Dissertation

zur Erlangung des akademischen Grades einer

Doktorin der Rechtswissenschaften

über das Thema:

Die europäische Signaturrichtlinie und ihre Umsetzung in Deutschland und Österreich

eingereicht bei:

Dr.phil.et Dr.iur. Ao.Univ.-Prof. Eilmannsberger für

Europarecht und Wirtschaftsrecht

Institut für Europarecht

der Paris-Lodron Universität Salzburg

von

Mag. Iur. Bettina Bauer

Jänner 2001, Wien

Inhaltsverzeichnis

1 EINLEITUNG

E-Commerce, E-Government, E-Banking, ... Die Liste dieser neuerdings in Mode gekommener Begriffe könnte wohl beinahe endlos fortgesetzt werden. An Fax und E-Mail scheinen sich ja inzwischen auch die schon älteren Generationen gewöhnt zu haben; Tag für Tag, ja Stunde für Stunde werden Tausende von mehr oder weniger persönlichen Nachrichten im elektronischen Datennetz kreuz und quer über den gesamten Erdball verschickt. Niemand scheint sich ernsthaft darüber Gedanken zu machen, inwieweit die Vertraulichkeit dieser Daten geschützt ist.

Doch sobald von geschäftlichen Transaktionen über das Internet die Rede ist, scheint bei Jedermann bzw. Jederfrau unvermeidlich - bildlich gesprochen - ein Warnlämpchen aufzuleuchten, welches an die Möglichkeit Trojanischer Pferde[1] und gewiefter Hackerorganisationen[2] erinnert. Der Gefahr von Datenmanipulation und Datendiebstahl wird sehr hohe Bedeutung beigemessen. Vielerorts wird von einem vollständigen Einstieg in das elektronische Zeitalter noch Abstand genommen. Doch die Realität zeigt, dass es kein

[1] Dies sind Programme, welche ähnlich wie ein Computer-Virus funktionieren. Auf den ersten Blick sehen diese wie normale Anwendungsprogramme aus mit den herkömmlichen Funktionalitäten und Verhaltensmustern. Wird das scheinbar harmlose Programm jedoch aufgerufen, so zeigt es auf einmal seine zerstörerische Wirkung.

[2] Unter einem Hacker wird eine Person verstanden, welche in einen Computer „einbricht“ und auf diesem Weg etwa Zugang zu vertraulichen Daten erhält. Siehe Praxishandbuch: Internet Business, Bd. 1, Stand Okt. 2000, Interest Verlag, Augsburg, S. 12

Entrinnen mehr gibt. Diejenigen, die überlebens- und wettbewerbsfähig sein werden bzw. bleiben wollen, müssen sich den neuen Anforderungen stellen. Ein breites Angebot an Seminaren und Kursen wird Geschäftsleuten wie Privatpersonen zur Verfügung gestellt, um sich mit neuen Technologien vertraut und schließlich und endlich von den neu eröffneten Möglichkeiten auch Gebrauch machen zu können. Auch im Bildungsbereich wird verstärkt auf die aktuellen Bedürfnisse des Arbeitsmarktes an qualifizierten Fachkräften, welche in allen Belangen mit den „Neuen Medien" umzugehen
imstande sind, Bedacht genommen; etwa durch das Anbieten zusätzlicher Lehrveranstaltungen im Rahmen eines Studiums.[3]

Das derzeitige Rechtssystem basiert auf dem Gedanken des papiergeschriebenen Dokuments und der daruntergesetzten eigenhändigen Unterschrift. Im neu hereingebrochenen Zeitalter von Informations- und Kommunikationstechnologie ersetzen elektronische Daten die herkömmliche Schrift- und Papierform. Der Einsatz dieser velangt wiederum eine Alternative für den Beweis der Authentizität, d.h. der Urheberschaft einer Willenserklärung. Gesamteuropäische wie einzelstaatliche Gesetzesinitiativen stellen zur Lösung dieses Problems die elektronische Signatur zur Verfügung, welche unter Einhaltung hoher Sicherheitsanforderungen sowohl die zweifelsfreie Zurechenbarkeit zu einer bestimmten Person als auch die Unverfälschtheit des Inhalts sicherstellen soll. Dabei stellen einheitliche rechtliche Rahmenbedingungen auf internationaler Ebene eine Grundvoraussetzung für die breite Akzeptanz neuer technologischer Möglichkeiten dar. Europäische legislative Initiativen orientieren sich dabei an amerikanischen Vorgaben.[4]

[3] Ich persönlich besuche den Universitätslehrgang für Informationsrecht und Rechtsinformation in Wien. Die Durchführung diese Post-Graduate-Studiums erfolgt in enger Zusammenarbeit mit der Wirtschaft und garantiert dementsprechend eine praxisorientierte Ausbildung. Genaueres unter http://www.informationsrecht.at

[4] Eine detaillierte Übersicht über sämtliche Gesetzgebungsinitativen bieten *Gidari, Morgan* und *Coie* im Survey of Electronic and Digital Signature Legislative Initiatives in the United States vom 12. September 1997, verfasst für das ILPF (Internet Lax & Policy Forum), einsehbar unter http://www.ilpf.org/digsig.

2 Bedeutung, Funktionsweise und Rechtsfolgen elektronischer Signaturen

Vorweggenommen seien vier Schlüsselbegriffe, die im Zusammenhang mit der Erörterung der konkreten Einsatzmöglichkeiten elektronischer Signaturen wiederholtermaßen im Mittelpunkt des Interesses stehen:

- Vertraulichkeit
- Datenintegrität
- Authentifizierung
- Nichtbestreitbarkeit

Um die absolute Vertraulichkeit einer übermittelten Nachricht zu gewährleisten, ist die Verschlüsselung dieser selbst notwendig; um die Integrität der Daten sicherzustellen, eine elektronische Signatur. Für die Erfüllung der beiden letztgenannten Anforderungen von Authentifizierung und Nichtbestreitbarkeit ist wiederum der gekoppelte Einsatz von Signatur und Zertifikat unentbehrlich. Die Richtigkeit dieser Behauptungen wird sich im Laufe meiner Arbeit herausstellen.

Im Wege elektronischer Datenübermittlung via Internet im privaten wie auch geschäftlichen Bereich konnte in Vergangenheit und Gegenwart erhebliche Zeit- und Kostenersparnis erzielt werden. Mit der weltweiten Vernetzung unvermeidlich verbunden ist jedoch auch das Auftreten gewisser Unsicherheitsfaktoren. Proportional mit der Kommunikation in öffentlichen und somit auch allgemein zugänglichen Netzen gestiegen ist die Gefahr von Missrauch und Datenmanipulation.

Die Mehrzahl der Rechtsgeschäfte ist dem „formfreien Bereich“ zuzuordnen, d.h. die Geschäftspartner sind an keine spezifischen Formerfordernisse gebunden. Im Sinne der Privatautonomie ist ein per Handschlag abgeschlossener Vertrag ebenso wirksam wie ein durch eine Person öffentlichen Glaubens beglaubigter. Schon bisher konnten Verträge auch über das Internet geschlossen werden, es bedurfte und bedarf dazu lediglich zweier übereinstimmender Willenserklärungen über die wesentlichen Vertragsbestandteile. Insofern behalten sämtliche im herkömmlichen Geschäftsverkehr gültigen Normen und Regelungen auch im elektronischen Bereich ihre Anwendbarkeit. Ein spezielles, nur für das Internet geltende und eigens dafür konzipierte Recht gibt es nicht. Die Gültigkeit von elektronisch erzielten Übereinkünften war und ist unbestritten, doch ergeben sich insbesondere im Beweisrecht erhebliche Schwierigkeiten. Nur allzuleicht kann die Urheberschaft einer Online-Erklärung bestritten werden, der Beweis des Gegenteiles ist so gut wie unmöglich.

Für besonders risikobehaftete und beweisrelevante Rechtsgeschäfte ist durch Gesetz die Schriftform mit eigenhändiger Unterschrift vorgesehen. Diese kann – dem Willen des europäischen Gesetzgeber entsprechend - durch eine elektronische Signatur ersetzt werden, wobei im Hinblick auf die besonderen Sicherheitsanforderungen nur eine nach dem Signaturgesetz bzw. der Richtlinie als „sicher“ geltende einer konventionellen Unterschrift gleichwertig ist. Durch legislative Maßnahmen auf weltweiter, europäischer und nationaler Ebene besteht nun grundsätzlich in weiten Bereichen die Möglichkeit der freien Wahl zwischen herkömmlicher Schriftform und neuer elektronischer Form.

2.1 Einsatzmöglichkeiten[5]

[5] Siehe dazu auch *Kutschera*, Axel, Funktion und Verwendbarkeit der elektronischen Signatur, in SWK 2000, W 7, welcher unter anderem auch die Gebührenselbstbemessung und die elektronische Übermittlung von Rechnungsabschlüssen an das zuständige Finanzamt als in naher Zukunft realisierbar sieht.

Neben dem hohen Rationalisierungspotential im privaten Geschäftsverkehr wird in Zukunft auch der Großteil des Schriftverkehrs mit Behörden online abgewickelt werden können. Derzeit laufende Projekte und Versuchsverfahren werden unter dem Schlagwort des „Electronic Government“ oder „E-Government“ zusammengefasst.

Benötigte Formulare werden rund um die Uhr angefordert und per Signatur elektronisch ausgefüllt werden können. Der Gang zu Melde-, Bau- und Gewerbebehörde könnte auf diese Weise schon bald überflüssig sein, wobei natürlich ein persönliches Beratungsgespräch nicht völlig ersetzbar sein wird. Steuererklärung und KFZ-Anmeldung werden online abgegeben werden können. Auch die elektronische Briefwahl ist aufgrund der besonderen Sicherheit der elektronischen Signatur denkbar.[6] Besonders umfangreich ist der Anwendungsbereich bei Ausweispapieren, wobei die Daten in Zukunft auf einer Chipkarte abgespeichert und digital signiert werden.[7] Auf diesem Wege wird die Überprüfung der Echtheit des Ausweises erleichtert und die Fälschungssicherheit erhöht. Neben der bisher üblichen Funktion des Identitätsnachweises kann ein digitaler Ausweis zusätzlich eine effiziente Zugangs- und Zugriffskontrolle etwa zu unternehmensinternen Computernetzwerken und eine Art Schlüsselersatz für den Zugang zu bestimmten, nicht der Öffentlichkeit zugänglichen Räumlichkeiten bilden.

„Virtueller Kaufhausbummel“ und „Online-Shopping“ mit Bezahlung per Mouseclick und Online-Banking gewinnen immer mehr an wirtschaftlicher Bedeutung. Entwicklungs- und Produktionsdaten können zuverlässig vor Einsichtnahme und Veränderung Dritter geschützt werden, der Urhebernachweis von Software und wissenschaftlichen Erkenntnissen per elektronischer Signatur ist herkömmlichen Methoden vorzuziehen. Der Einsatz von

---

[6] Siehe die Wahl des Studentenparlaments an der Universität Osnabrück unter http://www.ivote.de; die Präsidentschaftsvorwahl in Arizona unter https://www.election-primary.com/azvote und http://www.azdem.org; die erste weltweite Wahl im Internetbereich unter http://www.icann.org/cairo2000/atlarge-topic.htm.

[7] Siehe etwa auch http://www.heise.de/newsticker/data/jk-08.04.00-000/ und http://www.heise.de/newsticker/data/cp-29.02.00-001/.

Signaturverfahren bietet einen besonderen Schutz vor Computerviren, da diese die übermittelten Daten verändern und dies im Rahmen der Signaturprüfung sofort erkennbar gemacht wird. Neben den breiten Einsatzmöglichkeiten im Geschäfts-, Behörden- und Zahlungsverkehr ist zudem die Anwendung im Gesundheitswesen ins Auge zu fassen. Elektronische Arztausweise und elektronische Rezepte können in einem derart sensiblen Bereich einen wertvollen Beitrag zur Schaffung eines effizienten, auf Vertrauensbasis basierenden Gesundheitswesens leisten.[8]

2.2 ... und ihre Grenzen

Wie mir bereits von mehreren Seiten bestätigt und versichert wurde[9], wird sich der „Mann von der Straße" nicht näher mit den neu eröffneten Möglichkeiten der Informationstechnologie auseinandersetzen. Aufwand, Kosten und Mühe würden auch in keinem angemessenen Verhältnis zum neu geschaffenen Rationalisierungspotential stehen. Bei der Abwicklung alltäglicher Geschäfte lohnt sich der Einsatz einer mit hoher Sicherheit ausgestatteten elektronischen Signatur nicht. In sensibleren Bereichen, etwa dem Bankensektor oder der Kommunikation mit Behörden, Gerichten, Rechtsanwälten und Notaren, ist hingegen mit einer breiten Inanspruchnahme des am Markt befindlichen Angebots von Signaturen und Zertifikaten zu rechnen. Im Geschäftsverkehr zwischen Unternehmern[10] oder Unternehmern und Verbrauchern[11] erübrigt sich der Einsatz elektronischer Signaturen ebenfalls, da bei Bestehen jahrelanger Geschäftsbeziehungen und allfälliger interner Sicherheitsvorkehrungen das Risiko von Streitigkeiten etwa durch AGBs bereits relativ geringgehalten wird. Im herkömmlichen E-

[8] Siehe auch Artikel in den Salzburger Nachrichten vom 23. September 2000 betreffend DaMe - Das Datennetz der Medizin, S. 4 und 37 und unter http://www.datakom.at/dame.

[9] Persönliches Gespräch mit Dr. Viktor Mayer-Schönberger anläßlich eines Vortrages im Juni 2000 in Salzburg, siehe auch unter http://www.rdb.co.at/homepages/cover.htm.

[10] auch B2B – Business to Business genannt

[11] auch B2C – Business to Consumer genannt

Commerce dominieren wird das Sicherheitssystem Secure Electronic Transaction (SET[12]), welches bei der Identifizierung und Zahlung mittels Kreditkarte zur Anwendung kommt.

2.3 Das System der Kryptographie

Um Integrität, Sicherheit der Urheberschaft und Vertraulichkeit von elektronisch übermittelten Daten wahren zu können, ist die Verwendung spezieller, ausgereifter und zudem ständig weiterentwickelter Verschlüsselungstechniken und -verfahren unentbehrlich. Die sogenannte „Kryptographie“ oder „Kryptologie“ ermöglicht es, vertrauliche Daten vor Kenntnisnahme, Veränderung oder Unterdrückung durch unbefugte Dritte zu bewahren, beschäftigt sich also mit den Möglichkeiten der Verschlüsselung von Informationen.[13]

Zwischen den verschiedenen, am freien Markt zum Angebot stehenden Verschlüsselungsverfahren hat der einzelne Nutzer völlige Wahlfreiheit. Dem Recht auf Kommunikationsfreiheit, auf Privatsphäre, auf Datenschutz und Wahrung des Fernmeldegeheimnisses wird auf diese Weise Genüge getan. Doch unweigerlich mit der vermehrten Inanspruchnahme und Zugänglichkeit verschiedenster Verschlüsselungstechniken wird die organisierte Kriminalität gefördert und zugleich eine effiziente Kontrolle und Überwachung wesentlich erschwert. Für nationale und internationale Strafverfolgungsbehörden wird es schier unmöglich gemacht, wirksam gegen derartige Tendenzen vorzugehen.

---

[12] siehe unter http://www.visa.com/set oder http://www.mastercard.com/set und *Weissengruber*, Christian, Elektronische Zahlungssysteme: Sichere Zahlungen im Internet mit eigenem Standard, in Computerwelt 38/2000, S. 35. Das SET-Verfahren bildet einen Sicherheitsstandard für Kreditkartentransaktionen über das Internet, ihre Entwicklung wurde u.a. von Mastercard und Visa mitgetragen. Die Zertifizierungsinstanz SETCO hat die SET-Konformität von Softwareprodukten und –komponenten zu überprüfen, ehe diese zum Einsatz gelangen dürfen.

[13] Siehe dazu und zur grundrechtlichen Problematik von beschränkenden Regelungen *Beuscher*, *Schmoll*, Kryptotechnologie und Exportbeschränkungen, in CR 8/1999, S. 529f und *Mayer-Schönberger*, *Pilz*, E-Commerce: Rechtliche Rahmenbedingungen und Notwendigkeiten, AnwBl 1999, S. 217ff

In diesem Spannungsfeld zwischen Überwachungsstaat und „gläsernem Menschen“ auf der einen Seite und dem „Recht des einzelnen auf Privatsphäre“, in diesem Zusammenhang auf „private Informationssphäre“, auf der anderen Seite, ist der Gesetzgeber aufgefordert, effektive Überwachungs- und Kontrollmöglichkeiten zu schaffen. Aus diesem Grund sollten etwa Stellen eingerichtet werden, bei denen die Schlüssel zu hinterlegen sind, sodass die Exekutive im Falle des Vorliegens eines konkreten Verdachts bzw. eines richterlichen Beschlusses dazu imstande ist, auch verschlüsselte Informationen zu entschlüsseln. Hinsichtlich der konkreten Befugnisse derartiger „Trusted Third Parties“ besteht jedoch nach wie vor Uneinigkeit.[14] Allein die Einrichtung derartiger Institutionen zur Schlüsselhinterlegung stellt eine Beeinträchtigung des freien Informationsaustausches und des Grundrechtes auf Datenschutz dar, welche an EG-Vertrag und Datenschutz-Richtlinie 95/46/EC vom 24.10.1995 zu messen ist.

2.4 Funktionsäquivalenz von Unterschrift und Signatur

Die vielfach erwähnte elektronische Signatur hat mit einer Unterschrift nur wenig gemeinsam. Eine Signatur ist keine Unterschrift im herkömmlichen Sinn, sondern vielmehr eine komplexe Reihenfolge von Buchstaben und Zahlenkombinationen. Durch die Kompliziertheit des Signierungsverfahrens sind die Möglichkeiten von Verfälschung und Manipulation viel geringer als bei eigenhändig gefertigten Unterschriften. Zweitere können ohne große Anstrengung nachgemacht, d.h. kopiert werden; auch etwa eingescannte Unterschriften sind einer Verfälschung leicht zugänglich.

Behält man die bisher vorherrschende Papierform im Auge, so dient die eigenhändige Unterfertigung eines Dokuments den verschiedensten Zwecken. Zum einen ermöglicht sie die zweifelsfreie Feststellung der Identität des Unterzeichnenden. Zum anderen identifiziert sich der Verfasser durch seine Unterschrift mit dem jeweiligen Erklärungsinhalt. In der Regel ist sich

[14] http://www.crypto.com und http://wwwcrypto.com/key_study

der Unterzeichner im Zeitpunkt des Unterfertigens der damit verbundenen Rechtsfolgen bewusst.

Eine elektronische Signatur erfüllt im wesentlichen sämtliche wichtigen Funktionen einer handschriftlichen Unterschrift. Die Warnfunktion etwa durch die Aufwendigkeit des Verfahrens, die vorherige Darstellung des gesamten zu signierenden Dokuments und die verpflichtend vorgesehenen, rechtlichen Belehrungen durch die Zertifizierungsstellen.

Durch spezielle Methoden der Ver- und Entschlüsselung wird die Echtheit und Unverfälschtheit sichergestellt. Nachträgliche Veränderungen des Textes, d.h. das Hinzufügen oder Wegnehmen von Textteilen ohne Wissen des Signierenden, werden sichtbar gemacht. Elektronisch signiert werden können zudem nicht nur Nachrichten im herkömmlichen Sinn, sondern auch Bilder, Musik, Software, udgl. Der Nachweis der Echtheit einer elektronischen Signatur ist um einiges leichter zu erbringen, als dies bei der eigenhändigen Unterschrift der Fall ist. Das Überprüfen und Sichtbarmachen von Manipulationen erfolgt vollautomatisch durch die entsprechende, sicherheitsgeprüfte Software.

Die Verschlüsselung selbst ist dabei für jeden Empfänger, egal ob befugt oder unbefugt, erkennbar. Zum Zwecke der Erzielung von Integrität und Authentizität reicht eine elektronische Signatur aus, welche die Lesbarkeit des Inhalts selbst nicht berührt. Wird jedoch absolute Vertraulichkeit bzw. Gemeinhaltung einer zu übermittelnden Nachricht bezweckt, so ist der gesamte Inhalt mittels einer elektronischen Signatur zu verschlüsseln.

Die Signierung elektronisch übermittelter Daten dient somit vornehmlich zwei Zielen. Zum einen wird das Vertrauen des jeweiligen Empfängers in die Identität des Übermittlers und die Integrität der Daten gestärkt. Zum anderen wird durch die Möglichkeit des eindeutigen Feststellens der Authentizität und Urheberschaft der Verfasser der versendeten Nachricht in rechtsverbindlicher Weise gebunden.

2.5 Signierungsvorgang

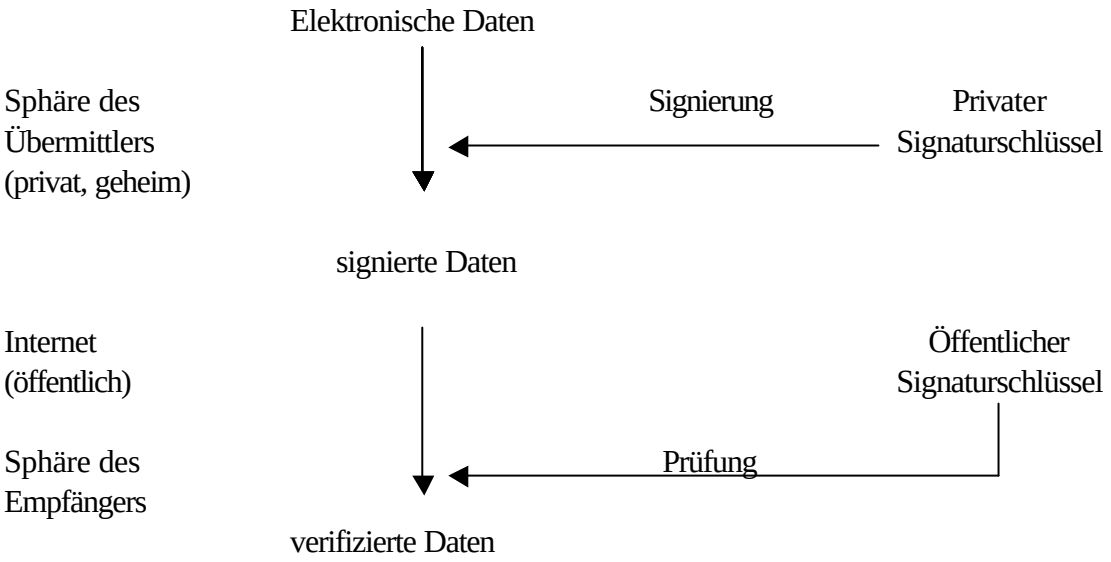
Die elektronische Signierung bildet den Überbegriff über sämtliche Verfahren der Kryptotechnologie. Europäische wie nationale Gesetzgebungsgremien verwenden diesen, um die Anwendbarkeit legislativer Vorgaben auch für künftige technische Verfahren sicherzustellen. Die digitale Signierung ist in diesem Zusammenhang ein Verfahren, welches dem heutigen Stand der Technik entspricht und dementsprechend zur Anwendung gelangt. Zum besseren Verständnis ist an dieser Stelle eine kurze Beschreibung der technischen Abläufe vonnöten:

Die digitale Signatur beruht auf dem Prinzip der asymmetrischen Verschlüsselung oder „Public Key Encryption", welches 1975[15] entwickelt wurde. Im Gegensatz zur weniger sicheren symmetrischen Verschlüsselung, bei welcher ein einziger, sowohl dem Sender wie auch dem Empfänger bekannter Schlüssel ausreicht, werden bei ersterer zwei, in komplementärer Weise zueinander stehende Schlüssel zur Ver- und Entschlüsselung benötigt. Zur Durchführung einer symmetrischen Verschlüsselung muss der Schlüssel beiden Kommunikationspartnern schon im vorhinein bekannt sein, er muss also ausgetauscht werden. Diese Tatsache allein birgt bereits einen gewissen Unsicherheitsfaktor in sich.[16]

[15] dazu ausführlich *Menzel*, Elektronische Signaturen, Wien 2000, S. 30ff

[16] *Stockinger*, Österreichisches Signaturgesetz: Bedeutung, Funktion und Rechtsfolgen elektronischer Signaturen, in MR 4/1999, S. 205

Zur besseren Veranschaulichung des Signaturvorgangs bei Asymmetrischer Verschlüsselungstechnik folgende Skizze:[17]



Um im Rahmen der derzeit als sichersten geltenden asymmetrischen Verschlüsselung eine elektronische Signatur erzeugen zu können, benötigt man einen Datenträger, etwa eine Chipkarte, auf dem der private Signaturschlüssel gespeichert ist, und einen PC mit Chipkartenlesegerät und Signaturfunktion. Für die Prüfung derselben genügt ein PC mit Signaturfunktion. Der Signierungsvorgang selbst wie auch die darauf folgende Signaturprüfung verlangen keine detaillierten technischen Vorkenntnisse, diese laufen über ein speziell aufzurufendes Programm mehr oder weniger automatisch ab. Die Signatur wird dem zu versendenden Dokument automatisch angehängt.

Im Rahmen der asymmetrischen Verschlüsselung kommen ein privater Schlüssel, welcher absolut geheim zu halten ist, und ein in einer speziellen mathematischen Umkehrbeziehung dazu stehender öffentlicher, allgemein zugänglicher Schlüssel zur Anwendung. Der öffentliche

[17] *Stockinger*, Österreichisches Signaturgesetz: Bedeutung, Funktion und Rechtsfolgen elektronischer Signaturen, MR 4/1999, S. 203 ff

Schlüssel muss aus dem privaten ableitbar sein, jedoch muss die Ableitbarkeit in umgekehrter Weise nach dem jeweiligen Stand der Technik
ausgeschlossen werden können. Der private Signaturschlüssel ist in der Regel auf einem Datenträger, etwa einer Chipkarte, gespeichert und kann nur in Verbindung mit einer geheimen Personenidentifikationsnummer, der PIN, aktiviert werden. Es ist auch ohne weiteres möglich und denkbar, die Signaturerstellungsdaten aus Sicherheitsgründen auf mehreren Signaturerstellungseinheiten zu speichern, d.h. aufzuteilen. Infolgedessen kann der Signierungsvorgang erst bei entsprechender Aktivierung aller Datenträger in ihrer Gesamtheit eingeleitet werden. Über diese Wirkung hat der Signator im vorhinein durch den Zertifizierungsdiensteanbieter auf jeden Fall informiert zu werden.[18]

Eine Nachricht, welche mit einem bestimmten privaten Schlüssel verschlüsselt wurde, ist nur mehr einzig und allein durch den dazu passenden öffentlichen Schlüssel entschlüsselbar. Aus Gründen der Einfachheit wird nach dem der Codierung zugrundeliegenden RSA-Algorithmus in der Regel nicht der gesamte Nachrichteninhalt verschlüsselt, sondern nur eine dafür repräsentative komprimierte Datenkombination. Diese wird mit Hilfe eines speziellen mathematischen Programms oder Verfahrens, dem sogenannten Hash-Algorithmus, ermittelt. Eine derartige verkürzte Version oder Quersumme des Dokumentes ist zwar bei jedem Dokument gleich lang, in ihrer konkreten Ausformung jedoch immer verschieden. Nur der solcherart ermittelte Hashwert wird mit dem privaten Schlüssel verschlüsselt. Zwischenzeitig ist es ohne weiteres auch möglich und technisch durchführbar, dass der Schlüssel im Verlauf des Verschlüsselungsvorganges niemals, auch nur kurzfristig, die Chipkarte verlässt, weshalb jede Möglichkeit einer unbefugten Abfrage vom jeweiligen PC von vornherein ausgeschlossen ist. Die verschlüsselte Kurzfassung des Dokuments bildet die eigentliche digitale Signatur und wird als Anhang zur übermittelten Nachricht dem Empfänger übermittelt.

Dieser kann nun mit dem ebenfalls mitübermittelten bzw. online abrufbaren öffentlichen Schlüssel den mit dem privaten Schlüssel verschlüsselten Hash-Wert entschlüsseln.

[18] siehe § 4 Abs 2 öSigV

Gleichzeitig mit dem Vorgang der Entschlüsselung wird aus dem empfangenen Dokument nochmals der dafür repräsentative Hash-Wert gebildet, d.h. auch der Empfänger lässt die unverschlüsselte Datei durch dieselbe Hash-Funktion laufen wie der Signator. Entsprechen sich nun beide ermittelten Werte, so ist damit die Integrität der Daten, d.h. ihre Unveränderheit und Vollständigkeit, gesichert.

Die Ingebrauchnahme einer Signatur gewährleistet die Zurechenbarkeit einer Willenserklärung, der Urheber kann sich nicht mehr so ohne weiteres davon distanzieren. Die bloße Behauptung, die Signatur wäre von einem unbefugten Dritten verwendet worden, ist als solche, d.h. ohne das Erbringen von Beweisen irrelevant. Die Signatur wird dem Inhaber des Signaturschlüssel zugeordnet. Von dieser besonderen Rechtsfolge, wie auch allgemein von den Gebrauchsmöglichkeiten und den damit verbundenen Pflichten und Risiken der Innehabung eines Signaturschlüssels, ist der Nutzer bei bzw. vor Ausgabe des privaten Schlüssels in Kenntnis zu setzen.

Will der Nutzer nicht nur die Authentizität und Integrität der Nachricht sicherstellen, sondern auch die alleinige Lesbarkeit durch einen bestimmten Empfänger, so ist der soeben beschriebene Vorgang in gewisser Weise umzukehren. Der jeweilige Absender hat die gesamte Nachricht, d.h. das Dokument als Ganzes, mit dem öffentlichen Schlüssel des Empfängers zu verschlüsseln. Die Nachricht ist nun für Dritte unlesbar gemacht, sie kann lediglich durch den privaten Schlüssel des Empfängers entschlüsselt und damit wieder verständlich gemacht werden. Es können jedoch auch beide Varianten miteinander verknüpft werden. Verschlüsselt der Sender eine Nachricht bzw. deren Hashwert etwa zuerst mit dem öffentlichen Schlüssel des Empfängers und hernach mit dem eigenen privaten Schlüssel, so ist die Echtheit, Unverfälschtheit, Zurechenbarkeit und absolute Vertraulichkeit auf beiden Seiten gesichert.[19]

[19] Die verschiedenen Varianten sind auch dargestellt in *Pankart*, Sichere E-Mail: Signieren und Verschlüsseln, in Datagraph 2/2000, S. 58

Nicht einer gesetzlichen Regelung unterworfene Signierungsverfahren sind etwa „Pretty Good Privacy (PGP)“[20] und „Verisign“[21] mit einem personenidentifizierenden Ansatz; „Secure Electronic Transaction (SET)“[22] mit einem kreditkartenidentifizierenden Ansatz oder „Secure Sockets Layer (SSL)“[23] mit einem rechneridentifizierenden Ansatz.

2.6 Zertifikate

Das soeben dargestellte Verschlüsselungsverfahren ermöglicht noch nicht die Zuordenbarkeit des verwendeten Schlüssels zu einer bestimmten Person. Dazu war die Schaffung einer Public Key Infrastructure, kurz PKI genannt, d.h. eine eigene Infrastruktur der Signaturschlüsselzuordnung, notwendig. Der Richtlinie entsprechend setzt sich diese aus einer Vielzahl von „vertrauenswürdigen Dritten“, sogenannten Zertifizierungsdiensteanbietern, „Trusted Third Parties“ oder „Trust Centers“, zusammen. Deren Aufgabe besteht im Ausstellen digitaler Zertifikate und im Bestätigen der Zuordnung eines „Public Key“ zu einem bestimmten Rechtssubjekt auf individuelle Anfrage hin. Durch Ausstellung eines für einen begrenzten Zeitraum geltenden elektronischen Zertifikats wird die Zugehörigkeit eines öffentlichen Schlüssels und dadurch mittelbar auch des privaten Schlüssels zu seinem Inhaber bestätigt. Die Zertifizierungsstellen generieren einzig dem Inhaber zuordenbare Schlüsselpaare und stellen darüber über Antrag Zertifikate aus, für deren inhaltliche Richtigkeit zum Zeitpunkt der Ausstellung sie auch einzustehen haben.

---

[20] Mit PGP erstellte Signaturen gelten aufgrund bestehender Sicherheitsmängel nicht als „sicher“ im Sinne des Signaturgesetzes. Bis zum Aufbau einer entsprechenden Public-Key Infrastruktur war es ein sehr weit verbreitetes und verbraucherfreundliches Verfahren. Siehe auch unter http://www.momentus.com.br/PGP/doc/howpgp.html.

[21] siehe unter http://www.verisign.com

[22] siehe FN 12

[23] siehe unter http://www.rsa.com/rsalabs/faq/html/5-1-2.html. SSL ist ein von Netscape entwickeltes Verschlüsselungsverfahren, welches hauptsächlich im elektronischen Geschäftsverkehr Anwendung findet und zur Zeit De-facto-Standard für die Übermittlung vertraulicher Daten ist.

Neben dem soeben dargestellten hierarchischen Zertifizierungsmodell, bei welchem die Zertifikate von eigens dafür zuständigen Zertifizierungsstellen ausgestellt werden, gibt es auch dezentrale Signatursysteme. In das österreichische Signaturgesetz wie auch in die Europäische Signaturrichtlinie hat lediglich ersteres Eingang gefunden. Grundsätzlich sind beide Systeme zulässig, jedoch entfalten lediglich Signaturen, die in einem hierarchischen System erzeugt werden, Rechtswirkungen. Die bereits erwähnte Verschlüsselungssoftware „Pretty Good Privacy" geht von einem dezentralen System aus, im Rahmen dessen sich die Anwender selbst wechselseitig die Inhaberschaft eines bestimmten Schlüsselpaares bestätigen. Durch die Verknüpfung mehrerer solcher Zertifikate verschiedener Anwender wird eine entsprechend hohe Sicherheit über die Identität des Signaturinhabers erreicht.

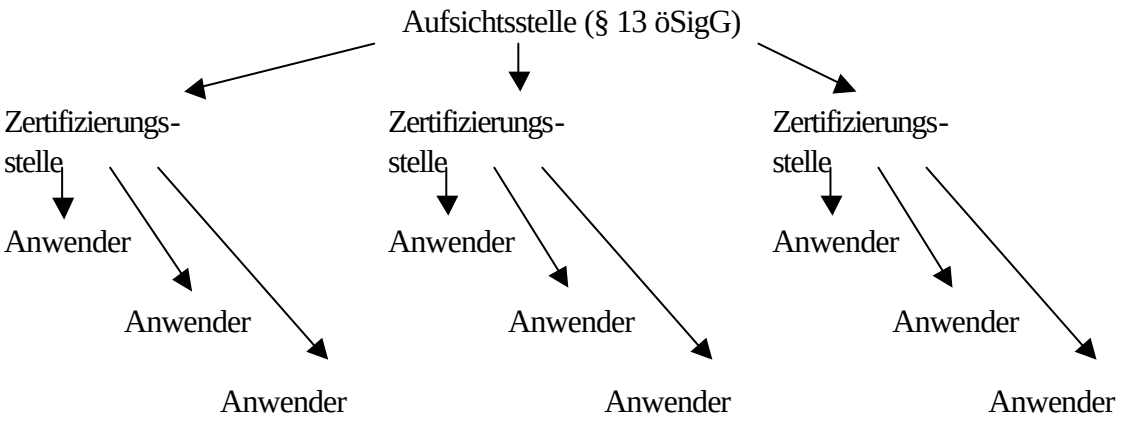


Abb.: Hierarchisches Zertifizierungsmodell in Österreich bzw. nach der Signaturrichtlinie[24]

Zertifikate können einer Vielzahl von Zwecken dienen und die verschiedensten Informationen zum jeweiligen Inhaber enthalten, wie etwa Name, Wohnort, Sozialversicherungs- und Steuernummer, Angaben über die Kreditwürdigkeit, Zahlungssicherheiten, spezifische Ermächtigungen, udgl. Anstelle des Namens kann auch ein Pseudonym in das Zertifikat aufgenommen werden, welches nur in besonderen Ausnahmefällen gegenüber Sicherheits- und Strafverfolgungsbehörden bzw. nur auf gerichtlichen Beschluss hin aufzudecken ist. Einer

einzelnen natürlichen Person kann auch eine Mehrzahl an Zertifikaten zugeordnet werden bzw. ist die Verwendung verschiedener Pseudonyme durch einen einzelnen Berechtigten denkbar. Die Zuerkennung eines Zertifikates ist nach österreichischem Recht auf natürliche Personen beschränkt, da auch juristische Personen letztendlich nur durch ihre vertretungsbefugten Organe handeln können. Aus diesem Grund sind Vollmachten, Vertretungsrechte und berufsrechtliche Zulassungen in sogenannte Attribut-Zertifikate aufzunehmen, die zusammen mit dem Grund- oder Hauptzertifikat abrufbar sind.

Die öffentlich zugänglichen Zertifikate werden dem Dokument ebenso wie der öffentliche Schlüssel angehängt oder im Internet für einen unbeschränkten Personenkreis abfragbar gemacht. Denkbar und der Praxis entsprechend ist etwa die Möglichkeit zum Download von der personen- oder unternehmenseigenen Homepage oder von einem Public-Key-Server, wie z.B. Pretty Good Privacy[25], oder das Versenden des öffentlichen Schlüssels per Email.

Die Zertifizierungsstellen haben zudem eigene Verzeichnisse zu führen, welche eine Auflistung sämtlicher von ihnen ausgegebener Zertifikate enthalten. Dadurch wird es den Nutzern ermöglicht, jederzeit online zu überprüfen, ob ein Zertifikat zum Zeitpunkt der Erzeugung einer elektronischen Signatur Gültigkeit hatte oder aber etwa bereits gesperrt war. Die Zertifikate werden, um ihrerseits fälschungssicher zu sein, mit der elektronischen Signatur der jeweiligen ausstellenden Zertifizierungsstelle versehen. Dadurch ist sichergestellt, dass die im Zertifikat enthaltenen Daten richtig und auch ihrerseits vor Manipulationen geschützt sind.

2.7 Conclusio

Vielfach wird die Verwendung elektronischer Signierungsverfahren kategorisch ausgeschlossen, da deren Vertrauenswürdigkeit in Zweifel gezogen wird. Vorweggenommen

[24] *Stockinger,* Österreichisches Signaturgesetz: Bedeutung, Funktion und Rechtsfolgen elektronischer Signaturen, Medien und Recht 4/1999, S. 206

[25] siehe http://www.pgp.net; Freeware: http://www.pgpi.org; kommerzielle Version: http://www.nai.com

sei hier, dass eine absolute Sicherheit vor Fälschung niemals bestehen wird, auch im herkömmlichen Geschäftsverkehr gibt es diese nicht. Nach einem gewissen Zeitraum wird es voraussichtlich immer wieder jemandem gelingen, einen Schlüssel bzw. ein Verfahren auszuforschen und zu manipulieren. Jedoch ist hier doch auch zu berücksichtigen, dass diejenigen, die derartig hoch ausgereifte wissenschaftliche Vorgänge zu knacken versuchen, ebenso in wirtschaftlichen Maßstäben zu denken haben. Spätestens, wenn sich Zeit- und Kostenaufwand nicht mehr mit dem zu erwartenden Nutzen decken, wird kein Interesse mehr daran bestehen, Kenntnis von einem bestimmten Schlüssel zu erlangen.

Zusammenfassend beruht die Sicherheit gesetzlich anerkannter elektronischer Signaturen auf folgenden Faktoren:

- durch führende Experten aus Wissenschaft, Wirtschaft und Behörden ständig geprüfte und weiterentwickelte mathematische Verfahren zur sicheren, „unknackbaren" Verschlüsselung
- Einmalige Signaturschlüssel, deren nochmaliges Auftreten mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann (z.B. beträgt beim RSA-Verfahren[26] die Schlüssellänge derzeit 1024 Bit, was etwa einer 300-stelligen Zahl entspricht).
- absolute Geheimhaltung des privaten Signaturschlüssels. Die Speicherung desselben bei der Zertifizierungsstelle ist untersagt. Die PIN ist ebenso wie die einer Bankomatkarte geheim zu halten, die Weitergabe der Chipkarte erfolgt auf eigene Gefahr. Wird diese gestohlen oder kommt sie sonstwie abhanden, ist das Zertifikat unverzüglich zu sperren.
- Die Bindung des Signaturschlüssels manifestiert sich durch Besitz, etwa der Chipkarte, und Wissen, etwa der PIN. Zusätzlich können auch biometrische Verfahren eingesetzt werden, welche die Möglichkeit eines Missbrauchs durch Unbefugte weiter einschränken. So ist es etwa möglich, Referenzdaten über Fingerabdrücke auf der

[26] Abkürzung für „Rivest/Shamir/Adleman"-Verfahren, entsprechend dem Namen seiner Entwickler

Chipkarte zu speichern[27], sodass die ebenfalls darauf befindliche elektronische Signatur erst nach einem Vergleich mit den Fingerstrukturen des jeweiligen Nutzers freigegeben wird.

- Durch spezielle PC-Zusatzkomponenten kann ausgeschlossen werden, dass fremde Daten unbemerkt zum Signieren untergeschoben oder Daten vor dem Signierungsvorgang heimlich verändert werden.
- zuverlässige Überprüfung von Signaturen und Vermeiden unzutreffender Korrektheitsbestätigungen[28]

[27] Von Siemens etwa wurde ein Sensor entwickelt, welcher direkt auf der Chiparte angebracht werden kann und dem Erfassen von Fingerabdrücken dient. Erst bei einer Übereinstimmung der über den Sensor erfaßten Fingerabdrücke mit den auf der Chipkarte gespeicherten Werten wird der Signaturschlüssel freigegeben. Denkbar ist nicht nur die Speicherung eines Fingerabdrucks, sondern auch aller sonstiger Merkmale, die bei jedem Menschen verscheiden und für eine Person eindeutig sind, wie etwa Druck, Dynamik und Form einer eigenhändigen Unterschrift, Sprache und Augenhintergrund.

[28] *Bieser/ Kersten*, Chipkarte statt Füllfederhalter: Daten beweissicher „elektronisch unterschreiben“ und zuverlässig schützen, Heidelberg: Hüthig, 1998, S. 20ff

3 OECD[29]

Die KRYPTOGRAPHIE-RICHTLINIE[30] wurde von einer im Jahre 1996 eingerichteten Ad-hoc-Gruppe ausgearbeitet und schließlich 1997 vom OECD-Rat angenommen. Sie hat lediglich empfehlenden Charakter und weist die Mitgliedstaaten an, für ihre Umsetzung auf nationaler Ebene zu sorgen. Um die Ungehindertheit des Einsatzes von Verschlüsselungstechniken zu fördern, ist in internationaler Zusammenarbeit nach folgenden Prinzipien vorzugehen:

- Verwendung von vertrauensschaffenden, kryptographischen Verfahren
- freie Wahl des Verschlüsselungssystems
- Marktorientiertheit der Verfahren: Die am Markt zum Angebot stehenden Verfahren haben sich an den individuellen Bedürfnissen von Konsumenten, Wirtschaftstreibenden und staatlichen Behörden zu orientieren.
- spezielle Haftungsvorschriften
- Wahrung der Persönlichkeitsrechte
- zwischenstaatliche Koordinierung und Zusammenarbeit

Dementsprechend ist in den meisten Mitgliedsländern der OECD wie auch der EU die Freiheit der elektronischen Verschlüsselung gesichert. In Österreich etwa findet sich keine einzige Norm, die das Chiffrieren von Nachrichten verbieten würde, wobei ein derartiges Verbot auf jeden Fall eine grundrechtliche Einschränkung darstellen würde.

In Frankreich existierte bis 1996 eine Verbot jeglicher Verschlüsselung. Infolge einer Gesetzesrevidierung ist nun der Einsatz kryptographischer Verfahren insofern zulässig, als die

[29] Organization of Economic Co-Operation and Development

[30] Recommendation of the Council concerning Guidelines for Cryptography Policy C(97)62 Nr. 21; unter http://www.oecd.org (/subject/e commerce) (publications/letter/0604.html)(dsti/iccp/cryptoe.html)

Signaturen im Bedarfsfall von den nationalen Behörden entschlüsselt werden können bzw. im Falle von besonders sicheren Verfahren zu hinterlegen und durch die DISSI[31] zu genehmigen sind. Zwingend vorgesehen ist weiters die Anmeldung kryptographischer Verfahren zu Zwecken der Authentifikation.[32]

[31] La Delegation Interministerielle pour la Securité des Systèmes d´Information (DISSI)

[32] unter http://www.ens.fr/dmi/equipes_dmi/grecc/loi.html und http://www.cnam.fr/Network/Crypto/

4 Uncitral[33]

Auch die Handelsrechtskommission der Vereinten Nationen beschäftigte sich eingehend mit den Problemen rund um die elektronische Signatur. Am 23.11.1998 legte sie einen Entwurf einheitlicher Regeln[34] betreffend neu geschaffener Möglichkeiten vor, welcher Mindeststandards, Haftungsregelungen und Bestimmungen zu Authentisierung und Zertifizierung beinhaltet. Der Uncitral folgend kann bei Einhaltung entsprechender Anforderungen an Identifizierung und Authentifizierung dem Erfordernis von Schriftlichkeit bzw. Unterschriftlichkeit auch bei elektronischen Dokumenten entsprochen werden.[35] Der derzeitige Entwurf ist relativ kurz gehalten, er beinhaltet lediglich 8 Artikeln. Artikel H des genannten Entwurfes lässt den Zertifizierungsstellen weitreichende Vertragsfreiheit bei der Abfassung ihrer Allgemeinen Geschäftsbedingungen. Eine haftungsrechtliche Einstandspflicht gilt grs. für die Fälle fehlender bzw. unzutreffender Angaben im Zertifikat, nicht rechtzeitiger Sperrung des Zertifikats und bei Verstößen gegen das Gesetz oder eigene unternehmensinterne Normen. Gelingt es dem jeweiligen Anbieter, fehlendes Verschulden auf seiner Seite nachzuweisen, kann er sich in den beiden erstgenannten Fällen von jeglicher Haftung freihalten. Wie auch in der Signaturrichtlinie ist die Anwendbarkeit des Zertifikats auf bestimmte Bereiche bzw. auf einen im vorhinein festzulegenden Transaktionswert beschränkbar.[36]

---

33 United Nations Commission on International Trade Law

34 siehe Draft Articles on Electronic Signatures, A/CN.9/WG.IV/WP.80 unter http://www.un.or.at/(uncitral/en-index.htm) und http://www.uncitral.org, Unterseite „Preparatory Documents - Working Group on Electronic Commerce"; die aktuelle Fassung: A/CN.9/WG.IV/WP.80 vom 15. Dezember 1998 - United Nations Commission on International Trade Law - Working Group on Electronic Commerce - Thirty-fourth session, Vienna, 8 - 19. February 1999 - Digital Signatures, Text unter http://www.uncitral.org/english/sessions/wg_ec/wp-80.htm

35 siehe Art H §§ 22-24 des Entwurfes 1999

36 *Riedl*, Sabine, Auch die UNCITRAL mengt sich in den elektronischen Geschäftsverkehr ein, in ecolex 4/1999, S. 241ff

5 Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

5.1 Hintergrund und Ziel

Die Richtlinie der Europäischen Union wurde erst kürzlich am 19.1.2000 im Amtsblatt L13/12 veröffentlicht und damit auch in Kraft gesetzt. Ihre Entstehung wurde maßgeblich vom deutschen Signaturgesetz und von den einschlägigen Gesetzen in den USA beeinflusst. Die für den gesamten E-Commerce wichtige Rahmenvorgabe soll das Vertrauen der Nutzer in die Sicherheit des Internet stärken.

Die Richtlinie wurde im Wege des Mitentscheidungsverfahrens, dargelegt in Artikel 251 EG-V, (ex-Artikel 189 b)[37] verabschiedet. Als rechtliche Grundlage dient unter anderem Artikel 5 EG-V (ex-Artikel 3 b), welcher das Prinzip der Subsidiarität innerhalb der Europäischen Gemeinschaft zum Ausdruck bringt. Demnach haben die Gesetzgebungsorgane der Gemeinschaft zusätzlich zu den in ihren ausschließlichen Zuständigkeitsbereich fallenden Bereichen auch tätig zu werden, soweit die Ziele besser auf Gemeinschaftsebene als auf nationaler Ebene verfolgt und erreicht werden können. Der Richtlinienvorschlag schafft dementsprechend bloß die erforderlichen Rahmenbedingungen, um die innerstaatliche Umsetzung zu erleichtern bzw. voranzutreiben.

Durch die Schaffung eines harmonisierten rechtlichen Rahmens für die Verwendung elektronischer Signaturen im Europäischen Raum wird versucht, das ordnungsgemäße

37 Vertrag von Amsterdam zur Änderung des Vertrags über die Europäische Union, der Verträge zur Gründung der Europäischen Gemeinschaften sowie einiger damit zusammenhängender Rechtsakte samt Schlussakte (Vertrag von Amsterdam), BGBl. III Nr. 83/1999

Funktionieren des Binnenmarktes zu gewährleisten. Die Fixierung allgemein geltender Sicherheitsanforderungen und die allmähliche Angleichung einzelstaatlicher Formvorschriften steht dabei im Vordergrund. Dies vor dem Hintergrund, die ebenfalls normierte rechtliche Anerkennung elektronischer Signaturen wirksam durchsetzen zu können. Der Aufbau entsprechender technischer und vor allem grenzüberschreitend einsetzbarer Infrastruktur ist eine Grundvoraussetzung, bei deren Fehlen sämtliche legistischen Bemühungen erfolglos bleiben müssen. Die Richtlinie zielt allgemein gesprochen auf die Harmonisierung nationaler Gesetze, die Errichtung eines rechtlichen Rahmens für elektronische Signaturen und die Stärkung des Vertrauens in ebendieselben. Diese ermöglichen es - kurz zusammengefasst - dem jeweiligen Empfänger einer elektronisch übermittelten Nachricht, die Herkunft der Daten sowie deren Vollständigkeit und Unverändertheit zweifelsfrei zu überprüfen.

Durch die Vorgaben der Richtlinie nicht berührt wird *„nationales Vertragsrecht, insbesondere betreffend den Abschluss und die Erfüllung von Verträgen, oder andere, außervertragliche Formvorschriften bezüglich der Unterschriften“*. *„Einzelstaatliche Formvorschriften, die den Abschluss von Verträgen oder die Festlegung des Ortes eines Vertragsabschlusses betreffen“*[38], bleiben weiterhin voll in Geltung. Weiters nicht angetastet wird der Grundsatz der Privatautonomie. Es wird den Geschäftspartnern überlassen, inwieweit sie elektronischen Signaturen in ihren wechselseitigen Geschäftsbeziehungen rechtliche Wirksamkeit zuzumessen zu gedenken. All jene Vorschriften, die die Schriftform unmittelbar de iure oder de facto voraussetzen, sind auf ihre absolute Notwendigkeit und Unersetzbarkeit hin zu überprüfen. Entsprechend dem Ziel der Richtlinie über elektronische Signaturen und der später zu behandelnden Richtlinie über den elektronischen Geschäftsverkehr, die mit rechtlichen Folgen verbundene Anwendung elektronischer Signaturen zu fördern, ist in weiterer Folge die

Rechtmäßigkeit der Implementierung neuer Schriftformerfordernisse unter einem besonders strengen Gesichtswinkel zu betrachten. Ansonsten wäre es einzelstaatlicher Kompetenz bzw. Willkür vollständig in die Hände gelegt, inwieweit sie neuen Technologien überhaupt die

[38] SigRl ABl L 13/12 vom 19.1.2000, Erwägungsgrund 17

Möglichkeit einräumen wollen, sich im Geschäfts- und Rechtsverkehr entsprechend zu etablieren.

Die ersten Initiativen betreffend die Erlassung einer Signaturrichtlinie begannen im Jahre 1997 in Form von Mitteilungen der Kommission mit den Titeln „Europäische Initiative für den elektronischen Geschäftsverkehr“ und „Sicherheit und Vertrauen in elektronische Kommunikation - Ein europäischer Rahmen für digitale Signaturen und Verschlüsselung“[39]. Diese heben die Notwendigkeit eines einheitlichen Konzeptes im Bereich der elektronischen Kommunikation hervor. Sowohl der Rat als auch das Europäische Parlament begrüßten die Bemühungen der Kommission mit Wohlwollen.

Am 13. Mai 1998 erging der „Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen“[40], welcher eine einheitliche Rechtsgrundlage für die Mitgliedstaaten der EU schaffen sollte. Nach offizieller Vorlage folgten Stellungnahmen des Wirtschafts- und Sozialausschusses[41] und des Ausschusses der Regionen[42]. Am 13. Januar 1999 befürwortete und billigte das Parlament in Erster Lesung den Vorschlag der Kommission mit Änderungen[43]. Die insgesamt 32 Änderungsvorschläge betreffen vornehmlich die gegenseitige rechtliche Anerkennung von elektronischen Signaturen durch die Mitgliedstaaten auf der Grundlage verbesserter Zertifizierungsdienste sowie die rechtliche Gleichwertigkeit der elektronischen Signatur mit der

---

39 KOM 503 endg. vom 8.10.1997

40 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen, Brüssel, den 13.5.1998, KOM (1998) 297 endg.

41 Stellungnahme des Wirtschafts- und Sozialausschusses, ABl. C 40 vom 15.2.1999

42 Stellungnahme des Ausschusses der Regionen zu dem „Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen“, ABl. C 93 vom 6.4.1999

43 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen, ABl C 104 vom 14.4.1999

handschriftlichen Unterzeichnung. Die Kommission hat die Mehrzahl der Änderungen, d.h. exakt 22, in den geänderten Vorschlag 195 endg. vom 30. April 1999[44] ohne weitere Korrekturen übernommen. Am 28. Juni 1999 legte der Rat einen Gemeinsamen Standpunkt[45] fest, welcher dem Europäischen Parlament zur Behandlung in Zweiter Lesung übermittelt wurde. Es folgte die Annahme von Änderungen am 27. Oktober 1999, welche darauf abzielen, die rechtliche Wirksamkeit der elektronischen Signaturen und ihre Zulässigkeit als Beweismittel im Gerichtsverfahren zu fixieren. Dem Europäischen Parlament folgend, unterliegt die Festlegung der Rechtsgebiete, in welchen elektronische Dokumente und elektronische Signaturen verwendet werden dürfen, weiterhin einzelstaatlichem Recht. Angesichts der Entwicklung des internationalen elektronischen Geschäftsverkehrs wird zur Sicherstellung der Interoperabilität auf globaler Ebene die Nützlichkeit von Vereinbarungen mit Drittländern über die gegenseitige Anerkennung hervorgehoben. Am 30. November 1999 wurde der Vorschlag schließlich durch den Rat angenommen. Die Veröffentlichung im Amtsblatt der Europäischen Gemeinschaften und damit auch das Inkrafttreten erfolgte schlussendlich am 19. Januar 2000. Die Mitgliedstaaten haben für die nationale Umsetzung der „Rahmenrichtlinie zur elektronischen Signatur“ innerhalb von 18 Monaten, d.h. bis Juli 2001, zu sorgen.

5.2 Grundsätze der Richtlinie

Da die Entwicklung einer Vielzahl von unterschiedlichen Authentifizierungsverfahren zu erwarten ist, wählte man bei der Richtlinie einen technologieneutralen Ansatz. Dies soll garantieren, dass die Richtlinie nicht nur auf die zur Zeit sicherste Art der elektronischen

---

[44] Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen, Brüssel, den 29.4.1999, KOM (1999) 195 endg.

[45] Gemeinsamer Standpunkt EG) Nr. 28/1999 vom Rat festgelegt am 28. Juni 1999 im Hinblick auf den Erlaß der Richtlinie 1999/.../EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. C 243 vom 27.8.1999

Signierung, nämlich die Verschlüsselungstechnik der digitalen Signierung, anwendbar ist und andere Authentifizierungsverfahren ebenso abdeckt.
Die Richtlinie legt die Kriterien fest, die als Grundlage für die rechtliche Anerkennung elektronischer Signaturen dienen. Ein Schwerpunkt dabei liegt auf den Zertifizierungsdiensten und ihren Anbietern.

Zentraler Regelungsbereich ist die Fixierung gemeinsamer:

- Anforderungen an Zertifizierungsdiensteanbieter, um die grenzüberschreitende Anwendbarkeit und Anerkennung von Signaturen und Zertifikaten sicherzustellen;
- Haftungsbestimmungen, um einerseits das Vertrauen der Nutzer in die neue Technologie zu stärken und andererseits das wirtschaftliche Risiko der Diensteanbieter kalkulierbar zu machen und
- Verfahren der Zusammenarbeit, um auch die Interoperabilität von Signaturen und Zertifikaten in Drittländern außerhalb der Europäischen Gemeinschaft zu erleichtern.

