2065 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP

Bericht

des Justizausschusses

über die Regierungsvorlage (1999 der Beilagen): Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG)

Die weitere Entwicklung des elektronischen Geschäfts- und Rechtsverkehrs über offene Netzwerke, insbesondere das Internet, hängt nicht zuletzt davon ab, daß die Teilnehmer den modernen Kommunikationstechnologien uneingeschränkt vertrauen. Sie müssen sich insbesondere auf die Identität ihres Ansprechpartners verlassen können und Gewißheit darüber haben, daß die ihnen zugesandten oder von ihnen abgeschickten Erklärungen nicht unerkannt verändert werden. Technologien zur Sicherstellung der Authentizität (Bestätigung der Echtheit einer Erklärung) und Integrität (Unverfälschtheit des Inhalts) stehen mit den elektronischen Signaturverfahren zur Verfügung. Die zunehmende Verwendung moderner Technologien in nahezu allen Lebensbereichen wird die traditionellen Handels-, Vertriebs- und Kommunikationsformen nachhaltig beeinflussen. Voraussetzung dafür, daß sich die neuen Medien in der Wirtschaftswelt sowie in der Kommunikation zwischen den Bürgern und der öffentlichen Hand durchsetzen können, ist die rechtliche Anerkennung elektronischer Signaturen. Die vollwertige rechtliche Anerkennung elektronischer Signaturen erfordert aber geeignete organisatorische, infrastrukturelle, personelle und technische Rahmenbedingungen. Wegen des grenzüberschreitenden Charakters der neuen Medien sollen diese Rahmenbedingungen auf europäischer Ebene einheitlich festgesetzt werden. Diesem Anliegen will der Gemeinsame Standpunkt für eine Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen Rechnung tragen. Die Richtlinie wird voraussichtlich Anfang 2000 verabschiedet werden. Da davon ausgegangen werden kann, daß der Richtlinientext keine wesentlichen Änderungen erfahren wird, kann die Umsetzung der Richtlinie schon frühzeitig erfolgen und auf diese Weise der insbesondere seitens der österreichischen Wirtschaft erhobenen Forderung, die bestehenden Rechtsunsicherheiten in der Verwendung elektronischer Medien im Rechts- und Geschäftsverkehr zu beseitigen, nachgekommen werden. Damit wird auch eine wichtige Weiche für die Attraktivität des Wirtschaftsstandorts Österreich gestellt.

Die Regierungsvorlage schafft die rechtlichen Grundlagen für die Erbringung von Signatur- und Zertifizierungsdiensten sowie für die Verwendung sicherer Technologien im Internet und in anderen elektronischen Netzwerken. Dementsprechend werden die Tätigkeit und die Verantwortung von Zertifizierungsdiensteanbietern, die in einem Zertifikat die Identität einer Person bescheinigen, geregelt. Die Regierungsvorlage statuiert gewisse Verhaltenspflichten der Zertifizierungsdiensteanbieter, die der Sicherstellung der Transparenz der bereitgestellten Signatur- und Zertifizierungsdienste sowie eines dem Stand der Technik entsprechenden Sicherheitsstandards, insbesondere für sichere Signaturverfahren, dienen. Weiters werden die Zertifizierungsdiensteanbieter einer Aufsicht unterstellt, die Mißbräuche rasch und zuverlässig abstellen soll. Zur Überprüfung der Einhaltung der Sicherheitsanforderungen durch Signaturkomponenten werden geeignete, über das erforderliche technische Know-how verfügende Stellen, die sogenannten “Bestätigungsstellen”, vorgesehen. Die Regierungsvorlage regelt auch das Verhältnis zwischen den Zertifizierungsdiensteanbietern und den Anwendern. In erster Linie sind hier die Informations- und Beratungspflichten der Zertifizierungsdiensteanbieter sowie die Haftungsregelungen zu nennen. Darüber hinaus beschäftigt sich die Regierungsvorlage auch mit den Rechtswirkungen elektronischer Signaturen im Rechts- und Geschäftsverkehr. Sichere elektronische Signaturen, die unter Einhaltung der gesetzlichen Sicherheitsanforderungen erstellt werden, sind in ihren Rechtswirkungen grundsätzlich der

eigenhändigen Unterschrift gleichgestellt. Das bedeutet, daß sie grundsätzlich die einfache Schriftform erfüllen können. Im zivilrechtlichen Bereich werden sicher signierte elektronische Dokumente den eigenhändig unterschriebenen Privaturkunden gleichgestellt. Diejenigen Signaturverfahren, die nicht die für sichere Verfahren vorgesehenen Sicherheitsanforderungen erfüllen, dürfen im elektronischen Geschäftsverkehr verwendet werden und sind auch als Beweismittel im gerichtlichen oder behördlichen Verfahren zugelassen. Österreich ist einer der ersten Mitgliedstaaten der Europäischen Union, der über ein mit den gemeinschaftsrechtlichen Vorgaben in Einklang stehendes Signaturgesetz verfügt.

Der Justizausschuß hat die gegenständliche Regierungsvorlage in seiner Sitzung am 6. Juli 1999 in Verhandlung genommen.

An der Debatte beteiligten sich die Abgeordneten Mag. Thomas **Barmüller,** Dr. Liane **Höbinger-Lehrer,** Anna **Huber,** Dr. Harald **Ofner** und die Ausschußobfrau Mag. Dr. Maria Theresia **Fekter** sowie der Bundesminister für Justiz Dr. Nikolaus **Michalek.**

Die Abgeordneten Mag. Dr. Maria Theresia **Fekter** und Anna **Huber** brachten einen Abänderungsantrag ein, der wie folgt begründet war:

“Zu § 2:

Zur Klarstellung soll in § 2 Z 13 eine eigene Definition für ‚Signaturprodukt‘ aufgenommen werden. Für die Einhaltung der technischen Sicherheitsanforderungen sind in erster Linie die Signaturprodukte und die von diesen verwendeten technischen bzw. mathematisch/kryptographischen Verfahren verantwortlich. Signaturprodukte sind – entsprechend der Definition im Gemeinsamen Standpunkt für die Signaturrichtlinie – Hard- oder Softwarekomponenten bzw. Hard- und Softwarekombinationen, die für die Bereitstellung von Signatur- und Zertifizierungsdiensten sowie für die Erstellung und die Überprüfung elektronischer Signaturen verwendet werden. Dazu zählen insbesondere Signaturerstellungseinheiten und -prüfeinheiten, und zwar sowohl jene, die beim Zertifizierungsdiensteanbieter zur Anwendung gelangen, als auch jene, die von den Anwendern, also von den Signatoren und den Empfängern elektronisch signierter Erklärungen, verwendet werden. Die nach heutigem Stand der Technik bekannteste Signaturerstellungseinheit ist die Chipkarte samt Chip und der von diesem verwendeten Software. Eine Chipkarte besteht aus Kartenkörper, Hardware, Betriebssystem und entsprechenden Anwendungen. Der Kartenkörper kann als Trägermedium angesehen werden.

Die Einhaltung der gesetzlich normierten Sicherheitsanforderungen setzt entsprechende technische Vorkehrungen voraus. Zur Beschreibung von Manipulationen an solchen Sicherheitsvorkehrungen verwendet die Regierungsvorlage die Begriffe ‚Kompromittierung‘ bzw. ‚kompromittieren‘. Dabei handelt es sich um informationstechnologische Fachbegriffe, die im Zusammenhang mit elektronischen Signaturen ausdrücken, daß die geheimen Signaturerstellungsdaten – bei der digitalen Signatur der private Signaturschlüssel – ermittelt werden können. Denkbar wäre etwa, daß der private Signaturschlüssel ausgespäht, der Chipspeicher gebrochen oder der Signaturalgorithmus mathematisch ausgeforscht wird. Da der Begriff ‚Kompromittierung‘ in der Rechtssprache nicht gebräuchlich ist, soll er in § 2 Z 14 definiert werden. Damit sind jene Beeinträchtigungen der zur Einhaltung der Sicherheitsanforderungen getroffenen Vorkehrungen gemeint, die sich auf die Qualität des jeweiligen Signaturverfahrens auswirken, also die vom Zertifizierungsdiensteanbieter zugrundegelegte technische Sicherheit nicht mehr garantieren und damit sicherheitsrelevant sind. Erfaßt sind nicht nur die vom Zertifizierungsdiensteanbieter selbst veranlaßten Sicherheitsmaßnahmen, sondern auch mathematisch/kryptographische Verfahren, wie zB Signaturalgorithmen.

Zu § 6 Abs. 7:

Zur Änderung des § 6 Abs. 7 sei auf die Erwägungen zur Änderung des § 13 Abs. 3 verwiesen. Da die Aufsichtsstelle keine ‚zentrale Wurzelinstanz‘ ist, müssen die Zertifikate für Zertifizierungsdiensteanbieter nicht notwendigerweise von der Aufsichtsstelle ausgestellt werden.

Zu § 7 Abs. 1 Z 6:

Der Gemeinsame Standpunkt für eine Signaturrichtlinie sieht für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, vor, daß diese über ausreichende Finanzmittel verfügen müssen, um den Anforderungen der Richtlinie entsprechend arbeiten zu können. Sie müssen weiters in der Lage sein, das Haftungsrisiko für Schäden, zB durch Abschluß einer entsprechenden Versicherung, zu tragen (Anhang II lit. h). Solche qualifizierten Zertifizierungsdiensteanbieter müssen also das potentielle Haftungsrisiko abdecken können. Der Abschluß einer Haftpflichtversicherung wird ein probates Mittel zur Abdeckung dieses Risikos sein. Grundsätzlich kommen aber auch andere Sicherungsmittel, wie etwa

Bankgarantien oder Bürgschaften, in Betracht, wobei der Sicherungsgrad allerdings mit jenem einer Haftpflichtversicherung vergleichbar sein muß.

