Bundesrat Drucksache **496/00**

18.08.00

Wi - Fz - In - R

Gesetzentwurf
der Bundesregierung

Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften

A. Zielsetzung

Der Gesetzentwurf dient der Ablösung des geltenden Signaturgesetzes vom 1. August 1997 (BGBl. I S. 1870, 1872). Der Entwurf verfolgt zwei Ziele: Erstens dient er der Umsetzung der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. EG 2000 Nr. L 13 S. 2; im Folgenden: Richtlinie). Zweitens greift er die Ergebnisse der Evaluierung des geltenden Signaturgesetzes (SigG) auf, wie sie im Bericht der Bundesregierung zum Informations- und Kommunikationsdienste-Gesetz vom 18. Juni 1999 (BT-Drs. 14/1191) festgestellt worden sind.

B. Lösung

Die im Gesetzentwurf vorgesehene Sicherheitsinfrastruktur für qualifizierte elektronische Signaturen ermöglicht es, im elektronischen Rechts- und Geschäftsverkehr den Urheber und die Integrität von Daten zuverlässig festzustellen. Dies ist die notwendige Voraussetzung dafür, dass die elektronische Signatur ein Substitut zur handschriftlichen Unterschrift darstellen und hierdurch eine entsprechende Rechtswirkung entfalten kann. Die Regelung der Rechtswirkung qualifizierter elektronischer Signaturen ist Gegenstand des Entwurfes eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr, der von der Bundesregierung gesondert in den Bundestag eingebracht wird.

Fristablauf: 29.09.00

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 1320, 53003 Bonn
Telefon: 0228/3820840, Telefax: 0228/3820844
ISSN 0720-2946

Der Gesetzentwurf sieht die Einführung einer freiwilligen Akkreditierung für Zertifizierungsdiensteanbieter vor, um den eingeführten und anerkannten Sicherheitsstandard nach dem geltenden Signaturgesetz für den Markt weiterhin anzubieten und zu erhalten. Eine im geltenden Signaturgesetz nicht vorgesehene Regelung zur Haftung der Zertifizierungsstellen und zur entsprechenden Deckungsvorsorge ist in den Entwurf aufgenommen worden. Der Entwurf trägt darüber hinaus den Erkenntnissen aus der Evaluierung des geltenden Signaturgesetzes durch Klarstellungen hinsichtlich der Befugnisse der Berufskammern, der Funktionen der Zertifizierungsstellen und der Anerkennung von Prüf- und Bestätigungsstellen Rechnung. Der Entwurf sieht weiterhin die Anpassung geltenden Bundesrechts an das neue Signaturgesetz vor. Weiterer Regelungsbedarf ergibt sich aus der Einführung des Euro.

C. Alternativen

Keine

D. Kosten der öffentlichen Haushalte

Mit diesem Gesetz sind folgende – im Vergleich zum geltenden SigG – zusätzliche Kosten für den Bundeshaushalt verbunden (Vollzugsaufwand):

Kosten entstehen im Zusammenhang mit dem nach Artikel 3 der Richtlinie vorgeschriebenen Überwachungssystem für Zertifizierungsstellen bei der nach § 3 SigG-E zuständigen Behörde, der Regulierungsbehörde für Telekommunikation und Post (RegTP). Soweit hierdurch zusätzlicher Personal- und Sachaufwand entsteht, wird dieser durch Gebühren und Beiträge abgedeckt. Im einzelnen wird hierüber im Rahmen der jeweiligen Haushaltsaufstellung entschieden.

Die Länder und Gemeinden werden nicht mit zusätzlichen Verwaltungskosten belastet. Das Verwaltungskostengesetz bleibt unberührt.

Weitere Kosten sind nicht zu erwarten. Den aufgeführten Kosten steht ein weitaus höheres Rationalisierungspotenzial, das mit der Nutzung qualifizierter elektronischer Signaturen nach dem Signaturgesetz verbunden ist, gegenüber.

...

E. Sonstige Kosten

Das Gesetz bildet eine wichtige Voraussetzung für eine erhebliche Effizienzsteigerung der Verwaltungen in Wirtschaft und Behörden. Zugleich gibt das Gesetz mit seinen EG-einheitlichen Rahmenbedingungen einen wichtigen Impuls für einen neuen Wirtschaftszweig der Datensicherheit (Zertifizierungsstellen, Produkte für elektronische Signaturen und Datensicherheit, Prüf- und Bestätigungsstellen) sowie für eine beschleunigte Modernisierung der Verwaltungen in Wirtschaft und Behörden. Die dafür notwendigen Investitionen kommen wiederum dem Arbeitsmarkt zugute.

Die Regelungen führen daher bei einer Gesamtbetrachtung zu einer Entlastung in Wirtschaft und Verwaltung. Von der Förderung des Wettbewerbs gehen tendenziell dämpfende Einflüsse auf Einzelpreise aus. Auswirkungen auf das Preisniveau, insbesondere das Verbraucherpreisniveau, sind nicht zu erwarten.

...

Bundesrat Drucksache **496/00**

18.08.00

Wi - Fz - In - R

Gesetzentwurf
der Bundesregierung

Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften

Bundesrepublik Deutschland
Der Bundeskanzler
022 (324) - 262 00 - Si 1/00

Berlin, den 18. August 2000

An den
Präsidenten des Bundesrates

Hiermit übersende ich gemäß Artikel 76 Abs. 2 des Grundgesetzes den von der Bundesregierung beschlossenen

> Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften

mit Begründung und Vorblatt.

Federführend ist das Bundesministerium für Wirtschaft und Technologie.

In Vertretung des Bundeskanzlers
Die Bundesministerin der Justiz

Fristablauf: 29.09.00

Drucksache 496/00

Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)[1)]

Inhaltsübersicht

Erster Abschnitt. Allgemeine Bestimmungen

§ 1 Zweck und Anwendungsbereich
§ 2 Begriffsbestimmungen
§ 3 Zuständige Behörde

Zweiter Abschnitt. Zertifizierungsdiensteanbieter

§ 4 Allgemeine Anforderungen
§ 5 Vergabe von qualifizierten Zertifikaten
§ 6 Unterrichtungspflicht
§ 7 Inhalt von qualifizierten Zertifikaten
§ 8 Sperrung von qualifizierten Zertifikaten
§ 9 Qualifizierte Zeitstempel
§ 10 Dokumentation
§ 11 Haftung
§ 12 Deckungsvorsorge
§ 13 Einstellung der Tätigkeit
§ 14 Datenschutz

Dritter Abschnitt. Freiwillige Akkreditierung

§ 15 Freiwillige Akkreditierung von Zertifizierungsdiensteanbietern
§ 16 Zertifikate der zuständigen Behörde

Vierter Abschnitt. Technische Sicherheit

§ 17 Produkte für elektronische Signaturen
§ 18 Anerkennung von Prüf- und Bestätigungsstellen

Fünfter Abschnitt. Aufsicht

§ 19 Aufsichtsmaßnahmen
§ 20 Mitwirkungspflicht

[1)] Die Mitteilungspflichten der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften (ABl. EG Nr. L 204 S 37 v. 21. Juli 1998), zuletzt geändert durch die Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20. Juli 1998 (ABl. EG Nr. L 217 S. 18 v.5. August 1998), und die Mitteilungspflichten der Richtlinie 1999/93/ EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. EG 2000 Nr. L 13 S. 2) sind beachtet worden.

Sechster Abschnitt. Schlussbestimmungen

§ 21 Bußgeldvorschriften
§ 22 Kosten und Beiträge
§ 23 Ausländische elektronische Signaturen und Produkte für elektronische Signaturen
§ 24 Rechtsverordnung
§ 25 Übergangsvorschriften

Erster Abschnitt. Allgemeine Bestimmungen

§ 1 Zweck und Anwendungsbereich

(1) Zweck des Gesetzes ist es, Rahmenbedingungen für elektronische Signaturen zu schaffen.

(2) Soweit nicht bestimmte elektronische Signaturen durch Rechtsvorschrift vorgeschrieben sind, ist ihre Verwendung freigestellt.

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

1. "elektronische Signaturen" Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,

2. "fortgeschrittene elektronische Signaturen" elektronische Signaturen nach Nummer 1, die

   a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
   b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
   c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
   d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,

3. "qualifizierte elektronische Signaturen" elektronische Signaturen nach Nummer 2, die
   a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
   b) mit einer sicheren Signaturerstellungseinheit erzeugt werden,

4. "Signaturschlüssel" einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden,

5. "Signaturprüfschlüssel" elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden,

6. "Zertifikate" elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigt wird,

7. "qualifizierte Zertifikate" elektronische Bescheinigungen nach Nummer 6 für natürliche Personen, die die Voraussetzungen des § 7 erfüllen und von Zertifizierungsdiensteanbietern ausgestellt werden, die die Anforderungen dieses Gesetzes und der Rechtsverordnung nach § 24 erfüllen,

8. "Zertifizierungsdiensteanbieter" natürliche oder juristische Personen, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen,

9. "Signaturschlüssel-Inhaber" natürliche Personen, die Signaturschlüssel besitzen und denen die zugehörigen Signaturprüfschlüssel durch qualifizierte Zertifikate zugeordnet sind,

10. "sichere Signaturerstellungseinheiten" Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die die Anforderungen dieses Gesetzes und der Rechtsverordnung nach § 24 erfüllen und die für qualifizierte elektronische Signaturen bestimmt sind,

11. "Signaturanwendungskomponenten" Software- und Hardwareprodukte, die dazu bestimmt sind,
    a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder
    b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen,

12. "technische Komponenten für Zertifizierungsdienste" Software- oder Hardwareprodukte, die dazu bestimmt sind,
    a) Signaturschlüssel zu erzeugen und in eine sichere Signaturerstellungseinheit zu übertragen,
    b) qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar zu halten oder
    c) qualifizierte Zeitstempel zu erzeugen,

13. "Produkte für elektronische Signaturen" sichere Signaturerstellungseinheiten, Signaturanwendungskomponenten und technische Komponenten für Zertifizierungsdienste,

14. "qualifizierte Zeitstempel" elektronische Bescheinigungen eines Zertifizierungsdiensteanbieters, der die Anforderungen dieses Gesetzes und der Rechtsverordnung nach § 24 erfüllt, darüber, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben,

15. "freiwillige Akkreditierung" Verfahren zur Erteilung einer Erlaubnis für den Betrieb eines Zertifizierungsdienstes, mit der besondere Rechte und Pflichten verbunden sind.

§ 3 Zuständige Behörde

Die Aufgaben der zuständigen Behörde nach diesem Gesetz und der Rechtsverordnung nach § 24 obliegen der Behörde nach § 66 des Telekommunikationsgesetzes.

Zweiter Abschnitt. Zertifizierungsdiensteanbieter

§ 4 Allgemeine Anforderungen

(1) Der Betrieb eines Zertifizierungsdienstes ist im Rahmen der Gesetze genehmigungsfrei.

(2) Einen Zertifizierungsdienst darf nur betreiben, wer die für den Betrieb erforderliche Zuverlässigkeit und Fachkunde sowie eine Deckungsvorsorge nach § 12 nachweist und die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 Nr. 1 und 3 gewährleistet. Die erforderliche Zuverlässigkeit besitzt, wer die Gewähr dafür bietet, als Zertifizierungsdiensteanbieter die für den Betrieb maßgeblichen Rechtsvorschriften einzuhalten. Die erforderliche Fachkunde liegt vor, wenn die im Betrieb eines Zertifizierungdienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen. Die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes liegen vor, wenn die Maßnahmen zur Erfüllung der Sicherheitsanforderungen nach diesem Gesetz und der Rechtsverordnung nach § 24 Nr. 1 und 3 der zuständigen Behörde in einem Sicherheitskonzept aufgezeigt und geeignet und praktisch umgesetzt sind.

(3) Wer den Betrieb eines Zertifizierungsdienstes aufnimmt, hat dies der zuständigen Behörde spätestens mit der Betriebsaufnahme anzuzeigen. Mit der Anzeige ist in geeigneter Form darzulegen, dass die Voraussetzungen nach Absatz 2 vorliegen.

(4) Die Erfüllung der Voraussetzungen nach Absatz 2 ist über die gesamte Zeitdauer der Tätigkeit des Zertifizierungsdienstes sicherzustellen. Umstände, die dies nicht mehr ermöglichen, sind der zuständigen Behörde unverzüglich anzuzeigen.

(5) Der Zertifizierungsdiensteanbieter kann unter Einbeziehung in sein Sicherheitskonzept nach Absatz 2 Satz 4 Aufgaben nach diesem Gesetz und der Rechtsverordnung nach § 24 an Dritte übertragen.

§ 5 Vergabe von qualifizierten Zertifikaten

(1) Der Zertifizierungsdiensteanbieter hat Personen, die ein qualifiziertes Zertifikat beantragen, zuverlässig zu identifizieren. Er hat die Zuordnung eines Signaturprüfschlüssels zu einer identifizierten Person durch ein qualifiziertes Zertifikat zu bestätigen und dieses jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten. Ein qualifiziertes Zertifikat darf nur mit Zustimmung des Signaturschlüssel-Inhabers abrufbar gehalten werden.

(2) Ein qualifiziertes Zertifikat kann auf Verlangen eines Antragstellers Angaben über seine Vertretungsmacht für eine dritte Person sowie berufsbezogene oder sonstige Angaben zu seiner Person (Attribute) enthalten. Hinsichtlich der Angaben über die Vertretungsmacht ist die Einwilligung der dritten Person nachzuweisen; berufsbezogene oder sonstige Angaben zur Person sind durch die für die berufsbezogenen oder sonstigen Angaben zuständige Stelle zu bestätigen. Angaben über die Vertretungsmacht für eine dritte Person dürfen nur bei Nachweis der Einwilligung nach Satz 2, berufsbezogene oder sonstige Angaben des Antragstellers zur Person nur bei Vorlage der Bestätigung nach Satz 2 in ein qualifiziertes Zertifikat aufgenommen werden. Weitere personenbezogene Angaben dürfen in ein qualifiziertes Zertifikat nur mit Einwilligung des Betroffenen aufgenommen werden.

(3) Der Zertifizierungsdiensteanbieter hat auf Verlangen eines Antragstellers in einem qualifizierten Zertifikat anstelle seines Namens ein Pseudonym aufzuführen. Enthält ein qualifiziertes Zertifikat Angaben über eine Vertretungsmacht für eine dritte Person oder berufsbezogene oder sonstige Angaben zur Person, ist eine Einwilligung der dritten Person oder der für die berufsbezogenen oder sonstigen Angaben zuständigen Stelle zur Verwendung des Pseudonyms erforderlich.

(4) Der Zertifzierungsdiensteanbieter hat Vorkehrungen zu treffen, damit Daten für qualifizierte Zertifikate nicht unbemerkt gefälscht oder verfälscht werden können. Er hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der Signaturschlüssel zu gewährleisten. Eine Speicherung von Signaturschlüsseln außerhalb der sicheren Signaturerstellungseinheit ist unzulässig.

(5) Der Zertifizierungsdiensteanbieter hat für die Ausübung der Zertifizierungstätigkeit zuverlässiges Personal und Produkte für elektronische Signaturen nach diesem Gesetz und der Rechtsverordnung nach § 24 einzusetzen.

(6) Der Zertifizierungsdiensteanbieter hat sich in geeigneter Weise zu überzeugen, dass der Antragsteller die zugehörige sichere Signaturerstellungseinheit besitzt.

§ 6 Unterrichtungspflicht

(1) Der Zertifizierungsdiensteanbieter hat den Antragsteller nach § 5 Abs. 1 über die Maßnahmen zu unterrichten, die erforderlich sind, um zur Sicherheit von qualifizierten elektronischen Signaturen und zu deren zuverlässiger Prüfung beizutragen. Er hat den Antragsteller darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

(2) Der Zertifizierungsdiensteanbieter hat den Antragsteller darüber zu unterrichten, dass eine qualifizierte elektronische Signatur im Rechtsverkehr die gleiche Wirkung hat wie eine eigenhändige Unterschrift, wenn durch Gesetz nicht ein anderes bestimmt ist. Zu diesem Zweck ist dem Antragsteller eine schriftliche Belehrung auszuhändigen, deren Kenntnisnahme dieser durch gesonderte Unterschrift zu bestätigen hat. Die elektronische Form ist bei der erstmaligen Antragstellung nicht zugelassen.

§ 7 Inhalt von qualifizierten Zertifikaten

(1) Ein qualifiziertes Zertifikat muss folgende Angaben enthalten und eine qualifizierte elektronische Signatur tragen:

1. den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muss,
2. den zugeordneten Signaturprüfschlüssel,
3. die Bezeichnung der Algorithmen, mit denen der Signaturprüfschlüssel des Signaturschlüssel-Inhabers sowie der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann,
4. die laufende Nummer des Zertifikates,
5. Beginn und Ende der Gültigkeit des Zertifikates,

6. den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist,
7. Angaben darüber, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt ist,
8. Angaben, dass es sich um ein qualifiziertes Zertifikat handelt, und
9. nach Bedarf Attribute des Signaturschlüssel-Inhabers.

(2) Attribute können auch in ein gesondertes qualifiziertes Zertifikat (qualifiziertes Attribut-Zertifikat) aufgenommen werden. Bei einem qualifizierten Attribut-Zertifikat können die Angaben nach Absatz 1 durch eindeutige Referenzdaten des qualifizierten Zertifikates, auf das sie Bezug nehmen, ersetzt werden, soweit sie nicht für die Nutzung des qualifizierten Attribut-Zertifikats benötigt werden.

§ 8 Sperrung von qualifizierten Zertifikaten

(1) Der Zertifizierungsdiensteanbieter hat ein qualifiziertes Zertifikat unverzüglich zu sperren, wenn ein Signaturschlüssel-Inhaber oder sein Vertreter es verlangt, das Zertifikat auf Grund falscher Angaben zu § 7 ausgestellt wurde, der Zertifizierungsdiensteanbieter seine Tätigkeit beendet und diese nicht von einem anderen Zertifizierungsdiensteanbieter fortgeführt wird oder die zuständige Behörde gemäß § 19 Abs. 4 eine Sperrung anordnet. Die Sperrung muss den Zeitpunkt enthalten, von dem an sie gilt. Eine rückwirkende Sperrung ist unzulässig. Wurde ein qualifiziertes Zertifikat mit falschen Angaben ausgestellt, kann der Zertifizierungsdiensteanbieter dies zusätzlich kenntlich machen.

(2) Enthält ein qualifiziertes Zertifikat Angaben nach § 5 Abs. 2, so kann auch die dritte Person oder die für die berufsbezogenen oder sonstigen Angaben zur Person zuständige Stelle, wenn die Voraussetzungen für die berufsbezogenen oder sonstigen Angaben zur Person nach Aufnahme in das qualifizierte Zertifikat entfallen, eine Sperrung des betreffenden Zertifikates nach Absatz 1 verlangen.

§ 9 Qualifizierte Zeitstempel

Stellt ein Zertifizierungsdiensteanbieter qualifizierte Zeitstempel aus, so gilt § 5 Abs. 5 entsprechend.

§ 10 Dokumentation

(1) Der Zertifizierungsdiensteanbieter hat die Sicherheitsmaßnahmen zur Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 Nr.1 und 3 sowie die ausgestellten qualifizierten Zertifikate nach Maßgabe des Satzes 2 so zu dokumentieren, dass die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind. Die Dokumentation muss unverzüglich so erfolgen, dass sie nachträglich nicht unbemerkt verändert werden kann. Dies gilt insbesondere für die Ausstellung und Sperrung von qualifizierten Zertifikaten.

(2) Dem Signaturschlüssel-Inhaber ist auf Verlangen Einsicht in die ihn betreffenden Daten und Verfahrensschritte zu gewähren.

§ 11 Haftung

(1) Verletzt ein Zertifizierungsdiensteanbieter die Anforderungen dieses Gesetzes und der Rechtsverordnung nach § 24 oder versagen seine Produkte für elektronische Signaturen oder sonstige technische Sicherungseinrichtungen, so hat er einem Dritten den Schaden zu ersetzen, den dieser dadurch erleidet, dass er auf die Angaben in einem qualifizierten Zertifikat, einem qualifizierten Zeitstempel oder einer Auskunft nach § 5 Abs. 1 Satz 2 vertraut. Die Ersatzpflicht tritt nicht ein, wenn der Dritte die Fehlerhaftigkeit der Angabe kannte oder kennen musste.

(2) Die Ersatzpflicht des Zertifizierungsdiensteanbieters ist ausgeschlossen, wenn er die Verletzung nicht zu vertreten hat.

(3) Wenn ein qualifiziertes Zertifikat die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt, tritt die Ersatzpflicht nur im Rahmen dieser Beschränkungen ein.

(4) Der Zertifizierungsdiensteanbieter haftet für beauftragte Dritte nach § 4 Abs. 5 und beim Einstehen für ausländische Zertifikate nach § 23 Abs. 1 Nr. 2 wie für eigenes Handeln. § 831 Abs. 1 Satz 2 des Bürgerlichen Gesetzbuchs findet keine Anwendung.

§ 12 Deckungsvorsorge

Der Zertifizierungsdiensteanbieter ist verpflichtet, eine geeignete Vorsorge zur Deckung der durch den Betrieb eines Zertifizierungsdienstes schuldhaft verursachten Schäden zu treffen. Die Mindestsumme beträgt 500 000 Deutsche Mark für einen durch ein haftungsauslösendes Ereignis der in § 11 bezeichneten Art verursachten Schaden.

§ 13 Einstellung der Tätigkeit

(1) Der Zertifizierungsdiensteanbieter hat die Einstellung seiner Tätigkeit unverzüglich der zuständigen Behörde anzuzeigen. Er hat dafür zu sorgen, dass die bei Einstellung der Tätigkeit gültigen qualifizierten Zertifikate von einem anderen Zertifizierungsdiensteanbieter übernommen werden, oder diese zu sperren. Er hat die betroffenen Signaturschlüssel-Inhaber über die Einstellung seiner Tätigkeit und die Übernahme der qualifizierten Zertifikate durch einen anderen Zertifizierungsdiensteanbieter zu benachrichtigen.

(2) Der Zertifizierungsdiensteanbieter hat die Dokumentation nach § 10 an den Zertifizierungsdiensteanbieter, welcher die Zertifikate nach Absatz 1 übernimmt, zu übergeben.

(3) Der Zertifizierungsdiensteanbieter hat einen Antrag auf Eröffnung eines Insolvenzverfahrens der zuständigen Behörde unverzüglich anzuzeigen.

§ 14 Datenschutz

(1) Der Zertifizierungsdiensteanbieter darf personenbezogene Daten nur unmittelbar beim Betroffenen selbst und nur insoweit erheben, als dies für Zwecke eines qualifizierten Zertifikates erforderlich ist. Eine Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zuläs-

sig. Für andere als die in Satz 1 genannten Zwecke dürfen die Daten nur verwendet werden, wenn dieses Gesetz es erlaubt oder der Betroffene eingewilligt hat.

(2) Bei einem Signaturschlüssel-Inhaber mit Pseudonym hat der Zertifizierungsdiensteanbieter die Daten über dessen Identität auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich ist oder soweit Gerichte dies im Rahmen anhängiger Verfahren anordnen. Die Auskünfte sind zu dokumentieren. Die ersuchende Behörde hat den Signaturschlüssel-Inhaber über die Aufdeckung des Pseudonyms zu unterrichten, sobald dadurch die Wahrnehmung der gesetzlichen Aufgaben nicht mehr beeinträchtigt wird oder wenn das Interesse des Signaturschlüssel-Inhabers an der Unterrichtung überwiegt.

(3) Soweit andere als die in § 2 Nr. 8 genannten Zertifizierungsdiensteanbieter Zertifikate für elektronische Signaturen ausstellen, gelten die Absätze 1 und 2 entsprechend.

Dritter Abschnitt. Freiwillige Akkreditierung

§ 15 Freiwillige Akkreditierung von Zertifizierungsdiensteanbietern

(1) Zertifizierungsdiensteanbieter können sich auf Antrag von der zuständigen Behörde akkreditieren lassen; die zuständige Behörde kann sich bei der Akkreditierung privater Stellen bedienen. Die Akkreditierung ist zu erteilen, wenn der Zertifizierungsdiensteanbieter nachweist, dass die Vorschriften nach diesem Gesetz und der Rechtsverordnung nach § 24 erfüllt sind. Akkreditierte Zertifizierungsdiensteanbieter erhalten ein Gütezeichen der zuständigen Behörde. Mit diesem wird der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen zum Ausdruck gebracht. Sie dürfen sich als akkreditierte Zertifizierungsdiensteanbieter bezeichnen und sich im Rechts- und Geschäftsverkehr auf die nachgewiesene Sicherheit berufen.

(2) Für den öffentlichen Bereich können qualifizierte elektronische Signaturen, die auf einem qualifizierten Zertifikat eines Zertifizierungsdiensteanbieters nach Absatz 1 beruhen, durch Rechtsvorschrift verlangt werden.

(3) Zur Erfüllung der Voraussetzungen nach Absatz 1 muss das Sicherheitskonzept nach § 4 Abs. 2 Satz 4 durch eine Stelle nach § 18 umfassend auf seine Eignung und praktische Umsetzung geprüft und bestätigt sein. Die Prüfung und Bestätigung ist nach sicherheitserheblichen Veränderungen sowie in regelmäßigen Zeitabständen zu wiederholen.

(4) Die Akkreditierung kann mit Nebenbestimmungen versehen werden, soweit dies erforderlich ist, um die Erfüllung der Voraussetzungen nach diesem Gesetz und der Rechtsverordnung nach § 24 bei Aufnahme und während des Betriebes sicherzustellen.

(5) Die Akkreditierung ist zu versagen, wenn die Voraussetzungen nach diesem Gesetz und der Rechtsverordnung nach § 24 nicht erfüllt sind; § 19 findet entsprechend Anwendung.