5.3 Art 1 - Anwendungsbereich

Artikel 1 legt Geltungsbereich und Zielrichtung der Richtlinie fest. Um die rechtliche Anerkennung elektronischer Signaturen zu erreichen, werden bestimmte Mindestanforderungen an Diensteanbieter und Zertifikate gestellt. *„Rechtliche Anerkennung in diesem Zusammenhang bedeutet, dass elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen, das von einem den in Anhang II niedergelegten Anforderungen genügenden Zertifizierungsdiensteanbieter ausgestellt wurde, zur Erfüllung des rechtlichen Erfordernisses einer handschriftlichen Unterschrift anerkannt werden und in Gerichtsverfahren in gleicher Weise wie handschriftliche Unterschriften*

als Beweismittel zugelassen sind.“[46] Durch die Richtlinie soll jedoch weder in nationale Regelungen betreffend Abschluss, Erfüllung, Form und Geltung von Verträgen noch in einzelstaatliche außervertragliche Formvorschriften, die eine eigenhändige Unterschrift voraussetzen, eingegriffen werden. Dementsprechend *„werden weder Aspekte im Zusammenhang mit dem Abschluss und der Gültigkeit von Verträgen oder anderen rechtlichen Verpflichtungen, für die nach einzelstaatlichem Recht oder Gemeinschaftsrecht Formvorschriften zu erfüllen sind, erfasst, noch werden im einzelstaatlichem Recht oder im Gemeinschaftsrecht vorgesehene Regeln und Beschränkungen für die Verwendung von Dokumenten berührt.“*[47]

Die auf freiwilliger privatrechtlicher Vereinbarung lediglich zwischen einer bestimmten Anzahl von Teilnehmern beruhenden Systeme, die sogenannten „geschlossenen Systeme“, fallen nicht unter den Anwendungsbereich der Richtlinie. Nach dem Grundsatz der Privatautonomie ist es auch hier möglich, die rechtliche Anerkennung elektronischer Signaturen zu vereinbaren. In Einschränkung der Willensfreiheit der Rechtssubjekte wird weiters jedoch zumindest nahegelegt, auch in diesem Bereich die rechtliche Wirksamkeit und Zulässigkeit elektronisch signierter Dokumente als Beweismittel anzuerkennen.

5.4 Art 2 - Begriffsbestimmungen

5.4.1 „Elektronische Signatur“

[46] Siehe die Begründung des Geänderten Vorschlages für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen, Brüssel, den 29.4..1999, KOM (1999) 195 endg., S. 5

[47] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Abl L 13/12 vom 19.1.2000, Art. 1

Artikel 2 der Richtlinie enthält eine Reihe von Definitionen relevanter und für das Verständnis des Regelungsbereiches der Richtlinie wichtiger Begriffe. Zuallererst wird durch Ziffer 1 festgelegt, was unter dem Konstrukt der „elektronischen Signaturen" zu verstehen ist. Diese werden definiert als *„Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen"*[48]. Vielleicht etwas vereinfacht ausgedrückt, ist die elektronische Signierung ein technisches Verfahren, im Zuge dessen die eindeutige Zuordnung elektronischer Daten zum Signierenden sichergestellt werden soll.

Die derzeit vorherrschende Form der elektronischen Signierung ist die digitale. Eine digitale Signatur ist eine elektronische Signatur, die mit Hilfe von Verfahren der asymmetrischen Kryptographie erstellt wird. Dabei wird durch ein spezielles mathematisches Verfahren der sogenannte Hashwert ermittelt und verschlüsselt. Unter dem Begriff des „Hashwertes" ist eine Datenkombination, eine Art Prüfsumme zu verstehen, welche vergleichbar einem Fingerabdruck für einen bestimmten Dokumenteninhalt repräsentativ ist. Die Verschlüsselung des elektronischen Fingerabdruckes erfolgt durch den privaten Schlüssel, d.h. die komprimierten Daten werden dabei unlesbar gemacht. Der Dokumenteninhalt bleibt dabei lesbar, er wird idR nicht auch verschlüsselt. Der private Schlüssel ist absolut geheim zu halten und nicht einmal dem Besitzer selbst bekannt. Eine Speicherung des privaten Schlüssels ist außer beim Signator selbst absolut unzulässig. Er kann etwa auf einer Chipkarte abgespeichert werden, welche dann, wie bei der Kredit- oder Bankomatkarte auch, sorgsam zu verwahren ist.

Mit Hilfe mathematischer Verfahren wird aus dem privaten Schlüssel der dazupassende öffentliche Schlüssel abgeleitet. Eine Rückberechnung muss jedoch mit hoher Wahrscheinlichkeit ausgeschlossen sein, d.h. der private Schlüssel darf umgekehrt aus dem öffentlichen nicht ableitbar sein. Der einzig zum privaten Signaturschlüssel dazupassende

[48] SigRl Abl L 13/12 vom 19.1.2000, Art 2 Z 1

komplementäre öffentliche Schlüssel ist frei zugänglich zu machen und dient zur Entschlüsselung der durch den privaten Schlüssel verschlüsselten Daten. Im
Rahmen dieser Entchiffrierung wird die Signatur durch den dem Dokument angehängten oder sonst frei zugänglich gemachten öffentlichen Schlüssel entschlüsselt und dabei eine bestimmte Prüfsumme ermittelt. Gleichzeitig wird der Hashwert des übermittelten Dokuments errechnet. Entspricht nun diese Prüfsumme der mitübermittelten, welche mit dem privaten Schlüssel verschlüsselt wurde und nun wieder in entschlüssselter Form vorliegt, sind also beide Hashwerte ident, so ist nachgewiesen, dass die Nachricht nicht verändert wurde.

5.4.2 „Zertifikat"

Die Zuordnung des Schlüssels zu einer bestimmten Person erfolgt durch ein Zertifikat, eine Art elektronischer Ausweis, welcher die eindeutige und zuverlässige Identifizierung des Signators ermöglicht. Die Definition laut Richtlinie lautet: *„Eine elektronische Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und die Identität dieser Person bestätigt wird"*[49]. Die Richtlinie enthält keine Bestimmung, welche die Ausstellung von Zertifikaten auf natürliche oder juristische Personen beschränken würde. Derartige Feststellungen fallen in einzelstaatliche Kompetenz, auch im Hinblick darauf, dass die unterschiedlichen nationalen Vorschriften auf dem Gebiet des Zivilrechts und im Umfeld des Stellvertretungsrechts sehr stark voneinander abweichen und dementsprechend einer gesonderten Regelung bedürfen.

Das Zertifikat wird von einer unabhängigen dritten Stelle, genannt Zertifizierungsdiensteanbieter, „Trusted Third Party" oder „Trust Center", ausgestellt und enthält Angaben zum Signator selbst, den ihm alleinig zugeordneten öffentlichen Schlüssel, den konkreten Anwendungsbereich, uvm. Dieses elektronische Formular wird dem Dokument angehängt oder sonst in einem Verzeichnis abrufbar gemacht. Auch das Anwender-Zertifikat

[49] SigRl Abl L 13/12 vom 19.1.2000, Art 2 Z 9

selbst wird mit einer sicheren Signatur des Diensteanbieters versehen und gilt somit ebenso als fälschungssicher.

Bei den Zertifikaten gibt es solche verschiedener Sicherheitsstufen, je nachdem welchen Aufwand man damit zu tätigen beabsichtigt. So gibt es etwa Zertifikate, die per e-Mail verschickt werden, solche, bei denen die Identität über eine per Fax geschickte Kopie des Personalausweises überprüft wird und solche, die nur nach persönlicher Vorsprache beim jeweiligen Aussteller erhältlich sind. Die Bestimmungen der Richtlinie selbst unterscheiden zwischen einfachen und qualifizierten Zertifikaten. Zweitgenannte sind dabei jene, die *„die Anforderungen des Anhangs I erfüllen und von einem Zertifizierungsdiensteanbieter bereitgestellt werden, der die Anforderungen des Anhangs II erfüllt“*[50]. Für die Erzeugung des Schlüsselpaares und des Zertifikates verrechnet die Zertifizierungsstelle dem jeweiligen Inhaber ein bestimmtes Entgelt, dessen Höhe von Qualität und Sicherheit des Produktes abhängt.

Abschließend kann also gesagt werden: „**Die elektronische Signatur bestätigt, dass die Daten vom Inhaber des privaten Signaturschlüssels stammen und auch nicht verändert wurden, das Zertifikat wiederum bestätigt, dass der Inhaber des privaten Signaturschlüssels tatsächlich derjenige ist, welcher bei der Prüfung als Inhaber aufscheint.“**[51]

5.4.3 Signaturerstellungs- und Signaturprüfeinheit

Unter einer *„Signaturerstellungseinheit“* ist der oftmals erwähnte private Schüssel zu verstehen, der vom Unterzeichner zur Erstellung der elektronischen Signatur verwendet wird

[50] SigRl, Abl L 13/12 vom 19.1.2000, Art 2 Z 10

[51] *Stockinger*, Österreichis ches Signaturgesetz: Bedeutung, Funktion und Rechtsfolgen elektronischer Signaturen, in MR 4/1999, S. 206

und unter allen Umständen geheim zu halten ist. Als Signaturerstellungseinheit kommen aber nicht nur private Schlüssel in Betracht, sondern auch irgendwelche Codes oder einmalig konfigurierte physische Werkzeuge.

Gewissermaßen das komplementäre Gegenstück dazu ist die *„Signaturprüfeinheit"*, auch öffentlicher Schlüssel genannt. Dieser öffentlich zugängliche Datenkomplex dient zur Überprüfung der elektronischen Signatur durch den Empfänger.

5.5 Art 3 - Marktzugang und Zulassungsfreiheit

Artikel 3 legt den freien Marktzugang für die Zertifikate ausstellenden Zertifizierungsdiensteanbieter fest. Ihre Hauptaufgabe besteht im Bestätigen der Zuordnung eines Zertifikats zu einer bestimmten natürlichen oder juristischen Person. Der Richtlinie folgend hat die Bereitstellung von Zertifizierungsdiensten nicht von einer vorherigen Genehmigung durch eine öffentliche oder private Stelle abhängig zu sein. Ebenso untersagt sind in ihrer Wirkung einer Genehmigungspflicht gleichkommende Maßnahmen, wie etwa eine Vorlagepflicht mit Wartezeit oder eine verpflichtende Registrierung.

Dies schließt jedoch nicht die Einführung bzw. Beibehaltung freiwilliger Akkreditierungssysteme auf Ebene der Mitgliedstaaten aus, welche auf höherwertige Zertifizierungsdienste abzielen und den jeweiligen Anbietern besondere Rechte einräumen, wie etwa die Befugnis, sich im Geschäftsverkehr als akkreditierte Zertifizierungsdiensteanbieter zu bezeichnen. Im Rahmen einer Akkreditierung wird durch eine dafür zuständige und kompetente Stelle bereits im vorhinein die Einhaltung der Anforderungen der Richtlinie explizit bescheinigt. Die mit den Akkreditierungssystemen verknüpften Anforderungen müssen den Grundsätzen von Objektivität, Transparenz, Verhältnismäßigkeit und Nichtdiskriminierung entsprechen. Die freiwillige Akkreditierung stellt laut Art 2 Ziffer 13 eine individuell erteilte Erlaubnis dar, d.h. einen auf Antrag des jeweiligen Zertifizierungsdiensteanbieters von einer

öffentlichen oder privaten Stelle ausgestellten konstitutiven Bescheid, welcher Rechte und Pflichten eines Anbieters von Zertifizierungsdiensten festlegt.

5.5.1 Aufsicht und Kontrolle

Abs. 3 des betreffenden Artikels verpflichtet die Mitgliedstaaten zur Schaffung geeigneter Infrastruktur zum Zwecke ordnungsgemäßer Kontrolle und Überwachung der in ihrem Hoheitsgebiet niedergelassenen Zertifizierungsstellen. Im Rahmen eines derartigen Aufsichtssystems sind Notifizierungs- und Registrierungsstellen einzurichten, welchen besondere Befugnisse zur regelmäßigen Kontrolle der Diensteanbieter eingeräumt werden. Gemäß Abs. 4 ist ebenso für die Prüfung der Übereinstimmung sicherer Signaturerstellungseinheiten mit Anhang III der Richtlinie Sorge zu tragen. Die darin gestellten Anforderungen werden zuvor von der Kommission in Zusammenarbeit mit den Mitgliedstaaten ausgearbeitet.

5.5.2 Normung

Die Richtlinie selbst enthält keine detaillierten Angaben bezüglich der Normung von Sicherheitsanforderungen, Signaturprodukten und -verfahren. In Ansätzen sind diese in den Anhängen I bis IV zu finden. Abs. 5 des in Rede stehenden Artikels eröffnet der Kommission die Möglichkeit der Festlegung von Referenznummern für allgemein anerkannte Normen für Signaturprodukte, welche sodann im Amtsblatt zu veröffentlichen sind. Aufgrund des offensichtlich bestehenden Regelungsbedarfes sind die nationalen Normungsgremien dazu aufgerufen, entsprechende Handlungen zu setzen. Derzeit läuft die Initiative „European Electronic Signature Standardization Initiative (EESSI), koordiniert vom „Telecommunications Standards Institute (ETSI)“.[52] Im Vordergrund ihrer Bemühungen steht die Erarbeitung

[52] Siehe dazu ausführlich http://www.ict.etsi.org(/activietiers/eesi/eessi.thm).

qualitativer Kriterien, interoperabler technischer Normen, technologiespezifischer Mechanismen, udgl.[53]

5.5.3 Verhältnis Richtlinie und nationales Recht

Weiters legt die Richtlinie bloße Mindestanforderungen fest. Diese Tatsache schließt Art 3 Abs. 7 folgend nicht aus, dass einzelne Mitgliedstaaten elektronische Signaturen im öffentlichen Bereich höheren Anforderungen unterstellen, wobei die im Rahmen der Akkreditierung dargelegten Grundsätze Beachtung zu finden haben. Auf keinen Fall dürfen die Bürger der Europäischen Gemeinschaft dadurch an der Inanspruchnahme grenzüberschreitender Dienste gehindert oder beschränkt werden.

Die Mitgliedstaaten verpflichten sich, Bestimmungen in Übereinstimmung mit den Vorgaben und Mindestanforderungen der Richtlinie zu erlassen. Diese sind auf die in ihren Hoheitsgebieten niedergelassenen Zertifizierungsdiensteanbieter und deren Dienste anzuwenden. Die Bereitstellung von Zertifizierungsdiensten durch Diensteanbieter aus anderen Mitgliedstaaten darf in den unter die Richtlinie fallenden Bereichen nicht eingeschränkt werden.

5.6 Art 4 - Binnenmarktgrundsätze

Artikel 4 hebt die Allgemeingültigkeit der Richtlinienbestimmungen und die zwingende Berücksichtigung der Binnenmarktgrundsätze hervor. Eine der Zielrichtungen der Richtlinie über elektronische Signaturen ist die grenzüberschreitende, gegenseitige Anerkennung von Signaturen, Zertifikaten und ihren Rechtswirkungen sowohl zwischen den Mitgliedstaaten der EU als auch im Verhältnis zu außerhalb der EU stehenden Drittländern. Insbesondere darf im Sinne der Dienstleistungs- wie auch der Niederlassungsfreiheit die Tätigkeit von ausländischen

---

[53] *Gravesen/ Dumortier/ Van Eecke*, Die europäische Signaturrichtlinie - Regulative Funktion und Bedeutung der Rechtswirkung, MMR 1999, S. 584f

Anbietern nicht eingeschränkt werden; die internationale Anerkennung elektronischer Signaturen ist voll zu gewährleisten. Andererseits ist aber auch jede Art von Inländerdiskriminierung verboten.

Für den Fall einer Ungleichbehandlung kann sich jeder EU-Bürger direkt auf die gegenständlichen Bestimmungen des EG-Vertrages und dessen unmittelbare Anwendbarkeit berufen. Wie dies auch in anderen Bereichen der Fall ist, sind Einschränkungen unter Berücksichtigung des Gebotes der Verhältnismäßigkeit und des Allgemeinwohles möglich und rechtlich zulässig.[54]

5.7 Art 5 - Rechtswirkung elektronischer Signaturen

5.7.1 Art 5 Abs. 2 - Nichtdiskriminierung

In Artikel 5 ist als Kernstück der Richtlinie die rechtliche Wirkung elektronischer Signaturen geregelt. Der Grundsatz der Nichtdiskriminierung in Art 5 Abs. 2 besagt, *„dass einer elektronischen Signatur die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen wird, weil sie in elektronischer Form vorliegt oder nicht auf einem qualifizierten Zertifikat beruht oder nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder nicht von einer sicheren Signaturerstellungseinheit erstellt wurde“*[55]. D.h., vereinfacht gesagt dürfen einfache elektronische Signaturen[56] im geschäftlichen Verkehr weder rechtlich diskriminiert noch verboten werden. Es wird ihnen unmittelbar kraft Gesetzes rechtliche Existenz zuerkannt. Dieser Grundsatz gilt für alle

[54] Siehe dazu ausführlich im Österreichischen Anwaltsblatt, AnwBl 8/2000, S. 481ff.

[55] SigRl, Abl L 13/12 vom 19.1.2000, Art 5 Abs 2

[56] Der Begriff der „einfachen elektronischen Signatur“ wird weder in der SigRl noch der E-Commerce-Rl noch im österreichischen Signaturgesetz verwendet. Dieser Terminus dient lediglich als Vereinfachung der Abgrenzung zur „qualifizierten“ bzw. „fortgeschrittenen elektronischen Signatur“.

elektronische Signaturen, also auch solche, die nicht auf einem Zertifikat beruhen oder den Anforderungen der Richtlinie nicht entsprechen. Derartige einfache Signaturen genießen zwar nicht dieselben Rechtswirkungen einer konventionellen Unterschrift, die gerichtliche oder behördliche Anerkennung kann ihnen aber lediglich nach entsprechender Überprüfung bei nachgewiesener mangelnder Sicherheit verweigert werden. Vor Gericht gilt weiterhin das Prinzip der freien Beweiswürdigung. Dementsprechend bleibt die richterliche Kompetenz erhalten, die Einhaltung der Anforderungen der Richtlinie, die Vertrauenswürdigkeit der verwendeten Technologie, die Umstände des Einzelfalls, udgl. je nach den Umständen des Einzelfalls zu bewerten und infolgedessen die Zulässigkeit als Beweismittel anzuerkennen bzw. im entgegengesetzten Fall abzusprechen.

5.7.2 Art 5 Abs. 1 - Gleichsetzung

Zusätzlich ist in Art 5 Abs. 1 die rechtliche Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift normiert. Mit dieser sind besonders die Identitäts-, Abschluss-, Beweis-, Warn- und Gläubigerschutzfunktion verbunden. In Bezug auf eine elektronische Signatur können diese Funktionen nur bei einem relativ hohen Sicherheitsstandard als erfüllt angesehen werden. Diesem Erfordernis wird bei Einhaltung der Anhänge I bis IV grundsätzlich entsprochen. Eine derartige Signatur muss eindeutig zuordenbar sein, sie muss sowohl die volle Echtheit, d.h. die Authentizität der Daten, als auch die volle Unverfälschtheit, d.h. die Integrität der Daten, gewährleisten. Die Warnfunktion dient dazu, den Erklärenden über die Risiken des Geschäftes besonders aufzuklären und vor übereilter Bindung zu schützen. Die Beweisfunktion wiederum dient dem Nachweis von Bestand und konkreter Ausgestaltung des Rechtsgeschäftes.

Die besonderen Form- und Beweiswirkungen der Signaturrichtlinie treten nur bei den besonders sicheren, den sogenannten „fortgeschrittenen elektronischen Signaturen“ ein. Demnach haben die Mitgliedstaaten sicherzustellen, dass elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen, welches von einem Zertifizierungsdiensteanbieter erteilt

wurde, der den Anforderungen der Richtlinie genügt, zur Erfüllung des rechtlichen Erfordernisses einer handschriftlichen Unterschrift anerkannt werden und in Gerichtsverfahren in gleicher Weise wie handschriftliche
Unterschriften als Beweismittel zugelassen sind. Die rechtliche Anerkennung fortgeschrittener elektronischer Signaturen ist dementsprechend geknüpft an die Erfüllung sämtlicher normierter Anforderungen an Zertifikate, dargestellt in Anhang I der Richtlinie, an Zertifizierungsdiensteanbieter[57], dargestellt in Anhang II, und an Signaturprodukte entsprechend Anhang III.

5.7.3 Nationale Umsetzung

Das Prinzip der Nichtdiskriminierung wirft in den Mitgliedstaaten der Europäischen Gemeinschaft keine Probleme auf, da dieses nur die grundsätzliche Zulässigkeit von Signaturen im Rechts- und Geschäftsverkehr vorsieht. Dadurch nicht berührt wird nationales Vertragsrecht, ebensowenig wie nationales Beweisrecht. Auch hier verlangt die Richtlinie lediglich die gleiche Zulässigkeit als Beweismittel, nicht aber eine qualifizierte Beweiswirkung. Die Festlegung, in welchen Bereichen die „elektronische Form" zulässig sein soll, verbleibt weiterhin im Rahmen einzelstaatlicher Autonomie. Hat man sich jedoch für die Anwendbarkeit der elektronischen Signatur entschieden, so ist die rechtliche Gleichstellung mit der eigenhändigen Unterschrift in diesem eingeschränkten Bereich eu-rechtlich zwingend vorgeschrieben. Elektronisch signierten Dokumenten darf demzufolge von nationalen Gerichten und Behörden nicht die rechtliche Beachtlichkeit abgesprochen werden, mit der alleinigen Begründung, dass sie „nur" in elektronischer Form vorliegen.

[57] *Fallenböck/ Schwab*, Zu der Charakteristik und den Rechtswirkungen elektronischer Signaturen: Regelungsmodelle in den USA und Europa, in MR 6/1999, S. 374

Die relativ große Entscheidungsfreiheit der Mitgliedstaaten muss in Zusammenhang mit Art 9 der Richtlinie über den elektronischen Geschäftsverkehr[58] gesehen werden, welcher folgendes normiert: *„Die Mitgliedstaaten stellen sicher, dass ihr Rechtssystem den Abschluss von Verträgen auf elektronischem Wege ermöglicht. Die Mitgliedstaaten stellen insbesondere sicher, dass ihre für den Vertragsabschluß geltenden Rechtsvorschriften weder Hindernisse für die Verwendung elektronischer Verträge bilden noch dazu führen, dass diese Verträge aufgrund des Umstandes, dass sie auf elektronischem Wege zustandegekommen sind, keine rechtliche Wirksamkeit oder Gültigkeit haben."* Nähere Ausführungen dazu unter Kapitel 6.6 und 6.8.

5.8 Art 6 - Haftung der Zertifizierungsstellen

Erwägungsgrund 22 der Europäischen Richtlinie folgend finden die nationalen Haftungsbestimmungen auf die ihre Dienste öffentlich anbietenden Diensteanbieter weiterhin Anwendung. Die Mitgliedstaaten können in Übereinstimmung mit der Richtlinie strengere Haftungsvorschriften beibehalten bzw. einführen, da diese bloße Mindeststandards vorschreibt.

Artikel 6 der Richtlinie orientiert sich an Verschuldensgrundsatz, Umkehr der Beweislast und Mindesthaftung. Zertifizierungsdiensteanbieter sind bei Aufnahme bzw. Führung ihres Zertifizierungsbetriebes keinen besonders hohen Hürden ausgesetzt, es besteht ein allgemeines Verbot der Genehmigungs- und Zulassungspflicht. Diese Tatsache wird durch relativ strenge, die Diensteanbieter treffende Haftungsregelungen ausgeglichen, denn nur so kann nach Auffassung der Kommission die Sicherheit des elektronischen Geschäftsverkehrs gewahrt werden. Siehe zur gegenteiligen Auffassung, zum Ausdruck gebracht im deutschen Signaturgesetz, dargestellt in Kapitel 8.4.4.

[58] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen

Der Richtlinie entsprechend hat ein, ein qualifiziertes Zertifikat ausstellender Diensteanbieter einzustehen gegenüber jeder Person, die vernünftigerweise auf das Zertifikat vertraut, dafür, dass

- alle darin enthaltenen Informationen zum Zeitpunkt seiner Ausstellung der Wirklichkeit entsprechen;
- alle Anforderungen der Richtlinie bei der Ausstellung des qualifizierten Zertifikats erfüllt wurden, d.h. etwa erforderliche Angaben enthalten sind;
- die im qualifizierten Zertifikat angegebene Person zum Zeitpunkt der Ausstellung im Besitz der Signaturerstellungsdaten ist, die den im Zertifikat angegebenen Signaturprüfdaten entsprechen;
- die von einem Zertifizierungsdiensteanbieter erstellten Signaturerstellungsdaten wie auch die Signaturprüfdaten in komplementärer Weise funktionieren.

Weiters haftet ein Zertifizierungsdiensteanbieter gemäß Abs. 2 für die unverzügliche Registrierung des Widerrufs eines qualifizierten Zertifikats.

Wie bereits eingangs erwähnt, besteht die Haftungspflicht gegenüber all jenen Personen, *„die vernünftigerweise auf das Zertifikat vertrauen“*. Dieser Terminus bedarf einer Konkretisierung. Etwas vereinfacht gesagt, sollen dadurch die Fälle ausgeschlossen werden, in denen etwa die Unrichtigkeit von in einem Zertifikat enthaltenen Angaben ganz offensichtlich, ja geradezu augenscheinlich ist. Ist die Falschheit für einen durchschnittlichen Nutzer sofort erkennbar, so soll die Haftung nach der SigRl grundsätzlich ausgeschlossen sein. In diesen Fällen wäre es völlig ungerechtfertigt, die Zertifizierungsdiensteanbieter mit relativ strengen Haftungsbestimmungen zu belasten.

Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“), Abl. L 178 vom 17.7.2000

Durch die Einschränkung der Anwendbarkeit des jeweiligen Zertifikates auf eine bestimmte Maximalsumme der jeweiligen Transaktion oder auf bestimmte Arten von Rechtsgeschäften kann die Haftung der Zertifizierungsdiensteanbieter minimiert oder zumindest kalkulierbar gemacht werden. Unter der Voraussetzung, dass die jeweiligen Beschränkungen für Dritte erkennbar sind, d.h. im Zertifikat ausdrücklich angeführt sind, ist für über diese Bereiche hinausgehende Tätigkeiten keine Einstandspflicht vorgesehen. Dies schließt jedoch nicht eine Haftung außerhalb der SigRl nach einzelstaatlichen Normen aus, etwa im Bereich des EKHG. Hier können unter Zuhilfenahme des
allgemeinen Schadenersatzrechtes des ABGB über die Haftungshöchstgrenze bzw. den konkreten Anwendungsbereich hinausgehende Schäden eingefordert werden.

Der Zertifizierungsdiensteanbieter kann sich zudem durch die Erbringung des Beweises, dass er bzw. die für ihn handelnden Personen weder fahrlässig gehandelt haben noch ihr Handeln kausal für den eingetretenen Schaden war, von einer etwaigen Haftungspflicht befreien. Den dargelegten Grundsätzen entsprechend hat er ebensowenig einzustehen für nicht der Realität entsprechende Angaben in einem qualifizierten Zertifikat, soweit diese auf Informationen des Zertifikatwerbers beruhen und der Diensteanbieter den Nachweis gehöriger Überprüfung[59] erbringt. Die Richtlinie normiert dementsprechend eine Verschuldenshaftung mit Beweislastumkehr zu Lasten des Zertifizierungsdiensteanbieters.

In den, meist bis in alle Einzelheiten detailliert geregelten, Vertragsbeziehungen zwischen Zertifikatsausstellern und -inhabern bestehen zudem oftmals besondere Regelungen, welche die Haftung im Rahmen dispositiven Schadenersatzrechtes zwischen ebendiesen genauestens regeln. Etwaige Ansprüche stützen sich hier vorrangig auf Vertragshaftung und allgemeiner Verschuldenshaftung.

[59] Welche Maßstäbe konkret im Hinblick auf diese Sorgfaltspflichten zu gelten haben, ist indes nicht weiter bestimmt.

5.9 Art 7 - Internationale Aspekte

In Artikel 7 wird die internationale Gültigkeit und gegenseitige Anerkennung von elektronischen Signaturen und Zertifikaten bekräftigt, um dem grenzüberschreitenden Charakter des elektronischen Geschäftsverkehrs Rechnung zu tragen. Qualifizierte Zertifikate innerhalb der Europäischen Union müssen ohne weitere rechtliche Voraussetzungen anerkannt, d.h. in allen Belangen rechtlich gleichgestellt werden. Die von einem Nicht-EU-Mitgliedstaat ausgestellten qualifizierten Zertifikate sind denen eines EU-Mitgliedstaates gleichwertig, soweit der jeweilige Diensteanbieter die Richtlinie
einhält und in einem Mitgliedstaat freiwillig akkreditiert ist. Alternativ dazu gilt ein ausländisches Zertifikat ebenso als rechtlich gleichwertig, soweit ein in einem Mitgliedstaat niedergelassener Anbieter, welcher wiederum den Anforderungen der Richtlinie zu genügen hat, für das ausländische Zertifikat haftet. Als letzte Variante gilt es, den Abschluss von bi- bzw. multilateralen Vereinbarungen betreffend die gegenseitige Anerkennung von Zertifikaten zu nennen.

5.10 Art 8 - Datenschutz

Um das Vertrauen der Nutzer in die neuen Technologien weiter zu stärken, haben die Mitgliedstaaten gemäß Art 8 dafür Sorge zu tragen, dass Zertifizierungsdiensteanbieter und die für Akkreditierung und Aufsicht zuständigen nationalen Stellen die nationalen Vorschriften betreffend Datenschutz und Schutz der Privatsphäre zur Umsetzung der Richtlinie 95/46/EG[60] einhalten.

[60] Rl 95/46 des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie), Abl. L 281 v. 23.11.1995

Entsprechend den in dieser Richtlinie festgelegten datenschutzrechtlichen Vorgaben[61] sind personenbezogene Daten nur unmittelbar vom Betroffenen zu ermitteln bzw. nur mit dessem Wissen weiterzugeben. Wie bereits erwähnt, ist die Erstellung eines Zertifikats unter Verwendung eines Pseudonyms zu ermöglichen. Die Aufdeckung desselben hat sich nach innerstaatlichen Rechtsvorschriften zu richten. Die Zulässigkeit der Einholung personenbezogener Daten seitens der Zertifizierungsdiensteanbieter ist nur insoweit gegeben, als dies für Zertifikatserstellung und -verwaltung vonnöten ist.

5.11 Art 9 und 10 - Ausschuss

Die Kommission wird von einem beratenden Ausschuss unterstützt, dem „Ausschuss für elektronische Signaturen". Dieser hat unter anderem Stellungnahmen zu den von der Kommission getroffenen Maßnahmen abzugeben. Tritt dabei ein Widerspruch von Maßnahme und Stellungnahme zutage, so ist ihre Durchführung um drei Monate zu verschieben. Dem Rat wird zusätzlich die Möglichkeit eingeräumt, während desselben Zeitraumes mit qualifizierter Mehrheit einen anderslautenden Beschluss zu fassen.

5.12 Art 11 - Notifizierung

Die Mitgliedstaaten haben der Kommission ehestmöglich folgende Informationen zu übermitteln:

- Angaben zu freiwilligen nationalen Akkreditierungssystemen einschließlich zusätzlicher Anforderungen beim Einsatz elektronischer Signaturen im öffentlichen Bereich

[61] Art 7 der Datenschutzrichtlinie

- Name und Anschrift der für Akkreditierung und Aufsicht zuständigen nationalen sowie der in Art 3 Abs. 4 genannten Stellen[62]
- Name und Anschrift der akkreditierten nationalen Zertifizierungsdiensteanbieter

5.13 Anhang I - Anforderungen an qualifizierte Zertifikate

Anhang I der Richtlinie fixiert die von qualifizierten Zertifikaten zu erfüllenden Mindestanforderungen. Diese haben eine Bezeichnung des ausstellenden Diensteanbieters, den unverwechselbaren Namen bzw. ein Pseudonym des Zertifikatinhabers, einen Beisatz, der die eindeutige Identifizierung des Inhabers
sicherstellen soll, wie etwa Adresse, Vollmacht, Steuernummer oder ähnliches, den zum privaten Schlüssel komplementären öffentlichen Schlüssel, die Angabe der Laufzeit des Zertifikats, einen eindeutigen Identitätscode des Zertifikats, die elektronische Signatur des Diensteanbieters, die Gültigkeitsdauer des Zertifikats und vor allem auch etwaige Haftungsbeschränkungen zu enthalten. Zudem ist ein qualifiziertes Zertifikat von einem Zertifizierungsdiensteanbieter bereitzustellen, der den Anforderungen des Anhanges II voll zu entsprechen hat.

5.14 Anhang II - Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen

Anhang II legt die Mindestanforderungen an Zertifizierungsdiensteanbieter fest, die qualifizierte Zertifikate ausstellen. Diese müssen die geeignete Hard- und Software besitzen und vor allem auch geschultes Personal, um die geforderte Zuverlässigkeit und Sicherheit überhaupt gewährleisten zu können. Weiters trifft sie gegenüber den Zertifikats-Inhabern die

[62] Angesprochen sind hier die Bestätigungsstellen, in Ö die A-Sit.

Verpflichtung zu ausführlicher Information über die Bedingungen für die Verwendung des Zertifikats, die haftungsrechtlichen Aspekte und über im Falle eines Rechtsstreites zu beschreitende gerichtliche oder verwaltungsbehördliche Verfahrenswege. Neben diesen Vorgaben bei der Ausstellung richtliniengetreuer qualifizierter Zertifikate ist in lit. h die Verfügbarkeit über ein haftungsdeckendes Grundkapital als Voraussetzung für die rechtlich zulässige Bereitstellung ihrer Zertifizierungsdienste ausdrücklich genannt.

5.15 Anhang III - Anforderungen an sichere Signaturerstellungseinheiten

Im daran anschließenden Anhang III sind die Anforderungen an sichere Signaturerstellungseinheiten aufgelistet. Unter Signaturerstellungseinheit ist laut Definition in Art 2 Z *5 „eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturerstellungsdaten verwendet wird“* zu verstehen. Damit eine derartige Einheit als „sicher“ bewertet wird, ist zum einen die Einmaligkeit des bei
der Signaturgenerierung zur Anwendung gelangenden privaten Schlüssels, dessen Geheimhaltung und ausschließliche Nutzung durch den alleinig Berechtigten zu gewährleisten. Zum anderen muss die Signatur nach dem jeweiligen Stand der Technik als vor Fälschung und Verfälschung bzw. Ableitbarkeit aus dem dazupassenden öffentlichen Schlüssel sicher eingestuft werden. Die Daten dürfen durch den Signierungsvorgang nicht verändert werden. Es muss möglich sein, die zu signierenden Daten vor der Signierung für den Unterzeichner sichtbar zu machen, worunter man die sogenannte „Viewer-Funktion“ versteht. Für die Bewertung der Übereinstimmung von sicheren Signaturerstellungseinheiten mit den dargelegten Anforderungen sind geeignete Stellen zu benennen, die sogenannten Bestätigungsstellen nach Artikel 3 Abs 4 der Richtlinie.

5.16 Anhang IV - Empfehlungen für die sichere Signaturprüfung

Anhang IV der Richtlinie betreffend die Signaturprüfeinheiten, die sogenannten öffentlichen Schlüssel, hat lediglich empfehlenden Charakter. Im wesentlichen muss die Signaturprüfung

zuverlässig und korrekt, die Echtheit und Gültigkeit des Zertifikats überprüfbar, Prüfergebnis sowie Identitätsfeststellung richtig und eine Anzeige des Pseudonyms möglich sein.

5.17 Resümee

Trotz des sehr weitreichenden und umfassenden Regelungsbereiches der Richtlinie treten im elektronischen Rechts- und Geschäftsverkehr eine Reihe von Fragen bzw. Problemen auf, die noch einer Klärung bedürfen, so etwa auch die Frage der Zustellung im Internet. Zu welchem Zeitpunkt eine Nachricht etwa als zugestellt gilt, wird zwar teilweise in der Richtlinie zum Europäischen Geschäftsverkehr geklärt. Doch wer haftet im Einzelfall, wenn eine Nachricht aus technischen Gründen nicht zugestellt werden kann, z.B. im Falle eines Serverausfalls? Kann ein Billigprovider seine Haftung ausschließen? Wer haftet,
wenn eine Nachricht von einem Spam-Filter[63] oder Antivirenprogramm[64] vernichtet oder zumindest eine gewisse Zeit zurückgehalten wird? Wie ist beim Wechsel einer E-Mail-Adresse zu verfahren?
Eine ansatzweise Behandlung und Lösung dieser Fragen findet sich bereits in der E-Commerce-Richtlinie[65], jedoch vermag diese nicht eine allgemeingültige Antwort auf die in der Praxis sehr vielschichtigen Probleme zu geben. Eine solche kann sicherlich nicht von einem Tag auf den anderen allein durch legistische Maßnahmen gefunden werden. Vielmehr wird sie im Laufe der Zeit herausgearbeitet müssen, sich orientierend an den jeweiligen Bedürfnissen des

---

63 Unter „Spam“ wird unerwünschte Direktwerbung per Internet verstanden, oftmals auch als „Unsoliceted Commercial E-Mail (UCE)“, „Unsolicited Bulk E-Mail (UBE) oder „Junk Mail“ bezeichnet. Mit Hilfe von eigenen Anti-Spam-Programmen, sogenannten „Spam-Filtern“, wird die eingehende Post untersucht, klassifiziert und im gegebenen Fall gelöscht. Dabei kann es auch passieren, daß eine Nachricht als Spam eingeordnet wird, obwohl sie dies nicht ist.

64 Dies dienen dazu, um Viren zu erkennen und bereits erfolgten Schaden so weit als möglich wiedergutzumachen, d.h. etwa Daten wiederherzustellen. Bekannte Virenschutzprogramme sind etwa McAffee VirusScan, Ikarus Virus Utilities, etc. Viren wiederum sind ebenso Programme, deren Zweck je nach konkreter Ausgestaltung darin besteht, sich weiterzuverbreiten und andere Programme zu befallen. Siehe dazu genauer *Mader*, Technische Grundlagen und Grundbegriffe, in *Jahnel/Mader*: EDV für Juristen², Wien 1998, S. 42f

65 Siehe dazu ausführlicher in Kapitel 6.8.

Geschäftsverkehrs via Internet. Auch die Rechtsprechung wird ihren Beitrag durch die Anwendung allgemeiner Grundsätze leisten müssen, um z.B. etwa in beweisrechtlichen Belangen zu einer zufriedenstellenden Lösung finden zu können.

6 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt

In untrennbarem Zusammenhang mit der Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen steht die erst kürzlich nun in ihrer endgültigen Fassung vorliegende „Richtlinie über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt“[66], kurz als E-Commerce-Richtlinie bezeichnet. Wie bereits dargestellt behandelt erstere fast ausschließlich die rechtliche Wirksamkeit elektronischer Signaturen. Demgegenüber finden sich in der Richtlinie über den elektronischen Geschäftsverkehr davon verschiedene Regelungsbereiche, darunter auch die Fixierung der rechtlichen Wertigkeit von elektronischen Signaturen, welche die Signaturrichtlinie in gewissen Bereichen ergänzen. In vier Kapiteln werden fünf wichtige

[66] E-Commerce-Richtlinie, Abl. L 178 vom 17.7.2000

Themenbereiche in Online-Handel und -Kommunikation angesprochen. Diese setzen sich wie folgt zusammen:

- elektronische Dienstleistungsfreiheit
- elektronische Werbefreiheit
- elektronischer Vertragsabschluß
- Providerhaftung
- Rechtsdurchsetzung im elektronischen Markt Internet

6.1 Ausgangslage

Wie auch bei der Signaturrichtlinie wird in den Erwägungsgründen wiederholt festgestellt, dass divergierende nationale Regelungen zu einer Verunsicherung der Nutzer und infolgedessen zu mangelnder Inanspruchnahme neuer, marktwirtschaftlich vorteilhafter Geschäftspraktiken führen können. Schon aus diesem Grund ist ein Tätigwerden der gesetzgebenden Organe auf Gemeinschaftsebene erforderlich und unabdingbar. Für ein reibungsloses Funktionieren des Binnenmarktes sind in den unbedingt notwendigen Bereichen spezifische, harmonisierte Rechtsvorschriften einzuführen. Um die vollwertige Entwicklung des elektronischen Geschäftsverkehrs zu fördern und zu unterstützen, muss Rechtssicherheit auf Seiten von Unternehmen und Verbrauchern gleichermaßen geschaffen werden. Dabei nehmen öffentliche Belange, wie etwa Verbraucherschutz und Schutz der öffentlichen Gesundheit, eine zentrale Rolle ein.

6.2 Art 2 - Begriffsbestimmungen

6.2.1 „Dienste der Informationsgesellschaft"

Der Anwendungsbereich erstreckt sich auf alle *„Dienste der Informationsgesellschaft"*, worunter der Richtlinie entsprechend Dienstleistungen zu verstehen sind, *„die in der Regel gegen Entgelt im Fernabsatz mittels Geräten für die elektronische Verarbeitung und Speicherung von Daten auf individuellen Abruf eines Empfängers erbracht werden"*.[67] Der Begriff der *„Dienste"* orientiert sich dabei an Art 50 des EG-Vertrages (ex-Artikel 60)[68]. Unter *„im Fernabsatz erbrachte Dienstleistungen"* sind wiederum solche zu verstehen, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht werden. Ferner ist eine Dienstleistung „auf individuellen Abruf" erbracht, soweit sie auf individuelle Anforderung hin durch Übertragung von Daten geleistet wird. Fernseh- und Radioübertragungen sind schon allein aus diesem Grund nicht unter den Begriff der „Dienste der Informationsgesellschaft" zu subsumieren, da hier an eine unbeschränkte und unbestimmte Anzahl von Empfängern gesendet wird, welche idR keine Möglichkeit haben, die Übertragung zu unterbrechen, anzuhalten oder zu verändern. Es muss sich weiters um eine geldwerte Leistung mit gewerblichem Charakter handeln, was nicht zwangsläufig bedeuten muss, dass der Nutzer selbst dafür aufzukommen hat. Ebenso ausreichend ist die Finanzierung z.B. über Werbeeinnahmen oder Sponsoring. Auf elektronischem Wege erbracht ist eine Dienstleistung, wenn sowohl beim Sender wie auch beim Empfänger Daten elektronisch verarbeitet und gespeichert werden. Unter den Begriff der elektronisch erbrachten Dienstleistungen fallen online-Angebote über Waren und Dienstleistungen wie auch der online-Verkauf von Waren oder die online-Erbringung von Dienstleistungen. Hingegen nicht Dienste im „offline"-Bereich und solche, die ohne Verarbeitung und Speicherung von Daten in Echtzeit erbracht werden.

6.2.2 „Niederlassung"

---

[67] Erwägungsgrund 17 und Art 2 lit a E-Commerce-Rl

Eine wichtige Rolle spielt die Festlegung des Ortes der Niederlassung als Anknüpfungspunkt für die Anwendbarkeit der Richtlinie. Erwägungsgrund 19 folgend hat diese *„gemäß den in der Rechtsprechung des Gerichtshofs entwickelten Kriterien zu erfolgen, nach denen der Niederlassungsbegriff die tatsächliche Ausübung einer wirtschaftlichen Tätigkeit mittels einer festen Einrichtung auf unbestimmte Zeit umfasst“*[69]. Allein maßgeblich ist demnach jener Ort, an dem die nachhaltige und schwerpunktmäßige Ausübung einer Tätigkeit erfolgt bzw. anders ausgedrückt der Ort der Hauptverwaltungstätigkeit. Nicht ausschlaggebend hingegen ist der Ort der technischen Mittel zum Anbieten der Dienste, etwa des Servers einer www-Seite, die Zugänglichkeit einer Internetseite oder das Anbieten einer Dienstleistung in einem Mitgliedstaat. Würde man daran anknüpfen, wäre es ohne weiteres möglich, dass ein Diensteanbieter in mehreren Staaten gleichzeitig niedergelassen wäre.

Da die Gewährleistung der Dienstleistungsfreiheit, dargestellt in Art. 49 des EG-Vertrages ein derart vorrangiges Ziel der Europäischen Union darstellt, sind Beschränkungen nur in Ausnahmefällen zulässig. Anerkannte Rechtfertigungsgründe nach Art 3 Abs. 4 können etwa der Schutz der öffentlichen Sicherheit, der öffentlichen Ordnung, der öffentlichen Gesundheit, Verbraucherschutz und Jugendschutz sein, soweit die zu treffenden Maßnahmen erforderlich und verhältnismäßig sind und zudem dem Anzeigeverfahren in lit. b entsprochen wird.

6.2.3 „Nutzer“ und „koordinierter Bereich“

Nutzer von Diensten der Informationsgesellschaft können natürliche wie juristische Personen sein, die Informationen in offenen Netzen anbieten, als auch solche, die diese zu privaten oder beruflichen Zwecken online nachfragen. Folglich setzt sich dieser Begriff aus den in Art 2 lit. c und e definierten *„Diensteanbietern“* und *„Verbrauchern“* zusammen.

---

[68] Vertrag von Amsterdam, BGBl. III Nr. 83/1999

[69] Siehe auch die Definition des „niedergelassenen Diensteanbieters“ in Art 2 lit. c E-Commerce-Rl.

Vielerorts Erwähnung findet auch der Begriff des *„koordinierten Bereiches“*, worunter gemäß lit h des genannten Artikels die *„für die Anbieter von Diensten der Informationsgesellschaft und die Dienste der Informationsgesellschaft in den Rechtssystemen der Mitgliedstaaten festgelegten Anforderungen“* zu verstehen sind. Der genannte Bereich legt die durch die Informationsdiensteanbieter zu erfüllenden Pflichten bei Aufnahme und Ausübung ihrer Tätigkeit fest, d.h. für den Zugang wie auch für die Erbringung dieser Dienste. Nicht erfasst werden Anforderungen betreffend die Ware selbst, die Lieferung und nicht auf elektronischem Wege erbrachte Dienste.

6.3 Art 3 - Herkunftsland- und Binnenmarktprinzip

Grundsätzlich hat die Aufsicht über sämtliche Dienste der Informationsgesellschaft am jeweiligen Herkunftsort zu erfolgen. Dementsprechend ist das Rechtssystem desjenigen Mitgliedstaates anzuwenden, in welchem der jeweilige Anbieter niedergelassen ist. Diesem „Herkunftslandprinzip“ entsprechend, muss jeder zum Angebot stehende Dienst mit den innerstaatlichen Rechtsvorschriften einschließlich dem geltenden Gemeinschaftsrecht konform gehen. Dahinter steht die Überlegung, dass eine effiziente Aufsicht bestmöglich an der Quelle und bei bloß geringer räumlicher Distanz durchführbar ist. Die Kontrolle eines Diensteanbieters hat dementsprechend ausschließlich durch das Land der Niederlassung zu erfolgen, zusätzliche Überwachungsmaßnahmen durch andere Staaten sind idR ausgeschlossen.

Im Falle des Vorliegens mehrerer Niederlassungen findet sich in der Richtlinie selbst keine trennscharfe Regelung betreffend der Anwendbarkeit einer Rechtsordnung. Kommt man auch über die Feststellung des Mittelpunkts der Tätigkeiten zu keinem Ergebnis, wäre es denkbar, die länger bestehende Niederlassung als die ausschlaggebende anzusehen. Weiters gilt es festzuhalten, dass im Bereich der elektronischen Verträge das Herkunftslandprinzip nur in den Fällen anwendbar ist, in denen auch die Regelungen des Internationalen Privatrechts zu demselben Ergebnis führen. Bei divergierenden Ergebnissen geben die einzelstaatlichen

Kollisionsregeln den Ausschlag. Führen die Vorschriften des Internationalen Privatrechts am Niederlassungsort aber gerade nicht zur Anwendbarkeit nationalen Rechts, so ist diejenige Rechtsordnung ausschlaggebend, auf welche das IPR verweist, auch wenn das Herkunftslandprinzip dadurch in vielen Bereichen ausgehöhlt wird. So etwa in werberechtlichen Belangen, bei denen nach dem Prinzip des finalen Markteingriffs das Recht des Staates bzw. der Staaten anzuwenden ist, in denen die rechtswidrige Tätigkeit konkrete Auswirkungen gezeigt hat bzw. noch zeigt.[70]

Wie eben dargestellt gilt grundsätzlich das Herkunftslandprinzip. Wurde jedoch eine Niederlassung ausschließlich oder vorwiegend allein aus dem Grund gewählt, um die Anwendbarkeit der sonst gültigen Rechtsvorschriften auszuschließen, so ist ein Mitgliedstaat nach ständiger Rechtsprechung des Gerichtshofes sehr wohl dazu berechtigt, Maßnahmen gegen einen in einem anderen Mitgliedstaat niedergelassenen Diensteanbieter zu ergreifen. Diese Eingriffsbefugnis besteht unter der Voraussetzung, dass sich die Tätigkeit des Diensteanbieters auf dessen Hoheitsgebiet konzentriert.[71] Dieser Überlegung folgend, normiert Art 3 Abs. 4 die Möglichkeit des Ergreifens von individuellen Vollzugsmaßnahmen, d.h. von Maßnahmen der Verwaltungsbehörden gegen ausländische Diensteanbieter. Jede einzelne Maßnahme ist an eine ernstzunehmende Beeinträchtigung oder Gefährdung eines der erklärten Schutzziele der öffentlichen Ordnung, der öffentlichen Sicherheit, der öffentlichen Gesundheit und des Verbraucherschutzes gebunden. Zeitlich noch vor einem den Grundsätzen von Verhältnismäßigkeit, Angemessenheit und Nicht-Diskriminierung entsprechenden Tätigwerden ist ein spezielles Aufforderungs-, Anzeige- und Unterrichtungsverfahren gegenüber dem jeweiligen Niederlassungsstaat und der Europäischen Kommission einzuhalten. Lediglich in Dringlichkeitsfällen genügt die nachträgliche Mitteilung über eine bereits durchgeführte Maßnahme, welche seitens der Kommission nachträglich einer eingehenden Überprüfung hinsichtlich ihrer Rechtmäßigkeit zu unterziehen ist.[72]

[70] BG v. 15. Juni 1978 über das internationale Privatrecht (IPR-Gesetz), BGBl Nr. 304/1978 idgF.

[71] Erwägungsgrund 57, E-Commerce-Rl

Keine Anwendung findet die Richtlinie allgemein jedoch auf Anbieter von Diensten der Informationsgesellschaft, die in einem Drittland außerhalb der Gemeinschaft niedergelassen sind. Da die Reichweite geschäftlicher Aktivitäten im Internet weit über die Grenzen Europas hinausgeht, ist auch hier auf eine entsprechende Abstimmung mit außerhalb der Europäischen Union stehenden Staaten und Wirtschaftsräumen hinzuwirken.

6.3.1 Ausnahmen von der Richtlinie bzw. von Art 3

Der freie Dienstleistungsverkehr, das Binnenmarktprinzip, die Niederlassungs - und die Zulassungsfreiheit dürfen nicht aus Gründen eingeschränkt werden, die in den Regelungsgehalt der Richtlinie, den sogenannten koordinierten Bereich, fallen. Zwingende Folge dieses allgemeinen Beschränkungsverbotes wäre, dass ein Mitgliedstaat keine Maßnahmen gegen Dienste setzen könnte, welche im Herkunftsstaat des Diensteerbringers erlaubterweise erbracht werden, innerstaatlich jedoch verboten sind. Um diesem Manko Abhilfe zu verschaffen, sieht die Richtlinie die Möglichkeit vor, in Einzelfällen von diesem Grundsatz abzuweichen. Demzufolge sind Ausnahmen denkbar und zulässig, jedoch nur insoweit, als dies aus Gründen der öffentlichen Ordnung, der öffentlichen Gesundheit, der öffentlichen Sicherheit oder des Verbraucherschutzes erforderlich ist. In Übereinstimmung mit der Regelung des Art 3 Abs. 4 dürfen die an die inländischen Anbieter gestellten Anforderungen näher ausgestaltet werden, soweit und solange die Entsprechung mit europarechtlichen Vorgaben gegeben ist.

Durch die Richtlinie über den elektronischen Geschäftsverkehr werden, wie bereits dargestellt, keine zusätzlichen Regelungen zum Internationalen Privatrecht geschaffen, diese bleiben voll in Geltung. Ebensowenig befasst sich diese mit der Bestimmung der gerichtlichen Zuständigkeit. Die E-Commerce-Richtlinie findet in ihrer Gesamtheit weiters keine Anwendung auf dem Gebiet des Steuerwesens und auf die von der Datenschutzrichtlinie erfassten Bereiche.

[72] Siehe dazu ausführlich Art 3 Abs. 4 bis 6 E-Commerce-Rl.

Ebensowenig geregelt wird die Tätigkeit von Notaren und von Rechtsanwälten sowie nicht zu Werbezwecken initiierte Gewinnspiele.

Art 3 Abs. 3 verweist auf die im Anhang genannten Bereiche, auf welche die Richtlinie als solche zwar anzuwenden ist, jedoch nicht das Binnenmarktprinzip. Unter anderem werden hier die *„vertraglichen Schuldverhältnisse in bezug auf Verbraucherverträge"* aufgezählt. Dies aus dem einfachen Grund, weil nach Auffassung der Kommission diese im Europäischen Vertragsrechtsübereinkommen (EVÜ)[73] abschließend geregelt werden. Dort ist in Zusammenhang mit Verbraucherverträgen in Art 5 eine Durchbrechung des Herkunftslandsprinzips vorgesehen. Primär können die Vertragsparteien eine Rechtswahl treffen. Machen sie von dieser Möglichkeit keinen Gebrauch, so gilt grs. das Prinzip der engsten Beziehung zur vertraglichen Verpflichtung. In diesen Fällen sind spezielle Anknüpfungspunkte, wie etwa Aufenthalt, Wohnsitz oder der Ort der Hauptverwaltung der Partei, welche die charakteristische Leistung eines konkreten Vertrages zu erbringen hat. In vielen Fällen führt diese Regelung ohnehin zur Anwendbarkeit des Rechtes des Herkunftsstaates der Vertragsparteien, jedoch nicht zwingendermaßen. Die zwingenden Verbraucherschutzbestimmungen des gewöhnlichen Aufenthaltsortes des Konsumenten behalten unabhängig von einer allfällig erfolgten Rechtswahl ihre volle Wirkung. In diesem Zusammenhang normiert Art 5 EVÜ für ihre Anwendbarkeit und Geltung bestimmte Voraussetzungen, etwa die Bewerbung oder Angebotsstellung im Staat des Verbrauchers. Wie aus dem soeben Dargelegten hervorgeht, nimmt der Verbraucherschutz in der europäischen Politik einen sehr großen Stellenwert ein. Dementsprechend normiert ist zusätzlich auch ein besonderes Rücktrittsrecht zugunsten des Verbrauchers bei sogenannten „Haustürgeschäften"[74]. Dieses ist innerhalb einer Frist von sieben Tagen nach

---

[73] Übereinkommen von Rom über das auf vertragliche Schuldverhältnisse anzuwendende Recht von 1980 (konsolidierte Fassung), ABl 1998 C 27/34 ff, auch Europäisches Vertragsrechtsübereinkommen (EVÜ) genannt.

[74] Darunter sind Kaufverträge zu verstehen, die außerhalb von Geschäftsräumen geschlossen werden. Das spezielle Rücktrittsrecht zugunsten des Verbrauchers ist in Ö fixiert in §§ 3 und 4 KSchG und auf EU-

Vertragsabschluß bzw. nach entsprechender Belehrung über das dem Konsumenten zustehende Widerrufsrecht auszuüben.

Neben den „vertraglichen Verpflichtungen in Verbraucherverträgen" wurden in den sehr breiten Katalog von Ausnahmen zudem das „Urheberrecht und verwandte Schutzrechte, gewerbliche Schutzrechte, Finanzdienstleistungen und nicht angeforderte kommerzielle Kommunikation mittels elektronischer Post" aufgenommen.[75]

6.4 Art 4 – Grundsatz der Zulassungsfreiheit

Durch Art 4 Abs. 1 wird im Sinne der Niederlassungsfreiheit, näher ausgeführt in Art 43 EG-Vertrag, die grundlegende Verpflichtung der Mitgliedstaaten normiert, die Aufnahme bzw. die Ausübung einer Tätigkeit als Diensteanbieter von jeglicher, d.h. von jeglicher spezifischer, nur für die Erbringung elektronischer Dienste geltender, Zulassungspflicht freizuhalten. Dies schließt gleichzeitig auch Maßnahmen gleicher Wirkung aus, welche den Zugang zur Tätigkeit eines Anbieters von Diensten der Informationsgesellschaft von einer behördlichen Entscheidung, Maßnahme oder Handlung abhängig machen. Nicht davon erfasst werden jedoch Aufsichtsmaßnahmen in Form von Notifizierungs- und Registrierungsverfahren oder regelmäßigen Kontrollen. Dies bedeutet umgekehrt, dass das Erfordernis einer Genehmigung oder Zulassung für die Aufnahme einer Tätigkeit in denjenigen Bereichen weiterhin rechtmäßig und zulässig ist, wo dies auch für den nicht-elektronischen Bereich vorgesehen ist. Von dem Verbot einer Genehmigungs- und Zulassungspflicht weiters ausgenommen sind auch *„freiwillige Akkreditierungssysteme, insbesondere für Anbieter von Diensten für die Zertifizierung elektronischer Signaturen"*[76]. Von der Möglichkeit, derartige Ausnahmen zu schaffen, wurde seitens des österreichischen Gesetzgebers durch § 17 öSigG auch Gebrauch gemacht.

Ebene in der Rl 85/577/EWG betreffend den Verbraucherschutz im Falle von außerhalb von Geschäftsräumen geschlossenen Verträgen, ABl 372/1985, 31.

