspekten digitaler Signaturen und digital signierter elektronischer Dokumente
Italien	• Allgemeines Gesetz zur Reform des öffentlichen Dienstes und zur Vereinfachung der Verwaltungsverfahrens in Kraft: Grundsatz der rechtlichen Anerkennung elektronischer Dokumente • Erlaß zur Erstellung, Archivierung und Übertragung elektronischer Dokumente und Verträge • Erlaß über die Anforderungen an Produkte und Dienste in Vorbereitung • Erlaß über die steuerlichen Verpflichtungen im Zusammenhang mit elektronischen Dokumenten in Vorbereitung
Niederlande	• Freiwilliges Akkreditierungssystem für Diensteanbieter in Vorbereitung • Steuergesetz, das die elektronische Erfassung von Einkommens-steuererklärungen vorsieht • Gesetzentwurf zur Änderung des Bürgerlichen Gesetzbuchs in Vorbereitung
Spanien	• Rundschreiben der Zollbehörde über den Einsatz digitaler Signaturen • Entschließung zum Einsatz elektronischer Mittel im Bereich der sozialen Sicherheit • Gesetze und Rundschreiben zu den Themen Hypotheken, Steuern, Finanzdienste und Registrierung von Unternehmen, in welchen der Einsatz elektronischer Verfahren gestattet wird • Haushaltsgesetz 1998, mit dem die Münzprägeanstalt ermächtigt wird, als Zertifizierungsdiensteanbieter aufzutreten
Schweden	Vorarbeiten
Vereinigtes Königreich	Gesetzentwurf über die freiwillige Lizenzierung von Zertifizierungsdiensteanbietern und die rechtliche Anerkennung elektronischer Signaturen

Wie diese Übersicht zeigt, führen die verschiedenen Initiativen der Mitgliedstaaten zu unterschiedlichen Rechtslagen. Zwar scheinen sich die Mitgliedstaaten auf dieselben Konzepte zu konzentrieren, insbesondere auf die Anforderungen an Diensteanbieter und Produkte, die Bedingungen, unter denen elektronische Signaturen rechtliche Wirkung entfalten und auf die Struktur von Akkreditierungssystemen; es wird aber deutlich, daß es aufgrund der entsprechenden Vorschriften, bzw. aufgrund des Mangels an solchen Vorschriften, zu stark voneinander abweichenden Rechtslagen kommen wird. Dies hat zur Folge, daß das Funktionieren des Binnenmarktes im Bereich der elektronischen Signaturen gefährdet ist. Divergierende Regeln hinsichtlich der rechtlichen Wirkung elektronischer Signaturen sind vor allem für die Weiterentwicklung des elektronischen Geschäftsverkehrs und damit für das Wirtschaftswachstum und die Beschäftigung in der Gemeinschaft von Nachteil. Ein weiterer Unsicherheitsfaktor ergibt sich aus den unterschiedlichen Haftungsregelungen und der drohenden rechtlichen Unsicherheit bei der Haftung im Bereich grenzüberschreitender Dienste. Auch hat es den Anschein, als ob die Mitgliedstaaten in unterschiedlicher Weise festlegen werden, unter welchen technischen Voraussetzungen elektronische Signaturen als sicher angesehen werden.

Diese uneinheitliche Entwicklung kann ein ernsthaftes Hindernis für die Kommunikation und den Geschäftsverkehr über offene Netze in der Europäischen Gemeinschaft darstellen, da sie die ungehinderte Nutzung und Bereitstellung digitaler Signaturdienste sowie die Entwicklung neuer wirtschaftlicher Tätigkeiten im Bereich des elektronischen Geschäftsverkehrs hemmen. Ziel des Richtlinienvorschlages ist es, Hindernisse zu beseitigen, insbesondere Unterschiede bei der rechtlichen Anerkennung elektronischer Signaturen sowie Beschränkungen des freien Verkehrs von Zertifizierungsdiensten und -produkten zwischen den Mitgliedstaaten. Unter Maßgabe dieser Zielvorgaben fällt die geplante Maßnahme in den ausschließlichen Zuständigkeitsbereich der Kommission. Der Vorschlag zielt auf die "Ermöglichung" des Einsatzes elektronischer Signaturen innerhalb eines Gebietes ohne interne Schranken, indem er sich auf die wesentlichen Anforderungen für Zertifizierungsdienste beschränkt und die detaillierten Durchführungsvorschriften den Mitgliedstaaten überläßt. Er stimmt mit der Rechtspolitik der Kommission im Bereich der Subsidiarität, Proportionalität und Vereinfachung überein.