(6) Bei Nichterfüllung der Pflichten aus diesem Gesetz oder der Rechtsverordnung nach § 24 oder bei Vorliegen eines Versagungsgrundes nach Absatz 5 hat die zuständige Behörde die Ak-

kreditierung zu widerrufen oder diese, soweit die Gründe bereits zum Zeitpunkt der Akkreditierung vorlagen, zurück zu nehmen, wenn Maßnahmen nach § 19 Abs. 2 keinen Erfolg versprechen.

(7) Im Falle des Widerrufs oder der Rücknahme einer Akkreditierung oder im Falle der Einstellung der Tätigkeit eines akkreditierten Zertifizierungsdiensteanbieters hat die zuständige Behörde eine Übernahme der Tätigkeit durch einen anderen akkreditierten Zertifizierungsdiensteanbieter oder die Abwicklung der Verträge mit den Signaturschlüssel-Inhabern sicherzustellen. Dies gilt auch bei Antrag auf Eröffnung eines Insolvenzverfahrens, wenn die Tätigkeit nicht fortgesetzt wird. Übernimmt kein anderer akkreditierter Zertifizierungsdiensteanbieter die Dokumentation gemäß § 13 Abs. 2, so hat die zuständige Behörde diese zu übernehmen.

(8) Bei Produkten für elektronische Signaturen muss die Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 und der Rechtsverordnung nach § 24 nach dem Stand von Wissenschaft und Technik hinreichend geprüft und durch eine Stelle nach § 18 bestätigt worden sein; Absatz 1 Satz 3 findet entsprechende Anwendung. Der akkreditierte Zertifizierungsdiensteanbieter hat

1. für seine Zertifizierungstätigkeit nur nach Satz 1 geprüfte und bestätigte Produkte für elektronische Signaturen einzusetzen,
2. qualifizierte Zertifikate nur für Personen auszustellen, die nachweislich nach Satz 1 geprüfte und bestätigte sichere Signaturerstellungseinheiten besitzen, und
3. die Signaturschlüssel-Inhaber im Rahmen des § 6 Abs. 1 über nach Satz 1 geprüfte und bestätigte Signaturanwendungskomponenten zu unterrichten.

§ 16 Zertifikate der zuständigen Behörde

(1) Die zuständige Behörde stellt den akkreditierten Zertifizierungsdiensteanbietern die für ihre Tätigkeit benötigten qualifizierten Zertifikate aus. Die Vorschriften für die Vergabe von qualifizierten Zertifikaten durch akkreditierte Zertifizierungsdiensteanbieter gelten für die zuständige Behörde entsprechend. Sie sperrt von ihr ausgestellte qualifizierte Zertifikate, wenn ein akkreditierter Zertifizierungsdiensteanbieter seine Tätigkeit einstellt oder wenn eine Akkreditierung zurückgenommen oder widerrufen wird.

(2) Die zuständige Behörde hat

1. die Namen, Anschriften und Kommunikationsverbindungen der akkreditierten Zertifizierungsdiensteanbieter,
2. den Widerruf oder die Rücknahme einer Akkreditierung,
3. die von ihr ausgestellten qualifizierten Zertifikate und deren Sperrung und
4. die Beendigung und die Untersagung des Betriebes eines akkreditierten Zertifizierungsdiensteanbieters

jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten.

(3) Bei Bedarf stellt die zuständige Behörde auch die von den Zertifizierungsdiensteanbietern oder Herstellern benötigten elektronischen Bescheinigungen für die automatische Authentifizierung von Produkten nach § 15 Abs. 8 aus.

Vierter Abschnitt. Technische Sicherheit

§ 17 Produkte für elektronische Signaturen

(1) Für die Speicherung von Signaturschlüsseln sowie für die Erzeugung qualifizierter elektronischer Signaturen sind sichere Signaturerstellungseinheiten einzusetzen, die Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung der Signaturschlüssel schützen. Werden die Signaturschlüssel auf einer sicheren Signaturerstellungseinheit selbst erzeugt, so gilt Absatz 3 Nr. 1 entsprechend.

(2) Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht. Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,

1. auf welche Daten sich die Signatur bezieht,
2. ob die signierten Daten unverändert sind,
3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,
4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und
5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 2 geführt hat.

Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Die Signaturschlüssel-Inhaber sollen solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.

(3) Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um

1. bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel zu gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit auszuschließen,
2. qualifizierte Zertifikate, die gemäß § 5 Abs. 1 Satz 2 nachprüfbar oder abrufbar gehalten werden, vor unbefugter Veränderung und unbefugtem Abruf zu schützen sowie
3. bei Erzeugung qualifizierter Zeitstempel Fälschungen und Verfälschungen auszuschließen.

(4) Die Erfüllung der Anforderungen nach den Absätzen 1 und 3 Nr. 1 sowie der Rechtsverordnung nach § 24 ist durch eine Stelle nach § 18 zu bestätigen. Zur Erfüllung der Anforderungen nach den Absätzen 2 und 3 Nr. 2 und 3 genügt eine Erklärung durch den Hersteller des Produkts für elektronische Signaturen.

§ 18 Anerkennung von Prüf- und Bestätigungsstellen

(1) Die zuständige Behörde erkennt eine natürliche oder juristische Person auf Antrag als Bestätigungsstelle nach § 17 Abs. 4 oder § 15 Abs. 8 Satz 1 oder als Prüf- und Bestätigungsstelle nach § 15 Abs. 3 an, wenn diese die für die Tätigkeit erforderliche Zuverlässigkeit, Unabhängigkeit und Fachkunde nachweist. Die Anerkennung kann inhaltlich beschränkt, vorläufig oder mit einer Befristung versehen erteilt werden und mit Auflagen verbunden sein.

(2) Die nach Absatz 1 anerkannten Stellen haben ihre Aufgaben unparteiisch, weisungsfrei und gewissenhaft zu erfüllen. Sie haben die Prüfungen und Bestätigungen zu dokumentieren und die Dokumentation im Falle der Einstellung ihrer Tätigkeit an die zuständige Behörde zu übergeben.

Fünfter Abschnitt. Aufsicht

§ 19 Aufsichtsmaßnahmen

(1) Die Aufsicht über die Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 obliegt der zuständigen Behörde; diese kann sich bei der Durchführung der Aufsicht privater Stellen bedienen. Mit der Aufnahme des Betriebes unterliegt ein Zertifizierungsdiensteanbieter der Aufsicht der zuständigen Behörde.

(2) Die zuständige Behörde kann gegenüber Zertifizierungsdiensteanbietern Maßnahmen zur Sicherstellung der Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 treffen.

(3) Die zuständige Behörde hat einem Zertifizierungsdiensteanbieter den Betrieb vorübergehend, teilweise oder ganz zu untersagen, wenn Tatsachen die Annahme rechtfertigen, dass er

1. nicht die für den Betrieb eines Zertifizierungsdienstes erforderliche Zuverlässigkeit besitzt,
2. nicht nachweist, dass die für den Betrieb erforderliche Fachkunde vorliegt,
3. nicht über die erforderliche Deckungsvorsorge verfügt,
4. ungeeignete Produkte für elektronische Signaturen verwendet oder
5. die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 nicht erfüllt

und Maßnahmen nach Absatz 2 keinen Erfolg versprechen.

(4) Die zuständige Behörde kann eine Sperrung von qualifizierten Zertifikaten anordnen, wenn Tatsachen die Annahme rechtfertigen, dass qualifizierte Zertifikate gefälscht oder nicht hinreichend fälschungssicher sind oder dass sichere Signaturerstellungseinheiten Sicherheitsmängel aufweisen, die eine unbemerkte Fälschung qualifizierter elektronischer Signaturen oder eine unbemerkte Verfälschung damit signierter Daten zulassen.

(5) Die Gültigkeit der von einem Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikate bleibt von der Untersagung des Betriebes und der Einstellung der Tätigkeit sowie der Rücknahme und dem Widerruf einer Akkreditierung unberührt.

(6) Die zuständige Behörde hat die Namen der bei ihr angezeigten Zertifizierungsdiensteanbieter sowie der Zertifizierungsdiensteanbieter, die ihre Tätigkeit nach § 13 eingestellt haben oder deren Betrieb nach § 19 Abs. 3 untersagt wurde, für jeden über öffentlich erreichbare Kommunikationsverbindungen abrufbar zu halten.

§ 20 Mitwirkungspflicht

(1) Die Zertifizierungsdiensteanbieter und die für diese nach § 4 Abs. 5 tätigen Dritten haben der zuständigen Behörde und den in ihrem Auftrag handelnden Personen das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten, auf Verlangen die in Betracht kommenden Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstigen Unterlagen in

geeigneter Weise zur Einsicht vorzulegen, auch soweit sie in elektronischer Form geführt werden, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren.

(2) Der zur Erteilung einer Auskunft Verpflichtete kann die Auskunft verweigern, wenn er sich damit selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr der Verfolgung wegen einer Straftat oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Er ist auf dieses Recht hinzuweisen.

Sechster Abschnitt. Schlussbestimmungen

§ 21 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4 Abs. 2 Satz 1, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1 und 3, einen Zertifizierungsdienst betreibt,
2. entgegen § 4 Abs. 3 Satz 1 oder § 13 Abs. 1 Satz 1 eine Anzeige nicht, nicht richtig oder nicht rechtzeitig erstattet,
3. entgegen § 5 Abs. 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1 eine Person nicht, nicht richtig oder nicht rechtzeitig identifiziert,
4. entgegen § 5 Abs. 1 Satz 2, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, ein qualifiziertes Zertifikat nicht nachprüfbar hält,
5. entgegen § 5 Abs. 1 Satz 3 ein qualifiziertes Zertifikat abrufbar hält,
6. entgegen § 5 Abs. 2 Satz 3 oder 4 eine Angabe in ein qualifiziertes Zertifikat aufnimmt,
7. entgegen § 5 Abs. 4 Satz 2, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, eine Vorkehrung nicht oder nicht richtig trifft,
8. entgegen § 5 Abs. 4 Satz 3 einen Signaturschlüssel speichert,
9. entgegen § 10 Abs. 1 Satz 1, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, eine Sicherheitsmaßnahme oder ein qualifiziertes Zertifikat nicht, nicht richtig oder nicht rechtzeitig dokumentiert,
10. entgegen § 13 Abs. 1 Satz 2, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, nicht dafür sorgt, dass ein qualifiziertes Zertifikat von einem anderen Zertifizierungsdiensteanbieter übernommen wird und ein qualifiziertes Zertifikat nicht oder nicht rechtzeitig sperrt oder
11. entgegen § 13 Abs. 1 Satz 3 in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1 einen Signaturschlüssel-Inhaber nicht, nicht richtig oder nicht rechtzeitig benachrichtigt.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nr. 1, 7 und 8 mit einer Geldbuße bis zu hunderttausend Deutsche Mark, in den übrigen Fällen mit einer Geldbuße bis zu zwanzigtausend Deutsche Mark geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist die Regulierungsbehörde für Telekommunikation und Post.

§ 22 Kosten und Beiträge

(1) Die zuständige Behörde erhebt für ihre folgenden Amtshandlungen Kosten (Gebühren und Auslagen):

1. Maßnahmen im Rahmen der freiwilligen Akkreditierung von Zertifizierungsdiensteanbietern nach § 15 Abs. 1, 3 bis 8 und der Rechtsverordnung nach § 24,
2. Maßnahmen im Rahmen der Ausstellung der qualifizierten Zertifikate nach § 16 Abs. 1 sowie der Ausstellung von Bescheinigungen nach § 16 Abs. 3,
3. Maßnahmen im Rahmen der Anerkennung von Prüf- und Bestätigungsstellen nach § 18 und der Rechtsverordnung nach § 24,
4. Maßnahmen im Rahmen der Aufsicht nach § 19 Abs. 1 bis 4 in Verbindung mit § 4 Abs. 2 bis 4 und der Rechtsverordnung nach § 24.

Kosten werden auch für den Verwaltungsaufwand erhoben, der dadurch entsteht, dass sich die Behörde bei der Durchführung der Aufsicht privater Stellen bedient. Das Verwaltungskostengesetz findet Anwendung.

(2) Zertifizierungsdiensteanbieter, die den Betrieb nach § 4 Abs. 3 angezeigt haben, haben zur Abgeltung des Verwaltungsaufwands für die ständige Erfüllung der Voraussetzungen nach § 19 Abs. 6 eine Abgabe an die zuständige Behörde zu entrichten, die als Jahresbeitrag erhoben wird. Zertifizierungsdiensteanbieter, die nach § 15 Abs. 1 akkreditiert sind, haben zur Abgeltung des Verwaltungaufwands für die ständige Erfüllung der Voraussetzungen nach § 16 Abs. 2 eine Abgabe an die zuständige Behörde zu entrichten, die als Jahresbeitrag erhoben wird.

§ 23 Ausländische elektronische Signaturen und Produkte für elektronische Signaturen

(1) Elektronische Signaturen, die mit Signaturprüfdaten überprüft werden können, für die ein ausländisches qualifiziertes Zertifikat aus einem anderen Mitgliedstaat der Europäischen Union oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum vorliegt, sind, soweit sie Artikel 5 Abs. 1 der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. EG 2000 Nr. L 13 S.2) in der jeweils geltenden Fassung entsprechen, qualifizierten elektronischen Signaturen gleichgestellt. Elektronische Signaturen aus Drittstaaten sind qualifizierten elektronischen Signaturen gleichgestellt, wenn das Zertifikat von einem dortigen Zertifizierungsdiensteanbieter öffentlich als qualifiziertes Zertifikat ausgestellt und für eine elektronische Signatur im Sinne von Artikel 5 Abs. 1 der Richtlinie 1999/93/99EG bestimmt ist und wenn

1. der Zertifizierungsdiensteanbieter die Anforderungen der Richtlinie erfüllt und in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum akkreditiert ist oder

2. ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, welcher die Anforderungen der Richtlinie erfüllt, für das Zertifikat einsteht oder

3. das Zertifikat oder der Zertifizierungsdiensteanbieter im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Europäischen Union und Drittstaaten oder internationalen Organisationen anerkannt ist.

(2) Elektronische Signaturen nach Absatz 1 sind qualifizierten elektronischen Signaturen, die auf einem qualifizierten Zertifikat eines Zertifizierungsdiensteanbieters nach § 15 Abs. 1 beruhen, gleichgestellt, wenn sie nachweislich gleichwertige Sicherheit aufweisen.

(3) Produkte für elektronische Signaturen, bei denen in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum festgestellt wurde, dass sie den Anforderungen der Richtlinie 1999/93/EG in der jeweils geltenden Fassung entsprechen, werden anerkannt. Den nach § 15 Abs. 8 geprüften Produkten für elektronische Signaturen werden Produkte für elektronische Signaturen aus einem in Satz 1 genannten Staat oder aus einem Drittstaat gleichgestellt, wenn sie nachweislich gleichwertige Sicherheit aufweisen.

§ 24 Rechtsverordnung

Die Bundesregierung wird ermächtigt, durch Rechtsverordnung die zur Durchführung der §§ 3 bis 23 erforderlichen Rechtsvorschriften zu erlassen über

1. die Ausgestaltung der Pflichten der Zertifizierungsdiensteanbieter in bezug auf die Betriebsaufnahme und während des Betriebes sowie bei Einstellung des Betriebes nach § 4 Abs. 2 und 3, §§ 5, 6 Abs. 1, §§ 8, 10, 12, 13 und 15,
2. die gebührenpflichtigen Tatbestände und die Gebührensätze sowie die Höhe der Beiträge und das Verfahren der Beitragserhebung durch die zuständige Behörde; bei der Bemessung der Beiträge ist der Verwaltungsaufwand (Personal- und Sachaufwand) zugrundezulegen soweit er nicht bereits durch eine Gebühr abgegolten wird,
3. die Ausgestaltung des Inhalts und die Gültigkeitsdauer von qualifizierten Zertifikaten nach § 7,
4. die näheren Anforderungen an Produkte für elektronische Signaturen nach § 17 Abs. 1 bis 3 sowie die Prüfung dieser Produkte und die Bestätigung, dass die Anforderungen erfüllt sind, nach § 17 Abs. 4 und § 15 Abs. 8,
5. die Einzelheiten des Verfahrens der Anerkennung sowie der Tätigkeit von Prüf- und Bestätigungsstellen nach § 18,
6. den Zeitraum sowie das Verfahren, nach dem Daten mit einer qualifizierten elektronischen Signatur nach § 6 Abs. 1 Satz 2 neu signiert werden sollten,
7. das Verfahren zur Feststellung der gleichwertigen Sicherheit von ausländischen elektronischen Signaturen und ausländischen Produkten für elektronische Signaturen nach § 23.

§ 25 Übergangsvorschriften

(1) Die nach dem Signaturgesetz vom 28. Juli 1997 (BGBl. I S. 1870, 1872) genehmigten Zertifizierungsstellen gelten als akkreditiert im Sinne von § 15. Diese haben der zuständigen Behörde innerhalb von drei Monaten nach Inkrafttreten dieses Gesetzes einen Deckungsnachweis nach § 12 vorzulegen.

(2) Die von den Zertifizierungsstellen nach Absatz 1 bis zum Zeitpunkt des Inkrafttretens dieses Gesetzes nach § 5 des Signaturgesetzes vom 28. Juli 1997 (BGBl. I S. 1870, 1872) ausgestellten Zertifikate sind qualifizierten Zertifikaten gleichgestellt. Inhaber von Zertifikaten nach Satz 1 sind innerhalb von sechs Monaten nach Inkrafttreten dieses Gesetzes durch die Zertifizierungsstelle nach § 6 Abs. 2 Satz 1 und 2 in geeigneter Weise zu unterrichten.

(3) Die von der zuständigen Behörde erfolgten Anerkennungen von Prüf- und Bestätigungsstellen nach § 4 Abs. 3 Satz 3 und § 14 Abs. 4 des Signaturgesetzes vom 28. Juli 1997 (BGBl. I S. 1870, 1872) behalten ihre Gültigkeit, soweit sie in Übereinstimmung mit § 18 dieses Gesetzes stehen.

(4) Technische Komponenten, bei denen die Erfüllung der Anforderungen nach § 14 Abs. 4 des Signaturgesetzes vom 28. Juli 1997 (BGBl. I S. 1870, 1872) geprüft und bestätigt wurde, sind Produkten für elektronische Signaturen nach § 15 Abs. 8 dieses Gesetzes gleichgestellt.

Artikel 2

Umstellung von Vorschriften auf Euro

Das Signaturgesetz vom ..... (BGBl. I S.....) wird wie folgt geändert:

1. In § 12 Satz 2 wird die Angabe „500 000 Deutsche Mark" durch die Angabe „250 000 Euro" ersetzt.

2. In § 21 Abs. 2 werden die Wörter „hunderttausend Deutsche Mark" durch die Wörter „fünfzigtausend Euro" und die Wörter „zwanzigtausend Deutsche Mark" durch die Wörter „zehntausend Euro" ersetzt.

Artikel 3

Anpassung von Bundesrecht

(1) In § 15 Satz 2 der Verordnung über die Vergabe öffentlicher Aufträge vom .....2000 (BGBl. I S. .....) werden die Wörter „Signatur im Sinne des Signaturgesetzes" durch die Wörter „einer qualifizierten elektronischen Signatur nach dem Signaturgesetz" ersetzt.

(2) In § 7 Abs. 3 der Sozialversicherungs-Rechnungsverordnung vom 15. Juli 1999 (BGBl. I S. 1627) wird die Angabe „digitalen Signatur nach § 2 Abs. 1 des Signaturgesetzes (Artikel 3 des Gesetzes vom 22. Juli 1997, BGBl. I S. 1870, 1872)" durch die Wörter „einer qualifizierten elektronischen Signatur nach dem Signaturgesetz" ersetzt.

Artikel 4

Rückkehr zum einheitlichen Verordnungsrang

Die auf Artikel 3 Abs. 1 und 2 beruhenden Teile der dort geänderten Rechtsverordnung können auf Grund der jeweils einschlägigen Ermächtigungen durch Rechtsverordnung geändert werden.

Artikel 5

Inkrafttreten; Außerkrafttreten

Dieses Gesetz tritt vorbehaltlich des Satzes 2 am Tage nach der Verkündung in Kraft; gleichzeitig tritt das Signaturgesetz vom 28. Juli 1997 (BGBl. I S. 1870, 1872) außer Kraft. Artikel 2 tritt am 1. Januar 2002 in Kraft.

Drucksache 496/00

Begründung

A. Allgemeines

I. Ausgangslage

Die elektronische Signatur ermöglicht es, im elektronischen Rechts- und Geschäftsverkehr den Urheber und die Integrität von Daten festzustellen. Die elektronische Signatur kann ein Substitut zur handschriftlichen Unterschrift darstellen und hierdurch eine entsprechende Rechtswirkung entfalten, wenn die rechtlichen Voraussetzungen hierfür bestehen. Elektronische Signaturen schaffen somit eine wichtige Grundlage für das Vertrauen in die neuen Informations- und Kommunikationsdienste.

Seit dem 1. August 1997 gilt das Gesetz zur digitalen Signatur (Signaturgesetz – SigG, BGBl. I S. 1870, 1872), das im Rahmen des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) verabschiedet worden ist. Die bisher im Rechts- und Geschäftsverkehr vor allem bekannten digitalen Signaturen sind von dem technologieoffeneren Begriff der elektronischen Signaturen mit umfasst (vgl. Teil B. zu Art. 1, § 2 Nr. 1 bis 3). Digitale bzw. elektronische Signaturen erfordern entsprechende Sicherheitsinfrastrukturen, wie sie beispielsweise im geltenden Signaturgesetz geregelt sind.

Bei der Verabschiedung des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) hat der Deutsche Bundestag die Bundesregierung aufgefordert, unter anderem auch die Entwicklung bei den digitalen Signaturen zu beobachten und spätestens zwei Jahre nach Inkrafttreten des Gesetzes zu berichten, ob und ggf. in welchen Bereichen Anpassungsbedarf besteht (Beschluß des Deutschen Bundestages vom 11. Juni 1997 – BT Drs. 13/7935).

Am 18. Juni 1999 wurde dem Deutschen Bundestag der Bericht der Bundesregierung über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) (BT-Drs. 14/1191; im folgenden: IuKDG-Bericht) vorgelegt. Darin wird festgestellt, dass sich die für digitale (bzw. elektronische) Signaturen erforderliche Sicherheitsinfrastruktur zügig entwickelt, endgültige Schlussfolgerungen jedoch verfrüht sind, da der Einsatz und die Nutzung dieser Signaturen in Deutschland und weltweit noch am Anfang stehen. In bezug auf das geltende Gesetz werden punktuelle technische Verbesserungen vorgeschlagen. Im IuKDG-Bericht wurde vorgeschlagen, die notwendigen Anpassungen in die Umsetzung der zum Berichtszeitpunkt noch in der Beratung befindlichen EG-Richtlinie über Rahmenbedingungen für elektronische Signaturen einzubeziehen.

Im gleichen Jahr wurde die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. EG L Nr. 13 v. 19. Januar 2000, S. 12 ff; im folgenden EGSRL) verabschiedet, die jetzt umzusetzen ist.

Die Voraussetzungen für eine rasche Umsetzung der Richtlinie bestehen und die Notwendigkeit hierfür ist gegeben. Deutschland verfügt mit dem Signaturgesetz seit 1997 über einheitliche gesetzliche Regelungen für digitale Signaturen. Die annähernd dreijährige Phase der Umsetzung des Gesetzes hat Deutschland damit einen erheblichen Erfahrungsvorsprung verschafft und seine Vorreiterrolle in Europa und international auf diesem Gebiet gefestigt. Es gilt nun, diese Position durch eine zügige Umsetzung der Richtlinie zu erhalten. Deutschland verfügt inzwischen über eine flächendeckende IT-Sicherheitsinfrastruktur (Einrichtung gesetzeskonformer Zertifizierungsdienste, technischer Komponenten und geeigneter Prüf- und Bestätigungsstellen).

Die Regulierungsbehörde für Telekommunikation und Post als zuständige Behörde nach geltendem Signaturgesetz und nach dem Gesetzentwurf hat einen eigenen Zertifizierungsdienst eingerichtet, der seit dem 23. September 1998 in Betrieb ist. Im Dezember 1998 hat die Regulierungsbehörde die erste Genehmigung für den Betrieb eines privaten Zertifizierungsdienstes erteilt. Die Deutsche Telekom AG und die

Deutsche Post AG bieten inzwischen bundesweit Leistungen nach dem geltenden Signaturgesetz an. Weitere Zertifizierungsdiensteanbieter stehen vor dem Markteintritt. Eine Reihe von Zertifizierungsdiensteanbietern, darunter auch solche, die den Markteintritt in der nächsten Zeit vorbereiten, haben sich zwischenzeitlich auf einen gemeinsamen technischen Standard für gesetzeskonforme Signaturen geeinigt. Damit können die Anwender von elektronischen Signaturen mit einer technischen Ausstattung die Leistungen verschiedener Anbieter nutzen.

II. Allgemeine Vorgaben

1. Zielsetzung

Der Gesetzentwurf dient der Ablösung des geltenden Signaturgesetzes vom 1. August 1997. Der Entwurf verfolgt zwei Ziele:

- Erstens dient er der Umsetzung der Richtlinie. Die Richtlinie ist am 19. Januar 2000 in Kraft getreten. Die Umsetzungsfrist für die Richtlinie läuft am 19. Juli 2001 ab. Es wird angestrebt, noch vor Ablauf der Umsetzungsfrist die Richtlinie in Deutschland bis Anfang 2001 umzusetzen.
- Zweitens greift er die Ergebnisse der Evaluierung des geltenden Signaturgesetzes auf, wie sie im IuKDG-Bericht der Bundesregierung vom 18. Juni 1999 niedergelegt sind. Die Ergebnisse der Evaluierung werden insoweit in den Gesetzentwurf aufgenommen, als diese im Einklang mit der Richtlinie stehen.

Wegen der erheblichen strukturellen und inhaltlichen Änderungen gegenüber dem geltenden Signaturgesetz soll dieses durch den vorgelegten Gesetzentwurf insgesamt abgelöst werden.

2. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz ergibt sich aus Artikel 74 Abs. 1 Nr. 11 Grundgesetz. Die besondere Bedeutung der elektronischen Signaturen für den Wirtschaftsstandort Deutschland, ihre grenzüberschreitenden Wirkungen und insbesondere die Tatsache, dass qualifizierte elektronische Signaturen ein Substitut zur handschriftlichen Unterschrift darstellen können und hierfür eine entsprechende Sicherheitsinfrastruktur benötigen, machen einheitliche Rahmenbedingungen unabdingbar erforderlich. Die Regelung durch Bundesgesetz ist deshalb zur Wahrung der Rechts- und Wirtschaftseinheit im gesamtstaatlichen Interesse erforderlich (Artikel 72 Abs. 2 GG).

3. Preise

Das Gesetz wird keine Auswirkungen auf das allgemeine Preisniveau haben.

4. Kosten

Mit diesem Gesetz sind folgende – im Vergleich zum geltenden Signaturgesetz – zusätzlichen Kosten verbunden:

Kosten entstehen im Zusammenhang mit dem nach Artikel 3 der Richtlinie vorgeschriebenen Überwachungssystem für Zertifizierungsdienste bei der nach § 3 SigG-E zuständigen Behörde, der Regulierungsbehörde für Telekommunikation und Post (RegTP). Soweit hierdurch zusätzlicher Personal- und Sachaufwand entsteht, wird dieser durch Gebühren und Beiträge abgedeckt. Im einzelnen wird hierüber im Rahmen der jeweiligen Haushaltsaufstellung entschieden.

Für Kosten, die im Zusammenhang mit dem Führen eines online abrufbaren Verzeichnisses nach §§ 16 Abs. 2 und 19 Abs. 6 SigG-E entstehen, ist die Erhebung eines Jahresbeitrages vorgesehen. Fiskalisches Ziel ist die Deckung dieser Kosten. Hierbei soll bei der Bemessung des Jahresbeitrages die Tatsache Berücksichtigung finden, dass zum Zeitpunkt des Gesetzesentwurfs nur wenige Anbieter am Markt sind. Aus diesem Grund ist bei der Festlegung der Höhe des Beitrages mit Blick auf die wirtschaftliche Zumutbarkeit für die Betroffenen eine Flexibilisierung vorgesehen.

Weitere Kosten sind nicht zu erwarten. Dies betrifft auch die Einführung des freiwilligen Akkreditierungssystems (vgl. § 15 SigG-E). Für das Akkreditierungsverfahren kann auf die für die Genehmigung nach dem geltenden SigG bereits geschaffene Infrastruktur bei der Regulierungsbehörde für Telekommunikation und Post zurückgegriffen werden.

Die Länder und Gemeinden werden nicht mit zusätzlichen Verwaltungskosten belastet. Das Verwaltungskostengesetz bleibt unberührt.

Den aufgeführten Kosten steht ein weitaus höheres betriebs- und volkswirtschaftliches Rationalisierungspotential, das mit der Nutzung (EG-einheitlicher) qualifizierter elektronischer Signaturen nach dem Signaturgesetz verbunden ist, gegenüber. Qualifizierte elektronische Signaturen ermöglichen es, nach Abschluss der vorgesehenen Rechtsänderungen (z. B. Einführung der „elektronischen Form“ nach

§ 126a BGB-E als Äquivalent zur Schriftform nach § 126 BGB) das herkömmliche Schriftdokument weitgehend durch das elektronische Dokument zu ersetzen.

Das Gesetz bildet damit eine wichtige Voraussetzung für eine erhebliche Effizienzsteigerung der Verwaltungen in Wirtschaft und Behörden. Zugleich gibt das Gesetz mit seinen EG-einheitlichen Rahmenbedingungen einen wichtigen Impuls für einen neuen Wirtschaftszweig der Datensicherheit (Zertifizierungsdienste, Produkte für elektronische Signaturen und Datensicherheit, Prüf- und Bestätigungsstellen) sowie für eine beschleunigte Modernisierung der Verwaltungen in Wirtschaft und Behörden. Die dafür notwendigen Investitionen kommen wiederum dem Arbeitsmarkt zugute. Da sich der Umstieg auf das elektronische Dokument und den elektronischen Geschäftsverkehr weltweit rasch vollziehen dürfte, ergeben sich für die (EG-einheitlichen) Leistungen und Produkte nach dem Signaturgesetz auch Exportchancen für Unternehmen in Deutschland, die aufgrund der bereits bestehenden Erfahrungen und Infrastrukturen im Rahmen des geltenden Signaturgesetzes zum Teil bereits genutzt werden.

Schließlich leistet das Gesetz einen Beitrag zur Entlastung von Verkehr und Umwelt, indem Leistungen und Produkte auch online sicher bereitgestellt werden können (z.B. durch Telearbeit oder Online-Übermittlung von Software).

Die Regelungen führen daher bei einer Gesamtbetrachtung zu einer Entlastung in Wirtschaft und Verwaltung. Von der Förderung des Wettbewerbs gehen tendenziell dämpfende Einflüsse auf Einzelpreise aus. Auswirkungen auf das Preisniveau, insbesondere das Verbraucherpreisniveau, sind nicht zu erwarten.

III. Im Einzelnen

1. Grundzüge der Richtlinie und Übersicht über die Umsetzung

Die Richtlinie soll gemäß Artikel 1 die Verwendung elektronischer Signaturen erleichtern und zu ihrer rechtlichen Anerkennung beitragen. Sie legt rechtliche Rahmenbedingungen für elektronische Signaturen fest, damit das reibungslose Funktionieren des Binnenmarktes gewährleistet ist. Dies wird durch die Bezeichnung des Gesetzes und die Zweckbestimmung in § 1 Abs. 1 SigG-E abgebildet.

In Artikel 2 EGSRL werden die in der Richtlinie verwendeten Fachbegriffe definiert. Die Begriffsbestimmungen werden in § 2 SigG-E unmittelbar bzw. sinngemäß aus der Richtlinie übernommen.

Nach Artikel 3 Abs. 1 EGSRL dürfen die Mitgliedstaaten die Bereitstellung von Zertifizierungsdiensten nicht von einer vorherigen Genehmigung abhängig machen. Dem wird entsprochen, indem das Genehmigungserfordernis des geltenden Signaturgesetzes für gesetzeskonforme Zertifizierungsdienste entfällt (vgl. § 4 SigG-E). Artikel 3 Abs. 2 EGSRL sieht statt dessen die Schaffung eines geeigneten Systems zur Überwachung vor. Diese Regelung wird durch die Aufnahme von Vorschriften zur Aufsicht (vgl. §§ 4, 19 und 20 SigG-E) und durch Bußgeldvorschriften (vgl. § 21 SigG-E) umgesetzt.

Artikel 3 Abs. 2 EGSRL sieht für die Mitgliedstaaten als eine Option zur Steigerung des Niveaus der erbrachten Zertifizierungsdienste vor, freiwillige Akkreditierungssysteme einzuführen bzw. beizubehalten. Die freiwillige Akkreditierung wird im § 15 SigG-E geregelt, um den eingeführten und anerkannten Sicherheitsstandard nach dem geltenden Signaturgesetz als Option für den Markt weiterhin anzubieten und zu erhalten.

Artikel 3 Abs. 7 EGSRL sieht darüber hinaus als Option für die Mitgliedstaaten vor, den Einsatz elektronischer Signaturen im öffentlichen Bereich zusätzlichen Anforderungen zu unterwerfen. Diese Möglichkeit wird im Gesetzentwurf aufgegriffen und es wird in § 15 Abs. 2 SigG-E eine Referenzvorschrift für den Einsatz elektronischer Signaturen im öffentlichen Bereich geschaffen. Die einzig zulässige zusätzliche Anforderung für den öffentlichen Bereich nach dem SigG-E ist somit die des Verfahrens der freiwilligen Akkreditierung nach § 15 SigG-E, um eine einheitliche Verfahrensweise auch in diesem Bereich sicherzustellen.

Darüber hinaus werden die Vorschriften für die Prüfung der Sicherheit von Produkten für elektronische Signaturen an Artikel 3 Abs. 3 bis 5 EGSRL angepasst (vgl. § 17 Abs. 4 SigG-E).

Artikel 4 EGSRL sieht die Einhaltung der Binnenmarktgrundsätze für die Bereitstellung von Zertifizierungsdiensten und Produkten für elektronische Signaturen vor. In § 23 SigG-E wird die Anerkennung der Zertifizierungsdienste und Produkte für elektronische Signaturen aus anderen EU-Staaten und Vertragsstaaten aus dem Europäischen Wirtschaftsraum sowie aus Drittstaaten geregelt.

Die zentrale Vorschrift der Richtlinie beinhaltet Artikel 5 Abs. 1. Darin wird die Rechtswirkung elektronischer Signaturen geregelt. Die Mitgliedstaaten haben danach dafür Sorge zu tragen, dass fortgeschrittene elektronische Signaturen, die (zusätzlich) die Voraussetzungen der Anhänge I bis III der Richtlinie erfüllen, die rechtlichen Anforderungen an eine Unterschrift in bezug auf elektronische Daten in gleicher Weise wie handschriftliche Unterschriften in bezug auf Daten in Papierform erfüllen und im Gerichtsverfahren als Beweismittel zugelassen sind. Diese Signaturen werden im Gesetz mit „qualifizierte elektronische Signaturen" bezeichnet (vgl. § 2 Nr. 3 SigG-E). Die Bezeichnung erfolgt in Anlehnung an das für diese Signaturen erforderliche qualifizierte Zertifikat. Wie bereits im geltenden Signaturgesetz werden im Gesetzentwurf lediglich die Anforderungen an die Sicherheitsinfrastruktur für qualifizierte elektronische Signaturen mit Rechtswirkung geregelt, nicht die Rechtswirkung selbst. Die Regelung der Rechtswirkung qualifizierter elektronischer Signaturen ist Gegenstand des Entwurfes eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr, der von der Bundesregierung gesondert in den Bundestag eingebracht wird. Dieser Gesetzentwurf sieht die Schaffung eines § 126 a für das BGB vor, der - im Einklang mit der Richtlinie - die Möglichkeit der Ersetzung der Schriftform durch die „elektronische Form" vorsieht, sofern das elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen ist. Entsprechende Änderungen der Formvorschriften im Bereich des öffentlichen Rechts werden zur Zeit von der Bundesregierung vorbereitet.

Der nach Artikel 5 Abs. 1 Buchst. b) und Abs. 2 EGSRL geforderten Zulassung elektronischer Signaturen als Beweismittel vor Gericht wird bereits durch den geltenden Rechtsgrundsatz der freien Beweiswürdigung der Gerichte entsprochen. Der erforderliche Schutz des Erklärungsempfängers soll im übrigen prozessrechtlich durch das Institut des Beweises des ersten Anscheins gewährleistet werden, das im

Gesetzentwurf zur Anpassung der Formvorschriften für die Frage der Echtheit einer in elektronischer Form nach § 126 a BGB-E abgegebenen Willenserklärung durch spezialgesetzliche Regelung in der ZPO (§ 292 a ZPO-E) ausdrücklich kodifiziert wird. Weitere technische Anpassungen der Regelungen der ZPO an die elektronische Form sind im genannten Gesetz vorgesehen.

Da die Richtlinie im Kern nur verbindliche Vorgaben für elektronische Signaturen nach Artikel 5 Abs. 1 EGSRL enthält, die im SigG-E mit dem Begriff „qualifizierte elektronische Signaturen" abgebildet sind, ist in § 1 Abs. 2 SigG-E klargestellt, dass im übrigen die Verwendung aller elektronischer Signaturen freigestellt ist, soweit nicht durch Rechtsvorschrift etwas anderes vorgeschrieben ist.

Artikel 6 EGSRL sieht Regelungen zur Haftung der Zertifizierungsdiensteanbieter vor. Das geltende Signaturgesetz enthält keine Haftungsregelungen; es gilt das allgemeine Haftungsrecht. Die Regelungen der Richtlinie werden in §§ 11 und 12 SigG-E umgesetzt. Die über die Mindestanforderungen der Richtlinie hinausgehende Haftungsregelung entspricht zugleich den Forderungen des Bundesrates bei der parlamentarischen Beratung des Signaturgesetzes (Bundesrats-Drucksache 420/97 (Beschluss)) und greift die Feststellungen des IuKDG-Berichts der Bundesregierung (BT-Drs. 14/1191) hierzu auf.

Den Datenschutzregelungen nach Artikel 8 EGSRL wird durch § 14 SigG-E entsprochen. Die Regelungen der Richtlinie zum Datenschutz gelten auch für Zertifizierungsdiensteanbieter, die andere als qualifizierte Zertifikate ausstellen. Der materielle Regelungsbereich des Signaturgesetzes wird daher beim Datenschutz entsprechend erweitert (vgl. § 14 Abs. 3 SigG-E). Aufgenommen wird außerdem eine Pflicht des Zertifizierungsdiensteanbieters zur Aufdeckung der Identität bei Verwendung von Pseudonymen im Rahmen der Durchsetzung von zivilrechtlichen Ansprüchen.

Artikel 9 der Richtlinie regelt die Einsetzung eines Ausschusses, der einheitliche technische Anforderungen der Richtlinie präzisieren sowie Normen und Kriterien festlegen soll. Der Gesetzentwurf ist so technologieoffen ausgestaltet, dass die Ergebnisse des Ausschusses über die noch anzupassende Signaturverordnung (vgl. § 24 SigG-E) umgesetzt werden können.

Die Richtlinie sieht darüber hinaus eine Überprüfung der Durchführung der Richtlinie bis zum 19. Juli 2003 vor.

2. Umsetzung der Erfahrungen aus der Evaluierung des Signaturgesetzes

Der Deutsche Bundestag hat anläßlich der Verabschiedung des IuKDG-Berichts die Bundesregierung aufgefordert, (auch) die Entwicklung digitaler Signaturen zu beobachten und aufgrund gemachter Erfahrungen ggf. vorzunehmende Änderungen und Ergänzungen vorzuschlagen; dabei war insbesondere die Frage der Haftung der Zertifizierungsdiensteanbieter gegenüber Dritten zu beobachten. Außerdem waren die Impulse der digitalen Signaturen für das bürgerliche Recht, das Zivilprozeßrecht und das öffentliche Recht im Bericht der Bundesregierung zu berücksichtigen.

Am 18. Juni 1999 hat die Bundesregierung den IuKDG-Bericht dem Deutschen Bundestag vorgelegt. Der Bericht nimmt Anregungen der betroffenen Kreise im Hinblick auf die Erfahrungen mit dem Gesetz auf und schlägt vor allem rechtstechnische Verbesserungen für das geltende Gesetz vor. Vor dem Hintergrund der zum Berichtszeitpunkt noch nicht verabschiedeten Richtlinie stellt der IuKDG-Bericht fest, dass diese Änderungen bei der Umsetzung der Richtlinien berücksichtigt werden sollen.

Es werden folgende Änderungsanregungen aus der Evaluierung in den Gesetzentwurf aufgenommen, die im Einklang mit der Richtlinie stehen bzw. die von der Richtlinie gewährten Freiräume für die Umsetzung nutzen:

- Klarstellung, dass das Gesetz die Möglichkeit einer Verlagerung von Aufgaben der Zertifizierungsdiensteanbieter auf Dritte bietet (vgl. § 4 Abs. 5 SigG-E),
- Schaffung einer klaren gesetzlichen Grundlage für die Anerkennung von Prüf- und Bestätigungsstellen (vgl. § 18 SigG-E),
- Aufgreifen von Anregungen der Berufskammern hinsichtlich der Ausstellung und Sperrung von Zertifikaten mit Angaben über berufsrechtliche Zulassungen (vgl. § 5 Abs. 2 und § 8 Abs. 2 SigG-E) sowie bezüglich der Verwendung von Pseudonymen (vgl. § 5 Abs. 3 SigG-E).

Dem Wunsch des Deutschen Bundestages und des Bundesrates nach Aufnahme einer spezifischen Haftungsregelung für Zertifizierungsdiensteanbieter gegenüber Dritten wird im Ergebnis durch die Aufnahme einer entsprechenden Haftungsregelung Rechnung getragen.

3. Weitere Regelungen

Darüber hinaus enthält der Gesetzentwurf im wesentlichen folgende Änderungen gegenüber dem geltenden Signaturgesetz:

- technologieneutrale Anforderungen an Zeitstempel, so dass auch Verfahren ohne Signatur möglich sind (vgl. § 2 Nr. 14 SigG-E), und Lockerung der geltenden Regelung zu Zeitstempeldiensten dahingehend, dass die Ausstellung von qualifizierten Zeitstempeln von einer Pflichtdienstleistung zu einer Wahldienstleistung wird (vgl. § 9 SigG-E),
- Erweiterung der Unterrichtungspflicht für Zertifizierungsdiensteanbieter nach geltendem Signaturgesetz über die Rechtswirkung von qualifizierten elektronischen Signaturen im Rechtsverkehr (vgl. § 6 Abs. 2 SigG-E),
- Bestandsschutzregelung für Unternehmen, die Leistungen oder Produkte nach dem geltenden Signaturgesetz anbieten (vgl. § 25 SigG-E).

Schließlich enthält der Gesetzentwurf die notwendigen Regelungen zur Umstellung von Vorschriften von Deutscher Mark auf Euro (vgl. Art. 2 SigG-E), zur Anpassung von Bundesrecht, das auf das geltende Signaturgesetz verweist (vgl. Art. 3 SigG-E), die Ermächtigung zur Änderung von Rechtsverordnungen (Rückkehr zum einheitlichen Verordnungsrang, vgl. Art. 4 SigG-E) und zum Inkrafttreten des Gesetzes (vgl. Art. 5 SigG-E).

B. Zu den einzelnen Bestimmungen

Zu Artikel 1
Änderung des Signaturgesetzes

Zur Bezeichnung des Gesetzes

Die Bezeichnung des Gesetzes wird an die Terminologie und Zielsetzung der Richtlinie angepasst.

Zu § 1

Zu Absatz 1

Absatz 1 bildet den Regelungszweck und die Reichweite der Richtlinie ab (Art. 1 EGSRL). Der Regelungsbereich des Signaturgesetzes wird gemäß Artikel 1 EGSRL auf alle elektronische Signaturen ausgedehnt.

Im Kern werden entsprechend der Richtlinie nur die materiellen Anforderungen an „qualifizierte elektronische Signaturen", an die nach Artikel 5 Abs. 1 EGSRL unmittelbare Rechtswirkungen geknüpft werden, geregelt. Darüber hinausgehende materielle Anforderungen betreffen nur die speziellen Datenschutzbestimmungen in § 14 Abs. 3 SigG-E, die auch diejenigen Zertifizierungsdiensteanbieter erfassen, die keine qualifizierten Zertifikate ausstellen.

Zu Absatz 2

Absatz 2 greift auf die bisherige Regelung nach § 1 Abs. 2 SigG zurück. Die Vorschrift macht deutlich, dass auch im Rahmen des SigG-E die Anwendung von elektronischen Signaturen, die nicht den materiellen Anforderungen des SigG-E entsprechen, freigestellt ist. Diese Klarstellung ist erforderlich, da das Signaturgesetz – wie zu Absatz 1 ausgeführt – im Kern nur die materiellen Anforderungen an „qualifizierte

elektronische Signaturen" und die durch die Richtlinie hierfür vorgegebenen Sicherheitsinfrastrukturen regelt.

Es bedarf daher auch keiner gesetzlichen Regelung für elektronische Signaturen, die ausschließlich in Systemen verwendet werden, die auf freiwilligen privatrechtlichen Vereinbarungen zwischen einer bestimmten Anzahl von Teilnehmern beruhen. Das SigG-E folgt auch insoweit der Richtlinie (vgl. Erwägungsgrund Nummer 16 EGSRL). Allerdings dürfen die Zertifikate und Zeitstempel in den Fällen, in denen den Anforderungen des Signaturgesetzes nicht vollständig entsprochen wird, nicht das Merkmal „qualifiziert" erhalten.

Unverändert gegenüber der bisherigen Regelung im § 1 Abs. 2 SigG gilt auch für diese Vorschrift, dass der Gesetzentwurf nicht die Anwendung von elektronischen Signaturen regelt; geregelt werden nur deren Sicherheit und die damit zusammenhängenden Fragen.

Zu § 2

Die Begriffsbestimmungen werden an Artikel 2 EGSRL angepasst.

Zu Nummer 1

Die Definition entspricht Artikel 2 Nr. 1 EGSRL. Sie bringt den technologieneutralen Ansatz der Richtlinie zum Ausdruck und ist mit keinen weiteren Sicherheitsanforderungen verbunden. Eine eingescannte Unterschrift kann z. B. genügen, um als elektronische Signatur zu gelten, auch wenn damit keinerlei Sicherheitswert verbunden ist, da die gescannte Unterschrift kopiert und unter beliebig viele andere elektronische Dokumente gesetzt werden kann.

Zu Nummer 2

Die Definition entspricht Artikel 2 Nr. 2 EGSRL. Es wird lediglich der in § 2 Nr. 2 SigG-E definierte Begriff „Signaturschlüssel-Inhaber" an Stelle der Bezeichnung „Unterzeichner" verwendet. Für Buchstabe c) wird an Stelle des Begriffs „erstellt" der treffendere Begriff

„erzeugt" verwendet; der Begriff „Erzeugung" wird auch in Anhang III Nr. 1 Buchst. a) EGSRL verwendet.

Für fortgeschrittene elektronische Signaturen gelten nach der Richtlinie und nach dem Gesetzentwurf nur die in der Definition enthaltenen Anforderungen. Sie unterliegen damit höheren Anforderungen als (einfache) elektronische Signaturen, erfüllen jedoch nicht die Anforderungen an digitale Signaturen nach dem geltenden Signaturgesetz oder die Anforderungen, die durch Artikel 5 Abs. 1 EGSRL für die Anerkennung im Rechtsverkehr vorgegeben werden. So reicht beispielsweise die Nutzung der frei verfügbaren Implementierungen von Pretty Good Privacy (PGP), die aus dem Netz heruntergeladen werden können und bei denen die Signaturschlüssel auf Diskette, Festplatte des PC und auf andere lesbare Datenträger gespeichert werden können, aus, um den Anforderungen an eine fortgeschrittene elektronische Signatur zu genügen. Die fortgeschrittenen elektronischen Signaturen stellen damit eine „Zwischenstufe" im Verhältnis zu den (einfachen) elektronischen Signaturen und den qualifizierten elektronischen Signaturen dar. Die Definition aus der Richtlinie wird übernommen, um auch insoweit der Richtlinie zu entsprechen und gleichzeitig diese Zwischenstufe für den Anwender transparent zu machen.

Buchstabe a) bedeutet, dass ein Zertifizierungsdiensteanbieter denselben Signaturschlüssel nicht mehreren Personen zuordnen darf. Die Vorschrift bezieht sich nur auf den jeweiligen Zertifizierungsdiensteanbieter, da im Rahmen der Globalisierung ein genereller Abgleich mit allen Zertifizierungsdiensteanbietern mit einem unvertretbaren Aufwand verbunden wäre.

Buchstabe b) bringt die Funktion der Authentizität zum Ausdruck. Die Identifizierung des Signaturschlüsselinhabers ist über das der Signatur zugrundeliegende Zertifikat möglich.

Buchstabe c) bringt zum Ausdruck, dass der Signaturschlüssel-Inhaber seine Signaturerstellungseinheit vor unbefugter Nutzung schützen können muss.

Buchstabe d) verlangt, dass bei Daten, die mit einer fortgeschrittenen elektronischen Signatur signiert sind, eine nachträgliche Veränderung erkennbar sein muss.

Zu Nummer 3

Nummer 3 verbindet die fortgeschrittene elektronische Signatur nach Nummer 2 mit den weiteren nach Artikel 5 Abs. 1 EGSRL vorgesehenen Anforderungen. Die Richtlinie verwendet für die elektronische Signatur nach Artikel 5 EGSRL keine besondere Bezeichnung. Die Richtlinie spricht von „fortgeschrittenen elektronischen Signaturen", die (zusätzlich) auf einem qualifizierten Zertifikat (Anhang I EGSRL) beruhen und die von einer sicheren Signaturerstellungseinheit (Anhang III EGSRL) erstellt wurden. Die Anforderungen an die Ausstellung qualifizierter Zertifikate sind in Anhang II EGSRL geregelt.

Die fortgeschrittenen elektronischen Signaturen, die die Zusatzanforderungen des Artikel 5 Abs. 1 EGSRL erfüllen, erhalten im SigG-E die Bezeichnung „qualifizierte elektronische Signaturen". Die Bezeichnung erfolgt in Anlehnung an das für diese elektronischen Signaturen erforderliche qualifizierte Zertifikat. Eine qualifizierte elektronische Signatur ist somit in richtlinienkonformer Auslegung eine fortgeschrittene elektronische Signatur, die zusätzlich die Anforderungen des Artikel 5 Abs. 1 i.V.m. den Anhängen I bis III der Richtlinie erfüllt. Die Definition nach Nummer 3 entspricht Artikel 5 Abs. 1 EGSRL. Bezüglich des qualifizierten Zertifikates erfolgt eine Präzisierung dahingehend, dass es zum Zeitpunkt der Erzeugung der qualifizierten elektronischen Signatur gültig gewesen sein muss (vgl. Buchstabe a)). Andernfalls besteht die Möglichkeit, dass es zu diesem Zeitpunkt noch nicht ausgestellt oder dass die Gültigkeitsdauer bereits abgelaufen oder dass es gesperrt war.

Zu Nummer 4

Die Definition entspricht Artikel 2 Nummer 4 EGSRL. Es wird jedoch an Stelle des Begriffs „Signaturerstellungsdaten" die Bezeichnung „Signaturschlüssel" des geltenden SigG beibehalten. Im Interesse einer Präzisierung der Vorschrift wird das Beispiel "Codes" nicht übernommen, da es hinsichtlich der geforderten Einmaligkeit der Signaturschlüssel eine Unschärfe darstellt. Mit der Formulierung „elektronische Daten" und der nur beispielhaften Aufzählung („...wie kryptographische Daten...") bleibt die Vorschrift für alle technischen Lösungen offen.