[75] *Brenn*, Der elektronische Geschäftsverkehr, ÖJZ 1999, S. 483

Die Zulassungsfreiheit bedingt im einzelnen, dass ein Diensteanbieter in jedem einzelnen Mitgliedstaat der Europäischen Gemeinschaft seine Tätigkeit auf rechtmäßige Art und Weise ausüben kann, wenn und solange er die rechtlichen Erfordernisse seines Heimatstaates erfüllt. Bestehen in einem Staat geringere Anforderungen als im jeweiligen Heimatstaat, so muss nur diesen nachgekommen werden, da im Sinne des Diskriminierungsverbotes an ausländische Diensteanbieter keine höheren Anforderungen als an inländische gestellt werden dürfen. Ebensowenig zulässig ist es etwa, aus einem anderen Mitgliedstaat erbrachte Dienste zusätzlich den eigenen Rechtsvorschriften zu unterwerfen, obwohl die entsprechenden Voraussetzungen bereits im Herkunftsland erfüllt wurden. Als Konsequenz einer anderslautenden Regelung wäre ein international tätiger Diensteanbieter einer doppelten bzw. vielfachen Kontrolle verschiedener Mitgliedstaaten und somit erheblichen Wettbewerbsnachteilen ausgesetzt.

6.5 „Kommerzielle Kommunikation"

Als sogenannte kommerzielle Kommunikation iSv Art 2 lit. f der Richtlinie sind *„alle Formen der Kommunikation, die der unmittelbaren oder mittelbaren Förderung des Absatzes von Waren und Dienstleistungen oder des Erscheinungsbildes eines Unternehmens, einer Organisation oder einer natürlichen Person dienen, die eine Tätigkeit in Handel, Gewerbe oder einen reglementierten Beruf ausübt"* zu verstehen, d.h. Werbung im weitesten Sinn. Auf Gemeinschaftsebene wird diese im Internet nun auch für standesrechtlich reglementierte Berufsgruppen, wie etwa Ärzte und Rechtsanwälte, als rechtmäßig und zulässig angesehen. Dies unter der Voraussetzung der Einhaltung berufs- und standesrechtlicher Regeln. Als Gegengewicht zu Dienstleistungs- und Niederlassungsfreiheit statuiert die Richtlinie in diesem Zusammenhang auf Seiten des Diensteanbieters spezielle Informations- und Kennzeichnungspflichten in Hinblick auf den werbenden Charakter elektronischer Mitteilungen oder sonstiger Internetangebote. Sobald kommerzielle Kommunikation zur Förderung des Verkaufs oder in Zusammenhang mit Zugaben, Geschenken, Preisausschreiben und

[76] Erwägungsgrund 28, E-Commerce-Rl

Gewinnspielen eingesetzt wird, ist diese klar als solche zu kennzeichnen. Die Person, auf deren Rechnung die Werbung betrieben wird, ist eindeutig als solche zu identifizieren. Dem Verbot der Schleichwerbung entsprechend soll sichergestellt werden, dass rein äußerlich als Fachtext erscheinende Information klar und eindeutig als Werbung erkenntlich ist. Diensteanbieter haben sich an sogenannte Robinson-Listen[77] zu halten, die sämtliche natürlichen und juristischen Personen auflisten, welche keine kommerziellen Kommunikationen zu erhalten wünschen.

Doch auch im alltäglichen Geschäftsverkehr ist durch die Angabe von Name und Anschrift des Diensteanbieters, dessen E-Mail-Adresse, Tätigkeit, Berufsbezeichnung im Herkunftsland, Kammerzugehörigkeit, gegebenenfalls Handelsregisternummer, Umsatzsteuernummer, Preisangabe in EURO udgl. den diversen Informationserfordernissen nachzukommen. Die Angaben zur Identifikation sind entsprechend Art 5 der Richtlinie leicht, unmittelbar und ständig verfügbar zu machen, wofür ein auf sämtlichen Seiten der Homepage sichtbares Symbol oder Logo in Verbindung mit einer Hypertext-Verknüpfung[78] als ausreichend gilt.

6.6 Art 9 - Elektronische Verträge

Vorweggenommen sei, dass allein über dieses Kapitel eine eigene Dissertation geschrieben werden könnte und wohl auch bereits geschrieben wird. Elektronische Verträge, die über staatliche Grenzen hinweg geschlossen werden, bringen eine Reihe von bisher ungelösten

---

[77] Derartige Listen sind aus konsumentenschutzrechtlicher Sicht sicher begrüßenswert, jedoch ohne Durchsetzungsanspruch. Beispiele sind einsehbar unter http://www.robinson-liste.de, eine Liste geführt von FSKnet-Freiwillige Selbstkontrolle der Werbetreibenden im Internet, sowie http://www.bigfoot.de, eine Privatliste, http://www.tradeport.de, eine Liste des Deutsche-Direktmarketing-Verbandes (DDV) sowie http://www.comm.or.at/wk/sv_ans.html#robinson.

[78] Durch eine derartige Verbindung wird es dem einzelnen Nutzer ermöglicht, durch einen einfachen Mouseclick auf ein bestimmtes Symbol, eine eine bestimmte markierte Fläche, eine Verbindung zu einem anderen Rechner oder auf eine andere Webseite herzustellen ohne die Notwendigkeit der Eingabe der Web-Adresse. Siehe die Definition im Praxishandbuch Internet Business, Bd. 1, Stand Okt. 2000, Augsburg, S. 13

Problemen mit sich. Nationales Recht allein führt in diesen Fällen zu keiner befriedigenden Lösung, es entsteht ein komplexes und zeitweilig beinahe undurchschaubares Nebeneinander von einzelstaatlichen, europäischen und internationalen Rechtsnormen, die im Rahmen ein- und desselben Sachverhaltes Berücksichtigung zu finden haben. Zu erwähnen wären hier etwa das UN-Kaufrechtsübereinkommen[79], die Verbraucherschutz-Richtlinie[80], das Konsumentenschutzgesetz[81] und die Fernabsatzrichtlinie[82]. In den kommenden Abschnitten möchte ich jedoch nur das für das Verständnis von über elektronische Netze zustandegekommenen Verträgen Notwendigste behandeln und die Signatur als Unterschriftenersatz in den Mittelpunkt stellen.

6.6.1 Anpassungsbedarf in den Mitgliedstaaten

In Ergänzung der Richtlinie über elektronische Signaturen wurde Art 9 in die hier gegenständliche Richtlinie eingefügt, welcher den Abschluss von „Online"-Verträgen regelt. Dementsprechend wird auch in Erwägungsgrund 34 festgestellt, dass *„jeder Mitgliedstaat seine Rechtsvorschriften zu ändern hat, in denen Bestimmungen festgelegt sind, die die Verwendung elektronisch geschlossener Verträge behindern könnten; dies gilt insbesondere für Formerfordernisse."* Die Verpflichtung der Mitgliedstaaten zur Beseitigung sämtlicher Hemmnisse bezieht sich verständlicherweise nur auf rechtliche. Praktische Hindernisse, die durch die tatsächliche Unmöglichkeit des Einsatzes elektronischer Mittel entstehen können, sind nicht darunter zu subsumieren. Ein Handlungsbedarf von

---

[79] Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf, BGBl. 1988/96

[80] Richtlinie 85/557/EWG betreffend den Verbraucherschutz im Falle von außerhalb von Geschäftsräumen abgeschlossenen Verträgen, Abl. 372/1985

[81] Bundesgesetz vom 8. März 1979, mit dem Bestimmungen zum Schutz der Verbraucher getroffen werden (Konsumentenschutzgesetz - KSchG), BGBl. 1979/140 idgF.

[82] Richtlinie 97/7/EG des Europäischen Parlaments und des Rates vom 20.5.1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz, ABl. L 144 vom 4.6.1997

Gesetzgebung, Gerichtsbarkeit und Verwaltung besteht jedoch sehr wohl bezüglich jener Bestimmungen, die die Verwendung elektronischer Mittel einschränken oder verhindern. Formvorschriften, die auf elektronischem Weg nicht erfüllt werden können und die Papierform faktisch begünstigen, sind aufzuheben und der neuen Rechtslage anzupassen. Von diesem Anpassungserfordernis umfasst sind sämtliche Phasen der Entstehung bzw. Erarbeitung eines Vertrages bis hin zu dessen Abschluss und Archivierung. Dem Erfordernis der Überprüfung bzw. Angleichung innerstaatlicher Rechtsvorschriften wird nicht durch die bloße Änderung von Schlüsselbegriffen, wie etwa der „Papierform" Genüge getan. Vielmehr sind sämtliche Aspekte zu ermitteln, die die tatsächliche Verwendung elektronischer Verträge verhindern oder beschränken. Verlangen gesetzliche Vorschriften etwa die physische Anwesenheit beider Geschäftspartner bei Vertragsabschluß oder einen bestimmten Ort, so machen diese die Verwendung elektronischer Technologien schlichtweg unmöglich. Unzulässig wäre etwa auch das Erfordernis der Hinterlegung einer Kopie des abgeschlossenen Vertrages bei einer Behörde, sofern dies für vergleichbare offline-Verträge nicht Voraussetzung ist. Ebenso auf ihre absolute Notwendigkeit hin zu überprüfen, sind sämtliche Vorgaben, die die Mitwirkung eines Dritten verlangen. Einem elektronisch zustandegekommenen Vertrag darf weder die Verwendung noch die rechtliche Wirksamkeit noch die rechtliche Gültigkeit abgesprochen werden, mit der alleinigen Begründung, dass dieser lediglich in elektronischer Form vorliege. Es handelt sich hiebei ganz allgemein um bloß ergebnisorientierte Vorgaben, von inhaltlichen, die Autonomie der Mitgliedstaaten einschränkenden Regelungen wird allgemein Abstand genommen.

Die Aufrechterhaltung bzw. Festlegung allgemeiner oder spezifischer Erfordernisse, etwa für sichere elektronische Signaturen, ist, soweit diese auf elektronischem Wege erfüllt werden können, weiterhin zulässig.

6.6.2 Ausschlusskatalog des Art 9

Art 9 Abs. 2 nimmt einen Aufzählung derjenigen Vertragstypen vor, auf welche der Grundsatz der Anerkennung elektronischer Verträge keine Anwendung zu finden hat. Diese setzen sich wie folgt zusammen:

- Verträge über die Begründung oder Übertragung von Rechten an Immobilien. Ausgenommen hievon sind wiederum Mietrechte.
- Verträge, bei denen die Mitwirkung von Gerichten, Behörden oder öffentliche Befugnisse ausübenden Berufen gesetzlich vorgeschrieben ist. Darunter fallen auch Verträge, bei denen die Mitwirkung von Gerichten, Behörden oder öffentliche Befugnisse ausübenden Berufen erforderlich ist, damit sie gegenüber Dritten wirksam sind und Verträge, bei denen eine notarielle Beurkundung oder Beglaubigung gesetzlich vorgeschrieben ist.
- Bürgschaftsverträge und Verträge über Sicherheiten, jedoch nur insoweit als diese von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit eingegangen werden und
- Verträge im Bereich von Familien- und Erbrecht.

Dieser Ausnahmekatalog ist nach Auffassung der Kommission als nicht abschließend anzusehen, da in Artikel 21 die Vorlage von Berichten über die Anwendung der Richtlinie durch diese selbst an das Europäische Parlament, den Rat und den Wirtschafts- und Sozialausschuss und die Anpassung der Richtlinie an die rechtlichen, technischen und wirtschaftlichen Entwicklungen im Bereich der Dienste der Informationsgesellschaft vorgesehen ist. Dies bedeutet im Ergebnis, dass der Ausnahmekatalog des Abs. 2 sowohl einer Erweiterung als auch einer Einschränkung durch die Kommission zugänglich ist.[83]

6.7 Art 10 - Informationspflichten der Diensteanbieter

[83] *Brisch*, EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr, CR 4/1999, S. 240

In Zusammenhang mit dem online-Abschluss von Verträgen treffen den Informationsdiensteanbieter spezielle Informationspflichten. Abweichungen davon sind nur bei besonderer Vereinbarung zwischen gewerblichen Vertragsparteien möglich, da hier das besondere Schutzbedürfnis auf Seiten des Verbrauchers wegfällt. Sobald jedoch ein solcher involviert ist, sind die Unterrichtungspflichten des Art 10 zwingender Natur. Die Informationen haben vor Abgabe der Bestellung durch den Nutzer in klarer, verständlicher und unzweideutiger Weise zu erfolgen. Die zum Vertragsabschluß führenden technischen Schritte, die Möglichkeit von Speicherung bzw. Zugänglichmachung, Erkennungs- und Korrekturmittel vor Abgabe der Bestellung fallen ebenso darunter wie die Angabe, in welchen Sprachen das jeweilige Dokument zur Verfügung steht.

Weiters hat der Diensteanbieter diejenigen Verhaltenskodices, denen er sich bindend unterworfen hat, bekanntzugeben, d.h. sowohl gegenüber dem einzelnen Nutzer wie auch gegenüber der Europäischen Kommission. Diese sollten in sämtlichen Amtssprachen der EU elektronisch abrufbar sein. Rechtliche Konsequenzen eines Nichtzugänglichmachens oder Nichterarbeitens sind bislang nicht normiert. In Art 16 wird die Erarbeitung dieser allgemein anerkannten Geschäftspraktiken und Gepflogenheiten Handels-, Berufs-, Verbraucherverbänden und Standesorganisationen auf Gemeinschaftsebene übertragen und dient vor allem der Förderung der Benutzungssicherheit des Internet. Damit auch der Nutzer selbst die Möglichkeit zu Speicherung und Reproduktion hat, sind Vertragsbestimmungen und Allgemeine Geschäftsbedingungen allgemein zugänglich zu machen. Will ein Diensteanbieter AGBs bei einem konkreten Vertrag zur Anwendung bringen, so ist diese Absicht zu offenbaren, d.h. auf der Homepage, auf dem elektronischen Bestellformular, deutlich sichtbar zu machen.[84] Nach zivilrechtlichen Grundsätzen gehen etwaige Unklarheiten zu Lasten dessen, der sich ihrer bedient, im gegebenen Fall also zu Lasten des Anbieters.[85]

---

[84] Siehe etwa die Allgemeinen Geschäftsbedingungen der Datakom GmbH, abrufbar unter http://a-sign.datakom.at/content/infodienst/richtlinien/richtlinien.html.

[85] *Schauer*, E-Commerce in der Europäischen Union, Wien 1999, S. 113ff

6.8 Art 11 - Zustandekommen eines Vertrages im Internet

6.8.1 Zugang einer Erklärung

Sind die Vertragsparteien darin übereingekommen, einen elektronischen Vertrag schließen zu wollen, so stellt sich unwillkürlich die Frage des Zustandekommens. Das Prozedere läuft im wesentlichen genauso ab wie auch bisher. Bei Vorliegen zweier übereinstimmender Willenserklärungen, im gegebenen Fall, zweiter inhaltlich korrespondierender Dateien, welche online übermittelt werden, kommt ein gültiger Vertrag zustande.[86] Zum Zwecke gegenseitiger Identifizierung und Authentifizierung, aber in ebendemselben Ausmaß auch in Zusammenhang mit den verschiedensten Zahlungsmodalitäten und der Sicherung von eventuell entstehenden Rückgriffsansprüchen, wird man sich vermehrt zur Verwendung einer elektronischen Signatur entschließen. Aufgrund der technischen Besonderheiten neuer Kommunikationstechnologien ist aber etwa der Zeitpunkt des Zugangs einer derartigen online-Erklärung nicht einfach zu bestimmen.

Im Hinblick darauf sieht Art 11 Abs. 1 der E-Commerce-Richtlinie verpflichtend vor, dass der Diensteanbieter den Eingang einer Bestellung unverzüglich auf elektronischem Wege zu bestätigen hat. Diese Empfangsbestätigung bedarf in der Praxis keines weiteren Willensentschlusses durch den Diensteanbieter, vielmehr ist sie auch elektronisch automatisiert möglich, wie dies im Bereich der EDI-Verträge auch allgemeine Praxis ist.

Über Internet abgegebene Erklärungen gelten ganz allgemein als solche unter Abwesenden, weshalb der Zeitpunkt des Einlangens in den Herrschaftsbereich des Gegenübers für Wirksamkeit und Eintreten der Bindungswirkung entscheidend ist. Sowohl die Bestellung selbst wie auch die Empfangsbestätigung gelten der Richtlinie folgend als eingegangen, sobald

---

[86] In Ö geregelt in § 861 ABGB. Durch Art 1 und 5 SigRl, Art 9 E-Commerce-Rl und § 4 öSigG vom Prinzip der Formfreiheit ausgenommen sind jedoch Rechtsgeschäfte, bei denen die elektronische Form ausdrücklich ausgeschlossen ist.

der jeweilige Ansprechpartner imstande ist, diese abzurufen. Mit dem Zeitpunkt des Eingangs beim Provider kann der Empfänger unter gewöhnlichen Umständen auch von seiner Nachricht, seiner e-Mail, Kenntnis nehmen. Nicht entscheidend ist der Zeitpunkt, in dem das Angebot konkret angenommen wurde, d.h. wann genau das Bildsymbol „OK" angeklickt wurde. Ebensowenig von Bedeutung ist, ob die Abrufung durch den Empfänger tatsächlich auch erfolgt. Der online-Vertrag gilt in dem Zeitpunkt als geschlossen, in dem das Angebot des Nutzers wie auch die entsprechende Annahme des Diensteanbieters wirksam beim jeweiligen Gegenüber zugegangen sind.

Betreffend den Zugang einer Willenserklärung[87] bedarf es jedoch einer klärenden Regelung. Durch das Abstellen auf die Abrufbarkeit wird den verschiedenen, in der Praxis vorkommenden technischen Gegebenheiten nicht Genüge getan. Zu unterscheiden wäre zwischen einer bloß zeitweise vorliegenden Netzverbindung durch ein Modem und dem Vorhandensein einer Standleitung oder eines eigenen Servers. Sinnvoll wäre im erstgenannten Fall das Abstellen auf den tatsächlich erfolgten Abruf des Empfängers und die entsprechende automatische Abrufbestätigung beim jeweiligen Sender. In der zweitgenannten Variante müsste dementsprechend das Vorliegen einer automatischen Empfangsbestätigung beim Sender ausschlaggebend sein.[88] Bei Einschaltung eines Mehrwertdienstes wiederum wären der tatsächliche Eingang der übermittelten Nachricht in die Mailbox des Mehrwertdienstes des jeweiligen Empfängers und kumulativ dazu das Einlangen einer dementsprechenden Eingangsbestätigung beim Sender als Voraussetzungen für einen wirksamen Zugang zu erwägen.[89]

Es stellt sich nun die Frage, ob die Zeit des wirksamen Eingangs einer Willenserklärung auch individuell bestimmt werden kann? Diese ist meines Erachtens in Hinblick auf den hohen

---

87 siehe dazu auch *Mottl*, Zur Praxis des Vertragsabschlusses im Internet, in: *Gruber/Mader*, Internet und e-commerce, Wien 2000, S. 17f

88 *Schauer*, Electronic Commerce in der Europäischen Union, Wien 1999, S. 201ff

89 siehe dazu auch *Mottl*, Electronic Commerce im Internet, in: *Jahnel/ Schramm/ Staudegger*, Informatikrecht, Wien 2000, S. 35ff

Stellenwert des Grundsatzes der Privatautonomie zu bejahen. Doch ist eine außerhalb dieser Zeit eingegangene Willenserklärung etwa erst am darauffolgenden Arbeitstag als wirksam zu betrachten?

Eines der Charakteristika auf elektronischem Wege abgegebener Erklärungen liegt in der durchgehenden und zeitunabhängigen Verfügbarkeit. Allein deshalb ist wohl davon auszugehen, dass ein Zugang dieser auch außerhalb der geschäftsüblichen Zeiten möglich sein sollte. Diese Feststellung gilt auf jeden Fall uneingeschränkt für den kommerziellen Bereich, nicht jedoch unbedingt auch für den privaten Nutzer. Gehen diesem Nachrichten zu, mit denen er nicht unbedingt zu rechnen brauchte, so wird wohl grundsätzlich erst der Zeitpunkt der tatsächlichen Kenntnisnahme als maßgeblich zu betrachten sein.

6.8.2 Abgrenzung der Herrschaftsbereiche

Probleme und rechtliche Unsicherheiten können zudem in den Fällen auftreten, in denen eine Nachricht zwar beim Provider eingeht, auf dem Weg zum jeweiligen Adressaten aber verlorengeht oder verändert wird. Ein gänzliches Abwälzen des Risikos wie auch der Beweislast auf den Sender einer Nachricht scheint sachlich nicht gerechtfertigt zu sein. Vielmehr ist die exakte Fixierung der Herrschaftsbereiche empfehlenswert, da sich die Möglichkeiten der Einflussnahme daran orientieren werden. Weiters mindern zusätzliche, gegenseitige Rückbestätigungspflichten und -obliegenheiten die Gefahr von Missverständnissen. Zudem hat der Empfänger einer Nachricht diese stets nach den Grundsätzen von Treu und Glauben zu verstehen. In diesem Zusammenhang gilt in Österreich die allseits bekannte Vertrauenstheorie[90]. Demnach ist eine Erklärung so zu verstehen, wie sie auch ein objektiver Dritter am Ort des Erklärungsempfängers verstehen musste. Diesen Regelungsansätzen entspricht auch das ABGB, wonach eine Willenserklärung grs. auf Risiko des Senders reist, wenn und solange diese noch nicht in den Herrschaftsbereich des

Empfängers gelangt ist. Der Empfängerhorizont erfährt dementsprechend eine nicht unerhebliche Erweiterung, da in der Regel bereits mit dem Eingang beim Internet-Provider das Risiko für Verstümmelungen und Übertragungsfehler übergehen wird.[91]

6.8.3 Rechtsform der Bestätigungen und Überlegungsfrist

Ebenso ungeklärt ist die Frage der Rechtsform der jeweiligen vom Diensteanbieter und vom Nutzer abzugebenden Bestätigungen und die Rechtsfolgen, wenn diese wider Erwarten nicht erfolgen. Für wie lange Zeit ist der Nutzer an seine Annahme gebunden, d.h. wie ist bei Nichtabgabe der Empfangsbestätigung seitens des Diensteanbieters zu verfahren? Kann er dieser Verpflichtung auch durch tatsächliche Vertragsausführung nachkommen?

Grundsätzlich wird im zivilrechtlichen Bereich einem bloßen „Schweigen" keinerlei Erklärungswert beigemessen. Auch für den Fall, dass in einem über Internet eingegangenen Angebot ausdrücklich erklärt wird, ein bloßes Untätigbleiben werde als Zustimmung gewertet, ist der Empfänger zu keinerlei aktivem Tun verpflichtet. Lediglich im Falle des Bestehens ständiger Geschäftsbeziehungen oder ausdrücklicher Bestimmungen in Allgemeinen Geschäftsbedingungen kann Abweichendes gelten und auch dem Schweigen Erklärungswert beigemessen werden. Eine dem Angebot entsprechende Leistung, beispielsweise das Absenden der bestellten Ware, lässt den Vertrag zustandekommen.[92]

Betreffend der zeitlichen Dauer der Bindungswirkung einer auf elektronischem Wege abgegebenen Erklärung gelten die allgemeinen Regeln des Zivilrechts. Im Gegensatz zum sehr

---

[90] siehe zur Vertrauenstheorie die Erläuterungen von *Koziol* in *Koziol/Welser*, Bürgerliches Recht[11], Bd. 1, Wien 2000, S. 95ff, 126 und *Dittrich/Tades*, ABGB[35], E 16ff zu § 863 und E 51ff zu § 914

[91] Siehe dazu auch *Mottl*, Electronic Commerce im Internet, in: *Jahnel/ Schramm/ Staudegger*, Informatikrecht, Wien 2000, S. 38ff

zeitaufwendigen Postweg ermöglicht das Internet idR eine Übertragung von Informationen ohne jede erwähnenswerte Verzögerung. Dies schließt natürlich umgekehrt ebensowenig erhebliche zeitliche Verzögerungen aus, die in Ausnahmefällen eintreten können. Diesem Unsicherheitsfaktor des tatsächlichen Zugangs einer Erklärung kann wie bereits dargestellt durch automatische Empfangs- und Eingangsbestätigungen entgegengewirkt werden. Wie auch im herkömmlichen Geschäftsverkehr steht dem jeweiligen Empfänger einer Nachricht eine angemessene Überlegungsfrist zu, deren Dauer etwaigen konsumentenschutzrechtlichen Beschränkungen unterworfen ist.[93] Eine als zu spät geltende Annahme ist als neues Angebot zu werten, welches einer erneuten Reaktion durch den Gegenüber bedarf.

6.8.4 Widerruf und Korrekturmöglichkeit

Auch die Möglichkeiten eines Widerrufes sind im Bereich des elektronischen Datenverkehrs sehr beschränkt. Sobald der Empfänger eine Zugriffsmöglichkeit hat, ist ein Abgehen von der ursprünglich abgegebenen Willenserklärung generell unzulässig. Nur bei zeitlich vorverlagerter oder zumindest gleichzeitig vorliegender Zugänglichkeit des Widerrufs ist ein solcher als gültig anzusehen. Auf die tatsächliche Kenntnisnahme des Erklärungsempfängers kann grs. nicht abgestellt werden.

Um rechtliche Streitigkeiten, entstanden durch Eingabefehler des Nutzers, zu vermeiden, sollten Diensteanbieter entsprechend Art 11 Abs. 2 angemessene Mechanismen zur Verfügung stellen, die die Überprüfung und Berichtigung von Fehlern ermöglichen. Diesem Erfordernis wird Genüge getan durch Aufscheinen eines eigenen Bestätigungsfensters nach dem bereits erfolgten erstmaligen Absenden einer Bestellung. Dabei werden dem Nutzer sämtliche von ihm eingegebenen Daten noch einmal angezeigt, um ihm die Möglichkeit zur Korrektur zu geben.

---

92 Siehe die österreichische Regelung in §§ 883ff ABGB.

93 § 6 Abs. 1 Z 1 KSchG verbietet unangemessen lange oder unbestimmte Fristen für die Annahme oder die Ablehnung des Vertragsantrages des Verbrauchers.

Die Bestellung wird schlussendlich erst durch ein wiederholtes Bestätigen endgültig abgesendet.

6.8.5 Invitatio ad offerendum

6.8.5.1 Online- und Offline-Bereich

Ordnet man die Darstellung von Waren und Dienstleistungen im Internet in die geltende Rechtslage[94] ein, so ist diese nicht als Angebotsstellung eines Diensteanbieters zu werten, genausowenig wie dies bei in Schaufenstern ausgestellten Konsumartikeln der Fall ist. Vielmehr hat erst die entsprechende Reaktion des Verbrauchers als Angebot zu gelten, welches einer gesonderten Annahme durch den Diensteanbieter bedarf. Andererseits ist bei einigen Verträgen auch die Vergleichbarkeit mit dem herkömmlichen Automatenkauf zu berücksichtigen. Bei diesem liegt ein an einen unbestimmten Personenkreis gerichtetes Angebot vor. Gegen die sofortige Erbringung einer Gegenleistung erhält der Käufer ohne zeitliche Verzögerung die gewünschte Ware. Letzteres ist auch der wesentliche Unterschied zu elektronischen Verträgen, da bei diesen idR mit sogenanntem elektronischem Geld gezahlt wird, die Kreditwürdigkeit des Kunden also nicht sogleich überprüft wird. Zumeist bestellt der Kunde online eine Ware, bezahlt diese aber erst im nachhinein, muss also nicht zuerst leisten, wie dies bei einem Automaten durch Einwurf des entsprechenden Geldbetrages der Fall ist. Meiner Einsicht nach, haben online-Angebote grs. als rechtlich unverbindlich zu gelten, allein um mit der bestehenden Rechtsordnung konform zu gehen.

Den dargestellten Erwägungen zufolge ist die Ähnlichkeit von online-Verträgen mit herkömmlichen Katalogen, Annoncen und Schaufenstern weitaus größer. Je nach dem konkreten Einzelfall sind jedoch Ausnahmen davon möglich. Bindungswille auf Seiten des Diensteanbieters wäre etwa anzunehmen, wenn die jeweiligen Angebote nur über ein bestimmtes Kennwort einer begrenzten Benützergruppe abrufbar oder ausschließlich an einen

begrenzten Personenkreis adressiert sind. Mit dem oben erwähnten Automatenkauf vergleichbar ist auch das Anbieten eines Softwareprogrammes auf einer Website. Dieses gilt als rechtlich bindendes Anbot, sofern das Programm direkt nach entsprechender Auswahl und Eingabe der Kreditkartennummer ohne weitere menschliche Einflussnahme, d.h. ohne zusätzlich erforderliche Willenserklärung auf Seiten des Diensteanbieters, direkt über Internet heruntergeladen werden kann. Auf der anderen Seite ist es jedoch auch ohne weiteres rechtlich zulässig und möglich, die Bindungswirkung eines Angebotes auf einer Homepage ausdrücklich auszuschließen.

6.8.5.2 Lösungsansatz der Richtlinie

Ein Vorschlag der Kommission[95] für eine Richtlinie über den elektronischen Geschäftsverkehr aus dem Jahre 1999[96] sah für einen wirksamen Vertragsabschluß noch vor, dass der Diensteanbieter den Eingang der Annahme durch den Nutzer und dieser seinerseits den Eingang dieser Empfangsbestätigung wiederum zu bestätigen hat. Die konkrete Vorgehensweise verlangte als Ausgangslage ein Anbot, welches der Nutzer nun annehmen konnte oder nicht. Demnach galt ein „Vertrag in dem Zeitpunkt als geschlossen, mit dem der Verbraucher vom Diensteanbieter eine Bestätigung des Empfanges der Annahme erhalten hat und er den Eingang der Empfangsbestätigung bestätigt hat."[97] Unter gewerblichen Vertragsparteien kann hievon jederzeit abgegangen werden. Das Anbieten von Diensten im Internet wurde allgemein als Angebot gewertet und nicht erst das darauffolgende Tätigwerden des Nutzers. Dabei wurde auch nicht weiter unterschieden, inwieweit der Adressatenkreis nun im Einzelfall konkretisiert war. Der Vorschlag der Richtlinie betrachtete die Rechtsfigur der

---

94 *Madl*, Peter, Vertragsabschluß im Internet, ecolex 1996, S. 79ff

95 Diesen hier ausdrücklich anzuführen, erscheint mir in der Hinsicht erforderlich, als sich der Standpunkt des Europäischen Gesetzgebungsgremiums innerhalb kürzester Zeit derart gewandelt hat.

96 Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, KOM (1999) 427 endg., Art 11

97 *Kilches*, Electronic Commerce Richtlinie, MR 1999, S. 3ff

„invitatio ad offerendum“ demzufolge im Bereich des elektronischen Geschäftsverkehrs als gänzlich hinfällig. Diese Verkomplizierung widersprach ganz allgemein ganz allgemein den erklärten Zielen der Richtlinie, wonach der Abschluss von Online-Verträgen vereinfacht werden sollte. Hätte der Diensteanbieter ausdrücklich jeden Bindungswillen auf seiner Seite ausgeschlossen, also die Rechtsfigur der invitatio ad offerendum zur Anwendung gebracht, so wären für einen gültigen Vertragsabschluß bloß die Stellung eines Angebots durch den Nutzer, die Annahme durch den Diensteanbieter und aus Gründen des Verbraucherschutzes wohl auch der Zugang der Annahmeerklärung beim Nutzer erforderlich gewesen. Nach Lösung der Kommission waren nun aber im Falle des Vorliegens eines bindenden Anbotes auf Seiten des Diensteanbieters zumindest vier Schritte notwendig, um einen wirksamen Vertragsabschluß herbeizuführen. Wäre man jedoch davon ausgegangen, dass erst die Reaktion des Nutzers als bindendes Offert zu werten wäre, so wäre das Verfahren erheblich kürzer geworden. Durch die Vielzahl der notwendigen Schritte bis hin zum wirksamen Vertragsabschluß, d.h. durch die wiederholten Bestätigungen wäre ein weiterer Unsicherheitsfaktor der Manipulation auf dem Datenweg hinzugetreten.

Nach der geltenden Rechtslage gilt ein Vertrag nun mit dem Zeitpunkt als geschlossen, als übereinstimmende Willenserklärungen, also Angebot und Annahme vorliegen, oder anders ausgedrückt, der Anbieter die Zustimmung zu seinem Anbot erhalten hat. Für den Bereich der elektronisch geschlossenen Verträge bedeutet dies im Ergebnis, dass der Vertrag schon durch die entsprechende Bestätigung der Bestellung des Verbrauchers zustande kommt.[98] In Österreich bestehen derzeit bereits ernsthafte Bestrebungen, die Vorgaben der Richtlinie in nationales Recht zu transformieren. Noch Ende des Jahres 2000 bzw. Anfang des Jahres 2001 wird eine Gesetzesvorlage der Abteilung für Zivilrechtswesen vorgelegt werden.

Ein besonderes Problem, welches nicht leicht einer Lösung zuzuführen sein dürfte, ergibt sich vor allem durch die nicht unerheblichen Divergenzen und Auffassungsunterschiede in den

europäischen Zivilrechtsordnungen. So etwa im Zusammenhang mit dem verpflichtenden Aufbau und Informationsgehalt von Verträgen. Die Richtlinie stellt jedoch einen wichtigen ersten Schritt in Richtung einer „einheitlichen europäischen Zivilrechtsordnung" dar.

Abschließend besonders hervorzuheben ist die weiterhin bestehende Geltung nationaler zivilrechtlicher Vorschriften beim Abschluss von online-Verträgen. Einzelstaatliche Normen zu Geschäftsfähigkeit, Anfechtbarkeit, Nichtigerklärung und Konsumentenschutz sind ebenso anwendbar wie spezialgesetzliche, den elektronischen Geschäftsverkehr im besonderen regelnde Vorschriften. Diese allgemeine Feststellung muss jedoch insoweit revidiert werden, als die Besonderheiten des Rechtsverkehrs im Internet bei der Problemlösung miteinzubeziehen sind. Auf diesem Wege kann es durchaus zu divergierenden Lösungen kommen.

6.9 Art 16 bis 20 - Umsetzung der Richtlinie

Entsprechend Kapitel III der Richtlinie soll auf die Etablierung und vermehrte Inanspruchnahme von Möglichkeiten vereinfachter außergerichtlicher Streitbeilegung auf elektronischem Wege, d.h. online ohne die Notwendigkeit physischer Anwesenheit der Anspruchsgegner, hingearbeitet werden. Der Einsatz elektronischer Signierung, unter anderem auch zum Zwecke der inhaltlichen Verschlüsselung, bietet gerade in einem derart sensiblen Bereich, der ein besonders hohes Maß an Vertrauenswürdigkeit und Sicherheit vor Kenntnisnahme unbefugter Dritter erfordert, ein rasches und effizientes Hilfsmittel.[99] Bestehende Hindernisse, etwa die verpflichtende Hinterlegung des Originals eines Schiedsspruchs, sind ehestmöglich zu beseitigen. Diese neuen Verfahrensvarianten tragen dem grenzüberschreitenden Charakter von Internet-Verträgen und der Notwendigkeit rascher

[98] Diese Rechtsansicht wird bereits auch im Gemeinsamen Standpunkt des Rates im Hinblick vom 28. Februar 2000, 14263/1/99 REV 1 vertreten und schließlich in der endgültigen Fassung der Richtlinie vom 17.7.2000 auf europäischer Ebene fixiert.

effektiver Rechtsdurchsetzung Rechnung. Überdies wird es sich in den meisten Fällen um relativ niedrige Streitbeträge handeln, bei denen es allein aus Kosten- und Zeitgründen nicht lohnen würde, den ordentlichen Klagsweg zu beschreiten. Um nicht in weiterhin allgemein zugängliche gerichtliche Klags- und Verfahrensvorschriften einzugreifen, ist die Freiwilligkeit sowohl der Teilnahme an derartigen neuen Verfahren als auch der Vollstreckung zu gewährleisten. Eine gerichtliche zwangsweise Durchsetzung einer Entscheidung bzw. eines Schiedsspruchs ist nicht vorgesehen. Wie auch die herkömmlichen Verfahren sind die neu zu schaffenden Varianten der online-vermittelten außergerichtlichen Streitbeilegung von den Grundsätzen der Unabhängigkeit, der Transparenz, des kontradiktorischen Verfahrens, der Verfahrenswirksamkeit, der Rechtmäßigkeit, der Handlungsfreiheit und der rechtsanwaltschaftlichen Vertretung bestimmt.

Derzeit noch ungeklärt ist die Frage, welche Institutionen diese Aufgaben zu erfüllen imstande sind. Die bestehenden Schiedsgerichtsverfahren sind für die Beilegung internationaler Rechtsstreitigkeiten im elektronischen Geschäftsverkehr völlig ungeeignet und zudem mit erheblichem Zeit- und Kostenaufwand verbunden. Weiters mangelt es in weiten Bereichen noch an ausreichend geschultem und mit den Besonderheiten der neuen Kommunikationstechnologien hinreichend vertrautem Personal.

Wie bereits erwähnt, bleibt weiterhin die Möglichkeit bestehen, vor den ordentlichen Gerichten gegen unerlaubte Tätigkeiten im World-Wide-Web zu klagen. Durch die Schaffung einer sogenannten Internetgerichtsbarkeit wird die Durchführung von Verfahren bzw. die Einbringung von Klagen bei den ordentlichen staatlichen Gerichten über Internet ermöglicht. Artikel 18 sieht auch die Zulässigkeit der Ergreifung vorläufiger Maßnahmen, wie etwa einstweiliger Verfügungen und Anordnungen, vor, um in Dringlichkeitsfällen weiteren Schaden abwehren und Rechtsgutverletzungen abstellen zu können. Weiters wird in Abs. 2 der

[99] Mehr noch, das Signaturgesetz hat erst die Grundlage dafür geschaffen, dass Schiedsverträge und Schiedssprüche auf ausschließlich elektronischem Wege zustande kommen können. Siehe dazu *Jud, Högler-Pracher,* Schiedsverfahren mit modernen Kommunikationstechniken, ecolex 1999, S. 601ff

genannten Rechtsvorschrift auf die Richtlinie über Unterlassungsklagen[100] verwiesen. Durch diese Bezugnahme werden in den harmonisierten Regelungsbereichen der E-Commerce-Richtlinie etwa auch Verbandsklagen zum Schutz von Verbraucherinteressen möglich.

Artikel 19 sieht eine weitgehende Zusammenarbeit der Mitgliedstaaten vor, sodass auf elektronischem Wege begangene Verbrechen und Vergehen über die bisher üblichen Grenzen hinweg verfolgt und geahndet werden können. Erwähnt ist die vermehrte Inanspruchnahme und das rasche Entsprechen von Amtshilfe- und Auskunftsbegehren seitens anderer Mitgliedstaaten oder der Europäischen Kommission - auch auf elektronischem Weg. Zum Zwecke der Erteilung von Informationen gegenüber Nutzern, Diensteanbietern und anderen Mitgliedstaaten sind sogenannte Verbindungsstellen einzurichten, die auch elektronisch zugänglich sein müssen.

Damit die Vorschriften der Richtlinie nicht leeres und im Falle des Zuwiderhandelns sanktionsloses Recht bleiben, haben die Mitgliedstaaten gemäß Artikel 20 für entsprechende Maßnahmen ihrer Durchsetzung zu sorgen. Wahl sowie Ausmaß der konkreten Sanktionen bleiben den nationalen Gesetzgebungsgremien vorbehalten. Deren Festlegung im einzelnen kann jedoch erst nach entsprechender Umsetzung der Richtlinie auf einzelstaatlicher Ebene erfolgen. Für diese fixiert Art 22 den Stichtag 17. Jänner 2001, bis zu welchem die rechtlich unverbindlichen Regelungen der E-Commerce-Richtlinie hinsichtlich ihrer Zielsetzung umzusetzen sind.[101]

---

[100] Richtlinie 98/27/EG des Europäischen Parlaments und des Rates vom 19. Mai 1998 über Unterlassungsklagen zum Schutz des Verbraucherinteressen, Abl. L 166 vom 11.6.1998

[101] Laut telefonischer Rücksprache mit dem BMJ, Abteilung für Zivilrechtswesen, ist ein entsprechendes Gesetz bereits in Vorbereitung, jedoch ist noch keine veröffentlichte Fassung verfügbar.

7 Bundesgesetz über elektronische Signaturen

7.1 Allgemeines

Mit dem Bundesgesetz über elektronische Signaturen verfügt Österreich als einer der ersten Mitgliedstaaten der Europäischen Union über einen nationalen Regelungsrahmen, der mit den europarechtlichen Vorgaben, im besonderen der Signatur-Richtlinie und der E-Commerce-Richtlinie weitgehend übereinstimmt. Entsprechend dem Bericht des Justizausschusses über die Regierungsvorlage „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“, womit wiederum „eine wichtige Weiche für die Attraktivität des Wirtschaftsstandorts Österreich gestellt“ wird.[102]

Bereits am 14.7.1999 verabschiedete der Nationalrat einstimmig das vom Bundesministerium für Justiz ausgearbeitete österreichische Bundesgesetz über elektronische Signaturen, welches noch vor der Signaturrichtlinie am 1.1.2000 in Kraft trat. Regelungsrahmen und Aufbau decken sich weitgehend mit der europarechtlichen Vorgabe, ihre Richtlinienkonformität dürfte in weiten Teilen gegeben sein. Am einfachsten erscheint es mir, bei der Besprechung des Signaturgesetzes entsprechend dessen Aufbau vorzugehen und die Probleme der Umsetzung bei jedem einzelnen Themenbereich gesondert zu besprechen.

7.2 § 1 - Anwendungsbereich und Ziele

§ 1 Abs. 1 des Bundesgesetzes *„regelt den rechtlichen Rahmen für die Erstellung und Verwendung elektronischer Signaturen sowie für die Erbringung von Signatur- und Zertifizierungsdiensten.“* Der in § 1 sehr allgemein gehaltene Regelungsbereich des Gesetzes konzentriert sich im wesentlichen auf folgende Grundsätze:

- Zulassung und Nichtdiskriminierung elektronischer Signaturen im Geschäfts- und Rechtsverkehr;
- weitgehende rechtliche Gleichstellung der sicheren elektronischen Signatur mit der eigenhändigen Unterschrift;
- Schaffung eines Aufsichtssystems über die Zertifizierungsstellen und ein eigenes System zur freiwilligen Akkreditierung,
- Einführung spezieller Haftungsregelungen für Diensteanbieter und schließlich
- Anerkennung ausländischer elektronischer Signaturen.

[102] NR: GP XX RV 1999 AB 2065 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP, 1

In geschlossenen Systemen ist das Signaturgesetz anzuwenden, sofern dies von den Teilnehmern vereinbart wurde. Derartige Systeme stehen nur einem im vorhinein begrenzten Teilnehmerkreis zur Verfügung und zeigen keinerlei Rechtswirkungen nach außen. Beispiele hierfür wären etwa das Intranet oder die von Kreditinstituten angebotenen elektronischen Netze. In diesen Bereichen können in Wahrung des Grundsatzes der Privatautonomie die Bedingungen des Vertragsabschlusses, insbesondere Inhalt und Form, im vorhinein vereinbart werden. Auch die Richtlinie sieht in Erwägungsgrund 16 vor, dass *„in Systemen, die auf freiwilligen privatrechtlichen Vereinbarungen beruhen“*, die Freiheit der beteiligten Parteien zu bestimmen, ob sie sich dem Signaturgesetz unterwerfen wollen, zu wahren ist.

Im *„offenen elektronischen Verkehr mit Gerichten und anderen Behörden“*[103], vornehmlich also in der Kommunikation von Unternehmen und Verbrauchern mit der nationalen Verwaltung, ist das Signaturgesetz hingegen anzuwenden, sofern durch Gesetz nicht anderes bestimmt ist. Grundsätzlich sollte mit dem Erfordernis der sicheren elektronischen Signatur das Auslangen gefunden werden. Die Normierung zusätzlicher Erfordernisse auf Gesetzesstufe ist lediglich aufgrund spezifischer Gegebenheiten in einzelnen Verwaltungsbereichen zulässig.[104]

Auch der Richtlinie folgend können für die Verwendung im öffentlichen Bereich zusätzliche Anforderungen an elektronische Signaturen gestellt werden, etwa im Sozialbereich oder in der Medizin. Artikel 3 Z 7 ermöglicht über die Bestimmungen des Signaturgesetzes hinausgehende Anforderungen, die einer sorgfältigen Prüfung im Hinblick auf Erforderlichkeit, Angemessenheit, Objektivität, Transparenz, Verhältnismäßigkeit und Nichtdiskriminierung standzuhalten haben. Demnach verlieren etwa das AVG[105] und das GOG[106] nicht vollständig

[103] siehe § 1 Abs. 2 öSigG

[104] NR: GP XX RV 1999 AB 2065 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP, 5

[105] etwa § 13 AVG

an Bedeutung. Es ist jedoch sicherzustellen, dass derartige, zusätzlich normierte Anforderungen den EU-Bürger in seinen grenzüberschreitenden Tätigkeiten und Geschäftsbeziehungen nicht einschränken.

Auffallend ist, dass im Text der Richtlinie vom *„öffentlichen Bereich"* gesprochen wird, das österreichische Signaturgesetz diesen Terminus jedoch nicht übernimmt. Da die Differenzierung zwischen öffentlichem und privatem Bereich oftmals Probleme aufwirft, stellt der österreichische Gesetzgeber auf die Existenz einer staatlichen Behörde als Kommunikationspartner ab. Dementsprechend fällt sowohl der Komplex der Hoheitsverwaltung wie auch die gesamte Privatwirtschaftsverwaltung unter den Regelungsbereich des Gesetzes. Doch auch Selbstverwaltungskörper und selbst beliehene Unternehmen fallen in Ausübung von ihnen übertragenen staatlichen bzw. öffentlichen Aufgaben unter Abs. 2.[107]

7.3 § 2 - Begriffsbestimmungen

Der Katalog der in § 2 des Gesetzes enthaltenen Definitionen orientiert sich stark am Aufbau der Richtlinie. Das Signaturgesetz wählt durch den Ausdruck der *„elektronischen Signatur"* ebenfalls einen technologieneutralen Ansatz, der nicht nur die zur Zeit zur Anwendung kommende digitale Verschlüsselungstechnik zuläßt. Vielmehr ist darunter jedes der Authentifizierung, also der Feststellung der Identität des Signators dienende Verfahren zu verstehen.

7.3.1 „Signator"

---

[106] etwa §§ 89a ff GOG

[107] *Brenn*, Signaturgesetz, Wien 1999, S. 51

Dem österreichischen Signaturgesetz folgend kann nur eine natürliche Person als Inhaber eines Signaturschlüssels, als sogenannter Signator, auftreten. Das einzelne Rechtssubjekt kann entweder für sich selbst oder im Rahmen einer Vertretungsbefugnis für eine juristische Person handeln, wobei bei einem Unterzeichnen in fremdem Namen die Vertretungsmacht im jeweiligen Zertifikat aufzuscheinen hat.[108] Die Einschränkung auf natürliche Personen ist zulässig und gemeinschaftsrechtskonform. Die Richtlinie über elektronische Signaturen überlässt durch Artikel 2 Z 3 dem nationalen Gesetzgeber hier Entscheidungsspielraum, indem ein Unterzeichner lediglich als *„eine Person, die ...“* definiert wird.

Lediglich bei Zertifikaten von Zertifizierungsdiensteanbietern kann auch eine juristische Person oder etwa auch eine Personenhandelsgesellschaft als Signator auftreten. Derartige Zertifikate dürfen ausschließlich zum Signieren von Anwender-Zertifikaten und zur Erbringung anderer Zertifizierungsdienste verwendet werden. Der nationale Gesetzgeber entschloss sich zu dieser Ausnahmeregelung, da die Gültigkeit dieser Zertifikate nicht von der aufrechten Vertretungsbefugnis einer natürlichen Person abhängig sein sollte. Will die Zertifizierungsstelle jedoch Rechtsgeschäfte abschließen, so kann sie wie jede andere juristische Person auch ebenso nur durch ihre vertretungsbefugten Organe tätig werden.

Da in geschlossenen Bereichen der Privatautonomie Vorrang eingeräumt wird, steht es hier den Vertragsparteien weiterhin frei, auch juristische Personen als Signatoren zuzulassen. Wollen sie jedoch das Signaturgesetz in ihren Geschäftsbeziehungen untereinander zur Anwendung bringen, so ist von einer derartigen Vereinbarung Abstand zu nehmen.

7.3.2 „Sichere elektronische Signatur“

[108] Vergleiche etwa §§ 26ff ABGB, §18 GmbHG, §§ 71ff AktG, ua. Der österreichischen Rechtslage entsprechend kann sich eine juristische Person nicht selbst als ebensolche, sondern nur durch befugte Organwalter, d.h. durch in ihrem Namen und auf ihre Rechnung tätige natürliche Personen, rechtsgeschäftlich binden.

§ 2 Z 3 setzt das Signaturgesetz in direkte Verbindung mit der Richtlinie. Demzufolge ist eine *„sichere elektronische Signatur"* als eine *„fortgeschrittene elektronische Signatur"* im Sinne der Richtlinie zu verstehen, die zudem deren Anhänge I bis III zu erfüllen hat. D.h. eine sichere elektronische Signatur muss auf einem qualifizierten Zertifikat nach Anhang I beruhen und außerdem von einer sicheren Signaturerstellungseinheit nach Anhang III erstellt werden.

Lit. a leg.cit. verlangt die ausschließliche Zuordenbarkeit zum jeweiligen Signator. Dies bedeutet, dass bestimmte Signaturerstellungsdaten wie auch die dazu komplementären Signaturprüfdaten einmalig und ausschließlich dem im Zertifikat genannten Inhaber zuordenbar sein müssen.

Lit. b nennt als weitere Voraussetzung des Vorliegens einer sicheren elektronischen Signatur die Möglichkeit der eindeutigen Identifizierung des Signators, die sogenannte Authentifikation. Aufgrund der Signatur muss ermittelbar sein, wem diese zuzuordnen ist. Dazu erforderlich ist die Einmaligkeit des privaten Signaturschlüssels, d.h. es muss ausgeschlossen werden können, dass dieser ein zweites Mal existent oder aus dem öffentlichen Signaturschlüssel ableitbar ist.

In diesem Zusammenhang bestimmt die öSigV in ihrem § 3 Abs. 3 und 5: *„Die Signaturerstellungsdaten für sichere elektronische Signaturen der Signatoren müssen die im Anhang I Punkt 2 festgesetzte Mindestlänge aufweisen"*, d.h. derzeit beim RSA-Verfahren 1023 Bit, und *„die Erzeugung der Signaturerstellungsdaten für sichere elektronische Signaturen muss auf einer tatsächlichen Zufälligkeit beruhen, der ein technischer Zufall oder ein signatorbezogener Zufall zu Grunde liegt. Die Signaturerstellungsdaten müssen in der im Anhang I Punkt 3 festgelegten Anzahl von Bitstellen durch tatsächliche Zufallselemente beeinflusst sein"*[109], d.h. beim RSA-Verfahren hinsichtlich aller 1023 Bit.

[109] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), BGBl. II 30/2000

Weiters muss die elektronische Unterschrift mit *„Mitteln erstellt werden, die der alleinigen Kontrolle“* des Signators unterliegen. Durch spezielle Sicherheitsvorkehrungen soll ausgeschlossen werden, dass ein unbefugter Dritter Kenntnis von den Signaturerstellungsdaten eines berechtigten Inhabers erlangen kann. Derzeit versucht man diesem Erfordernis durch Bindung der Signaturerstellungsdaten an Besitz, etwa einer Chipkarte, und Wissen, etwa einer PIN oder eines Passwortes, gerecht zu werden. In Zukunft sollen weitere Methoden, darunter Stimmerkennungsverfahren, Körperfrequenzmessung und Fingerabdruckvergleich, die eindeutige Identifikation des Unterzeichnenden sicherstellen.

Lit. d setzt die Möglichkeit der Feststellung von nachträglichen Datenveränderungen voraus. Diese können im Rahmen des elektronischen Signierungsverfahrens bzw. des Verfahrens der Signaturprüfung sichtbar gemacht werden, da die Hashwerte zweier unterschiedlicher Dokumente bei einem Vergleich niemals übereinstimmen können.

7.3.3 „Signaturerstellungsdaten und -einheiten“

Die darauffolgenden Begriffsbezeichnungen von *„Signaturerstellungsdaten“* und *„Signaturerstellungseinheiten“* entsprechen vollinhaltlich den Definitionen der Signatur-Richtlinie und deren Anhang III, welche wiederum durch die legistischen Vorarbeiten der UNCITRAL beeinflusst wurden. Wenn möglich, d.h. bei Verfügbarkeit der notwendigen technischen Mittel, ist der private Schlüssel beim Inhaber selbst zu erzeugen, nur in Ausnahmefällen bei einem Zertifizierungsdiensteanbieter. Die Speicherung desselben ist aus Sicherheitsgründen jedenfalls nur beim Betroffenen selbst zulässig, nicht aber bei der Zertifizierungsstelle oder einer anderen dritten Stelle. Durch einen relativ hohen Sicherheits- und Technikstandard soll die Erzeugung sicherer elektronischer Signaturen ermöglicht werden.

Anhang III der Richtlinie legt die an die Signaturerstellungseinheiten gestellten Mindestanforderungen fest, welche wiederum die Signaturerstellungsdaten mitumfassen. Sowohl Hard- wie auch Software, d.h. Chipkarte, Chipkartenlesegerät, Algorithmus,

Hashwert und Verschlüsselungsverfahren und die Kombination von diesen Einheiten haben den festgelegten Sicherheitsanforderungen zu entsprechen.

Die öSigV legt die zeitlich limitierten Anforderungen in Anhang I und II detailliert fest. Demzufolge muss beim Verfahren RSA die Mindestschlüssellänge der Signaturerstellungsdaten für sichere elektronische Signaturen 1023 Bit betragen, wobei sämtliche von diesen Bitstellen durch tatsächliche Zufallselemente beeinflusst sein müssen. Nur die in den Auflistungen enthaltenen Hashverfahren und Algorithmen, worunter Verfahren zur Signaturerstellung und zur Verschlüsselung des Hashwertes zu verstehen sind, gelten grundsätzlich als sicher. Andere Verfahren sind diesen gleichgestellt, insofern sie den gleichen Sicherheitsstandard aufweisen und von einer Bestätigungsstelle anerkannt und entsprechend veröffentlicht wurden. Zur Vereinfachung und Ermöglichung des grenzüberschreitenden Einsatzes von Verschlüsselungstechniken sollen international anerkannte Formate zur Anwendung gelangen. Für sämtliche technischen Verfahren und Komponenten, für Formate wie auch Algorithmen, gilt die Sicherheitsvermutung derzeit bis zum 31. Dezember 2005.

7.3.4 „Signaturprüfdaten und -einheiten“

Entsprechendes gilt für die *„Signaturprüfdaten“* und die *„Signaturprüfeinheiten“* in Z 6 und 7 bzw. Art 2 Z 7 und 8. Anhang IV der Richtlinie normiert Empfehlungen betreffend einer sicheren Signaturprüfung, in deren Verlauf der jeweilige Empfänger einer unterzeichneten Nachricht den Urheber eindeutig feststellen können muss. Die dafür erforderlichen Prüfkomponenten sind von den nationalen Zertifizierungsdiensteanbietern zur Verfügung zu stellen.

7.3.5 „Zertifikat“

Durch die Ausstellung von Zertifikaten, welche neben anderen Angaben den Inhaber und dessen öffentlichen Schlüssel zu enthalten haben, wird die eindeutige Identifikation des

Unterzeichners ermöglicht. Dies aus dem einfachen Grund, weil der Signator alleiniger Inhaber des dazu komplementären privaten Signaturschlüssels zu sein hat und unter dieser Voraussetzung die entsprechende Signatur zu erstellen alleinig imstande ist. Die öffentliche Bescheinigung der Zuordnung eines Schlüsselpaares wird entweder direkt mit dem signierten Dokument versendet oder sonst online abrufbar gemacht.

Um den Zusatz *„qualifiziert"* zu erhalten, haben Z 9 entsprechend spezifische Voraussetzungen erfüllt zu sein. Zum einen hat das Zertifikat einen bestimmten Mindestinhalt aufzuweisen, welcher aufgezeigt ist in § 5 Abs. 1 und 2 bzw. Anhang I der Richtlinie. Zwingend vorgesehen sind unter anderem Angaben über den Signator, den ihm zugeordneten öffentlichen Schlüssel, die Ausstellungsstelle, die Gültigkeitsdauer des Zertifikats und allfällige Beschränkungen des Anwendungsbereiches oder des Transaktionswertes. Zudem ist ausschließlich ein Zertifizierungsdiensteanbieter, der den Anforderungen des § 7 bzw. des Anhangs II der Richtlinie genügt, zur Ausstellung von „qualifizierten Zertifikaten" berechtigt. Dieser hat für die erforderlichen technischen, organisatorischen und personellen Gegebenheiten zu sorgen, damit der durch das Gesetz vorausgesetzte Sicherheitsstandard eingehalten und die Gefahr der Zertifikatsfälschung minimiert werden kann. Neben der Zuverlässigkeit der Identitätsprüfung und des Verzeichnis- und Widerrufsdienstes hat er bei Aufnahme seiner Tätigkeit unter anderem die Verfügbarkeit über ein haftungsdeckendes Risikokapital nachzuweisen.