Die Regierungsvorlage schreibt den qualifizierten Zertifizierungsdiensteanbietern eine obligatorische Haftpflichtversicherung mit einer Versicherungssumme von mindestens 56 Millionen Schilling je Versicherungsfall vor. Mangels ausreichender praktischer Erfahrungen mit der Tätigkeit von Zertifizierungsdiensteanbietern kann das tatsächliche Haftungsrisiko und das daraus resultierende Haftungspotential allerdings noch nicht verläßlich eingeschätzt werden. Es kann daher auch nicht beurteilt werden, ob die vorgeschlagene Versicherungssumme angemessen ist. Weiters können auch zu den für die einschlägigen Versicherungsleistungen aufzuwendenden Versicherungsprämien keine näheren Aussagen getroffen werden. Um rasch auf marktbedingte Veränderungen des Haftungsrisikos reagieren zu können, soll im Gesetz keine Mindestversicherungssume vorgeschrieben, sondern – in Konformität mit dem Gemeinsamen Standpunkt für eine Signaturrichtlinie – nur vorgesehen werden, daß die Zertifizierungsdiensteanbieter Vorsorge für die Befriedigung von Schadenersatzansprüchen zu treffen haben. Die nähere Regelung, auf welche Weise die für die Ausübung der Tätigkeit als Zertifizierungsdiensteanbieter sowie zur Abdeckung des Haftungsrisikos notwendige Kapitalausstattung nachgewiesen werden muß, soll der Signaturverordnung vorbehalten bleiben. In der Signaturverordnung soll auch eine adäquate Mindestversicherungssumme für eine Haftpflichtversicherung festgesetzt werden. Dabei geht der Ausschuß davon aus, daß eine Versicherungssumme von 14 Millionen Schilling auf Grund der derzeit gegebenen Umstände ausreichen wird.

Zu § 9:

Bei qualifizierten Zertifikaten muß verpflichtend ein Widerrufsdienst geführt werden (§ 9 Abs. 4 der Regierungsvorlage). Bei ‚einfachen' Zertifikaten muß diese Entscheidung den Zertifizierungsdiensteanbietern überlassen werden, um inländische Zertifizierungsdiensteanbieter nicht gegenüber ausländischen Anbietern zu benachteiligen. Insbesondere bei Zertifikaten mit kurzer Gültigkeitsdauer oder Gratiszertifikaten wird in der Regel kein Widerrufsdienst geführt (vgl. § 6 Abs. 6 der Regierungsvorlage). Dem Zeitpunkt, zu dem der Widerruf eines Zertifikats wirksam wird, kommt große Bedeutung zu. Nur solche elektronischen Signaturen, die vor diesem Zeitpunkt erstellt wurden, sind gültig. Für den Empfänger einer elektronisch signierten Erklärung, der auf deren Gültigkeit vertraut, muß verläßlich feststellbar sein, ob zum Zeitpunkt der Erstellung der Signatur das Zertifikat noch gültig war. Aus diesem Grund wird in § 9 Abs. 3 die Wirksamkeit eines Widerrufs (bzw. einer Sperre) an die Eintragung in das Sperr- bzw. Widerrufsverzeichnis geknüpft, sofern nach dem Sicherheits- und Zertifizierungskonzept ein Widerrufsdienst geführt wird. Der Empfänger einer elektronischen Signatur hat somit die Gewähr, daß gegen ihn nur eingetragene Tatsachen, also solche Tatsachen, die ihm zugänglich sind, wirken können. Wird kein Widerrufsdienst geführt, so müssen die Sperre und der Widerruf vom Zertifizierungsdiensteanbieter zeitlich gesichert werden. Ein rückwirkendes Wirksamwerden dieser Maßnahmen ist ausgeschlossen.

Zur Änderung des § 9 Abs. 5 der Regierungsvorlage sei auf die Erwägungen zur Änderung des § 13 Abs. 3 verwiesen. Da die Aufsichtsstelle keine ‚zentrale Wurzelinstanz' ist, muß das Zertifikat eines Zertifizierungsdiensteanbieters nicht notwendigerweise von der Aufsichtsstelle ausgestellt werden.

Zu § 13:

Zur Änderung des § 13 Abs. 1 sei auf die Erwägungen zur Änderung des § 13 Abs. 3 verwiesen. Da die Aufsichtsstelle keine ‚zentrale Wurzelinstanz' ist, müssen die Zertifikate für Zertifizierungsdiensteanbieter nicht notwendigerweise von der Aufsichtsstelle ausgestellt werden.

Bei der Aufsichtsstelle sind unter anderem ein Verzeichnis der Zertifikate für Zertifizierungsdiensteanbieter sowie ein Verzeichnis der inländischen Zertifizierungsdiensteanbieter zu führen. Um Fälschungen dieser Verzeichnisse auszuschließen, müssen sie von der Aufsichtsstelle sicher elektronisch signiert werden. Die Verzeichnisse der (qualifizierten) Zertifikate für Zertifizierungsdiensteanbieter und der Zertifizierungsdiensteanbieter können gleichzeitig dazu verwendet werden, um zu prüfen, ob das von einem Zertifizierungsdiensteanbieter verwendete Zertifikat tatsächlich diesem zugeordnet ist, ihm also vertraut werden kann. Bei einem regulären Ablauf der Gültigkeitsdauer des Zertifikats eines Zertifizierungsdiensteanbieters wird der Anwender (vor allem der Empfänger einer elektronisch signierten Erklärung) in der Regel automatisch durch sein System dazu angehalten, das erneuerte Zertifikat des Zertifizierungsdiensteanbieters zu überprüfen und dessen Vertrauenswürdigkeit zu beurteilen. Zertifikate für Zertifizierungsdiensteanbieter können entweder von der Aufsichtsstelle oder vom jeweiligen Zertifizierungsdiensteanbieter selbst ausgestellt werden. In das bei der Aufsichtsstelle

geführte Zertifikatsverzeichnis dürfen allerdings nur qualifizierte Zertifikate für Zertifizierungsdiensteanbieter aufgenommen werden.

Die Eintragung eines Zertifizierungsdiensteanbieters in das bei der Aufsichtsstelle geführte Verzeichnis besagt im Grunde nur, daß der Zertifizierungsdiensteanbieter von der Aufsichtsstelle registriert wurde und die gesetzmäßige Aufsicht stattfindet. Den Anwendern (Signatoren und Empfängern signierter Erklärungen) steht es frei, als Ausgangspunkt ihres Vertrauenssystems ihren Zertifizierungsdiensteanbieter zu wählen, dh. die Vertrauenskette beim Zertifizierungsdiensteanbieter enden zu lassen und den Verzeichnisdienst der Aufsichtsstelle nicht ständig in Anspruch zu nehmen. Ein Zertifizierungsdiensteanbieter kann somit auch die Zertifikate anderer, vor allem ausländischer Zertifizierungsdiensteanbieter anerkennen und damit sogenannte ‚Cross-Zertifizierungen' vornehmen.

‚Wurzel-Zertifizierungsstelle' bzw. ‚zentrale Wurzelinstanz' bedeutet, daß bei der Signaturprüfung die Vertrauenskette jeweils bis zur höchsten Stelle in der Zertifizierungshierarchie geschlossen sein muß und diese höchste Stelle als Authentifizierungsgeber auftritt. Bei der Aufssichtsstelle nach dem Signaturgesetz handelt es sich nicht um eine derartige zentrale Wurzelinstanz. Wird der private Signaturschlüssel der Aufsichtsstelle kompromittiert, so sind damit nicht alle inländischen Zertifikate ungültig. Vielmehr behalten die Zertifikate der Zertifizierungsdiensteanbieter ihre Gültigkeit; die Vertrauenskette bis zum Zertifizierungsdiensteanbieter kann uneingeschränkt nachvollzogen werden. Das Zertifikat der Aufsichtsstelle kann etwa auch nicht mit Mitteln, die das Gesetz vorsieht, widerrufen werden. Auch aus diesem Grund muß das Zertifikat der Aufsichtsstelle im ‚Amtsblatt zur Wiener Zeitung' veröffentlicht werden. Im übrigen stellt die Kompromittierung des privaten Signaturschlüssels der Aufsichtsstelle ein Szenario dar, das nicht eintreten sollte. Zur Klarstellung soll aber § 13 Abs. 3 der Regierungsvorlage modifiziert werden, um alle Mißverständnisse auszuschließen.

Die Regierungsvorlage sieht in § 13 Abs. 5 vor, daß sich die Aufsichtsstelle zur Wahrnehmung ihrer Aufgaben einer Bestätigungsstelle bedienen kann. Hier soll klargestellt werden, daß sich die Tätigkeit einer Bestätigungsstelle auf sicherheitsrelevante technische Belange beschränkt und daß sich die Aufsichtsstelle im übrigen zur Beratung jeglicher geeigneter Person oder Einrichtung bedienen kann.

Zu § 14:

Von der Aufsichtsstelle sollen jeweils die gelindesten Aufsichtsmaßnahmen ergriffen werden, um die Einhaltung des gesetzmäßigen Zustandes sicherzustellen. Dementsprechend wird der Aufsichtsstelle in § 14 Abs. 6 der Regierungsvorlage die Möglichkeit eingeräumt, den Zertifizierungsdiensteanbietern Auflagen zu erteilen oder zur Behebung aufgezeigter Mängel geeignete Maßnahmen anzudrohen. In den Abs. 2, 3, 4 und 6 des § 14 soll dieser Vorrang ‚gelinderer Mittel' gegenüber der Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters ausdrücklich klargestellt werden.

Zu § 15:

Zur Änderung des § 15 Abs. 2 Z 3 sei auf die Erwägungen zur Änderung des § 13 Abs. 3 verwiesen. Da die Aufsichtsstelle keine ‚zentrale Wurzelinstanz' ist, müssen die Zertifikate für Zertifizierungsdiensteanbieter nicht notwendigerweise von der Aufsichtsstelle ausgestellt werden.

Zur Änderung des § 15 Abs. 3 sei auf die Erwägungen zur Änderung des § 13 Abs. 5 verwiesen. Wie die Aufsichtsstelle soll sich auch die Telekom-Control GmbH zur Beratung geeigneter Einrichtungen bedienen können.