Zu Nummer 5

Die Definition entspricht Artikel 2 Nr. 7 EGSRL. Es wird jedoch – in Anlehnung an die Bezeichnung „öffentlicher Schlüssel" im geltenden Signaturgesetz und in Anpassung an den Begriff „Signaturschlüssel" nach Nummer 4 - an Stelle des Begriffs „Signaturprüfdaten" der Richtlinie im SigG-E die Bezeichnung „Signaturprüfschlüssel" gewählt. Anhand des Signaturprüfschlüssels kann der Empfänger einer elektronischen Signatur nachprüfen, ob die signierten Daten vom Signaturschlüssel-Inhaber stammen und unverändert sind. Im Interesse einer Präzisierung der Vorschrift wird - wie bei der Definition des Signaturschlüssels (vgl. Nummer 4) - das Beispiel „Codes" nicht übernommen.

Zu Nummer 6

Die Definition entspricht Artikel 2 Nr. 9 EGSRL. Im Gegensatz zum qualifizierten Zertifikat nach Nummer 7, das Grundlage für die Abbildung der handschriftlichen Unterschrift ist, kann ein (einfaches) Zertifikat auch auf juristische Personen ausgestellt werden.

Zu Nummer 7

Die Definition entspricht Artikel 2 Nr. 10 EGSRL. Der Begriff „qualifizierte Zertifikate" umfasst auch „qualifizierte Attribut-Zertifikate" (vgl. § 7 Abs. 2 SigG-E).

Die Beschränkung der qualifizierten Zertifikate auf natürliche Personen ist durch die nach Artikel 5 Abs. 1 EGSRL vorgesehene rechtliche Gleichstellung der darauf beruhenden qualifizierten elektronischen Signaturen mit der handschriftlichen Unterschrift vorgegeben.

Zu Nummer 8

Die Definition entspricht Artikel 2 Nr. 11. Die in der Richtlinie enthaltene Bezeichnung „eine Stelle" ist durch die Formulierung „eine juristische oder natürliche Person" mit

umfasst. Der Begriff „Zertifizierungsstelle“ des geltenden SigG und der Begriff „Zertifizierungsdiensteanbieter“ im SigG-E decken sich.

Die Definition wird im übrigen dahingehend präzisiert, dass tatsächlich nur die Dienste der Zertifizierungsdiensteanbieter (nicht z.B. auch die Dienste der Prüf- und Bestätigungsstellen nach § 18 SigG-E) erfasst werden.

Die Definition erfasst alle Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate einschließlich Attribut-Zertifikate (vgl. § 7 Abs. 2 SigG-E) oder Zeitstempel mit dem Merkmal „qualifiziert“ ausstellen. Diese Zertifizierungsdiensteanbieter sind – mit Ausnahme der Vorschriften zum Datenschutz (§ 14 Abs. 3 SigG-E) - ausschließlich Adressat des SigG-E.

Ebenso wie die Richtlinie verzichtet das Gesetz auf eine gesonderte Definition von „Zertifizierungsdiensten“. Die Aufgaben der Zertifizierungsdienste werden aus der Definition „Zertifizierungsdiensteanbieter“ deutlich.

Die Ausstellung von Zertifikaten für technische Komponenten ist nicht Gegenstand dieses Gesetzes, mit Ausnahme der speziellen Vorschrift in § 16 Abs. 3 SigG-E zur Ausstellung von Zertifikaten für Authentisierungsschlüssel, die in Produkten für elektronische Signaturen verwendet werden.

Zu Nummer 9

Mit der Vorschrift wird Artikel 2 Nr. 3 EGSRL umgesetzt. An Stelle des in der Richtlinie verwendeten Begriffs "Unterzeichner" wird der Begriff „Signaturschlüssel-Inhaber“ aus dem geltenden Signaturgesetz (vgl. § 2 Abs. 1 und § 7 Abs. 1 Nr. 1 SigG) beibehalten, der den Begriff „Unterzeichner" umfasst, aber den Sachverhalt genauer trifft. Bei den meisten Vorschriften des Gesetzes ist der Normadressat nicht in der Funktion des Unterzeichners, sondern in der Funktion des Signaturschlüssel-Inhabers mit den damit verbundenen Rechten und Pflichten angesprochen.

Die Definition der (einfachen) „Signaturerstellungseinheit“ in Artikel 2 Nr. 5 EGSRL ist in die Definition der „sicheren Signaturerstellungseinheit“ eingegangen; ein Bedarf für eine gesonderte Definition im Signaturgesetz besteht nicht.

Zu Nummer 10

Die Definition entspricht Artikel 2 Nr. 6 EGSRL, präzisiert jedoch die „Implementierung der Signaturerstellungsdaten" durch die Formulierung „Speicherung und Anwendung von Signaturschlüsseln".

Zu Nummer 11

Mit der Vorschrift wird Artikel 2 Nr. 8 EGSRL umgesetzt. An die Stelle des Begriffs „Signaturprüfeinheit" in der Richtlinie wird jedoch der präzisere Begriff „Signaturanwendungskomponenten" verwendet, der alle Sicherheitsaspekte bei der Anwendung elektronischer Signaturen abdeckt.

Bei der Anwendung qualifizierter elektronischer Signaturen muss der Unterzeichner vor allem sicher sein können, dass er nur das signiert, was ihm angezeigt wird und was er signieren will. Er muss bei Bedarf auch den Inhalt der zu signierenden oder zu prüfenden signierten Daten feststellen können. Schließlich muss er die qualifizierten Zertifikate gemäß § 5 Abs. 1 Satz 2 SigG-E zuverlässig nachprüfen können.

Zu Nummer 12

Mit der Vorschrift wird Anhang II Buchst. f) EGSRL umgesetzt. Die dort genannten Systeme und Produkte („müssen vertrauenswürdige Systeme und Produkte einsetzen, die vor Veränderungen geschützt sind und die die technische und kryptographische Sicherheit der von ihnen unterstützten Verfahren gewährleisten") erhalten eine eigene Bezeichnung, um diese im Gesetz und in der Rechtsverordnung nach § 24 SigG-E deutlich adressieren zu können. In der Richtlinie sind diese zwar in Artikel 2 Nr. 12 („Produkt für elektronische Signaturen") definiert, jedoch nur im Kontext mit anderen Produkten.

Zu Nummer 13

Die Definition ist Artikel 2 Nr. 12 EGSRL nachgebildet. An Stelle der in der Richtlinie isoliert vorgenommenen Definition des Sammelbegriffs „Produkte für elektronische Signaturen" wird auf die vorhandenen Definitionen der einzelnen Produktarten nach den Nummern 10 – 12 zurückgegriffen.

Zu Nummer 14

Nummer 14 setzt Anhang II Buchst. c) EGSRL um. Um den dort genannten Anforderungen („müssen gewährleisten, dass Datum und Uhrzeit der Ausstellung oder des Widerrufs eines Zertifikates genau bestimmt werden können") Rechnung zu tragen, können Zeitstempel notwendig sein. Darüber hinaus sind Zeitstempel für elektronische Dokumente mit Zeitbezug (z.B. fristgerechte Einreichung von Unterlagen und Empfangsbestätigungen) generell von großer Bedeutung.

Bei der Definition wird auf § 2 Abs. 4 SigG zurückgegriffen. Der Begriff „Zeitstempel" erhält zur Unterscheidung von anderen, nicht im SigG-E geregelten Zeitstempeln den Zusatz „qualifiziert".

Die Definition wird zugleich technikneutraler gefasst, indem diese nicht mehr zwingend eine Signatur verlangt. Damit können neben der herkömmlichen technischen Lösung auch andere technische Verfahren zur Anwendung kommen, bei denen mehrere „Hash-Werte" (eine Art von Quersummen), z.B. des elektronischen Dokumentes, der Zeitangabe und des Zertifizierungsdienstes, verknüpft werden.

Zu Nummer 15

Die Definition entspricht - auf die Kernelemente der freiwilligen Akkreditierung reduziert - Artikel 2 Nr. 13 EGSRL.

Zu § 3

Die Vorschrift dient der Umsetzung von Artikel 3 Abs. 3 EGSRL. Sie greift auf die Regelung des § 3 SigG zurück. Da der zuständigen Behörde alle administrativen Aufgaben nach dem Signaturgesetz und der Signaturverordnung übertragen sind, wird die bisherige beispielhafte Aufzählung von Aufgaben durch eine Generalklausel ersetzt.

Zu § 4

Mit der Vorschrift wird Artikel 3 Abs. 1 EGSRL umgesetzt. Der im Signaturgesetz enthaltene Genehmigungsvorbehalt für gesetzeskonforme Zertifizierungsdiensteanbieter entfällt. Statt dessen wird gemäß Artikel 3 Abs. 3 EGSRL ein „geeignetes System zur Überwachung" eingeführt (vgl. §§ 19 und 20 SigG-E).

In § 4 SigG-E werden in Übereinstimmung mit Artikel 3 und Anhang II EGSRL die allgemeinen Anforderungen an Zertifizierungsdiensteanbieter geregelt. Die speziellen Anforderungen an Zertifizierungsdiensteanbieter nach Anhang II EGSRL sind in den §§ 5 bis 14 SigG-E enthalten, die in der Rechtsverordnung nach § 24 SigG-E näher ausgeführt werden.

Zu Absatz 1

Mit dieser Vorschrift wird Artikel 3 Abs. 1 EGSRL umgesetzt. Die Vorschrift stellt die allgemeine Handlungs- und Gewerbefreiheit (Artikel 2, 12 GG) auch für Zertifizierungsdiensteanbieter klar. Durch die Formulierung „im Rahmen der Gesetze" wird deutlich gemacht, dass sonstige Genehmigungserfordernisse des allgemeinen Rechts, etwa gewerberechtlicher oder wirtschaftsrechtlicher Art oder nach dem Telekommunikationsrecht, unberührt bleiben.

Zu Absatz 2

Mit dieser Vorschrift wird Anhang II EGSRL umgesetzt. Sie enthält die allgemeinen Anforderungen an Zertifizierungsdiensteanbieter, die in den folgenden Vorschriften des

Gesetzes und in der Rechtsverordnung nach § 24 SigG-E näher ausgeführt werden. Die Regelung des Satzes 1 ist bußgeldbewehrt (vgl. § 21 Abs. 1 Nr. 1 SigG-E).

Zu Absatz 3

Das nach Artikel 3 Abs. 3 EGSRL vorgesehene Überwachungs- bzw. Aufsichtssystem (vgl. §§ 19 und 20 SigG-E) macht es erforderlich, dass der Betrieb eines Zertifizierungsdienstes bei der zuständigen Behörde angezeigt und durch den Zertifizierungsdiensteanbieter dargelegt wird, dass die Anforderungen des Signaturgesetzes erfüllt sind. Die Regelung des Satzes 1 ist bußgeldbewehrt (vgl. § 21 Abs. 1 Nr. 2 SigG-E).

Die Anzeige muss spätestens mit der Betriebsaufnahme erfolgen, damit die zuständige Behörde bei Nichterfüllung der gesetzlichen Vorgaben rechtzeitig gemäß § 19 SigG-E tätig werden kann.

Die Darlegungspflicht nach Satz 2 bezieht sich auf die Vorlage der Nachweise für die Zuverlässigkeit (z.B. Auszüge aus dem Bundeszentralregister), Fachkunde (z.B. Zeugnisse) und Deckungsvorsorge (z.B. Versicherungspolice, Bankbürgschaft) sowie die Vorlage des Sicherheitskonzeptes mit einer Erläuterung der praktischen Umsetzung. Aus dem Sicherheitskonzept muss insbesondere hervorgehen, dass die eingesetzten Produkte für elektronische Signaturen und deren Implementierung sowie die Ablauforganisation des Zertifizierungsdiensteanbieters den Anforderungen des Signaturgesetzes und der Rechtsverordnung nach § 24 SigG-E entsprechen.

Zu Absatz 4

Die Vorschrift stellt klar, dass die nach Anhang II EGSRL vorgegebenen Anforderungen an die Sicherheit über die gesamte Dauer des Betriebs des Zertifizierungsdienstes aufrechterhalten werden müssen.

Zu Absatz 5

Diese Vorschrift greift die im Rahmen der Evaluierung des Signaturgesetzes erhobene Forderung nach einer Präzisierung der Reichweite des Begriffs „Zertifizierungsstelle" (jetzt: „Zertifizierungsdiensteanbieter") auf. Im Kern geht es um die rechtswissenschaftliche Diskussion, ob und inwieweit das geltende Signaturgesetz die Möglichkeit bietet, Aufgaben des Zertifizierungsdiensteanbieters auf Dritte auszulagern. Mit der Regelung in Absatz 5 wird klargestellt, dass eine Übertragung von Aufgaben des Zertifizierungsdiensteanbieters an Dritte zulässig ist. Dritte sind alle, die Teilaufgaben eines Zertifizierungsdiensteanbieters übernehmen können, wie z. B. Unternehmen, Behörden, Berufskammern, privatwirtschaftliche oder kommunale Träger. Die Richtlinie steht einer Übertragung von Aufgaben des Zertifizierungsdiensteanbieters auf Dritte nicht entgegen.

Die Vorschrift räumt damit Zertifizierungsdiensteanbietern bei ihrer innerbetrieblichen Organisation richtlinienkonform ausdrücklich einen großen Gestaltungsspielraum ein, soweit die Einhaltung der gesetzlichen Vorgaben gewährleistet bleibt. Ihre Gesamtverantwortung für den Betrieb des Zertifizierungsdienstes und ihre Haftung bleiben von der möglichen Aufgabenübertragung an Dritte unberührt (vgl. auch § 11 Abs. 4 SigG-E).

Zu § 5

Mit der Vorschrift wird Anhang II EGSRL umgesetzt, dies gilt insbesondere für die Buchstaben b), d), f), g), j) und l). Die Vorschrift greift auf § 5 SigG zurück.

Zur Überschrift

Redaktionelle Anpassung an die neuen Begriffe in § 2 SigG-E.

Zu Absatz 1

Neben redaktionellen Anpassungen an die neuen Begriffe in § 2 SigG-E beinhaltet die Vorschrift durch Wahl des Begriffes „Kommunikationsverbindungen" einen technologieoffenen Ansatz, der heutige und künftige Formen der Online-Kommunikation erfasst (im Vergleich zur engeren Regelung des geltenden Signaturgesetzes, das lediglich von „Telekommunikationsverbindungen" spricht).

Die Regelungen der Sätze 1 bis 3 sind bußgeldbewehrt (vgl. § 21 Abs. 1 Nr. 3 bis 5 SigG-E).

Zu Absatz 2

Mit den Änderungen gegenüber dem geltenden Signaturgesetz wird einem wesentlichen Anliegen vor allem der Berufskammern, das im Rahmen der Evaluierung des Signaturgesetzes vorgebracht wurde, entsprochen. Die Richtlinie lässt den Mitgliedstaaten bei der Umsetzung im Hinblick auf die „spezifischen Attribute der Person" in Anhang II Buchst. d) ausdrücklich einen weiten Spielraum („..mit geeigneten Mitteln nach einzelstaatlichem Recht...").

Zunächst erfolgt mit der gegenüber dem geltenden Signaturgesetz vorgenommenen Erweiterung auf „berufsbezogene oder sonstige Angaben" eine Öffnung, so dass alle potenziell relevanten Angaben zu einer Person, z.B. Zugehörigkeit zu einer Institution, Aufgabenbereich, Berufsbezeichnung, berufsrechtliche Zulassungen, in ein Zertifikat aufgenommen werden können.

Vor allem aber wird die „Einwilligung", die in der bisherigen Regelung des § 5 Abs. 2 SigG lediglich bei der Aufnahme von Angaben über Vertretungsrechte für eine dritte Person in ein qualifiziertes Zertifikat vorgesehen ist, künftig auch als „Bestätigung" seitens der für berufsbezogene oder sonstige Angaben zur Person zuständigen Stellen (z.B. Berufskammern) verlangt. Eine aktuelle Bestätigung ist erforderlich, um zu verhindern, dass überholte, zum aktuellen Zeitpunkt unzutreffende Angaben zu einer Person in ein qualifiziertes Zertifikat aufgenommen werden. Zugleich erhalten die

register- und berufsaufsichtsführenden Stellen durch das konkrete Bestätigungserfordernis die Informationen über Zertifizierungsvorgang und Zertifizierungsdienst, die sie zur Geltendmachung ihrer Rechte nach § 8 Abs. 2 SigG-E benötigen.

Berufsbezogene Angaben können von verschiedenen Stellen (z.B. von Arbeitgebern, Zulassungsstellen oder registerführenden Stellen) kommen. Während es den Arbeitgebern - im Rahmen der Gesetze - grundsätzlich in deren freies Ermessen gestellt bleibt, ob sie die berufsbezogenen Angaben für ein Zertifikat bestätigen, müssen die für berufsrechtliche Zulassungen oder das Führen von Berufsregistern zuständigen Stellen im Rahmen ihrer pflichtgemäßen Aufgabenerfüllung (gebundenes Ermessen) bei Vorliegen der Voraussetzungen die Angaben bestätigen. Dies gilt nicht, sofern bei Verwendung eines Pseudonyms berechtigte Interessen entgegenstehen (vgl. Absatz 3 Satz 2). Die Regelung des Satzes 3 wurde zum Zwecke der Möglichkeit einer Bußgeldbewehrung aufgenommen; auch Satz 4 ist bußgeldbewehrt (vgl. dazu § 21 Abs. 1 Nr. 6 SigG-E).

Satz 4 greift auf die bisherige Regelung in § 7 Abs. 3 SigG zurück. Er wird wegen des Sachzusammenhangs an dieser Stelle eingefügt.

Zu Absatz 3

Satz 1 wird redaktionell an die neuen Begriffe in § 2 SigG-E angepasst.

Mit dem neuen Satz 2 wird einem weiteren Wunsch der Berufskammern im Rahmen der Evaluierung des Signaturgesetzes entsprochen, die Bedenken äußerten, dass ein qualifiziertes Zertifikat mit Angaben über eine berufsrechtliche Zulassung auf ein Pseudonym ausgestellt werden und dadurch das Vertrauen in die berufsrechtliche Zulassung erschüttert werden könnte. Mit der neuen Regelung wird z.B. den Ärztekammern die Möglichkeit eingeräumt, auszuschließen, dass Ärzte medizinische Leistungen unter einem Pseudonym anbieten. Eine solche Regelung ist im Hinblick auf den weiten Spielraum, den die Richtlinie hinsichtlich der spezifischen Attribute zur Person lässt (vgl. Anhang II Buchst. d) EGSRL), auch richtlinienkonform.

Zu Absatz 4

Die redaktionelle Anpassung in dieser Vorschrift berücksichtigt, dass der im geltenden Signaturgesetz in Satz 3 verwendete Zusatz „privater" Signaturschlüssel infolge der Definition des Begriffs „Signaturschlüssel" in § 2 Nr. 4 SigG-E, die den Begriff „privat" umfasst, entbehrlich ist.

Mit der Änderung von Satz 2 gegenüber dem geltenden Signaturgesetz wird klargestellt, dass jede Speicherung eines Signaturschlüssels außerhalb der jeweiligen sicheren Signaturerstellungseinheit (beim Zertifizierungsdienst oder anderswo) unzulässig ist. Während sich Satz 2 dieser Vorschrift an die Zertifizierungsdiensteanbieter richtet (sofern diese Signaturschlüssel bereitstellen), betrifft die gleichlautende Vorschrift in § 17 Abs. 3 Nr. 1 SigG-E die technischen Komponenten für Zertifizierungsdienste bzw. deren Hersteller. Die Regelungen der Sätze 2 und 3 sind bußgeldbewehrt (vgl. § 21 Abs. 1 Nr. 7 und 8 SigG-E).

Zu Absatz 5

Die Regelung greift auf § 5 Abs. 5 SigG zurück und passt die dortigen Anforderungen an die Begriffsbestimmung nach § 2 Nr. 13 SigG-E an.

Zu Absatz 6

Mit der Vorschrift wird Artikel 5 Abs. 1 EGSRL entsprochen. Sie soll ausschließen, dass ein qualifiziertes Zertifikat für einen Signaturschlüssel ausgestellt wird, der sich nicht auf einer sicheren Signaturerstellungseinheit befindet.

Bei einer Signatur, die mit einer nicht-sicheren Signaturerstellungseinheit (z.B. nicht auf einer sicheren Chipkarte) erstellt wurde, kann nicht ausgeschlossen werden, dass Unbefugte durch Hacking, „trojanische Pferde" oder andere Angriffe an den Signaturschlüssel gelangen. Mit einem Duplikat des Signaturschlüssels könnten sie dann beliebig gefälschte Signaturen erzeugen, die von den Signaturen des rechtmäßigen Signaturschlüssel-Inhabers nicht zu unterscheiden wären.

Die Verpflichtung des Zertifizierungsdiensteanbieters, sich gemäß Absatz 6 zu überzeugen, gilt unabhängig davon, ob er die sichere Signaturerstellungseinheit bereitstellt oder ob der Signaturschlüssel-Inhaber diese von anderer Seite erworben hat. Der Zertifizierungsdiensteanbieter hat sich sowohl davon zu überzeugen, dass es sich um eine sichere Signaturerstellungseinheit handelt (z.B. anhand eines Authentisierungsmerkmales des Herstellers), als auch davon, dass diese den zugehörigen Signaturschlüssel zu dem im Zertifikat aufgeführten Prüfschlüssel enthält. Dieser Vorgang muss spätestens abgeschlossen sein, wenn das qualifizierte Zertifikat gemäß Absatz 1 Satz 2 öffentlich nachprüfbar ist. Ist für einen Signaturschlüssel bereits ein gültiges qualifiziertes Zertifikat vorhanden, so muss der Zertifizierungsdiensteanbieter sich bei der Ausstellung weiterer Zertifikate für diesen Schlüssel nicht erneut überzeugen.

Zu § 6

Mit der Vorschrift wird Anhang II Buchst. k) EGSRL umgesetzt. Sie greift auf § 6 SigG zurück.

Zu Absatz 1

Neben redaktionellen Anpassungen an die neuen Begriffsbestimmungen in § 2 SigG-E entfällt Satz 2 des geltenden § 6 SigG, da die dortige Regelung bereits von Satz 1 umfasst wird. Unabhängig von dieser rechtstechnischen Änderung ist eine Unterrichtung der Signaturschlüssel-Inhaber über Signaturanwendungskomponenten aus Gründen des Vertrauensschutzes zwingend erforderlich, da andernfalls die Gefahr besteht, dass ungewollt qualifizierte elektronische Signaturen erzeugt werden, z.B. durch Unterschieben elektronischer Dokumente zur Erzeugung einer Signatur. Die näheren Einzelheiten bleiben der Rechtsverordnung vorbehalten (vgl. § 24 Nr. 1 SigG-E).

Zu Absatz 2

Absatz 2 erweitert die Unterrichtungspflicht auf die Rechtswirkungen von mit qualifizierten elektronischen Signaturen versehenen Willenserklärungen. Sie bezieht

sich damit auf die Rechtsfolgen, die sich durch das vorgesehene Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr ergeben. Mit diesem Gesetz soll eine elektronische Form nach § 126 a BGB eingeführt werden, die bei Verwendung einer qualifizierten elektronischen Signatur die Schriftform nach § 126 BGB ersetzen kann. Der Antragsteller ist darüber zu informieren, dass eine qualifizierte elektronische Signatur die Rechtswirkung einer handschriftlichen Unterschrift hat und dass damit einer elektronisch signierten Erklärung erhöhte rechtliche Bedeutung beigemessen wird.

Durch die vorgeschriebene Unterrichtung wird ein Teil der mit der Schriftform bezweckten Warnfunktion auf den elektronischen Bereich übertragen. Dem Antragsteller ist eine schriftliche Belehrung auszuhändigen, deren Kenntnisnahme dieser gesondert zu unterschreiben hat. Das persönliche Erscheinen des Antragstellers ist für die Unterrichtung – einschließlich der Belehrung nach Satz 2 – nicht erforderlich; ein schriftliches Verfahren ist ausreichend. Die elektronische Form ist bei der erstmaligen Antragstellung ausgeschlossen. Bei einer erneuten Antragstellung (bei demselben oder einem anderen Zertifizierungsdienst) ist eine erneute Unterrichtung generell – auch die nach Absatz 2 – entbehrlich.

Diese Unterrichtung und die traditionelle Ausgestaltung (Schriftform) bei der erstmaligen Beantragung erscheint solange notwendig, bis sich die „elektronische Form" nach § 126a BGB-E im Rechts- und Geschäftsverkehr breit etabliert hat. Sie dient für eine Übergangszeit als Bindeglied zwischen der herkömmlichen Schriftform (mit ihren bekannten Funktionen) und der „elektronischen Form", die ein Äquivalent zu dieser bildet. Der durch die Belehrung den Beteiligten einmalig entstehende Aufwand ist im Hinblick auf die qualitativ tiefgreifenden Auswirkungen der Verwendung qualifizierter elektronischer Signaturen im Rechtsverkehr angemessen und vertretbar.

Zu § 7

Mit der Vorschrift wird Anhang I der Richtlinie umgesetzt. Sie greift auf § 7 SigG zurück.

Zur Überschrift

Redaktionelle Anpassung an die neuen Begriffe in § 2 SigG-E.

Zu Absatz 1

Absatz 1 verlangt für das Zertifikat eine qualifizierte elektronische Signatur. Diese Vorschrift setzt Anhang I Buchst. h) EGSRL unter Berücksichtigung der Vorgaben von Artikel 5 Abs. 1 EGSRL um. Signaturen mit einem geringen Sicherheitswert könnten nicht nur eine Fälschung der qualifizierten Zertifikate ermöglichen, sondern in der Folge auch eine Fälschung der darauf beruhenden qualifizierten elektronischen Signaturen.

Im übrigen wird die Vorschrift redaktionell an die neuen Begriffe in § 2 SigG-E angepasst und gemäss Anhang I EGSRL gegenüber dem geltenden § 7 SigG erweitert.