7.3.6 „Zertifizierungsdiensteanbieter"

Während nach dem Signaturgesetz bloß eine natürliche Person als Signator auftreten kann, ist für die Erbringung von Zertifizierungsdiensten auch eine juristische Person oder eine sonstige rechtsfähige Einrichtung berechtigt. Ebensowenig wie die Aufnahme ihrer Tätigkeit an eine Genehmigung, Lizenz oder ähnliches gebunden ist, ist die Zahl der Zertifizierungsdiensteanbieter begrenzt. Ihre Haupttätigkeit liegt in der Erstellung von Zertifikaten, d.h. in der Zuordnung von Signaturprüfdaten zum jeweiligen Inhaber. Daneben

sind aber auch die Führung des Verzeichnis- und Widerrufsdienstes, die Verwaltung der Zertifikate und die Bereitstellung von Signaturverfahren, -produkten und -diensten nach Z 11 von ihrem Tätigkeitsbereich erfasst.

Zertifizierungsdiensteanbieter haben die Möglichkeit der Zertifikatsausstellung lautend auf Anwender, lautend auf sich selbst zur Ausübung ihrer Tätigkeit wie auch lautend auf andere Mitkonkurrenten. Diese letzte Variante wird als „Cross-Zertifizierung“[110] bezeichnet. Eine derartige Zertifizierung für andere Diensteanbieter begründet im wesentlichen die Vertrauenswürdigkeit der von diesen ausgestellten Zertifikaten gegenüber den jeweiligen Signatoren. Auf diesem Wege ist es ohne weitere Verkomplizierung möglich, auch qualifizierte ausländische Zertifikate mit österreichischen praktisch gleichzustellen.

Unter den Begriff der Signaturverfahren sind sämtliche Verfahren zur Erstellung und Überprüfung von elektronischen Signaturen wie auch zur Darstellung der Daten vor und nach dem Signierungsvorgang zu subsumieren, wofür die von den Zertifizierungsdiensteanbietern nach Z 13 verwendeten bzw. zur Verfügung gestellten Signaturprodukte erforderlich sind. Dies sind die Signaturerstellungs- wie auch Signaturprüfeinheiten, die auf Seiten des Signators wie auch auf Seiten des jeweiligen Empfängers zur Anwendung gelangen. Eine heute noch vorherrschende und als sicher geltende Signaturerstellungseinheit ist die Chipkarte mit dem dazugehörigen Chip, wobei unter ersterem Kartenkörper, Hardware, Betriebssystem und Anwendungen zusammengefasst werden.

Feststellungen des Justizausschusses folgend können neben den im Signaturgesetz angeführten Signatur- und Zertifzierungsdiensten auch Dienste zur Verschlüsselung des Dateninhalts selbst angeboten werden. In diesem Falle ist jedoch sicherzustellen, dass nicht ein und dieselben Signaturerstellungs- und Signaturprüfdaten zur Ver- bzw. Entschlüsselung des Hashwertes wie auch des Nachrichteninhalts verwendet werden. Ebensowenig darf ein und dieselbe PIN oder ein und dasselbe Passwort beide Vorgänge auslösen. In den eben genannten Fällen wäre es

für den durchschnittlichen Nutzer nicht länger eindeutig ersichtlich und vorhersehbar, ob im konkreten Fall nun die Signaturfunktion oder die Verschlüsselungsfunktion aktiviert wird.[111]

Nicht alle diese Leistungen müssen von ein und demselben Diensteanbieter erbracht werden; die Zurverfügungstellung von Signaturprodukten allein reicht jedoch nicht aus, um als Anbieter von Zertifzierungsdiensten zu gelten. Zum Betrieb eines derartigen Unternehmens ist nicht nur eine staatliche Stelle, etwa mit Öffentlichkeitsrecht, sondern auch jede private Einrichtung berechtigt. Das Signaturgesetz wie auch die Richtlinie bringen eine sehr marktwirtschaftliche Orientierung zum Ausdruck. Nicht staatliche Einmischung sondern freier Wettbewerb sollen dazu führen, dass sich schließlich diejenigen Anbieter durchsetzen, die die vertrauenswürdigsten Systeme anbieten und das bessere Preis-Leistungs-Verhältnis vorzuweisen haben.[112]

7.3.7 „Kompromittierung"

Den Anregungen des Justizausschusses folgend, wurde in Z 14 eine Definition des bisher ungebräuchlichen Begriffes der *„Kompromittierung"* aufgenommen. Darunter sind sicherheitsrelevante Beeinträchtigungen in Zusammenhang mit Signaturerstellung und -prüfung zu verstehen. Als Beispiele werden das Ausspähen des privaten Signaturschlüssels, die Ausforschung des zugrundeliegenden Algorithmus und das Brechen des Chipspeichers genannt.[113] Tritt einer der genannten Fälle ein, so kann nicht länger absolut sichergestellt werden, dass ein unberechtigter Dritter nicht Rechtsgeschäfte unter Verwendung des

---

[110] siehe auch § 12 Abs 5 öSigV

[111] *Brenn*, Signaturgesetz, Wien 1999, S. 59f

[112] Eine geradezu gegenteilige Auffassung vertritt der deutsche Gesetzgeber, welcher eine staatliche Einflußnahme für unentbehrlich hält. Siehe dazu in Kapitel 8.4.3.

[113] NR: GP XX RV 1999 AB 2065 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP, 2

unrechtmäßig erlangten privaten Schlüssels abschließt und so den Anschein erweckt, der rechtmäßige Signaturschlüsselinhaber würde beabsichtigen, sich rechtlich zu binden. Eine derartige Kompromittierung liegt nicht erst bei tatsächlicher Ingebrauchnahme des einem anderen zugeordneten Schlüssels vor, sondern bereits bei dessen unbefugter Kenntnisnahme.

7.4 § 3 - Nichtdiskriminierungsklausel - Zulässigkeit der Verwendung elektronischer Signaturen

Die in Artikel 5 Abs. 2 der Richtlinie über elektronische Signaturen zum Ausdruck kommende Nichtdiskriminierungsklausel wurde mehr oder weniger wortwörtlich vom österreichischen Gesetzgeber übernommen. § 3 statuiert demzufolge die rechtliche Wirksamkeit von elektronischen Signaturen im Rechts- und Geschäftsverkehr und deren grundsätzliche Zulässigkeit als gerichtliches Beweismittel. Ein generelles Verbot bzw. eine generelle Nichtbeachtung ist demnach unzulässig, solange dies mit der Begründung erfolgt, die Signatur liege nur in elektronischer Form vor, beruhe nicht auf einem qualifizierten Zertifikat[114], basiere nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter[115] ausgestellten Zertifikat oder sei nicht von einer sicheren Signaturerstellungseinheit[116] erstellt worden. Diese Feststellungen gelten für den formfreien Bereich, dem jedoch die Mehrzahl der tagtäglich abzuwickelnden Geschäfte zuzuordnen ist. Bloß „allgemeine Rechtswirkungen“ entfalten demnach sämtliche am Markt zum Angebot stehenden Signatur- und Zertifizierungsverfahren und nicht nur die dem Signaturgesetz folgend als „sicher“ geltenden. Ein Mindestmaß bzw. -standard betreffend Sicherheit ist dabei nicht vorgesehen. Im Rahmen der freien gerichtlichen Beweiswürdigung ist je nach Qualitäts- und Sicherheitsstufe der Signatur ein entsprechendes Maß an damit verbundenen Rechtswirkungen zu bestimmen.

---

[114] siehe § 5 SigG und Anhang I SigRl

[115] siehe § 17 SigG

[116] siehe § 18 SigG und Anhang III SigRl

Die Zertifizierungsdiensteanbieter verfügen aus marktwirtschaftlichen Gründen bereits jetzt über ein breites Angebot an unterschiedlichen Zertifikatsklassen der Datakom, wie z.B. über ein Light-, Medium-, Strong- und Premium-Zertifikat, und unterschiedlichen Sicherheitsstufen, wobei etwa kein Zertifikat ausgestellt wird, bloß ein einfaches oder ein sicheres. Aufgrund der mit Erstellung und Zuteilung einer Signatur bzw. eines Zertifikats zwangsläufig verbundenen Kosten wird sich der Nutzer je nach dem beabsichtigten Geschäftsumfang für ein Signaturverfahren mit einem bestimmten Sicherheitslevel entscheiden. Freilich steht es im privaten Rechtsverkehr den jeweiligen Vertragsparteien offen, sich für die Anwendbarkeit des Signaturgesetzes zu entschließen oder auch die Zulässigkeit von elektronischen Unterschriften in ihren wechselseitigen Geschäftsbeziehungen generell auszuschließen.

7.5 § 4 - Besondere Rechtswirkungen sicherer elektronischer Signaturen - Gleichsetzung mit der eigenhändigen Unterschrift

Die wichtigste Errungenschaft des Signaturgesetzes wie auch der Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen ist in der Gleichstellung elektronischer Signaturen mit eigenhändigen Unterschriften zu sehen. Demzufolge müssen die durch die nationale Rechtsordnung mit einer eigenhändigen Unterschrift verbundenen besonderen Rechtswirkungen auch sicheren bzw. fortgeschrittenen elektronischen Signaturen zuerkannt werden. Aufgrund ihres zentralen Stellenwertes wird der Gesetzestext im folgenden vollinhaltlich angeführt:

§ 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 (§ 1364 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.

7.5.1 Form der Verträge in der österreichischen Rechtsordnung

Die österreichische Rechtsordnung ist geprägt vom Prinzip der Formfreiheit laut § 883 ABGB[117], wonach *„ein Vertrag mündlich oder schriftlich; vor Gerichte oder außerhalb desselben; mit oder ohne Zeugen errichtet werden kann. Diese Verschiedenheit der Form macht, außer den im Gesetze bestimmten Fällen, in Ansehung der Verbindlichkeit keinen Unterschied."* Weiters bestimmt § 886 ABGB[118], dass *„ein Vertrag, für den Gesetz oder Parteiwille Schriftlichkeit bestimmt, durch die Unterschrift der Parteien, oder ..., zustande kommt. Der schriftliche Abschluss des Vertrages wird durch gerichtliche oder notarielle Beurkundung ersetzt. Eine Nachbildung der eigenhändigen Unterschrift auf mechanischem Wege ist nur da genügend, wo sie im Geschäftsverkehr üblich ist."*

[117] Dittrich/Tades, ABGB[35], Wien 1999, § 883 samt Erläuterungen

Bestimmen weder individuelle Parteienvereinbarung noch generelle Norm Gegenteiliges, so kann grs. jede beliebige Form für einen gültigen Vertragsabschluß gewählt werden. Ist jedoch ein bestimmtes Formerfordernis zwingend vorgesehen, so haben die Parteien des jeweiligen Vertrages dieses einzuhalten. Im entgegengesetzten Fall entbehrt das zwischen den Vertragsparteien abgeschlossene Rechtsgeschäft jeglicher Rechtsgültigkeit. Es entfaltet grundsätzlich keine Bindungswirkung, die Erfüllung kann weder eingefordert noch eingeklagt werden. Wurde auf Grundlage eines formungültig abgeschlossenen Vertrages bereits geleistet, so kann dies ebensowenig zurückgefordert werden, da es sich um eine sogenannte Naturalobligation nach § 1432 ABGB handelt. Die Erfüllung der eingegangenen Verpflichtung ist demnach nicht einklagbar, sehr wohl aber erfüllbar. Ein eventuell vorliegender Formmangel wird durch die tatsächliche Leistung des Versprochenen geheilt. Im gegebenen Zusammenhang wird von einer bestehenden Leistungsverbindlichkeit ausgegangen, welche einerseits zwar auf einem mit Nichtigkeit behafteten Rechtsgeschäft beruht, andererseits aber sowohl Schadenersatz- wie auch Bereicherungsansprüche von vornherein ausschließt.

7.5.2 Gesetzliches Schriftformerfordernis

Der Zweck gesetzlicher Formvorschriften liegt in Übereilungsschutz, Beweiserbringung, Gläubigerschutz, Offenkundigkeit, Sicherung sachkundiger Beratung, Verbraucherschutz, uvm. Gesetzlich vorgeschrieben ist die Schriftform im Sinne des § 886 ABGB bei der Verpflichtungserklärung des Bürgen nach § 1346 Abs. 2 ABGB[119], der Rücktrittserklärung des Verbrauchers von einem Haustürgeschäft nach § 3 KSchG[120], der Einräumung von

[118] Dittrich/Tades, ABGB[35], Wien 1999, § 886 samt Erläuterungen

[119] Allgemeines Bürgerliches Gesetzbuch [Anlage des kaiserlichen Patents vom 1.6.1811, JGS. Nr. 946]

[120] Bundesgesetz vom 8. März 1979, mit dem Bestimmungen zum Schutz der Verbraucher getroffen werden (Konsumentenschutzgesetz - KSchG), BGBl. Nr. 140/1979

Wohnungseigentum nach § 2 Abs. 2 und § 12 Abs. 2 WEG[121], dem Abschluss und der Auflösung eines befristeten Mietvertrages nach § 29 MRG[122] und in vielen anderen Fällen.

Dem gesetzlichen Schriftformerfordernis wird durch Einhaltung der einfachen Schriftform entsprochen. Dabei muss die Unterschrift eigenhändig gefertigt sein, der Text selbst kann auch auf der Schreibmaschine oder auf dem PC geschrieben sein. Die Errichtung eines Notariatsaktes entfaltet besondere urkundliche Beweiskraft und ist beispielsweise verpflichtend vorgesehen in den Fällen des § 1 NZwG[123] und in Normen des GmbHG[124].

7.5.2.1 Verpflichtungserklärung des Bürgen

§ 1346 Abs. 2 ABGB[125] bestimmt im einzelnen, dass *„es zur Gültigkeit des Bürgschaftsvertrages erforderlich ist, dass die Verpflichtungserklärung des Bürgen schriftlich abgegeben wird“*. Im Rahmen dieser Vereinbarung hat sich der Bürge gegenüber dem Gläubiger zu verpflichten, für den Fall der Nichterfüllung einer konkreten Verbindlichkeit durch den ersten Schuldner für dessen Befriedigung zu sorgen. Das Schriftlichkeitserfordernis gilt ausschließlich für die Verpflichtungserklärung des Bürgen, nicht aber für die Annahmeerklärung durch den Gläubiger, welche ohne weiteres auf mündliche oder auch konkludente Weise erfolgen kann. Ebensowenig bedarf eine Abänderung der Bürgschaftserklärung der Schriftlichkeit, soweit dadurch die Haftung des Bürgen weder erweitert noch verschärft wird. Die Aufhebung als solche ist ebenso formfrei.

---

121 Bundesgesetz vom 1. Juli 1975 über das Eigentum an Wohnungen und sonstigen Räumlichkeiten (Wohnungseigentumsgesetz 1975 - WEG 1975), BGBl. Nr. 417/1975

122 Bundesgesetz vom 12. November 1981 über das Mietrecht (Mietrechtsgesetz - MRG), BGBl. Nr. 520/1981

123 Gesetz RGBl 1871/76 betreffend das Erfordernis der notariellen Errichtung einiger Rechtsgeschäfte

124 Gesetz vom 6. März 1906 über Gesellschaften mit beschränkter Haftung (GmbHG), RGBl. 1906/58

Für die Bürgschaft gelten die Grundsätze von Akzessorietät und Subsidiarität. Einerseits hängen Entstehung, Weiterbestand und Umfang der Bürgschaftsschuld vom tatsächlichen Bestand der Hauptschuld ab, und andererseits hat der Bürge erst bei nachgewiesener Nichterfüllung durch den Hauptschuldner zu leisten. Die Einwilligung des Hauptschuldners ist bei Begründung einer Haftungsübernahme nicht erforderlich. An das Schriftformerfordernis gebunden sind Personen, die als Bürge und Zahler, als Ausfallsbürge oder als Entschädigungsbürge auftreten. Aus der Bürgschaftserklärung muss lediglich der Bürgschaftswille, d.h. der Wille, für eine fremde Schuld einstehen zu wollen, eindeutig und unmittelbar hervorgehen. Dies erfordert idR die Angabe der wesentlichen Merkmale der Bürgschaftsverpflichtung, worunter im wesentlichen die Bezeichnung des Gläubigers, des Hauptschuldners und der konkreten Schuld zu verstehen sind. Handelt es sich auf Seiten des Bürgen um ein Handelsgeschäft, d.h. ist dieser Vollkaufmann iSd HGB, so ist gemäß § 350 HGB iVm §§1ff, § 343 und §§ 349ff die Bestimmung des § 1346 Abs. 2 nicht anzuwenden. Tritt jemand als Scheinkaufmann auf, so hat sich dieser ebenfalls an das Erfordernis der Schriftlichkeit als gebunden zu erachten.

Abs. 2 wird im österreichischen Recht analog angewandt auf den Garantievertrag nach § 880 a ABGB. Im Rahmen dieses Rechtsgeschäftes wird einem Begünstigten zugesichert, ihm durch einen Dritten eine Leistung zu erbringen. Darin liegt auch der grundlegende Unterschied zur Bürgschaft. Während durch diese die Erfüllung einer Drittschuld gesichert wird, zielt eine Garantie auf die Erbringung einer Leistung eines Dritten. Dies hat wiederum zur Folge, dass durch den Garantievertrag eine eigenständige, vom Bestand der Hauptschuld unabhängige und abstrakte Verbindlichkeit entsteht.

Zu überprüfen wäre in diesem Zusammenhang, ob es aufgrund der Ähnlichkeit dieser beiden Rechtsinstitute nicht angebracht wäre, in diesem Bereich allgemein die Unzulässigkeit der elektronischen Signierung festzulegen. Meines Erachtens dafür sprechen würde die schwierige

[125] siehe *Dittrich/Tades*, ABGB[35], Wien 1999 und *Rummel*, Kommentar zum Allgemeinen bürgerlichen

Abgrenzung zwischen dem Rechtsinstitut der Bürgschaft und der Garantie und das oftmalige Vorliegen von Mischformen. Wird hauptsächlich auf die Abdeckung des Risikos der Zahlungsunfähigkeit des Hauptschuldners gezielt, ist in der Regel ein Bürgschaftsvertrag anzunehmen. Liegt der Hauptzweck in der Abdeckung des Risikos von eventuell in Zukunft entstehenden Rechtsunsicherheiten und Rechtsstreitigkeiten so liegt eher ein Garantievertrag vor. Dabei handelt es sich lediglich um Entscheidungs- und Auslegungshilfen, keinesfalls um verbindliche Trennkriterien.

7.5.2.2 Einräumung von Wohnungseigentum

§ 2 Abs. 2 Z 1 des Wohnungseigentumsgesetzes 1975 idgF.[126] kurz WEG, sieht zur erstmaligen Einräumung von Wohnungseigentum eine schriftliche Vereinbarung zwischen dem künftigen Wohnungseigentümer und allen anderen Miteigentümern vor. Diese Vorschrift ist zwingender Natur. Für die bloße Übertragung bzw. den Erwerb von Wohnungseigentum von einem Vormann gilt die genannte Formvorschrift nicht. Sehr wohl ist die Schriftlichkeit jedoch von zwingender Natur beim Vorvertrag, d.h. für das Versprechen Wohnungseigentum einzuräumen, für einen Eigentumserwerb an bloßen Liegenschaftsanteilen, falls dieser in sachlichem und zeitlichem Zusammenhang mit zu begründendem Wohnungseigentum erfolgt und auch für all jene Vereinbarungen, die den konkreten Umfang des Wohnungseigentums betreffen.[127]

Gesetzbuch[2], 2. Band, Wien 1992, § 1346 samt Erläuterungen

[126] siehe *Würth/Zingher*, Miet- und Wohnrecht[20], Wien 1997 und *Rummel*, Kommentar zum Allgemeinen bürgerlichen Gesetzbuch[2], 2.Band, Wien 1992 und *Dittrich/Tades*, ABGB[35], Wien 1999, § 2 WEG samt Erläuterungen

[127] siehe ausführlich dazu OGH 29.4.1975, 5 Ob 61, 62/75, MietSlg-WE 639

7.5.2.3 Befristete Mietverträge

Eine weitere, sehr detaillierte Regelung, die das Erfordernis der Schriftlichkeit nach § 886 ABGB ausdrücklich vorsieht, findet sich in § 29 MRG,[128] welcher Abschluss, Verlängerung und Auflösung eines befristeten Mietvertrages zum Regelungsgegenstand hat. Demzufolge sind Mietverträge, *„die durch den Ablauf der bedungenen Zeit ohne Kündigung erlöschen“*, schriftlich abzuschließen. Dabei handelt es sich um sogenannte Bestandverhältnisse mit unbedingtem Endtermin, zu deren Erlöschen es weder einer gesonderten Erklärung noch der Angabe besonderer Gründe bedarf. Die Vertragsteile sind während der gesamten Dauer des Mietverhältnisses gebunden, lediglich in besonders gelagerten Fällen ist eine vorzeitige Auflösung möglich. In Abs. 1 der genannten Norm erfolgt eine Aufzählung der besonderen Endigungsgründe, in Abs. 1 Z 3 sowie Abs. 2 eine Regelung der durchsetzbaren Befristungen und schließlich in Abs. 3 eine Regelung betreffend Vertragsverlängerung. Besonders hervorzuheben ist die auch weiterhin in vollem Umfang bestehende Anwendbarkeit der sonstigen Kündigungsvorschriften des MRG. Von § 29 völlig unberührt bleiben die allgemeinen Endigungsgründe, wie etwa die einverständliche Auflösung, der Rücktritt vom Mietvertrag nach § 918 ABGB oder die Irrtumsanfechtung nach §§ 871ff ABGB. Um die rechtliche Durchsetzbarkeit von in einem Mietvertrag vorgesehenen Befristungen zu gewährleisten, ist die Schriftform, d.h. die Unterfertigung der gegenständlichen Urkunde durch alle Vertragsteile, unbedingt erforderlich. Direkt aus dem Vertrag ergeben muss sich insbesondere ein im vorhinein zu bestimmender Endtermin, entweder durch Angabe eines konkreten Datums oder einer abzulaufenden Frist.

7.5.2.4 Maklerverträge

[128] siehe *Würth/Zingher*, Miet- und Wohnrecht[20], Wien 1997 und *Rummel*, Kommentar zum Allgemeinen bürgerlichen Gesetzbuch[2], 2. Band, Wien 1992 und *Dittrich/Tades*, ABGB[35], Wien 1999, § 29 MRG samt Erläuterungen

Im Bereich des Maklerwesens ist § 31 KSchG[129] zu erwähnen, der zum Schutz des Verbrauchers vor unliebsamen Überraschungen zwingend die Schriftlichkeit und Ausdrücklichkeit von Bestimmungen im Rahmen eines Maklervertrages anordnet. Demzufolge ist der Abschluss wie auch die Verlängerung eines Alleinvermittlungsauftrages, worunter die Verpflichtung des Auftraggebers, keine anderen Makler für das zu vermittelnde Geschäft zu beauftragen, zu verstehen ist, lediglich in schriftlicher und dem Bestimmtheitserfordernis genügender Form rechtswirksam. Grundsätzlich hat der Makler keinen Anspruch auf Ersatz von Aufwendungen, die in den gewöhnlichen Geschäftsbetrieb fallen, vielmehr wird er nur bei Zustandekommen des auf seine Tätigkeit hin vermittelten Rechtsgeschäftes entlohnt. Wird für besondere, über das übliche Maß hinausgehende Aufträge Aufwandersatz vereinbart, so hat dies ebenso schriftlich zu erfolgen. Vom Schriftformerfordernis betroffen ist nur die jeweilige Entgeltsvereinbarung, nicht aber die Vereinbarung über den zusätzlichen Auftrag. Dem Erfolgsprinzip fremd sind Vereinbarungen über die Leistung einer Provision auch in den Fällen, in denen es zu keiner Vermittlung kommt. Diese in § 15 Maklergesetz taxativ aufgezählten Fälle bedürfen ebenso der Schriftform.

Wird in einem der genannten Fälle von der gesetzlichen Vorgabe des § 31 KSchG abgewichen, so hat dies nach herrschender Meinung absolute Nichtigkeit zur Folge. Dies bedeutet im einzelnen, dass sich einerseits der Makler nicht auf seinen bloß mündlich begründeten Entgeltanspruch berufen, andererseits aber auch der Verbraucher sich nicht auf eine bloß mündliche Vereinbarung stützen kann. Dies entspricht ganz offensichtlich weder dem Schutzzweck des Maklergesetzes noch des Konsumentenschutzgesetzes.

7.5.3 Gewillkürtes Schriftformerfordernis

[129] siehe *Josesnik-Wehrle/Lehofer/Mayer*: Konsumentenschutzgesetz, Wien 1997, § 31 KSchG samt Erläuterungen

Haben die Vertragsparteien eine bestimmte Form, etwa Schriftlichkeit, als Gültigkeitserfordernis des zwischen ihnen abzuschließenden Rechtsgeschäftes vereinbart, was im Rahmen von Allgemeinen Geschäftsbedingungen erfolgen kann, so bleibt es ihnen überlassen, jederzeit einvernehmlich wieder davon abzuweichen. Demzufolge kann von einer Schriftformvereinbarung auch durch nur konkludente Willenserklärung abgegangen werden. Ist man sich jedoch bezüglich des Formerfordernisses der Schriftlichkeit einig, so kommt der Vertrag § 884 ABGB folgend erst durch Unterzeichnung des Vertrages durch alle Vertragsparteien zustande. Vor diesem Zeitpunkt entfaltet dieser keinerlei Rechtswirkung. Schriftlichkeit in diesem Zusammenhang bedeutet Unterschriftlichkeit, d.h. das Setzen der eigenhändigen Unterschrift unter einen ebenfalls von Hand geschriebenen oder gedruckten Text. Weder Telegramm noch Fax reichen grundsätzlich für die Erfüllung des Schriftformerfordernisses aus - trotz etwaig darauf dargestellter eigenhändiger Unterschrift. Im Rahmen der Privatautonomie bleibt es den Geschäftspartnern natürlich überlassen, auch diesen auf elektronischem Wege übermittelten Erklärungen die Rechtswirkung einer eigenhändigen Unterschrift beizumessen.

7.5.4 Konkretes Ausmaß der Gleichstellung

Art 1 Satz 2 der Richtlinie über elektronische Signaturen überlässt es den Mitgliedstaaten zu bestimmen, ob und in welchen Bereichen sie die elektronische Form konkret einführen wollen; einzelstaatliche Vorschriften betreffend Form, Inhalt und Gültigkeit von Verträgen bleiben von der Richtlinie unberührt. Die besonderen Rechtswirkungen einer elektronischen Signatur können demzufolge durch Gesetz oder Parteienvereinbarung ausgeschlossen werden.

Faktisch hätte nun der nationale Gesetzgeber die durch Art 1 eingeräumte Befugnis, in allen erdenklichen Fällen Ausnahmen vorzusehen und so die Anwendungsmöglichkeiten des Geschäftsabschlusses auf elektronischem Weg erheblich einzuschränken. In den Bereichen, in denen von dieser Möglichkeit nicht Gebrauch gemacht wird, wird § 4 Abs. 1 des Signaturgesetzes entsprechend dem Schriftformerfordernis durch eine elektronische

Unterschrift Genüge getan. Diese Rechtsfolge gilt sowohl für den zivilrechtlichen wie für den verwaltungsrechtlichen Bereich, d.h. im Rechts- und Geschäftsverkehr zwischen Bürgern untereinander wie auch zwischen Bürgern und Behörden.

7.6 Art 9 - 11 E-Commerce-Richtlinie

In diesem Zusammenhang ist die Richtlinie über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs, kurz E-Commerce-Richtlinie oder Haftungs-Richtlinie, zu erwähnen, welche die scheinbare Entscheidungsfreiheit der Mitgliedstaaten in nicht unerheblichem Maße einschränkt. Diese behandelt - neben den Bereichen der elektronischen Dienstleistungsfreiheit und der Zuständigkeit nationaler Gesetzgebung, der elektronischen Werbefreiheit, der Rechtsdurchsetzung im elektronischen Markt Internet - in Art 9 bis 11 auch den Bereich des elektronischen Vertragsabschlusses.

Art 9 der Richtlinie enthält die sogenannte „Ermöglichungsklausel". Diese bestimmt im wesentlichen, dass die Mitgliedstaaten den wirksamen Abschluss elektronischer Verträge zu ermöglichen haben. Nationale Bestimmungen, welche den elektronischen Vertragsabschluß untersagen bzw. einschränken, sind aufheben und allfällige Behinderungen elektronischer Medien zu beseitigen. Elektronischen Verträgen darf keine eingeschränkte Rechtswirkung beigemessen werden; spezifische Formvorschriften, die mittels elektronischer Kommunikation nicht erfüllt werden können, sind so weit als möglich zu verhindern.

7.6.1 Art 9 Abs. 2 - Ausnahmen von Art 9 Abs. 1

Gemäß Abs. 2 der genannten Regelung sind Ausnahmen davon nur sehr eingeschränkt in gewissen sensiblen Bereichen möglich. Während die Richtlinie nur *„Verträge"* als solche nennt, spricht der österreichische Gesetzestext aus Gründen der Systemkohärenz allgemein von *„Willenserklärungen, Rechtsgeschäften und Eingaben"*. Die Mitgliedstaaten haben der Kommission darüber Bericht zu erstatten, inwieweit sie den Ausnahmekatalog der

Richtlinie ausschöpfen, d.h. bei welchen Rechtsgeschäften eine elektronischen Signatur als nicht ausreichend erachtet wird. Der, nach Meinung der Kommission nicht abschließende Ausnahmenkatalog wurde in § 4 Abs. 2 SigG weitgehend übernommen:

In den im folgenden genannten Bereichen wird das Erfordernis der Unterschriftlichkeit und das Abstellen auf die Papierform weiterhin beibehalten. Wird ungeachtet dessen elektronisch signiert, so ist die konkrete formgebundene Willenserklärung unwirksam, was jedoch nicht bedeuten muss, dass damit keine Rechtswirkungen einhergehen können. Wie bereits oben im Zusammenhang mit der Nichteinhaltung sonstiger gesetzlich oder vertraglich vereinbarter Formvorschriften erwähnt, ist der Bestand einer Naturalobligation anzunehmen, d.h. die tatsächliche Leistung heilt den Formmangel, weshalb eine Rückabwicklung generell ausgeschlossen ist. Dient das Formerfordernis jedoch dem Gläubigerschutz bzw. öffentlichen oder Verkehrsinteressen, so ist zu differenzieren. In diesen Fällen liegt ein formungültiges Rechtsgeschäft vor, welches trotz ordnungsgemäßer Erbringung der vereinbarten Leistung keine Gültigkeit erlangt. Der aufgrund einer nicht bestehenden Rechtsgrundlage Leistende hat die Möglichkeit der Geltendmachung von Rückforderungs- und Bereicherungsansprüchen. Würde man auch hier das Bestehen einer Naturalobligation annehmen, so könnten die statuierten Formvorschriften leicht umgangen und der verfolgte Formzweck vereitelt werden.[130]

7.6.1.1 Familien- und erbrechtliche Rechtsgeschäfte (Z 1)

Z 1 des Gesetzes nennt *„Rechtsgeschäfte im Bereich des Familien- und des Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind“*, da hier vermögensrechtliche Belange besonders schutzwürdiger Personen betroffen sind und ein Beweis oftmals nur schwer zu erbringen sein wird. Laut Richtlinie können „alle“ Rechtsgeschäfte des Familien- und Erbrechts in den Ausnahmenkatalog aufgenommen

werden. Laut österreichischem Signaturgesetz sind von dieser Ausnahme jedoch nur solche erfasst, die der einfachen Schriftlichkeit oder einer strengeren Form, wie etwa der Eigenhändigkeit bedürfen. Z 1 schränkt den Regelungsbereich der E-Commerce-Richtlinie erheblich ein, was im Hinblick auf das erklärte Ziel der Richtlinie, die Zulässigkeit elektronischer Verträge zu fördern, ohne weiteres zulässig ist. Demzufolge ist etwa ein Testament in elektronischer Form unwirksam, da sowohl Text wie auch Unterschrift mit eigener Hand zu schreiben sind. Genaugenommen ist die Bezugnahme auf ein strengeres Formerfordernis eigentlich überflüssig, da ohnehin nur die Gleichstellung der sicheren elektronischen Signatur mit der einfachen Schriftlichkeit normiert ist und nicht etwa auch mit Notariatsakt, Beurkundung oder ähnlichem.

7.6.1.2 Willenserklärungen und Rechtsgeschäfte mit besonderen Formerfordernissen (Z 2 und 3)

Z 2 betrifft *„Willenserklärungen oder Rechtsgeschäfte, die zu ihrer Wirksamkeit an die Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsaktes gebunden sind“*. Ebenso unwirksam sind elektronische Signaturen - entsprechend Z 3 - im Bereich von *„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 bedürfen“*. Z 2 und 3 sollen vor allem eine fachkundige, unparteiliche Beratung und Belehrung der Betroffenen sicherstellen, was bei elektronischer Form nicht in demselben Ausmaß gegeben ist.

---

130 *Koziol/Welser*, Grundriß des bürgerlichen Rechts I[10], Wien 1995, S. und OGH vom 26.2.1996, 4 Ob

In diesem Zusammenhang besonders kritisiert wurde seitens des Österreichischen Rechtsanwaltskammertages die sehr weite Grenzziehung der zulässigen Ausnahmen.[131] Während der Richtlinienvorschlag über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt[132] in seinem Art 9 Abs. 2 lit. a lediglich *„Verträge, die die Mitwirkung eines Notars erfordern"* von Abs. 1 leg.cit. ausnahm, ging das Gesetz weit über den vorgegebenen Rahmen hinaus. Wie bereits dargestellt, fallen laut österreichischer Gesetzeslage auch sämtliche *„Willenserklärungen oder Rechtsgeschäfte, die zu ihrer Wirksamkeit an de Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts gebunden sind"* unter den Ausnahmekatalog. Während die Mitwirkung einer öffentlichen Person, wie die eines Notars, besonderen Beweissicherungszwecken und Verbraucherschutzzwecken dient, wird mittels einer „einfachen" Beglaubigung bloß die inhaltliche Übereinstimmung von Kopie und Urschrift und die Echtheit der Unterschrift auf formelle Weise bestätigt. Diese Zielrichtung kann durch die elektronische Signatur und den damit verbundenen besonders strengen Sicherheitsvorkehrungen auf bestmögliche Weise verfolgt werden, denn die elektronische Signatur gilt als vor Fälschung und Verfälschung sicherer als die bisher übliche eigenhändige Unterschrift.

Sowohl durch einen Notariatsakt als auch durch eine gerichtliche wie notarielle Beurkundung wird die Funktion der Belehrung in den Vordergrund gerückt. Unterer ersteren ist die Beurkundung von Rechtsgeschäften und Rechtserklärungen zu verstehen, unter zweiteren die in einem Protokoll, einem Amtsvermerk oder einer Amtsbestätigung enthaltene Bestätigung von Tatsachen und Erklärungen, welche direkt in Anwesenheit des Notars bzw. des Gerichtes stattfinden bzw. abgegeben werden.

518/96 in RdW 1997, S. 12 und OGH vom 7.7.1988, 6 Ob 612/88 in ZfRV 1989, S. 51

131 *Huemer/ Saxinger/ Baumann & Partner*, Bundesgesetz über elektronische Signaturen, AnwBl 1999, S. 392ff

Z 3 verringert den Bereich der zulässigen Ausnahmen durch die Einschränkung auf Verträge, die zwecks ihrer Eintragung in ein öffentliches Register der öffentlichen Form bedürfen. Dies ist etwa der Fall im Rahmen des § 12 HGB, wonach die Anmeldung zur Eintragung in das Firmenbuch durch einen Bevollmächtigten nur in Verbindung mit einer öffentlich beglaubigten Vollmacht udgl. möglich ist. Diese Vorschrift bezweckt, zum einen den Schutz desjenigen, der eingetragen werden möchte, und zum anderen die Verhinderung der Eintragung nicht mit der Realität übereinstimmender Tatsachen. Wie auch bei Z 2 spielen hier Übereilungsschutz, Sachkundigkeit der Belehrung und Identitätsfeststellung eine wichtige Rolle.[133]

In der nunmehr aktuell verabschiedeten Ausformung des Art 9 der E-Commerce-Richtlinie wurden die Ausnahmetatbestände des lit. a und b kurz zusammengefasst, wonach für *„Verträge, bei denen die Mitwirkung von Gerichten, Behörden oder öffentliche Befugnisse ausübenden Berufen gesetzlich vorgeschrieben ist“*, spezifische Formvorschriften aufrechterhalten werden können, denen mittels einer elektronischen Signatur nicht nachgekommen werden kann. Durch die erfolgte Umformulierung der Richtlinie kann das Signaturgesetz nun als übereinstimmend mit der europarechtlichen Vorgabe angesehen werden.

7.6.1.3 Bürgschaftserklärung (Z 4)

Letztere Ziffer 4 des Signaturgesetzes nimmt Bezug auf die vorhin erwähnten Bürgschaftserklärungen eines Nicht- oder Minderkaufmannes nach § 1364 Abs. 2 ABGB. Auch hier wird der von der Richtlinie einer Einschränkung zugängliche Regelungsrahmen bei weitem nicht voll ausgeschöpft, da in Art 9 lit. c nicht nur Bürgschaftsverträge, sondern auch *„Verträge über Sicherheiten, die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit eingegangen werden“* Erwähnung finden. Diese

[132] Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, KOM (1999) 427 endg., Art 9

Ausnahme versucht man damit zu rechtfertigen, dass der künftige Bürge vor Übereilung geschützt und aufgrund des Eingehens eines gewissen Risikos in besonderer Weise gewarnt werden sollte. Doch würde meiner Meinung nach wohl auch eine elektronische Signatur und der mit ihr verbundene Aufwand, d.h. der gesonderte Einsatz einer Chip-Karte, die Eingabe des PIN-Codes und die vorherig zu erfolgende Belehrung über die mit der Aktivierung eines elektronischen Signaturverfahrens verbundenen Rechtsfolgen durch den Zertifizierungsdiensteanbieter, näher ausgeführt in § 20 SigG, diese Funktionen erfüllen.

7.7 Beweiswirkungen

7.7.1 § 294 ZPO - Echtheitsvermutung unterschriebener Privaturkunden

Grundsätzlich unterliegt die Feststellung der inhaltlichen Richtigkeit einer Privaturkunde der freien gerichtlichen Beweiswürdigung. Als Privaturkunden gelten vereinfacht ausgedrückt all diejenigen Schriftstücke, die nicht den öffentlichen zuzuordnen sind. Zu diesen wiederum zählen die von einer nationalen öffentlichen Behörde innerhalb ihrer Amtsbefugnisse und die von einer mit öffentlichem Glauben versehenen Person innerhalb ihrer Geschäftskreises errichteten, die durch gesetzliche Vorschriften als öffentlich erklärten und schließlich auch die ausländischen öffentlichen Urkunden. Um als Urkunde zu gelten, genügt die Feststellung bestimmter Tatsachen in Papierform, eine Unterschrift ist dabei nicht erforderlich.

Die einzige Beweisregel betreffend Privaturkunden statuiert § 294 ZPO, welche lautet: *„Privaturkunden begründen, sofern sie von den Ausstellern unterschrieben oder ..., vollen Beweis dafür, dass die in denselben enthaltenen Erklärungen von den Ausstellern herrühren“.*[134] Dies impliziert auf keinen Fall auch die Vermutung des Vorliegens der

[133] *Jud/ Högler-Pracher*: Die Gleichsetzung elektronischer Signaturen mit der eigenhändigen Unterschrift, ecolex 1999, S. 612ff

[134] *Rechberger*, Kommentar zur ZPO, Wien 1994, S. 758

inhaltlichen Richtigkeit, d.h. der Beweiskraft, einer Urkunde. Die in der Urkunde enthaltenen Angaben über Tatsachen und Vorgänge, wie auch nichtunterschriebene Privaturkunden unterliegen weiterhin der freien gerichtlichen Beweiswürdigung. Im Rahmen des § 294 ZPO gilt ein unterschriebener Text als echt, d.h. als vom Unterzeichner stammend, soweit die Echtheit der Unterschrift erwiesen bzw. unbestritten ist. Im Rahmen der Beweislastumkehr ist derjenige, der die Falschheit eines unterzeichneten Erklärungsinhaltes behauptet, dazu aufgerufen, darüber Beweis zu führen. Die Umkehr der ansonsten geltenden Beweislastregeln gilt, um es noch einmal zu betonen, nur hinsichtlich der Echtheit des Inhalts, nicht jedoch auch hinsichtlich der Echtheit der Unterschrift.[135]

7.7.2 § 4 Abs. 3 SigG - Echtheitsvermutung signierter Dokumente

Gemäß Abs. 3 ist die qualifizierte Echtheitsvermutung für den Erklärungsinhalt bei unterschriebenen Privaturkunden auch auf elektronische Dokumente anzuwenden, die mit einer sicheren elektronischen Signatur versehen wurden. Dies bedeutet im einzelnen, dass bei unbestrittener Echtheit der elektronischen Signatur auch die Echtheit des elektronischen Dokuments vermutet wird. Die darin enthaltenen Erklärungen werden dem Inhaber des privaten Signaturschlüssels in rechtlich bindender Weise zugerechnet. Der Beweis des Gegenteils bleibt natürlich jederzeit möglich. Von der Vermutung der Echtheit nicht erfasst ist die Unterschrift[136] als solche. Wird deren Echtheit bestritten, so ist dies im Streitfall vom Beweisführer zu belegen. D.h. es wird nicht gleichzeitig die Vermutungsregel aufgestellt, das die Signaturerstellungsdaten vom dazu berechtigten Inhaber benutzt wurden. Ausschließlich bei unbestrittener bzw. bewiesener Feststellung der Echtheit der Unterschrift gilt der dazugehörige Text als vom Unterzeichner stammend. In diesem Bereich ist der gerichtlichen

---

[135] siehe auch in *Stohanzl*, Zivilprozeßgesetze7, Wien 1995 und *Stohanzl*, Jurisdiktionsnorm und Zivilprozeßordnung14, Wien 1990 und *Fasching*, Lehrbuch des österreichischen Zivilprozeßrechts2, Wien 1990 und *Rechberger/ Simotta*, Grundriß des österreichischen Zivilprozeßrechts4, Wien 1994, jeweils §§ 292ff

[136] Für unterschriebene Privaturkunden normiert in § 312 ZPO.

Beweiswürdigung kein Entscheidungsspielraum eingeräumt.[137] Anders ausgedrückt, besteht nach österreichischer Rechtslage eine gesetzliche Vermutung der Integrität von elektronischen Willenserklärungen, nicht jedoch bezüglich der Identität des Signaturerstellers.

Aus dieser Bestimmung folgt die Gleichstellung der elektronischen Dokumente mit Privaturkunden im Zivilrecht, in strafrechtlicher Hinsicht fehlt bislang eine Gleichstellung mit dem Urkundenbegriff. Die Ausdehnung der qualifizierten Echtheitsvermutung der ZPO ist im Hinblick auf die bei der Signaturerstellung und -zuordnung einzuhaltenden hohen Sicherheitsanforderungen auf jeden Fall gerechtfertigt. Sichere elektronische Signaturen erlauben einen eindeutigen Rückschluss auf den jeweiligen Inhaber, da im Normalfall nur dieser selbst Zugriff auf seine Signaturerstellungsdaten hat. Im Falle einer Kompromittierung hat er das ihm zugeteilte Zertifikat unverzüglich sperren zu lassen, sodass nicht unbefugte Dritte Erklärungen in seinem Namen und auf seine Rechnung abzugeben imstande sind.
Beweisrechtlich gilt ein am Bildschirm dargestelltes elektronisches Dokument als Augenscheinsobjekt gemäß § 368 Abs. 1 ZPO; in ausgedruckter Form als nicht unterschriebene Urkunde.

7.8 § 4 Abs. 4 - Sicherheitsvermutung

§ 4 Abs. 4 folgend, *„treten die Rechtswirkungen der Abs. 1 und 3 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.“* Da grundsätzlich von der Einhaltung der Sicherheitsanforderungen nach dem Signaturgesetz ausgegangen wird, entfalten elektronische Signaturen in der Regel dieselben

[137] Anders die deutsche Rechtslage gemäß den Novellierungsbestrebungen der dtZPO, wonach entsprechend der herkömmlichen Anscheins- bzw. Duldungsvollmacht zwei Vermutungsregeln aufgestellt werden. Erstere ordnet eine elektronische Willenserklärung dem jeweiligen Signaturschlüssel-Inhaber zu. Zweitere statuiert sogar die Vermutung des Vorliegens einer Bevollmächtigung für den Fall, daß ein Dritter von den Signaturerstellungsdaten eines anderen Gebrauch gemacht hat. Siehe dazu Kapitel 8.5.1.2.

Rechtswirkungen wie eigenhändige Unterschriften. Unter anderem gilt auch der Inhalt einer mit einer elektronischen Signatur unterzeichneten Privaturkunde als echt - wie soeben dargelegt. Wird diese Sicherheitsvermutung widerlegt, so kommt § 4 nicht zur Anwendung. Denkbar sind etwa Fälle, in denen nachgewiesenermaßen der Algorithmus ausgeforscht, der Chipspeicher gebrochen, die Signaturerstellungseinheit ausgespäht oder diverse technische Manipulationen an Signaturhard- oder Software durchgeführt wurden.

In engem Zusammenhang mit dieser Bestimmung ist § 23 Abs. 3 SigG zu sehen, welcher die Voraussetzungen des Einstehenmüssens von Zertifizierungsdiensteanbietern näher ausführt. Ist etwa das Grundgeschäft aufgrund eines Formmangels als nichtig anzusehen und kann infolgedessen das bereits Geleistete vom Leistungsempfänger nicht mehr zurückgefordert werden, so ist die Inanspruchnahme des Zertifizierungsdienstanbieters bei Vorliegen der in § 23 normierten Haftungsvoraussetzung möglich und denkbar. Genaueres dazu unter Kapitel 7.28.5.

7.9 § 5 - Qualifizierte Zertifikate

Anhang I der Signaturrichtlinie entsprechend werden die an sogenannte *„qualifizierte Zertifikate“* gestellten Anforderungen im Rahmen des § 5 SigG ausformuliert. Vorweggenommen sei, dass Zertifikate lediglich auf die Stellung eines entsprechenden Antrages hin ausgestellt werden. Wird jedoch die Ausstellung eines im Angebotskatalog eines Zertifizierungsdiensteanbieters enthaltenen Zertifikats beantragt, so besteht insoweit Kontrahierungszwang auf Seiten des Anbieters. Da es sich dabei um ein herkömmliches Rechtsgeschäft handelt, sind die Vorschriften des ABGB anwendbar, vor allem auch im Hinblick auf die Geschäfts- und Handlungsfähigkeit. Ist der Antragsteller etwa nicht voll geschäftsfähig oder zumindest nicht in Bezug auf die beabsichtigten Einsatzmöglichkeiten des Zertifikats, so hat der Zertifizierungsdiensteanbieter von einer entsprechenden Ausstellung Abstand zu nehmen. Möglich ist auch die ausdrückliche Aufnahme des Vorliegens etwa der Minderjährigkeit oder einer Sachwalterschaft in das Zertifikat. Infolgedessen sind derartige

Beschränkungen der Geschäftsfähigkeit für jeden potentiellen Geschäftspartner des Zertifikatinhabers ersichtlich.[138]

7.9.1 Mindestinhalt

§ 5 SigG folgend haben Zertifikate einen bestimmten Mindestinhalt aufzuweisen, ansonsten ihnen die speziellen Sicherheitsvermutungen des Signaturgesetzes nicht zuerkannt werden. Zuallererst ist im Zertifikat selbst oder ansonsten im Zertifikatsverzeichnis die ausdrückliche Bezeichnung „qualifiziert" anzuführen. Zwingend vorgeschrieben ist weiters die Angabe des Namens des ausstellenden Zertifizierungsdiensteanbieters in unverwechselbarer und eindeutiger Weise. Dies hat vor allem den Zweck, im Falle von eventuell auftretenden Rechtsstreitigkeiten Probleme hinsichtlich der Passivlegitimation des Antragsgegners hintanzuhalten. Weiters muss der Staat, in dem der Diensteanbieter seine Niederlassung hat, angegeben sein, um die Anwendbarkeit der nationalen Haftungsvorschriften bestimmen zu können.

In das qualifizierte Zertifikat aufzunehmen sind - allgemein gesagt - sämtliche rechtserheblichen Eigenschaften zum Zwecke der Authentifizierung des Senders einer Nachricht. Auch spezielle Vertretungs- oder berufsrechtliche Befugnisse, also Tatsachenfragen im eigentlichen Sinne können in das Zertifikat aufgenommen werden, jedoch nur auf Verlangen des Zertifikatwerbers. Zum Zwecke der Zurordenbarkeit des Zertifikats zu seinem Inhaber innerhalb des Unternehmens eines Zertifizierungsdiensteanbieters ist der ebenso unverwechselbare Name des Signators bzw. ein Pseudonym anzuführen. Zweiteres ist als solches kenntlich zu machen und darf weder Verwechslungs- oder Täuschungsgefahr in sich bergen noch andere Namens- oder Kennzeichenrechte beeinträchtigen. Bei Vorliegen eines *„überwiegenden berechtigten Interesses"*[139], wie beispielsweise bei vermuteten

---

[138] NR: GP XX RV 1999 AB 2065 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP, 6

[139] siehe § 22 Abs 2 SigG

Rechtsverletzungen durch den Zertifikatsinhaber, hat die Aufdeckung des Pseudonyms nach den Grundsätzen des Datenschutzgesetzes zu erfolgen. Von zusätzlicher Bedeutung für die Unverwechselbarkeit der Person des Unterzeichners ist - neben der Erwähnung eventuell vorliegender Vertretungsverhältnisse und sonstiger rechtserheblicher Tatsachen und Eigenschaften - die Angabe der ihm allein zugehörigen Signaturprüfdaten.

Sinn und Zweck der Fixierung eines derartigen Mindestinhaltes eines qualifizierten Zertifikates liegt vor allem darin, den staatlichen Behörden auch im Bereich des Internet die Möglichkeit der Strafverfolgung zu bewahren. Diesem Erfordernis wird - wie soeben dargestellt - auch bei Angabe eines Pseudonyms entsprochen, da dieses einerseits die Wahrung der Anonymität in Alltagsgeschäften wahrt und andererseits unter bestimmten Voraussetzungen, wie etwa bei Vorliegen eines entsprechenden richterlichen Befehls, sehr wohl aufgedeckt werden kann. Das tatsächliche Vorliegen einer gewerberechtlichen oder berufsrechtlichen Befugnis, einer durch eine juristische oder natürliche Person eingeräumte Vertretungs- und Handlungsvollmacht oder einer sonstigen Zulassung ist vor Aufnahme in das Zertifikat durch den Diensteanbieter entsprechend zu überprüfen.[140] Derartige Angaben können wahlweise entweder direkt in das Hauptzertifikat oder in ein dazugehöriges Attribut-Zertifikat aufgenommen werden, wobei im letztgenannten Fall ersteres einen Hinweis auf zweiteres zu enthalten hat. Die Ausstellung des Attribut-Zertifikates kann selbstverständlich auch von einem zweiten Zertifizierungsdiensteanbieter übernommen werden. Denkbar und zweckmäßig ist es etwa im Falle ebengenannter gewerbe- und berufsrechtlicher Zulassungen, die Bestätigung ihres tatsächlichen Vorliegens dem jeweiligen öffentlich- oder privatrechtlichen Vertretungskörper zu überlassen, d.h. im konkreten der Notariatskammer, der Rechtsanwaltskammer, udgl.

Darüber hinaus ist das Anführen zusätzlicher Angaben im Hauptzertifikat bzw. im dazugehörigen Attribut-Zertifikat zulässig, solange die Funktionsfähigkeit und Sicherheit der

[140] Der Zertifikatsaussteller hat aber nur für die Richtigkeit der Angaben, d.h. für das tatsächliche Bestehen der Vertretungsmacht, zum Ausstellungszeitpunkt einzustehen. Eine Widerrufspflicht trifft diesen nur bei Bekanntwerden entgegenstehender Tatsachen, er ist aber nicht zu einer regelmäßigen Überprüfungsmöglichkeit verpflichtet. Schon aus diesem Grund ersetzt die Einsichtnahme in das Zertifikat nicht die Einsichtnahme in die öffentlichen Register, wie etwa Firmen- und Grundbuch.

Überprüfung nicht beeinträchtigt wird. Der Umfang des absolut notwendig erscheinenden Inhaltes wird im Einzelfall je nach konkretem Anwendungsbereich verschieden ausfallen.

7.9.2 Gültigkeitsdauer und Beschränkungen

Da Rechtsgültigkeit und Rechtswirksamkeit einer elektronischen Signatur unter anderem auf der Gültigkeit des zugehörigen Zertifikats beruhen, sind zudem die konkrete Gültigkeitsdauer desselben und eventuell vorliegende Beschränkungen des Anwendungsbereiches wie auch des Transaktionswertes anzuführen. Beginn und Ende des Gültigkeitszeitraumes haben sich an den technischen Gegebenheiten zu orientieren, um die Fälschungssicherheit der Zertifikate und der zugehörigen elektronischen Signaturen zu gewährleisten. Die in § 12 Abs. 3 SigV[141] vorgesehene maximale Gültigkeitsdauer von Zertifikaten beträgt 3 Jahre, wobei der Zeitraum der Eignung der im Umfeld des Signierungsvorganges zum Einsatz kommenden Algorithmen, Hashverfahren udgl. entsprechend Anhang I und II der Verordnung nicht überschritten werden darf. Darin wird wiederholt die Vermutung des Vorliegens ausreichender Sicherheit bis zum 31. Dezember 2005 aufgestellt. Lediglich während des Gültigkeitszeitraumes gefertigte Signaturen sind gültig. Die Signatur darf nur während der konkreten Gültigkeitsdauer genutzt werden, die Abrufbarkeit des Zertifikats und die damit verbundene Überprüfbarkeit des öffentlichen Signaturschlüssels muß hingegen wesentlich länger gegeben sein.

Im Zertifikat angeführte Begrenzungen dienen dem Zertifizierungsdiensteanbieter vor allem dazu, um dessen Haftung nach § 23 Abs. 4 SigG bzw. nach der korrespondierenden Bestimmung des Art 6 Abs. 3 und 4 der SigRl zu beschränken. Dementsprechend hat er nicht einzustehen *„für Schäden, die sich aus einer über diese Beschränkungen hinausgehenden Verwendung des qualifizierten Zertifikats“* wie auch *„aus der Überschreitung dieser Höchstgrenze ergeben“*. Die Begrenzung des Transaktionswertes gilt selbstredend für jedes

[141] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV), BGBl II 30/2000

Rechtsgeschäft gesondert[142], eine absolute Haftungshöchstgrenze zugunsten des Zertifikatausstellers ist weder im Signaturgesetz noch in der Signaturrichtlinie vorgesehen. Wird das Zertifikat über einen bestimmten Bereich bzw. über eine bestimmte Wertgrenze hinaus verwendet, so schließt dies - wie bereits dargestellt - lediglich die Haftung des Zertifizierungsdiensteanbieters aus, davon unberührt bleibt das Vertragsverhältnis zwischen dem Signierenden und dessen Geschäftspartner. In diesem Bereich entfaltet der abgeschlossene Vertrag volle Rechtswirkungen.[143]

Anders jedoch Stockinger[144], welcher die besonderen Rechtswirkungen des § 4 öSigG bloß bei einer im Zeitpunkt des Unterzeichnens gültigen und innerhalb ihres sachlichen oder zeitlichen Anwendungsbereich liegenden Signatur eintreten lassen will. Seiner Meinung folgend, begründet die in der Regierungsvorlage enthaltene, sehr programmatisch und allgemein gehaltene Äußerung, wonach eine sichere elektronische Signatur bloß auf einem gültigen Zertifikat zu „beruhen“ hat, nicht die Vermutung einerseits der Gültigkeit sämtlicher, auch in Überschreitung eventueller Begrenzungen abgegebener Signaturen und andererseits des Eintritts der besonderen Rechtswirkungen.

7.9.3 Verlängerung der Gültigkeit und Nachsignierung

---

142 Die betragsmäßige Begrenzung des Transaktionswertes gilt für jedes einzelne Rechtsgeschäft, was natürlich nicht verhindert, daß innerhalb einer sehr kurzen Zeitspanne eine Vielzahl derartiger, unter diesem Wert liegender Geschäfte abgeschlossen werden. In Übereinstimmung mit dem Gesetz können diese in ihrer Gesamtheit weit über die Betragsgrenze hinausgehen. Überlegenswert wäre daher eine, wie auch im Rahmen des Gebrauchs einer Bankomatkarte übliche, Wertgrenze in Verbindung mit einer zeitlichen Beschränkung.

143 *Brenn*, Signaturgesetz, Wien 1999, S. 74. Der Anwendungsbereich des jeweiligen Zertifikats hat demzufolge keinerlei Auswirkungen auf die Gültigkeit des Zertifikats als solches und des damit abgeschlossenen Geschäfts, sondern ausschließlich auf die Haftung des ZDA.