Daher schlägt die Kommission Artikel 57 Absatz 2, Artikel 66 und 100 a als Rechtsgrundlage für diese Richtlinie vor. Aus Gründen der Verhältnismäßigkeit hält sie eine Richtlinie für die angemessene Form des Rechtsinstruments.

III. ZIEL UND GELTUNGSBEREICH DER MITTEILUNG

1. Mit dieser Richtlinie soll das reibungslose Funktionieren des Binnenmarktes im Bereich elektronischer Signaturen gewährleistet werden. Hierzu sind angemessene harmonisierte rechtliche Rahmenbedingungen für den Einsatz elektronischer Signaturen in der Europäischen Gemeinschaft zu schaffen und Kriterien festzulegen, die die Grundlage für die rechtliche Anerkennung elektronischer Signaturen darstellen.

2. Weltweite elektronische Kommunikation und weltweiter elektronischer Geschäftsverkehr sind auf die schrittweise Anpassung des internationalen und einzelstaatlichen Rechts an die sich rasch entwickelnde technologische Infrastruktur angewiesen. Obwohl in einigen Fällen Analogien zu bestehenden Regeln zu zufriedenstellenden Lösungen führen können, sind aufgrund der neuen Technologien Anpassungen dieser bestehenden Regeln unerläßlich, um unerwünschte Auswirkungen zu vermeiden. Die auf der Grundlage kryptographischer Technologien erstellten digitalen Signaturen gelten zwar derzeit als eine wichtige Form der elektronischen Signatur; europäische ordnungspolitische Rahmenbedingungen müssen jedoch flexibel genug sein, um auch andere Techniken der Authentifizierung zu umfassen.

3. Die Technik der digitalen Signatur wird bereits vielfach in geschlossenen Umgebungen eingesetzt, z.B. dem lokalen Netz eines Unternehmens oder einem Banksystem. Zertifikate und elektronische Signaturen werden auch für Zugangskontrollen verwendet, z.B. für den Zugang zu einem Privatkonto. Der Grundsatz der Vertragsfreiheit gestattet es den Parteien, auf der Grundlage der nationalen Rechtsvorschriften, die Bedingungen für ihre Geschäftstätigkeit, z.B. die Akzeptanz elektronischer Signaturen, frei zu vereinbaren. In diesen Bereichen bedarf es nicht unbedingt gesetzgeberischer Maßnahmen.

4. Angesichts des breiten Spektrums von Diensten und ihrer möglichen Anwendungen sollten Anbieter von Zertifizierungsdiensten diese ohne vorherige Genehmigung bereitstellen können. Diensteanbieter möchten sich jedoch möglicherweise freiwillig einem Akkreditierungssystem unterwerfen, welches sich auf gemeinsame Anforderungen stützt, um von den Vorteilen rechtsgültiger elektronischer Signaturen zu profitieren. Die

Akkreditierung sollte als öffentliches Serviceangebot für Zertifizierungsdiensteanbieter, die hochwertige Dienste anbieten möchten, verstanden werden. Auf keinen Fall sollte es aber bedeuten, daß nicht-akkreditierte Dienste zwangsläufig weniger sicher sind.

5. Ein Zertifizierungsdiensteanbieter kann eine breite Palette unterschiedlicher Dienste anbieten. Der Schwerpunkt der vorliegenden Richtlinie liegt auf Zertifizierungsdiensten im Zusammenhang mit elektronischen Signaturen. Zertifikate können einer Vielzahl von Zwecken dienen und verschiedene Informationen enthalten. Dazu können herkömmliche Angaben wie Name, Anschrift, Registrier-, Sozialversicherungs- oder (Mehrwert-) Steuernummer gehören, aber auch spezifische Eigenschaften des Unterzeichners, z.B. seine Ermächtigung, im Namen eines Unternehmens zu handeln, seine Kreditwürdigkeit, Zahlungssicherheiten oder der Besitz spezieller Genehmigungen und Lizenzen. Daher ist eine Vielzahl von Zertifikaten für verschiedene Zwecke denkbar. Ein rechtlicher Rahmen ist vor allem dazu erforderlich, um die Authentifizierung der elektronischen Signatur eines Unterzeichners zu ermöglichen. Die vorliegende Richtlinie konzentriert sich daher auf die Funktion eines Zertifikats (eines sog. „qualifizierten Zertifikats") zum Nachweis der zivilen Identität oder Funktion einer Person.