Nummer 6 wird entsprechend Anhang I Buchst. b) EGSRL ergänzt um den Zusatz „und des Staates, in dem er niedergelassen ist".

In Nummer 7 wird das Wort „und" durch das Wort „oder" ersetzt und damit klargestellt, dass die genannten Möglichkeiten der Beschränkung alternativ gelten.

Nummer 8 wird entsprechend Anhang II Buchst. a) EGSRL neu aufgenommen.

Nummer 9 wird entsprechend Anhang I Buchst. d) EGSRL neu aufgenommen. Es wird darin richtlinienkonform klargestellt, dass Attribute des Signaturschlüssel-Inhabers Teil des qualifizierten Zertifikates sind.

Zu Absatz 2

Mit der Vorschrift wird – wie bereits im geltenden SigG - der Tatsache Rechnung getragen, dass qualifizierte Attribut-Zertifikate im Rechts- und Geschäftsverkehr eine entscheidende Rolle spielen (z.B. bei Vertretungsrechten und berufsrechtlichen Zulassungen) und zunehmend an Bedeutung gewinnen werden.

Die Richtlinie macht eine Änderung des geltenden § 7 Abs. 2 SigG erforderlich. Zwar enthält die Richtlinie keine eigene Definition der Attribut-Zertifikate, wie im geltenden SigG, erwähnt jedoch sowohl in Anhang I Buchst. d) als auch in Anhang II Buchst. d) das „spezifische Attribut". In Anhang I Buchst. d) wird das spezifische Attribut als Bestandteil des qualifizierten Zertifikates („Platz für ein spezifisches Attribut..") definiert. Die gegenüber § 7 Abs. 2 SigG geänderte Vorschrift stellt richtlinienkonform klar, dass qualifizierte Attribut-Zertifikate von dem Begriff „qualifizierte Zertifikate" mit umfasst sind und enthält die notwendige spezielle Rahmenregelung für qualifizierte Attribut-Zertifikate.

Bei der Referenzierung von Attribut-Zertifikaten wird offengelassen, welche Angaben aus dem qualifizierten Zertifikat in das qualifizierte Attribut-Zertifikat übernommen werden, so dass die Angaben in qualifizierten Attribut-Zertifikaten an den Bedürfnissen der jeweiligen Nutzung des qualifizierten Zertifikates ausgerichtet werden können. Die näheren Einzelheiten bleiben der Rechtsverordnung nach § 24 SigG-E vorbehalten, da diese durch internationale Entwicklungen und die Ergebnisse des Ausschusses nach Artikel 9 EGSRL beeinflusst werden können. Die Richtlinie lässt den Mitgliedstaaten im übrigen einen großen Spielraum bei der Ausgestaltung der Regelungen zu Attributen (vgl. Anhang I Buchst. d) EGSRL).

Absatz 3 des geltenden Signaturgesetzes wird in § 5 Abs. 2 Satz 3 SigG-E aufgenommen.

Zu § 8

Mit der Vorschrift wird Anhang II Buchst. b) EGSRL umgesetzt. Sie greift auf § 8 SigG zurück.

Zur Überschrift

Redaktionelle Anpassung an die neuen Begriffe in § 2 SigG-E.

Zu Absatz 1

Neben redaktionellen Anpassungen an die neuen Begriffe in § 2 SigG-E wird in Umsetzung von Anhang II Buchst. b) EGSRL in Satz 1 vor den Worten „zu sperren" das Wort „unverzüglich" eingefügt. Weiter wird in Satz 1 zur Präzisierung das Wort „erwirkt" durch das Wort „ausgestellt" ersetzt. Das Wort „erwirkt" stellt darauf ab, dass absichtlich ein Zertifikat mit falschen Angaben herbeigeführt wurde; eine Sperrung soll jedoch auch möglich sein, wenn in ein Zertifikat irrtümlich falsche Angaben aufgenommen wurden.

Die Vorschrift in Satz 3 trägt den Erfahrungen im Rahmen der Evaluierung des Signaturgesetzes Rechnung. Wird in einem qualifizierten Zertifikat einer Person z.B. fälschlicherweise die Zulassung als Arzt bescheinigt und das Zertifikat erst einige Zeit später, nachdem dies festgestellt wurde, gesperrt, kann noch eine große Anzahl von zuvor signierten elektronischen Dokumenten im Umlauf sein. Erhält ein Dritter ein vor dem Zeitpunkt der Sperrung des Zertifikates signiertes elektronisches Dokument, wird er grundsätzlich von einer rechtmäßigen Signatur und zutreffenden Angaben im Zertifikat ausgehen. Um in solchen Fällen potenziellen Schaden nach Möglichkeit zu vermeiden, soll dem Zertifizierungsdiensteanbieter ausdrücklich das Recht eingeräumt werden, den Umstand, dass ein Zertifikat mit falschen Angaben ausgestellt wurde, z.B. in den Zertifikatverzeichnis-Auskünften (vgl. § 5 Abs. 1 Satz 2 SigG-E) kenntlich zu machen. Da das Kenntlichmachen des Umstandes vor allem im Interesse des für den korrekten Inhalt der Zertifikate haftenden Zertifizierungsdiensteanbieters liegt, soll es auch in dessen Ermessen gestellt sein.

Zu Absatz 2

Die Vorschrift wird an die Änderungen in § 5 Abs. 2 SigG-E angepasst. Sie greift vor allem die im Rahmen der Evaluierung des Signaturgesetzes geäußerten Petita der Berufskammern auf, nach der auch die für die berufsbezogenen Angaben zuständigen Stellen eine Sperrung veranlassen können sollen, wenn Zertifikate unzutreffende Angaben über Zulassungen aus ihrem Zuständigkeitsbereich enthalten. Mit der Vorschrift in Absatz 2 erhalten die für berufsbezogene oder sonstige Angaben zur Person zuständigen Stellen ausdrücklich das Recht eingeräumt, eine Sperrung der

betreffenden Zertifikate zu beantragen. Die Vorschrift nutzt den von der Richtlinie zugestandenen Freiraum für die Regelungen von Attributen zur Person (vgl. Anhang I Buchst. d) EGSRL). Unabhängig davon können die genannten Stellen Sperrungen im Rahmen ihrer Zuständigkeit und der geltenden Rechtsvorschriften auch aus anderen Gründen veranlassen; es wird hierzu auf die Ausführungen zu § 5 Abs. 2 verwiesen.

Absatz 3 des geltenden Signaturgesetzes wird in § 16 Abs. 1 Satz 3 SigG-E aufgenommen.

Zu § 9

Die Vorschrift setzt Anhang II Buchst. c) EGSRL um (vgl. Begründung zu § 2 Nr. 14 SigG-E). Sie greift auf § 9 SigG zurück.

Die Richtlinie umschreibt in Anhang II Buchst. c) nur abstrakt die Möglichkeit des Einsatzes von Zeitstempeln („..Datum und Uhrzeit der Ausstellung oder des Widerrufs eines Zertifikats.."), ohne diese als solche zu nennen oder deren Einsatz oder Funktion näher zu beschreiben. Hieraus ergibt sich, dass dieser Dienst nach der Richtlinie nicht zwingend Bestandteil des Leistungsumfanges eines Zertifizierungsdiensteanbieters ist. Deshalb erfolgt eine Änderung des geltenden § 9 SigG dahingehend, dass die Ausstellung von qualifizierten Zeitstempeln von einer Pflichtdienstleistung zu einer Wahldienstleistung wird. Damit wird zugleich die Möglichkeit eröffnet, gesetzeskonforme Zeitstempeldienste auch separat anzubieten.

Zu § 10

Mit der Vorschrift wird Anhang II Buchst. i) EGSRL umgesetzt. Sie greift auf § 10 SigG zurück.

Zu Absatz 1

Neben einer redaktionellen Anpassung von Satz 1 an die neuen Begriffe nach § 2 SigG-E werden die Sätze 2 und 3 neu angefügt.

Mit der Vorschrift in Absatz 1 wird den Anforderungen des Anhangs II Buchst. b) und i) EGSRL Rechnung getragen. Die Dokumentation kann im Streitfalle bei Gericht als wichtiges Beweismittel dienen. Dies gilt insbesondere, wenn öffentlich anerkannte fachkundige Dritte die Sicherheit geprüft und bestätigt haben (vgl. § 18 Abs. 2 Satz 2 SigG-E). Mit der Haftungsregelung nach § 11 Abs. 2 SigG-E und der Bußgeldvorschrift nach § 21 SigG-E kommt der Dokumentation zusätzliche Bedeutung zu. Die Regelung des Satzes 1 ist bußgeldbewehrt (vgl. § 21 Abs. 1 Nr. 9 SigG-E).

Den Vorschriften in Absatz 1 Satz 2 und 3 kann dadurch entsprochen werden, dass die Dokumentation organisatorisch getrennt und in elektronischer Form mit qualifiziertem Zeitstempel erfolgt. So können z.B. Telefonanrufe zwecks Sperrung von Zertifikaten und daraufhin durchgeführte Sperrungen an einer technisch und organisatorisch getrennten Stelle unter den datenschutzrechtlichen Voraussetzungen gespeichert und mit qualifizierten Zeitstempeln versehen werden.

Zu Absatz 2

Absatz 2 ist notwendige Folge des von der Richtlinie (vgl. Art. 3 Abs. 1) vorgegebenen Wegfalls des bisherigen Genehmigungsvorbehaltes für Zertifizierungsdienste (mit vorheriger Prüfung der Sicherheit). Die Vorschrift eröffnet dem Signaturschlüssel-Inhaber die Möglichkeit, sich von der Korrektheit der ihn betreffenden Daten und Verfahrensschritte (z.B. der unverzüglichen Durchführung einer beantragten Sperrung eines qualifizierten Zertifikates) zu überzeugen, ohne ein Gerichtsverfahren anstrengen zu müssen. Dies dient dem Vertrauensschutz und der Entlastung der Gerichte. Der Zertifizierungsdiensteanbieter kann dem Signaturschlüssel-Inhaber die damit verbundenen Kosten in Rechnung stellen.

Zu § 11

Mit der Vorschrift wird Artikel 6 EGSRL umgesetzt und dem Petitum des Bundesrates im Gesetzgebungsverfahren zum Informations- und Kommunikationsdienstegesetz (vgl. Bundesrats-Drucksache 420/97 (Beschluss)) entsprochen. Außerdem trägt die Regelung dem Entschließungsauftrag des Deutschen Bundestages vom 11. Juni 1997 zum Informations- und Kommunikationsdienste-Gesetz (IuKDG) Rechnung (BT-Drs.

13/7935). Mit diesem Beschluss hat der Deutsche Bundestag die Bundesregierung beauftragt, die Frage der Haftung im Zusammenhang mit der Einführung und Umsetzung digitaler Signaturen im Rahmen der Evaluierung des Gesetzes gesondert zu überprüfen. Im IuKDG-Bericht zum Gesetz hat die Bundesregierung auf die Notwendigkeit einer spezifischen Haftungsregelung für Zertifizierungsdiensteanbieter hingewiesen (vgl. BT-Drs. 14/1191, S. 33).

Die vorgesehene Haftung erstreckt sich über die Mindestregelungen in Artikel 6 EGSRL hinaus auf die gesamten Leistungen eines Zertifizierungsdiensteanbieters (Ausstellung von qualifizierten Zertifikaten, Auskünfte aus dem Zertifikat-Verzeichnis, Ausstellung von qualifizierten Zeitstempeln), die schädigende Auswirkungen gegenüber Dritten haben können.

Mit der Ausstellung eines qualifizierten Zertifikates ist auch die Aussage verbunden, dass der Signaturschlüssel-Inhaber über eine sichere Signaturerstellungseinheit verfügt (vgl. § 5 Abs. 6 SigG-E) und dass der jeweilige Signaturschlüssel nur auf dieser gespeichert ist (vgl. § 5 Abs. 4 Satz 3 und § 17 Abs. 3 Nr. 1 SigG-E).

Die rechtliche Gleichstellung der qualifizierten elektronischen Signatur mit der eigenhändigen Unterschrift (vgl. Begründung zu § 6 Abs. 2 SigG-E) in allen Lebensbereichen macht eine umfassende Haftung erforderlich. Die Richtlinie erfasst nach Artikel 6 Abs. 1 nur, dass die Angaben in einem qualifizierten Zertifikat zum Zeitpunkt der Ausstellung richtig und vollständig sein müssen (Buchstabe a)), der Signaturschlüssel-Inhaber zum Zeitpunkt der Ausstellung des qualifizierten Zertifikates im Besitz des betreffenden Signaturschlüssels gewesen sein muss (Buchstabe b)) und dass der Signaturschlüssel im Besitz des Signaturschlüssel-Inhabers und der Signaturprüfschlüssel im qualifizierten Zertifikat zusammenpassen müssen (Buchstabe c)). Diese „Mindestregelung" (vgl. Art. 6 Abs. 1 Satz 1 EGSRL) erfasst damit Sachverhalte von entscheidender Bedeutung nicht, etwa die Nutzung ungeeigneter Produkte für elektronische Signaturen (mit der möglichen Folge, dass qualifizierte Zertifikate gefälscht werden können) oder die Preisgabe von Signaturschlüsseln (mit der Folge, dass qualifizierte elektronische Signaturen nach Belieben gefälscht werden können).

Die im SigG-E vorgesehene umfassende Haftung gibt allen, die Angaben in einem qualifizierten Zertifikat, einer Auskunft aus dem Zertifikat-Verzeichnis oder einem qualifizierten Zeitstempel vertrauen, Sicherheit und trägt so auch zur Etablierung der elektronischen Signatur im Rechts- und Geschäftsverkehr bei. Die Haftungsregelung gilt für alle Zertifikate und Zeitstempel mit dem Merkmal „qualifiziert" (vgl. auch Begründung zu § 2 Nr. 8 SigG-E).

Mit der Vorschrift wird zugleich eine unsichere Rechtslage beendet. In der Literatur ist es umstritten, ob Zertifizierungsdiensteanbieter nach geltendem Recht, z. B. gegenüber einem auf ein Zertifikat vertrauenden Dritten, für ein fahrlässig falsch ausgestelltes oder verwaltetes Zertifikat haften, wenn dem Dritten dadurch ein reiner Vermögensschaden entstanden ist. Teilweise wird in diesen Fällen eine Haftung verneint; teilweise wird angenommen, dass bestimmte Vorschriften des Signaturgesetzes und der Signaturverordnung Schutzgesetze i.S. von § 823 Abs. 2 BGB sind oder dass die Grundsätze des Vertrages mit Schutzwirkung zugunsten Dritter zur Anwendung kommen. Rechtsprechung zu dieser Frage liegt noch nicht vor.

Zu Absatz 1

Absatz 1 beschreibt den objektiven Haftungstatbestand. Der Zertifizierungsdiensteanbieter haftet bei Verletzung der Anforderungen des Signaturgesetzes und der Signaturverordnung beim Erbringen der gesetzlich vorgesehenen Dienstleistungen. Er ist in diesem Zusammenhang auch verantwortlich für das Funktionieren seiner Produkte für elektronische Signaturen und seiner sonstigen technischen Sicherungseinrichtungen (z.B. Firewall-Rechner und Zutrittskontrollsysteme). Satz 1 beschreibt die Kernaufgaben des Zertifizierungsdiensteanbieters, deren ordnungsgemäße und zuverlässige Erfüllung für die Wirkung der qualifizierten elektronischen Signaturen im Rechtsverkehr notwendige Voraussetzung ist.

Die Haftung für Verrichtungsgehilfen bestimmt sich nach § 831 des Bürgerlichen Gesetzbuches. An die für die Auswahl und Überwachung der Personen im Verkehr erforderliche Sorgfalt (vgl. § 831 Abs. 1 Satz 2 BGB) sind angesichts der besonders verantwortungsvollen Aufgabe des Zertifizierungsdiensteanbieters hohe Anforderungen zu stellen.

Zu ersetzen ist der einem in redlicher Weise (vgl. Absatz 1 Satz 2) vertrauenden Dritten adäquat kausal entstandene Schaden nach dem Leitbild des Vertrauensschadens in § 122 BGB. Art und Umfang des Schadensersatzes bestimmen sich nach den §§ 249 ff. BGB. § 254 BGB findet Anwendung, wenn auf Seiten des in redlicher Weise vertrauenden Dritten ein Mitverschulden vorliegt. Dies gilt sowohl für ein Mitverschulden bei Entstehung des Schadens, als auch für ein Verschulden im Hinblick auf die Schadensminderungspflicht. Ein Mitverschulden liegt regelmäßig vor, wenn der Dritte den Schaden durch Nachprüfung des Zertifikates hätte verringern oder vermeiden können.

Zu Absatz 2

Die Vorschrift stellt klar, dass es sich um eine Verschuldenshaftung mit Beweislastumkehr handelt. Kann der Zertifizierungsdiensteanbieter nachweisen, dass er die Verletzung nicht zu vertreten hat, tritt die Haftung nicht ein. Akkreditierte Zertifizierungsdiensteanbieter können sich dabei auf die dokumentierten Ergebnisse der Prüfungen durch öffentlich anerkannte fachkundige Dritte (vgl. § 15 Abs. 3 und Abs. 8 sowie 18 Abs. 2 Satz 2 SigG-E) stützen.

Zu vertreten ist gemäß § 276 Abs. 1 BGB Vorsatz und Fahrlässigkeit. An die „im Verkehr erforderliche Sorgfalt" sind in diesem Zusammenhang keine geringen Anforderungen zu stellen. Zertifizierungsdiensteanbieter müssen vertrauenswürdig sein und nehmen besonders verantwortungsvolle Aufgaben wahr, auf deren ordnungsgemäße Ausführung sich der Rechtsverkehr verlassen muss.

Zu Absatz 3

Absatz 3 bestimmt, unter welchen Voraussetzungen die Ersatzpflicht nicht eintritt. Eine Haftungsbeschränkung ist nur über eine Verwendungsbeschränkung des Signaturschlüssels im Zertifikat möglich. Eine davon losgelöste Beschränkung der Haftung des Zertifizierungsdiensteanbieters ist – im Einklang mit der Richtlinie – nicht zulässig.

Enthält das Zertifikat gemäß § 7 Abs. 1 Nr. 7 SigG-E Angaben, dass die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt ist, so wird für Nutzungen, die diese Einschränkung überschreiten, nicht gehaftet. Der Dritte ist insofern auch nicht schutzwürdig, da diese Einschränkung aus dem Zertifikat für jedermann ersichtlich ist. Damit die Einschränkung wirksam wird, muss sie im qualifizierten Zertifikat angegeben sein (vgl. auch Art. 6 Abs. 3 und 4 EGSRL). Nur so ist sichergestellt, dass alle potenziell Betroffenen entsprechende Kenntnis erhalten.

Eine Beschränkung der Nutzung des Signaturschlüssels nach § 7 Nr. 7 SigG-E kann im Rahmen des Dienstleistungsvertrages zwischen Zertifizierungsdiensteanbieter und Signaturschlüssel-Inhaber sowohl vom Signaturschlüssel-Inhaber als auch von dem das Zertifikat ausstellenden Zertifizierungsdiensteanbieter ausgehen, falls dieser sein Haftungsrisiko begrenzen will.

Zu Absatz 4

Die Vorschrift stellt klar, dass der Zertifizierungsdiensteanbieter auch dann haftet, wenn er sich Dritter bedient oder wenn er für Dritte einsteht. Artikel 6 EGSRL sieht unabhängig von der Organisationsform eine Haftung bei allen von dem Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikaten vor. Die nach Artikel 7 Abs. 1 Buchst. b) EGSRL vorgesehene Möglichkeit, dass ein Zertifizierungsdiensteanbieter für einen ausländischen Zertifizierungsdienstdienst „einsteht", schließt zwangsläufig die Haftung ein.

Durch Satz 2 wird spezialgesetzlich angeordnet, dass der Entlastungsbeweis der allgemeinen Regelung des § 831 Abs. 1 Satz 2 BGB nicht zur Anwendung kommt. Der Anwendungsbereich von Satz 2 ist begrenzt: Er greift tatbestandlich nur ein, wenn der beauftragte Dritte Verrichtungsgehilfe im Sinne des § 831 BGB ist. Für alle anderen beauftragten Dritten haftet der Zertifizierungsdiensteanbieter ohnehin nach Satz 1 ohne Entlastungsmöglichkeit. Dies wird in der Regel bei einer Aufgabenübertragung mit einem gewissen Grad an Selbständigkeit der Fall sein. Für den Fall, dass ein eingebundener Dritter einmal Verrichtungsgehilfe des Zertifizierungsdiensteanbieters sein sollte, führt Satz 2 zum gleichen Haftungsmaß des Zertifizierungsdiensteanbieters: Hiernach haftet - abweichend vom Regelfall nach § 831 Abs. 1 Satz 2 BGB –

ausnahmsweise ein Zertifizierungsdiensteanbieter für eingebundene Dritte auch dann, wenn er darlegen kann, dass er bei der Auswahl und Überwachung die erforderliche Sorgfalt beachtet hat. Diese Ausnahmeregelung von § 831 Abs. 1 Satz 2 BGB ist durch die besondere Konstellation bedingt und daher nicht verallgemeinerbar. Da die Auslagerung von Tätigkeiten der Zertifizierungsdiensteanbieter die Regel sein dürfte (vgl. § 4 Abs. 5 SigG-E mit Begründung), würde bei der Möglichkeit des Entlastungsbeweises die umfassende Haftungsregelung in diesen Fällen zu einem wesentlichen Teil leerlaufen, und es würde eine Verlagerung von Aufgaben der Zertifizierungsdiensteanbieter auf Dritte als Verrichtungsgehilfen geradezu provoziert. Eine unterschiedliche haftungsrechtliche Behandlung von beauftragten Dritten, die Verrichtungsgehilfen sind, und solchen, für die der Zertifizierungsdiensteanbieter nach Satz 1 ohne Exkulpationsmöglichkeit haftet, wäre aus Sicht des Geschädigten, der keinen Einblick in das interne Verhältnis zwischen Zertifizierungsdiensteanbieter und Dritten hat, nicht nachvollziehbar und nicht gerechtfertigt. Die Ausnahme von § 831 Abs. 1 Satz 2 BGB ist deshalb im Interesse einer einheitlichen umfassenden Haftung notwendig und durch die zentrale Bedeutung der Zertifizierungsdiensteanbieter für den elektronischen Rechts- und Geschäftsverkehr und das ihnen entgegengebrachte Vertrauen gerechtfertigt.

Zu § 12

Die Vorschrift dient der Umsetzung von Artikel 6 und Anhang II Buchstabe h) EGSRL. Sie stellt sicher, dass Zertifizierungsdiensteanbieter ihrer gesetzlichen Verpflichtung zum Schadensersatz nach § 11 SigG-E auch tatsächlich nachkommen können.

Die Mindestdeckungssumme gilt für den einzelnen Schadensfall, wobei ein auslösendes Ereignis (z.B. gefälschtes Zertifikat) zu einer Vielzahl von Einzelschäden führen kann. Da Anzahl und Höhe potenzieller Schäden damit nur schwer vorhersehbar sind (so kann z.B. ein Zertifikat für eine Vielzahl von Transaktionen verwendet werden), kommt zur Deckungsvorsorge vor allem eine entsprechende Versicherung in Betracht. Alternativ kann die Deckungsvorsorge auch in einer entsprechend hohen Kapitaldeckung, wie sie etwa bei einer Bank vorhanden ist, bestehen.

Eine nähere inhaltliche Bestimmung (z.B. des notwendigen Versicherungsschutzes) bleibt der Rechtsverordnung nach § 24 SigG-E vorbehalten. Dabei werden insbesondere auch Regelungen zum Umfang einer zulässigen Begrenzung der Versicherungsleistung und eines zulässigen Deckungsausschlusses zu treffen sein.

Die vorgesehene Mindestdeckungssumme ist angemessen. Sie deckt auf der einen Seite die üblichen Rahmen von geldwerten Transaktionen (z.B. beim Online-Banking) ab und hält auf der anderen Seite die erforderliche Deckungsvorsorge für die betroffenen Zertifizierungsdiensteanbieter in vertretbaren Grenzen.

Zu § 13

Mit der Vorschrift werden die Anforderungen des Anhangs II EGSRL für den Fall der Einstellung der Tätigkeit abgebildet. Die Regelung ist integraler Bestandteil eines geeigneten Systems zur Überwachung der Zertifizierungsdiensteanbieter nach Artikel 3 Abs. 3 EGSRL. Sie greift auf § 11 SigG zurück.

Zu Absatz 1

Die Vorschrift wird gegenüber der bisherigen Regelung in § 11 Abs. 2 SigG präzisiert („..hat die Einstellung ihrer Tätigkeit unverzüglich..“). Satz 2 wird an die Begriffe des § 2 SigG-E angepasst. Die Regelungen der Sätze 1 bis 3 sind bußgeldbewehrt (vgl. § 21 Abs. 1 Nr. 2, 10 und 11 SigG-E).

Zu Absatz 2

Die Vorschrift wird gegenüber der bisherigen Regelung präzisiert („..Zertifikate nach Satz 1 ..“). Die Regelung „oder andernfalls an die zuständige Behörde zu übergeben“ entfällt; sie wird in § 15 Abs. 7 Satz 3 SigG-E aufgenommen und gilt damit nur für akkreditierte Zertifizierungsdiensteanbieter.

Die Richtlinie sieht eine Übernahme der Dokumentation nicht ausdrücklich vor, schließt eine solche jedoch auch nicht aus. Die Pflicht der zuständigen Behörde zur Übernahme der Dokumentation eines Zertifizierungsdiensteanbieters, wenn dieser seinen Betrieb

einstellt und kein anderer Zertifizierungsdiensteanbieter zur Übernahme bereit ist, gilt daher nur für akkreditierte Zertifizierungsdiensteanbieter nach § 15 SigG-E. Unabhängig davon würde eine generelle Übernahmeverpflichtung für die zuständige Behörde eine nicht übersehbare Belastung bedeuten. Es kann nicht ausgeschlossen werden, dass Zertifizierungsdiensteanbieter bereits nach kurzer Zeit wieder aus dem Markt ausscheiden. Bei akkreditierten Zertifizierungsdiensteanbietern, die vor ihrer Akkreditierung einer umfassenden Prüfung unterzogen werden, ist diese Wahrscheinlichkeit deutlich geringer.