144 *Stockinger*, Österreichisches Signaturgesetz, MR 4/99, S. 234

Während die Möglichkeit der Verlängerung der Gültigkeitsdauer eines Zertifikats nicht vorgesehen ist, ist eine Erneuerung, also eine wiederholte Zertifizierung derselben Zertifikatsinhalte gesetzlich geregelt. In diesem Zusammenhang ist es § 12 Abs. 4 SigV folgend zulässig, *„bis zum Ablauf der Gültigkeit eines qualifizierten Zertifikats mit Ausnahme der Gültigkeitsdauer dieselben Inhalte samt denselben Signaturprüfdaten neu zu zertifizieren und auf diese Weise ein neues Zertifikat auszustellen“*. Hiebei muss sichergestellt sein, dass sich der Inhalt des alten Zertifikats mit dem des neuen deckt, beide dieselbe Qualifikation aufweisen, die Sicherheitsanforderungen eingehalten werden und auf keinen Fall eine neue Chipkarte mit demselben privaten Signaturschlüssel ausgestellt wird.

In diesem Zusammenhang ist die Möglichkeit der Nachsignierung nach § 17 öSigV zu erwähnen. Nachdem, wie soeben dargestellt, ein Zertifikat bzw. eine darauf beruhende Signatur nur für einen begrenzten Zeitraum als sicher gilt, ist eine dementsprechende Erneuerung, d.h. die neuerliche Anbringung einer den Sicherheitserfordernissen genügenden Signatur notwendig, um einen bestimmten Sicherheitsstandard beibehalten zu können. Noch vor dem Ablauf der Eignung einer Signatur ist diese selbst mitsamt dem signierten Dokument erneut digital zu signieren, und zwar auf eine dem neuesten Stand von Wissenschaft und Technik entsprechende Weise.[145] Der Vorgang der Nachsignierung ist aus Sicherheitsgründen zeitlich zu dokumentieren, was die Verwendung eines Zeitstempels erfordert.

7.9.4 Signierung des qualifizierten Zertifikats

Um überdies auch die Fälschungssicherheit des mit einem spezifischen Identitätscode[146] ausgezeichneten Zertifikats zu gewährleisten, ist dieses selbst mit einer sicheren elektronischen

[145] Die neue Signatur schließt dabei die alte mitein, diese wird also Teil des neuen, zu verschlüsselnden Hashwertes.

[146] Das Anführen eines Identitätscodes, eine Art eindeutige Kennung, dient dazu, die Unterscheidbarkeit und Zuordenbarkeit der Zertifikate zu den Zertifizierungsdiensteanbietern sicherzustellen, da auch die Ausstellung mehrerer Zertifkate zu ein- und demselben Signaturschlüssel möglich und denkbar ist.

Signatur des Zertifizierungsdienstanbieters zu versehen. Mit der Signierung seitens des Zertifikatausstellers wird die Richtigkeit der Angaben bestätigt, welche in all jenen Zertifikaten enthalten sind, die von diesem ausgestellt wurden. Für diese Zertifikate besteht auch eine Haftungspflicht nach § 23 SigG bzw. Art 6 SigRl. Hinsichtlich dieser Signierung ist auch die Verwendung eines auf eine juristische Person ausgestellten Zertifikates denkbar, obwohl - wie bereits unter § 2 SigG dargestellt - dem Signaturgesetz folgend ansonsten nur natürliche Personen als Inhaber eines Zertifikates bzw. eines Signaturschlüssels auftreten können.

7.10 § 6 - Tätigkeit eines Zertifizierungsdiensteanbieters

7.10.1 Genehmigungsfreiheit

§ 6 SigG entspricht Art 3 der Richtlinie, welcher die Genehmigungsfreiheit für die Aufnahme wie auch für die Ausübung von Zertifizierungsdiensten statuiert. Den angeführten Normen folgend untersagt sind alle Arten einer spezifischen Genehmigungspflicht, *„auch alle sonstigen Maßnahmen mit der gleichen Wirkung“*.[147]

Dementsprechend kann weder eine Konzessionierung oder Lizensierung noch die Erwirkung der Ausstellung eines Bescheides für die Erbringung von Zertifizierungsdiensten in gesetzes- bzw. richtlinienkonformer Weise angeordnet werden. Weiterhin zulässig sind hingegen allgemeine, auch im offline-Bereich vorgesehene Zulassungsverfahren, da nur spezielle, d.h. nur für Zertifizierungsdiensteanbieter geltende Genehmigungsverfahren ausgeschlossen sind. Ebensowenig untersagt sind Aufsichtsverfahren wie etwa Notifizierungs-, Registrierungs- oder Kontrollverfahren. Im Gegenteil, das Europäische Parlament fordert die Mitgliedstaaten ausdrücklich dazu auf, durch die Etablierung von öffentlichen wie privaten Aufsichtsstellen für eine effiziente Überwachung der Einhaltung der Richtlinie zu sorgen.[148] Auch im Rahmen der

[147] siehe Erwägungsgrund 10 SigRl

E-Commerce-Richtlinie findet sich in Artikel 4 eine entsprechende, mit der Signaturrichtlinie und dem österreichischen Signaturgesetz übereinstimmende Regelung, welche den Grundsatz der Zulassungsfreiheit von Diensten der Informationsgesellschaft ausdrücklich festhält. [149]

Die übrige nationale Rechtsordnung verliert dabei nicht an Bedeutung. Aus diesem Grund sind etwa auch die Vorschriften der Gewerbeordnung[150] sehr wohl zu berücksichtigen, da die Tätigkeit eines Zertifizierungsdiensteanbieters in der Regel als freies Gewerbe[151] zu qualifizieren sein wird, welches einer Anmeldepflicht unterliegt.[152]

7.10.2 Vertrauenswürdigkeit - Policy, Sicherheits- und Zertifizierungskonzept

Da die „Gesellschafts- bzw. Salonfähigkeit" elektronischer Signaturen in direktem Zusammenhang mit dem Ausmaß des Vertrauens zusammenhängt, das von Seiten der Unternehmer, Verbraucher und Behörden den neuen Techniken entgegengebracht wird, ist es besonders wichtig, für die absolute Vertrauenswürdigkeit der Zertifizierungsdiensteanbieter zu sorgen. Demzufolge ist gemäß § 6 Abs. 2 öSigG iVm § 18 Abs. 1 öSigV die Aufnahme der Tätigkeit unverzüglich, d.h. ohne unnötigen Aufschub, bei der jeweiligen, national zuständigen Aufsichtsstelle auf elektronischem Wege anzuzeigen[153]. Entsprechend den konkreten

---

148 siehe Erwägungsgrund 12f sowie Art 3 SigRl. Die Freiheit der Ausübung der Zertifizierungstätigkeit ist aus diesem Grund bloß eine relative, der Umfang der Informations-, Anzeige- und Mitwirkungspflichten wie auch die Aufsicht allgemein schränkt diese nicht unerheblich ein.

149 Art 4 E-Commerce-Rl

150 Gewerbeordnung 1994 - GewO 1994 BGBl Nr. 194/1994

151 Ein Zertifizierungsdiensteanbieter ist als Datenverarbeiter zu qualifizieren, der gemäß § 271 GewO *„Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik"* erbringt. §§ 339f iVm § 5 Abs 3 GewO folgend ist eine derartige Tätigkeit zu den freien Gewerben zu zählen, welche lediglich anzumelden ist und keiner gesonderten Genehmigung bedarf.

152 *Brenn*, Signaturgesetz, Wien 1999, 77 sowie GewO 1994

153 Die Wendung *„unverzüglich"* in § 6 Abs 2 bedingt wiederum, daß die Anzeige so bald als möglich, also auch noch bei bzw. nach Aufnahme der Tätigkeit zulässig ist. Die Konzepte hingegen müssen

Ausführungen des § 15 SigV ist das Sicherheits- wie auch das Zertifizierungskonzept sicher zu signieren und ist zudem *„elektronisch jederzeit allgemein abrufbar"*[154] zu halten. Jede natürliche wie juristische Person privaten oder öffentlichen Rechts, jede staatliche wie nicht-staatliche Stelle kann eine derartige Anzeige der Aufnahme der Zertifizierungstätigkeit einbringen, welche insbesondere auch die zum Angebot stehenden Zertifizierungsklassen bzw. die dabei eingehaltenen Sicherheitsstufen in concreto anzuführen hat. Zu diesem Zwecke ist *„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."*[155] Nähere Ausführungen zu den konkreten Sicherheitsanforderungen finden sich unter § 18 öSigG. Als Folge einer durchgeführten, mit einer elektronischen Signatur versehenen Anzeige haben einerseits sämtliche potentieller Kunden eine Auflistung aller innerstaatlichen Diensteanbieter zur Verfügung und andererseits kann die Kontrolltätigkeit seitens der Aufsichtsstelle aufgenommen werden.

Die vom Zertifizierungsdiensteanbieter verfasste Policy[156] enthält in der Regel einen Überblick über die von ihm angebotenen Dienste, das dafür in Rechnung gestellte Entgelt, die seinerseits wie auch von Seiten des Anwenders zu erfüllenden Pflichten betreffend Information und Geheimhaltung des privaten Schlüssels, genaue Angaben über die Haftungspflicht und -reichweite, über die Zertifizierungsinfrastruktur und -hierarchie und über einen eventuell geführten Widerrufsdienst. Dieser ist etwa entbehrlich bei Zertifikaten mit nur kurzer Gültigkeitsdauer bzw. Billig- und Gratiszertifikaten. Auf Grundlage der in der Policy enthaltenen Ausführungen kann der einzelne Anwender entscheiden, ob ein konkretes, im

---

hingegen bei Aufnahme der Tätigkeit der Aufsichtsstelle bereits vorliegen. Siehe dazu auch *Mayer-Schönberger/Pilz/Reiser/Schmölzer*, Signaturgesetz: Praxiskommentar, Wien 1999, S. 89

154 Dies muß jedoch nicht unbedingt auch bedeuten, daß die Einsichtnahme unentgeltlich zu erfolgen hat.

155 siehe § 6 Abs 2 ö. SigG, BGBl. I Nr. 190/1999

156 so gibt es etwa a-sign Policies abrufbar unter
http://www.datakom.at/content/infodienst/richtlinien/richtlinien.html

Angebot stehendes Zertifikat einer bestimmten Sicherheitsstufe seinen Anforderungen bzw. den Erfordernissen eines bestimmten zu tätigenden Rechtsgeschäfts genügt.

Im Rahmen des Sicherheitskonzeptes darzulegen ist kurz gesagt die Einhaltung der Sicherheitsanforderungen des Gesetzes wie auch der darauf beruhenden Verordnungen. Insbesondere anzugeben sind sämtliche infrastrukturellen, personellen, organisatorischen und technischen Maßnahmen, die gesetzt werden, um das im Konzept angegebene Sicherheitsniveau einhalten zu können. Dementsprechend ist für geeignete Räumlichkeiten, Schulung und Fachkunde des Personals, Vernichtung unzulässiger bzw. ungültiger Daten, Archivierung und Protokollierung der Zertifizierungsdaten, Sicherheit bei Erzeugung von Zertifikaten und Schlüsseln, uvm. zu sorgen.

Im Zertifizierungskonzept wiederum sind die näheren Angaben zu den konkreten im Angebot stehenden Zertifizierungsdiensten anzuführen. Konkret handelt es sich dabei um die Darstellung der genauen Vorgehensweise bei der Identifizierung von Zertifikatswerbern, der Antragstellung, der Generierung des privaten wie auch des öffentlichen Schlüssels, des Erhaltes eines Zertifikates wie auch dessen Erneuerung, des Verzeichnis- und des Widerrufsdienstes, udgl.

All die sowohl in Sicherheits- als auch in Zertifizierungskonzept enthaltenen Angaben müssen während der gesamten Dauer des Anbietens der Zertifizierungsdienste eingehalten werden.[157] Eventuelle Änderungen bzw. Qualitätsminderungen sind der Aufsichtsstelle unverzüglich anzuzeigen, um auch die Anwender zuverlässig davon informieren zu können.[158]

7.10.3 Zertifikat eines Zertifizierungsdiensteanbieters

[157] *Brenn*, Signaturgesetz, Wien 1990, S. 78ff

[158] siehe § 6 Abs. 4 und 5 ö. SigG, BGBl. I Nr. 190/1999

Abs. 7 entsprechend darf ein auf einen Zertifizierungsdiensteanbieter ausgestelltes Zertifikat ausschließlich für die Erbringung von Zertifizierungsdiensten verwendet werden, worunter unter anderem die Signierung von Widerrufsverzeichnis, Policy und Zeitstempelangabe zu subsumieren ist, nicht jedoch der Abschluss eigenständiger Rechtsgeschäfte. Bietet ein Zertifizierungsdiensteanbieter die Ausstellung einfacher wie auch qualifizierter Zertifikate an, so hat er dafür zwei unterschiedliche Signaturen zu verwenden, sich dementsprechend also zwei Zertifikate ausstellen zu lassen bzw. selbst auszustellen. Den Erläuterungen des Abänderungsantrages folgend, können die hier in Rede stehenden Zertifikate nämlich auch von anderen öffentlichen oder privaten Stellen als der nationalen Aufsichtsstelle ausgestellt werden, da diese in Österreich nicht als sogenannte „zentrale Wurzelinstanz" gilt.[159]

7.10.4 Österreichische Zertifizierungsdiensteanbieter

7.10.4.1 Datakom Austria GmbH[160]

Die österreichische Datakom bietet eine breite Palette unterschiedlichster Sicherheitsklassen und Typen von Zertifikaten an, um den individuellen Bedürfnissen des Verbrauchers gerecht zu werden. Bei alltäglichen Rechtsgeschäften mit nur geringen Geldbeträgen lohnt sich der Einsatz aufwendiger Verfahren zur Identitätsfeststellung idR. nicht, die Kosten der Anschaffung und Verwaltung des Zertifikats würden hier außer Verhältnis zum konkreten Verwendungszweck stehen. Hingegen werden Notare[161], Rechtsanwälte, Banken, udgl. von vornherein nur den

---

[159] NR: GP XX RV 1999 AB 2065 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP, 2

[160] siehe unter http://www.a-sign.datakom.at und http://www.a-sign.at

[161] siehe NZ 1999, S. 409ff. Entsprechend Artikel IV der Richtlinien der Österreichischen Notariatskammer vom 21. Oktober 1999 über das Verhalten und die Berufsausübung der Standesmitglieder (Standesrichtlinien – STR 2000) haben Notare im Rahmen ihrer Berufsausübung ausschließlich sichere elektronische Signaturen zu verwenden. Die Angabe von Pseudonymen in diesen zugeordneten

Einsatz besonders vertrauenswürdiger, auch mit höheren Kosten verbundener Zertifizierungssysteme erwägen, um das von Klienten, Mandanten und Kunden geforderte Sicherheitsniveau einhalten zu können. Per Web und E-Mail angefordert werden kann das A-Sign Zertifikat Light, auch die Identitätsüberprüfung erfolgt auf diesem Weg. Bei Erwerb eines Medium-Zertifikat ist zumindest die Übermittlung eines Lichtbildausweises per Fax vorgesehen. Strenger sind die Anforderungen beim A-Sign Zertifikat Strong, welches nur nach persönlicher Identitätsüberprüfung bei einem Postamt, das hier als Bestätigungsstelle tätig wird, erhältlich ist. Die bisher aufgezählten Zertifikate sind bloß tauglich für die Erstellung einfacher Signaturen. Bei einem A-Sign Zertifikat Premium wird das Zertifikat nach vorheriger Identitätsprüfung beim nächsten Postamt auf einer Smart- (Chip-) Card erzeugt und gespeichert. Dieses gilt somit als sicherste Zertifizierungsklasse, die derzeit im Angebot von Datakom steht. Darin besteht auch eine der wesentlichen Unterschiede zu den vorherig genannten Zertifikatsklassen, denn während bei ersteren der private Schlüssel sich auf der Festplatte des PCs befindet und durch ein Kennwort oder eine Kennnummer geschützt ist, befindet sich dieser bei einem Premium-Zertifikat auf einer Chipkarte, welche er auch niemals, d.h. auch nicht während des Signierungsvorganges, verlässt. Dieses Zertifikat allein entspricht auch den Anforderungen des österreichischen Signaturgesetzes und gilt als „qualifiziert“ iSv. § 5.

Zusätzlich zu dem hier dargestellten Angebot, stellt die Datakom ein sogenanntes Demo-Zertifikat zur Verfügung. Die Überprüfung der Identität erfolgt, wie auch beim A-Sign Zertifikat Light, bloß über Web und E-mail, es ist gratis erhältlich und hat eine maximale Gültigkeitsdauer von dreißig Tagen. Die Verfügbarmachung dieses Zertifikates mit nur geringem Sicherheitswert dient vor allem dazu, die Verbraucher an den Gebrauch elektronischer Signaturen zu gewöhnen bzw. zu einer erstmaligen Ingebrauchnahme zu motivieren.

Zertifikaten ist ausgeschlossen, die ausstellenden Zertifizierungsdiensteanbieter sind von der Österreichischen Notariatskammer anzuerkennen.

Weiters wird unterschieden hinsichtlich der konkreten Zweckwidmung der elektronischen Bescheinigung. Hinlänglich bekannt sind die User Zertifikate, die von natürlichen Personen zu Zwecken der Verschlüsselung und Authentifizierung verwendet werden. Davon zu unterscheiden sind Server Zertifikate und Software Developer Zertifikate. Erstere dienen den Nutzern vornehmlich zur zweifelsfreien Identifizierung des Servers, zweitere zu Überprüfung von Herkunft und Unverfälschtheit eines bestimmten Programmes.

Eine der Tätigkeitsbereiche der Datakom ist die Wirtschaftsuniversität (WU) Wien. Das gesamte Verwaltungssystem dort läuft bereits auf ausschließlich elektronischer Basis, die Studentenkarten haben das äußere Erscheinungsbild von Chipkarten. Diese dienen zugleich als herkömmlicher Studentenausweis und Speichermedium des jedem Studenten individuell zugeordneten privaten Schlüssels. Damit sind sämtliche WU-Studenten mit Signaturen ausgestattet, die zudem den Erfordernissen des österreichischen Signaturgesetzes voll entsprechen. Aufgrund der ihnen individuell zugeordneten a-sign-Zertifikate können verschiedenartigste Dienste in Anspruch genommen werden: Inskription, Studienwechsel, Prüfungsanmeldung, das Drucken von Erfolgsnachweisen und Zeugnissen wie auch universitäre Wahlen können unter Verwendung von Signaturen selbständig auf elektronischem Wege durchgeführt werden.[162]

7.10.4.2 Arge Daten AG[163]

Sie haben sich der Zertifizierung von PGP Public Keys, d.h. von öffentlichen Schlüsseln, gewidmet, bieten jedoch keine Zertifikate an, die dem Qualifiziertheitserfordernis genügen würden.

---

[162] siehe Artikel in Presse vom 29.9.2000, S. 17

[163] siehe unter http://www.ad-cert.at

7.10.4.3 Generali Office-Service und Consulting AG[164]

Eine Einzigartigkeit am österreichischen Markt ist die Koppelung von Zertifizierungsdiensten mit einem Versicherungspaket, bestehend aus Haftpflicht-, Missbrauch- und Rechtsschutzversicherung. Der Web-Site folgend werden im Rahmen der Rechtsschutzversicherung etwa Sachverständigen-, Gerichts- und Anwaltskosten bis zu einem Wert von S 450.000,-- übernommen. Auf Basis der Haftpflichtversicherung tritt die Generali für Personen-, Sach- oder Vermögensschäden ebenso bis zu dieser Höhe ein. Die zu entrichtende Gebühr richtet sich nach der Höhe der konkreten Versicherungssumme, bei S 100.000 etwa S 1.090 pro Jahr. Die von der Generali Versicherung ausgegebenen Zertifikate entsprechen den a-sign Strong Zertifikaten, wobei ein dafür zuständiger Betreuer die Aufgabe der Identitätsüberprüfung anhand persönlicher Vorsprache des Zertifikatwerbers und dessen Ausweisung durch einen amtlichen Lichtbildausweis zu erfüllen hat.[165]

7.10.4.4 A-Trust[166]

Diese Zertifizierungsstelle, derzeit bestehend aus Österreichischen Geldinstituten, der Österreichischen Nationalbank, der PTA/Telekom, der Österreichischen Notariatskammer, dem Österreichischen Rechtsanwaltskammertag und der Wirtschaftskammer Österreich, hat sich die Zurverfügungstellung von ausschließlich qualifizierten, den Anforderungen des Signaturgesetzes und der Signaturrichtlinie genügenden, Zertifikaten zur Aufgabe gemacht.[167]

---

164 siehe unter http://www.generali.co.at/netsecurity.nsf

165 Ausführlicher dazu und zu den konkreten Versicherungssummen *Pankart*, Sichere E-Mail: Signieren und Verschlüsseln, in Datagraph 2/2000, S. 59f.

166 siehe unter http://www.e-sign.at

167 Als weitere Zertifizierungsstelle hatte sich auch Globalsign Austria NV/SA, eine belgische GmbH beworben. Diese vertreibt unter anderem auch Zertifikate in Österreich, in den von ihr ausgestellten Zertifikaten tritt sie selbst als Ausstellerin auf. Das in Ö ansässige Unternehmen Innovation Systems

7.11 § 7 - Mindestanforderungen an Zertifizierungsdiensteanbieter für qualifizierte Zertifikate

Anhang II der Richtlinie findet sich verwirklicht in § 7 des österreichischen Signaturgesetzes. Demnach hat ein Zertifizierungsdiensteanbieter bestimmten Mindesterfordernissen nachzukommen, um zur Ausstellung qualifizierter Zertifikate ermächtigt zu sein. Auffallend an dieser Norm ist die Anhäufung juristisch unscharfer und einer Auslegung bedürfenden Begriffe, wie etwa „erforderlich", „zuverlässig", „geeignet" und „ausreichend".

Ziffer 1 leg.cit. spricht das Erfordernis des Vorliegens „der erforderlichen Zuverlässigkeit" ausdrücklich an. Darunter ist im allgemeinen zu verstehen, dass von der Einhaltung der maßgeblichen Rechtsvorschriften durch die Zertifizierungsdiensteanbieter ausgegangen werden kann.

Ein funktionierender und schneller Verzeichnis-, Widerrufs- und Zeitstempeldienst ist vor allem im Hinblick auf den online-Abschluss von Verträgen von immenser Bedeutung. Nur so kann eruiert werden, ob eine elektronische Signatur im Zeitpunkt ihrer Verwendung noch Rechtswirkungen entfalten konnte oder im entgegengesetzten Fall das zugrundeliegende Zertifikat etwa bereits gesperrt bzw. widerrufen war. Durch das Anbringen derartiger qualifizierter, d.h. den Anforderungen des § 18 entprechender Zeitangaben, ist es möglich, den genauen Zeitpunkt einer Rechtshandlung, wie z.B. eines Widerrufs oder einer Zertifikats-Ausstellung, festzustellen.

Die Bereitstellung eines derartigen Dienstes ist nicht notwendige Voraussetzung des Betriebes einer Zertifizierungsstelle. Sie ist ohne weiteres auch durch ausgegliederte Diensteanbieter möglich und muss nicht notwendigerweise von demjenigen angeboten werden, der die

fungiert dabei nur als Registrierungsstelle, weshalb Art 4 SigRl belgisches Recht anzuwenden ist und demzufolge der Antrag der Globalsign Austria mangels Zuständigkeit zurückzuweisen war.

Ausstellung und Verwaltung des Zertifikats übernimmt. Andererseits kann ein Zertifizierungsdiensteanbieter gleichzeitig auch Dienste anbieten, die nicht als Zertifizierungsdienste iSd. Gesetzes gelten. In diesem Fall ist der Betrieb der Zertifizierungsstelle organisatorisch, personell, technisch und wirtschaftlich eigenständig zu führen und von der übrigen Tätigkeit sorgfältig zu trennen.

Wie bereits wiederholt festgestellt, kommt der Identitätsprüfung einer, um die Ausstellung eines Zertifikats ansuchenden Person besondere Bedeutung zu. Ziffer 4 leg.cit. entsprechend ist die Richtigkeit sämtlicher personenbezogener Daten wie auch aller rechtserheblicher Eigenschaften auf zuverlässige Art und Weise zu überprüfen. Von dieser Verpflichtung kann abgesehen werden, wenn bereits dieser Antrag selbst durch den Zertifikatswerber sicher signiert worden ist, d.h. dessen Identität im Rahmen einer ersten Zertifikatszuteilung hinreichend überprüft wurde. Gemäß § 23 Abs. 1 Z 1 hat der Zertifizierungsdiensteanbieter dementsprechend für die Richtigkeit der in das Zertifikat aufgenommenen Angaben zum Zeitpunkt der Ausstellung einzustehen.

In diesem Zusammenhang weiters zu berücksichtigen ist die Regelung des § 22, wonach unter Einhaltung datenschutzrechtlicher Grundsätze personenbezogene Daten entweder nur bei der Person selbst oder nur mit deren Zustimmung erhoben werden dürfen. Können die für die Überprüfung eines Zertifikats notwendigen Angaben nicht ermittelt werden, so ist die Ausstellung zu versagen. Bislang nicht eindeutig geklärt ist, wie weit der Kreis der zulässigerweise zu erhebenden Daten zu ziehen ist. Angaben über die finanzielle und wirtschaftliche Leistungsfähigkeit etwa fallen jedenfalls nicht unter den Begriff der *„rechtlich erheblichen Eigenschaften des Signators“* und dürfen demzufolge auch nicht erhoben werden.

Da ein Zertifizierungsdiensteanbieter schlussendlich nur durch sein Personal handlungsfähig ist und die Vertrauenswürdigkeit des Unternehmens somit in direktem Zusammenhang mit der seiner Angestellten steht, hat ersterer für geeignete und wiederholte Schulungsmaßnahmen zu sorgen. Laut Signaturverordnung darf *„ein Zertifizierungsdiensteanbieter, der qualifizierte*

Zertifikate ausstellt, im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste nicht Personen beschäftigen, die wegen einer mit Vorsatz begangenen strafbaren Handlung zu einer Freiheitsstrafe von mehr als einem Jahr oder wegen strafbarer Handlungen gegen das Vermögen oder gegen die Zuverlässigkeit von Urkunden und Beweiszeichen zu einer Freiheitsstrafe von mehr als drei Monaten verurteilt wurden",[168] getilgte Strafen haben dabei außer Betracht zu bleiben. Das Verbot der Einstellung dieser Personen bezieht sich nur auf rechtkräftige Verurteilungen. Dementsprechend ziehen Vorstrafen der Angestellten grs. ihre Zuverlässigkeit in Zweifel, wobei nur bei einem konkreten Verdacht die Pflicht zur Einholung einer Strafregisterauskunft seitens der Aufsichtsstelle besteht. Verurteilungen, welche noch nicht der Rechtskraft fähig sind oder unterhalb des genannten Strafrahmens liegen, sind im Rahmen der allgemeinen Zuverlässigkeitsprüfung nach § 7 Abs. 1 Z 5 des Gesetzes in den jeweiligen Personalentscheidungsprozeß miteinzubeziehen. Im allgemeinen ist die Aufsichtsstelle verpflichtet, die Einhaltung der durch die Zertifizierungsdiensteanbieter zur Anzeige gebrachten Sicherheits- und Zertifizierungskonzepte *„in regelmäßigen Abständen"* zu kontrollieren; nur bei konkret vorliegenden Verdachtsgründen ist eine stichprobenartige Überprüfung zulässig.[169]

7.11.1 Haftungsrechtliche Aspekte

Um das Haftungsrisiko und eventuell in Zukunft entstehende Schadenersatzansprüche, abdecken zu können, hat der Zertifizierungsdiensteanbieter laut § 7 Abs. 1 Z 6 öSigG die Verfügbarkeit über ausreichende Finanzmittel nachzuweisen. Zu diesem Zweck hat er von der Möglichkeit, eine Haftpflichtversicherung, eine Bürgschaft, eine Bankgarantie oder ein anderes Sicherungsmittel mit einem vergleichbaren Sicherungsgrad einzugehen, Gebrauch zu machen. Anhang II der SigRl entsprechend *„müssen Zertifizierungsdiensteanbieter über*

[168] siehe § 10 Abs 4 öSigV

[169] siehe § 18 Abs 4 öSigV

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

Während das Gesetz keine bestimmte Form zur Risikoabdeckung vorschreibt, verlangt die darauf beruhende Durchführungsverordnung in § 2 Abs. 2 den Nachweis des Abschlusses einer Haftpflichtversicherung mit einer bestimmten Mindestversicherungssumme je Versicherungsfall. Reine bilanzielle Rückstellungen werden in diesem Zusammenhang als nicht gleichwertig angesehen, da sie als bloße buchhalterische Größen weder als konkursfest noch als gesichert realisierbar gelten. Aus Sicht der Gesellschafter sind diese auch nicht besonders empfehlenswert, da sie bei bewiesener Erkennbarkeit mangelnder Abdeckung des Haftungsrisikos eine persönliche Einstandspflicht begründen können. Die in der Richtlinie wie im nationalen Signaturgesetz empfohlene und laut nationaler Signaturverordnung verpflichtend vorgeschriebene Haftpflichtversicherung begründet nach § 157 VersVG[170] ein Absonderungsrecht des geschädigten Anwenders und des geschädigten Dritten an der Entschädigungssumme, die der Versicherer dem Zertifizierungsdiensteanbieter auszuzahlen verpflichtet ist. Diese Forderungen bleiben auch bei Eröffnung eines Konkurses weiter bestehen, sind also konkursfest. Die Haftung des Diensteanbieters ist der Höhe nach unbegrenzt, dieser hat mit seinem gesamten Vermögen einzustehen.[171]

Da die konkrete Höhe des zu erwartenden abzudeckenden Risikos noch nicht genau eingeschätzt werden kann und diese zudem Schwankungen unterworfen sein wird, erfolgt die Festlegung der konkreten Summe auf dem Verordnungsweg.[172] Die ö. Signaturverordnung

---

[170] Bundesgesetz vom 2. Dezember 1958 über den Versicherungsvertrag (Versicherungsvertragsgesetz 1958), BGBl. Nr. 2/1959 idgF.

[171] *Brenn*, Signaturgesetz, Wien 1999, S. 86f

[172] NR: GP XX RV 1999 AB 2065 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP, 2f

sieht in § 2 verpflichtend vor, dass ein qualifizierter Zertifizierungsdiensteanbieter bei Aufnahme seiner Tätigkeit über ein Mindestkapital von 300 000 Euro zu verfügen und pro Versicherungsfall eine Haftpflichtversicherung mit einer Mindestversicherungssumme von 1 000 000 Euro abzuschließen hat. Gebietskörperschaften, d.h. Bund, Länder, Gemeindeverbände und Ortsgemeinden mit mehr als 50 000 Einwohnern sind gemäß Abs. 3 leg.cit. von den genannten Verpflichtungen befreit.

7.11.2 Weitere Pflichten qualifizierter Zertifizierungsdiensteanbieter

Für den Fall eventuell auftretender Rechtsstreitigkeiten und der Notwendigkeit der Beweiserbringung vor Gericht ist eine genaue Protokollierung sämtlicher rechtserheblicher Umstände von grundlegender Bedeutung. § 7 Abs. 6 leg.cit. folgend hat die Verifizierung von damit in Zusammenhang stehenden Behauptungen und Angaben ebenso wie die Signaturprüfung selbst auf Ersuchen von staatlichen Behörden wie Gerichten durch die Zertifizierungsdiensteanbieter zu erfolgen, da in der Regel erstere nicht über die nötigen technischen Gegebenheiten verfügen. Die Dauer der Aufzeichnungspflicht des Abs. 1 Z 7 richtet sich nach dem konkreten Verwendungszweck. Dementsprechend wird je nach den konkreten Fristen für das Eintreten der Verjährung zu differenzieren sein. Die genaue Aufzeichnungs- und Verfügbarkeitsdauer ist im Zertifikat ausdrücklich anzuführen.

Absolute Geheimhaltung und Vertrauenswürdigkeit sind substantiell für die Zurechenbarkeit einer elektronischen Signatur zu einem bestimmten Rechtssubjekt. Aus diesem Grund sind entsprechend Ziffer 8 *„Vorkehrungen dafür zu treffen, dass die Signaturerstellungsdaten der Signatoren weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden.“* Ebensowenig dürfen die in Zertifikaten enthaltenen Daten unerkannterweise ge- oder verfälscht werden können. Sicherzustellen ist nach Abs. 3 auch der Schutz des privaten Schlüssels vor unbefugtem Zugriff, was einerseits absolute Geheimhaltung seitens des Schlüsselerstellers wie auch seitens des Schlüsselinhabers und andererseits das Vorhandensein geeigneter, abschließbarer Räumlichkeiten, wie etwa Tresore, voraussetzt.

Um das bei der Erstellung und Verwaltung des Zertifikates eingehaltene Sicherheitsniveau für jedermann sichtbar zu machen, ist die Qualifizierung in dieses selbst aufzunehmen. Die zusätzliche Bescheinigung des Vorliegens der in Gesetz und Verordnung statuierten Voraussetzungen, auch freiwillige Akkreditierung genannt, erfolgt bereits im vorhinein durch die Aufsichtsbehörde und stellt eine zusätzliche vertrauensfördernde Maßnahme dar.
So wie ein qualifiziertes Zertifikat als solches zu kennzeichnen ist, so muss auch eine sichere elektronische Signatur vom jeweiligen Empfänger klar und eindeutig als solche erkennbar sein. Dies sieht zumindest der österreichische Gesetzgeber in § 7 Abs. 5 verpflichtend vor. Da die Gleichsetzung ausländischer mit inländischen sicheren elektronischen Signaturen eines der Prinzipien der europäischen Richtlinie ist und die Zuerkennung der besonderen Rechtswirkungen, d.h. der Gleichstellung mit der eigenhändigen Unterschrift, ausschließlich an die Einhaltung der Anforderungen der Anhänge I und II der Richtlinie über elektronische Signaturen geknüpft ist, spielt die innerstaatlich geforderte Erkennbarkeit einer sicheren elektronischen Signatur als solche in diesem Zusammenhang keine Rolle.

Wie bereits wiederholt dargestellt ist bei der Ausstellung qualifizierter Zertifikate, also der Zuordnung der Signaturerstellungs- und -prüfeinheiten zu einer natürlichen Person, ein besonders hohes Maß an Vorsicht geboten, um die Urheberschaft einer elektronischen Erklärung eindeutig feststellbar und unbestreitbar zu machen. Die Gültigkeit bzw. Ordnungsgemäßheit einer elektronischen Signatur basiert schlussendlich auf der Existenz eines gültigen und inhaltlich richtigen Zertifikats und der Möglichkeit der Überprüfung einer Signatur auf Grundlage desselben. Um eine allgemeine Kontrollmöglichkeit einzurichten, ist das Zertifikat entweder dem signierten Dokument anzuhängen und mit diesem dem Empfänger mitzuübermitteln oder mit Zustimmung des Zertifikatinhabers öffentlich abrufbar zu machen. Für den Fall, dass dieser weder der Veröffentlichung zustimmt noch die individuelle Zugänglichkeit veranlasst, wird die elektronische Signatur als ungültig angesehen.

7.11.3 Wettbewerbsrechtliche Aspekte

In Österreich wird vor allem im Bereich neuer Informations- und Kommunikationstechnologien ganz allgemein versucht, in die freie Entwicklung des Marktes so wenig als möglich regulierend bzw. lenkend einzugreifen. Es wird davon ausgegangen, dass sich auf einem funktionierenden Markt diejenigen Diensteanbieter mit dem besten Preis-Leistungs-Verhältnis auch ohne staatliche Einflussnahme durchsetzen werden können. Der österreichische Nationalrat bringt diese Überzeugung auch in dem Signaturgesetz 1999 zum Ausdruck. Durch dieses werden zwei Arten von Diensteanbietern geschaffen, je nachdem welche Klassen von Zertifikaten auszustellen sie anbieten: Die Anbieter von bloß einfachen Zertifikaten, die ihre Tätigkeit ohne besondere staatliche Kontrolle und Aufsicht auszuüben berechtigt sind, deren Zertifikate jedoch auch bloß eingeschränkte und allgemeine Rechtswirkungen entfalten. Für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, bestehen Sonderregelungen. Diese sind zur Erfüllung besonderer, nur für sie geltender Anforderungen verpflichtet, nur sie trifft die für ihre Seite nachteilige Beweislastumkehr nach § 23 öSigG.

Aber nicht nur im Bereich der Anforderungen liegen erhebliche Unterschiede zwischen einfachen und qualifizierten Zertifizierungsdiensteanbietern vor, sondern auch bei der Gebührenfestsetzung nach der öSigV. Der Regierungsvorlage[173] folgend sind die zu entrichtenden Gebühren als „kostendeckendes Entgelt“ für „konkret erbrachte Leistungen“ zu sehen. Allein aus diesem Grund scheinen die nicht unerheblichen Differenzen bei der konkreten Festsetzung der Gebühren für die Aufsichtstätigkeiten der Aufsichtsstelle und der Telekom-Control GmbH nicht einleuchtend. Während ein Anbieter einfacher Zertifikate anlässlich der Anzeige seiner Tätigkeit für die Überprüfung und Registrierung 100 Euro zu leisten hat, steigt dieser Betrag bei Anbietern qualifizierter Zertifikate auf 6 000 Euro. Ein derart eklatanter Unterschied scheint auch bei der Notwendigkeit etwas umfassenderer und aufwendigerer Aufsicht nicht gerechtfertigt zu sein.

[173] vgl. dazu EBRV zu § 13 Abs 4 SigG

Auch § 1 Abs. 2, wonach für jedes ausgestellte und gültige qualifizierte Zertifikat eine Gebühr zu entrichten ist und zwar unabhängig vom konkret notwendigen Handlungsbedarf seitens der Aufsichtsstelle, widerspricht der Regierungsvorlage völlig. Diese Regelung schafft im Ergebnis eine neue Art von „Zertifikats-Steuer", welche noch dazu aus unerfindlichen Gründen ausschließlich nur für qualifizierte Zertifikate zu entrichten ist.
Weiters sehr unpräzise ausgedrückt ist der folgende Absatz 3, wonach die Aufsichtsstelle und die ihr zur Seite gestellte Telekom-Control GmbH zur Bewältung ihrer Aufgaben eine Bestätigungsstelle heranziehen können und dabei entstehende Kosten als Barauslagen iSd. AVG vorgeschrieben werden. Es werden keinerlei Aussagen getroffen, nach welchen Kriterien sich die Aufsichtsbehörden bei der Wahl einer Bestätigungsstelle zu halten haben. Selbiges gilt auch für die Wahl eines übernehmenden Zertifizierungsdiensteanbieters im Falle der Einstellung oder Untersagung der Tätigkeit durch die Aufsichtsstelle laut §§ 12 und 14.

Ebensowenig juristisch einwandfrei ist § 2 der Verordnung. Während Zertifizierungsdiensteanbieter bei Anzeige ihrer Tätigkeit ganz allgemein über ausreichende Finanzmittel zu verfügen haben, trifft die Aussteller qualifizierter Zertifikate zusätzlich die Verpflichtung nachzuweisen, *„Vorsorge für die Befriedigung von Schadenersatzansprüchen"* getroffen zu haben. Während § 7 Abs. 1 Z 6 öSigG den Abschluss einer Haftpflichtversicherung bloß als eine mögliche, dem Erfordernis der Risikoabdeckung genügende Variante vorschlägt, sieht § 2 Abs. 2 dies verpflichtend vor. Es wird weiters nicht unterschieden zwischen Zertifizierungsdiensteanbietern, welche eine Vielzahl von Zertifikaten ohne Begrenzung des Transaktionswertes ausgegeben haben und solchen, welche über ein relativ geringes Angebot an Zertifikaten mit niedrigen Wertgrenzen verfügen. Zweitere werden offensichtlich erheblich benachteiligt.

Überdies nimmt Abs. 3 öffentlich-rechtliche Gebietskörperschaften, namentlich Bund, Länder, Gemeindeverbände und Ortsgemeinden von der Verpflichtung des Abschlusses einer Versicherung mit einer Mindestsumme pro Versicherungsfall ausdrücklich aus. Auf welche tatsächlich bestehenden Unterschiede diese Differenzierung gestützt wird, bleibt im Text der Verordnung unangesprochen. In der Realität sind finanzschwache und oftmals sogar stark

verschuldete Körperschaften viel weniger zur Befriedigung etwaiger Schadenersatzansprüche imstande, als so manches finanzstarke, am Internationalen Markt eingebundene, private Unternehmen. Allein durch diese verordnungsrechtlich geschaffenen Ausnahmen sehen sich private Diensteanbieter im Vergleich zu öffentlich-rechtlichen Gebietskörperschaften erheblichen Wettbewerbsnachteilen und –verzerrungen ausgesetzt, was vor allem im Hinblick auf die Grundsätze von Dienstleistungsfreiheit und verfassungsrechtlich normiertem Gleichheitssatz fragwürdig erscheint.[174]

Man kann sich aus den erwähnten Gründen nicht des Eindrucks erwehren, es werde seitens des österreichischen Staates der Versuch unternommen, einerseits die Zahl der am Markt befindlichen Zertifizierungsdiensteanbieter von qualifizierten Zertifikaten von vornherein gering zu halten und andererseits staatliche Stellen im Vergleich zu privaten zu bevorzugen.

7.12 § 8 - Ausstellung qualifizierter Zertifikate

Entsprechende Anträge auf Ausstellung eines qualifizierten Zertifikats sind nach § 11 öSigV Abs. 1 eigenhändig zu unterschreiben und gemeinsam mit einer Ablichtung des vorzulegenden Lichtbildausweises durch den Zertifizierungsdiensteanbieter zu dokumentieren.

§ 8 des österreichischen Signaturgesetzes fordert in diesem Zusammenhang die eindeutige Feststellung der Identität des Zertifikatwerbers durch Vorlage eines amtlichen Lichtbildausweises. Ist der Antrag des Zertifikatwerbers jedoch bereits mit einer elektronischen Signatur versehen, so ist die Identitätsfeststellung bereits aufgrund dieses Umstandes möglich und durchführbar. In diesem Fall werden erneute Nachforschungen als verzichtbar angesehen. Werden bei ein- und demselben Zertifizierungsdiensteanbieter mehrere

---

174 siehe dazu ausführlich *Mayer-Schönberger*, Bedauerlich: Signatur-Dienstleister nach der SigV, ecolex 2000, S. 130. Allerdings ist hier festzuhalten, dass lediglich Gebietskörperschaften und nicht Körperschaften öffentlichen Rechts schlechthin von der Versicherungspflicht ausgenommen sind. Dieses Versicherungsprivileg zugunsten der öffentlich-rechtlichen Körperschaften gibt es etwa auch im Bereich der Kraftfahrzeughaftpflichtversicherung und ist allgemein anerkannt.

auf eine Person lautende Zertifikate beantragt, so genügt idR die einmalige Vorlage eines Lichtbildausweises bzw. das einmalige persönliche Erscheinen vor der Ausstellungsstelle. Die Überprüfung der Person des zukünftigen Zertifikatinhabers kann auch durch eine andere, dafür beauftragte Stelle erfolgen als jener, die die Ausstellung des Zertifikates übernimmt. Diese sogenannte Registrierungsstelle wird auf Rechnung des Zertifikatausstellers tätig und ist an sämtliche, die Ausstellung und Erhebung personenbezogener Daten betreffenden Rechtsvorschriften gebunden. Im Rahmen der Erfüllungsgehilfenhaftung nach ABGB hat der Zertifizierungsdiensteanbieter auch für diese, von ihm beauftragten Unternehmen und deren Personal einzustehen, da idR zwischen Zertifikatswerber und Registrierungsstelle kein Vertragsverhältnis besteht. Die Tätigkeit der Registrierungsstelle hat ebenso als Zertifizierungsdienst zu gelten, weshalb auch diese die Einstandspflicht nach § 23 SigG trifft.

7.13 § 9 - Widerruf und Sperre von Zertifikaten

§ 9 des öSigG regelt den für sämtliche, d.h. auch für die einfachen Zertifikate, verpflichtend vorgesehenen Widerrufsdienst. Bei qualifizierten Zertifikaten gilt das Zusatzerfordernis der Unverzüglichkeit und Sicherheit des Dienstes, wie bereits dargestellt unter § 7 Abs. 1 Z 2. Ziffer 1 bis 6 nennen in sehr weit auslegbarer Art und Weise die verschiedensten Gründe, aufgrund deren ein Zertifikat zu widerrufen bzw. zu sperren ist.

7.13.1 Anlassgründe

Zuallererst hat natürlich der Zertifikatsinhaber selbst wie auch ein im Zertifikat infolge der Anführung einer Vertretungsmacht genannter Machtgeber das Recht, den Widerruf zu verlangen. Au diesem Wege kann etwa im Fall rechtlicher Änderungen oder vermuteter unerlaubter Ausforschung der Signaturschlüsseldaten durch einen Dritten die Rechtswirksamkeit damit abgeschlossener Rechtsgeschäfte ausgeschlossen werden. Solange ein derartiger Widerruf nicht erfolgt ist, sind die unter Berufung auf eine besondere Handlungs- und Vertretungsbefugnis abgeschlossenen Rechtsgeschäfte idR dem Machtgeber zuzurechnen;

der Rechtsschein wird meist gegen ihn sprechen. Da die im Zertifikat bescheinigten Angaben der Realität zu entsprechen haben, hat ein Widerruf nicht nur bei Änderungen in Bezug auf eine besondere Vertretungsbefugnis zu erfolgen, sondern auch bei allen sonstigen Änderungen von im Zertifikat bescheinigten Umständen, welche von rechtserheblicher Bedeutung sind. Dazu zählen etwa der Verlust der Staatsbürgerschaft, der berufsrechtlichen Zulassung oder die Verlegung des Wohnsitzes. Hier trifft den Zertifikatsinhaber die individuelle Verpflichtung, und nicht bloß die Ermächtigung, den Widerruf zu verlangen.[175] Eventuell eintretende Folgen einer Nichtbeachtung dieser konkreten Handlungspflicht sind bislang nicht normiert, insbesondere wird in der Auflistung verwaltungsstrafrechtlicher Tatbestände in § 26 öSigG nicht darauf eingegangen.

Im Falle freiwilliger Einstellung der Tätigkeit eines Zertifizierungsdiensteanbieters und gleichzeitiger Übernahme bzw. Fortführung der Verzeichnis- und Widerrufsdienste durch einen anderen Diensteanbieter können sowohl die Zertifikate der Anwender wie auch das des einstellenden Unternehmens weitergeführt werden. Erfolgt jedoch eine solche Weiterführung nicht, so darf der Zertifizierungsdiensteanbieter ab dem Zeitpunkt des Widerrufs keine neuen Zertifikate mehr ausstellen und hat zudem sämtliche, während seiner Unternehmensführung ausgestellten Zertifikate zu widerrufen. So wie die nationale Aufsichtsstelle imstande ist, das Zertifikat eines Zertifizierungsdiensteanbieters und infolge dessen auch alle von ihm ausgestellten und signierten Anwender-Zertifikate zu widerrufen, so kann sie diesem gegenüber auch den Auftrag erteilen, nur bestimmte Anwender-Zertifikate zu widerrufen.[176]

Ziffer 6 wiederholt nochmals den Widerrufsgrund der Missbrauchsgefahr, welche etwa anzunehmen ist bei nicht mehr technisch als sicher geltenden kryptographischen Verfahren.

---

[175] siehe §§ 9 u. 21 öSigG

[176] siehe § 9 Abs 1 Z 5 iVm § 14 Abs 1 SigG

Tritt einer der genannten Fälle ein, so hat grundsätzlich ein Widerruf des betreffenden Zertifikats zu erfolgen. Oftmals wird es jedoch nicht eindeutig und zweifelsfrei feststehen, ob ein derartiger, zum Widerruf anlassgebender Grund vorliegt. Hier ist bis zu einer Klärung der Angelegenheit die unverzügliche Sperrung des Zertifikats anzuordnen. „Während ein Widerruf die vorzeitige Beendigung der Gültigkeit des Zertifikats darstellt, ist eine Sperre als vorübergehendes Aussetzen der Gültigkeit eines Zertifikats zu verstehen“.[177] Wird im Zuge von Nachforschungen ein Widerrufsgrund festgestellt, so ist das Zertifikat unverzüglich zu sperren.

7.13.2 Rechtsfolgen

Da sowohl Widerruf als auch Sperre die Rechtsfolge der Nichtanwendbarkeit der elektronischen Signatur und der Rechtsungültigkeit danach abgeschlossener Rechtsgeschäfte begründen, ist der Zeitpunkt ihres Wirksamwerdens durch Angabe von Datum und Uhrzeit genauestens zu dokumentieren. Wird laut Sicherheits- und Zertifizierungskonzept etwa ein eigener Widerrufsdienst geführt, so ist dies dem Gesetz entsprechend der Zeitpunkt der Eintragung in das entsprechende Verzeichnis. Dritte haben erst mit diesem Vorgang die Möglichkeit, auf verlässliche Art und Weise festzustellen, ob eine Signatur noch rechtsgültig zustandegekommen ist; sie haben grs. nur bereits eingetragene Tatsachen gegen sich gelten zu lassen.

Im Falle eines bereits erfolgten und auch entsprechend eingetragenen Widerrufes bzw. einer Sperre muss bei Abruf des jeweiligen Zertifikates eine Negativmeldung erfolgen. Langt bei einem beliebigen Empfänger eine elektronisch signierte Nachricht ein und kommt er im Zuge der Identitätsabfrage zu dem Ergebnis, dass die Signatur noch volle Gültigkeit haben müsste, obwohl in Wirklichkeit das Zertifikat bereits widerrufen bzw. gesperrt ist, diese Tatsache jedoch noch nicht in das entsprechende Verzeichnis aufgenommen wurde, so kommt das

[177] *Brenn*, Signaturgesetz, Wien 1999, S. 92

jeweilige Rechtsgeschäft zwischen Signator und Geschäftspartner zustande. Insofern kommt den genannten Verzeichnissen eine dem Firmen- oder Grundbuch vergleichbare Publizitätsfunktion eines öffentlichen Registers zu. Verzögerungen bei der Eintragung gehen grs. zu Lasten des Zertifikatinhabers. Trifft den Zertifizierungsdiensteanbieter Verschulden an der Säumnis, so wird er gegenüber dem Signator selbst wie auch gegenüber einem Dritten, d.h. einem Geschäftspartner des Signators, nach § 23 Abs. 1 Z 4 schadenersatzpflichtig. Dem Empfänger eines elektronisch signierten Dokuments soll nicht zugemutet werden werden, sich bei einem Zertifizierungsdiensteanbieter, mit dem er nie in vertraglicher Beziehung gestanden hat, schadlos halten zu müssen. Vielmehr geht eine nicht bzw. bloß verzögerte Eintragung in das Widerrufsregister zu Lasten des Signators, dieser kann Regress nehmen beim Aussteller seines ihm zugeordneten Zertifikats.

§ 7 Abs. 2 sieht die Führung eines schnellen und sicheren Verzeichnisdienstes für qualifizierte Zertifikate verpflichtend vor. Grundsätzlich hat der Zertifizierungsdiensteanbieter ab Bekanntwerden des Widerrufsgrundes drei Stunden Zeit, um das Verzeichnis zu aktualisieren.[178] Außerhalb der Geschäftszeiten ist für eine automatisierte Entgegennahme und eine entsprechende Sperre des betreffenden Zertifikats Sorge zu tragen.[179] Für Gratiszertifikate bzw. Zertifikate mit bloß niedrigem Transaktionswert wird aus wirtschaftlichen und praktischen Gründen oftmals auf derartige Verzeichnisdienste verzichtet. Hier müssen Sperre und Widerruf zeitlich gesichert sein, um dem jeweiligen Empfänger eines signierten Dokuments die Möglichkeit der Überprüfung zu erhalten. Vor Wirksamwerden des Widerrufs bzw. der Sperre ausgehandelte und abgeschlossene Rechtsgeschäfte bleiben weiterhin gültig.[180]

---

[178] Im Hinblick auf die besondere Schnelligkeit des elektronischen Geschäftsverkehrs dürfte der zur Verfügung stehende Zeitraum von drei Stunden viel zu großzügig ausgefallen sein. Innerhalb dieser Zeit könnten eine Unmenge von rechtlich unzulässigen Rechtsgeschäften getätigt werden. Schon aus diesem Grund scheint es viel ökonomischer und sicherer, einen Antrag auf Widerruf außerhalb der Geschäftszeiten einzubringen, da in diesen Fällen die Sperre des jeweiligen Zertifikats „sofort“ auf elektronische Weise veranlaßt wird.

[179] siehe dazu genauer § 13 Abs 4 öSigV

Der in diesem Zusammenhang sehr wichtige Zeitpunkt der Signaturerzeugung ist dementsprechend durch Angabe eines Zeitstempels nach § 10 zu definieren, um Rechtsstreitigkeiten von vornherein gering zu halten. Genauso wichtig zu dokumentieren ist der Empfangs- und Eingangszeitpunkt sämtlicher rechtserheblicher Willenserklärungen durch einen entsprechenden Zeitstempel. Durch einen Vergleich dieser Daten mit den im Zertifikat bzw. in eigenen online-abrufbaren Listen über den genauen Zeitpunkt der Ausstellung, des Widerrufs oder eventueller Sperren[181] und in Listen über den Gültigkeitszeitraum eines Zertifikats enthaltenen Angaben ist es möglich, nachweislich festzustellen, ob die Signatur zu einem Zeitpunkt erstellt wurde, als das Zertifikat Gültigkeit hatte.

Um Rechtsunsicherheit hintanzuhalten, ist eine rückwirkende Sperre bzw. ein rückwirkender Widerruf rechtlich nicht vorgesehen, ebensowenig wie das Rückgängigmachen eines Widerrufs, dieser gilt als unaufhebbar. Die Einrichtung der Sperre hingegen ist nach § 13 Abs. 7 öSigV bloß von vorübergehender Wirkung. Der maximale Zeitraum, für den diese wirken darf, darf drei Werktage nicht übersteigen. Wird die Sperre während dieses Zeitraumes aufgehoben, so erlangt das Zertifikat wieder seine volle Wirkung, die Aufhebung gilt „ex tunc“, was die Rechtswirksamkeit auch während des aufrechten Bestehens der Sperre erzeugter Signaturen bedingt. Wird sie nicht aufgehoben, so ist das Zertifikat zu widerrufen, wobei der Zeitpunkt der erstmaligen Sperre bereits als Zeitpunkt des Widerrufs gewertet wird. Alle seit Wirksamwerden der ursprünglichen Sperre abgeschlossenen Rechtsgeschäfte sind dann als ungültig zu betrachten.

7.13.3 Widerruf des Zertifikats eines Zertifizierungsdiensteanbieters

[180] NR: GP XX RV 1999 AB 2065 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP, S. 3

[181] siehe verpflichtende Regelung des § 9 Abs 4 SigG

Während § 9 Abs. 1 bis 4 die Widerrufbarkeit von Anwender-Zertifikaten durch die Zertifizierungsdiensteanbieter behandelt, setzt Abs. 5 eine Stufe höher an, und zwar bei der Aufsichtsstelle. Diese hat nach § 13 Abs. 3 die Möglichkeit, Zertifikate für Zertifizierungsdiensteanbieter auszustellen, wobei sie sinngemäß die Regelung des § 8 betreffend die Ausstellung qualifizierter Zertifikate durch Zertifizierungsdiensteanbieter zu berücksichtigen hat. Dementsprechend kann sie in Übereinstimmung mit § 12 und § 14 Abs. 5 aus den gesetzlich genannten Gründen der Untersagung bzw. Einstellung der Zertifizierungstätigkeit ohne gleichzeitige Übernahme der Verzeichnislisten die Zertifikate von Zertifizierungsdiensteanbieters auch wieder widerrufen. In einem solchen Fall müssen alle von dem jeweiligen Zertifizierungsdiensteanbieter erstellten Zertifikate widerrufen werden, nach dem Widerrufszeitpunkt erstellte Signaturen – auch die der Anwender - entbehren jeglicher Rechtsgültigkeit. Um die Überprüfbarkeit davor erstellter Signaturen weiterhin zu gewährleisten, ist eine Weiterführung des Widerrufsdienstes unverzichtbar. Grundsätzlich ist der Zertifizierungsdiensteanbieter selbst dafür verantwortlich, erfüllt er diese Verpflichtung nicht, so wird auf dessen Kosten durch die Aufsichtsstelle dafür Sorge getragen.[182]

7.14 § 10 - Zeitstempel

Die im vorstehenden Paragraphen erwähnte Möglichkeit der Anbringung eines Zeitstempels findet eine nähere Regelung in § 10. Ein Zeitstempel gilt „als automatisch erteilte, elektronisch signierte Bescheinigung eines Zertifizierungsdiensteanbieters, dass (ihm) bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen sind".[183] D.h. im Zuge des auf individuelles Verlangen hin erfolgten Anbringens eines Zeitstempels werden die jeweiligen, nach Mitteleuropäischer Zeit gerichteten Angaben[184] elektronisch signiert, wobei hier der

[182] sieh § 14 Abs 5 SigG

[183] *Brenn*, Signaturgesetz, Wien 1999, S. 95

[184] d.h. Datum und Uhrzeit

gesamte Inhalt verschlüsselt wird und nicht wie bei der Signierung eines sonstigen Dokumentes bloß sein Hash-Wert. Das Anbringen eines Zeitstempels erfolgt in der Praxis automatisch, indem das um die Zeitangaben erweiterte Dokument elektronisch signiert und hernach sofort wieder an den Absender zurückgeschickt wird.