Zu § 19:

Aus Gründen der Verwaltungsvereinfachung soll die Verordnung zur Feststellung geeigneter Bestätigungsstellen nach § 19 Abs. 3 vom Bundeskanzler im Einvernehmen (nur) mit dem Bundesminister für Justiz erlassen werden.

Als Bestätigungsstelle kommt jede Einrichtung in Betracht, die die in § 19 enthaltenen Kriterien erfüllt. Denkbar ist, daß auch private Einrichtungen als Bestätigungsstellen fungieren. Um den Wettbewerb zwischen mehreren Bestätigungsstellen nicht auszuschließen, soll das von den Zertifizierungsdiensteanbietern einer Bestätigungsstelle für deren im Rahmen des Evaluationsmanagements erbrachten Leistungen zu bezahlende Entgelt nicht mit Verordnung festgesetzt werden. Aus diesem Grund soll § 19 Abs. 5 der Regierungsvorlage entfallen. Die Bestätigungsstellen können damit den Zertifizierungsdiensteanbietern ein für ihre Leistungen angemessenes Entgelt in Rechnung stellen.

Zu § 23 Abs. 3:

Die Verursachungsvermutung einer wahrscheinlich gemachten Pflichtwidrigkeit oder eines solchen sicherheitsrelevanten technischen Eingriffs stellt zwar eine Beweiserleichterung für den Geschädigten

dar, sie soll aber nicht zu einer Umkehr der Beweislast führen, die dem Zertifizierungsdiensteanbieter den Gegenbeweis dafür auferlegt, daß die Pflichtwidrigkeit oder der Sicherheitseingriff nicht schadenskausal war. Vielmehr soll es genügen, daß der Zertifizierungsdiensteanbieter die Kausalität der Pflichtwidrigkeit zweifelhaft macht, also seinerseits wahrscheinlich macht, daß die Schadensursache nicht in einer Pflichtwidrigkeit bzw. in einem sicherheitsrelevanten Eingriff gelegen ist. Er muß also nur den vom Geschädigten geführten Anscheinsbeweis außer Kraft setzen. Insoweit soll § 23 Abs. 3 der Regierungsvorlage ergänzt werden. Außerdem steht dem Zertifizierungsdiensteanbieter der Beweis offen, daß er nicht pflichtwidrig oder nicht schuldhaft gehandelt hat.

Zu § 24 Abs. 3:

Nach dem Inkrafttreten der Signaturrichtlinie müssen von allen Mitgliedstaaten der Europäischen Union eine oder mehrere Bestätigungsstellen der Europäischen Kommission notifiziert werden. Bescheinigungen dieser Stellen über die Einhaltung der relevanten Sicherheitsanforderungen durch Signaturerstellungseinheiten müssen in allen anderen Mitgliedstaaten anerkannt werden, sind also den Bescheinigungen einer inländischen Bestätigungsstelle gleichzuhalten. Bis zum Inkrafttreten der Signaturrichtlinie muß für die Bescheinigungen schon bestehender Bestätigungsstellen in anderen Mitgliedstaaten eine ausdrückliche Anerkennungsregelung vorgesehen werden.

Zu § 25:

Aus Gründen der Verwaltungsvereinfachung soll die Kompetenz zur Erlassung der Signaturverordnung dem Bundeskanzler im Einvernehmen (nur) mit dem Bundesminister für Justiz zukommen.

Das von einer Bestätigungsstelle für ihre im Rahmen des Evaluationsmanagements erbrachten Leistungen vorgeschriebene Entgelt soll nicht mit Verordnung festgesetzt werden. Das erfordert eine Änderung des § 25 Z 1 der Regierungsvorlage.

Da im Gesetz aus den zu § 7 Abs. 1 Z 6 genannten Gründen keine Mindestversicherungssumme für eine Haftpflichtversicherung vorgeschrieben werden soll, müssen in der Verordnung auch Aussagen über die zur Abdeckung des Haftungsrisikos ausreichenden Finanzmittel getroffen werden. Insbesondere soll die Festsetzung einer Mindestversicherungssumme für eine Haftpflichtversicherung der Verordnung vorbehalten bleiben (siehe die Änderung des § 25 Z 2 der Regierungsvorlage).

Neben § 18 enthalten auch die §§ 7 Abs. 2 und 10 technische Sicherheitsanforderungen. Diese Sicherheitsanforderungen sind durch die Verordnung näher zu konkretisieren (siehe die Änderung des § 25 Z 4 der Regierungsvorlage).

Zu § 26:

Für Zertifizierungsdiensteanbieter besteht eine Reihe gesetzlicher Verhaltenspflichten, die der Sicherstellung der Transparenz der bereitgestellten Signatur- und Zertifizierungsdienste sowie eines dem Stand der Technik entsprechenden Sicherheitsstandards, insbesondere für sichere Signaturverfahren, dienen. Die Nichteinhaltung der für die Qualitätssicherung besonders wichtigen Verhaltenspflichten soll unter Verwaltungsstrafdrohung gestellt werden. Damit sollen allfällige Mißstände abgestellt und generalpräventiv verhindert werden können. Je nach der Bedeutung der Verhaltenspflichten für die Bereitstellung qualitätsgesicherter und vertrauenswürdiger Signatur- und Zertifizierungsdienste soll eine Gewichtung in den Strafdrohungen vorgenommen werden.

Zu den §§ 27 und 28:

Die neuen Bezeichnungen werden durch die Einfügung eines neuen § 26 notwendig.

Zu § 28:

Der neue § 26 ist in die Vollzugsklausel aufzunehmen (siehe die Änderung in der Z 3). Die übrigen Änderungen in den Vollzugsklauseln dienen der Verwaltungsvereinfachung.

Bei der Abstimmung wurde die Regierungsvorlage unter Berücksichtigung des erwähnten Abänderungsantrages in der diesem Bericht beigedruckten Fassung einstimmig angenommen.

Weiters hat der Justizausschuß einstimmig folgende Ausschußfeststellungen beschlossen:

“Zu § 1 Abs. 2:

Der Ausschuß ist der Auffassung, daß die Anforderungen des Signaturgesetzes an sichere elektronische Signaturverfahren grundsätzlich auch für die Verwendung im öffentlichen Bereich, dh. im Kommuni-

kationsverkehr unter und mit den Behörden und Gerichten, ausreichen. Daher müssen im öffentlichen Bereich keine zusätzlichen Anforderungen an das Signaturverfahren gestellt werden. Dieser Grundsatz gilt vorbehaltlich der spezifischen Gegebenheiten in einzelnen Verwaltungsbereichen, die vom jeweils zuständigen Ressort darzulegen sind.

Zu § 2 Z 11:

Von den Zertifizierungsdiensteanbietern dürfen sowohl Signatur- und Zertifizierungsdienste als auch Dienste zur Verschlüsselung des Inhalts elektronischer Daten bereitgestellt werden. Allerdings dürfen dadurch die Sicherheitsanforderungen für elektronische Signaturverfahren nicht beeinträchtigt werden. Die Aufrechterhaltung des Sicherheitsniveaus elektronischer Signaturen ist als oberste Maxime anzusehen. Insbesondere darf derselbe private Signaturschlüssel bzw. dasselbe Schlüsselpaar nicht zum Signieren und zur Verschlüsselung des Inhalts elektronischer Daten verwendet werden. Pflichten zur Mitwirkung an der Entschlüsselung gegenüber Gerichten oder anderen Strafverfolgungsbehörden könnten zu einer Offenlegung des privaten Signaturschlüssels führen. Darüber hinaus dürfen unterschiedliche Kryptographieschlüssel, die einerseits zum Signieren bzw. andererseits zur Verschlüsselung des Dateninhalts verwendet werden, etwa auch nicht durch dieselbe Personenidentifikationsnummer (PIN) gesichert sein, weil der Anwender nicht unterscheiden könnte, ob bei Anwendung des Schlüssels in einer bestimmten Umgebung die Signaturfunktion oder die Funktion zur Verschlüsselung des Dateninhalts ausgelöst wird. Beide Funktionen müssen für den Anwender nachvollziehbar auf unterschiedliche Weise ausgelöst werden.

Zu § 5 Abs. 1 Z 3:

Die Antragstellung sowie die Erbringung der Dienstleistung bleibt den vertraglichen Vereinbarungen zwischen den Beteiligten vorbehalten. Ist ein Zertifikatswerber nicht voll geschäftsfähig (zB minderjährig), so richtet sich die Möglichkeit des Erwerbs eines Zertifikats und der Verwendung der Signatur nach den Bestimmungen des ABGB zur Geschäftsfähigkeit. Hat ein Zertifizierungsdiensteanbieter Bedenken, daß der Zertifikatswerber geschäftsfähig ist, so darf er das beantragte Zertifikat nicht ausstellen. Bei dieser Beurteilung ist nicht nur auf den Erwerb des Zertifikats an sich, sondern auch auf die gegebenen Einsatzmöglichkeiten des Zertifikats abzustellen. Der Umstand der Minderjährigkeit, allenfalls auch einer Sachwalterbestellung, kann auch in das Zertifikat aufgenommen werden (vgl. § 5 Abs. 2 der Regierungsvorlage). Die verpflichtende Aufnahme des Geburtsdatums in das qualifizierte Zertifikat ist in Anhang I zur Signaturrichtlinie nicht vorgesehen. Inländische Zertifikate sollen gegenüber ausländischen nicht schlechter gestellt werden."

Als Ergebnis seiner Beratungen stellt der Justizausschuß den **Antrag,** der Nationalrat wolle dem **angeschlossenen Gesetzentwurf** die verfassungsmäßige Zustimmung erteilen.

Wien, 1999 07 06

Mag. Dr. Josef Trinkl	**Mag. Dr. Maria Theresia Fekter**
Berichterstatter	Obfrau

Anlage

Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG)

Der Nationalrat hat beschlossen:

1. Abschnitt

Gegenstand und Begriffsbestimmungen

Gegenstand und Anwendungsbereich

§ 1. (1) Dieses Bundesgesetz regelt den rechtlichen Rahmen für die Erstellung und Verwendung elektronischer Signaturen sowie für die Erbringung von Signatur- und Zertifizierungsdiensten.