6. Die rechtliche Wirkung elektronischer Signaturen ist ein zentraler Faktor in einem offenen, aber vertrauenswürdigen System. Die Anwendung dieser Richtlinie soll auch dadurch zu harmonisierten rechtlichen Rahmenbedingungen in der Gemeinschaft beitragen, daß gewährleistet wird, daß einer elektronischen Signatur nicht die Rechtsgültigkeit, Rechtswirkung oder Durchsetzbarkeit mit der Begründung abgesprochen werden kann, daß die Signatur in elektronischer Form vorliegt, nicht auf einem qualifizierten oder nicht auf einem von einem akkreditierten Diensteanbieter ausgestellten Zertifikat basiert. Ferner ist sicherzustellen, daß elektronische Signaturen in gleicher Weise wie handschriftliche Signaturen rechtlich anerkannt werden. In den nationalen Beweisvorschriften sollten elektronische Signaturen ebenfalls anerkannt werden.

7. Die rechtliche Anerkennung elektronischer Signaturen sollte auf objektiven, transparenten, nichtdiskriminierenden und verhältnismäßigen Kriterien basieren und nicht mit einer Genehmigung oder Akkreditierung des betreffenden Diensteanbieters verknüpft sein. Gemeinsame Anforderungen an Zertifizierungsdiensteanbieter könnten die grenzüberschreitende Anerkennung von Signaturen und Zertifikaten innerhalb der Europäischen Gemeinschaft unterstützen. Der Anforderungskatalog für Zertifizierungs-diensteanbieter ist unabhängig vom konkreten Akkreditierungssystem der einzelnen Mitgliedstaaten anwendbar. Da die künftige technologische und marktwirtschaftliche Entwicklung gegebenenfalls Anpassungen erforderlich macht, sind die Anforderungen von Zeit zu Zeit zu überprüfen. Die Kommission kann aufgrund künftiger Erfahrungen revidierte Anforderungskataloge vorschlagen.

8. Gemeinsame Haftungsregelungen würden die Vertrauensbasis sowohl bei den Verbrauchern und Unternehmen, die sich auf Zertifikate verlassen, als auch bei den Diensteanbietern stärken und damit zur breiten Akzeptanz elektronischer Signaturen beitragen.

9. Kooperative Mechanismen, die die grenzüberschreitende Anerkennung von Signaturen und Zertifikaten im Verkehr mit Drittländern fördern, sind für die Entwicklung des internationalen elektronischen Geschäftsverkehrs wichtig. Vor allem die Möglichkeit, daß

ein Zertifizierungsdiensteanbieter in der Europäischen Gemeinschaft für Zertifikate aus Drittländern in gleichem Umfang einstehen kann wie für seine eigenen, könnte grenzüberschreitende Dienste auf einfache, aber effiziente Weise unterstützen.

Vorschlag für eine
Richtlinie des Europäischen Parlaments und des Rates
(KOM...) vom (Datum)
über gemeinsame Rahmenbedingungen für elektronische Signaturen

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN GEMEINSCHAFTEN -

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

auf Vorschlag der Kommission;

nach Stellungnahme des Wirtschafts- und Sozialausschusses;

nach Stellungnahme des Ausschusses der Regionen;

gemäß dem Verfahren in Artikel 189 b des Vertrages;

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 elektronische Geschäftsverkehr“ vor.

(2) Auf der Bonner Ministerkonferenz vom 6. - 8. Juli 1997 wurde auf die Notwendigkeit rechtlicher und technischer Rahmenbedingungen für digitale Signaturen hingewiesen.

(3) 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“.

(4) 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. Im Rahmen der internationalen Expertenanhörung am 23/24. April 1998 in Kopenhagen wurden die wichtigsten rechtlichen Fragen im Bereich digitaler Signaturen erörtert.

(5) 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.

(6) Die Interoperabilität von Produkten für elektronische Signaturen sind zu fördern. Gemäß Artikel 7 a 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. Zur Zeit besteht kein eindeutiger Bedarf an Harmonisierungsmaßnahmen für von Verbrauchern genutzte Produkte.

(7) 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.

(8) 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.

(9) 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.

(10) Diese Richtlinie soll daher zur Verwendung und zur rechtlichen Anerkennung elektronischer Signaturen in der Europäischen 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 gelten die Regelungen über die rechtliche Anerkennung elektronischer Signaturen unbeschadet von gesetzlichen Formvorschriften, die den Abschluß von Verträgen oder die Festlegung des Ortes eines Vertragsabschlusses betreffen.