Ein derartiger Antrag auf Anbringung eines Zeitstempels ist empfehlenswert bezüglich besonders beweiserheblicher Rechtshandlungen, etwa bei Widerruf, Sperre, Ausstellung und Fixierung der Gültigkeitsdauer eines Zertifikats. Auch bei sonstigen Willenserklärungen ist ein solcher von Vorteil, um eine Vor- bzw. Rückdatierung von elektronischen Dokumenten zu verhindern. Bei qualifizierten Zertifikaten ist die Verwendung qualitätsgesicherter Zeitangaben verpflichtend vorgesehen. Ansonsten ist das Anbieten von Zeitstempeldiensten verschiedenster Sicherheitsstufen freiwilliger Natur, verlangt aber die ausdrückliche Darstellung im jeweiligen Sicherheits- und Zertifizierungskonzept.

Wie bereits erwähnt, können einzelne Dienstleistungen, die in Zusammenhang mit der Erstellung und Verwaltung von Zertifikaten erbracht werden, von verschiedenen Zertifizierungsdiensteanbietern erbracht werden, auch wenn es sich um ein- und dasselbe Zertifikat handelt. Dementsprechend ist das Anbringen von Zeitstempeln allein, ohne zusätzliche Dienste anzubieten, als Tätigkeit eines Zertifizierungsdiensteanbieters nach § 2 Z 10 und 11 zu werten, die Haftungsregelungen des § 23 und die Regelungen betreffend Aufsichtsführung finden dementsprechend volle Anwendung.

Es ist abermals zu unterscheiden zwischen einfachen und qualitätsgesicherten bzw. sicheren Zeitstempeldiensten, erwähnt in § 7 Abs. 1 Z 3 und § 10 SigG und § 14 öSigV. Zweitere haben stets auf einem qualifizierten Zertifikat zu beruhen und den Anforderungen des § 18 vollinhaltlich zu entsprechen, um Richtigkeit und Unverfälschtheit der Zeitangaben zu gewährleisten.

7.15 § 11 - Dokumentation

Die Dokumentation bzw. Protokollierung von im Betriebe einer Zertifizierungsstelle getroffenen Sicherheitsmaßnahmen, von Widerruf, Sperre und Ausstellung eines Zertifikats richtet sich nach § 11 SigG iVm § 16 öSigV. Demzufolge beträgt die Mindestdauer von Bereitstellung, Aufbewahrung und Sicherung genannter Daten 33 Jahre, beginnend mit dem Zeitpunkt der letzten Eintragung. Die dokumentierten Daten sind entsprechend zu signieren. Handelt es sich um einen Diensteanbieter, der qualifizierte Zertifikate ausstellt, so ist dafür wiederum eine sichere elektronische Signatur zu verwenden.

Die vorgesehene Frist von 33 Jahren behält auch bei unvorhersehbaren Zwischenfällen, wie etwa der Einstellung[185] bzw. Untersagung[186] der Tätigkeit eines Zertifizierungsdiensteanbieters ihre Gültigkeit. In diesen Fällen ist die bisher erfolgte Dokumentation an den jeweiligen Übernehmer bzw. der Aufsichtsstelle zu übergeben. Wie bereits unter § 9 öSigG behandelt, sind im Falle des Widerrufs des Zertifikats eines Zertifizierungsdiensteanbieters sämtliche Daten zu archivieren und der Aufsichtsstelle zu übergeben. Eine derartige Archivierung dient der Aufrechterhaltung der Überprüfbarkeit einer alten Signatur auch noch nach dem Widerruf des Zertifikats eines Diensteanbieters.

Das Anlegen von Protokollen dient vor allem der Erleichterung von Beweisführung und nachhaltiger Überprüfbarkeit. Auf Ansuchen von Gerichten und Behörden sind die dokumentierten Daten unter Beachtung innerstaatlicher Verfahrensvorschriften auszuhändigen. Im Falle einer Übernahme trifft die Pflicht zur Aushändigung sodann den übernehmenden Diensteanbieter bzw. die Aufsichtsstelle selbst.[187]

---

[185] siehe § 12 öSigG

[186] siehe § 14 öSigG

[187] *Brenn*, Signaturgesetz, Wien 1999, S. 97ff

7.16 § 12 - Einstellung der Tätigkeit eines Zertifizierungsdiensteanbieters

§ 12 öSigG regelt den Fall der freiwilligen Aufgabe der Zertifizierungstätigkeit. Die Einstellung ist sowohl der Aufsichtsstelle wie auch allen Inhabern eines noch gültigen Zertifikats unverzüglich bekanntzugeben. Um die Überprüfbarkeit bis zu diesem Zeitpunkt erstellter Signaturen zu gewährleisten, hat der Zertifizierungsdiensteanbieter dafür Sorge zu tragen, dass sein Verzeichnis- und Widerrufsdienst durch einen anderen übernommen wird. Gelingt ihm dies nicht, so sind sämtliche Anwender-Zertifikate zu widerrufen. Schäden aus der vorzeitigen Vertragsbeendigung können seitens der Zertifikatsinhaber selbstverständlich geltend gemacht werden. Ist der Diensteanbieter nicht gewillt, für eine derartige Übernahme zu sorgen, so ist die Aufsichtsstelle dazu aufgerufen, auf Kosten des Zertifizierungsdiensteanbieters die Weiterführung der genannten Dienste sicherzustellen.

Eine Übernahme[188] verlangt lediglich den Konsens mit dem neuen Diensteanbieter, nicht jedoch den der Zertifikatsinhaber. Diese haben ohnehin die Möglichkeit, den Widerruf ihrer Zertifikats zu verlangen und zwar zu jeder Zeit und ohne Angabe bestimmter Gründe.

Die Regelung des § 12 findet ebenso Anwendung auf die Fälle der Eröffnung eines Ausgleichs- oder Konkursverfahrens über das Vermögen des Zertifizierungsdiensteanbieters. Diese sind der Aufsichtsstelle unverzüglich anzuzeigen, damit sie in Absprache mit dem Masse- bzw. Ausgleichsverwalter die nötigen Schritte, wie etwa die Übernahme der Dokumentations- und Protokollierungsdienste durch andere Zertifizierungsdiensteanbieter, veranlassen kann. Führt der Masse- bzw. Ausgleichsverwalter die Protokollierungsdienste nicht selbst fort, so hat er die Möglichkeit, diese an einen anderen Diensteanbieter zu übergeben bzw. alle Anwender-Zertifikate zu widerrufen. Grundsätzlich sollte aber aus Gründen des Verbraucherschutzes und der Schadensbegrenzung die Weiterführung bzw.

---

[188] Die Übernahme ist vor allem in den Fällen problematisch, in denen sich die Sicherheits- und Zertifizierungskonzepte des einstellenden und des übernehmenden Zertifizierungsdiensteanbieters unterscheiden. Eine problemlose Übernahme wird daher nur in den Fällen möglich sein, in denen die Konzepte weitgehend übereinstimmen bzw. die Zertifikatsinhaber einer Vertragsänderung zustimmen.

Übernahme sämtlicher angebotener Zertifzierungsdienste angestrebt werden. Die der Aufsichtsstelle durch die Weiterführung der Widerrufsdienste entstehenden Kosten stellen eine bevorrechtete Forderung im Insolvenzverfahren dar.[189]

7.17 §§ 13 und 14 - Die Aufsichtsstelle - Die Telekom-Control-Kommission

Um Sicherheit und Vertrauen in die neuartigen Verfahren zu gewährleisten bzw. zu erhöhen, sind besondere Aufsichtsstellen einzurichten. In Österreich ist dies konkret die idR nur alle zwei Wochen tagende Telekom-Control-Kommission (TKK)[190], eine weisungsfreie Kollegialbehörde mit richterlichem Einschlag. Sie setzt sich aus drei, von der Bundesregierung auf jeweils fünf Jahre ernannten Mitgliedern zusammen, die über die notwendigen technischen, juristischen und ökonomischen Kenntnisse zu verfügen haben. Den Vorsitz unter den ständigen Mitgliedern führt ein Richter. Bei der Bewältigung ihrer Aufgaben stehen ihnen die Telekom-Control Österreichische Gesellschaft für Telekommunikationsregulierung m.b.H., kurz Telekom-Control GmbH (TKC)[191], und eigene Bestätigungsstellen zur Seite. Die Aufsichtsstelle und die in ihrem Namen tätigen weisungsfreien und der Amtsverschwiegenheit unterliegenden Mitarbeiter haben die Einhaltung der Bestimmungen des Signaturgesetzes und der auf dessen Grundlage ergehenden Verordnungen zu überwachen, den Sicherheitsstandard der angebotenen Verfahren durch Expertisen festzustellen und geeignete Aufsichtsmaßnahmen zu treffen.

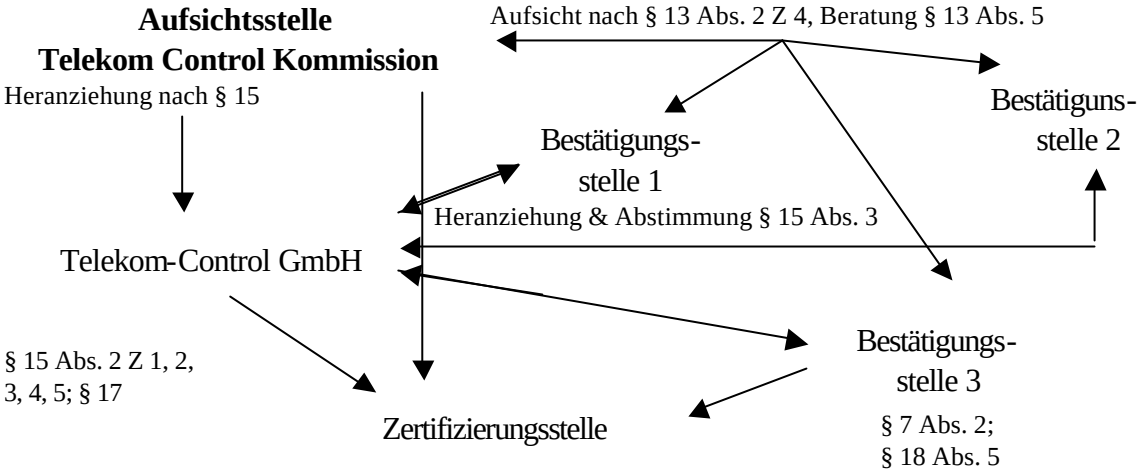
---

189 § 46 KO zählt die bevorrechteten Masseforderungen in taxativer Weise auf. Diejenigen der Aufsichtsstelle beruhen auf den Regeln über die Geschäftsführung ohne Auftrag, d.h. § 1042 ABGB iVm § 12 SigG. Diese finden keine Erwähnung in der betreffenden konkursrechtlichen Norm und würden als schlichte Konkursforderungen zu gelten haben.

190 siehe unter http://www.tkc.at/www/TKC_main.nsf/pages/Signatur

191 Gesetzliche Grundlage der Telekom-Control-GmbH und der ihr untergeordneten Behörden ist das BG betreffend die Telekommunikation 1997 (Telekommunikationsgesetz - TKG), BGBl. I Nr. 100/1997

Zur besseren Veranschaulichung des doch etwas kompliziert aufgebauten Aufsichtssystems im österreichischen Signaturgesetz die folgende Skizze:[192]



Vorbehaltlich spezialgesetzlicher Regelungen findet das AVG 1991 volle Anwendung, der Instanzenzug geht bis zum VwGH[193]. So wie die Telekom-Control Kommission selbst bzw. ihre Mitarbeiter in Ausübung ihrer Tätigkeit unabhängig und weisungsfrei agieren, so kommt ihr auch gegenüber den Bestätigungsstellen kein Recht zur Erteilung von Weisungen zu.[194] Als Bundesbehörde unterliegt die Tätigkeit der Aufsichtsstelle dem Amtshaftungsgesetz und sämtlichen strafrechtlichen Vorschriften betreffend Amtsdelikte. § 18 Abs. 5 öSigV entsprechend unterliegen die Aufsichtsstelle selbst und auch sämtliche für sie tätigen Organe, Personen und Einrichtungen der Amtsverschwiegenheit nach Art. 20 Abs.3 B-VG.

---

192 *Mayer-Schönberberger/ Pilz/ Reiser/ Schmölzer*, Signaturgesetz: Praxiskommentar, Wien 1999, S. 34

193 Der VwGH ist die Instanz bezüglich jeder Entscheidung der Telekom-Control-Kommission, sowohl wegen einer Verletzung von Verfahrensvorschriften wie auch wegen einer allfälligen inhaltlichen Rechtswidrigkeit. Im Verwaltungsstrafverfahren geht der Instanzenzug von der zuständigen Bezirksverwaltungsbehörde zum Unabhängigen Verwaltungssenat des jeweiligen Landes.

194 so ausdrücklich auch § 13 Abs 6 öSigG

7.17.1 Aufgabenbereich

In § 13 SigG wie auch im Telekommunikationsgesetz werden die der Aufsichtsstelle zukommenden Aufgaben in demonstrativer, nicht abschließender Art und Weise aufgezählt.[195] Im Rahmen ihrer Aufsichtstätigkeit hat sie unter anderem Bescheide über die Erteilung von Auflagen zur Mängelbehebung oder zur Untersagung der Zertifizierungstätigkeit zu erlassen und ist ebenso zuständig für das Verfahren der freiwilligen Akkreditierung.

Die Aufsichtsstelle wie auch die Zertifizierungsdiensteanbieter selbst sind ermächtigt, Zertifikate für die Erbringung der Zertifizierungstätigkeit auszustellen. Stellt sich ein Zertifizierungsdiensteanbieter sein Zertifikat selber aus, so ist dieses der Aufsichtsstelle anzuzeigen und in das dort geführte Verzeichnis aufzunehmen. Auf diesem Weg, d.h. durch die Signierung seitens der Aufsichtsstelle wird auch dieses, ursprünglich von der Zertifizierungsstelle ausgestellte Zertifikat zu einem ihr zuzuordnenden.

Neben den Zertifikaten sind auch die von ihr geführten Verzeichnisse mit einer sicheren Signatur zu schützen. Das dafür erforderliche zugrundeliegende Zertifikat hat sie sich selber auszustellen und bedarf zudem einer Veröffentlichung im Amtsblatt zur Wiener Zeitung. Infolgedessen ist selbst dieses Zertifikat trotz fehlender Aufnahme in ein entsprechendes Verzeichnis auf ihre Richtigkeit hin jederzeit und allgemein überprüfbar. Die Signaturverordnung sieht weiters vor, dass die Aufsichtsstelle zu jeder von ihr verwendeten Signatur auch eine Zweitsignatur zu erzeugen und alle ihre Signierungen auch mit diesem Zweitschlüssel durchzuführen hat.[196] Dieses Erfordernis bezweckt eine doppelte Sicherheit

---

[195] siehe § 111 TKG

[196] Dies bedeutet im einzelnen, daß die Aufsichtsstelle alle von ihr ausgestellten Signaturen auch mit dem jeweiligen privaten Zweitschlüssel zu signieren hat. Der öffentliche Zweitschlüssel wird wiederum mit dem privaten Erstschlüssel signiert und ist im Gegensatz zu sonstigen Signaturprüfdaten vorerst nicht öffentlich zugänglich zu machen. Erst im Falle einer Kompromittierung des Erstschlüssels steht auch dieser zur Verfügung, um den Fortbestand und die Sicherheit aller bereits signierten Dokumente weiter zu sichern - diesmal auf Grundlage des Zweitschlüsselpaares, welches nicht kompromittiert wurde.

und die Möglichkeit einer ununterbrochenen und ungestörten Weiterführung ihres Betriebes bei Ausfall oder Unbrauchbarkeit des Erstschlüssels.[197]

Die Führung der in Abs. 3 genannten Verzeichnisse begründet eine weitere nicht unbedingt in Anspruch zu nehmende Überprüfungsmöglichkeit der Zertifikats-Aussteller. Zertifikate der Zertifizierungsdiensteanbieter sind auch insoweit unabhängig von dem der Aufsichtsstelle, als bei Kompromittierung des zweiteren die Gültigkeit des erstgenannten nicht berührt wird.

Gesetzlich bisher nicht geregelt bzw. überhaupt nicht in Betracht gezogen ist die Möglichkeit des Widerrufs des Zertifikats einer Aufsichtsstelle – diese wäre in das Gesetz noch einzufügen. Vielmehr sind für den Fall, dass die Sicherheit, Einmaligkeit und Geheimhaltung des ihr zugeordneten privaten Signaturschlüssels nicht mehr absolut gewährleistet ist, sämtliche von ihr mit den alten Signaturerstellungsdaten unterzeichneten Daten mit einem neu zu generierenden Schlüssel zu signieren.[198]

7.17.1.1 Aufsichtsmaßnahmen

Wie bereits erwähnt, hat die Telekom-Control-Kommission die Verpflichtung zur Führung der Aufsicht über die im Inland ansässigen Zertifizierungsdiensteanbieter. Zu diesem Zweck ist ihr von gesetzlicher Seite ein breiter Handlungsspielraum eingeräumt bishin zur gänzlichen oder teilweisen bescheidmäßigen Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters. Während § 14 Abs. 3 und 4 ausschließlich auf Aussteller qualifizierter Zertifikate Bezug nehmen, sind ansonsten generell alle Zertifizierungsdiensteanbieter unter die Kontrolle der Aufsichtsstelle gestellt. Unter Berücksichtigung der Grundsätze von Verhältnismäßigkeit und Angemessenheit ist das jeweils gelindeste, zum angestrebten Ziel führende Mittel einzusetzen.

---

[197] siehe Regelung des § 3 Abs 1 öSigV

[198] NR: GP XX RV 1999 AB 2065 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP, S. 3f

In diesem Sinne ermöglicht Abs. 6 leg.cit. die bloße Androhung von Maßnahmen unter Setzung einer Frist wie auch die Erteilung von Auflagen. Reichen diese Mittel nicht aus, um die Einhaltung gesetzlicher und verordnungsrechtlicher Pflichten sicherzustellen, kann die Aufsichtsstelle die Tätigkeit als Zertifizierungsdiensteanbieter untersagen und im Zuge dessen deren Zertifikate wie auch die auf Inhaber lautenden widerrufen.

Im Falle einer Untersagung hat sie entweder für den Widerruf der jeweiligen Zertifikate und bzw. oder für die Übernahme der Signatur- und Zertifizierungsdienste bzw. der Verzeichnisdienste zu sorgen. Einer Übernahme müssen sowohl die übergebenden als auch die übernehmenden Diensteanbieter zustimmen, da unter anderem auch die Firma des von der Aufsichtsstelle untersagten Anbieters weiterzuführen ist. Eine Zustimmung der Signatoren selbst ist hingegen nicht vorgesehen, da diese ohnehin auf eine weitere Inanspruchnahme ihrer Signatur verzichten bzw. ihr Zertifikat jederzeit widerrufen können. Unentbehrlich ist die Weiterführung der Verzeichnisse der widerrufenen Zertifikate, um deren Überprüfbarkeit auch nach dem Wegfall des Zertifizierungsdiensteanbieter-Zertifikats weiterhin zu ermöglichen.

7.17.2 Vorschreibung von Gebühren

Berechtigterweise umstritten ist die Regelung des § 13 Abs 4, welcher die Vorschreibung von Gebühren für die Erbringung der Dienstleistungen der Aufsichtsstelle, der Telekom-Control GmbH und der Bestätigungsstellen auf verordnungsrechtlichem Wege beinhaltet. Siehe ausführlich dazu unter Kapitel 7.29.

7.18 § 15 - Die Telekom-Control GmbH[199]

Die Agenden der Aufsichtsstelle zur Seite gestellten Telekom-Control GmbH sind hauptsächlich unterstützender Natur, demonstrativ und beispielhaft aufgeführt in § 15. In ihren Aufgabenbereich fallen hauptsächlich Registrierungs- und Überwachungstätigkeiten.

Eine ihrer wichtigsten Agenden dürfte die Erstellung und Führung von online-abrufbaren Verzeichnissen über sämtliche gültigen, widerrufenen und gesperrten Zertifikate von inländischen Diensteanbietern sein. Weiters sind sämtliche inländischen, die von ihr akkreditierten sowie alle Diensteanbieter aus Drittstaaten, für deren Zertifikate ein inländischer Zertifizierungsdiensteanbieter einsteht, in die jeweiligen Zertifikate aufzunehmen. Laut Begründung im Abänderungsantrag dürfen in das Verzeichnis der Zertifikate für Zertifizierungsdiensteanbieter nur qualifizierte Bescheinigungen aufgenommen werden.

Sind bei der Bewältigung ihrer gesetzlich übertragenen Aufgaben auch komplizierte technische Belange betroffen, so kann sich die TKC der Hilfe einer Bestätigungsstelle bedienen. Im Rahmen ihres Tätigwerdens für die Aufsichtsstelle ist das Personal weisungsgebunden. Die Telekom-Control GmbH ist jene Stelle, die für die tagtäglich wiederkehrenden Kontroll- und Aufsichtstätigkeiten zuständig ist. Dementsprechend ist ihr auch die Möglichkeit eingeräumt, bei begründetem Verdacht vorläufige Maßnahmen anzuordnen. § 15 Abs. 1 Z 7 räumt ihr auch die Möglichkeit der vorläufigen Untersagung der Zertifizierungstätigkeit ein. Die endgültige Entscheidung wird jedoch auch hier von der Telekom Control Kommission getroffen. Dies bedeutet im einzelnen, dass die Zurücknahme eines vorläufig angeordneten Widerrufs , d.h. ein zweiter Widerruf, ex nunc zu gelten hat. Ist der zuerst erfolgte Widerruf der Telekom-Control GmbH zu Unrecht erfolgt, so wäre das Bestehen einer Haftungspflicht gesondert zu überprüfen.

199 einsehbar unter http://www.signatur.tkc.at

Unbeschadet der Möglichkeit der Beschreitung des gerichtlichen Klageweges kommt der TKC im Rahmen der Streitschlichtung eine besondere Stellung zu. Privatpersonen wie auch Interessenvertretungen, Zertifizierungsdiensteanbieter wie auch Zertifikatsinhaber können Differenzen vor die Telekom-Control-GmbH bringen, welche auf eine einvernehmliche, außergerichtliche Streitbeilegung hinzuwirken hat.[200]

Soweit sie in Vollziehung der Gesetze tätig wird, hat sie sich als beliehenes Unternehmen an die Verpflichtung zu Amtsverschwiegenheit zu halten, unterliegt dem AHG und den strafrechtlichen Bestimmungen betreffend Amtsdelikte. Besteht ein unmittelbarer Handlungsbedarf, etwa bei vermuteter Ausforschung der Signaturerstellungsdaten, so kann sie vorläufig spezielle Maßnahmen, darunter auch die Untersagung der Tätigkeit anordnen. Die endgültige Entscheidung obliegt einzig und allein der nationalen Aufsichtsstelle in Form der Erlassung von Bescheiden. Genauere Regelungen betreffend das Verhältnis von Telekom-Control-GmbH, Telekom-Control-Kommission und Bestätigungsstelle finden sich im Telekommunikationsgesetz, kurz TKG.

7.19 § 16 - Mitwirkungspflichten am Aufsichtsverfahren

Entsprechend § 16 sind die involvierten Zertifizierungsdiensteanbieter bei Durchführung der Aufsicht zu Auskunftserteilung und Mitwirkung verpflichtet, da ansonsten keine effiziente Kontrolle möglich wäre. Unter anderem ist das Betreten der Geschäfts- und Betriebsräume zu gestatten, ebenso wie die Einsichtnahme in Geschäftsbücher und sonstige Unterlagen. Auf Ersuchen der Aufsichtsstelle hin haben auch die Organe des öffentlichen Sicherheitsdienstes entsprechend Hilfe zu leisten. Von diesen Offenlegungs- und Unterstützungspflichten unberührt bleiben bestehende, andersgesetzlich fixierte Rechte zu Verschwiegenheit und Aussageverweigerung. Zertifizierungsdiensteanbieter haben sich ebenso an außerhalb des

[200] genauer ausgeführt in § 15 Abs 4 öSigG

Signaturgesetzes normierten Verpflichtungen zu Auskunftserteilung und Datenübermittlung gegenüber staatlichen Behörden als gebunden zu erachten. Das hier in Rede stehende Regelungswerk schafft insoweit keine spezialgesetzlichen Normen. Die Durchführung der Aufsicht hat Abs. 3 folgend unter möglichster Schonung der Betroffenen zu erfolgen, dies vor allem im Hinblick darauf, dass die Sicherheit der Signatur- und Zertifizierungsdienste dabei weiterhin gewahrt bleibt. Der damit angesprochene Grundsatz der Verhältnismäßigkeit scheint jedoch insoweit zumindest ernstlich gefährdet zu sein, als sämtliche Eingriffsbefugnisse ohne vorherig einzuholende gerichtliche oder behördliche Genehmigung voll ausgeschöpft werden können. Es ist zu überlegen, ob nicht die Aufsichtsmittel des Widerrufes bzw. einer Sperre des Zertifikats eines Zertifizierungsdiensteanbieters voll ausreichen würden, um die Einhaltung der gesetzlich normierten Anforderungen sicherstellen zu können. Allein durch diese Zwangsmittel könnte die für die Durchführung von Aufsicht und Kontrolle unbedingt erforderliche Zugänglichmachung von Räumlichkeiten und Unterlagen erzielt werden, ohne einen ernsthaften Eingriff in die Grundrechte des Diensteanbieters in Kauf nehmen zu müssen. Wäre auf diesem Wege eine ordnungsgemäße und störungsfreie Kontrolltätigkeit nicht durchführbar, so könnte noch immer auf die eingriffsintensiveren Zwangsmittel der StPO[201] zurückgegriffen werden.[202]

7.20 § 17 - Freiwillige Akkreditierung

Genehmigungspflichten und die Ausübung der Tätigkeit eines Zertifizierungsdiensteanbieters einschränkende und behindernde Maßnahmen sind der Richtlinie über elektronische Signaturen folgend generell ausgeschlossen. Davon nicht erfasst sind Systeme der freiwilligen Akkreditierung, die auf die Bereitstellung höherwertiger Dienste abzielen. Eine genauere Regelung dieser findet sich in § 17 leg.cit., wobei sich dessen Anwendbarkeit nur auf Anbieter qualifizierter Zertifizierungsdienste erstreckt. Auf individuellen Antrag hin werden im Rahmen des Verfahrens der Akkreditierung nach eingehender Überprüfung bereits vor Aufnahme der

[201] Strafprozessordnung 1975/631 idgF., §§ 139ff

[202] siehe auch die Ausführungen des Österreichischen Rechtsanwaltskammertages, AnwBl 1999, S. 392ff

Tätigkeit die Einhaltung des Gesetzes und der darauf beruhenden Verordnungen bescheinigt und infolge dieser Bescheiderteilung besondere Rechte zuerkannt. Diese bestehen etwa in der Ermächtigung des Diensteanbieters, öffentlich die Bezeichnung eines „akkreditierten" Unternehmens tragen zu dürfen, womit wettbewerbsrechtliche Vorteile verbunden sein dürften, da ihre Signaturprodukte als besonders sicher einzustufen sind. Denkbar ist auch die Akkreditierung erst im nachhinein, d.h. nach Aufnahme der Zertifizierungsdienste. Da sich die Kontrolle der Aufsichtsstelle speziell auf alle im Inland akkreditierten Diensteanbieter erstreckt,[203] ist die Aberkennung der Akkreditierung und der damit verbundenen Rechte ebenso jederzeit möglich, falls die entsprechenden Anforderungen nicht mehr eingehalten werden.

Um dem Publizitätserfordernis gerecht zu werden, hat die Aufsichtsstelle bzw. die Telekom-Control-GmbH[204] ein Verzeichnis der akkreditierten Zertifizierungsdiensteanbieter zu führen. Die freiwillige Akkreditierung ist in das jeweilig Zertifikat aufzunehmen bzw. sonst allgemein zugänglich zu machen.

7.21 § 18 - Technische Sicherheitsanforderungen

Wiederholt Bezug genommen wird auf § 18 des Gesetzes, welcher die Anforderungen an Signaturerstellungs- und Signaturprüfeinheiten wie auch an Zertifikate festlegt, um die Bezeichnung „sicher" tragen zu können. Dabei sind sowohl die im Rahmen der Signierung auf Seiten der Zertifizierungsdiensteanbieter wie auch auf Seiten der Anwender, der Signatoren selbst, zum Einsatz kommenden Produkte und Verfahren, umfasst. Die konkrete Ausgestaltung dieser Norm orientiert sich sehr stark an den Vorgaben der Richtlinie.

---

[203] Allein entscheidend ist die Akkreditierung im Inland, unabhängig davon, ob es sich um in- oder Ausland niedergelassene Zertifizierungsdiensteanbieter handelt.

[204] siehe § 15 Abs 2 Z 3 öSigG

Die Basis des Vertrauens der Anwender bildet die absolute Sicherheit sämtlicher technischer Komponenten, die während eines Signierungsvorganges zum Einsatz gelangen. Diese unterliegen einer ständigen Überprüfung, um dem neuesten Stand der Technik und Wissenschaft jederzeit voll zu entsprechen. Dabei werden verschiedenste, einer ständigen Veränderung unterliegende Standards festgelegt, um die angebotenen Sicherheitstechnologien nach Qualität und Vertrauenswürdigkeit einstufen zu können.[205] Detaillierte Regelungen finden sich in der Signaturverordnung, welche der Kurzweiligkeit technischer Neuheiten und dem ständigen Anpassungsbedarf gerecht wird. Unentbehrlich in diesem Kontext ist die Interoperabilität der verwendeten Formate, Algorithmen und Standards. Der elektronische Geschäftsverkehr operiert über bestehende Grenzen hinweg, allzugroße Differenzen bei verwendeten Verfahren würden zu einer ernsthaften Behinderung führen. Aus diesem Grund ist besonders in diesem Bereich ein Tätigwerden der Europäischen Kommission auf übernationaler Ebene gefragt.

7.22 § 19 - Bestätigungsstellen

Da für den einzelnen Anwender die Qualität der von den Dienstleistungsanbietern angepriesenen Signaturkomponenten aufgrund fehlender Sachkunde nicht feststellbar ist, haben sogenannte Bestätigungsstellen schon im vorhinein durch Gutachtenserstellung zu bescheinigen, ob bei den jeweiligen Signaturprodukten und -verfahren die Einhaltung der in § 18 öSigG normierten Sicherheitsanforderungen überhaupt denkbar ist. Für die Erstellung sicherer elektronischer Signaturen dürfen ausschließlich Produkte und Verfahren verwendet werden, die einer vorherigen Prüfung durch eine Bestätigungsstelle standgehalten haben.[206] Will ein Zertifizierungsdiensteanbieter die Einhaltung sämtlicher, in § 18 normierter technischer Erfordernisse bestätigt wissen, so kann er dies im Rahmen einer Akkreditierung erreichen. Die

---

[205] siehe Standard ITSEC, Standard Common Criteria unter http://www.a-sit.at, British Standard

[206] *Brenn*, Das österreichische Signaturgesetz - Unterschriftenersatz in elektronischen Netzwerken, ÖJZ 1999, S. 593

mit besonderer Fachkunde ausgestatteten Stellen haben Erkenntnisse von Sicherheitsbehörden und ausländischen Behörden bei ihren Nachforschungen zu berücksichtigen.

Vertrauenswürdigkeit und Objektivität der öffentlichen oder privaten Bestätigungsstellen wird durch die zwingend vorgeschriebene vorherige Benennung durch eine dafür zuständige Stelle[207] gewährleistet. Ein zeitgleiches Tätigwerden als Bestätigungsstelle und Zertifizierungsdiensteanbieter ist schon dem Grunde nach miteinander unvereinbar. Im Rahmen ihrer Prüf- und Evaluationstätigkeit unterliegen die Bestätigungsstellen der organisatorischen Kontrolle der Aufsichtsstelle und gelten ebenso wie die Telekom-Control-GmbH als beliehenes Unternehmen. Das entsprechende Entgelt für die Erbringung ihrer Dienste einschließlich für die von anderen Stellen verfassten Prüfberichte haben sie selbst einzuheben, nicht die Aufsichtsstelle oder andere dritte Stellen, deren Hilfe sich die Bestätigungsstelle bedient. Im Falle von Untätigkeit oder mangelhafter Erfüllung ihrer Aufgaben ist den Antragstellern laut § 13 Abs. 2 Z 4 die Möglichkeit eingeräumt, Beschwerde bei der Aufsichtsstelle einzubringen, wobei jedoch kein subjektives Recht auf Behandlung bzw. Entscheidung besteht.

7.22.1 Zentrum A-Sit

In Österreich übernimmt die Aufgabe einer Bestätigungsstelle zur Zeit der erst im Mai dieses Jahres gegründete Verein „Zentrum für sichere Informationstechnologie (A-Sit)“,[208] dem Aufgaben im Bereich von Evaluation, Koordination, Forschung und öffentlicher Bewusstseinsbildung zukommen. Mitglieder des Vereines sind das BMinFin, die Österreichische Nationalbank und die Technische Universität Graz. Bislang ist dies die einzige Bestätigungsstelle, deren Eignung durch Verordnung des Bundeskanzlers öffentlich festgestellt

[207] Gemäß § 19 Abs. 3 ist die Eignung mit VO des Bundeskanzlers im Einvernehmen mit dem BM für Justiz festzustellen.

[208] Rechtliche Grundlage des Vereines A-Sit ist BGBl II 31/2000; einsehbar unter http://www.a-sit.at.

wurde. Die Beurteilung der Eignung hat sich an den Vorgaben des Gesetzes zu orientieren, wobei wiederum die Kommission zur Fixierung bestimmter Kriterien ermächtigt ist, welche sodann als Grundlage heranzuziehen sind.[209] Aufgrund der Kostspieligkeit und Kompliziertheit von durch die Bestätigungsstelle vorzunehmenden Prüfverfahren ist ihr durch Abs. 4 leg.cit. ausdrücklich die Ermächtigung eingeräumt, zur Erfüllung ihrer Aufgaben Prüfberichte anderer kompetenter Stellen einzuholen.

Wird von einer nationalen, gegenüber der Kommission notifizierten Bestätigungsstelle die Übereinstimmung mit den Anforderungen der Anhänge der Richtlinie bzw. des § 18 des öSigG festgestellt, so ist diese Bescheinigung auch in allen anderen Mitgliedstaaten der Europäischen Gemeinschaft anzuerkennen.[210] Die Kommission kann laut Art 3 Abs. 5 iVm Art 9 in Zusammenarbeit mit einem dafür zuständigen „Ausschuss für elektronische Signaturen" spezielle Normen[211] für Signaturprodukte und -verfahren, wie auch für sichere Signaturerstellungseinheiten festlegen. Entsprechen nun die zum Einsatz gelangenden Komponenten diesen, so haben die geltenden Sicherheitsanforderungen automatisch ebenso als erfüllt zu gelten.[212] Die eben genannte Rechtsfolge der automatischen Anerkennung ist bislang im österreichischen Signaturgesetz nicht ausdrücklich normiert, weshalb bis dato das Gleichwertigkeitserfordernis gegenüber Bescheinigungen aus Drittstaaten wie auch aus Mitgliedstaaten gleichermaßen gilt. Um der Richtlinie voll zu entsprechen, ist eine Ergänzung in

---

209 siehe § 19 öSigG und Art 3 Abs 4 SigRl

210 siehe Art 3 Abs 4 SigRl

211 Unter einer Norm ist, der Ansicht der Kommission folgend, ein rechtlich unverbindlicher Standard zu verstehen, der lediglich aufgrund seiner wiederholten Bezugnahme durch ein anerkanntes Normungsgremium eine Art Muster- und Vorbildwirkung erlangt hat. Diese Standards sind unverbindlicher Natur, es kann jederzeit davon abgegangen werden, jedoch hat der jeweilige Diensteanbieter in diesem Fall die Übereinstimmung mit den Sicherheitsanforderungen des Gesetzes bzw. der Richtlinie gesondert nachzuweisen. Diese Pflicht entfällt bei Verwendung bereits vorgegebener Kriterien, hier wird die Richtlinienkonformität vermutet. Dargestellt in *Gravesen/Dumortier/Van Eecke*, Europäische Signaturrichtlinie, MMR 10/1999, S. 584

212 siehe *Brenn*, Signaturgesetz, S. 123f

der Hinsicht erforderlich, dass eine in einem Mitgliedstaat der Union ausgestellte Bestätigung per se und ohne jegliche weitergehende Überprüfung den inländischen gleichzuhalten ist.

7.23 §§ 20 und 21 - Rechte und Pflichten der Anwender

In der Regel dürfte der einzelne Anwender über ein relativ geringes technisches Hintergrundwissen bezüglich Signaturverfahren und -komponenten verfügen. Um trotz dieses Faktums die absolute Sicherheit einer Signierung auf elektronischem Wege gewährleisten zu können, sind die technisch versierten Zertifizierungsdiensteanbieter zu entsprechender Information und Unterrichtung aufgerufen. Wird einer Person etwa ein Zertifikat bzw. ein qualifiziertes Zertifikat ausgestellt, so ist ihm *„über alle sicherheitsrelevanten Maßnahmen bei deren Anwendung (z.B. Sicherheit des Autorisierungscodes, Prüfung des Ausschlusses fremder Verwendung, Inanspruchnahme der Verzeichnis- und Widerrufsdienste, Möglichkeit der Anzeige zu signierender Daten, Verwendung geeigneter Formate)“*[213] Auskunft zu erteilen. Erst auf diesem Wege ist es dem einzelnen Anwender überhaupt möglich, sich in gesetzeskonformer Weise zu verhalten, für die Geheimhaltung seines ihm alleinig zugeordneten privaten Schlüssels zu sorgen und im Falle von Rechtsstreitigkeiten Rückgriffsmöglichkeiten auf den Zertifikatsaussteller in Anspruch nehmen zu können. Laut Anhang II lit. k der Richtlinie müssen die genannten Infos *„mit einem dauerhaften Kommunikationsmittel“* erbracht werden, d.h. auf schriftlichem oder elektronischem Wege in klar verständlicher Sprache. Die Informationen müssen dem Empfänger dauerhaft zugänglich gemacht werden. Diesem Erfordernis wird voll Rechnung getragen, wenn der Text online abgerufen, gespeichert oder ausgedruckt werden kann. Da in der Regel auch von Seiten der mit dem Zertifikatsinhaber in Verbindung stehenden Geschäftspartner ein rechtliches Interesse an der Einsichtnahme bestehen wird, ist die Zugänglichkeit auch diesen auf individuellen Antrag hin zu gewähren.

Bei ordnungsgemäßer Informationserbringung seitens der Zertifizierungsdiensteanbieter hat sich der Signator entsprechend zu verhalten und seinen ihn individuell treffenden Sorgfalts- und

Anzeigepflichten nachzukommen. Werden ihm etwa Umstände bekannt, die eine Kompromittierung seiner Signaturerstellungsdaten vermuten lassen oder stimmen die in das Zertifikat bei dessen Ausstellung aufgenommenen Daten aufgrund geänderter Rechts- oder Tatsachenverhältnisse nicht mehr mit der Realität überein, so hat er die Zertifizierungsstelle bzw. die Aufsichtsstelle unverzüglich davon in Kenntnis zu setzen bzw. in gravierenden Fällen den Widerruf seines Zertifikats zu verlangen - was schließlich und endlich auch zu seiner eigenen Sicherheit erfolgt, da er ansonsten aufgrund des Rechtsscheins für in seinem Namen unbefugterweise abgeschlossene Rechtsgeschäfte in Anspruch genommen werden könnte.[214]

7.24 § 22 - Datenschutzrechtliche Aspekte

Artikel 8 der Signaturrichtlinie bzw. der entsprechende § 22 des österreichischen Signaturgesetzes iVm den jeweiligen zur Anwendung gelangenden datenschutzrechtlichen Vorschriften dürften in der Praxis an Bedeutung gewinnen. Die europäischen Gesetzgebungsorgane hielten es in Erwägungsgrund 24 der Signaturrichtlinie ausdrücklich fest, dass *„die Zertifizierungsdiensteanbieter die Vorschriften über den Datenschutz und den Schutz der Privatsphäre achten müssen“*. Damit gemeint ist vor allem die Datenschutzrichtlinie aus dem Jahr 1995[215], aber auch die damit in Einklang stehenden nationalen Vorschriften, wie das DSG[216] in Österreich.

Die Erhebung personenbezogener Daten hat nach den Grundsätzen von Verhältnismäßigkeit und Zweckbindung zu erfolgen, zudem ist idR die Zustimmung des Betroffenen einzuholen.

---

213 siehe § 10 Abs 7 öSigV

214 siehe dazu wie auch zur Problematik des Vertrauensschutzes und haftungsrechtlicher Fragen bei einer Vertretung ohne entsprechende Vertretungsmacht (falsus procurator) *Koziol* in *Koziol/Welser*, Bürgerliches Recht[11], Bd. 1, Wien 2000, S. 182ff und *Dittrich/Tades*, ABGB[35], E 102 zu § 863

215 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, Art. 1, 6, 7, 10

216 BG über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000) BGBl. I Nr. 165/1999

Erklärt sich ein Zertifikatswerber nicht dazu bereit, die zur Ausstellung unbedingt erforderlichen Angaben zu erteilen und kann infolgedessen der Aussteller die Richtigkeit der in das Zertifikat aufzunehmenden Daten nicht verlässlich überprüfen, so ist die Ausstellung zu verweigern. Da die Verwendung eines Pseudonyms anstelle des bürgerlichen Namens nach § 8 Abs. 4 gerade den Zweck hat, im täglichen Geschäftsverkehr ohne Angabe der Identität auftreten zu können, ist die Aufdeckung und Übermittlung dieses Decknamens nach den Regelungen des Datenschutzgesetzes nur bei nachgewiesenem rechtlichen Interesse vorgesehen. Wird etwa das Einbringen einer zivilrechtlichen Klage beabsichtigt, so ist dazu die Angabe des Namens unbedingt erforderlich, ein Pseudonym allein genügt dem Bestimmtheitserfordernis nicht. Auch die nationalen Sicherheitsbehörden sind im Rahmen der Verfolgung strafbarer Handlungen auf die Offenlegung seitens der Zertifizierungsdiensteanbieter angewiesen.

7.25 § 23 - Haftung von Zertifizierungsdiensteanbietern

7.25.1 Vertragshaftung

Zwischen Zertifizierungsstelle und Zertifikatsinhaber besteht aufgrund des zwischen ihnen bestehenden Vertragsverhältnisses eine relativ umfangreiche Haftung für Haupt-, Schutz- und Fürsorgepflichten. Dabei handelt es ich um einen Vertrag sui generis, der aus hauptsächlich dienst- und werkvertraglichen Elementen besteht. Die Zertifizierungsstelle hat in dessen Rahmen einzustehen für die ordnungsgemäße Schlüsselzuordnung und -verwaltung, die Ausstellung und Verwaltung eines gültigen Zertifikats, die Auskunftserteilung durch einen jederzeit aktuellen Verzeichnisdienst und die Einhaltung ausreichender Sicherheitsvorkehrungen.

Die jeweiligen Ansprüche gründen sich dabei auf dem Institut der positiven Vertragsverletzung gemäß § 1295 Abs. 1 ABGB. Dies impliziert den vollen Ersatz von Vermögensschäden auch bei bloßer Fahrlässigkeit, den Ersatz von Mangelfolgeschäden nach § 932 Abs. 1 letzter Satz

iVm 1435 ABGB, die Umkehr der Beweislast nach § 1298 ABGB und volle Erfüllungsgehilfenhaftung. Als Rechtsgrundlage letzteren Charakteristikums der Vertragshaftung dient § 1313 a ABGB, aufgrund dessen sämtliche Mitarbeiter - auch die ausgegliederter Registrierungsstellen - als Erfüllungsgehilfen zu qualifizieren sind, für welche der Diensteanbieter in vollem Umfang einzustehen hat. Die Verschiebungen hinsichtlich der Beweislast beziehen sich nur auf das Verschulden, nicht jedoch auf die Kausalität, welche weiterhin vom Gläubiger, d.h. in diesem Fall vom geschädigten Zertifikatsinhaber, darzulegen ist. Als Folge der dargestellten Rechtslage hat die Zertifizierungsstelle bei zu vertretender leichter Fahrlässigkeit gemäß § 1324 iVm § 1323 ABGB nur den positiven Schaden zu ersetzen. Handelt es sich jedoch um ein Handelsgeschäft im Sinne von Art.8/2 der 4.EVHGB oder um grob fahrlässiges oder vorsätzliches Handeln so ist volle Genugtuung zu leisten, worunter auch der Ersatz eventuell entgangenen Gewinnes fällt. Die Beweislast für grobe Fahrlässigkeit wie auch Vorsatz hat der Geschädigte zu tragen. Abschließend erwähnt sei die weiterhin bestehende Möglichkeit der Vertragspartner, im Rahmen jedes einzelnen Vertrages das Ausmaß der Haftung individuell festzulegen, d.h. bis zu einem gewissen Maß zu begrenzen.

Wie eben dargelegt ist der in einer Vertragsbeziehung stehende Zertifikats-Inhaber durch die Regelungen des allgemeinen Schadenersatzrechtes ausreichend geschützt. Hier bedarf es keiner zusätzlichen Normen, welche auf die Besonderheiten des elektronischen Geschäftsverkehrs im speziellen eingehen, keiner Gefährdungshaftung und keiner Analogieschlüssel zu vergleichbaren Vorschriften.

7.25.2 Deliktische Haftung

Zwischen der Zertifizierungsstelle und etwaigen zukünftigen Vertragspartnern des Zertifikatsinhabers besteht in der Regel keinerlei Vertragsbeziehung. In vielerlei Fällen können diese - vorerst „unbeteiligen - Dritten“ auf den ursprünglichen Vertragspartner nicht mehr zurückgreifen, sei es etwa weil es auf Seiten des Zertifikatinhabers an jedem Verschulden fehlt oder weil dieser schlichtweg nicht ausgeforscht werden kann. In diesen Fällen bleibt lediglich

die Möglichkeit, etwaige Ansprüche auf Deliktshaftung zu begründen. Diese ist jedoch nur vorgesehen bei sogenannten Schutzgesetzen[217], welche den Schutz des einzelnen und nicht bloß der Allgemeinheit bezwecken.

Der Regierungsvorlage[218] folgend, gilt dies für die Haftungsbestimmungen des § 23 SigG. Diese Norm begründet eine Haftung für qualifizierte Zertifikate - beruhend auf Deliktsrecht - aber eben nur eingeschränkt für „qualifizierte" Zertifikate. Bei der Geltendmachung deliktischer Ansprüche befinden sich diese Dritten jedoch in einer wesentlich schlechteren Position verglichen mit der des Zertifikatinhabers, welcher seine Ansprüche seinerseits auf ein bestehendes Vertragsverhältnis stützen kann. Im Rahmen der Deliktshaftung verneint wird ein Ersatz von Vermögensschäden bei bloßer Fahrlässigkeit, es besteht keine Beweislastumkehr und bloße Besorgungsgehilfenhaftung nach § 1315 ABGB. Demnach hat eine Zertifizierungsstelle bzw. ihr Betreiber lediglich die Pflicht für entstandenen Schaden einzustehen, wenn sie sich einer untüchtigen oder wissentlich gefährlichen Person bedient.

Zusammenfassend sei nochmals festgestellt, dass ein Diensteanbieter für qualifizierte Zertifikate nach Deliktsrecht nur in eben dargestellten eingeschränktem Ausmaß einzustehen hat, für einfache Zertifikate zudem nur bei vorsätzlichem, schädigendem Verhalten. Dementsprechend wird sich ein Vertragspartner des Signaturinhabers für die Geltendmachung von innerhalb der Haftungsgrenzen bzw. Einschränkungen liegendenden Schäden direkt auf § 23 SigG stützen und lediglich darüber hinausgehende Schäden im Rahmen des Deliktsrechts geltend machen. Auch bei Schädigungen infolge des Gebrauchs einer einfachen Signatur ist dieser auf deliktische Ansprüche beschränkt.

[217] Bei der Verletzung eines Schutzgesetzes trägt der Schädiger nach § 1298 ABGB die Beweislast, daß ihn an der Übertretung desselben kein Verschulden trifft. Das Vorliegen von grober Fahrlässigkeit bzw. von Vorsatz hat der Geschädigte weiterhin zu beweisen. Siehe dazu *Dittrich/Tades*, ABGB[35], S. 1996ff, E 25ff

[218] 1999 der Beilagen zu den Stenographischen Protokollen des Nationalrates der XX. Gesetzgebungsperiode, S. 43

7.25.3 Vertrag mit Schutzwirkung zugunsten Dritter[219]

Vorab erwähnt sei, dass eine Haftung, beruhend auf dem verwandten Institut des Vertrages zugunsten Dritter von vornherein ausscheidet. Um zur Anwendbarkeit des § 881 gelangen zu können, müsste die Leistung des Diensteanbieters, d.h. Ausstellung und eventuell auch Verwaltung des Zertifikats, direkt dem Dritten zugute kommen. Diese Tatsache müsste weiters bereits bei Vertragsabschluß allen beteiligten Parteien bewusst sein. Ganz offensichtlich mangelt es hier einerseits an der Konkretisierbarkeit der zukünftigen Vertragspartner des Zertifikat-Inhabers, da diese bei Vertragsabschluß weder der Zahl noch der Person nach feststehen werden, und andererseits an der Zielrichtung der Begünstigung des Zertifizierungsvertrages. Dieser wird doch hauptsächlich zugunsten des Zertifikatwerbers ausgestellt, auch wenn die dadurch geschaffene Möglichkeit der Identitätsprüfung eine bedeutende Rolle spielt.

In Zusammenhang mit dem Konstrukt des „Vertrages mit Schutzwirkung zugunsten Dritter" unterschiedlich weit gezogen und definiert wird der Kreis der Begünstigten. Bydlinski[220] etwa verlangt, dass bei Vertragsabschluß bereits voraussehbar sein muss, dass ein Dritter mit der Hauptleistung in Kontakt kommt. Dabei muss der Vertragspartner den Dritten durch die Zuwendung der Hauptleistung erkennbar begünstigen oder alternativ dazu diesem gegenüber einer rechtlichen Fürsorgeverpflichtung unterliegen. Koziol wiederum definiert den Kreis der geschützten Personen als solche mit erhöhtem Schutzbedürfnis und Zugehörigkeit zur Interessenssphäre eines Partners.

Im Rahmen dieser Variante besteht nur eine Haftung für Leben und Eigentum des Dritten, jedoch nicht für bloße Vermögensschäden, ausgenommen die Hauptleistung kommt einem Dritten zugute, der der Interessenssphäre des Vertragspartners angehört. Auch aus diesem

219 Siehe auch *Harrer*, Praxiskommentar zum ABGB samt Nebengesetzen², Bd. 7, S. 78ff und *Dittrich/Tades*, ABGB35, S. 2023ff, E 85ff

220 Siehe auch *Koziol*, Österreichisches Haftpflichtrecht, Bd. II, Besonderer Teil, Wien 1975

Grund wäre die Berufung auf das hier in Rede stehende Rechtsinstitut wenig sinnvoll und zielführend, da es sich im Zusammenhang mit der Erbringung von Zertifizierungsdiensten meist um reine Vermögensschäden handeln wird. Die Anwendungsmöglichkeiten des Konstituts des „Vertrages mit Schutzwirkung zugunsten Dritter" dürfte überdies in vielen Fällen zweifelhaft sein, da es in den meisten Fällen einerseits an der Voraussehbarkeit des Kontaktes mit einem Dritten und andererseits auch an einer rechtlichen Fürsorgeverpflichtung fehlen wird.

7.25.4 Produkthaftung[221]

Könnte sich der beweisrechtlich schlecht gestellte Dritte auf die Regelungen betreffend Produkthaftung stützen, so wäre damit die Begründung einer verschuldensunabhängigen Gefährdungshaftung denkbar und möglich. Gemäß § 4 Produkthaftungsgesetz[222] haben jedoch lediglich bewegliche körperliche Sachen einschließlich Energie als Produkte zu gelten. Zertifikate und Schlüssel fallen schon allein aus diesem Grund aus dem Anwendungsbereich dieses Gesetzes heraus, auf dessen Grundlage eine wesentliche Besserstellung Dritter erreicht werden könnte. Entschließt man sich dazu, ein Zertifikat als Software zu definieren, so bleibt es noch immer zweifelhaft, ob diese als Produkt iSd genannten Norm zu gelten hat. Einhellig wird die Meinung vertreten, dass Individualprogramme, bei denen die geistige Leistung im Vordergrund steht und die keine bloß massenweise erzeugten Standardanwendungen darstellen, nicht unter die Produkthaftung fallen.[223] Auch Zertifikate werden individuell auf

---

221 Siehe auch die Kommentierung des PHG samt Richtlinie *Fitz/Purtscheller/Reindl,* Produkthaftung, Wien 1988

222 BG vom 21. Jänner 1988 über die Haftung für ein fehlerhaftes Produkt (Produkthaftungsgesetz) BGBl. Nr. 99/1988. Dieses BG setzt die Rl 85/374/EWG zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte, ABl L 210/1985, 29 um.

223 Anders jedoch *Andreewitch,* Zur Anwendbarkeit des Produkthaftungsgesetzes für Softwarefehler, EDVuR 1990, S. 50ff, der die Unterscheidung in Standard- und Individualsoftware für verfehlt hält. Jedoch kommt auch er zu dem Ergebnis, dass Software, soweit diese als selbständige und isolierte Sache in Erscheinung tritt, aufgrund ihres Charakteristikums als unkörperliche Sache nicht als Produkt iSd PHG zu gelten hat.

persönliche Anfrage hin erstellt und sind schon allein aus diesem Grund unter Berücksichtigung ebengenannter Definition nicht unter den Begriff der „Produkte“ zu reihen.

7.25.5 § 23 österreichisches Signaturgesetz

Die Einstandspflicht des § 23 SigG seitens der Zertifizierungsstelle besteht gegenüber jedermann, d.h. nicht nur gegenüber den in einem konkreten Vertragsverhältnis zu diesem stehenden Zertifikatswerbern, sondern auch gegenüber Geschäftspartnern des Zertifizierten. Demzufolge wurde durch das Signaturgesetz - zumindest in Zusammenhang mit dem Gebrauch qualifizierter Zertifikate - zugunsten des aufgrund einer fehlenden Vertragsbeziehung relativ schlecht positionierten Dritten ein besonders hohes Schutzniveau normiert.

Vorweggenommen sei die Konformität der haftungsrechtlichen Bestimmungen des österreichischen Signaturgesetzes und der Europäischen Signaturrichtlinie in Bezug auf die Haftungsbestimmungen. Die nationalen Gesetzgebungsgremien haben sich zugunsten von Zertifikatsinhabern und Dritten zu einer Erweiterung der Einstandspflicht auf Seiten der Zertifizierungsstellen entschieden. Dem Gesetz folgend kann sich jeder, der sich auf ein Zertifikat verlässt und diesem gutgläubig gegenübersteht, auf die dort normierten Haftungsbestimmungen berufen. Im Gegensatz zum deutschen, schweizerischen und italienischen Gesetzeswerk geht das österreichische Signaturgesetz über ein reines Technologiegesetz weit hinaus, welches nur die infrastrukturellen Belange der Zertifizierungsstellen regelt und etwaige Rechtsfolgen für falsch ausgestellte Zertifikate völlig ausklammert. Zudem ist die sehr weit gefasste Einstandspflicht nur in den Fällen gegeben, in denen die Regelungen des Internationalen Privatrechts zur Anwendbarkeit des nationalen Signaturgesetzes führen.

Mit § 23 SigG wird dem Art 6 der Richtlinie entsprechend die Haftung von Ausstellern qualifizierter Zertifikate und von Diensteanbietern, die für diese einstehen, festgelegt. Gegenständliche Norm ist zwingender Natur, ihr Anwendungsbereich kann also durch

privatrechtliche Vereinbarung weder ausgeschlossen noch eingeschränkt werden. Neben dieser spezialgesetzlich normierten Einstandspflicht voll in Geltung bleiben die Vorschriften des Allgemeinen Bürgerlichen Gesetzbuches und anderer Regelungswerke, vor allem auch des Internationalen Privatrechts betreffend die Anwendbarkeit oder Nicht-Anwendbarkeit nationalen Rechts und der Zuständigkeit nationaler Gerichte. Weiterhin zulässig und mit den Vorgaben der Richtlinie durchaus in Übereinstimmung bleiben strengere Haftungsregelungen, da die in der europäischen Vorgabe dargestellten bloß eine Mindesthaftung vorsehen. Dementsprechend geht die österreichische Haftungsregelung auch über den Bereich der Richtlinie hinaus, da zusätzlich zu den in Art 6 Abs. 1 lit. a bis c aufgestellten Haftungstatbeständen auch noch die Einhaltung der Anhänge II bis IV bzw. §§ 7 und 18 gefordert wird. Ausdrücklich nochmals festgestellt sei, dass die hier genannte Vorschrift nur auf diejenigen Zertifizierungsdiensteanbieter Anwendung zu finden hat, die qualifizierte Zertifikate ausstellen oder bereitstellen, wobei es ausschließlich auf die Bezeichnung im jeweiligen Zertifikat ankommt[224], oder für ein solches Zertifikat nach § 24 Abs. 2 Z 2 einstehen. Für alle übrigen Diensteanbieter, die einfache Zertifikate ausstellen, gelten lediglich die allgemein geltenden Haftungsvorschriften.[225] Das Anbieten von Zertifizierungsdiensten nach § 2 Z 11, wie etwa das bloße Führen von Zeitstempel-, Rechner- und Beratungsdiensten, fällt ebensowenig unter den Anwendungsbereich des § 23. Selbiges gilt auch für diejenigen Schadenssituationen, die nicht unter einen der Haftungstatbestände des § 23 subsumierbar sind.