(2) Dieses Bundesgesetz ist auch anzuwenden in geschlossenen Systemen, sofern deren Teilnehmer dies vereinbart haben, sowie im offenen elektronischen Verkehr mit Gerichten und anderen Behörden, sofern durch Gesetz nicht anderes bestimmt ist.

Begriffsbestimmungen

§ 2. Im Sinne dieses Bundesgesetzes bedeuten

1. elektronische Signatur: elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators, dienen;
2. Signator: eine natürliche Person, der Signaturerstellungsdaten und die entsprechenden Signaturprüfdaten zugeordnet sind und die entweder im eigenen oder im fremden Namen eine elektronische Signatur erstellt, oder ein Zertifizierungsdiensteanbieter, der Zertifikate für die Erbringung von Zertifizierungsdiensten verwendet;
3. sichere elektronische Signatur: eine elektronische Signatur, die
   a) ausschließlich dem Signator zugeordnet ist,
   b) die Identifizierung des Signators ermöglicht,
   c) mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann,
   d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, daß jede nachträgliche Veränderung der Daten festgestellt werden kann, sowie
   e) auf einem qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen, erstellt wird;
4. Signaturerstellungsdaten: einmalige Daten wie Codes oder private Signaturschlüssel, die vom Signator zur Erstellung einer elektronischen Signatur verwendet werden;
5. Signaturerstellungseinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturerstellungsdaten verwendet wird;
6. Signaturprüfdaten: Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden;
7. Signaturprüfeinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturprüfdaten verwendet wird;
8. Zertifikat: eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird;
9. qualifiziertes Zertifikat: ein Zertifikat, das die Angaben des § 5 enthält und von einem den Anforderungen des § 7 entsprechenden Zertifizierungsdiensteanbieter ausgestellt wird;

10. Zertifizierungsdiensteanbieter: eine natürliche oder juristische Person oder eine sonstige rechtsfähige Einrichtung, die Zertifikate ausstellt oder andere Signatur- und Zertifizierungsdienste erbringt;
11. Signatur- und Zertifizierungsdienste: die Bereitstellung von Signaturprodukten und -verfahren, die Ausstellung, Erneuerung und Verwaltung von Zertifikaten, Verzeichnis-, Widerrufs-, Registrierungs- und Zeitstempeldienste sowie Rechner- und Beratungsdienste im Zusammenhang mit elektronischen Signaturen;
12. Zeitstempeldienst: eine elektronisch signierte Bescheinigung eines Zertifizierungsdiensteanbieters, daß bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen sind;
13. Signaturprodukt: Hard- oder Software bzw. deren spezifische Komponenten, die für die Erstellung und Überprüfung elektronischer Signaturen oder von einem Zertifizierungsdiensteanbieter für die Bereitstellung von Signatur- oder Zertifizierungsdiensten verwendet werden;
14. Kompromittierung: die Beeinträchtigung von Sicherheitsmaßnahmen oder Sicherheitstechnik, sodaß das vom Zertifizierungsdiensteanbieter zugrundegelegte Sicherheitsniveau nicht eingehalten ist.

2. Abschnitt

Rechtserheblichkeit elektronischer Signaturen

Allgemeine Rechtswirkungen

§ 3. (1) Im Rechts- und Geschäftsverkehr können Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen verwendet werden.

(2) Die rechtliche Wirksamkeit einer elektronischen Signatur und deren Verwendung als Beweismittel können nicht allein deshalb ausgeschlossen werden, weil die elektronische Signatur nur in elektronischer Form vorliegt, weil sie nicht auf einem qualifizierten Zertifikat oder nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder weil sie nicht unter Verwendung von technischen Komponenten und Verfahren im Sinne des § 18 erstellt wurde.

Besondere Rechtswirkungen

§ 4. (1) Eine sichere elektronische Signatur erfüllt das rechtliche Erfordernis einer eigenhändigen Unterschrift, insbesondere der Schriftlichkeit im Sinne des § 886 ABGB, sofern durch Gesetz oder Parteienvereinbarung nicht anderes bestimmt ist.

(2) Eine sichere elektronische Signatur entfaltet nicht die Rechtswirkungen der Schriftlichkeit im Sinne des § 886 ABGB bei

1. Rechtsgeschäften des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind,
2. anderen Willenserklärungen oder Rechtsgeschäften, die zu ihrer Wirksamkeit an die Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts gebunden sind,
3. Willenserklärungen, Rechtsgeschäften oder Eingaben, die zu ihrer Eintragung in das Grundbuch, das Firmenbuch oder ein anderes öffentliches Register einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts bedürfen, und
4. einer Bürgschaftserklärung (§ 1346 Abs. 2 ABGB).

(3) Die Bestimmung des § 294 ZPO über die Vermutung der Echtheit des Inhalts einer unterschriebenen Privaturkunde ist auf elektronische Dokumente, die mit einer sicheren elektronischen Signatur versehen sind, anzuwenden.

(4) Die Rechtswirkungen der Abs. 1 und 3 treten nicht ein, wenn nachgewiesen wird, daß die Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen nicht eingehalten oder die zur Einhaltung dieser Sicherheitsanforderungen getroffenen Vorkehrungen kompromittiert wurden.

Qualifizierte Zertifikate

§ 5. (1) Ein qualifiziertes Zertifikat hat zumindest folgende Angaben zu enthalten:

1. den Hinweis darauf, daß es sich um ein qualifiziertes Zertifikat handelt,
2. den unverwechselbaren Namen des Zertifizierungsdiensteanbieters und den Staat seiner Niederlassung,

3. den Namen des Signators oder ein Pseudonym, das als solches bezeichnet sein muß,
4. gegebenenfalls auf Verlangen des Zertifikatswerbers Angaben über eine Vertretungsmacht oder eine andere rechtlich erhebliche Eigenschaft des Signators,
5. die dem Signator zugeordneten Signaturprüfdaten,
6. Beginn und Ende der Gültigkeit des Zertifikats,
7. die eindeutige Kennung des Zertifikats,
8. gegebenenfalls eine Einschränkung des Anwendungsbereichs des Zertifikats und
9. gegebenenfalls eine Begrenzung des Transaktionswerts, auf den das Zertifikat ausgestellt ist.

(2) Auf Verlangen des Zertifikatswerbers können weitere rechtlich erhebliche Angaben in das qualifizierte Zertifikat aufgenommen werden.

(3) Ein qualifiziertes Zertifikat muß mit der sicheren elektronischen Signatur des Zertifizierungsdiensteanbieters versehen sein.

3. Abschnitt

Zertifizierungsdiensteanbieter

Tätigkeit der Zertifizierungsdiensteanbieter

§ 6. (1) Die Aufnahme und die Ausübung der Tätigkeit eines Zertifizierungsdiensteanbieters bedürfen keiner gesonderten Genehmigung.

(2) Ein Zertifizierungsdiensteanbieter hat die Aufnahme seiner Tätigkeit unverzüglich der Aufsichtsstelle (§ 13) anzuzeigen. Er hat der Aufsichtsstelle spätestens mit Aufnahme der Tätigkeit oder bei Änderung seiner Dienste ein Sicherheitskonzept sowie ein Zertifizierungskonzept für jeden von ihm angebotenen Signatur- und Zertifizierungsdienst samt den verwendeten technischen Komponenten und Verfahren vorzulegen.

(3) Ein Zertifizierungsdiensteanbieter, der sichere elektronische Signaturverfahren bereitstellt, hat in seinem Sicherheitskonzept die Einhaltung der Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen darzulegen.

(4) Ein Zertifizierungsdiensteanbieter hat die im Sicherheits- und im Zertifizierungskonzept dargelegten Angaben sowohl bei der Aufnahme als auch während der Ausübung seiner Tätigkeit zu erfüllen.

(5) Ein Zertifizierungsdiensteanbieter hat alle Umstände, die eine ordnungsgemäße und dem Sicherheits- sowie dem Zertifizierungskonzept entsprechende Tätigkeit nicht mehr ermöglichen, unverzüglich der Aufsichtsstelle anzuzeigen.

(6) Stellt ein Zertifizierungsdiensteanbieter Zertifikate aus, so hat er im Sicherheitskonzept darzulegen, ob und gegebenenfalls in welcher Form Verzeichnis- und Widerrufsdienste geführt werden.

(7) Ein Zertifikat für Zertifizierungsdiensteanbieter darf von diesen nur für die Erbringung von Zertifizierungsdiensten verwendet werden.

Zertifizierungsdiensteanbieter für qualifizierte Zertifikate

§ 7. (1) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, hat

1. die erforderliche Zuverlässigkeit für die von ihm bereitgestellten Signatur- oder Zertifizierungsdienste aufzuweisen,
2. den Betrieb eines schnellen und sicheren Verzeichnisdienstes sowie eines unverzüglichen und sicheren Widerrufsdienstes sicherzustellen,
3. in qualifizierten Zertifikaten sowie für Verzeichnis- und Widerrufsdienste qualitätsgesicherte Zeitangaben (Zeitstempel) zu verwenden und jedenfalls sicherzustellen, daß der Zeitpunkt der Ausstellung und des Widerrufs eines qualifizierten Zertifikats bestimmt werden kann,
4. anhand eines amtlichen Lichtbildausweises die Identität und gegebenenfalls besondere rechtlich erhebliche Eigenschaften der Person, für die ein qualifiziertes Zertifikat ausgestellt wird, zuverlässig zu überprüfen,
5. zuverlässiges Personal mit den für die bereitgestellten Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Managementfähigkeiten sowie mit Kenntnissen der Technologie elektronischer Signaturen und angemessener Sicherheitsverfahren, zu beschäftigen und geeignete Verwaltungs- und Managementverfahren, die anerkannten Normen entsprechen, einzuhalten,
6. über ausreichende Finanzmittel zu verfügen, um den Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen zu entsprechen, sowie Vorsorge für die

Befriedigung von Schadenersatzansprüchen, etwa durch Eingehen einer Haftpflichtversicherung, zu treffen,

7. alle maßgeblichen Umstände über ein qualifiziertes Zertifikat während eines für den Verwendungszweck angemessenen Zeitraums – gegebenenfalls auch elektronisch – aufzuzeichnen, sodaß insbesondere in gerichtlichen Verfahren die Zertifizierung nachgewiesen werden kann, sowie
8. Vorkehrungen dafür zu treffen, daß die Signaturerstellungsdaten der Signatoren weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden können.