(11) Um die allgemeine Akzeptanz elektronischer Signaturen zu fördern, darf einer elektronischen Signatur nicht die Rechtsgültigkeit mit der alleinigen 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 der Gemeinschaft 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.

(12) 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 Europäischen Gemeinschaft beitragen und sich damit positiv auf das Funktionieren des Binnenmarktes auswirken.

(13) 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.

(14) 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. Nationales Recht legt fest, 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.

(15) Es empfiehlt sich, einen beratenden Ausschuß einzusetzen, der die Kommission in ihrem Bestreben unterstützt, einheitliche und verhältnismäßige Bestimmungen zu schaffen, die dem Bedarf des Marktes und der breiten Öffentlichkeit gerecht werden.

(16) Nach den in Artikel 3 b des Vertrages niedergelegten Grundsätzen der Subsidiarität und Proportionalität kann das Ziel der Schaffung harmonisierter rechtlicher Rahmenbedingungen für die Bereitstellung elektronischer Signaturen von den Mitgliedstaaten nicht ausreichend erreicht werden und läßt sich daher besser auf

Gemeinschaftsebene verwirklichen. Diese Richtlinie beschränkt sich auf die zur Erreichung dieses Ziels notwendigen Mindestanforderungen -

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Geltungsbereich und Begriffsbestimmungen

Artikel 1

Geltungsbereich und Zielsetzung

Mit dieser Richtlinie soll die Verwendung elektronischer Signaturen gefördert und ihre rechtliche Anerkennung gewährleistet werden. 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, um das reibungslose Funktionieren des Binnenmarktes im Bereich elektronischer Signaturen sicherzustellen.

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.

Grundsätze für die Bereitstellung von Zertifizierungsdiensten

Artikel 3

Grundsätze für den 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 Punkt 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.

Rechtswirkung, Haftung

Artikel 5

Rechtswirkung

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 nicht auf 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 die Anforderungen in Anhang II erfüllt,

(a) das rechtliche Erfordernis einer handschriftlichen Unterschrift erfüllen,

(b) 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) der im qualifizierten Zertifikat angegebene Inhaber 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 haftbar ist, 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 Zertifikates vorgeben können. Der Zertifizierungsdiensteanbieter ist nicht haftbar 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 ist nicht haftbar für Schäden, die sich aus der Überschreitung dieser Höchstgrenze ergeben.

5. Die obigen Bestimmungen gelten unbeschadet der Richtlinie 93/13/EG.

Internationale Aspekte, Datenschutz

Artikel 7

Internationale Aspekte

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

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

(b) ein in der Europäischen Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen in 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 Europäischen 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 und 97/66/EG 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.

Beratender Ausschuß

Artikel 9

Zusammensetzung und Verfahren

1. 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.

2. 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.

3. 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 zu Protokoll genommen. Darüber hinaus kann jeder Mitgliedstaat verlangen, daß sein Standpunkt im Protokoll festgehalten wird. Die Kommission trägt der Stellungnahme des Ausschusses so weit wie möglich Rechnung. Sie unterrichtet den Ausschuß darüber, inwieweit seine Stellungnahme berücksichtigt wurde, und faßt innerhalb eines Monats nach Eingang der Stellungnahme des Ausschusses einen Beschluß.

4. Die Kommission konsultiert regelmäßig Industrie, Benutzer- und Verbrauchergruppen. Sie informiert den Ausschuß regelmäßig über die Ergebnisse dieser Konsultationen.

Allgemeine und Schlußbestimmungen

Artikel 10

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 innerhalb eines Monats von den Mitgliedstaaten zu übermitteln.

Artikel 11

Überprüfungen

1. Die Kommission überprüft die Durchführung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat bei erster Gelegenheit, spätestens aber zum 1. Januar 2003, darüber Bericht.

2. Bei der Überprüfung ist u.a. 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 12

Durchführung

1. Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie bis zum 1. Januar 2001 nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis. Wenn die Mitgliedstaaten diese Maßnahmen 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 alle übrigen innerstaatlichen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 13

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

Artikel 14

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 Ermächtigung, für ein Unternehmen zu handeln, Kreditwürdigkeit, (Mehrwert-) Steuernummer, Zahlungsgarantien oder spezielle Genehmigungen bzw. Lizenzen);

(d) eine Signaturprüfeinheit, die einer vom Inhaber kontrollierten Signaturerstellungs-einheit 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 Handlungsbefugnis 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.