7.25.5.1 Haftungstatbestände im Signaturgesetz

---

[224] Gemäß § 5 Abs. 1 Z 1 müssen qualifizierte Zertifikate *„einen Hinweis darauf enthalten, dass es sich um ein qualifiziertes Zertifikat handelt,...“* .

[225] Dies scheint auf den ersten Blick etwas verwunderlich, da die Aussteller von einfachen Zertifikaten nicht einer ex-ante Kontrolle unterliegen, wie dies etwa im Rahmen des Akkreditierungsverfahrens vorgesehen ist. Obwohl die staatliche Aufsicht bei diesen also in bloß abgeschwächter Form stattfindet und schon allein aus diesem Grund eine Gesetzesverletzung nicht unwahrscheinlich ist, treffen diese nur die allgemeinen Haftungsregelungen des ABGB, d.h. die Beweislastumkehr gilt für diese nicht.

Ein Zertifizierungsdiensteanbieter hat für die Richtigkeit der Angaben in den von diesem ausgestellten Zertifikaten zum Ausstellungszeitpunkt einzustehen.[226] Schon aus diesem Grund wird er ein besonderes Interesse daran haben, die Person des Antragstellers und dessen Angaben genauestens zu überprüfen. Der im Zertifikat bezeichnete Signator hat der Inhaber jenes privaten Schlüssels zu sein, der dem dort bezeichneten öffentlichen Schlüssel entspricht. Die Komplementarität von Signaturerstellungs- und Signaturprüfeinheiten muss gegeben sein. Die Führung eines effizienten und jederzeit aktuellen Verzeichnis- und Widerrufsdienstes ist im Hinblick auf die durchgehende Überprüfbarkeit der Rechtsgültigkeit abgegebener Signaturen ein besonderes Anliegen des Signaturgesetzes. Da zu den Verpflichteten des § 23 ausschließlich die Aussteller qualifizierter Zertifikate zählen, ist in Abs. 2 die Einstandspflicht für das Einhalten der laut Anhang III der SigRl bzw. § 18 öSigG an sichere Signaturerstellungseinheiten zu stellenden Anforderungen normiert. Zusätzlich sind die in § 7 öSigG aufgelisteten Anforderungen an Zertifizierungsdiensteanbieter für qualifizierte Zertifikate und an Verfahren bei der Erzeugung und Speicherung des privaten Schlüssels einzuhalten.

Zusammenfassend ist also festzustellen, dass in Österreich niedergelassenen Zertifizierungsdiensteanbieter über die in Art 6 Abs. 1 lit. a bis c genannten Haftungstatbestände der Signaturrichtlinie hinaus zusätzlich einzustehen haben für die Einhaltung der Anforderungen und Empfehlungen der Anhänge II, III und IV und alle sonstigen, im österreichischen Signaturgesetz vorgesehenen technischen Sicherheitserfordernisse.

7.25.5.2 Verschuldenshaftung und Beweislastumkehr in § 23 SigG

[226] dargestellt in Anhang I der SigRl und § 5 öSigG

Gemeinschaftsrechtlichen Vorgaben folgend ist der Zertifizierungsdiensteanbieter im Schadensfall verpflichtet zu beweisen, *„dass er nicht fahrlässig gehandelt hat“* [227], d.h. anders ausgedrückt, „dass ihn an der schadensbegründenden Pflichtverletzung bzw. objektiven Sorgfaltswidrigkeit kein Verschulden trifft.“[228] Abs. 1 und 2 leg.cit. sind als Schutzgesetze nach § 1311 ABGB anzusehen, weshalb vermutet wird, dass die Missachtung der jeweiligen Norm für den eingetretenen Schaden kausal ist. Der gesonderte Nachweis einer Kausalkette bzw. eines Kausalitätszusammenhangs ist nicht erforderlich. Einen solchen zu erbringen, wäre für den Kläger in den meisten Fällen wohl schlichtweg auch unmöglich, da es sich hauptsächlich um unternehmensinterne Abläufe handeln wird, die für einen außenstehenden Dritten nicht einsehbar sind. Zudem wird in diesem Zusammenhang auch von einer größeren „Nähe zum Beweis“ auf Seiten des Unternehmers gesprochen, da es ihm in aller Regel leichter fallen wird, einen allfälligen Gegenbeweis zu erbringen. Der Beklagte hat in diesem Sinne die Möglichkeit, sich freizubeweisen, d.h. fehlendes Verschulden oder fehlende Kausalität der Normübertretung am konkret eingetretenen Schaden nachzuweisen. Im erstgenannten Fall wird das Vorliegen eines Verschuldens, einer Pflichtwidrigkeit überhaupt verneint, im zweiteren bloß die Kausalität desselben. In Entsprechung des § 23 Abs. 3, hat der Geschädigte die Kausalität einer Pflichtverletzung bloß wahrscheinlich zu machen, um sich beim Zertifizierungsdiensteanbieter schadlos halten zu können. Kann dieser wiederum das Fehlen der Ursächlichkeit für den konkret eingetretenen Schaden wahrscheinlich machen, so wird er von seiner Haftungspflicht befreit - ausgenommen, es gelingt dem Geschädigten der volle Beweis des Gegenteils.[229]

Es gilt der Grundsatz, dass auch der Zertifizierungsdiensteanbieter lediglich für dasjenige einzustehen hat, was in seinem Machtbereich liegt. Kann er die exakte Einhaltung der an ihn

---

[227] SigRl Art 6 Abs. 1 u. 2

[228] siehe *Brenn*, Signaturgesetz, S. 134 und *Mayer-Schönberger/Pilz/Reiser/Schmölzer*, Signaturgesetz: Praxiskommentar, Wien 1999, S. 140f

[229] Die Umkehr der Beweislast gilt also nur im Bezug auf das Vorliegen eines Verschuldens, nicht jedoch für die Kausalität als solche. Diese wird nicht einfach vermutet, sondern ist vom Geschädigten zumindest wahrscheinlich zu machen.

gestellten Anforderungen beweisen, so wäre eine Einstandspflicht unbillig. Der Zertifizierungsdiensteanbieter haftet für sein gesamtes Personal wie für sämtliche Gehilfen und für ihn tätiggewordenen Personen, worunter auch die zur Erstellung von Prüfberichten oder Erbringung anderer Leistungen ersuchten, nicht zum eigenen Betrieb gehörenden Stellen zu zählen sind. In diesem Zusammenhang genügt bereits ein bloßes Entkräften der Verursachungsvermutung, d.h. er hat bloß wahrscheinlich zu machen, dass die Schadensursache nicht in einer Pflichtwidrigkeit seinerseits liegt, denn Abs. 3 normiert eine bloße Beweiserleichterungsregel zu Gunsten des Geschädigten und nicht eine völlige Umkehr der Beweislast zu Lasten des Zertifizierungsdiensteanbieters.[230]

7.25.5.3 Haftungsausmaß und -beschränkung

Im allgemeinen bestimmt sich das konkrete Haftungsausmaß nach der jeweiligen Zertifizierungsklasse und dem konkreten Haftungshöchstmaß. Durch diese Determinanten wird einerseits das Risiko auf Seiten des Zertifikat-Ausstellers einschätzbar gemacht und andererseits hat der einzelne Anwender die Gewähr, dass der Diensteanbieter über ein bestimmtes Grund- und Haftungskapital verfügt.

In Übereinstimmung mit Art 6 Abs. 3 und 4 SigRl ist nach Abs. 4 der nationalen Rechtsgrundlage die Haftung generell auszuschließen, wenn aus dem qualifizierten Zertifikat Einschränkungen des Anwendungsbereiches oder des verfügbaren Transaktionswertes ersichtlich sind. In einem solchen Fall haftet er nicht für Schäden, *„die sich aus einer anderen Verwendung des Zertifikats oder aus der Überschreitung dieses Transaktionswerts ergeben.“*[231] Hier hat er bereits bei Ausstellung der elektronischen Bescheinigung alles in seinem Machtbereich Mögliche getan. Unsachgemäßes Auftreten des

---

[230] dazu ausführlich NR: GP XX RV 1999 AB 2065 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP, 4

[231] § 23 Abs. 4 BGBl. I Nr. 190/1999

Signaturschlüsselinhabers im Rechtsverkehr kann ihm nicht angelastet werden, zumal die Existenz spezifischer Einschränkungen durch die allgemeine Zugänglichmachung des Zertifikats für jeden Dritten ohne besondere Anstrengungen leicht erhoben werden kann.

7.25.5.4 Resümee

§ 23 SigG ist aus dem Grund notwendig, da die Schadenersatzregelungen des ABGB uneingeschränkt nur für das Verhältnis zwischen Diensteanbieter und Signator gelten würden. Hier tritt § 1298 folgend bei Vermögensschäden eine Beweislastumkehr ein, für Erfüllungsgehilfen wird über § 1313 gehaftet, dies auch bei bloßer Fahrlässigkeit. § 23 SigG greift im Gegensatz dazu, wie bereits eingangs kurz erwähnt, auch bei Schäden, die bei außenstehenden Dritten eintreten, beispielsweise einem Geschäftspartner des Signators, welcher mit dem Zertifizierungsdiensteanbieter keine vertraglichen Beziehungen unterhält. Diese deliktische Haftung würde nach ABGB nur eine Haftung für Besorgungsgehilfen nach § 1315 begründen und überdies bei Fahrlässigkeit mit einigen Ausnahmefällen[232] nicht greifen.

Nach § 23 wird auch bei bloßer Fahrlässigkeit gehaftet, nur bei Wahrscheinlichmachung des Fehlens jeglicher Nachlässigkeit wird der Zertifizierungsdiensteanbieter von seiner Haftungspflicht befreit. Folglich kann sich auch jeder Dritte, welcher gutgläubig auf die inhaltliche Richtigkeit eines Zertifikats vertraut, schon bei fahrlässigem Verhalten des Zertifizierungsdiensteanbieters bei diesem unschädlich halten, obwohl er mit diesem in keiner wie immer gearteten vertraglichen Beziehung steht. § 23 ermöglicht in diesem Fall den Umweg über eine Haftung nach § 1315 basierend auf der Verletzung eines Schutzgesetzes und legt von vornherein eindeutig fest, dass ein Dritter in gleicher Weise wie ein Zertifikatsinhaber geschützt ist.

[232] siehe dazu näher *Brenn*, Signaturgesetz, S, 137

7.26 § 24 - Anerkennung ausländischer Zertifikate und Signaturen

Das Wesen des elektronischen Geschäftsverkehrs liegt in der Ermöglichung des Abschlusses von Verträgen auf zeit- und kostensparende Art und Weise über Staatengrenzen hinweg. Schon aus diesem Grund war die Einfügung des § 24 öSigG unentbehrlich.

7.26.1 Zertifikate aus Mitgliedstaaten der Europäischen Gemeinschaft

Abs. 1 sieht die rechtliche Gleichbehandlung und Gleichstellung sämtlicher innerhalb der Gemeinschaft ausgestellten Zertifikate vor; qualifizierte Zertifikate eines Mitgliedstaates entfalten dieselben Rechtswirkungen wie die im Inland ausgestellten. Für diese grundsätzliche rechtliche Anerkennungspflicht werden keinerlei zu erfüllende Anforderungen gestellt. Grundvoraussetzung ist lediglich die Überprüfbarkeit der ausländischen Zertifikate und Signaturen durch die inländischen Empfänger vom Inland aus. Die Sicherheit und Vertrauenswürdigkeit derartiger ausländischer Zertifikate ist im Wege der Beweiswürdigung festzustellen. Durch diese Vorschrift erfolgt die Umsetzung des Art 5 der SigRl, welche bei Einhaltung der Sicherheitsanforderungen, dargestellt in Anhang I bis IV, sämtlichen in der Gemeinschaft ausgestellten Signaturen die besonderen Rechtswirkungen einer eigenhändigen Unterschrift zubilligt.

7.26.2 Zertifikate aus Drittstaaten

Abs. 2 setzt sich mit den, in Drittstaaten außerhalb der Europäischen Gemeinschaft niedergelassenen Zertifizierungsdiensteanbietern und den von ihnen ausgestellten Zertifikaten auseinander. Die sogenannten „Einfachen“ sind anzuerkennen, d.h. ihnen ist nach § 3 Abs. 2 die rechtliche Wirksamkeit zuzusprechen, sofern *„deren Gültigkeit vom Inland aus überprüft werden kann“*. Diese Voraussetzung gilt gleichermaßen für die Anerkennung und Gleichstellung aller europäischen wie außereuropäischen Zertifikate und beinhaltet die freie und jederzeitige Zugänglichkeit der Verzeichnisdienste von Österreich aus.

7.26.2.1 Alternative Voraussetzungen der Anerkennung

Die rechtliche Gleichstellung ausländischer, d.h. von einem Drittstaat ausgestellter, elektronischer Bescheinigungen ist nur unter Einhaltung besonderer, in alternativer Weise zueinander stehender Voraussetzungen vorgesehen. § 24 Abs. 2 2. Satz entspricht beinahe wortwörtlich Art 7 Abs. 1 der SigRl.

Ziffer 1 verlangt die vorherige freiwillige Akkreditierung in einem Mitgliedstaat, wobei der ausländische Zertifizierungsdiensteanbieter dem § 7 öSigG voll zu entsprechen hat.

Die zweite Möglichkeit besteht in der Übernahme der Haftung für die qualifizierten Zertifikate eines ausländischen Zertifizierungsdiensteanbieters durch einen im Inland ansässigen Zertifizierungsdiensteanbieter des § 7. Entsprechend § 13 Abs. 3 hat die Aufsichtsstelle ein Verzeichnis der Drittstaatenzertifizierungsdiensteanbieter zu führen, für die wie ausgeführt gehaftet wird. In diesem Zusammenhang hat der Haftungsübernehmer selber dafür zu sorgen, dass im Hinblick auf die Sicherheit von Signierungsverfahren und -komponenten den Anforderungen der Richtlinie bzw. der innerstaatlichen Normen entsprochen wird. Dies aus dem einfachen Grund, weil er selbst infolge der Haftungsübernahme einerseits für die Einhaltung der gemeinschaftsrechtlichen Vorgaben voll einzustehen hat und andererseits der in einem Drittstaat niedergelassene Diensteanbieter nicht an die EU-rechtlichen Normen gebunden ist.

Schlussendlich gibt es noch die Möglichkeit des Abschlusses bi- oder multilateraler Vereinbarungen zwischen der Europäischen Gemeinschaft auf der einen Seite und einer Internationalen Organisation oder einem Drittstaat auf der anderen Seite. Deren Inhalt ist die Anerkennung und Gleichstellung von aus diesen stammenden Zertifikaten mit innerhalb der Gemeinschaft ausgestellten qualifizierten Zertifikaten.

7.26.3 Gleichwertigkeit von Bescheinigungen anerkannter Bestätigungsstellen

In Entsprechung des § 19 sieht Abs. 3 des hier in Rede stehenden Paragraphen die Gleichwertigkeit sämtlicher, in einem Mitgliedstaat oder in einem Drittstaat durch eine anerkannte Bestätigungsstelle ausgestellter Bescheinigungen über die Einhaltung der Sicherheitsanforderungen für die Erzeugung sicherer elektronischer Signaturen vor. In diesem Zusammenhang hat die Aufsichtsstelle bezüglich Bestätigungsstellen in Drittstaaten im vorhinein die Gleichwertigkeit der bei diesen zum Einsatz gelangenden technischen Verfahren festzustellen. Bestätigungsstellen in einem Mitgliedstaat müssen zu ihrer Eignungsfeststellung, in Österreich zu ihrer Benennung durch Verordnung des Bundeskanzlers nach § 19 Abs. 3, den Anforderungen des Gesetzes bzw. der Richtlinie sowieso entsprechen und bedürfen aus diesem Grund keiner zusätzlichen Gleichwertigkeitsüberprüfungen.

7.27 § 25 - Verordnungsermächtigung

Das Gesetz räumt dem Bundeskanzler die öffentlich-rechtliche Befugnis ein, im Einvernehmen mit dem Bundesminister für Justiz die zur Durchführung des Signaturgesetzes notwendigen Verordnungen[233] zu erlassen. Die in § 25 aufgezählten Regelungsbereiche betreffen etwa die Gebührenfestsetzung für Dienste der Aufsichtsstelle und der Telekom-Control-GmbH[234], die Festsetzung des erforderlichen Mindestkapitals zur Abdeckung des Haftungsrisikos der Zertifizierungsdiensteanbieter[235], die Fixierung der Anforderungen an technische Komponenten und Verfahren[236], die genaue Ausgestaltung von Zeitstempeldienst[237] und

---

[233] Siehe etwa die Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV) BGBl. II Nr. 30/2000 und die VO des Bundeskanzlers über die Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie–Austria (A-Sit)“ als Bestätigungsstelle, BGBl. II 31/2000.

[234] siehe § 13 Abs 4 öSigG und § 1 öSigV

[235] siehe § 7 Abs 1 Z 6 öSigG und § 2 öSigV

[236] siehe §§ 5 ff öSigV

Nachsignierung[238] udgl. Auf dem Weg des Erlassens von Verordnungen wird es ermöglicht, die konkreten Anforderungen dem jeweiligen Stand der Technik entsprechend innerhalb relativ kurzer Zeit und ohne den aufwendigen Weg eines Verfahrens zur Gesetzesänderung bzw. -ergänzung anzupassen.

7.28 § 26 - Strafbestimmungen

§ 26 Abs. 4 enthält eine Subsidiaritätsklausel, wonach strafbare Handlungen erst dann als Verwaltungsstraftatbestand nach dem Signaturgesetz zu gelten haben, wenn weder die Zuständigkeit der Gerichte begründet ist noch andere Verwaltungsstrafbestimmungen mit höherer Strafandrohung zur Anwendung kommen. Oftmals wird im Falle einer missbräuchlichen Verwendung einer elektronischen Signatur ein gerichtlich strafbarer Tatbestand nach dem österreichischen Strafgesetzbuch verwirklicht sein, wie etwa Betrug udgl. Die mit einer elektronischen Signatur unterzeichneten Dokumente werden in naher Zukunft unter den strafrechtlichen Urkundsbegriff nach §§ 223 ff StGB zu reihen sein und demnach den Bestimmungen betreffend Urkundsdelikte unterliegen. Adressaten der Strafandrohung nach dem Signaturgesetz sind einerseits die eine Signatur unbefugt und missbräuchlich verwendenden Dritten und andererseits die Zertifizierungsdiensteanbieter. Betreffend Letztgenannter sind in Signaturgesetz und -verordnung wiederholt spezifische Verhaltenspflichten normiert, deren Nichteinhaltung je nach Gewichtung mit Strafe bedroht ist.

Wird einem Zertifizierungsdiensteanbieter die weitere Ausübung seiner Tätigkeit untersagt und sein Zertifikat widerrufen,[239] so hat er von jeglicher weiterer Dienstleistungserbringung abzusehen. Wird etwa einem in Österreich tätigen ausländischem Zertifizierungsdiensteanbieter

---

[237] siehe § 10 öSigG und § 14 öSigV

[238] siehe § 17 öSigV

[239] siehe § 14 öSigG

von der Aufsichtsstelle seines Herkunfts- bzw. Niederlassungsstaates die Tätigkeit untersagt, so bezieht sich dieses Verbot auch auf seine Tätigkeit in Österreich. Wurde er jedoch in Österreich zwischenzeitig nach § 17 freiwillig akkreditiert, so ist er hierzulande zur weiteren Ausübung seiner Tätigkeit befugt.[240]

Laut Artikel 13 SigRl haben *„die Mitgliedstaaten die erforderlichen Rechts- und Verwaltungsvorschriften zu erlassen, um dieser Richtlinie vor dem 19. Juli 2001 nachzukommen."* Diesem Erfordernis ist der österreichische Gesetzgeber bereits nachgekommen, mehr noch, das Signaturgesetz ist bereits vor der europäischen Rechtsgrundlage mit 1.1.2000 in Kraft getreten.

Zu wenig Beachtung in der derzeitigen Fassung des österreichischen Signaturgesetzes findet der Elektronische Rechtsverkehr mit Behörden, die Durchsetzbarkeit von Ansprüchen im Ausland, insbesondere Nicht-EU-Staaten und der strafrechtliche Schutz der elektronischen Signatur und elektronisch übermittelter Daten.

Weiterer Regelungsbedarf besteht im Bereich des strafrechtlichen Urkundenbegriffs, welcher vom Signaturgesetz in der derzeitigen Fassung nicht berücksichtigt wird. Dieser sollte im Sinne einer vollständigen Gleichstellung auch auf elektronische Dokumente ausgedehnt werden. Auch die Notariatsordnung bedarf einer Ergänzung, um die berufsrechtlichen Voraussetzungen für die Verwendung elektronischer Signaturen durch Notare zu schaffen. Nach §§ 89ff GOG und §§ 13 und 18 AVG sind elektronische Eingaben möglich, jedoch bestehen bislang keine Regelungen betreffend die Zulässigkeit elektronischer Signaturen - welche ebenso so bald wie möglich zu treffen wären.[241]

---

[240] *Brenn*, Signaturgesetz, S. 144f

[241] In Deutschland versucht man bereits jetzt durch eine entsprechende Änderung der Zivilrechtsordnung den rechtlichen Grundstein dafür zu legen. Siehe den Referentenentwurf des BMJ vom 5. Juni 2000 betreffend ein Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, dargestellt in Kapitel 8.5.

7.29 Novelle des Signaturgesetzes

Einem eventuell noch bestehenden Anpassungsbedarf des Signaturgesetzes ist der österreichische Gesetzgeber in kürzester Zeit nachgekommen. Durch den inzwischen bereits angenommenen „Entwurf für ein Bundesgesetz, mit dem das Signaturgesetz (SigG) geändert wird“[242] werden vornehmlich bloß redaktionelle und weniger inhaltliche Änderungen und Ergänzungen vorgenommen, die zur vollständigen Konformität mit der Richtlinie über elektronische Signaturen führen soll. Dementsprechend erfolgt dadurch auch die bisher fehlende, jedoch laut Art 13 Abs. 1 der europäischen Vorgabe verpflichtend vorgesehene, Bezugnahme auf die Richtlinie.

Die Novelle verfolgt im wesentlichen drei Zielrichtungen. Zum einen dehnt sie die Anwendbarkeit so mancher Vorschriften auch auf die Vertragsstaaten des Europäischen Wirtschaftsraumes aus[243] - so wie auch die Richtlinie dies vorsieht. Zum anderen fanden in der ursprünglichen Fassung des Signaturgesetzes eventuell entstehende, über die ansonsten üblichen Ausgaben hinausgehende Anlaufkosten von Telekom-Control-Kommission und Telekom-Control GmbH keine Berücksichtigung - dieses Manko versucht man gleichfalls auszugleichen. Und schließlich entstand ganz allgemein durch die formelle Verabschiedung der Richtlinie am Beginn des Jahres 2000 ein sehr eng begrenzter Anpassungsbedarf.

7.29.1 Definition eines qualifizierten Zertifikates

Während § 5 Abs. 3 (alt) für das Vorliegen eines qualifizierten Zertifikates bislang das Anfügen einer sicheren elektronischen Signatur seitens des Diensteanbieters verlangte, was in der Richtlinie nicht der Fall ist, wird in dem nun vorliegenden Entwurf bloß eine Signatur des §

---

[242] Bundesgesetz, mit dem das Signaturgesetz geändert wird, BGBl. II Nr. 137/2000, einsehbar unter http://www.bmj.gv.at/gesetzes/signatur.html. Am 22.11.2000 wurde der Entwurf in dritter Lesung angenommen – siehe dazu unter http://www.parlinkom.gv.at/pd/pm/XXI/A/his/003/A00313_.html.

[243] siehe § 18 Abs 5, § 24 Abs 1, § 24 Abs 2 Z 1, § 24 Abs 2 Z 2 jeweils in der Fassung des Entwurfes

2 Z 3 lit. a bis d verlangt. Eine solche muss nicht unbedingt auf einem qualifizierten Zertifikat beruhen und unter Verwendung dem Signaturgesetz entsprechender technischer Komponenten und Verfahren erstellt werden.

Mit dieser Änderung wird der Überlegung Rechnung getragen, dass die von der Aufsichtsstelle ausgestellten qualifizierten Zertifikate allein durch das gemeinsame Tätigwerden von der ihr zur Seite gestellten Telekom-Control GmbH und die Bestätigungsstelle ohnehin einen sehr hohen Sicherheitsstand aufweisen.

7.29.2 Anlaufkosten der Aufsichtsstelle

Durch einen neuen § 13 Abs. 4 wird der Telekom-Control-Kommission wie auch der Telekom-Control GmbH ein Zuschuss zur Deckung der Anlaufkosten gewährt. Dieser wird für die Dauer von drei Jahren aus Bundesmitteln bestritten, nach diesem Zeitraum sollen die einlaufenden Gebühren, die für die Aufsichtstätigkeiten zu entrichten sind, ausreichend sein. Da durch das Signaturgesetz selbst[244] eine strenge organisatorische und finanzielle Trennung der Tätigkeit nach diesem Bundesgesetz mit anderweitig zugewiesenen Aufgaben verlangt wird, scheidet von vornherein auch die Bestreitung ihrer Kosten aus zweiteren aus.

7.29.3 Bestätigungsstellen und Bescheinigungen

Zur Benennung einer Bestätigungsstelle sind die Mitgliedstaaten selbst aufgerufen, dabei haben sie Art 3 Abs. 4 folgend die von der Kommission aufgestellten Mindestkriterien zur Feststellung der Eignung zu berücksichtigen. Wie bereits oben dargestellt haben diese Stellen die Aufgabe, die Übereinstimmung von sicheren Signaturerstellungseinheiten mit den Anforderungen des Anhangs III zu überprüfen bzw. zu bescheinigen. Ist eine solche Bescheinigung einmal erteilt, so hat sie auch in jedem Mitgliedstaat der Europäischen Union

[244] siehe § 13 Abs 7 und § 15 Abs 5 SigG

und des Europäischen Wirtschaftsraumes automatisch als gleichwertig anerkannt zu sein. Eine abermalige Kontrolle durch eine ausländische Bestätigungsstelle ist der Richtlinie folgend unzulässig. Zudem hat die Kommission auch die Möglichkeit der Vergabe von Referenznummern für technische Komponenten und Verfahren. Wird seitens der Bestätigungsstelle die Übereinstimmung mit diesen allgemein anerkannten Standards festgestellt, so gelten automatisch auch sämtliche innerstaatlich fixierten rechtlichen Erfordernisse als erfüllt.

Die, ohne jegliches zusätzliche Verfahren vonstatten gehende Gleichstellung ausländischer Bescheinigungen von Bestätigungsstellen, welche den europäischen Kriterien entsprechend benannt wurden und somit auch mit innerstaatlichem Recht konform gehen, wird durch den hier in Rede stehenden Entwurf ausdrücklich in § 18 Abs. 5 (ergänzt) und 6 (neu) und § 19 Abs. 3 (neu) normiert.

7.30 Die Anwendbarkeit nationaler Vorschriften

Auf dem Datenhighway abgeschlossene Rechtsgeschäfte stehen schon lange nicht mehr in einem mehr oder weniger rechtsfreien Raum, sondern unterliegen ebenso rechtlichen Normen und Rahmenbedingungen - darüber dürfte inzwischen kein Zweifel mehr bestehen. Ein viel größeres Problem liegt jedoch in der Feststellung, das Recht welchen Staates zur Anwendung zu kommen und welche nationale Behörde zu entscheiden hat Das eine muss sich mit dem anderen keineswegs decken. Die in dieser Arbeit gegenständliche SigRl wie auch die E-Commerce-Richtlinie lassen diesen Gesichtspunkt gänzlich außer Betracht, die Autonomie der Mitgliedstaaten, auf gesetzlicher Ebene für einen entsprechenden Regelungsrahmen zu sorgen, wird in keinster Weise eingeschränkt.

Sogenannte nationale „Kollisionsnormen“[245] regeln detailliert die Anwendbarkeit bzw. Nicht-Anwendbarkeit nationalen Rechts. Vielfach wird an den Ort des Vertragsabschlusses, des Deliktes oder dgl. abgestellt, vielfach an das Vorliegen eines Naheverhältnisses bzw. eines Nahebezuges zu einem bestimmten Staat. Die entsprechenden Regelungen finden sich in einzelstaatlichen Normen wie auch in zwischenstaatlichen Übereinkommen, beispielsweise im „Lugano-Übereinkommen“,[246] im „Brüsseler Übereinkommen“,[247] im Europäischen Schuldrechtsübereinkommen[248] und in der Jurisdiktionsnorm.[249] Die Vielzahl der denkbaren Anknüpfungspunkte etwa nach Immaterialgüterrecht, Wettbewerbsrecht, Medienrecht, Strafrecht etc. erscheint mir jedoch aufgrund des nur marginalen Zusammenhangs mit elektronischen Signaturen hier nicht notwendig zu sein.[250]

7.31 Einsatzbereiche der elektronischen Signatur in der Realität

7.31.1 help.gv.at

Eines der Vorzeigebeispiele Österreichs im Bereich von E-Government ist das bereits im Dezember 1997 in Betrieb genommene Internet-Bürgerinformationssystem namens help.gv. Zwischenzeitlich ist es möglich, mit Hilfe des als besonders bürgerfreundlich zu bewertenden

245 IPRG, BGBl. 1978/304 idgF.

246 Luganer Gerichtsstand- und Vollstreckungsübereinkommen, (LGVÜ) BGBl 1996/448

247 Brüsseler Gerichtsstands- und Vollstreckungsübereinkommen (EuGVÜ), ABl. C 189/2 1990; RV 1285 BlgNR XX. GP

248 Übereinkommen vom 19. Juni 1980 über das auf vertragliche Schuldverhältnisse anzuwendende Recht, BGBl. III Nr. 208/1998 (EVÜ)

249 Gesetz vom 1. August 1895, RGBl 1895/111, über die Ausübung der Gerichtsbarkeit und die Zuständigkeit der ordentlichen Gerichte in bürgerlichen Rechtssachen (JN)

Systems über 40 verschiedene Lebenssituationen, in denen der einfache Bürger mit staatlichen Behörden in Kontakt zu treten hat, erfolgreich und vor allem wesentlich schneller und kostengünstiger als bisher zu bestreiten. Die wichtigsten Amts- und Behördengänge, von der Anforderung eines Führerscheins über die Gründung eines Betriebes oder den Antrag auf Erteilung einer Baubewilligung werden durch help.gv in absehbarer Zeit vollständig auf elektronischem Wege erledigt werden können.[251]

Das Projekt „help.gv.at" war und ist in drei, zeitlich aufeinanderfolgenden Stufen geplant. Erstere ist bereits als abgeschlossen zu betrachten und läuft auch derzeit noch unter der Bezeichnung „@mtshelfer online". Dabei erfolgt eine individuelle und detaillierte Auskunftserteilung, bezogen auf eine ganz bestimmte Lebenssituation. Eine Identifizierung der über das Datennetz anfragenden Person ist nicht erforderlich, zum Zwecke der Bestimmung der örtlichen und sachlichen Behördenzuständigkeit muss lediglich die Angabe eines Bezirkes, einer Gemeinde, etc. erfolgen. Im Zuge der Informationserteilung können die für den späteren Behördengang nötigen Formulare zum Zwecke des eigenhändigen Ausfüllens heruntergeladen oder teilweise in bereits komplettierter Form ausgedruckt werden.

Im Rahmen der derzeit laufenden Ausbaustufe „@ntrag online", ist die online Verbindung mit der jeweils zuständigen Behörde geplant, davon umfasst ist auch das Einreichen von Anbringen über die behördeneigene Homepage. Diese Stufe sollte mit Ende des Jahres 2001 abgeschlossen sein, die Implementierung des österreichischen Signaturgesetzes bildet dafür eine wesentliche Voraussetzung - auch im Hinblick auf die dritte und letzte Stufe, genannt „@mtsweg online". Bei der Ermöglichung letzterer ist die Übermittlung und Verarbeitung personenbezogener Daten vorgesehen, weshalb auf die Einhaltung von Privatsphäre und Datenschutz besondere Rücksicht zu nehmen ist.

---

250 siehe dazu etwa in *Schauer*, eCommerce in der EU, Bd. 3, Wien 1999, S. 243ff und *Roth* in: *Gruber/Mader*, Internet und e-commerce, Wien 2000, S. 165ff und *Mayer-Schönberger/ Pilz*, E-Commerce: Rechtliche Rahmenbedingungen und Notwendigkeiten, AnwBl 1999, S. 217ff

251 siehe unter http://www.rdb.co.at/homepages/jdm.htm und http://www.help.gv.at

7.31.2 „Finanzonline“[252]

Auch die finanzrechtlichen Daten werden in naher Zukunft für jedermann, der über die erforderliche Berechtigung dazu verfügt, welche er mittels elektronischer Signatur bzw. elektronischem Zertifikat nachzuweisen hat, einsehbar sein. Der genannte online-Dienst wurde 1998 aufgenommen und ist derzeit noch ausschließlich für österreichische Wirtschaftstreuhänder, für die im Verzeichnis der Notare eingetragenen Notare, die selbständigen Substitute und die Notar-Partnerschaften zugänglich. Ein Großteil dieser hat sich dem System bereits angeschlossen und auf diesem Wege die Möglichkeit des Abrufs bzw. der Bearbeitung sämtlicher finanzrechtlicher Daten betreffend die Abgabenpflichtigen erlangt. Bürokratieabbau, Verkürzung und Vereinfachung der Behördenwege, jederzeitige Verfügbarkeit und wesentliche Kostenersparnis sind nur einige der Vorteile des neuen Systems.[253] Im Rahmen dieses Datennetzes sind Amtshilfeersuchen, die Einsichtnahme in Akten und die Bewältigung sämtlicher Agenden, welche im Zuge der berufsrechtlichen Vertretungsbefugnisse von Wirtschaftstreuhändern und Notaren an der Tagesordnung stehen, vollständig auf elektronischem Wege abwickelbar. Durch standardisierte Anbringen und in weiterer Folge auch standardisierte Erledigungen soll von vornherein unnötiger Zeit- und Arbeitsaufwand verhindert werden; ein ständiger Medienbruch von elektronischer Datei zu Papierdokument und umgekehrt wird gänzlich verhindert. Die erfolgreiche Übermittlung einer elektronischen Eingabe hat durch eine unmittelbar und technisch automatisiert zu erfolgende Rückmeldung seitens der Behörde bestätigt zu werden. Erfolgt eine Eingabe in standardisierter Form, obwohl diese in eingangs erwähnter Verordnung bzw. in den darauf beruhenden Richtlinien nicht aufgelistet ist, so hat sie als unbeachtlich zu gelten, d.h. ihr Einlangen bei der Finanzbehörde entfaltet keinerlei Rechtswirkung. Ihre Unbeachtlichkeit ist seitens der Behörde

252 Die rechtliche Grundlage von FINANZOnline bildet die FINANZOnline-Verordnung (FOnV) BGBl. II Nr. 71/1998

gegenüber dem Einbringer ausdrücklich festzustellen.[254] Derzeit läuft finanz-online nicht über das allgemein zugängliche World-Wide-Web, sondern über eine eigene Datenleitung, genannt „Highway 194“. Der Zugriff auf die finanzrechtlichen Daten ist an die Leistung eines bestimmten Entgeltes und eine gesonderte Ausweisung gebunden. Dieses Faktum allein erhöht die Sicherheit der Geheimhaltung der relativ prekären Daten in wesentlicher Weise.[255]

253 siehe ebenfalls unter http://www.rdb.co.at/homepages/jdm.htm
und http://finon.datakom.at: 2048/samples - Projekt ... Static/

254 detailliert dazu *Weninger*, FINANZOnline in der zweiten Ausbaustufe: Elektronische Anbringen und Erledigungen rücken näher, ÖStZ 2000/699

255 siehe ausführlicher „Amtsweg per Mausklick“ bereits Realität für 920 WT - „FINANZonline“ ermöglicht Zugriff auf Finanzdateien“, SWK 1998, T 114

8 Deutsche Rechtslage

8.1 Überblick

Noch viel diffiziler als in Österreich ist die Rechtslage in unserem Nachbarstaat Deutschland. Besonders augenfällig und gravierend sind die Diskrepanzen des deutschen Signaturgesetzes mit der europäischen Vorgabe. Diese sind natürlich einfach damit zu erklären, dass ersteres lange vor Inkrafttreten der Richtlinie bereits im Jahre 1997 entwickelt wurde. Die deutsche Rahmenvorgabe bringt demgemäß wesentliche Auffassungsunterschiede zum Ausdruck. Diese manifestieren sich in differenten Normen, welche etwa eine Genehmigungspflicht für Zertifizierungsdiensteanbieter vorsehen und die Rechtswirkungen einer elektronischen Signatur völlig unbehandelt lassen. Der deutsche Gesetzgeber hat die derzeit noch bestehenden rechtlichen Unstimmigkeiten so bald als möglich zu beseitigen, da die europäische Sigaturrichtlinie bis zum 19. Juli 2001 in nationales Recht transformiert sein muss. Hinsichtlich der notwendigen Änderungen bzw. Anpassungen bestehen jedoch noch erhebliche Auffassungsunterschiede[256], welche wiederum Unternehmen wie Privatpersonen vom Gebrauch elektronischer Signaturen abhalten. Zu welchem Zeitpunkt die erforderliche Angleichung erfolgen wird, ist derzeit noch nicht voraussehbar, im folgenden wird zuallererst die derzeit geltende Rechtslage dargestellt.

Das Gesetz zur digitalen Signatur (dtSigG) (Artikel 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste [Informations- und

256 Siehe dazu etwa *Rossnagel*, Europäische Signaturrichtlinie, MMR 5/1999, S. 262ff: „Der Regelungsansatz des Signaturgesetzes bedarf keiner Änderung“ mit darauffolgenden Erläuterungen, in denen bloß die Notwendigkeit von mehr formellen und weniger inhaltlichen Anpassungen zum Ausdruck gebracht wird.

Kommunikationsdienstegesetz - IuDKG][257])[258] vom 22. Juli 1997 ist bereits am 1. August 1997 in Kraft getreten. Die Fixierung der von den Zertifizierungsstellen zu erfüllenden Aufgaben, der einzuhaltenden Sicherheitsanforderungen, der bestehenden Informationspflichten gegenüber den Kunden und der Voraussetzungen für die Aufnahme der Tätigkeit als Diensteanbieter stellen die wesentlichsten Regelungsinhalte des Gesetzes dar. Über einen sehr hohen technischen Sicherheitsstandard soll faktisch ein großes Ausmaß an Beweiswirkung und Vertrauenswürdigkeit erreicht werden.

Um Flexibilität und Zeitgemäßheit der gestellten Anforderungen jederzeit voll gewährleisten zu können, entschied man sich, in § 16 dtSigG eine Verordnungsermächtigung einzufügen. Auf dessen Grundlage erging bereits am 8. Oktober 1997 eine Verordnung zur digitalen Signatur,[259] welche die Details betreffend Lizenzierungsverfahren, Technik und Gebührenleistung enthält. §§ 12 und 16 dieser Verordnung sehen weiters die Erarbeitung von sogenannten Maßnahmenkatalogen vor, welche als Orientierungshilfe für Konsumenten, Zertifizierungsdiensteanbieter, Regulierungsbehörde, Prüf- und Bestätigungsstellen den Einsatz bestimmter technischer Komponenten in rechtlich unverbindlicher Weise empfehlen. Zwischenzeitig gibt es zwei, ordnungsgemäß im Bundesanzeiger veröffentliche Maßnahmenkataloge,[260] welche gemeinsam von der Regulierungsbehörde[261] für Telekommunikation und Post mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt wurden. Ersterer gilt für Zertifizierungsstellen, zweiterer für die technischen

---

257 Für einen Überblick über das IuKDG siehe *Engel-Flechsig/ Maennel/Tettenborn*, Das neue Informations- und Kommunikationsdienste-Gesetz, NJW 45/1997, S. 2981ff und *Kilches*, Mediendienste-Staatsvertrag und IuKDG: Deutschlands Weg in die Informationsgesellschaft, MR 1997, S. 183ff

258 veröffentlicht im dtBGBl I vom 28. Juli 1997, S. 1870; auch einsehbar unter http://www.regtp.de/gesetze

259 veröffentlicht im dtBGBl I vom 22.10.1997, S 2498; auch einsehbar unter http://www.iid.de/rahmen/sigv.html

260 Beilage zu Bundesanzeiger Nr. 204a; siehe auch unter http://www.regtp.de

261 Die Regulierungsbehörde ist Genehmigungsbehörde als Wurzel-Zertifizierungsstelle nach § §4 dSigG iVm § 66 des Telekommunikationsdienstegesetzes (TKG) und bereits seit 23.9.1998 voll funktionsfähig.

Komponenten. Das mit der Erlassung derartiger Entscheidungshilfen verfolgte Ziel der Verfahrensverkürzung und -vereinfachung wurde jedoch keineswegs erreicht. Da die gegenständlichen Kataloge großteils bloß den Wortlaut des Gesetzes bzw. der Verordnung wiedergeben und kaum konkrete Standards enthalten, wird die Arbeit der zuständigen Behörden und Stellen aufgrund bestehender Rechtsunsicherheit noch weiter erschwert.[262]

Aus den genannten Gründen gibt es in Deutschland immer noch erhebliche Schwierigkeiten bei der Anerkennung von Prüf - und Bestätigungsstellen einerseits und der Genehmigung von Zertifizierungsstellen andererseits. In der Gesetzesvorlage selbst fehlt jegliche Regelung bezüglich Kriterien des Anerkennungsverfahrens, die Anerkennung als solche wird vielmehr einfach vorausgesetzt. Aus diesem Grund besteht auch kein Rechtsanspruch auf Anerkennung bei Vorliegen sämtlicher Voraussetzungen, weil diese viel zu unbestimmt und vage gehalten sind.

Bislang sind lediglich das BSI und drei private Unternehmen als zuständige Stellen nach §§ 4 Abs. 3 und 14 Abs. 4 dtSigG anerkannt.[263] Für den Betrieb einer Zertifizierungsstelle liegen zig Anträge vor, aufgrund der wenig aussagefähigen Maßnahmenkataloge und der ebenso zu berücksichtigenden, aber ebensowenig eindeutigen „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)“ bereitet die Überprüfung erhebliche Schwierigkeiten. Lediglich die Telekom/TeleSec ist seit 1.2.1999 dazu ermächtigt, gesetzeskonforme Signaturverfahren anzubieten.

8.2 § 1 - Sicherheitsvermutung

[262] Siehe auch Roßnagel, Das Signaturgesetz nach zwei Jahren, NJW 22/1999, S. 1591ff

[263] Siehe BAnz 1998, 1787; auch abgedruckt in *Engel-Flechsig/Roßnagel*, Muldimedia-Recht 1998, S. 448ff

Die Kernaussage des deutschen Signaturgesetzes trifft § 1 Abs. 1 leg.cit., welcher eine Vermutung für die Sicherheit einer mit dem Gesetz in Übereinstimmung stehenden digitalen Signatur aufstellt. Die Wendung *„als sicher gelten"* schafft keine zusätzliche Beweisregel; der Nutzer einer Signatur muss weiterhin die Unverfälschtheit dieser und die Entsprechung mit den Anforderungen des dtSigG nachweisen, wobei hier die Vermutungsregeln des Entwurfes, welche weiter unten eingehend behandelt werden. Im Rahmen der freien gerichtlichen Beweiswürdigung nach § 286 ZPO sind signierte Dokumente als Beweismittel, d.h. als Augenscheinsbeweis zu sehen. Dabei sind Signaturverfahren, die von einem nicht lizenzierten Diensteanbieter angeboten und verwendet werden, benachteiligt gegenüber solchen, welche nachgewiesenermaßen den spezifischen Anforderungen des Gesetzes genügen.

Wie auch in Österreich schreibt der deutsche Gesetzgeber nicht die Verwendung einer bestimmten Technik oder eines bestimmten Signaturverfahrens vor. Die freie Wahl zwischen diesen bleibt völlig unangetastet; lediglich in den auf gesetzlicher Ebene ausdrücklich normierten Fällen sind ausschließlich digitale Signaturen nach dem dtSigG zulässig. Festgestellt sei hier jedoch, dass es bislang an einer derartigen Norm fehlt. Ebenso völlig freigestellt bleibt es den Diensteanbietern, um eine Lizenz anzusuchen. Der Betrieb einer nicht-genehmigten Zertifizierungsstelle wie auch die Ausstellung von Zertifikaten durch eine solche ist nicht verboten, jedoch mangelt es den darauf beruhenden Signaturen etwa an der Sicherheitsvermutung des § 1 Abs. 1.

8.3 § 15 - Internationale Anerkennung

In Zusammenhang mit der Gleichwertigkeit und der Anerkennung ausländischer Zertifikate normiert § 15 das Erfordernis der *„gleichwertigen Sicherheit"*. Während für Zertifikate eines in einem anderen Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum niedergelassenen Diensteanbieters lediglich nachgewiesenermaßen dasselbe Sicherheitsniveau aufzuweisen haben, um ebenfalls in den Genuss der Sicherheitsvermutung des § 1 Abs. 1 dtSigG zu

kommen, ist bei Zertifikaten von Nicht-EU-Staaten zusätzlich ein zwischenstaatliches Übereinkommen notwendig. Dieses hat die Komponenten festzulegen, bei deren Vorliegen die Gleichwertigkeit ebenso anzunehmen ist.

8.4 Unzulänglichkeiten

8.4.1 Schriftlicher Antrag

Geradezu gegenläufig zu den erklärten Zielen der Richtlinie ist die Anforderung des § 3 Abs. 1 dtSigV, welche darin besteht, dass ein Antrag auf Ausstellung eines Zertifikates eigenhändig zu unterschreiben ist. Dies steht in einem offensichtlichen Gegensatz zu einem der erklärten Ziele des Gesetzes bzw. der Europäischen Vorgabe, bestehende Formvorschriften so weit als möglich zu beseitigen. Durch das hier geschaffene Erfordernis wird es einem deutschen Staatsbürger etwa sehr schwer gemacht, ein ausländisches Zertifikat zu erlangen; ein online-Antrag wird von vornherein ausgeschlossen.

8.4.2 Schriftform

Während österreichische Gesetzgebungsgremien in § 4 Abs. 1 öSigG bei Einhaltung der Anforderungen des Gesetzes das Erfordernis der Schriftlichkeit in § 886 ABGB durch eine elektronische Signatur als erfüllt ansehen, findet sich im gegenständlichen Regelungswerk keine Norm, welche eine derartige Rechtswirkung vorsieht. Die Erfüllung der Schriftform nach § 126 BGB ist nicht ausdrücklich normiert. In offensichtlichem Gegensatz dazu steht Art 5 Abs. 1 der europäischen Signaturrichtlinie, welcher ausdrücklich eine materiellrechtliche Gleichstellung zur Schriftform vorsieht.

Schreibt ein Gesetz Schriftform oder eine höhere Form vor, wie etwa öffentliche Beglaubigung, so ist die Abgabe einer elektronischen Willenserklärung unzulässig; diese würde

zur Nichtigkeit des Rechtsgeschäftes gemäß § 125 BGB führen. Auch bei zwischen den Vertragspartnern vereinbarter Schriftform, erfüllt eine digitale Signatur nicht das Erfordernis des § 127 dtSigG. Hier sind die Rechtsfolgen einer Verletzung nach den konkret getroffenen Vereinbarungen und gemäß den Regeln des Verbraucherschutzes vom Einzelfall abhängig, müssen also nicht unbedingt zur Nichtigkeit des Rechtsgeschäftes führen.

Frank Ebbing tätigt in diesem Zusammenhang eine sehr treffende Aussage, welcher man sich nicht so ohne weiteres entziehen kann: „Formerfordernisse müssen daraufhin überprüft werden, ob sie unter Berücksichtigung ihres Zwecks und den Anforderungen moderner Kommunikation mit ihrem bisherigen Inhalt noch aufrechterhalten werden können."[264] Um die Unwirksamkeit allein aufgrund eines Formfehlers zu vermeiden, ist jede derzeit bestehende Vorschrift zeitgemäß teleologisch auszulegen und die Formbedürftigkeit in vielen Bereichen aufzugeben.

In offensichtlichem Gegensatz zur deutschen Rechtslage steht Art 5 Abs. 1 der europäischen Signaturrichtlinie, welcher ausdrücklich eine materiellrechtliche Gleichstellung zur Schriftform vorsieht.

8.4.3 Freiwilligkeitsprinzip

„Aufbau und Betrieb der Infrastruktur soll privatwirtschaftlich im freien Wettbewerb, jedoch unter behördlicher Kontrolle erfolgen"[265] - einer der Leitsätze, an denen man sich bei der Er- und Ausarbeitung des deutschen Signaturgesetzes offensichtlich orientierte. Nach § 3 dtSigG ist für die Bestimmung der Behörde, welche für die Erteilung von Lizenzen, für die Ausstellung von Zertifikaten für Zertifzierungsdiensteanbieter und für Überwachungstätigkeiten zuständig ist, § 66 des Telekommunikationsgesetzes (TKG) heranzuziehen. Dieser Norm folgend hat die

264 *Ebbing*, Schriftform und E-Mail, CR 5/1996, S. 273

Regulierungsbehörde für Telekommunikation und Post (RegTP) die genannten Aufgaben zu erfüllen; ihre Tätigkeit hat sie bereits im Januar 1998 aufgenommen. Sämtliche Zertifikate, welche Zertifizierungsdiensteanbieter für die Ausübung ihrer Tätigkeit benötigen, beruhen letztendlich auf einem Zertifikat der RegTP. Diese hat als sogenannte Wurzelinstanz sämtliche von ihr ausgegebenen Zertifikate mit ihrem Schlüssel zu signieren. Im Rahmen der Erfüllung ihr übertragener Aufgaben hat sie weitgehend nur für eine entsprechend effiziente Koordination und Beaufsichtigung zu sorgen und einen Großteil der Vollzugsagenden privaten Prüf- und Bestätigungsstellen zu übertragen. Diese haben die Normkonformität der zum Einsatz gelangenden technischen Komponenten zu bestätigen, für die Korrektheit der Umsetzung des angezeigten Sicherheitskonzeptes und die Durchführung von Routinekontrollen zu sorgen.

Bereits im Februar 1998 hat die RegTP die folgenden Stellen zur Erfüllung der genannten Aufgaben anerkannt: Das Bundesamt für Sicherheit in der Informationstechnik (BSI), die Debis Systemhaus Information Security Services GmbH, die TÜV Informationstechnik GmbH und die TÜV Product Service GmbH. Das Tätigwerden dieser geht großteils ohne Dazwischentreten der Regulierungsbehörde vonstatten, in großen Bereichen treffen sie selbst eine abschließende Entscheidung. Ein Großteil dieser Agenden beruht auf den gesetzlichen Grundlagen des §§ 4 Abs. 3 Satz 3, 14 Abs. 4 dtSigG und §§ 15 Abs. 1, 17 Abs. 1 und 3 dtSigV und ist aus diesem Grund als hoheitliches Handeln zu betrachten.[266]

Die soeben dargestellte Rechtslage widerspricht den Grundsätzen der europäischen Vorgabe wesentlich. Artikel 3 normiert ausdrücklich die Genehmigungsfreiheit von Aufnahme und Ausübung der Tätigkeit als Zertifizierungsdiensteanbieter. Um wirksam zertifizieren zu können, bedarf es - der derzeitigen Rechtslage folgend- einer Lizenz. Denkbar und möglich wäre es, das in Signaturgesetz und Signaturverordnung dargestellte Genehmigungsverfahren in ein System zur freiwilligen Akkreditierung gemäß Abs. 2 des genannten Artikels umzugestalten,

---

[265] *Engel-Flechsig*, Rechtliche Grundlagen für die Informationsgesellschaft, in: *Geis*, Rechtsaspekte des elektronischen Geschäftsverkehrs, Eschborn 1999, S. 42f

[266] zu den Details betreffend Aufgaben, Haftung und Rechtsschutz siehe *Roßnagel*, Anerkennung von Prüf- und Bestätigungsstellen nach dem Signaturgesetz, MMR 6/1999, S. 342ff

das jeglichen zwingenden Charakters entbehrt.[267] Während die Signaturrichtlinie eine Kategorisierung von dreierlei Signaturen vorsieht, nämlich die in einfache, fortgeschrittene und auf einer freiwilligen Akkreditierung beruhende, fordert das nationale Signaturgesetz von vornherein Signaturen der höchsten Sicherheitsstufe, ohne die Rechtswirksamkeit auch anderer Verfahren ausdrücklich anzuerkennen.

Allein das zwingende Erfordernis der Anerkennung von Prüf- und Bestätigungsstellen ist im Hinblick auf die Dienstleistungsfreiheit nach Art 59 EGV als unzureichend und europarechtlich bedenklich anzusehen. Im dtSigG wie auch in der dtSigV fehlen detaillierte Regeln betreffend das Verfahren der Anerkennung, Kriterien zur Entscheidungsfindung sind ebensowenig vorgesehen. Aufgrund dieser verfassungswidrigen Normlücken ist die Erfüllung der gesetzlich festgelegten Voraussetzungen nicht eindeutig und unzweifelhaft nachweisbar, ein Rechtsanspruch auf Anerkennung besteht derzeit ebensowenig.

8.4.4 Haftung[268]

Ein weiteres gravierendes Manko des deutschen Regelungswerkes besteht im gänzlichen Fehlen von Haftungsregelungen. Den allgemeinen Grundsätzen des Zivil- und Schadenersatzrechtes folgend hat der Geschädigte ein Verschulden auf der gegnerischen Seite

---

[267] So auch *Roßnagel*, Europäische Signatur-Richtlinie und Optionen ihrer Umsetzung, MMR 5/1999, S. 262ff. Weiters schlägt er vor, im öffentlichen Bereich die Notwendigkeit von Signaturverfahren, welche der heutigen Fassung des dtSigG entsprechen, beizubehalten. Denn gemäß Art 3 Abs. 7 kann hier der Einsatz elektronischer Signaturen zusätzlichen Anforderungen unterworfen werden, soweit diese berechtigterweise erfolgen. Die Vorabkontrolle im Rahmen des Genehmigungsverfahrens würde dem Nutzer folglich auch den Vorteil bieten, dass dieser die Einhaltung der Anforderungen des Signaturgesetzes und die Sicherheit der Signatur im Streitfall nicht zu beweisen hätte, da die Sicherheitsvermutung des § 1 Abs 1 dtSigG zum Tragen kommen würde.

[268] Siehe hierzu ausführlich *Leier*, Haftung der Zertifizierungsstellen nach dem SigG, MMR 1/2000, S. 13ff

nachzuweisen, um etwa auf der Grundlage von §§ 276ff BGB oder 823ff BGB volle Genugtuung zu erhalten. Während der europäische Gesetzgeber durch die Einfügung des Art 6 dem geschädigten Verbraucher die Beweisführung erheblich zu erleichtern versucht und dementsprechend eine Beweislastumkehr zuungunsten des Zertifizierungsanbieters vorsieht, hält das dtSigG an der bisherigen, für den Konsumenten wesentlich nachteiligeren, Rechtslage fest:

In schadenersatzrechtlicher Hinsicht ist die deutsche Rechtslage mit der österreichischen vergleichbar. Vertragspartner eines Zertifizierungsdiensteanbieters erhalten, den Regeln über die positive Vertragsverletzung, Erfüllungsgehilfenhaftung und Beweiserleichterung folgend, volle Genugtuung nach §§ 278 und 282 analog.

Probleme ergeben sich insbesondere bei Vertragspartnern des Zertifikat-Inhabers, welche in der Regel in keinerlei vertraglicher Beziehung mit dem Diensteanbieter stehen.

Die alleinige Abfrage eines Zertifikats lässt keinen Auskunftsvertrag zwischen den jeweils Beteiligten entstehen. Die Pflicht zur Auskunftserteilung bzw. zur Führung jederzeit aktueller Zertifikatsverzeichnisse seitens der Zertifizierungsdiensteanbieter ergibt sich direkt aus dem Gesetz und nicht aus einem individuell abgeschlossenen Vertrag.

Die Anwendbarkeit des Produkthaftungsgesetzes scheidet aus denselben Gründen aus, welche bei Behandlung dieses Themas in Zusammenhang mit der österreichischen Rechtslage angeführt wurden.

Weiters wird in Deutschland einhellig die Meinung vertreten[269], dass es den Normen des Signaturgesetzes an der Schutzgesetzqualität mangelt. Würde man diese als gegeben ansehen, so wäre gemäß § 823 Abs. 2 BGB iVm den Regelungen des dtSigG eine Ersatz reiner

[269] siehe *Leier*, S. 16 sowie BT-Drs. 13/7385 und *Emmert*, Haftung der Zertifizierungsstellen, CR 4/1999, S. 246f

Vermögensschäden auch bei bloßer Fahrlässigkeit möglich. Die in Rede stehenden Vorschriften sind generell-abstrakt formuliert und dienen ganz allgemein dem Schutz des Rechtsverkehrs. Hinter diesem steht natürlich - wie sonst überall auch - die Summe aller Individualinteressen, doch der Wille des Gesetzgebers zielt vornehmlich auf die Wahrung eines Allgemeininteresses.