(2) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, hat für die Signatur- und Zertifizierungsdienste sowie für die Erstellung und Speicherung von Zertifikaten vertrauenswürdige Systeme, Produkte und Verfahren, die vor Veränderungen geschützt sind und für die technische und kryptographische Sicherheit sorgen, zu verwenden. Er hat insbesondere geeignete Vorkehrungen dafür zu treffen, daß Signaturerstellungsdaten geheimgehalten werden, daß Daten für qualifizierte Zertifikate nicht unerkannt gefälscht oder verfälscht werden können und daß diese Zertifikate nur mit Zustimmung des Signators öffentlich abrufbar sind. Für die Bereitstellung von Signaturerstellungsdaten sowie für die Erstellung und Speicherung von qualifizierten Zertifikaten sind technische Komponenten und Verfahren, die den Anforderungen des § 18 entsprechen, zu verwenden.

(3) Signaturerstellungsdaten der Zertifizierungsdiensteanbieter sind vor unbefugtem Zugriff zu sichern.

(4) Für sichere elektronische Signaturen kann das Vorliegen der Voraussetzungen der Abs. 1 bis 3 im Rahmen der freiwilligen Akkreditierung (§ 17) bescheinigt werden.

(5) Stellt der Zertifizierungsdiensteanbieter ein sicheres elektronisches Signaturverfahren bereit, so muß der Umstand, daß es sich um eine sichere elektronische Signatur handelt, im Zertifikat oder in einem elektronisch jederzeit allgemein zugänglichen Verzeichnis aufscheinen.

(6) Auf Ersuchen von Gerichten oder anderen Behörden hat ein Zertifizierungsdiensteanbieter die Prüfung der auf seinen qualifizierten Zertifikaten beruhenden sicheren Signaturen vorzunehmen.

Ausstellung qualifizierter Zertifikate

§ 8. (1) Ein Zertifizierungsdiensteanbieter hat die Identität von Personen, denen ein qualifiziertes Zertifikat ausgestellt werden soll, anhand eines amtlichen Lichtbildausweises zuverlässig festzustellen. Er hat die Zuordnung bestimmter Signaturprüfdaten zu dieser Person durch ein qualifiziertes Zertifikat zu bestätigen.

(2) Das Verlangen auf Ausstellung eines qualifizierten Zertifikats kann auch bei einer im Auftrag des Zertifizierungsdiensteanbieters tätigen anderen Stelle eingebracht werden, die die Überprüfung der Identität des Zertifikatswerbers vorzunehmen hat.

(3) Ein Zertifizierungsdiensteanbieter hat nach Maßgabe des Zertifizierungskonzepts auf Verlangen des Zertifikatswerbers Angaben über seine Vertretungsmacht oder eine andere rechtlich erhebliche Eigenschaft in das qualifizierte Zertifikat aufzunehmen, sofern ihm oder einer anderen Stelle (Abs. 2) diese Umstände zuverlässig nachgewiesen werden.

(4) Ein Zertifizierungsdiensteanbieter kann nach Maßgabe des Zertifizierungskonzepts auf Verlangen des Zertifikatswerbers im Zertifikat anstatt des Namens des Signators ein Pseudonym angeben. Das Pseudonym darf weder anstößig noch offensichtlich zur Verwechslung mit Namen oder Kennzeichen geeignet sein.

Widerruf von Zertifikaten

§ 9. (1) Ein Zertifizierungsdiensteanbieter hat ein Zertifikat unverzüglich zu widerrufen, wenn

1. der Signator oder ein im Zertifikat genannter Machtgeber dies verlangt,
2. der Zertifizierungsdiensteanbieter Kenntnis vom Ableben des Signators oder sonst von der Änderung im Zertifikat bescheinigter Umstände erlangt,
3. das Zertifikat auf Grund unrichtiger Angaben erwirkt wurde,
4. der Zertifizierungsdiensteanbieter seine Tätigkeit einstellt und seine Verzeichnis- und Widerrufsdienste nicht von einem anderen Zertifizierungsdiensteanbieter übernommen werden,
5. die Aufsichtsstelle gemäß § 14 den Widerruf des Zertifikats anordnet oder
6. die Gefahr einer mißbräuchlichen Verwendung des Zertifikats besteht.

(2) Können die in Abs. 1 genannten Umstände nicht sofort zweifelsfrei festgestellt werden, so hat der Zertifizierungsdiensteanbieter das Zertifikat jedenfalls unverzüglich zu sperren.

(3) Die Sperre und der Widerruf müssen den Zeitpunkt, ab dem sie wirksam werden, enthalten. Wird ein Widerrufsdienst geführt, so werden die Sperre und der Widerruf mit der Eintragung in das entsprechende Verzeichnis wirksam. Eine rückwirkende Sperre oder ein rückwirkender Widerruf ist unzulässig. Der Signator bzw. sein Rechtsnachfolger ist von der Sperre oder dem Widerruf unverzüglich zu verständigen.

(4) Ein Zertifizierungsdiensteanbieter hat ein elektronisch jederzeit allgemein zugängliches Verzeichnis der gesperrten und der widerrufenen qualifizierten Zertifikate zu führen.

(5) Die Aufsichtsstelle hat das Zertifikat eines Zertifizierungsdiensteanbieters unverzüglich zu widerrufen, wenn

1. dem Zertifizierungsdiensteanbieter die Ausübung seiner Tätigkeit untersagt wird und seine Verzeichnis- und Widerrufsdienste nicht von einem anderen Zertifizierungsdiensteanbieter übernommen werden oder
2. der Zertifizierungsdiensteanbieter seine Tätigkeit einstellt und seine Verzeichnis- und Widerrufsdienste nicht von einem anderen Zertifizierungsdiensteanbieter übernommen werden.

Zeitstempeldienste

§ 10. Stellt ein Zertifizierungsdiensteanbieter Zeitstempeldienste bereit, so hat er im Sicherheits- und im Zertifizierungskonzept die näheren Angaben darzulegen. Für sichere Zeitstempeldienste sind technische Komponenten und Verfahren zu verwenden, die die Richtigkeit und Unverfälschtheit der Zeitangabe sicherstellen und den Anforderungen des § 18 entsprechen.

Dokumentation

§ 11. (1) Ein Zertifizierungsdiensteanbieter hat die Sicherheitsmaßnahmen, die er zur Einhaltung dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen getroffen hat, sowie das Ausstellen und gegebenenfalls die Sperre und den Widerruf von Zertifikaten zu dokumentieren. Dabei müssen die Daten und ihre Unverfälschtheit sowie der Zeitpunkt ihrer Aufnahme in das Protokollierungssystem jederzeit nachprüfbar sein.

(2) Auf Ersuchen von Gerichten oder anderen Behörden hat ein Zertifizierungsdiensteanbieter die Dokumentation nach Abs. 1 auszufolgen.

Einstellung der Tätigkeit

§ 12. Ein Zertifizierungsdiensteanbieter hat die Einstellung seiner Tätigkeit unverzüglich der Aufsichtsstelle anzuzeigen. Weiters hat er die im Zeitpunkt der Einstellung seiner Tätigkeit gültigen Zertifikate zu widerrufen oder dafür Sorge zu tragen, daß zumindest seine Verzeichnis- und Widerrufsdienste von einem anderen Zertifizierungsdiensteanbieter übernommen werden. Die Signatoren sind von der Einstellung der Tätigkeit sowie vom Widerruf oder der Übernahme unverzüglich zu verständigen. Auch im Fall des Widerrufs der Zertifikate hat der Zertifizierungsdiensteanbieter sicherzustellen, daß die Widerrufsdienste weitergeführt werden; kommt er dieser Verpflichtung nicht nach, so hat die Aufsichtsstelle für die Weiterführung der Widerrufsdienste auf Kosten des Zertifizierungsdiensteanbieters Sorge zu tragen.

4. Abschnitt

Aufsicht

Aufsichtsstelle

§ 13. (1) Aufsichtsstelle ist die Telekom-Control-Kommission (§ 110 TKG). Ihr obliegt die laufende Aufsicht über die Einhaltung der Bestimmungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen.

(2) Die Aufsichtsstelle hat insbesondere

1. die Umsetzung der Angaben im Sicherheits- und im Zertifizierungskonzept zu überprüfen,
2. im Fall der Bereitstellung sicherer elektronischer Signaturen die Verwendung geeigneter technischer Komponenten und Verfahren (§ 18) zu überwachen,
3. Zertifizierungsdiensteanbieter nach § 17 zu akkreditieren und
4. die organisatorische Aufsicht über Bestätigungsstellen (§ 19) durchzuführen.

(3) Die Aufsichtsstelle hat dafür Sorge zu tragen, daß ein elektronisch jederzeit allgemein zugängliches Verzeichnis der gültigen, der gesperrten und der widerrufenen Zertifikate für Zertifizierungsdiensteanbieter geführt wird. Weiters hat die Aufsichtsstelle dafür Sorge zu tragen, daß ein elektronisch jederzeit allgemein zugängliches Verzeichnis der im Inland niedergelassenen Zertifizierungsdiensteanbieter, der von ihr akkreditierten Zertifizierungsdiensteanbieter und der Drittstaatenzertifizierungsdiensteanbieter, für deren Zertifikate ein im Inland niedergelassener Zertifizierungsdiensteanbieter nach § 24 Abs. 2 Z 2 einsteht, geführt wird. Auf Antrag sind auch andere im Ausland niedergelassene Zertifizierungsdiensteanbieter in dieses Verzeichnis aufzunehmen. In das Verzeichnis der Zertifikate für Zertifizierungsdiensteanbieter sind deren qualifizierte Zertifikate für die Erbringung von Zertifizierungsdiensten einzutragen. Solche Zertifikate können auch von der Aufsichtsstelle ausgestellt werden. Die Aufsichtsstelle hat die bei ihr geführten Verzeichnisse mit ihrer sicheren elektronischen Signatur zu versehen. Das Zertifikat der Aufsichtsstelle ist im Amtsblatt zur Wiener Zeitung zu veröffentlichen.