Zu Absatz 3

Die Vorschrift greift auf § 11 Abs. 3 SigG zurück.

Zu § 14

Mit der Vorschrift wird Artikel 8 EGSRL umgesetzt. Sie greift auf § 12 SigG zurück. Die Regelungen des § 12 SigG entsprechen den Vorgaben der Richtlinie bereits weitgehend; daher sind nur geringfügige Anpassungen erforderlich.

Zu Absatz 1

Neben einer redaktionellen Anpassung an die neuen Begriffe nach § 2 SigG-E wird die Verwendung von personenbezogenen Daten entsprechend Artikel 8 Abs. 2 EGSRL einer engeren Zweckbindung unterworfen, indem in Satz 3 des geltenden § 12 SigG die Worte „oder einer anderen Rechtsvorschrift" entfallen. Damit wird ausgeschlossen, dass die Regelung als nicht richtlinienkonformer Verweis auf andere Rechtsvorschriften (z.B. § 28 BDSG) verstanden werden könnte. Die Daten dürfen für andere Zwecke als für ein Zertifikat danach nur verwendet werden, wenn das Signaturgesetz es erlaubt (z.B. für Auskünfte nach § 5 Abs. 1 Satz 2 SigG-E) oder der Betroffene eingewilligt hat.

Zu Absatz 2

Absatz 2 enthält – wie bisher im § 12 Abs. 2 SigG - die erforderlichen Regelungen zur Aufdeckung eines Pseudonyms, um den berechtigten Interessen der

Sicherheitsbehörden Rechnung zu tragen. Die Vorschrift wird insoweit ergänzt, als die Aufdeckung eines Pseudonyms auch für Zwecke der Finanzbehörden und zum Zwecke der Durchsetzung zivilrechtlicher Ansprüche vor Gericht zulässig ist.

In Satz 1 wird der zu enge Begriff des „Zollkriminalamtes" nach geltendem Signaturgesetz durch den weiteren Begriff „Finanzbehörden" ersetzt, der den des Zollkriminalamtes mit umfasst. Es wird klargestellt, dass die Finanzbehörden das Recht haben, bei Geschäften im elektronischen Handel unter Pseudonymen die Identität einer handelnden Person festzustellen; die Zertifizierungsdiensteanbieter sollen insoweit auch zur Auskunft gegenüber den Finanzbehörden und gegenüber den Gerichten verpflichtet sein. Durch den letzten Teilsatz des § 14 Abs. 2 Satz 1 SigG-E werden die Anordnungsbefugnisse der Gerichte nicht erweitert. Diese bestimmen sich nach den einschlägigen Verfahrensordnungen. Der Teilsatz verpflichtet den Zertifizierungsdiensteanbieter nach einer entsprechenden Anordnung der Gerichte, die Daten über die Identität des Signaturschlüssel-Inhabers an diese zu übermitteln. Eine Übermittlung der Daten darf nicht unter Hinweis auf den Datenschutz verweigert werden.

Dies bedeutet zwar für das zivil- und arbeitsgerichtliche Verfahren, dass das Gericht – abgesehen vom Fall der §§ 429, 422 ZPO – private Zertifizierungsdiensteanbieter nicht um Mitteilung von Urkunden ersuchen darf. Diese scheinbare Lücke wird jedoch dadurch geschlossen, dass es die Vernehmung einer Auskunftsperson des Zertifizierungsdiensteanbieters (z.B. eines Sachbearbeiters) als Zeuge anordnen darf. Aufgrund des § 14 Abs. 2 Satz 1 letzter Teilsatz SigG-E wäre es dem Zeugen verwehrt, sich auf ein Zeugnisverweigerungsrecht nach § 383 Abs. 1 Nr. 6 ZPO zu berufen; er wäre nach § 14 Abs. 2 Satz1 erster Teilsatz zur Übermittlung der Identität des Signaturschlüssel-Inhabers verpflichtet.

Zu Absatz 3

Die Vorschrift entspricht Artikel 8 Abs. 2 EGSRL. Nach der Systematik des SigG-E fallen unter „Zertifizierungsdiensteanbieter" nur solche, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen (vgl. § 2 Nr. 8 SigG-E). Die Datenschutzregelung nach Artikel 8 EGSRL erfasst jedoch auch andere Zertifizierungsdiensteanbieter. Dies

gilt unabhängig davon, ob Zertifikate öffentlich oder nur für eine geschlossene Benutzergruppe ausgestellt werden. Soweit nicht die Tätigkeit von Zertifizierungsdiensteanbietern im Zusammenhang mit der Ausstellung von Zertifikaten steht, gelten die Regelungen des Bundesdatenschutzgesetzes.

Den Vorgaben von Artikel 8 Abs. 1 EGSRL wird bereits durch das Bundesdatenschutzgesetz und Artikel 8 Abs. 3 EGSRL durch § 5 Abs. 3 SigG-E entsprochen.

Die bisherige Regelung des § 12 Abs. 3 SigG entfällt; sie ist im Hinblick auf die Neufassung des § 38 BDSG (Aufhebung der Anlasskontrolle) entbehrlich.

Zu § 15

Die Vorschrift setzt die in Artikel 3 Abs. 2 EGSRL für die einzelnen Mitgliedstaaten vorgesehene Option zur Einführung bzw. Beibehaltung freiwilliger Akkreditierungssysteme, die auf eine Steigerung des Niveaus der erbrachten Zertifizierungsdienste abzielen, um. Die freiwillige Akkreditierung soll nach der Richtlinie den Zertifizierungsdiensteanbietern den geeigneten Rahmen für die Weiterentwicklung ihrer Dienste bieten, um das erforderliche Maß an Sicherheit, Qualität und Vertrauen zu erreichen. Entsprechend der Richtlinie (vgl. Erwägungsgrund Nr. 11) steht es den Zertifizierungsdiensteanbietern frei, sich nach § 15 SigG-E akkreditieren zu lassen oder sich auf die Anzeige des Betriebes nach § 4 Abs. 3 SigG-E zu beschränken.

Die Umsetzung des von der Richtlinie vorgesehenen Konzepts der freiwilligen Akkreditierung („Steigerung des Sicherheitsniveaus") besteht nach § 15 SigG-E darin, dass die Erfüllung der gesetzlichen Anforderungen bei den Zertifizierungsdiensteanbietern und den Produkten für elektronische Signaturen vorab (bei Zertifizierungsdiensteanbietern auch danach in regelmäßigen Zeitabständen sowie bei sicherheitserheblichen Veränderungen) durch öffentlich anerkannte fachkundige Dritte umfassend geprüft und bestätigt wird.

Mit dieser Vorschrift kann das anerkannte Sicherheitsniveau des geltenden Signaturgesetzes als eine Option für den Markt beibehalten werden. Es wird hierbei weitgehend auf die Regelungen des geltenden SigG (Vorschriften über die Prüfungs-

und Bestätigungsmodalitäten für die Sicherheit der Zertifizierungsdienste und der Produkte für elektronische Signaturen) zurückgegriffen, da diese Regelungen das Konzept der Richtlinie zur freiwilligen Akkreditierung hinsichtlich des Verfahrens („Erlaubnis") und des angestrebten höheren Sicherheitsniveaus („Steigerung") richtlinienkonform abbilden.

Bei der Akkreditierung handelt es sich um ein Qualitätssicherungssystem. Für die Akkreditierung ist die zuständige Behörde verantwortlich. Es wird für das Verfahren auf die Regulierungsbehörde für Telekommunikation und Post zurückgegriffen, da diese über die notwendigen Erfahrungen im Zusammenhang mit dem der freiwilligen Akkreditierung ähnlichen Genehmigungsverfahren nach geltendem SigG verfügt. Hierdurch wird zugleich eine rasche und reibungslose Umsetzung des Verfahrens der freiwilligen Akkreditierung in Deutschland sichergestellt. Die zuständige Behörde kann sich hierbei – wie bereits beim Genehmigungsverfahren nach dem geltenden Signaturgesetz - privater Stellen bedienen. Das Akkreditierungsverfahren bietet damit nicht nur ein hohes Maß an Sicherheit, sondern trägt auch wirtschaftlichen Aspekten wie Kosten, Zeitdauer und Transparenz Rechnung. Zugleich wird der Grundsatz der Subsidiarität staatlichen Handelns gewahrt.

Eine Akkreditierung kann sowohl vor als auch nach Betriebsaufnahme (und Anzeige nach § 4 SigG-E) erfolgen.

Zu Absatz 1

Mit den Sätzen 1 und 2 wird wegen der Vergleichbarkeit der Verfahren im wesentlichen auf die Regelung in § 4 Abs. 1 SigG zurückgegriffen. Die Vorschrift sieht vor, dass sich die Behörde bei der Akkreditierung privater Stellen (z.B. der Prüf- und Bestätigungsstellen nach § 18 SigG-E) bedienen kann. Es ist zu erwarten, dass - wie bereits bisher im Rahmen der Genehmigung - die Aufgaben nach § 15 SigG-E weitgehend durch die von der zuständigen Behörde anerkannten privaten Prüf- und Bestätigungsstellen im Wettbewerb erledigt werden. Der zuständigen Behörde ist jedoch in jedem Falle die letzte Entscheidung über die jeweilige Akkreditierung vorbehalten. Damit wird eine einheitliche Praxis im Hinblick auf das angestrebte Sicherheitsniveau gewährleistet.

Durch das nach Satz 3 und Absatz 8 Satz 2 vorgesehene Gütezeichen sollen sichere Zertifizierungsdienste und Produkte für elektronische Signaturen gefördert werden. Dies führt zu einer Markttransparenz, die für die Schaffung eines raschen Vertrauensschutzes im täglichen Rechts- und Geschäftsverkehr unerläßlich ist und den zunehmenden Sicherheitsanforderungen in den Netzen Rechnung trägt.

Mit Satz 4 wird beschrieben, dass durch das Gütezeichen der Aspekt der Qualitätssicherung und die hierfür notwendigen Nachweise deutlich zum Ausdruck gebracht werden sollen. Das Sicherheitsniveau qualifizierter elektronischer Signaturen, die auf einem qualifizierten Zertifikat eines akkreditierten Zertifizierungsdiensteanbieters beruhen, entspricht dem der digitalen Signaturen nach dem geltenden Signaturgesetz. An die Stelle der Sicherheitsvermutung aus § 1 Abs. 1 SigG („als sicher gelten können") tritt jedoch eine objektive Beschreibung der Sicherheit in Satz 4 („....wird der Nachweis der umfassend geprüften technischen und administrativen Sicherheit erbracht").

Es ist zu erwarten, dass qualifizierten elektronischen Signaturen nach § 15 SigG-E damit im Rahmen von § 292 ZPO-E (vgl. Teil A, Abschnitt 1. Absatz 9) und im Rahmen der freien Beweiswürdigung der Gerichte ein besonders hoher Beweiswert zukommt, der im Ergebnis als eine Art „Sicherheitsvermutung" gewertet werden kann. An der bisherigen Rechtslage ändert sich insoweit nichts.

Bei einer qualifizierten elektronischen Signatur, die auf einem Verfahren der freiwilligen Akkreditierung nach dieser Vorschrift beruht, kann sicher davon ausgegangen werden, dass sie mit dem Signaturschlüssel des im zugrundeliegenden qualifizierten Zertifikat angegebenen Signaturschlüssel-Inhabers erzeugt wurde und dass die signierten Daten danach nicht verändert wurden. Aufgrund der nach dem Signaturgesetz und der Signaturverordnung vorgesehenen Sicherheitsvorkehrungen ist weiter zu vermuten, dass der im qualifizierten Zertifikat benannte Signaturschlüssel-Inhaber die Signatur erzeugt oder die Erzeugung autorisiert hat, soweit im Einzelfall nicht andere Fakten entgegenstehen. Die mögliche Autorisierung einer anderen Person (z.B. durch Weitergabe der sicheren Signaturerstellungseinheit und PIN) kann ausgeschlossen werden, indem die Signaturerstellungseinheit über die Nutzung biometrischer Merkmale ausschließlich an eine Person gebunden wird.

Mit Satz 5 wird den Zertifizierungsdiensteanbietern ausdrücklich das Recht eingeräumt, sich als akkreditierte Zertifizierungsdiensteanbieter zu bezeichnen und sich auf die nachgewiesene Sicherheit zu berufen.

Die Vorschrift erfüllt die Anforderungen nach Artikel 3 Abs. 2 EGSRL. Sie ist objektiv (eindeutige, sachbezogene Anforderungen), transparent (durch die Regelung im Gesetz und in der Rechtsverordnung nach § 24 SigG-E), verhältnismäßig (die umfassende Prüfung der Sicherheit ist durch die vielfältigen technisch-administrativen Risiken begründet und aufgrund vorliegender Erfahrungen mit vertretbarem Aufwand möglich) und nicht diskriminierend (der Sicherheitswert anderer Verfahren bleibt unberührt).

Zu Absatz 2

Die Vorschrift macht von der Option des Artikel 3 Abs. 7 EGSRL Gebrauch, wonach die Mitgliedstaaten den Einsatz elektronischer Signaturen im öffentlichen Bereich „möglichen zusätzlichen Anforderungen" unterwerfen können. Die Regelung des Einsatzes elektronischer Signaturen im öffentlichen Bereich bleibt den jeweiligen Rechtsvorschriften vorbehalten. Die Vorschrift bildet zur Sicherstellung der Einheitlichkeit des Einsatzes elektronischer Signaturen im öffentlichen Bereich die Referenzvorschrift für alle Rechtsvorschriften des öffentlichen Bereichs, soweit diese in die Zuständigkeit des Bundes fallen. Um einen Wildwuchs der möglichen zusätzlichen Anforderungen für den Einsatz elektronischer Signaturen im öffentlichen Bereich zu vermeiden, ist einzig zulässige „zusätzliche Anforderung" gegenüber den nach dem SigG-E (§ 2 Nr. 1 bis 3) vorgesehenen elektronischen Signaturen nur das Verfahren der freiwilligen Akkreditierung nach § 15 SigG-E. Die Beschränkung auf das Verfahren der freiwilligen Akkreditierung im Absatz 2 trägt gleichzeitig den Vorgaben von Art. 3 Abs. 7 Satz 2 der Richtlinie Rechnung, wonach die Anforderungen an den Einsatz elektronischer Signaturen im öffentlichen Bereich objektiv, transparent und verhältnismäßig sein müssen sowie nicht diskriminierend sein dürfen (vgl. Ausführungen zu Abs. 1). Es reicht jedoch nicht aus, dass Vorschriften, die künftig „zusätzliche Anforderungen" für den Einsatz elektronischer Signaturen im öffentlichen Bereich vorsehen, lediglich auf das Verfahren der freiwilligen Akkreditierung nach § 15

SigG-E verweisen. Auch diese haben darüber hinaus in jedem Falle die Anforderungen nach Artikel 3 Abs. 7 Satz 2 EGSRL zu erfüllen.

Da nur bei diesen Signaturen eine nachgewiesene Sicherheit und dauerhafte Überprüfbarkeit gegeben ist, werden sie im Interesse der Rechtssicherheit aller Beteiligten (Bürger, Unternehmen, Staat) im öffentlichen Bereich in vielen Fällen als Äquivalent zur eigenhändigen Unterschrift erforderlich sein.

Zu Absatz 3

Die Vorschrift in Satz 1 greift auf § 4 Abs. 3 Satz 3 SigG zurück. Mit Satz 2 wird nun im Gesetz selbst (bisher nur in § 15 Abs. 1 der Signaturverordnung) klargestellt, dass die Prüfung unter den genannten Voraussetzungen zu wiederholen ist.

Mit einer Akkreditierung entfällt die Anmeldung nach § 4 Abs. 3 Satz 1 SigG-E; die übrigen Bestimmungen des § 4 SigG-E bleiben unberührt. Das Nähere wird in der Rechtsverordnung nach § 24 SigG-E geregelt.

Zu Absatz 4

Die Vorschrift greift auf § 4 Abs. 4 SigG zurück.

Zu Absatz 5

Die Vorschrift greift auf § 4 Abs. 2 Satz 1 SigG zurück.

Zu Absatz 6

Die Vorschrift greift auf § 13 Abs. 3 SigG zurück. Der Widerruf oder die Rücknahme einer Akkreditierung sind eigenständige Verwaltungsakte, die z.B. von dem Verwaltungsakt der Untersagung des Betriebes eines Zertifizierungsdienstes nach § 19 Abs. 3 SigG-E zu trennen sind.

Zu Absatz 7

Die Vorschrift greift auf § 11 Abs. 1 und § 13 Abs. 4 SigG zurück. Sie führt zu einem erheblichen zusätzlichen Mehrwert von qualifizierten elektronischen Signaturen nach § 15 Sig-E, indem sie sicherstellt, das diese Signaturen langfristig (mindestens 30 Jahre nach § 13 Abs. 2 der Signaturverordnung) nachprüfbar bleiben. Sie schafft damit einen zusätzlichen Anreiz für die Nutzung der freiwilligen Akkreditierung.

Zu Absatz 8

Die Vorschrift greift auf § 14 Abs. 4 SigG zurück. Sie wird redaktionell angepasst. Bei der Prüfvorgabe erfolgt eine Präzisierung, indem gemäß einer Anregung aus der Rechtswissenschaft der „Stand der Wissenschaft" einbezogen wird. Die Bestätigung der vorgeschriebenen Prüfung der Produkte und Erfüllung der Anforderungen erfolgt durch nach § 18 anerkannte Stellen. Die Verantwortung des Zertifizierungsdiensteanbieters und der von ihm beauftragten Dritten (vgl. § 4 Abs. 5 SigG-E) beschränkt sich darauf, dass die Vorgaben nach Satz 2 Nr. 1 bis 3 eingehalten werden.

Zu § 16

Die Vorschrift, die eine Ergänzung zu § 15 SigG-E bildet, greift auf § 5 Abs. 4 SigG zurück. Die qualifizierten Zertifikate der zuständigen Behörde bilden ein entscheidendes Sicherheitselement des Akkreditierungssystems.

Das „Wurzel-Zertifikat" der Regulierungsbehörde bildet eine einheitliche Referenz für alle qualifizierten elektronischen Signaturen nach § 15 SigG-E. Dies ermöglicht es jedermann, automatisch festzustellen, ob eine solche Signatur vorliegt. Die zuständige Behörde hat den für die Ausstellung qualifizierter Zertifikate benötigten Zertifizierungsdienst seit September 1998 in Betrieb. Diese zukunftsorientierte Lösung gewährleistet auch die für die praktische Anwendung von Signaturen notwendige Interoperabilität zwischen den Leistungen verschiedener Zertifizierungsdiensteanbieter.

Zu Absatz 1 und 2

Die Vorschrift aus § 4 Abs. 5 Satz 1 SigG wird präzisiert, indem die Ausstellung von Zertifikaten durch die zuständige Behörde auch Zertifikate für die Signaturschlüssel zum Signieren von Auskünften aus dem Zertifikatsverzeichnis sowie zum Signieren von qualifizierten Zeitstempeln umfasst. Dies entspricht dem tatsächlichen Bedarf, dem in der Praxis bereits entsprochen wird. Es ist zu erwarten, dass damit kein nennenswerter zusätzlicher Aufwand für die Behörde verbunden ist; im übrigen werden für diese Leistungen Kosten erhoben.

Die von der zuständigen Behörde mit einem Zertifikat versehenen Signaturschlüssel können von dem Zertifizierungsdiensteanbieter auch zum Signieren von Zertifikaten für ausschließliche Zwecke der Authentisierung oder der Verschlüsselung eingesetzt werden, soweit die für verschiedene Zwecke bestimmten Zertifikate durch die Nutzer eindeutig zu unterscheiden sind. Damit bildet das „Wurzel-Zertifikat" der zuständigen Behörde eine einheitliche Referenz für alle drei kryptographischen Funktionen: Signatur, Authentisierung und Verschlüsselung, die in weiten Bereichen für Zwecke des Informations- und Datenschutzes gemeinsam benötigt werden. Dies dient dem allgemeinen Informations- und Datenschutz, wie er zur Wahrung von Grundrechten und Sicherheitsinteressen von Unternehmen und Behörden etwa bei der Nutzung des Internet benötigt wird. Damit ist in keiner Weise die Möglichkeit verbunden, verschlüsselte Informationen durch die Behörde oder Dritte zu entschlüsseln.

Zu Absatz 3

Die Vorschrift greift eine Forderung der (vorhandenen und potenziellen) Zertifizierungsdienstanbieter auf und trägt damit den Bedürfnissen der Praxis entsprechend Rechnung.

Signaturanwendungskomponenten, die Dritten (z.B. Kunden von Kaufhäusern) geschäftsmäßig zur Nutzung für qualifizierte elektronische Signaturen nach § 15 SigG-E angeboten werden, sollen sich gegenüber dem Nutzer authentisieren (z.B. durch automatische Entschlüsselung und Anzeige eines nur ihm bekannten Codewortes, das

sich auf seiner sicheren Signaturerstellungseinheit befindet). Damit erhält der Nutzer eine zuverlässige Bestätigung, dass es sich um eine Signaturanwendungskomponente handelt, die den gesetzlichen Anforderungen entspricht und die sich in einem sicheren Zustand befindet.

Zu diesem Zwecke werden von den Produktherstellern für die Authentisierungsschlüssel in den Produkten „technische Zertifikate" ausgestellt, die bei der Authentifizierung automatisch zum Einsatz kommen. Wie die akkreditierten Zertifizierungsdiensteanbieter benötigen auch die Hersteller von Produkten nach § 15 Abs. 8 SigG-E eine „Wurzelinstanz". Dafür bietet sich der bereits bestehende Zertifizierungsdienst bei der zuständigen Behörde, die herstellerneutral und vertrauenswürdig ist, an. Es ist zu erwarten, dass die Übernahme dieser Aufgabe durch die zuständige Behörde mit keinem wesentlichen zusätzlichen Aufwand verbunden ist. Diese trägt vielmehr dazu bei, dass die vorhandenen technischen Einrichtungen für die Vergabe von Zertifikaten eine höhere Auslastung erfahren. Im übrigen werden für die Leistungen Kosten erhoben.

Zu § 17

Zu Absatz 1

Die Vorschrift, die auf § 14 Abs. 1 SigG zurückgreift, setzt Anhang III EGSRL um. Die näheren Einzelheiten werden wie bisher in der Rechtsverordnung (vgl. § 24 SigG-E) geregelt.

Die von der Richtlinie vorgesehenen Anforderungen an sichere Signaturerstellungseinheiten des Anhangs III bedingen insbesondere die Einmaligkeit und Geheimhaltung des Signaturschlüssels sowie einen wirksamen Schutz der sicheren Signaturerstellungseinheit vor einer Nutzung durch Unbefugte. Schließlich darf der Signaturschlüssel nicht aus dem Signaturprüfschlüssel oder signierten Daten errechnet werden können.

Signaturschlüssel können wahlweise auf einer sicheren Signaturerstellungseinheit (Satz 2) oder bei einem Zertifizierungsdiensteanbieter erzeugt und dort auf die

Signaturerstellungseinheit geladen werden (Absatz 3 Nr. 1). Nach dem Stand der Technik sind sichere Signaturerstellungseinheiten (z.B. Chipkarten), auf denen die Signaturschlüssel selbst erzeugt werden, in naher Zukunft zu erwarten. Die Vorschrift trägt bereits diesen Entwicklungen Rechnung. Derzeit werden die Signaturschlüssel noch bei den Zertifizierungsdiensteanbietern erzeugt und dort unter hohen Sicherheitsvorkehrungen auf sichere Signaturerstellungseinheiten übertragen.

Um einer Nutzung von sicheren Signaturerstellungseinheiten durch Unbefugte wirksam vorzubeugen, können biometrische Merkmale genutzt werden. Dabei macht es die moderne Technik möglich, die Referenzdaten unmittelbar über die Signaturerstellungseinheit selbst (z.B. Sensoren auf einer Chipkarte) oder auf andere Weise so zu erfassen und auf diese zu übertragen, dass die Daten ausschließlich auf ihr gespeichert werden, und damit keine Datenschutzprobleme entstehen. Die Vorschrift ist für die Nutzung biometrischer Merkmale entwicklungsoffen. Die Vorschrift in § 16 Abs. 2 Satz 3 der Signaturverordnung sieht die Nutzung biometrischer Merkmale bereits als zusätzliches Identifikationsmerkmal (zu Besitz und Wissen) vor.

Aus der Wirtschaft und von der Arbeitsgemeinschaft der Verbraucherverbände wird unter Hinweis auf den technischen Fortschritt auf diesem Gebiete jedoch einvernehmlich die Forderung erhoben, die Nutzung biometrischer Merkmale künftig nicht nur ergänzend, sondern auch alternativ zur Identifikation durch Wissen (Personenidentifikationsnummer – PIN) zuzulassen. Damit soll die Nutzung biometrischer Merkmale gefördert und mit der Nutzung die Rechtssicherheit im elektronischen Rechts- und Geschäftsverkehr im Interesse aller Beteiligten weiter verbessert werden. Die Bundesregierung wird diese Frage im Rahmen der Neufassung der Signaturverordnung aufgreifen.

Zu Absatz 2

Mit der Vorschrift, die auf § 14 Abs. 2 SigG zurückgreift, wird Anhang IV EGSRL umgesetzt; dieser ist als Empfehlung zwar nicht verbindlich umzusetzen, eine Umsetzung ist jedoch nach Artikel 3 Abs. 6 EGSRL ausdrücklich erwünscht, um die Entwicklung und die Nutzung von Signaturprüfeinheiten zu fördern. Die Vorschrift nimmt darüber hinaus eine Präzisierung dahingehend vor, dass alle bei Anwendung

(Erzeugung oder Prüfung) qualifizierter elektronischer Signaturen relevanten Sicherheitsaspekte erfasst werden (vgl. auch Begründung zu § 2 Nr. 11 SigG-E).