(4) Die Aufsichtsstelle hat den Zertifizierungsdiensteanbietern für ihre Tätigkeit und für die Heranziehung der Telekom-Control GmbH eine mit Verordnung festgelegte kostendeckende Gebühr vorzuschreiben. Die Einnahmen aus dieser Gebühr fließen der Aufsichtsstelle zu und sind nach Heranziehung der Telekom-Control GmbH oder der Bestätigungsstelle nach deren Aufwand weiterzuleiten.

(5) Die Aufsichtsstelle kann sich zur Beratung geeigneter Personen oder Einrichtungen wie etwa einer Bestätigungsstelle (§ 19) bedienen.

(6) Die Mitglieder der Aufsichtsstelle sind gemäß Art. 20 Abs. 2 B-VG bei Ausübung ihres Amtes an keine Weisungen gebunden. Sofern gesetzlich nicht anderes bestimmt ist, hat die Aufsichtsstelle das AVG 1991 anzuwenden. Sie entscheidet in oberster Instanz. Die Anrufung des Verwaltungsgerichtshofs ist zulässig.

(7) Die Tätigkeit der Aufsichtsstelle nach diesem Bundesgesetz ist von ihrer Tätigkeit nach anderen Bundesgesetzen organisatorisch und finanziell zu trennen.

Aufsichtsmaßnahmen

§ 14. (1) Die Aufsichtsstelle hat den Zertifizierungsdiensteanbietern Maßnahmen zur Sicherstellung der Erfüllung der Pflichten aus diesem Bundesgesetz und der auf seiner Grundlage ergangenen Verordnungen vorzuschreiben. Sie kann einem Zertifizierungsdiensteanbieter insbesondere die Verwendung ungeeigneter technischer Komponenten und Verfahren oder die Ausübung der Tätigkeit ganz oder teilweise untersagen. Weiters kann die Aufsichtsstelle Zertifikate für Zertifizierungsdiensteanbieter oder von Signatoren widerrufen oder den Widerruf der Zertifikate von Signatoren durch den Zertifizierungsdiensteanbieter anordnen.

(2) Sofern nicht nach Abs. 6 gelindere Mittel in Betracht kommen, ist einem Zertifizierungsdiensteanbieter die Ausübung der Tätigkeit ganz oder teilweise zu untersagen, wenn

1. er oder sein Personal nicht die für die bereitgestellten Signatur- oder Zertifizierungsdienste erforderliche Zuverlässigkeit aufweist,
2. er oder sein Personal nicht über die erforderlichen Fachkenntnisse verfügt,
3. ihm keine ausreichenden Finanzmittel zur Verfügung stehen,
4. er bei der Ausübung seiner Tätigkeit die im Sicherheits- oder im Zertifizierungskonzept dargelegten Angaben nicht erfüllt,
5. er die vorgeschriebenen Verzeichnis- oder Widerrufsdienste nicht oder nicht ordnungsgemäß führt oder der Sperr- oder Widerrufspflicht (§ 9) nicht oder nur unzureichend nachkommt oder
6. er der Anzeigepflicht nach § 6 Abs. 2 nicht nachkommt.

(3) Sofern nicht nach Abs. 6 gelindere Mittel in Betracht kommen, ist einem Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, die Ausübung seiner Tätigkeit zudem ganz oder teilweise zu untersagen, wenn die übrigen für die Ausübung einer solchen Tätigkeit erforderlichen Voraussetzungen nach diesem Bundesgesetz oder den auf seiner Grundlage ergangenen Verordnungen nicht erfüllt werden.

(4) Sofern nicht nach Abs. 6 gelindere Mittel in Betracht kommen, ist einem Zertifizierungsdiensteanbieter, der sichere elektronische Signaturverfahren bereitstellt, die Ausübung seiner Tätigkeit auch dann ganz oder teilweise zu untersagen, wenn die verwendeten technischen Komponenten und Verfahren nicht die Sicherheitsanforderungen nach § 18 erfüllen.

(5) Wenn die Aufsichtsstelle einem Zertifizierungsdiensteanbieter die Ausübung seiner Tätigkeit untersagt, hat sie für den Widerruf der Zertifikate des Zertifizierungsdiensteanbieters und der Signatoren Sorge zu tragen oder die Übernahme der erbrachten Signatur- und Zertifizierungsdienste oder zumindest seiner Verzeichnis- und Widerrufsdienste durch einen anderen Zertifizierungsdiensteanbieter zu veranlassen, sofern die beteiligten Zertifizierungsdiensteanbieter der Übernahme zustimmen. Die Signatoren sind von der Untersagung sowie vom Widerruf oder der Übernahme unverzüglich zu verständigen. Auch im Fall des Widerrufs der Zertifikate hat der Zertifizierungsdiensteanbieter sicherzustellen, daß die Widerrufsdienste weitergeführt werden; kommt er dieser Verpflichtung nicht nach, so hat die Aufsichtsstelle für die Weiterführung der Widerrufsdienste auf Kosten des Zertifizierungsdiensteanbieters Sorge zu tragen.

(6) Die Aufsichtsstelle hat von einer Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters abzusehen, soweit die Anordnung gelinderer Mittel ausreicht, um die Einhaltung der Bestimmungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen sicherzustellen. Sie kann insbesondere Auflagen erteilen oder unter Setzung einer angemessenen Frist zur Behebung von ihr aufgezeigter Mängel Maßnahmen androhen.

Heranziehung der Telekom-Control GmbH

§ 15. (1) Die Aufsichtsstelle kann sich bei der Durchführung der Aufsicht der Telekom-Control GmbH (§ 108 TKG) bedienen.

(2) Die Telekom-Control GmbH hat insbesondere

1. die Aufsichtsstelle bei der laufenden Aufsicht der Zertifizierungsdiensteanbieter zu unterstützen und die technischen Produkte, Verfahren und sonstigen Mittel, die im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste eingesetzt werden, sowie die Qualifikation des Personals zu überprüfen,
2. die Zertifizierungsdiensteanbieter nach der Anzeige der Aufnahme ihrer Tätigkeit zu registrieren,
3. Verzeichnisse der Zertifikate für Zertifizierungsdiensteanbieter und der Zertifizierungsdiensteanbieter (§ 13 Abs. 3) sowie ein Verzeichnis der akkreditierten Zertifizierungsdiensteanbieter (§ 17 Abs. 1) zu führen,
4. für den Fall der Einstellung oder Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters einen Widerrufsdienst zu führen, sofern keine Übernahme im Sinne der §§ 12 oder 14 Abs. 5 erfolgt,
5. auf Anordnung der Aufsichtsstelle die Erfüllung der Voraussetzungen einer freiwilligen Akkreditierung (§ 17) zu erheben,
6. bei der Feststellung der Gleichwertigkeit von Prüfberichten aus Drittstaaten im Sinne des § 24 Abs. 3 mitzuwirken und
7. im Fall des begründeten Verdachts, daß die Sicherheitsanforderungen dieses Bundesgesetzes oder der auf seiner Grundlage ergangenen Verordnungen nicht eingehalten werden, oder auf Verlangen eines Zertifizierungsdiensteanbieters unmittelbar die vorläufige Untersagung der Tätigkeit des Zertifizierungsdiensteanbieters oder vorläufig Maßnahmen im Sinne des § 14 Abs. 1 anzuordnen.

(3) Die Telekom-Control GmbH hat alle organisatorischen Vorkehrungen dafür zu treffen, daß sie ihre Aufgaben erfüllen und die Aufsichtsstelle bei Erfüllung ihrer Aufgaben unterstützen kann. Sie kann sich zur Beratung geeigneter Personen oder Einrichtungen wie etwa einer Bestätigungsstelle (§ 19) bedienen. Die Wahrnehmung ihrer Aufgaben in technischen Belangen hat in Abstimmung mit einer Bestätigungsstelle (§ 19) zu erfolgen. Im Rahmen ihrer Tätigkeit für die Aufsichtsstelle ist das Personal der Telekom-Control GmbH an die Weisungen des Vorsitzenden oder des in der Geschäftsordnung bezeichneten Mitgliedes gebunden.

(4) Unbeschadet der Zuständigkeit der ordentlichen Gerichte können Kunden oder Interessenvertretungen Streit- oder Beschwerdefälle, insbesondere über die Qualität eines Zertifizierungsdienstes, die mit dem Zertifizierungsdiensteanbieter nicht befriedigend gelöst worden sind, der Telekom-Control GmbH vorlegen. Die Telekom-Control GmbH hat sich zu bemühen, innerhalb angemessener Frist eine einvernehmliche Lösung herbeizuführen. Die Zertifizierungsdiensteanbieter sind verpflichtet, an einem solchen Verfahren mitzuwirken und alle zur Beurteilung der Sachlage erforderlichen Auskünfte zu erteilen. Die Telekom-Control GmbH hat Richtlinien für die Durchführung dieses Verfahrens festzulegen, die in geeigneter Form zu veröffentlichen sind.

(5) § 13 Abs. 7 über die organisatorische und finanzielle Trennung ist auf die Tätigkeit der Telekom-Control GmbH anzuwenden.

Durchführung der Aufsicht

§ 16. (1) Die Zertifizierungsdiensteanbieter haben den im Auftrag der Aufsichtsstelle handelnden Personen das Betreten der Geschäfts- und Betriebsräume während der Geschäftszeiten zu gestatten, die in Betracht kommenden Bücher und sonstigen Aufzeichnungen oder Unterlagen einschließlich der Dokumentation nach § 11 vorzulegen oder zur Einsicht bereitzuhalten, Auskünfte zu erteilen und jede sonst erforderliche Unterstützung zu gewähren. Bestehende gesetzliche Verschwiegenheits- und Aussageverweigerungsrechte bleiben unberührt.

(2) Die Organe des öffentlichen Sicherheitsdienstes haben der Aufsichtsstelle und den in ihrem Auftrag handelnden Personen über deren Ersuchen zur Durchführung der Aufsicht im Rahmen ihres gesetzmäßigen Wirkungsbereichs Hilfe zu leisten.

(3) Die Durchführung der Aufsicht nach den Abs. 1 und 2 ist unter möglichster Schonung der Betroffenen und ohne unnötiges Aufsehen so durchzuführen, daß dadurch die Sicherheit der Signatur- und Zertifizierungsdienste nicht verletzt wird.

Freiwillige Akkreditierung

§ 17. (1) Zertifizierungsdiensteanbieter, die sichere elektronische Signaturverfahren bereitstellen und der Aufsichtsstelle vor der Aufnahme ihrer Tätigkeit als akkreditierte Zertifizierungsdiensteanbieter die Einhaltung der Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen nachweisen, sind auf Antrag von der Aufsichtsstelle zu akkreditieren. Akkreditierte Zertifizierungsdiensteanbieter dürfen sich mit Zustimmung der Aufsichtsstelle im Geschäftsverkehr als solche bezeichnen. Im Zusammenhang mit Signatur- und Zertifizierungsdiensten sowie mit Signaturprodukten darf diese Bezeichnung nur verwendet werden, wenn die Sicherheitsanforderungen nach § 18 erfüllt werden. Die Aufsichtsstelle hat dafür Sorge zu tragen, daß die akkreditierten Zertifizierungsdiensteanbieter in ein elektronisch jederzeit allgemein zugängliches Verzeichnis aufgenommen werden.

(2) Die freiwillige Akkreditierung eines Zertifizierungsdiensteanbieters ist in das qualifizierte Zertifikat aufzunehmen oder sonst in geeigneter Weise zugänglich zu machen.

(3) Die Aufsichtsstelle hat für die laufende Aufsicht über die von ihr akkreditierten Zertifizierungsdiensteanbieter Sorge zu tragen.

5. Abschnitt

Technische Sicherheitserfordernisse

Technische Komponenten und Verfahren für sichere Signaturen

§ 18. (1) Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer Signaturen sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar machen und die die unbefugte Verwendung von Signaturerstellungsdaten verläßlich verhindern.

(2) Die bei der Erstellung einer sicheren Signatur verwendeten technischen Komponenten und Verfahren müssen zudem sicherstellen, daß die zu signierenden Daten nicht verändert werden; sie müssen es weiters ermöglichen, daß dem Signator die zu signierenden Daten vor Auslösung des Signaturvorgangs dargestellt werden. Die Signaturerstellungsdaten dürfen mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen, sie dürfen weiters mit hinreichender Sicherheit nicht ableitbar sein; ihre Geheimhaltung muß sichergestellt sein.

(3) Bei der Erstellung und Speicherung von qualifizierten Zertifikaten sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung und Verfälschung von Zertifikaten verhindern.

(4) Für die Überprüfung von sicher signierten Daten sind solche technische Komponenten und Verfahren anzubieten, die sicherstellen, daß

1. die signierten Daten nicht verändert worden sind,
2. die Signatur zuverlässig überprüft und das Ergebnis dieser Überprüfung korrekt angezeigt wird,
3. der Überprüfer feststellen kann, auf welche Daten sich die elektronische Signatur bezieht,
4. der Überprüfer feststellen kann, welchem Signator die elektronische Signatur zugeordnet ist, wobei die Verwendung eines Pseudonyms angezeigt werden muß, und

5. sicherheitsrelevante Veränderungen der signierten Daten erkannt werden können.

(5) Die technischen Komponenten und Verfahren für die Erzeugung sicherer Signaturen müssen nach dem Stand der Technik hinreichend und laufend geprüft sein. Die Erfüllung der Sicherheitsanforderungen muß von einer Bestätigungsstelle (§ 19) bescheinigt sein.

Bestätigungsstelle

§ 19. (1) Die nach diesem Bundesgesetz und den auf seiner Grundlage ergangenen Verordnungen einer Bestätigungsstelle zugewiesenen Aufgaben können nur von einer dazu geeigneten Einrichtung wahrgenommen werden.

(2) Eine Einrichtung ist zur Wahrnehmung der einer Bestätigungsstelle zugewiesenen Aufgaben geeignet, wenn sie

1. die erforderliche Zuverlässigkeit aufweist,
2. zuverlässiges Personal mit den für diese Aufgaben erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Kenntnissen über elektronische Signaturen, angemessene Sicherheitsverfahren, Kryptographie, Kommunikations- und Chipkartentechnologien sowie die technische Begutachtung solcher Komponenten, beschäftigt,
3. über ausreichende technische Einrichtungen und Mittel sowie eine ausreichende wirtschaftliche Leistungsfähigkeit verfügt und
4. die erforderliche Unabhängigkeit, Unparteilichkeit und Unbefangenheit sicherstellt.

(3) Der Bundeskanzler hat im Einvernehmen mit dem Bundesminister für Justiz mit Verordnung festzustellen, daß eine Einrichtung als Bestätigungsstelle geeignet ist. Eine solche Verordnung kann nur auf Antrag der betreffenden Einrichtung erlassen werden. Die Eignung kann nur festgestellt werden, wenn die Einrichtung nach ihren Statuten oder Satzungen oder nach ihrem Gesellschaftsvertrag, nach ihrer Organisation und nach ihrem Sicherheits- und Finanzierungskonzept die in Abs. 2 genannten Anforderungen erfüllt.

(4) Eine Bestätigungsstelle kann zur Erfüllung der ihr nach diesem Bundesgesetz oder der auf seiner Grundlage ergangenen Verordnungen zugewiesenen Aufgaben von anderen Einrichtungen oder Stellen Prüfberichte zu technischen Komponenten und Verfahren einholen.

6. Abschnitt

Rechte und Pflichten der Anwender

Allgemeine Informationspflichten der Zertifizierungsdiensteanbieter

§ 20. (1) Ein Zertifizierungsdiensteanbieter hat den Zertifikatswerber vor Vertragschließung schriftlich oder unter Verwendung eines dauerhaften Datenträgers klar und allgemein verständlich über den Inhalt des Sicherheits- und des Zertifizierungskonzepts zu unterrichten. Bei der Ausstellung eines qualifizierten Zertifikats hat der Zertifizierungsdiensteanbieter zudem die Bedingungen der Verwendung des Zertifikats, wie etwa Einschränkungen seines Anwendungsbereichs oder des Transaktionswerts, bekanntzugeben; weiters ist auf eine freiwillige Akkreditierung (§ 17) sowie auf besondere Streitbeilegungsverfahren hinzuweisen.

(2) Auf Verlangen sind die in Abs. 1 genannten Angaben auch Dritten, die ein rechtliches Interesse daran glaubhaft machen, zugänglich zu machen.

(3) Ein Zertifizierungsdiensteanbieter hat weiters den Zertifikatswerber darüber zu unterrichten, welche technischen Komponenten und Verfahren für das verwendete Signaturverfahren geeignet sind, gegebenenfalls auch darüber, welche technischen Komponenten und Verfahren sowie sonstigen Maßnahmen die Anforderungen für die Erzeugung und Prüfung sicherer Signaturen erfüllen. Ferner ist der Zertifikatswerber über die möglichen Rechtswirkungen des von ihm verwendeten Signaturverfahrens, über die Pflichten eines Signators sowie über die besondere Haftung des Zertifizierungsdiensteanbieters zu belehren. Der Zertifikatswerber ist auch darüber zu unterrichten, daß und wie gegebenenfalls eine neue elektronische Signatur anzubringen ist, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

Pflichten des Signators

§ 21. Der Signator hat die Signaturerstellungsdaten sorgfältig zu verwahren, soweit zumutbar Zugriffe auf Signaturerstellungsdaten zu verhindern und deren Weitergabe zu unterlassen. Er hat den Widerruf des Zertifikats zu verlangen, wenn die Signaturerstellungsdaten abhanden kommen, wenn

Anhaltspunkte für eine Kompromittierung der Signaturerstellungsdaten bestehen oder wenn sich die im Zertifikat bescheinigten Umstände geändert haben.

Datenschutz

§ 22. (1) Ein Zertifizierungsdiensteanbieter darf nur jene personenbezogenen Daten verwenden, die er zur Durchführung der erbrachten Dienste benötigt. Diese Daten dürfen nur unmittelbar beim Betroffenen selbst oder mit seiner ausdrücklichen Zustimmung bei einem Dritten erhoben werden.

(2) Bei Verwendung eines Pseudonyms hat der Zertifizierungsdiensteanbieter die Daten über die Identität des Signators zu übermitteln, sofern an der Feststellung der Identität ein überwiegendes berechtigtes Interesse im Sinne des § 8 Abs. 1 Z 4 und Abs. 3 DSG glaubhaft gemacht wird. Die Übermittlung ist zu dokumentieren.

(3) Die Auskunfts- und Mitwirkungspflichten des Zertifizierungsdiensteanbieters gegenüber Gerichten und anderen Behörden bleiben unberührt.

Haftung der Zertifizierungsstellen

§ 23. (1) Ein Zertifizierungsdiensteanbieter, der ein Zertifikat als qualifiziertes Zertifikat ausstellt oder für ein solches Zertifikat nach § 24 Abs. 2 Z 2 einsteht, haftet gegenüber jeder Person, die auf das Zertifikat vertraut, dafür, daß

1. alle Angaben im qualifizierten Zertifikat im Zeitpunkt seiner Ausstellung richtig sind,
2. der im qualifizierten Zertifikat angegebene Signator im Zeitpunkt der Ausstellung des Zertifikats im Besitz jener Signaturerstellungsdaten ist, die den im Zertifikat angegebenen Signaturprüfdaten entsprechen,
3. die Signaturerstellungsdaten und die ihnen zugeordneten Signaturprüfdaten einander bei Verwendung der von ihm bereitgestellten oder als geeignet bezeichneten Produkte und Verfahren in komplementärer Weise entsprechen,
4. das Zertifikat bei Vorliegen der Voraussetzungen unverzüglich widerrufen wird und die Widerrufsdienste verfügbar sind sowie
5. die Anforderungen des § 7 erfüllt und für die Erzeugung und Speicherung von Signaturerstellungsdaten technische Komponenten und Verfahren nach § 18 verwendet werden.