Die Nutzung geeigneter Signaturanwendungskomponenten bleibt in das Ermessen der Signaturschlüssel-Inhaber gestellt. Unabhängig davon wird mit Satz 2 die Notwendigkeit zum Einsatz geeigneter Signaturanwendungskomponenten unterstrichen.

Mit der Formulierung „soll" in Satz 3 wird im Hinblick auf die Richtlinie und unterschiedlichen Auslegungsmöglichkeiten des Signaturgesetzes zugleich klargestellt, dass die Verwendung von geeigneten Signaturanwendungskomponenten nicht Voraussetzung für die Erzeugung einer qualifizierten elektronischen Signatur ist. Dies ergibt sich schon daraus, dass aus einer elektronischen Signatur nicht ersichtlich ist, welche Signaturanwendungskomponente bei ihrer Erzeugung zum Einsatz kam. Hinzu kommt, dass im Einzelfall auch „andere geeignete Maßnahmen" (z.B. PC oder Laptop unter ständiger Kontrolle und ohne Anschluss an ein Kommunikationsnetz) ausreichend Sicherheit bieten können.

Zu Absatz 3

Mit der Vorschrift, die auf § 14 Abs. 3 SigG zurückgreift, wird Anhang II Buchst. f) EGSRL umgesetzt. Danach müssen Zertifizierungsdiensteanbieter vertrauenswürdige Systeme und Produkte einsetzen, die vor Veränderung geschützt sind und die die technische und kryptographische Sicherheit der von ihnen unterstützten Verfahren gewährleisten.

Bei dem Übertragen von Signaturschlüsseln auf sichere Signaturerstellungseinheiten nach Nummer 1 bleiben technisch unvermeidbare temporäre Zwischenspeicherungen unberührt.

Zu Absatz 4

Die Vorschrift entspricht Artikel 3 Abs. 4 bis 6 EGSRL. Die näheren Einzelheiten bleiben der Rechtsverordnung nach § 24 SigG-E vorbehalten. Dort können auch die zur Zeit

des Gesetzgebungsverfahrens noch ausstehenden Arbeitsergebnisse des Ausschusses nach Artikel 9 EGSRL berücksichtigt werden.

Zu § 18

Die Vorschrift setzt vor allem die Ergebnisse der Evaluierung des Signaturgesetzes um und nutzt den von der Richtlinie gegebenen Spielraum, namentlich in bezug auf die Ausgestaltung der freiwilligen Akkreditierung und den hierfür notwendigen Einsatz von Prüf- und Bestätigungsstellen.

Zu Absatz 1

Die Vorschrift greift eine Anregung aus der Rechtswissenschaft im Rahmen der Evaluierung des Signaturgesetzes auf und setzt sie in dieser Vorschrift um. Es wurde diskutiert, ob die gesetzliche Grundlage für die Anerkennung von Prüf- und Bestätigungsstellen nach den Regelungen des geltendem SigG (vgl. § 4 Abs. 3 und § 14 Abs. 4) ausreichend ist, um dem rechtlichen Erfordernis für einen Eingriff in das Grundrecht nach Artikel 12 Abs. 1 GG Rechnung zu tragen. Es ging im Kern um die Frage der ausreichenden gesetzlichen Kriterien für die im geltenden Signaturgesetz genannte Anerkennung von Prüf- und Bestätigungsstellen und darum, ob die Prüf- und Bestätigungsstellen als Beliehene gelten oder (nur) als „Verwaltungshelfer" für die Regulierungsbehörde tätig werden. Auch wenn diese Frage keine praktische Bedeutung erlangt hat, wird im Hinblick auf die vorgetragenen verfassungsrechtlichen Bedenken jetzt durch diese Vorschrift Rechtssicherheit geschaffen.

Während die Prüfung und Bestätigung der Sicherheit von Zertifizierungsdiensten durch dieselbe Stelle erfolgt, muss die Prüfung und anschließende Bestätigung der Sicherheit von Produkten nach den europäischen Normen EN 45 000 ff durch getrennte Stellen erfolgen. Die für die Bestätigung der Sicherheit von Produkten zuständigen Stellen akkreditieren die Prüfstellen gemäß den genannten Normen selbst.

Zu Absatz 2

Die Vorschrift in Satz 1 orientiert sich am Gewerberecht (vgl. § 9 Gerätesicherungsgesetz). Die näheren Einzelheiten bleiben der Rechtsverordnung nach § 24 SigG-E vorbehalten.

Die Vorschrift in Satz 2 gewährleistet, dass bei qualifizierten elektronischen Signaturen nach § 15 SigG-E jederzeit rückwirkend (für die relevanten Zeitpunkte der Erzeugung oder Prüfung von Signaturen) die Sicherheit festgestellt werden kann.

Zu § 19

Die Vorschrift entspricht Artikel 3 Abs. 3 EGSRL. Sie greift auf § 4 und § 13 SigG zurück.

Zu Absatz 1

Die Vorschrift weist in Satz 1 der zuständigen Behörde die Aufsicht über die Zertifizierungsdiensteanbieter zu. Gleichzeitig wird klargestellt, dass die Behörde sich bei ihrer Aufsicht privater Stellen (z.B. der Prüf- und Bestätigungsstellen nach § 18 SigG-E) bedienen kann.

Die Aufsicht beginnt mit Aufnahme des Betriebes (Satz 2). Die Aufsicht muss die Vorgaben des Art. 3 Abs. 3 EGSRL erfüllen. Dies lässt nur Kontrollen nach Betriebsaufnahme zu. Eine systematische Kontrolle ist nicht vorgesehen; die Aufsicht ist vielmehr auf anders bezogene Maßnahmen beschränkt. Dies entspricht dem Leitbild der Richtlinie, die Genehmigungsverfahren oder solche, die diesen in der Struktur ähneln oder von den Wirkungen her einer Genehmigung vergleichbar sind, nicht zulässt (vgl. Art. 3 Abs. 1 i.V.m. Erwägungsgrund Nr. 10 EGSRL). Die zuständige Behörde kann sich unabhängig hiervon im Rahmen einer freiwilligen Akkreditierung von der Sicherheit überzeugen.

Zu Absatz 2

Die Vorschrift greift auf § 13 Abs. 1 Satz 1 SigG zurück.

Zu Absatz 3

Die Vorschrift greift auf § 4 Abs. 2 und § 13 Abs. 1 Satz 2 SigG zurück.

Zu Absatz 4

Die Vorschrift in Satz 1 greift auf § 13 Abs. 5 Satz 2 SigG zurück. Sie schließt eine rückwirkende Auswirkung auf die Gültigkeit von qualifizierten Zertifikaten (und damit auf die zu einem früheren Zeitpunkt erzeugten qualifizierten elektronischen Signaturen) aus; eine mögliche Sperrung der Zertifikate bleibt unberührt. Der Vorschrift kommt für die Rechtssicherheit bei der Anwendung qualifizierter elektronischer Signaturen hohe Bedeutung zu.

Stellt ein Zertifizierungsdiensteanbieter zu einem Zeitpunkt, zu dem er die formalen Voraussetzungen für den Betrieb nach dem Signaturgesetz nicht oder nicht mehr erfüllt (z.B. nach Untersagung des Betriebes), Zertifikate aus, so liegen in diesem Falle keine qualifizierten Zertifikate im Sinne des Signaturgesetzes vor.

Zu Absatz 5

Die Vorschrift greift auf § 13 Abs. 5 Satz 1 SigG zurück.

Zu Absatz 6

Die Vorschrift dient der Umsetzung von Artikel 1 Satz 1 und Artikel 5 Abs. 1 EGSRL.

Damit das Konzept der Richtlinie, das eine EU-weite Anerkennung elektronischer Signaturen nach Artikel 5 Abs. 1 EGSRL zum Ziel hat, greift, müssen die Nutzer dieser Signaturen jederzeit online feststellen können, ob eine Signatur tatsächlich Artikel 5

Abs. 1 EGSRL bzw. den entsprechenden nationalen Rechtsvorschriften entspricht. Dies erfordert, dass die jeweilige nationale Aufsichtsstelle ein online abrufbares Verzeichnis der Zertifizierungsdiensteanbieter führt, die berechtigt sind, qualifizierte Zertifikate für elektronische Signaturen nach Artikel 5 Abs. 1 EGSRL auszustellen. Die Vorschrift ist durch Wahl des Begriffes „Kommunikationsverbindungen" technologieoffen gestaltet. Es wird darüber hinaus auf die Ausführungen zu § 16 Abs. 1 und 2 und zu § 5 Abs. 1 SigG-E verwiesen. Um eine unbemerkte Fälschung oder Verfälschung des Verzeichnisses auszuschließen, muss dieses mit einer qualifizierten elektronischen Signatur signiert sein.

Zu § 20

Die Vorschrift dient der Umsetzung von Artikel 3 Abs. 3 EGSRL. Sie greift auf § 13 Abs. 2 SigG zurück.

Zu Absatz 1

Die Vorschrift greift auf § 13 Abs. 2 Satz 1 SigG zurück. Durch die Einfügung der Worte „in geeigneter Weise" wird klargestellt, dass die Verpflichtung zur Auskunft und Unterstützung einschließt, dass der Zertifizierungsdiensteanbieter oder für ihn tätige Dritte der zuständigen Behörde die für die Nutzung elektronischer Daten erforderlichen Einrichtungen zur Verfügung stellen.

Durch die Einfügung der Worte „auch soweit sie in elektronischer Form vorliegen" sollen in der Rechtswissenschaft geäußerte Zweifel, ob unter die bisherige Aufzählung auch elektronische Dokumente fallen, ausgeräumt werden

Zu Absatz 2

Die Vorschrift greift auf § 13 Abs. 2 Satz 2 SigG zurück.

Zu § 21

Die Bußgeldvorschrift dient der Umsetzung von Artikel 3 Abs. 3 EGSRL. Das dort beschriebene „geeignete System zur Überwachung" erfordert nach Wegfall der Genehmigungspflicht für Zertifizierungsdiensteanbieter eine entsprechende Bußgeldvorschrift, um eine wirksame Durchsetzung der gesetzlichen Vorschriften zu ermöglichen. Die Bußgeldvorschrift greift, anders als die zivilrechtliche Haftung, auch dann, wenn durch das normwidrige Verhalten noch kein Schaden eingetreten oder dieser strittig ist.

Ein Bußgeld stellt im Vergleich zu anderen Maßnahmen, die von der zuständigen Behörde im Rahmen ihrer Aufsicht nach § 19 SigG-E getroffen werden können (z.B. vollständige oder teilweise Untersagung des Betriebes), regelmäßig das mildere und auch flexiblere Mittel zur Durchsetzung der Einhaltung der Vorschriften des SigG-E und der Verordnung dar. Überwachung dar. Eine Bußgeldvorschrift ist daher zur Wahrung des allgemeinen Grundsatzes der Verhältnismäßigkeit geboten.

Normadressat der Bußgeldregelung ist der Zertifizierungsdiensteanbieter. Als Täter einer Ordnungswidrigkeit nach dem Ordnungswidrigkeitengesetz (OWiG) kommt grundsätzlich nur eine natürliche Person in Betracht. In bezug auf Handlungen von Personen, die für den Normadressaten tätig sind, gilt § 9 OWiG. Die Festsetzung von Bußgeldern gegenüber juristischen Personen regelt § 30 OWiG.

Zu Absatz 1

Absatz 1 enthält die Tatbestände, die erhebliche Auswirkungen auf die Sicherheit qualifizierter elektronischer Signaturen haben können und denen im Hinblick auf die notwendige Rechtssicherheit bei Anwendung qualifizierter elektronischer Signaturen Haftungsregelungen für den Schadensfall allein nicht gerecht werden können.

Zu Nummer 1

Nummer 1 erfasst den zentralen Tatbestand für das Betreiben eines Zertifizierungsdienstes. Es handelt sich bei der Erfüllung der in § 4 Abs. 2 Satz 1 SigG-E beschriebenen Pflichten um Kernpflichten des Zertifizierungsdiensteanbieters, ohne die das ordnungsgemäße Betreiben eines Zertifizierungsdienstes nach diesem Gesetz nicht möglich ist. Der Verweis auf die Rechtsverordnung dient durch Verwendung des Wortes „auch" vor allem der Klarstellung; einer Konkretisierung des Handlungsgebotes durch die Rechtsverordnung bedarf es hier nicht.

Zu Nummer 2

Die Erfüllung der Anzeigepflichten nach § 4 Abs. 3 Satz 1 und nach § 13 Abs. 1 Satz 1 SigG-E ist notwendige Voraussetzung dafür, dass die zuständige Behörde ihre Aufsicht nach § 19 SigG-E wahrnehmen kann.

Zu Nummer 3

Nummer 3 erfasst den Tatbestand, dass der Zertifizierungsdiensteanbieter eine Person, die ein qualifiziertes Zertifikat beantragt, nicht zuverlässig identifiziert. Es handelt sich bei der Identifikation des Antragstellers um eine Kernpflicht des Zertifizierungsdiensteanbieters. Eine mangelnde Identifikation kann zur Folge haben, dass ein qualifiziertes Zertifikat auf einen falschen Namen ausgestellt und dieses für Betrugszwecke eingesetzt wird. Qualifizierte Zertifikate bilden die Grundlage für die Zuordnung qualifizierter elektronischer Signaturen, die ein Substitut zur handschriftlichen Unterschrift bilden können. Ihnen kommt daher im Rechts- und Geschäftsverkehr hohe Bedeutung zu. Der Verweis auf die Rechtsverordnung bedeutet, dass zur Konkretisierung des Handlungsgebotes zusätzlich die Rechtsverordnung heranzuziehen ist.

Zu Nummer 4

Nummer 4 erfasst den Tatbestand, dass der Zertifizierungsdiensteanbieter qualifizierte Zertifikate nicht nachprüfbar hält. In diesem Falle sind die Nutzer elektronischer Signaturen im elektronischen Rechts- und Geschäftsverkehr nicht handlungsfähig; damit kann eine entscheidende Funktion der qualifizierten elektronischen Signatur, die Authentifizierung einer Person, nicht erfüllt werden.
Zum Verweis auf die Rechtsverordnung vgl. oben zu Nummer 1.

Zu Nummer 5

Nummer 5 erfasst den Tatbestand, dass der Zertifizierungsdiensteanbieter qualifizierte Zertifikate ohne Zustimmung des Signaturschlüssel-Inhabers abrufbar hält. Da Zertifikate wichtige persönliche Daten (z.B. Prokura-Berechtigung in erheblichem Umfange für ein Unternehmen) enthalten können, kann dies für die betroffenen Signaturschlüssel-Inhaber schwerwiegende Folgen haben (z. B. Erpressungsversuche).

Zu Nummer 6

Nummer 6 erfasst den Tatbestand, dass der Zertifizierungsdiensteanbieter Angaben in ein qualifiziertes Zertifikat aufnimmt, ohne dass bei Vertretungsrechten die Einwilligung der dritten Person oder bei berufsbezogenen oder sonstigen Angaben die erforderliche Bestätigung der zuständigen Stelle vorliegt. In einem solchen Fall könnten Zertifikate z. B. für besonders schwerwiegende Betrugshandlungen genutzt werden.

Zu Nummer 7

Nummer 7 erfasst den Tatbestand, dass der Zertifizierungsdiensteanbieter die Geheimhaltung von Signaturschlüsseln nicht gewährleistet Die Geheimhaltung von Signaturschlüsseln ist notwendige Voraussetzung für das Vertrauen in den Rechts- und Geschäftsverkehr mit qualifizierten elektronischen Signaturen. Es handelt sich um eine Kernpflicht der Zertifizierungsdiensteanbieter nach dem Gesetz. Zum Verweis auf die Rechtsverordnung vgl. oben zu Nummer 1.

Zu Nummer 8

Nummer 8 erfasst den Tatbestand, dass der Zertifizierungsdiensteanbieter Signaturschlüssel außerhalb der jeweiligen sicheren Signaturerstellungseinheit speichert. In einem solchen Falle könnten mit Kopien des Signaturschlüssels gefälschte Signaturen erzeugt werden, die von „echten" Signaturen nicht zu unterscheiden sind.

Zu Nummer 9

Nummer 9 erfasst den Tatbestand, dass ein Zertifizierungsdiensteanbieter die gesetzlich vorgeschriebene Dokumentation nicht führt. Die Dokumentation bildet eine wichtige Grundlage für gerichtliche Entscheidungen im Falle von Rechtsstreitigkeiten über die Sicherheit von Signaturen oder die pflichtgemäße Aufgabenerfüllung eines Zertifizierungsdiensteanbieters. Zum Verweis auf die Rechtsverordnung vgl. oben zu Nummer 1.

Zu Nummer 10

Nummer 10 erfasst den Tatbestand, dass ein Zertifizierungsdiensteanbieter seinen Pflichten bei Einstellung des Betriebes hinsichtlich der Übergabe der qualifizierten Zertifikate und der Sperrung nicht nachkommt. Es geht um die Sicherung der notwendigen Kontinuität der Nutzung qualifizierter Zertifikate sowie um die erforderliche Transparenz im Falle der Einstellung des Betriebes, die für das Vertrauen des Rechts- und Geschäftsverkehrs in die Nutzung qualifizierter elektronischer Signaturen wichtig ist. Zum Verweis auf die Rechtsverordnung vgl. oben zu Nummer 1.

Zu Nummer 11

Die Signaturschlüssel-Inhaber müssen unterrichtet sein, um sich entscheiden zu können, ob sie ihr Zertifikat sperren lassen wollen oder ob sie mit der Übergabe an einen anderen Zertifizierungsdiensteanbieter einverstanden sind. Zum Verweis auf die Rechtsverordnung vgl. oben zu Nummer 3.

Zu Absatz 2

Die Vorschrift trägt durch die unterschiedlichen Höchstmaße einer Geldbuße für die Tatbestände des Absatzes 1 Nr. 1, 7 und 8 sowie für die Tatbestände des Absatzes 1 Nr. 2 bis 6 sowie Nr. 9 bis 11 der jeweiligen Schwere und Bedeutung der Verstöße gegen das Gesetz Rechnung.

Die Tatbestände des Absatzes 1 Nr. 1, 7 und 8 belegen Verstöße gegen zentrale Handlungsgebote des SigG-E mit einem Bußgeld von bis zu hunderttausend Deutsche Mark. Die Erfüllung dieser Handlungsgebote ist unerläßliche Voraussetzung zur Schaffung bzw. Aufrechterhaltung einer sicheren Infrastruktur im Rahmen des Verfahrens für qualifizierte elektronische Signaturen. Daher ist für diese Handlungen der höchste Bußgeldbetrag vorgesehen.

Die übrigen Tatbestände des Absatzes 1, die mit einer Geldbuße von bis zu zwanzigtausend Deutsche Mark belegt werden können, sind im Regelfall in der Gesamtbetrachtung nicht so schwerwiegend wie die oben genannten Fälle des Absatzes 1. Es handelt sich hierbei um Formalverstöße, für die wegen des vergleichsweise geringeren Unrechtsgehalts ist ein entsprechend abgesenkter Bußgeldbetrag vorgesehen. Es handelt sich jedoch um Handlungen, die für das ordnungsgemäße Funktionieren des Verfahrens für qualifizierte elektronische Signaturen eine wichtige Rolle spielen und im Einzelfall die Sicherheitsinfrastruktur erheblich treffen können. Daher ist eine Bußgeldbewehrung dieser Handlungen angemessen und gerechtfertigt.

Es liegt im pflichtgemäßen Ermessen der zuständigen Behörde, ob und in welcher Höhe sie im Einzelfall je nach Schwere des Verstoßes gegen die bußgeldbewehrten Vorschriften des Gesetzes eine Geldbuße verhängt (Kann-Bestimmung). Sie kann im Vorfeld einer möglichen Bußgeldverhängung gegenüber dem Zertifizierungsdiensteanbieter auch nur eine entsprechende Verwarnung aussprechen oder – bei geringeren Verstößen – lediglich auf die Verletzung von Vorschriften hinweisen mit der Bitte, diese abzustellen.

Zu Absatz 3

Diese Vorschrift entspricht den Vorgaben des Gesetzes über Ordnungswidrigkeiten, die eine Benennung der zuständigen Verwaltungsbehörde für die Verfolgung der Ordnungswidrigkeiten, hier die Regulierungsbehörde für Telekommunikation und Post, verlangt.

Die Zuständigkeit für die Verhängung von Bußgeldern soll bei der zuständigen Behörde nach § 3 SigG-E liegen. Sie verfügt über die erforderliche Fachkompetenz, um die relevanten Tatbestände entsprechend beurteilen zu können.

Zu § 22

Die Vorschrift greift auf § 4 Abs. 6 SigG zurück. Sie wird im Rahmen der neuen Struktur des Gesetzentwurfs an dieser Stelle als eigenständige Vorschrift eingefügt.

Der Wortlaut der Kostenvorschrift in Absatz 1 geht über den des geltenden Signaturgesetzes hinaus, in dem nur von „öffentlichen Leistungen" die Rede ist. Der für Absatz 1 gewählte Begriff „Amtshandlungen" entspricht dem des Verwaltungskostengesetzes, das hier Anwendung findet. Die weitergehende Fassung mit der enumerativen Beschreibung der kostenpflichtigen Maßnahmen der zuständigen Behörde ist im Hinblick auf die nach den Vorgaben der Richtlinie neu hinzutretenden Aufgaben der zuständigen Behörde (Aufsicht über die Zertifizierungsdiensteanbieter) notwendig. Diese Maßnahmen decken alle Amtshandlungen im Zusammenhang mit der Aufsicht ab. Die Vorschrift des § 19 SiG-E sieht keine systematischen, sondern vielmehr anlassbezogene Aufsichtsmaßnahmen vor (vgl. dazu Ausführungen zu § 19 Abs.1). Mit dem neuen Satz 2 wird sichergestellt, dass alle Kosten für beauftragte private Stellen von dieser Regelung erfasst werden. Bei der Inanspruchnahme privater Stellen ist stets der Tatbestand nach § 22 Abs. 1 SigG-E gegeben.

Absatz 2 regelt Kosten, die im Zusammenhang mit dem Führen eines online abrufbaren Verzeichnisses nach §§ 16 Abs. 3 und 19 Abs. 6 SigG-E entstehen. Es wird im übrigen hinsichtlich der Bemessung der Jahresgebühr auf die Ausführungen zu den Kosten unter A. II. 4 verwiesen.

Zu § 23

Mit der Vorschrift werden die Artikel 4 EGSRL (Binnenmarktgrundsätze), Artikel 5 EGSRL (Rechtswirkung elektronischer Signaturen) und Artikel 7 EGSRL (internationale Aspekte) umgesetzt.

Zu Absatz 1

Elektronische Signaturen, die auf einem ausländischen qualifizierten Zertifikat beruhen und die Voraussetzungen nach Artikel 5 Abs. 1 EGSRL erfüllen, werden qualifizierten elektronischen Signaturen gleichgestellt. Dies bezieht sich sowohl auf die EG-Mitgliedstaaten (Satz 1) als auch auf Drittstaaten (Satz 2), wenn eine der unter den Nummern 1 bis 3 genannten Voraussetzungen vorliegt.

Die Vorschrift bezieht sich nur auf qualifizierte elektronische Signaturen und die an diese geknüpften Rechtsfolgen. Andere elektronische Signaturen, die im Gesetz nicht näher geregelt werden, sind bereits nach der bestehenden Rechtslage gleichgestellt.

Zu Absatz 2

Damit ausländische elektronische Signaturen den qualifizierten elektronischen Signaturen des Verfahrens der freiwilligen Akkreditierung nach § 15 SigG-E rechtlich gleichgestellt werden können, müssen diese nachweislich gleichwertige Sicherheit aufweisen. Dazu müssen sie gleichen oder gleichwertigen Anforderungen, wie sie im SigG-E und der Rechtsverordnung nach § 24 SiG-E festgelegt sind, unterliegen. Außerdem muss die Erfüllung der Anforderungen vorab im Rahmen eines Akkreditierungsverfahrens (sowie bei den Zertifizierungsdiensteanbietern danach in regelmäßigen Zeitabständen und bei sicherheitserheblichen Veränderungen) in gleicher oder gleichwertiger Weise geprüft und bestätigt worden sein. Die Gleichwertigkeit wird durch die für die freiwillige Akkreditierung zuständige Behörde festgestellt. Einzelheiten regelt die Rechtsverordnung nach § 24 SigG-E.

Hiervon unberührt bleibt die Anerkennung von Zertifikaten und den darauf basierenden Signaturen nach Artikel 7 Abs. 1 Buchst. a) EGSRL, wie sie in Absatz 1 geregelt ist. Zertifikate, die nach Artikel 7 Abs. 1 Buchst. a) EGSRL aufgrund eines Verfahrens der freiwilligen Akkreditierung gemäß der Richtlinie außerhalb des Geltungsbereichs des Signaturgesetzes ausgestellt wurden, werden nach Absatz 1 anerkannt. Das Gleiche gilt für den Fall des Artikel 7 Abs. 1 Buchst. c) EGSRL (bilaterale oder multilaterale Vereinbarungen), der ebenfalls im Absatz 1 geregelt ist. Um eine Anerkennung nach Absatz 2 zu erreichen, müssen die oben genannten Voraussetzungen namentlich des § 15 SigG-E, erfüllt sein.

Das Verfahren der freiwilligen Akkreditierung nach § 15 SigG-E steht jedem ausländischen Anbieter offen; er unterliegt den gleichen Bedingungen wie deutsche Anbieter. Die Richtlinie räumt nach Artikel 3 Abs. 2 den einzelnen Mitgliedstaaten ausdrücklich die Möglichkeit ein, freiwillige Akkreditierungssysteme einzuführen oder beizubehalten.

Zu Absatz 3

Mit der Vorschrift in Satz 1 wird Artikel 4 Abs. 2 EGSRL umgesetzt. Produkte für elektronische Signaturen, bei denen die Erfüllung der Anforderungen nach der Richtlinie in einem anderen EG-Mitgliedstaat festgestellt wurde, werden denen nach dem Signaturgesetz gleichgestellt.

Etwas anderes gilt nach Satz 2 für die im Rahmen einer freiwilligen Akkreditierung nach besonderen Modalitäten geprüften Produkte gemäß § 15 Abs. 8 SigG-E. Damit ausländische Produkte diesen Produkten gleichgestellt werden können, müssen sie nachweislich gleichwertige Sicherheit aufweisen, d.h. sie müssen gleichen oder gleichwertigen Sicherheitsanforderungen unterliegen und die Sicherheit muss in gleicher oder gleichwertiger Weise geprüft und bestätigt worden sein.

Zu § 24

Die Vorschrift greift auf § 16 SigG zurück und wird an den Gesetzentwurf angepasst. Neben einer redaktionellen Anpassung an die neuen Begriffe des § 2 SigG-E wird der Ermächtigungsumfang dem veränderten Regelungsumfang des SigG-E angepasst und präzisiert.

Zu Nummer 1

Nummer 1 greift auf § 16 Nr. 3 SigG zurück und wird hinsichtlich des Ermächtigungsumfangs präzisiert. Es handelt sich bei Nummer 1 um die gesetzlichen Kernpflichten der Zertifizierungsdiensteanbieter. Eine Ausgestaltung der Pflichten der Zertifizierungsdiensteanbieter in der Signaturverordnung trägt zur Rechts- und Planungssicherheit für die Unternehmen bei und schafft die erforderliche Handlungsgrundlage für die zuständige Behörde zur Umsetzung eines geeigneten Systems der Überwachung nach den Vorgaben der Richtlinie. Der Ausgestaltung bedürfen daher die Regelungen zur Betriebsanzeige (§ 4 Abs. 2 und 3 SigG-E), zur Vergabe der qualifizierten Zertifikate (§ 5 SigG-E), der Unterrichtungspflicht (§ 6 Abs. 1 SigG-E), der Sperrung von qualifizierten Zertifikaten (§ 8 SigG-E), der Dokumentation (§ 10 SigG-E), der Deckungsvorsorge (§ 12 SigG-E), der Einstellung des Betriebes (§13 SigG-E) und der freiwilligen Akkreditierung (§ 15 SigG-E).

Zu Nummer 2

Nummer 2 umfasst die Ermächtigung für die in § 22 Abs. 1 und 2 geregelten Kosten. Hinsichtlich der Bemessung der Beiträge für die Jahresgebühr nach § 22 Abs. 2 SigG-E wird auf die Ausführungen zu den Kosten unter A. II. 4. verwiesen.

Zu Nummer 3

Nummer 3 greift auf § 16 Nr. 4 SigG zurück. Im Hinblick auf mögliche notwendige Anpassungen an Ergebnisse des Ausschusses nach Artikel 9 EGSRL und im Interesse

der Rechtssicherheit wird die bisher auf die Gültigkeitsdauer beschränkte Ermächtigung auf den näheren Inhalt der Zertifikate erweitert.

Zu Nummer 4

Nummer 4 greift auf § 16 Nr. 6 SigG zurück. Die Vorschrift wird nur an die neuen Begriffe in § 2 SigG-E angepasst und durch Nennung der Bezugsvorschriften im SigG-E präzisiert.

Zu Nummer 5

Die Nummer 5 ist Folge der neuen Vorschrift nach § 18 SigG-E.

Zu Nummer 6

Die Nummer 6 greift auf § 16 Nr. 7 SigG zurück.

Zu Nummer 7

Die Nummer 7 ist Folge der neuen Vorschrift nach § 23 SigG-E.

Zu § 25

Die Übergangsvorschrift gibt Unternehmen und Privatpersonen, die im Vertrauen auf das geltende Signaturgesetz in eine entsprechende Infrastruktur investiert haben, Bestands- und Investitionsschutz.

Absatz 1 gilt für Zertifizierungsdiensteanbieter, die über eine Genehmigung nach geltendem SigG verfügen. Die Regelungen der Absätze 2 und 4 betreffen darüber hinaus den Bestandsschutz für Privatpersonen sowie für Unternehmen und Behörden bezüglich deren Mitarbeiter, die Zertifikate und Produkte für die Anwendung elektronischer Signaturen beschafft haben. Die Regelung in Absatz 3 betrifft die Prüf- und Bestätigungsstellen, die sich auf Prüfungen oder Bestätigungen nach dem geltenden Signaturgesetz eingerichtet haben. Die Regelung in Absatz 4 betrifft vor

allem auch Hersteller von gesetzeskonformen Produkten, die in die Herstellung und Entwicklung dieser Produkte investiert haben.

Die Gleichstellung der Leistungen und Produkte nach dem geltenden Signaturgesetz ist gerechtfertigt, da diese auch die Anforderungen des SigG-E, namentlich die des § 15 SigG-E, in vollem Umfange erfüllen. Die nach dem geltenden Signaturgesetz ausgestellten Zertifikate sind lediglich nicht formal als „qualifiziert" klassifiziert. Dies kann dadurch behoben werden, dass die Zertifizierungsdiensteanbieter ihren Kunden automatisch neue Zertifikate mit diesem Zusatz ausstellen.

Zu Artikel 2
Umstellung von Vorschriften auf Euro

Im Gesetz sind zur Regelung der Deckungsvorsorge nach § 12 SigG-E und zum Bußgeld nach § 21 SigG-E Beträge vorgesehen, die in Deutscher Mark beziffert sind. Die Bußgeldbeträge sind erst dann in Euro anzugeben, wenn das Gesetz zur Währungsumstellung am 1. Januar 2002 in Kraft tritt, da die öffentliche Verwaltung erst ab diesem Zeitpunkt mit Euro-Beträgen operieren wird.

Zu Artikel 3
Anpassung von Bundesrecht

Artikel 3 nennt Regelungen des Bundes, die auf digitale Signaturen nach geltendem Signaturgesetz verweisen.

Zu Absatz 1

§ 15 Satz 2 der Verordnung über die Vergabe öffentlicher Aufträge sieht für elektronische Dokumente vor, dass diese mit einer Signatur nach geltendem Signaturgesetz zu versehen sind. Der Wortlaut wird durch den Verweis auf qualifizierte elektronische Signaturen nach § 2 Nr. 3 SigG-E an die künftige Rechtslage angepasst.

Zu Absatz 2

§ 7 Absatz 3 der Sozialversicherungs-Rechnungsverordnung sieht vor, dass die Zahlungsanordnung im Rahmen der Verordnung von dem zur Anordnung Befugten entweder durch Unterschrift oder mit einer digitalen Signatur nach dem geltenden Signaturgesetz zu versehen ist. Der Wortlaut wird durch den Verweis auf qualifizierte elektronische Signaturen nach § 2 Nr. 3 SigG-E an die künftige Rechtslage angepasst.

Zu Artikel 4

Rückkehr zum einheitlichen Verordnungsrang

Um zu vermeiden, dass die im Rahmen des auf Artikel 3 Abs. 1 und 2 beruhenden Teile der dort geänderten Rechtsverordnung künftig nur noch durch Gesetz, aber nicht mehr vom Verordnungsgeber späteren Erfordernissen angepasst werden können, wird eine besondere Bestimmung vorgesehen, die dies gestattet.

Zu Artikel 5

Inkrafttreten

Artikel 5 regelt das Inkrafttreten der Artikel 1 bis 4 sowie das zeitgleiche Außerkrafttreten des geltenden Signaturgesetzes. Das neue Signaturgesetz löst damit das geltende Signaturgesetz ab. Artikel 2 tritt erst mit Umstellung der Währung von Deutscher Mark auf Euro in Kraft.

Die Richtlinie sieht in Artikel 14 eine Umsetzungsfrist bis zum 19. Juli 2001 vor. Eine frühzeitige Umsetzung bereits zum 1. Januar 2001 ist zulässig. Sie trägt dem Erfordernis der raschen Anpassung an die Standards der Europäischen Union Rechnung und soll einen Beitrag dazu leisten, den erreichten Vorsprung auf dem Gebiet der digitalen bzw. elektronischen Signaturen zu sichern und weiter auszubauen.

Bundesrat Drucksache **496/00** (Beschluss)

29.09.00

Stellungnahme
des Bundesrates

Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften

Der Bundesrat hat in seiner 754. Sitzung am 29. September 2000 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Abs. 2 des Grundgesetzes wie aus der Anlage ersichtlich Stellung zu nehmen.

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 1320, 53003 Bonn
Telefon: 0228/3820840, Telefax: 0228/3820844
ISSN 0720-2946

Anlage

Stellungnahme

zum

Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften

1. Zu Artikel 1 (§ 2 SigG)

Die Bundesregierung wird gebeten, im weiteren Gesetzgebungsverfahren zu prüfen, ob

1. in § 2 eine Definition für die in § 15 Abs. 2 angesprochenen dauerhaft überprüfbaren qualifizierten Signaturen, die auf einem qualifizierten Zertifikat eines akkreditierten Anbieters beruhen, getroffen werden kann.
2. in § 2 eine gesonderte Definition für diejenigen Nachweise zu treffen ist, die in § 16 Abs. 1 Satz 1 als qualifizierte Zertifikate bezeichnet werden.

Begründung:

Zu Nummer 1

Die in § 15 Abs. 2 angesprochenen qualifizierten elektronischen Signaturen unterscheiden sich von anderen qualifizierten elektronischen Signaturen im Sinne des § 2 Nr. 3 dadurch, dass sie auf einem qualifizierten Zertifikat eines akkreditierten Zertifizierungsdiensteanbieters beruhen und deshalb dauerhaft überprüfbar sind. Eine Legaldefinition hätte den Vorteil, dass auf sie in anderen Rechtsvorschriften Bezug genommen werden kann.

Zu Nummer 2

Soweit ersichtlich, wird der Begriff des qualifizierten Zertifikats in § 16 Abs. 1 Satz 1 in einem anderen Sinne als in den übrigen Vorschriften verwendet. Nach § 2 Nr. 7 sind qualifizierte Zertifikate ausschließlich von Zertifizierungsdiensteanbietern für natürliche Personen ausgestellte

besonderen Anforderungen genügende elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer bestimmten Person zugeordnet werden. Hingegen wird in § 16 Abs. 1 Satz 1 der Begriff des qualifizierten Zertifikates auch für einen Nachweis verwendet, den die zuständige Behörde akkreditierten Zertifizierungsdiensteanbietern ausstellt.

2. Zu Artikel 1 (§ 6 Abs. 2 Satz 1 SigG)

In Artikel 1 sind in § 6 Abs. 2 Satz 1 nach dem Wort "Antragsteller" die Wörter "bei der erstmaligen Antragstellung" einzufügen.

Begründung:

Der Antrag dient der Klarstellung des Gewollten. Der Begründung des Gesetzentwurfs (vgl. S. 44) ist zu entnehmen, dass eine Unterrichtung bei einer erneuten Antragstellung (bei demselben oder einem anderen Zertifizierungsdienst) generell entbehrlich sein soll. Dies kommt im Text des § 6 Abs. 2 SigG-E aber nicht zum Ausdruck. Ganz im Gegenteil verleitet § 6 Abs. 2 Satz 3 SigG-E sogar dazu, den umgekehrten Schluss zu ziehen.

3. Zu Artikel 1 (§ 6 Abs. 2 Satz 2 SigG)

In Artikel 1 sind in § 6 Abs. 2 Satz 2 nach dem Wort "schriftliche" die Wörter ", nicht notwendig eigenhändig unterschriebene" einzufügen.

Begründung:

Es ist zur Erreichung des Zwecks der Unterrichtung nicht erforderlich, dass die schriftliche Belehrung vom Zertifizierungsdiensteanbieter eigenhändig unterschrieben wird. Dass kein Erfordernis einer eigenhändigen Unterschrift besteht, muss in der Regelung aber wegen § 126 Abs. 1 BGB zum Ausdruck kommen.

4. Zu Artikel 1 (§ 11 SigG)

In Artikel 1 ist § 11 wie folgt zu fassen:

"§ 11

Haftung

(1) Verletzt ein Zertifizierungsdiensteanbieter seine Pflichten nach diesem Ge-

...

setz oder der Rechtsverordnung nach § 24 oder versagen seine Produkte für elektronische Signaturen oder sonstige technische Sicherungseinrichtungen, so hat er

1. dem Empfänger einer qualifizierten elektronischen Signatur, die auf einem von ihm ausgestellten Zertifikat beruht,
2. dem Empfänger eines von ihm ausgestellten qualifizierten Zeitstempels,
3. einer dritten Person, für die nach einem von ihm ausgestellten qualifizierten Zertifikat der Signaturschlüssel-Inhaber die Vertretungsmacht haben soll oder
4. dem Empfänger einer Auskunft nach § 5 Abs. 1 Satz 2

den aus der Pflichtverletzung oder dem Versagen der Sicherungseinrichtungen entstehenden Schaden zu ersetzen. Die Ersatzpflicht tritt nicht ein, wenn der Zertifizierungsdiensteanbieter nicht schuldhaft gehandelt hat.

(2) Wenn ein qualifiziertes Zertifikat oder ein qualifizierter Zeitstempel die Nutzung des Signaturschlüssels oder des Zeitstempels auf bestimmte Anwendungen nach Art oder Umfang beschränkt, tritt die Ersatzpflicht nur im Rahmen dieser Beschränkungen ein.

(3) § 831 Abs. 1 Satz 2 des Bürgerlichen Gesetzbuchs ist nicht anzuwenden.

(4) Ein Zertifizierungsdiensteanbieter, der gemäß § 23 Abs. 1 Satz 2 Nr. 2 für ein Zertifikat eines Anbieters aus einem Drittstaat einsteht, haftet für dessen Handeln wie für eigenes Handeln.

(5) Die Absätze 1 bis 4 sind auf sonstige Zertifikate oder Zeitstempel entsprechend anzuwenden, soweit nicht die Zertifizierungsstelle ihre Pflichten oder ihre Haftung in dem Zertifikat oder Zeitstempel beschränkt hat."

...

Begründung:

Die Haftungsvorschrift ist so zu fassen, dass sie unmissverständlich eine deliktische Haftung zum Gegenstand hat. Diese Klarstellung ist erforderlich, damit kein Zweifel darüber besteht, welche allgemeinen Vorschriften für die Haftung gelten, insbesondere hinsichtlich der Gehilfenhaftung und der Verjährung.

Die deliktische Haftung ist sachangemessen, wenn für Gehilfen uneingeschränkt gehaftet wird und wenn die Beweislast hinsichtlich des Verschuldens beim Zertifizierungsdiensteanbieter liegt. Die vertragliche Haftung gegenüber dem Signaturschlüssel-Inhaber bedarf keiner besonderen gesetzlichen Regelung. Für die Haftung gegenüber Dritten ist zwar auch an eine Haftung auf Grund eines Vertrages mit Schutzwirkung zu Gunsten Dritter zu denken (vgl. Palandt/Heinrichs, BGB-Komm., 59. Aufl., § 328 Rdnr. 32). Die deliktische Haftung bietet jedoch den Vorteil, dass sie nicht durch Rechtswahl gemäß Artikel 27 EGBGB eingeschränkt werden kann. Sie ist auch nicht mit einer Haftungsobergrenze beschränkt, wie das bei einer Gefährdungshaftung zu erwarten wäre.

In Absatz 1 sind - einem allgemeinen Grundsatz des Deliktsrechts folgend - die Ansprüche auf einen Personenkreis zu beschränken, der unmittelbar Adressat der elektronischen Signatur, des Zeitstempels oder der Auskunft ist. Ohne eine solche Beschränkung würde die Haftung uferlos und für den Haftenden nicht mehr kalkulierbar.

Andererseits müssen auch diejenigen einen Ersatzanspruch erhalten, über die in einem Zertifikat zu Unrecht bescheinigt wird, der Signaturschlüssel-Inhaber habe für sie Vertretungsmacht. Gerade in diesem Punkt muss ein wesentliches Schadenspotenzial angenommen werden.

Absatz 1 Satz 2 der vorgeschlagenen Fassung übernimmt im Kern den Regelungsgehalt des Absatzes 2 des Entwurfs, bringt ihn aber in die sachgerechte Fassung. Der Entwurf will zu Recht und in Übereinstimmung mit Artikel 6 Abs. 1 der Richtlinie die Beweislast hinsichtlich des Verschuldens dem Zertifizierungsdiensteanbieter auferlegen, weil der Geschädigte kaum eine Chance hätte, das Verschulden zu beweisen. Die Fassung des Entwurfs "wenn er die Verletzung nicht zu vertreten hat" knüpft an § 276 Abs. 1 Satz 1 BGB an, der sich allerdings auf bestehende Schuldverhältnisse bezieht und deshalb für eine deliktische Haftung gegenüber Dritten nicht sachgerecht ist. Es muss vielmehr ausgesprochen werden, dass der Zertifizierungsdiensteanbieter darzulegen und zu beweisen hat, dass ihn kein Verschulden trifft.

Auf die Regelung in Absatz 1 Satz 2 des Entwurfs sollte verzichtet werden. Ohne eine solche Vorschrift gilt § 254 BGB und führt zu einem angemessenen Interessenausgleich zwischen den Beteiligten. Hingegen gibt es keinen hinreichenden Grund, einen Ersatzanspruch des Geschädigten schon dann vollständig auszuschließen, wenn ihn nur leichtes Verschulden trifft, selbst bei einem schweren Verschulden auf der Seite des Zertifizierungsdiensteanbieters.

Die in Absatz 3 des Entwurfs enthaltene Regelung der Verwendungsbeschränkung für qualifizierte Zertifikate muss auf Verwendungsbeschränkungen in qualifizierten Zeitstempeln ausgedehnt werden (Absatz 2 der vorgeschlagenen Fassung). Bei Zeitstempeln gibt es in gleicher Weise wie bei Zerti-

...

fikaten ein Bedürfnis, die Verwendung nach Art und Umfang einzuschränken und damit das Haftungsrisiko zu verringern.

Dass der Entwurf in Absatz 4 Satz 2 die Anwendung von § 831 Abs. 1 Satz 2 BGB ausschließen will, ist sachgerecht. Allerdings muss die Möglichkeit des Entlastungsbeweises für alle Verrichtungsgehilfen ausgeschlossen werden, nicht nur für die gemäß § 4 Abs. 5 beauftragten Dritten und für ausländische Zertifizierungsstellen, für die der Anbieter einsteht. Insbesondere muss für die eigenen Leute eine uneingeschränkte Gehilfenhaftung gelten. Anderenfalls könnte die Haftung empfindlich eingeschränkt sein, denn in aller Regel werden die Zertifizierungsdiensteanbieter juristische Personen sein, und die Organhaftung nach § 31 BGB wird nur in den seltensten Fällen eingreifen. Deswegen kommt es auf eine uneingeschränkte Haftung für die Mitarbeiter an. Entscheidend ist es deshalb, die Entlastungsmöglichkeit des § 831 Abs. 1 Satz 2 BGB umfassend auszuschließen.

Unter dieser Voraussetzung ist es nicht erforderlich, in Absatz 4 Satz 1 des Entwurfs eine Haftung des Anbieters für beauftragte Dritte zu regeln, weil sie Verrichtungsgehilfen sind, für die ohnehin nach § 831 BGB gehaftet wird. Lediglich hinsichtlich des Einstehens für Zertifikate aus Drittstaaten sollte die Regelung in Absatz 4 übernommen werden.

Die Haftungsregelung wäre jedoch unvollständig, wenn sie auf qualifizierte Zertifikate und Zeitstempel beschränkt würde. Die Richtlinie gestattet nicht nur solche qualifizierten Produkte und dementsprechend geht auch der Entwurf davon aus, dass es daneben einfache und fortgeschrittene elektronische Signaturen geben kann. In der Praxis können insbesondere Kostengesichtspunkte dafür sprechen, solche einfacheren Formen anzubieten und zu akzeptieren, ebenso der Umstand, dass im Rahmen der Richtlinie nur eingeschränkte Möglichkeiten einer Haftungsbeschränkung bestehen. Auch bei diesen Signaturen kann sich die Haftungsfrage stellen. Wenn es insoweit an einer speziellen Regelung fehlt, müssen die allgemeinen Normen herangezogen werden, etwa eine Haftung auf Grund eines Vertrages mit Schutzwirkung zu Gunsten Dritter (vgl. Palandt/Heinrichs, BGB-Komm., 59. Aufl., § 328 Rdnr. 32). Es wäre jedoch schwer hinnehmbar, wenn für Zertifikate mit und ohne Qualifikation nach grundsätzlich unterschiedlichen Anspruchsnormen gehaftet würde.

Deshalb empfiehlt es sich, in Absatz 5 die Vorschriften der Absätze 1 bis 4 auf Zertifikate und Zeitstempel ohne Qualifikation für entsprechend anwendbar zu erklären, jedoch mit der wesentlichen Einschränkung, dass die Anbieter im Zertifikat ihre Pflichten und ihre Haftung - auch betragsmäßig - einschränken können. Ob solche Leistungen, zu geringeren Preisen, aber auch mit eingeschränkter Haftung, akzeptiert werden, kann der Markt entscheiden.

5. Zu Artikel 1 (§ 12 SigG)

In Artikel 1 ist § 12 wie folgt zu ändern:

...

a) Satz 1 ist wie folgt zu fassen:

"Der Zertifizierungsdiensteanbieter hat dafür Sorge zu tragen, dass er seinen gesetzlichen Verpflichtungen zum Ersatz von Schäden nachkommen kann, die dadurch entstehen, dass er die Anforderungen dieses Gesetzes oder der Rechtsverordnung nach § 24 verletzt oder seine Produkte für elektronische Signaturen oder sonstige technische Sicherungseinrichtungen versagen."

b) In Satz 2 ist die Angabe "§ 11" durch die Angabe "Satz 1" zu ersetzen.

Begründung:

Der Bundesrat begrüßt die Einführung einer Verpflichtung der Zertifizierungsdiensteanbieter zur Deckungsvorsorge. Die Anknüpfung der Verpflichtung an "durch den Betrieb eines Zertifizierungsdienstes schuldhaft verursachte Schäden" ist jedoch abzulehnen. Für eine Haftung nach § 11 SigG-E reicht es bereits aus, dass der Zertifizierungsdiensteanbieter fehlendes Verschulden nicht nachweisen kann. § 11 SigG-E setzt demnach die positive Feststellung eines Verschuldens nicht voraus. Außerdem sollte in § 12 Satz 2 SigG-E nicht nur der Anspruch nach § 11 SigG-E als Anknüpfungspunkt der Deckungsvorsorgepflicht gewählt werden, sondern wie in § 19 UmweltHG das Schadensrisiko, um auch unter Umständen gegebene konkurrierende Ansprüche einzubeziehen.

6. Zu Artikel 1 (§ 12 Satz 2 SigG)

Der Bundesrat bittet die Bundesregierung, im weiteren Gesetzgebungsverfahren zu prüfen, ob die Mindestdeckungssumme von 500 000 Deutsche Mark bzw. 250 000 Euro je haftungsauslösendem Ereignis ausreichend ist.

Begründung:

Die in der Begründung des Gesetzentwurfs (S. 55) enthaltenen Ausführungen zur Festlegung der Mindestdeckungssumme von 500 000 DM bzw. 250 000 Euro (vgl. Artikel 2) je haftungsauslösendem Ereignis sind sehr knapp gehalten und können nicht befriedigen. Der Hinweis, dass geldwerte Transaktionen (z.B. beim Online-Banking) regelmäßig unter den genannten Beträgen liegen, lässt außer Betracht, dass - wie in der Begründung auf S. 54 zutreffend ausgeführt - ein haftungsauslösendes Ereignis (z.B. ein gefälschtes Zertifikat) eine unbestimmte Vielzahl von Einzelschäden auslösen kann, für die die Mindestsumme insgesamt nur einmal bereitsteht.

...

7. Zu Artikel 1 (§§ 12 und 24 Nr. 1 SigG)

Der Bundesrat bittet die Bundesregierung sicherzustellen, dass die Verordnung zur Ausgestaltung der Deckungsvorsorge zusammen mit dem reformierten Signaturgesetz in Kraft tritt.

Begründung:

Es erscheint inakzeptabel, die nähere Ausgestaltung der Deckungsvorsorge einer Verordnung zu überlassen, wenn nicht sicher gestellt ist, dass sie zusammen mit dem reformierten Signaturgesetz in Kraft tritt. Andernfalls ließe sich - nach den Erfahrungen im Bereich des Gentechnikgesetzes und der Umwelthaftung - kaum vorhersagen, ob und wann die Verordnung jemals erlassen werden wird. Auch bliebe völlig unklar, was unter einer geeigneten Deckungsvorsorge im Sinne des § 12 SigG-E zu verstehen ist. Die daraus resultierende Rechtsunsicherheit wäre nicht nur für potenzielle Anspruchsteller, sondern auch für die Zertifizierungsdiensteanbieter angesichts der nach § 19 Abs. 3 Nr. 3 SigG-E drohenden Sanktionen untragbar. Ob eine hohe Kapitaldeckung einer Zertifizierungsstelle als Deckungsvorsorge ausreicht, wie in der Entwurfsbegründung (S. 54) ausgeführt, erscheint sehr zweifelhaft.

8. Zu Artikel 1 (§ 24 Nr. 1 SigG)

Der Bundesrat bittet die Bundesregierung, im weiteren Gesetzgebungsverfahren zu prüfen, ob die Verordnungsermächtigung zur Ausgestaltung der Deckungsvorsorge in der gegenwärtigen Fassung (§ 24 Nr. 1) ausreichend ist.

Begründung:

Angesichts der strengen Vorgaben des Artikels 80 Abs. 1 Satz 2 GG bestehen erhebliche Bedenken, ob die Verordnungsermächtigung in § 24 Nr. 1 SigG-E zur Ausgestaltung der Deckungsvorsorge (§ 12 SigG-E) hinreichend bestimmt ist.