(2) Ein Zertifizierungsdiensteanbieter, der sichere elektronische Signaturverfahren bereitstellt, haftet zudem dafür, daß für die von ihm bereitgestellten oder als geeignet bezeichneten Produkte, Verfahren und sonstigen Mittel für die Erstellung elektronischer Signaturen sowie für die Darstellung zu signierender Daten nur technische Komponenten und Verfahren nach § 18 verwendet werden.

(3) Der Zertifizierungsdiensteanbieter haftet nicht, wenn er nachweist, daß ihn und seine Leute an der Verletzung der Verpflichtungen nach den Abs. 1 und 2 kein Verschulden trifft. Kann der Geschädigte als wahrscheinlich dartun, daß die Verpflichtungen nach den Abs. 1 und 2 verletzt oder die zur Einhaltung der Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen getroffenen Vorkehrungen kompromittiert wurden, so wird vermutet, daß der Schaden dadurch verursacht wurde. Diese Vermutung ist widerlegt, wenn der Zertifizierungsdiensteanbieter als wahrscheinlich dartut, daß der Schaden nicht durch eine Verletzung bzw. Kompromittierung der im zweiten Satz genannten Verpflichtungen und Vorkehrungen verursacht wurde.

(4) Enthält ein qualifiziertes Zertifikat eine Einschränkung des Anwendungsbereichs, so haftet der Zertifizierungsdiensteanbieter nicht für Schäden, die sich aus einer anderen Verwendung des Zertifikats ergeben. Enthält ein qualifiziertes Zertifikat einen bestimmten Transaktionswert, bis zu dem das Zertifikat verwendet werden darf, so haftet der Zertifizierungsdiensteanbieter nicht für Schäden, die sich aus der Überschreitung dieses Transaktionswerts ergeben.

(5) Die Haftung eines Zertifizierungsdiensteanbieters nach Abs. 1 bis 3 kann im vorhinein weder ausgeschlossen noch beschränkt werden.

(6) Bestimmungen des Allgemeinen Bürgerlichen Gesetzbuchs und anderer Rechtsvorschriften, nach denen Schäden in anderem Umfang oder von anderen Personen als nach diesem Bundesgesetz zu ersetzen sind, bleiben unberührt.

7. Abschnitt

Anerkennung ausländischer Zertifikate

Anerkennung

§ 24. (1) Zertifikate, die von einem in der Europäischen Gemeinschaft niedergelassenen Zertifizierungsdiensteanbieter ausgestellt wurden und deren Gültigkeit vom Inland aus überprüft werden kann, sind inländischen Zertifikaten gleichgestellt. Qualifizierte Zertifikate solcher Zertifizierungsdiensteanbieter entfalten dieselben Rechtswirkungen wie inländische qualifizierte Zertifikate.

(2) Zertifikate, die von einem in einem Drittstaat niedergelassenen Zertifizierungsdiensteanbieter ausgestellt wurden und deren Gültigkeit vom Inland aus überprüft werden kann, werden im Inland anerkannt. Qualifizierte Zertifikate werden inländischen qualifizierten Zertifikaten rechtlich gleichgestellt, wenn

1. der Zertifizierungsdiensteanbieter die Anforderungen nach § 7 erfüllt und unter einem freiwilligen Akkreditierungssystem eines Mitgliedstaates der Europäischen Union akkreditiert ist,
2. ein in der Europäischen Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen nach § 7 erfüllt, für das Zertifikat haftungsrechtlich einsteht oder
3. im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Europäischen Gemeinschaft einerseits und Drittstaaten oder internationalen Organisationen andererseits das Zertifikat als qualifiziertes Zertifikat oder der Zertifizierungsdiensteanbieter als Aussteller qualifizierter Zertifikate anerkannt ist.

(3) Ist in einem Mitgliedstaat der Europäischen Union oder in einem Drittstaat zum Nachweis der Sicherheitsanforderungen für sichere elektronische Signaturen eine staatlich anerkannte Stelle eingerichtet, so werden Bescheinigungen dieser Stelle über die Einhaltung der Sicherheitsanforderungen für die Erzeugung sicherer elektronischer Signaturen den Bescheinigungen einer Bestätigungsstelle (§ 19) gleichgehalten, soweit die Aufsichtsstelle feststellt, daß die den Beurteilungen dieser Stellen zugrunde liegenden technischen Anforderungen, Prüfungen und Prüfverfahren jenen der Bestätigungsstelle gleichwertig sind.

8. Abschnitt

Schlußbestimmungen

Signaturverordnung

§ 25. Der Bundeskanzler hat mit Verordnung im Einvernehmen mit dem Bundesminister für Justiz die nach dem jeweiligen Stand der Wissenschaft und Technik zur Durchführung dieses Bundesgesetzes erforderlichen Rechtsvorschriften zu erlassen über

1. die Festsetzung pauschaler kostendeckender Gebühren für die Leistungen der Aufsichtsstelle und der Telekom-Control GmbH sowie die Vorschreibung dieser Gebühren,
2. die Festsetzung der zur Erfüllung der Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen ausreichenden Finanzmittel sowie der für die Abdeckung des Haftungsrisikos der Zertifizierungsdiensteanbieter ausreichenden Finanzmittel, insbesondere die Festsetzung einer Mindestversicherungssumme für eine Haftpflichtversicherung,
3. die Zuverlässigkeit des Zertifizierungsdiensteanbieters und seines Personals (§§ 7 Abs. 1 und 14 Abs. 2),
4. die näheren Anforderungen an die technischen Komponenten und Verfahren sowie die technischen Produkte und sonstigen Mittel zur Anwendung der §§ 7 Abs. 2, 10 und 18, die Durchführung der Prüfung der technischen Komponenten und Verfahren nach § 18 sowie die Ausstellung der Bestätigung, daß diese Anforderungen erfüllt sind,
5. die Dauer der Weiterführung der Widerrufsdienste durch die Aufsichtsstelle (§ 12 und § 14 Abs. 5),
6. die Anwendungsbereiche, Anforderungen und Toleranzen von sicheren Zeitstempeldiensten,
7. die Gültigkeitsdauer und die Erneuerung der qualifizierten Zertifikate sowie den Zeitraum und das Verfahren, nach denen eine neue elektronische Signatur angebracht werden sollte (Nachsignieren),
8. die Form, Darstellung und Verfügbarkeit des Zertifizierungskonzepts (zB Klartext),
9. die Dauer der Aufbewahrung einer Dokumentation (§ 11) und
10. die Art und Form der Kennzeichnung akkreditierter Zertifizierungsdiensteanbieter.

Verwaltungsstrafbestimmungen

§ 26. (1) Eine Verwaltungsübertretung begeht und ist mit Geldstrafe bis zu 56 000 S zu bestrafen, wer fremde Signaturerstellungsdaten ohne Wissen und Willen des Signators mißbräuchlich verwendet.

(2) Ein Zertifizierungsdiensteanbieter begeht eine Verwaltungsübertretung und ist mit Geldstrafe bis zu 112 000 S zu bestrafen, wenn er

1. entgegen § 9 Abs. 1 seine Widerrufspflicht verletzt,
2. entgegen § 11 seine Dokumentationspflicht verletzt,
3. entgegen § 16 Abs. 1 nicht Einsicht in die dort genannten Bücher, sonstige Aufzeichnungen oder Unterlagen gewährt oder nicht die notwendigen Auskünfte erteilt oder
4. entgegen § 20 Abs. 1 und 3 den Zertifikatswerber nicht unterrichtet.

(3) Ein Zertifizierungsdiensteanbieter begeht eine Verwaltungsübertretung und ist mit Geldstrafe bis zu 224 000 S zu bestrafen, wenn er

1. entgegen § 6 Abs. 2 die Aufnahme seiner Tätigkeit nicht anzeigt oder das Sicherheitskonzept oder das Zertifizierungskonzept nicht vorlegt,
2. entgegen § 6 Abs. 5 nicht alle Umstände, die eine ordnungsgemäße und dem Sicherheits- sowie dem Zertifizierungskonzept entsprechende Tätigkeit nicht mehr ermöglichen, der Aufsichtsstelle anzeigt,
3. entgegen § 7 Abs. 1 Z 2 keinen geeigneten Widerrufsdienst oder keinen geeigneten Verzeichnisdienst führt,
4. entgegen § 7 Abs. 1 Z 8 keine geeigneten Vorkehrungen dafür trifft, daß die Signaturerstellungsdaten der Signatoren weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden können,
5. entgegen § 18 keine geeigneten technischen Komponenten und Verfahren für sichere elektronische Signaturen verwendet, bereitstellt oder bezeichnet oder
6. trotz Untersagung durch die Aufsichtsstelle (§ 14 Abs. 2 bis 4) die ihm untersagte Tätigkeit weiterhin ausübt.

(4) Eine Verwaltungsübertretung gemäß den Abs. 1 bis 3 liegt nicht vor, wenn die Tat den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist.

(5) Im Straferkenntnis können die Gegenstände, mit denen die strafbare Handlung begangen wurde, für verfallen erklärt werden.

Inkrafttreten und Verweisungen

§ 27. (1) Dieses Bundesgesetz tritt mit 1. Jänner 2000 in Kraft.

(2) Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

Vollzug

§ 28. Mit der Vollziehung dieses Bundesgesetzes sind betraut:

1. hinsichtlich der §§ 3, 4 und 23 der Bundesminister für Justiz,
2. hinsichtlich der §§ 13 bis 17 der Bundesminister für Wissenschaft und Verkehr,
3. hinsichtlich der §§ 22 und 26 der Bundeskanzler,
4. hinsichtlich der §§ 7 Abs. 1 Z 6 und 13 Abs. 4 der Bundeskanzler im Einvernehmen mit dem Bundesminister für Justiz und dem Bundesminister für Finanzen und
5. hinsichtlich der übrigen Bestimmungen der Bundeskanzler im Einvernehmen mit dem Bundesminister für Justiz.