Deliktsrechtlich nicht ersatzfähig sind reine Vermögensschäden; ersatzfähig hingegen sind all jene Schäden, die sich aus der Verletzung eines absoluten Rechtsgutes, wie etwa Eigentum, ergeben haben. Zudem besteht diese Einstandspflicht nur bei vorsätzlichem Handeln[270] auf Seiten des Zertifizierungsdiensteanbieters, welches nachzuweisen oftmals Schwierigkeiten bereiten dürfte. Weiters wird dieser von der Einstandspflicht für seine Mitarbeiter dadurch befreit, indem er entweder ein pflichtgemäßes Auswahl- und Überwachungsverfahren sein Personal betreffend oder das Fehlen jeglicher Kausalität für den eingetretenen Schaden nachweist. Durch diese Exkulpationsmöglichkeit kann sich ein Diensteanbieter von der Haftung gemäß § 831 Abs. 1 S 2 BGB befreien. Zusammenfassend kann in deliktsrechtlicher Hinsicht nur die Einstandspflicht gemäß § 823 Abs. 1 BGB und § 831 Abs. 1 BGB geltend gemacht werden.

Denkbar ist jedoch die Begründung der Haftung auf Grundlage eines Vertrages mit Schutzwirkung zu Gunsten Dritter. Für das Vorliegen dieser sind kumulativ verschiedene Voraussetzungen zu erfüllen. Zum einen muss eine sogenannte Vertrags- bzw. Leistungsnähe des Dritten vorliegen. Dies kann ohne weitere Probleme bejaht werden, da der Abschluss des Zertifizierungsvertrages zwischen Zertifikatsinhaber und -aussteller ja gerade dazu dient, die Identität des Signaturschlüssel-Inhabers auf verlässliche Weise feststellen zu können. Weiters muss der Vertragsgläubiger, d.h. der Zertifikats-Inhaber ein berechtigtes Interesse am Schutz des Dritten haben, wobei dieses auch bei Vorliegen rein geschäftlicher Beziehungen zu bejahen ist. Ersterer hat verständlicherweise ein besonderes Interesse am Schutz des Dritten, da die Verlässlichkeit der Überprüfungsmöglichkeiten ein entscheidendes Kriterium bei der Wahl

seiner zukünftigen Vertragspartner sein wird. Drittere Voraussetzung ist die Erkennbarkeit des geschützten Personenkreises, wobei dieser bei Vertragsabschluß nicht bereits zahlenmäßig konkret bestimmt bzw. bestimmbar sein muss. Der Abschluss eines Zertifizierungsvertrages bezweckt die Schaffung einer Überprüfungsmöglichkeit für die breite Öffentlichkeit, die Zahl der Personen, die diese in Anspruch nehmen werden, ist ungewiss, wobei dies aber wiederum ein Wesensmerkmal des hier in Rede stehenden Vertrages ist. Der Zertifizierungsdiensteanbieter kann dieses, vordergründig unüberschaubare, Risiko durch entsprechende Vorkehrungen, wie etwa den Abschluss einer Haftpflichtversicherung, bis zu einem gewissen Maß einschränken. Schlussendlich ist auch das Vorliegen einer gewissen Schutzbedürftigkeit des Dritten zu bejahen, da, wie eben dargestellt, jeder andere wirksame haftungsrechtliche Schutz zu seinen Gunsten ausfällt. In Deutschland wird dementsprechend eine Haftungspflicht, beruhend auf §§ 278 und 282 BGB bejaht[271].

8.4.5 Aufbewahrungspflicht

Ebenso fraglich ist es, ob ein bloß in elektronischer Weise vorliegendes und signiertes Dokument dem Erfordernis einer „dauerhaften Aufbewahrung" genügt. Eine derartige Pflicht ist wiederholt in rechtsvertretenden Berufen etwa aus Gesetz, Vertrag oder aus Gründen der Beweissicherung vorgesehen. Umstritten ist in diesem Zusammenhang, ob ein ausschließlich in einem online-Verzeichnis enthaltenes signiertes Dokument als „hinterlegt" gelten kann. In diesem Zusammenhang wird es auf die dauerhafte Lesbarkeit des signierten Textes ankommen, d.h. im Bereich moderner Kommunikation auf die über Jahrzehnte aufrechtzuerhaltende Verfügbarmachung der Mittel zur Lesbarmachung elektronischer Dokumente.[272]

---

[270] Siehe etwa *Leier*, MMR 1/2000 S. 16

[271] siehe *Leier* und *Emmert*, S. 254f

[272] siehe auch unter http://www.mz.iao.fhg.de

8.4.6 Zugang einer elektronischen Willenserklärung und Rechtsfolgen einer Störung

Wie bereits in Kapitel 6.8. zum Abschluss eines Vertrages über Internet erwähnt, gilt eine Erklärung unter Abwesenden mit dem Zeitpunkt des Zugangs beim rechtmäßigen Empfänger und entfaltet dementsprechend Rechtswirkungen. Ein Widerruf ist nur insofern gültig und beachtlich, als er vor oder zumindest zeitgleich mit der Willenserklärung selbst zugeht.[273] Die Problematik liegt in jenen Fällen, in denen eine über Internet verschickte Nachricht verändert wird, sei es, dass die Ursachen dafür im Bereich des Absenders, des Netzbetreibers oder des Empfängers liegen.

Im erstgenannten Fall ist ein Empfangsbericht keinesfalls als Indiz, als Anscheinsbeweis für einen rechtzeitigen Zugang anzusehen. Dieser bildet keinen verlässlichen Nachweis dafür, dass in keinem Zeitpunkt des Übertragungsweges eine Störung aufgetreten ist, auch er ist Manipulationen zugänglich. Allenfalls deutet ein solcher auf den tatsächlichen Eingang beim Empfänger hin, sofern im Empfangsbericht sämtliche Daten über Sende- und Empfangsnummer, Übertragungsweg und Umfang des übertragenen Dokuments detailliert aufgelistet sind.[274]

Viel häufiger werden die Fälle sein, in denen ein Fehler vermuteterweise irgendwo auf dem Übertragungswege aufgetreten ist. Dies ist natürlich für den Absender nicht sichtbar und auch sehr schwer zu beweisen. Nimmt man im Verhältnis zwischen dem Betreiber des Übertragungsnetzes und dem Absender einen Vertrag werkvertraglichen Typs an, so ist auf die gesetzlich normierten Gewährleistungsregeln zurückzugreifen. Diese sehen jedoch keinerlei Haftung für Folgeschäden vor, welche in diesem Zusammenhang eine besonders wichtige Rolle spielen dürften. Geht man von einem Dienstvertrag aus, so ist der Absender wiederum verpflichtet, das Vorliegen eines Verschuldens auf der gegnerischen Seite nachzuweisen, um Ersatz zu erlangen.

---

[273] siehe § 130 Abs 1 BGB

Handelt es sich um die dritte Variante, d.h. liegt die Fehlerquelle im Bereich des Empfängers, so ist allgemein festzustellen, dass eine Haftung auf Seiten des Absenders unbillig wäre, sobald die Nachricht beim Empfänger unverändert zugegangen ist. Geht diese etwa erst im Rechner des zweiteren verloren, so geschieht dies auf Gefahr desselben und schließt einen Rückgriff auf seinen Vertragspartner aus.

8.5 Reformbestrebungen

8.5.1 Entwurf des deutschen Bundesministeriums für Justiz[275]

Das Bundesministerium für Justiz regt die Anpassung des deutschen Privatrechts an den modernen Geschäftsverkehr an; im Detail durch das Einfügen zahlreicher Normen in das BGB. Unter anderem sehen diese etwa eine die im Vergleich zur herkömmlichen Schriftform wesentlich leichter zu erfüllende sogenannte „Textform" vor. Diese hat weder die Verkörperung in einer Urkunde noch die Handschriftlichkeit der Unterzeichnung als Voraussetzung. Vielmehr soll es „genügen, wenn eine Willenserklärung einem anderen gegenüber so abgegeben wird, dass sie in Schriftzeichen lesbar und die Person des Erklärenden erkennbar ist."[276] Zusätzlich soll diese dem Erfordernis der gewillkürten Schriftform des § 127 BGB genügen.

In § 126 Abs. 3 des Entwurfes zum BGB kommt eine weitere Grundtendenz zum Ausdruck, wonach eine neue Form, die sogenannte „elektronische", in Zukunft als gleichwertiges Äquivalent zur Schriftform gelten soll, insofern und insoweit die spezifischen Funktionen einer Unterschrift auch in der elektronischen Umgebung voll erfüllt werden können. Sieht das Gesetz

274 siehe hiezu ausführlich http://www.mz.iao.fhg.de

275 Ausführlich hiezu *Müglich,* Neue Formvorschriften für den E-Commerce, MMR 1/2000, S. 9ff

276 in: *Geis*, Rechtsaspekte des elektronischen Geschäftsverkehrs, Eschborn 1999, S. 92

ausdrücklich die Schriftform als ein konstitutives Wirksamkeitserfordernis vor, so ist in diesem Bereich auch weiterhin kein Raum für die neue Technologie. Von dieser Grundregel abweichend sieht § 126 a Abs. 1 ausdrücklich die Möglichkeit der Hinzufügung des Namens und einer Signatur nach dem SigG vor. In diesem Falle ist auch ein auf Gesetzesstufe normiertes Schriftlichkeitserfordernis als erfüllt anzusehen.

Aufgrund der einzuhaltenden, besonders hohen Sicherheitsanforderungen in Zusammenhang mit der Erstellung einer mit dem Gesetz in Übereinstimmung stehenden Signatur wird durch § 292a ZPO eine besondere Beweiserleichterung zugunsten des Empfängers einer elektronischen Willenserklärung aufgestellt.

Ursprünglich wurde versucht, die hier in Rede stehenden Vermutungsregeln in einem neu einzufügenden § 126a Abs. 3 umzusetzen. Satz 1 dieser Norm fingiert die Zurechnung einer Willenserklärung zum Signaturschlüsselinhaber, wobei dieser erste Anschein jedoch jederzeit widerlegt werden kann. Die hier angesprochene Funktion der Identitätsfeststellung ist nicht gleichzusetzen mit dem Nachweis der Echtheit und Unverändertheit einer signierten Erklärung. Die Fülle der einzuhaltenden Sicherheitsmaßnahmen stellt in Zusammenhalt mit der Pflicht des Signators, eine vertrauenswürdige Umgebung der Signaturschlüsselgenerierung und -verwendung zu schaffen, einen wichtigen Anhaltspunkt dafür dar, dass der Signator zugleich auch Urheber der jeweiligen Erklärung ist. § 126 a Abs. 3 Satz 2 leg.cit. fixiert zweitere Regel, wonach bei Abgabe einer Signatur durch einen Dritten dessen Bevollmächtigung vermutet wird. Die hier zur Anwendung gelangenden Normkonstrukte von Anscheins- und Duldungsvollmacht verlangen auf Seiten des Schlüsselinhabers zu dessen eigener Sicherheit ein besonderes Maß an Sorgfalt und Vorsorge und schaffen beinahe eine der Gefährdungshaftung vergleichbare Situation. Die Gutgläubigkeit des Empfängers einer elektronisch signierten Erklärung wird unterstellt, offen bleibt natürlich die Frage, auf welche Weise es ersterem möglich sein soll, den Beweis des Gegenteiles zu erbringen, d.h. den Beweis eventuell vorliegender Bösgläubigkeit oder fehlender Bevollmächtigung des Dritten.

Nunmehr wurden diese Regeln kurz zusammengefasst, wonach der „Anschein der Echtheit, der sich aus der Überprüfung einer solchen Signatur nach dem Signaturgesetz zugunsten des Empfängers der in elektronischer Form dokumentierten Willenserklärung ergibt, nur durch Tatsachen erschüttert werden können, die es ernsthaft als möglich erscheinen lassen, dass die signierte Erklärung nicht mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist."[277]

Die derzeit aktuellste Fassung der hier angesprochenen Reformwünsche stellt der Referentenentwurf über ein Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Geschäftsverkehr mit Stand vom 5. Juni 2000 dar.[278] Dieser unternimmt in 34 Artikeln den ansatzweisen Versuch, die deutsche Privatrechtsordnung an die Eigenheiten neuer Kommunikationstechnologien anzupassen. Wie eingangs kurz dargestellt, implementiert der Gesetzesentwurf im wesentlichen zwei neue, bisher rechtlich nicht existente Formen in die bestehende Rechtsordnung. Zum einen die elektronische Form, welche den speziellen technischen Errungenschaften im Bereich der Informationstechnologien voll Rechnung trägt und als gleichwertiges Äquivalent zur herkömmlichen eigenhändigen Unterschrift dient. D.h. überall dort, wo die Eigenhändigkeit einer Willenserklärung vorgesehen ist, kann in Zukunft auch elektronisch signiert werden, wobei sämtliche Rechtsfolgen in ihrer Gesamtheit eintreten. Zum anderen neu eingeführt wird die, von der elektronischen Form völlig unabhängige, Textform. Von dieser kann in den Bereichen Gebrauch gemacht werden, in denen von der Notwendigkeit der eigenhändigen Unterzeichnung aufgrund nicht mehr gegebenen Erfordernisses abgesehen wird. Die Textform ist dementsprechend nicht gleichzusetzen mit der Schriftform, sie ist vielmehr eine Erleichterung und Abschwächung dieser.

[277] siehe BMJ-Entwurf, http://www.bmj.bund.de, S. 48

[278] vollständig zu lesen unter http://www.bmj.bund.de

Derzeit noch keinen Raum für den Einsatz der elektronischen Form bieten die gesetzlich fixierten detaillierten Verfahrensregelungen zur Erwirkung einer Eintragung in das Grundbuch oder in das Schiffsregister. Hier wird zwar nicht ausdrücklich ausschließlich die herkömmliche Unterschriftlichkeit für zulässig und anwendbar erklärt, jedoch sind die Eingaben in der Praxis an die Papierform gebunden. Dieses bestehende Erfordernis dient der Sicherstellung der Genauigkeit der Dokumentation des Rangverhältnisses entsprechend dem jeweiligen zeitlichen Eingang der Eingaben. Schon aus diesem Grund sind elektronische Erklärungen hier derzeit kategorisch ausgeschlossen, deren Einsatz in naher Zukunft ist jedoch keinesfalls ausgeschlossen.

Neben den grundlegenden Änderungen und Ergänzungen des Allgemeinen Bürgerlichen Gesetzbuches und der Zivilprozessordnung, welche im folgenden näher behandelt werden, werden in eine Reihe von weiteren deutschen Gesetzen Normen eingefügt, um dem rechtlichen Anpassungsbedarf voll Rechnung zu tragen. Zu erwähnen wäre hier etwa das Verbraucherkreditgesetz,[279] das Wohnungseigentumsgesetz,[280] das Handelsgesetzbuch[281] oder das Aktiengesetz.[282]

Im Referentenentwurf wird Bezug genommen auf die europäische Signaturrichtlinie und die E-Commerce-Richtlinie; Kompatibilität und Übereinstimmung der jeweiligen Gesetzesänderungen in ihrer geänderten Fassung werden ausdrücklich festgestellt. Gleichzeitig wird nicht ausgeschlossen, dass hinsichtlich des Signaturgesetzes ein Anpassungsbedarf

279 siehe im einzelnen § 4 Abs 1 Satz 3 Verbraucherkreditgesetz vom 17. Dezember 1990, BGBl I S. 2840 idgF, in: Referentenentwurf des Bundesministerium für Justiz: Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 5. Juni 2000

280 siehe im einzelnen § 24 Abs 4 Satz 1 Wohnungseigentumsgesetz BGBl III GNr. 403-1 idgF, in: siehe FN 168

281 siehe im einzelnen § 100 Abs 1 Satz 3 Handelsgesetzbuch BGBl III GNr 4100-1, in: siehe FN 168

282 siehe im einzelnen §§ 109 Abs 3, 121 Abs 4 Satz 1, 122 Abs 1 Satz 2 Aktiengesetz vom 6. September 1965 BGBl I S. 1089 idgF, in: siehe FN 168

bestehen könnte, dem nachzukommen jedoch nicht Aufgabe der hier in Rede stehender Revisionsbestrebungen sein kann.

Ebenso wie auch in Österreich wird seitens des deutschen Bundesministeriums für Justiz gänzlich darauf verzichtet, spezielle, nur für die elektronische Form geltende Regelungen zu Anfechtung, Zugang oder Widerruf einer Willenserklärung einzuführen. Sämtliche allgemeinen zivilrechtlichen Vorschriften behalten auch hier ihre volle Anwendbarkeit und Geltung. In manchen Bereichen ergeben sich aufgrund unterschiedlicher tatsächlicher Voraussetzungen und Gegebenheiten erhebliche Divergenzen. Um diese zu überwinden und zu entsprechenden situationsgerechten Lösungen zu gelangen, sind die von Lehre und Rechtsprechung entwickelten Auslegungskriterien heranzuziehen.

8.5.1.1 Änderung des bürgerlichen Gesetzbuches

8.5.1.1.1 Die elektronische Form

„§ 126 (3) (neu) Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt.“

Durch die soeben zitierte Vorschrift wird als Äquivalent zur herkömmlichen, die eigenhändige Unterschrift des Erklärenden voraussetzenden, Schriftform die sogenannte „elektronische Form“ rechtlich für zulässig erklärt. Um sämtliche mit einer Unterschrift verknüpften Rechtsfolgen herbeizuführen, hat der Unterzeichnende mit einer Signatur zu agieren, die dem Signaturgesetz entspricht. Ist in einer auf Gesetzesstufe stehenden Vorschrift ausdrücklich die Unzulässigkeit der elektronischen Signierung normiert, so schließt dies eine Verwendung kategorisch aus. In diesen Bereichen behält die Handschriftlichkeit oder alternativ dazu die notarielle Beurkundung weiterhin ihre konstitutive Bedeutung; die Unterzeichnung mittels elektronischer Medien führt in diesen Fällen zur Nichtigkeit des Rechtsgeschäftes.

„§ 126a (1) (neu) Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.

Zur Gänze neu eingefügt und nicht bloß im Zuge der Anpassungserfordernisse entsprechend geändert wurde § 126a zum BGB-Entwurf. Dieser nimmt Bezug auf die konkrete Ausgestaltung und die konkreten Erfordernisse einer elektronischen Signatur, welche der Schriftform des § 126 (in geänderter Form) genügen.

Grundvoraussetzung für die rechtliche und tatsächliche Gleichstellung ist laut dtBMJ die volle Funktionsäquivalenz, d.h. sämtliche im Rahmen der Schriftform verfolgten Ziele[283] sind auch bei Verwendung einer Signatur bestmöglich zu erfüllen. Festzustellen ist hier jedoch, dass manche Funktionen von der Schriftform, manche wiederum von der elektronischen Form besser erfüllt werden können. Im Hinblick auf die Funktion der Erbringung eines Beweises wird zweiterer ein erheblich höherer Wert beigemessen. Der Gesetzgeber stellt elektronische Urkunden nicht bloß auf die Stufe schriftlicher Privaturkunden, sondern fügt eine neue Vorschrift in die deutsche Zivilprozessordnung ein, welche spezielle Beweiserleichterungen zugunsten des Signaturschlüssel-Inhabers normiert.[284] Diese Bevorrechtung qualifizierter elektronischer Signaturen erfolgt aufgrund der hohen technischen Sicherheitsanforderungen des Art 5 SigRl und des dtSigG anerkanntermaßen zurecht. Andererseits bestehen in Zusammenhang mit der Warnfunktion einer elektronischen Signatur offensichtlich Defizite. Diese sollen zumindest teilweise ausgeglichen werden durch eine dementsprechende Kompliziertheit und Aufwendigkeit des Verfahrens der Signierung. Dies allein vermag jedoch nicht, die schon allein aufgrund der langjährigen Tradition mit der Eigenhändigkeit einer

283 Darunter zu subsumieren sind die Abschluss-, Perpetuierungs-, Identitäts-, Echtheits-, Verifikations-, Beweis-, Warn- und Kontrollfunktion

284 detailliert dargestellt in Kapitel 8.5.1.2.2 zu § 292a ZPO neu

Unterschrift verbundenen Vorteile vollständig auszugleichen. Diesem Faktum wird durch das zusätzliche Erfordernis einer auf besondere Weise zu erfolgenden Belehrung des Zertifikats- und Signaturschlüssel-Werbers entgegenzuwirken versucht. Diese hat durch eine Zertifizierungsstelle zu erfolgen, welche ihrerseits von staatlicher Seite hohen Anforderungen ausgesetzt ist, um ihre Vertrauenswürdigkeit bestmöglich zu gewährleisten, und ist vom Antragsteller zudem gesondert zu unterschreiben.

(2) (neu) Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren.

Mit Absatz 2 soll bloß sichergestellt werden, dass beide Vertragsparteien ihre Signatur unter ein inhaltlich übereinstimmendes Dokument setzen, so wie dies auch bei einem herkömmlichen Vertrag der Fall ist. Es kann daher auf keinen Fall genügen, dass der Angebotssteller lediglich sein eigenes Anbot und der Annehmende seine eigene Annahmeerklärung elektronisch signiert. Vielmehr ist zum Zwecke der Gegenzeichnung jeweils das konkrete Vertragsdokument mitsamt der zugehörigen elektronischen Signatur an den Geschäftspartner zu versenden.

8.5.1.1.2 Die Textform

§ 126b (neu) Ist durch Gesetz Textform vorgeschrieben, so muss die Erklärung einem anderen gegenüber so abgegeben werden, dass sie in Schriftzeichen lesbar, die Person des Erklärenden angegeben und der Abschluss der Erklärung in geeigneter Weise erkennbar gemacht ist.“

Unabhängig von der neu eröffneten Möglichkeit der Unterschriftsleistung durch eine qualifizierte elektronische Signatur, führt der Gesetzgeber in lit. b leg.cit. eine gegenüber der herkömmlichen Schriftform wesentlich erleichterte Form ein, die sogenannte „Textform“.

Um dieser zu genügen, hat die übermittelte Nachricht in lesbaren Schriftzeichen, d.h. in Buchstaben und Ziffern, beim Empfänger vorzuliegen. Eine nur hörbare Mitteilung, welche erst durch entsprechendes Tätigwerden in Text umgewandelt wird, genügt diesem Erfordernis nicht. Handelt es sich aber etwa um eine E-Mail, von welcher sich der Empfänger mittels eines Mail-Call-Dienstes Kenntnis verschafft, so liegt eine in Schriftzeichen lesbare Erklärung sehr wohl vor. Die auch inhaltlich einer Kenntnisnahme zugängliche und allgemein verständliche Willenserklärung hat in den Zugangs- und Machtbereich des Gegenübers zu gelangen, um Rechtswirkungen zu entfalten.

Als weitere Voraussetzung ist die Erkennbarkeit des Erklärenden genannt, um die übermittelten Daten auch entsprechend zuordnen zu können. Auf Details hierzu wird verzichtet, den konkreten Umständen entsprechend kann die Nennung eines lediglich zwischen den Vertragsparteien gebräuchlichen Spitznamens ebenso ausreichend sein.

Die Bezeichnung „Unterschrift“ allein deutet auf die Funktion des räumlichen Abschlusses einer Erklärung hin. Durch diese identifiziert sich der Unterschreibende mit dem jeweiligen Erklärungsinhalt. Bedient man sich der Textform, so ist dafür Sorge zu tragen, dass das Ende, der Abschluss eines Textes erkennbar und offensichtlich ist, etwa durch Anbringung eines entsprechenden kurzen Zusatzes, ein Faksimile, eine eingescannte Unterschrift udgl. Wird anstatt gesetzlich normierter Textform eigenhändig unterschrieben, elektronisch signiert, notariell beurkundet oder öffentlich beglaubigt, so ist dem Formerfordernis selbstverständlich ebenso Genüge getan, da es sich bei all diesen Formen um höherwertige Ersatzformen handelt.

8.5.1.1.3 Gewillkürte Form

„§ 127 (ergänzt) (1) Die Vorschriften des §§ 126, 126a oder des §126b gelten im Zweifel auch für die durch Rechtsgeschäft bestimmte Form.
(2) Zur Wahrung der durch Rechtsgeschäft bestimmten schriftlichen Form genügt, soweit nicht ein anderer Wille anzunehmen ist, die telekommunikative Übermittlung und

bei einem Vertrag der Briefwechsel. Wird eine solche Form gewählt, so kann nachträglich eine dem § 126 entsprechende Beurkundung verlangt werden.

(3) Zur Wahrung der durch Rechtsgeschäft bestimmten elektronischen Form genügt, soweit nicht ein anderer Wille anzunehmen ist, auch eine andere als die in § 126a bestimmte elektronische Signatur und bei einem Vertrag der Austausch von Angebots- und Annahmeerklärung, die jeweils mit einer elektronischen Signatur versehen wind. Wird eine solche Form gewählt, so kann nachträglich eine dem § 126a entsprechende elektronische Signierung oder, wenn diese einer der Parteien nicht möglich ist, eine dem § 126 entsprechende Beurkundung verlangt werden."

Auch die Regelungen betreffend der auf privatrechtlichem Wege vereinbarten Schriftform mussten in der Hinsicht verändert bzw. ergänzt werden, als dass nun auch in diesem Bereich vorstehende Normen betreffend elektronische Form und Textform voll Anwendung zu finden haben. Es gibt jedoch eine Erleichterung insoweit, als zur Wahrung der gewillkürten Form grundsätzlich auch eine Signatur, welche nicht den Anforderungen der deutschen Gesetzesvorlage entspricht, ausreicht. Der nationale Gesetzgeber versucht sich durch diese Regelung einerseits dem europarechtlichen Standard, festgelegt in der Signaturrichtlinie, anzunähern und andererseits den bereits bestehenden Nachholbedarf aufzuholen. Denn während Telefax und Telegramm in weiten Bereichen seit geraumer Zeit anerkanntermaßen als Unterschriftenersatz eingesetzt werden, ist dies bislang bei Signaturen mit weitaus höherem Sicherheitsstandard nicht der Fall.[285]

[285] Dementsprechend können nach deutscher Rechtsprechung Schriftsätze auch bei absolutem Anwaltszwang formwirksam durch Telefax bei Gericht eingebracht werden. Vom Gemeinsamen Senat der obersten Gerichtshöfe der Bundesrepublik Deutschland derzeit rechtlich zu beurteilen ist die Frage, ob auch ein Computerfax diesem Formerfordernis genügt. Während bei ersterem der unterschriebene Schriftsatz in körperlicher Form vorliegt, ehe er per Faxgerät versendet wird, wird bei zweiterem die Unterschrift eingescannt und einer Textdatei zugefügt. Beim Computerfax entfällt folglich der vorherige Ausdruck. Siehe auch *Thiele*, Clemens, Form- und Fristwahrung durch elektronische Übermittlung einer Textdatei?, MR 1999, S. 7ff

8.5.1.2 Änderung der Zivilprozessordnung

8.5.1.2.1 Elektronische Eingaben

„§ 130 (2) (neu) Soweit für Anträge und Erklärungen der Parteien sowie für Auskünfte, Aussagen, Gutachten und sonstige Handlungen hinzugezogener Personen oder Stellen die Schriftform vorgesehen ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn dieses für die Bearbeitung des Gerichts geeignet ist. Das Dokument soll mit einer qualifizierten elektronischen Signatur der das Schriftstück verantwortenden Person versehen und bei der Übermittlung gegen unbefugte Kenntnisnahme Dritter gesichert sein. Entsprechendes gilt für elektronische Dokumente anderen Inhalts. Bund und Länder bestimmen für ihren Bereich den Zeitpunkt, von dem an elektronische Dokumente den Gerichten in einer für ihre Bearbeitung geeigneten Form übermittelt werden können. Über die Eignung eines elektronischen Dokuments für seine Bearbeitung entscheidet das Gericht.

Das Unterschriftserfordernis bei gerichtlichen Eingaben bleibt aufrecht, jedoch lediglich in Form einer Ordnungsvorschrift. Dies bedeutet im Ergebnis, dass die Klageschrift ebenso wie alle anderen bestimmenden und vorbereitenden Schriftsätze in Zukunft trotz fehlender Unterschrift zulässigerweise eingebracht werden können. Eine Zurückweisung, gestützt auf einen bestehenden Formmangel, ist in diesem Zusammenhang nicht weiter vorgesehen.

Voraussetzung der Zulässigkeit elektronischer Eingaben bei Gericht ist natürlich das Bestehen ausreichender infrastruktureller Gegebenheiten. Dem Gericht muss die Erfassung, Bearbeitung und Verwaltung des Dokuments möglich sein, geeignete Hard- wie auch Software muss bereits vorhanden sein. Dementsprechend wird es dem Bund bzw. den Ländern überlassen, individuell für ihren räumlichen Bereich den Zeitpunkt zu bestimmen, ab welchem Schriftsätze auf elektronischem Wege eingebracht und übermittelt werden können.

Da es sich bei derartigen Angaben charakteristischerweise um vertrauliche Nachrichten handeln wird, ist einerseits die Vertraulichkeit der Daten, etwa mittels Verschlüsselung des gesamten Inhalts, und andererseits die Zuordenbarkeit zu ihrem Urheber absolut sicherzustellen. Letzterem Erfordernis wird in diesem Zusammenhang ausschließlich mittels einer qualifizierten elektronischen Signatur entsprochen, eine einfache Signatur wie bei der gewillkürten Form ist nicht ausreichend.

(3) (neu) Durch die rechtzeitige Übermittlung eines dem Absatz 1 Nr. 6, Absatz 2 nicht genügenden Schriftsatzes wird eine Frist gewahrt, wenn der Schriftsatz für das Gericht lesbar und in ihm die Person angegeben ist, die zu der Prozesshandlung befugt ist und den Schriftsatz verantwortet."

Die Einfügung eines neuen Absatz 3 konkretisiert die rechtlichen Folgen eines nicht formgerecht eingebrachten elektronischen Dokuments im Detail. Entsprechend der Ausgestaltung des Unterschriftserfordernisses als bloße Ordnungsvorschrift, treten im gegebenen Fall keine Säumnisfolgen ein, einzuhaltende Fristen werden trotz fehlender Unterschrift gewahrt. Das übermittelte Dokument muss lediglich lesbar und diejenige Person, welcher die Erklärung rechtlich zuzuordnen ist, also in der Regel der befugte Rechtsvertreter, erkennbar sein.

„§ 132 (3) (neu) Ein als elektronisches Dokument oder in anderer Weise durch Telekommunikation übermitteltes Schriftstück ist eingereicht, wenn die für den Empfang bestimmte Einrichtung des Gerichts es aufgezeichnet hat."

Entsprechend dieser Norm ist der Zeitpunkt des Einlangens eines Schriftstücks bei Gericht mit dem Zeitpunkt der dortigen Speicherung zu bestimmen; nur in Ausnahmefällen, d.h. bei veralterten Geräten ohne entsprechende Zwischenspeicherung, ist der vollständige Ausdruck maßgeblich.

8.5.1.2.2 Beweisrechtliche Behandlung elektronischer Dokumente

„§ 292a (neu) Der Anschein der Echtheit einer in elektronischer Form vorliegenden Willenserklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die es ernsthaft als möglich erscheinen lassen, dass die Erklärung nicht mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist. Der Beweis dieser Tatsachen kann auch durch den Antrag auf Parteivernehmung nach § 445 geführt werden."

In der Praxis von besonderer Relevanz ist die beweisrechtliche Handhabe elektronischer Dokumente. Vereinzelt wird die Gleichstellung mit Privaturkunden gefordert, die rechtlichen Konsequenzen daraus würden der in Deutschland vertretenen Meinung folgend[286] den unterschiedlichen tatsächlichen Gegebenheiten jedoch auf keinste Weise genügen. Die Echtheitsvermutung, dargelegt in §§ 439, 440 ZPO, statuiert lediglich die Vermutung der Echtheit des Inhalts eines Dokuments, insofern und insoweit die Unterschrift als solche nicht angezweifelt wird. Lediglich in diesem Fall gilt der Erklärungsinhalt als solcher des Unterzeichnenden. Würde diese, bislang ausschließlich auf Urkunden anzuwendende Beweisregel nun auch auf Dokumente in elektronischer Form ausgedehnt werden, so würde dies den Empfänger einer Erklärung erheblich benachteiligen. Jederzeit und ohne Anführung besonderer Gründe könnte von Seiten des Beweisgegners die Echtheit der elektronischen Unterschrift angezweifelt werden, die rechtliche Situation des ersteren wäre mehr als bloß unsicher einzuschätzen. Vielmehr wäre er in diesem Falle dazu verpflichtet, das Gegenteil, d.h. die Echtheit der Unterschrift, zu beweisen. Er müsste eindeutig und unzweifelhaft nachweisen, dass die Signatur vom Inhaber des Signaturschlüssels persönlich oder doch in seinem Namen und mit dessen Einverständnis im Rahmen einer Vollmacht abgegeben wurde. Dies dürfte in den meisten Fällen so gut wie unmöglich sein.

Der deutsche Gesetzgeber empfiehlt unter Berücksichtigung eben dargelegter Gründe daher eine Beweiserleichterung zugunsten des Erklärungsempfängers. Demnach soll eine Signatur derjenigen Person rechtlich zuordenbar sein, welche im Rahmen des dem Signaturgesetz entsprechenden Überprüfungsverfahrens als solche ausgewiesen ist. Dem Grundsatz des ersten Anscheins folgend hat dieser für sämtliche Signaturen einzustehen, welche mit dem ihm zugeordneten privaten Schlüssels erzeugt wurden. Der Beweis entgegenstehender Tatsachen, welche es ernsthaft für möglich erscheinen lassen, dass die Abgabe der Signatur ohne seinen Willen und ohne sein Wissen erfolgte, bleibt ihm jederzeit offen.

Durch diese Spezialvorschrift betreffend den Beweiswert und die beweisrechtliche Behandlung elektronisch signierter Dokumente wird dem, im Vergleich zu herkömmlichen, auf Papier geschriebenen Willenserklärungen, wesentlich höheren Sicherheits- und Fälschungsstandard entsprechend Rechnung getragen.[287]

Im übrigen unterfallen elektronische Dokumente den allgemeinen Regelungen über den Beweis durch Augenschein. Der jeweilige gegenständliche Datenträger ist dem Gericht vorzulegen, auch die elektronische Übermittlung der gespeicherten Daten ist denkbar. Die Richtigkeit der in der Erklärung behaupteten Tatsachen kann selbstverständlich durch Zeugen, Sachverständige, zusätzliche Beweismittel, Urkunden, udgl. bewiesen bzw. untermauert werden.

[286] siehe BMJ-Entwurf, http://www.bmj.bund.de, S. 46ff

[287] In Österreich wird ein elektronisch signiertes Dokument beweisrechtlich einer unterschriebenen Privaturkunde gleich-, jedoch nicht bessergestellt. Siehe dazu ausführlich unter Kapitel 7.7.2.

8.5.2 Vorschlag der deutschen Bundesnotarkammer[288]

8.5.2.1 „Elektronische Form“ und „elektronischer Urkundsbeweis“

Die Bundesnotarkammer wiederum trat bereits im Jahre 1997 als Verfechterin eines umfassende Reformgedankens auf, im Zuge dessen ein neue „elektronische Form“ wie auch ein neuer „elektronischer Urkundsbeweis“ in das BGB Eingang finden sollten, welcher sich offensichtlich jedoch nicht durchzusetzen vermochte. Erstere „soll gewahrt sein, wenn eine Erklärung digital signiert ist und der dazu verwendete Signaturschlüssel von einer Zertifizierungsstelle erst ausgegeben worden ist, nachdem der Schlüsselinhaber von einem Notar über die rechtlichen Risiken und deren Begrenzung unabhängig und unparteilich beraten und dies in einer notariellen Urkunde dokumentiert wurde.“[289] Wie die Zusammenarbeit von Zertifizierungsstelle und Notar im Detail aussehen soll, wird offengelassen. Im Zuge zahlreicher Änderungen und Ergänzungen soll auch eine Irrtumsanfechtung bei im Zuge der Übertragung aufgetretenen Fehlern möglich sein.[290]

Der Änderungsvorschlag der Bundesnotarkammer zu § 126 a sieht im einzelnen wie folgt aus:[291]

(1) Ist durch Gesetz die elektronische Form vorgeschrieben, so muss der Aussteller der Erklärung dem Text seinen Namen hinzusetzen und beides elektronisch unterzeichnen (elektronische Unterschrift). Die elektronische Unterschrift muss in einem als sicher

---

288 Siehe dazu ausführlich auch Geis, Die digitale Signatur, NJW 45/1997, S 3002ff

289 in: *Geis*, Rechtsaspekte des elektronischen Geschäftsverkehrs, Eschborn 1999, S. 93

290 siehe die einzelnen zu ändernden bzw. einzufügenden Paragraphen unter http:/www.mz.iao.fhg.de

291 siehe unter http://www.mz.iao.fhg.de

anerkannten Verfahren erklärungsabhängig und unterzeichnerabhängig hergestellt werden. Erklärung und Unterschrift muss auf eine Urkunde verweisen, in der der Aussteller die Zuordnung des verwendeten Unterschriftsschlüssels zu seiner Person erklärt hat, die Erklärung wiedergeben und die Stelle nennen, bei der der Unterschriftsschlüssel überprüft werden kann. Die Erklärung bedarf der notariellen Beurkundung.

(2) Die Anerkennung von Verfahren nach Abs. 1 Satz 2 erfolgt durch das Bundesministerium des Inneren. Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates die Anforderungen an diese Verfahren zu regeln. Die Zulassung von Stellen, die für die Ausgabe, Verwaltung und Überprüfung von Unterschriftsschlüsseln zuständig sind, erfolgt durch das Bundesministerium... Das Nähere regelt ein Bundesgesetz.

Durch zweitere, angestrebte Änderung soll dem faktisch sehr hohen Beweiswert elektronischer Signaturen Rechnung getragen werden; das Verfahren der Beweiswürdigung und -erbringung wäre dem bei einer schriftlichen Privaturkunde einzuhaltenden Procedere, dargestellt in § 416 ZPO, anzugleichen. Denn obwohl die Signaturrichtlinie durch Art 5 Abs. 2 keine eigene Beweisregel aufstellt bzw. vorschreibt, ist eine Differenzierung zwischen herkömmlicher und elektronischer Urkunde wohl kaum mehr zu rechtfertigen. Ebenso wie auch in der österreichischen Rechtsordnung umfasst die Beweiskraft einer Privaturkunde nur die formelle, nicht jedoch die materielle, also inhaltliche. Die Glaubwürdigkeit des Inhalts ist nach wie vor Gegenstand der freien gerichtlichen Beweiswürdigung nach § 286 ZPO. Im Rahmen der formellen Beweiskraft wird lediglich vermutet, dass die durch die Unterschrift ausgewiesene Person auch Urheber der unterzeichneten Erklärung ist. Allgemein gesprochen, ist eine elektronische Urkunde beweisrechtlich nur dann von Wert, wenn deren Abgabe, Zugang und inhaltliche Unverändertheit auf zuverlässige Weise nachweisbar sind.

Prozessualrechtlich ist eine elektronische Privaturkunde in gespeicherter wie auch visualisierter Form ein Augenscheinsobjekt. Wird ein elektronisches Dokument ausgedruckt, so ist dieses stets Kopie; wird es eigenhändig unterschrieben, so entsteht dadurch eine Urkunde.

9 Aktivitäten in den Mitgliedstaaten der Europäischen Gemeinschaft[292]

Neben Österreich und Deutschland unternehmen auch die übrigen Mitgliedstaaten der Europäischen Gemeinschaft erhöhte Anstrengungen, um einerseits den von der Europäischen Kommission aufgestellten Anpassungs- und Umsetzungserfordernissen gerecht zu werden und andererseits ihre Wettbewerbsposition und -fähigkeit am Internationalen Markt behalten bzw. fördern zu können.

Dementsprechend verabschiedete Italien ein Gesetz über den Gebrauch elektronischer Dokumente und Verträge,[293] Belgien,[294] Dänemark[295] und Spanien sind ebenso mit der Erarbeitung einer entsprechenden rechtlichen Grundlage für elektronische Signaturen beschäftigt. In keinem geringerem Maß tätig sind die Niederlande, Schweden und Großbritannien.

Aufbau und Grundprinzipien der in den Mitgliedstaaten laufenden Gesetzesinitiativen ähneln sich weitgehend, die konkrete Ausgestaltung weicht nur in geringem Maße voneinander ab. Geringfügige Differenzen werden aufgrund teils erheblicher Unterschiede in den nationalen

---

292 Einen umfassenden Überblick über den derzeitigen Stand der Gesetzgebungsverfahren in Europa wie auch in den USA bietet der Digital Signature Law Survey von *Simone van der Hof*, einsehbar unter http://www.kub.nl/~frw/people/hof/ds-lawsu.htm sowie eine Analyse des ILPF, einsehbar unter http://www.ilpf.org/digsig/analysis_IEDSII.htm.

293 siehe unter http://www.notariato.it/forum und http://ewis.kub.nl/~frw/people/hof/DS-lawsu.htm#it

294 sieh unter http://www.agoraproject.org

Rechtssystemen nicht zu verhindern sein, jedoch verzögern diese die Interoperabilität und grenzüberschreitende Einsetzbarkeit unterschriftenersetzender Signaturen. Auf jeden Fall ist dafür Sorge zu tragen, dass in all jenen Bereichen, in denen dies möglich ist, eine weitgehende Übereinstimmung erzielt wird. In technischen Belangen etwa ist von nationalen Abweichungen generell abzusehen.

[295] siehe unter http://www.fsk.dk/fsk/div/hearing/draft.html

10 Ausblick und Zusammenfassung

Die Entwicklung neuer Informationstechnologien ist einem ständigen Wandel unterworfen, wir befinden uns nicht am Ende eines Zeitalters, welches von rasantem technischen Fortschritt geprägt war, sondern inmitten desselbigen. Jedermann bzw. Jederfrau sollte sich dieser Tatsache bewusst sein und schon aus diesem Grund danach streben, Systeme, Verfahren und Methoden im täglichen Privat- und Geschäftsleben einzusetzen bzw. zu entwickeln, welche im Vergleich zu den dem jeweiligen Stand der Technik bereits entsprechenden noch sicherer, schneller, kostengünstiger und einfacher sind.

Dementsprechend gibt es auch auf europarechtlicher Ebene Initiativen, welche sich das Erreichen einer Fülle von Zielen innerhalb einer festgesetzten Frist zur Aufgabe gemacht haben. Als ein sehr breit angelegtes und demzufolge erfolgversprechendes Programm der Europäischen Kommission gilt eEurope 2002[296], welches Ende 1999 gestartet wurde. Sichere Netze und intelligente Chipkarten, Förderung des elektronischen Geschäftsverkehrs, elektronischer Zugang zu öffentlichen Diensten und Gesundheitsfürsorge über das Netz sind, um nur einige wenige zu nennen, erklärte Ziele dieses Aktionsplans. Durch entsprechende Maßnahmen und die Schaffung legislativer Rahmenbedingungen wird versucht, auch Europa am weltweiten wirtschaftlichen Wachstum, ausgelöst und gefördert durch den vermehrten Einsatz und die breite Akzeptanz neuer Medien, teilnehmen zu lassen.

Abschließend möchte ich noch ein letztes Mal hervorheben, dass kein spezielles Internetrecht existiert. Nationale und internationale Vorschriften, welche bislang nur auf den offline-Geschäftsverkehr anzuwenden waren und deren konkrete Ausgestaltung aus diesem einfachen Grund auf die herkömmliche Papierform zugeschnitten sind, gelten nun in gleicher Weise auch für sämtliche Aktivitäten im online-Bereich. Die Eigenheiten der neuen Informations- und

---

[296] siehe dazu ausführlich unter http://www.rdb.co.at/aktuell/t_0.htm und unter http://europa.eu.int/comm/information_society/eeurope/documentation/index_en.htm

Kommunikationstechnologien bergen spezifische und neuartige Sachverhaltskonstellationen und Problemstellungen in sich, welche einer Lösung zuzuführen sind. In diesem Zusammenhang besonders gefordert ist die Judikative, welche entsprechende Lösungsansätze zu entwickeln hat, ohne auf gefestigte Judikatur zurückgreifen zu können.

LITERATURVERZEICHNIS

Andreewitch, Markus, Zur Anwendbarkeit des Produkthaftungsgesetzes für Softwarefehler, EDVuR 1990

Beuscher, Klaus, *Schmoll*, Andrea, Kryptotechnologie und Exportbeschränkungen, in CR 8/1999

Bieser, Wendelin/ *Kersten*, Heinrich, Chipkarte statt Füllfederhalter: Daten beweissicher „elektronisch unterschreiben" und zuverlässig schützen, Heidelberg: Hüthig, 1998

Brenn, Christoph, Das österreichische Signaturgesetz - Unterschriftenersatz in elektronischen Netzwerken, in ÖJZ 16/1999

Brenn, Christoph, Der elektronische Geschäftsverkehr, in ÖJZ 13/1999

Brenn, Christoph, Signaturgesetz: SigG: Bundesgesetz BGBl I 1999/190 mit den Materialien und zusätzlichen Anmerkungen, Wien 1999

Brenn, Christoph, Verbürgung durch mouse-click?, in ecolex 4/1999

Brenn, Christoph, Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet, in ÖJZ 17/1997

Brisch, Klaus M., EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr, in CR 4/1999

Ebbing, Frank, Schriftform und E-Mail, in CR 5/1996

Emmert, Ulrich, Haftung der Zertifizierungsstellen, in CR 4/1999

Engel-Flechsig, Rechtliche Grundlagen für die Informationsgesellschaft, in: *Geis*, Rechtsaspekte des elektronischen Geschäftsverkehrs, Eschborn 1999

Engel-Flechsig, Stefan/ *Maennel*, Frithjof A./ *Tettenborn*, Alexander, Das neue Informations- und Kommunikationsdienste-Gesetz, in NJW 45/1997

Engel-Flechsig/Roßnagel, Muldimedia-Recht 1998

Fallenböck, Markus/ *Schwab*, Guido, Zu der Charakteristik und den Rechtswirkungen elektronischer Signaturen: Regelungsmodelle in den USA und Europa, in MR 6/1999

Fitz/Purtscheller/Reindl, Produkthaftung: Kommentierung des PHG samt Richtlinie, Wien 1988

Forgo, Nikolaus, Sicher ist sicher? - Das Signaturgesetz, in ecolex 9/1999

Forgo, Nikolaus, Was sind und wozu dienen digitale Signaturen?, in ecolex 4/1999

Geis, Ivo, Die digitale Signatur, in NJW 45/1997

Gidari, Albert/ *Morgan*, John P./ *Coie*, Perkins, Survey of Electronic and Digital Signature Legislative Initiatives in the United States, prepared for ILPF (Internet Law & Policy Forum), September 12, 1997

Gravesen, Gavan G./ *Dumortier*, Jos/ *Van Eecke*, Patrick, Die europäische Signaturrichtlinie - Regulative Funktion und Bedeutung der Rechtswirkung, in MMR 10/1999

Greindl, Georg/ Köck, Bettina/ Zehetmayer, Georg; Recht haben im Internet, trend-manager 1/2000
Kapp, Mario, Digitale Signatur: Zertifizierung und Gesetzesentwurf, in Datagraph 2/1999

Huemer, *Saxinger*, *Baumann & Partner*, Bundesgesetz über elektronische Signaturen, AnwBl 1999

Jud, *Högler-Pracher*: Die Gleichsetzung elektronischer Signaturen mit der eigenhändigen Unterschrift, ecolex 1999

Jud,Waldemar *Högler-Pracher*, Renate, Schiedsverfahren mit modernen Kommunikationstechniken, ecolex 1999

Kilches, Ralph, Electronic Commerce Richtlinie, in MR 1999

Kilches Ralph, Mediendienste-Staatsvertrag und IuKDG: Deutschlands Weg in die Informationsgesellschaft, MR 1997

Koziol, Helmut in *Koziol/Welser*, Bürgerliches Recht[11], Bd. 1, Wien 2000

Koziol/Welser, Grundriß des bürgerlichen Rechts I10, Wien 1995

Kuner, Christopher, Das Signaturgesetz aus internationaler Sicht, in CR 10/1997

Kutschera, Axel, Funktion und Verwendbarkeit der elektronischen Signatur: Die geltende Rechtslage im Überblick: Praktische Relevanz des Signaturgesetzes, in SWK 2000, W 7

Leier, Barbara, Haftung der Zertifizierungsstellen nach dem SigG: Betrachtung der geltenden und Überlegungen zur zukünftigen Rechtslage, in MMR 1/2000

Mader, Peter, Technische Grundlagen und Grundbegriffe, in: *Jahnel*, Dietmar/ *Mader*, Peter, EDV für Juristen[2], Wien 1998

Madl, Peter, Vertragsabschluß im Internet, ecolex 1996

Mayer-Schönberger, Viktor/ *Pilz*, Michael/ *Reiser*, Christian/ *Schmölzer*, Gabriele, Sicher & echt: Der Entwurf eines Signaturgesetzes, in MR 1998

Mayer-Schönberger, Viktor/ *Pilz*, Michael/ *Reiser*, Christian/ *Schmölzer*, Gabriele, Signaturgesetz: Praxiskommentar, Wien 1999

Mayer-Schönberger, Viktor/ *Pilz*, Michael, E-Commerce: Rechtliche Rahmenbedingungen und Notwendigkeiten, in AnwBl 4/1999

Mayer-Schönberger, Bedauerlich: Signatur-Dienstleister nach der SigV, ecolex 2000

Menzel, Thomas, Elektronische Signaturen, Bd. 2, Wien 2000

Mottl, Ingeborg, Electronic Commerce im Internet, in: *Jahnel*, Dietmar/ *Schramm*, Alfred/ *Staudegger*, Elisabeth, Informatikrecht, Wien 2000

Mottl, Ingeborg, Zur Praxis des Vertragsabschlusses im Internet, in: *Gruber*, Michael/ *Mader*, Peter, Internet und e-commerce: Neue Herausforderungen an das Privatrecht, Wien 2000

Müglich, Andreas, Neue Formvorschriften für den E-Commerce, Zur Umsetzung der EU-Signaturrichtlinie in deutsches Recht, in MMR 1/2000

OGH vom 7.7.1988, 6 Ob 612/88 in ZfRV 1989

OGH vom 26.2.1996, 4 Ob 518/96 in RdW 1997

Österreichisches Anwaltsblatt, AnwBl 8/2000

Österreichischer Rechsanwaltskammertag, Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), in AnwBl 1999

Pankart, Sichere E-Mail: Signieren und Verschlüsseln, in Datagraph 2/2000

Riedl, Sabine, Auch die UNCITRAL mengt sich in den elektronischen Geschäftsverkehr ein, in ecolex 1999

Roth, Marianne, Gerichtsstand und Kollisionsrecht bei Internetgeschäften in: *Gruber*, Michael /*Mader*, Peter: Internet und e-commerce: Neue Herausforderung an das Privatrecht, Wien 2000, S. 165ff

Roßnagel, Alexander, Anerkennung von Prüf- und Bestätigungsstellen nach dem Signaturgesetz, in MMR 6/1999

Roßnagel, Alexander, Das Signaturgesetz nach zwei Jahren, in NJW 22/1999
Roßnagel, Alexander, Europäische Signatur-Richtlinie und Optionen ihrer Umsetzung, in MMR 5/1999

Salzburger Nachrichten vom 29.5.1998, Elektronische Signatur, Geschäfte im „globalen Markt“ - Richterwoche Schruns

Salzburger Nachrichten vom 23. September 2000 betreffend DaMe - Das Datennetz der Medizin

Schauer, E-Commerce in der Europäischen Union, Wien 1999

Schauer, Bernd, eCommerce in der EU, Bd. 3, Wien 1999

Schweighofer, Erich/ *Menzel*, Thomas (Hg.): E-Commerce und E-Government: aktuelle Fragestellungen der Rechtsinformatik, Bd. 1, Wien 2000

Starl, Klaus, Änderungen der Verordnung zum elektronischen Rechtsverkehr, in Datagraph 2/1999

Starl, Klaus, Europäische Regelungen zum E-Commerce, in Datagraph 2/1999

Stockinger, Stefan, Österreichisches Signaturgesetz: Bedeutung, Funktion und Rechtsfolgen elektronischer Signaturen, in MR 4/1999

SWK 1998, T 114, „Amtsweg per Mausklick“ bereits Realität für 920 WT - „FINANZonline“ ermöglicht Zugriff auf Finanzdateien“

Thiele, Clemens, Form- und Fristwahrung durch elektronische Übermittlung einer Textdatei?, MR 1999

Van der Hof, Sabine, Digital Signature Law Survey, Version 3.9, April 2000, unter http://cwis.kub.nl/~frw/people/hof/ds-lawsu.htm

Weissengruber, Christian, Elektronische Zahlungssysteme: Sichere Zahlungen mit eigenem Standard, in Computerwelt 38/2000

Weninger, FINANZOnline in der zweiten Ausbaustufe: Elektronische Anbringen und Erledigungen rücken näher, ÖStZ 2000/699

Gesetzestexte

Aktiengesetz vom 6. September 1965 BGBl I S. 1089 idgF

Allgemeines Bürgerliches Gesetzbuch [Anlage des kaiserlichen Patents vom 1.6.1811, JGS. Nr. 946]

Bericht des Justizausschusses über die Regierungsvorlage (1999 der Beilagen): Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), 2065 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP

Brüsseler Gerichtsstands- und Vollstreckungsübereinkommen (EuGVÜ), ABl. C 189/2 1990; RV 1285 BlgNR XX. GP

Bundesgesetz, mit dem das Signaturgesetz geändert wird, BGBl. II Nr. 137/2000

Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000) BGBl. I Nr. 165/1999

Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), BGBl. I Nr. 190/1999 idgF.

Bundesgesetz vom 2. Dezember 1958 über den Versicherungsvertrag (Versicherungsvertragsgesetz 1958), BGBl. Nr. 2/1959 idgF.

Bundesgesetz vom 1. Juli 1975 über das Eigentum an Wohnungen und sonstigen Räumlichkeiten (Wohnungseigentumsgesetz 1975 - WEG 1975), BGBl. Nr. 417/1975

Bundesgesetz vom 15. Juni 1978 über das internationale Privatrecht (IPR-Gesetz), BGBl Nr. 304/1978 idgF

Bundesgesetz vom 8. März 1979, mit dem Bestimmungen zum Schutz der Verbraucher getroffen werden (Konsumentenschutzgesetz - KSchG), BGBl. 1979/140 idgF.
Bundesgesetz vom 12. November 1981 über das Mietrecht (Mietrechtsgesetz - MRG), BGBl. Nr. 520/1981

Bundesgesetz vom 21. Jänner 1988 über die Haftung für ein fehlerhaftes Produkt (Produkthaftungsgesetz) BGBl. Nr. 99/1988

FINANZOnline-Verordnung (FOnV) BGBl. II Nr. 71/1998

Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen, Brüssel, den 29.4..1999, KOM (1999) 195 endg.

Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, KOM (1999) 427 endg.

Gemeinsamer Standpunkt des Rates im Hinblick auf den Erlaß der Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), Brüssel, den 28. Februar 2000, 14263/1/99

Gemeinsamer Standpunkt des Rates im Hinblick vom 28. Februar 2000, 14263/1/99 REV 1

Gemeinsamer Standpunkt EG) Nr. 28/1999 vom Rat festgelegt am 28. Juni 1999 im Hinblick auf den Erlaß der Richtlinie 1999/.../EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. C 243 vom 27.8.1999

Gesetz RGBl 1871/76 betreffend das Erfordernis der notariellen Errichtung einiger Rechtsgeschäfte

Gesetz vom 6. März 1906 über Gesellschaften mit beschränkter Haftung (GmbHG), RGBl. 1906/58

Gesetz vom 1. August 1895, RGBl 1895/111, über die Ausübung der Gerichtsbarkeit und die Zuständigkeit der ordentlichen Gerichte in bürgerlichen Rechtssachen (JN)

Gesetz zur digitalen Signatur (dtSigG) (Artikel 3 des Gesetzes, Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste[Informations- und Kommunikationsdienstegesetz - IuDKG]) vom 13. Juni 1997, veröffentlicht im dt. BGBl. I vom 28. Juli 1997, S 1870

Gewerbeordnung 1994 - GewO 1994 BGBl Nr. 194/1994

Handelsgesetzbuch BGBl III GNr 4100-1

IPRG, BGBl. 1978/304 idgF.

KOM 503 endg. vom 8.10.1997

Luganer Gerichtsstand- und Vollstreckungsübereinkommen, (LGVÜ) BGBl 1996/448

Politische Übereinkunft über einen gemeinsamen Standpunkt des Rates zu einer Richtlinie über elektronische Signaturen (22. April 1999), http://europa.eu.int/comm/dg15/de/media/sign/composde.htm

Referentenentwurf des Bundesministerium für Justiz: Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 5. Juni 2000

Richtlinie 85/374/EWG zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte, ABl L 210/1985, 29 um.

Richtlinie 85/557/EWG betreffend den Verbraucherschutz im Falle von außerhalb von Geschäftsräumen abgeschlossenen Verträgen, Abl. 372/1985
Richtlinie 95/46 des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. L 281 v. 23.11.1995

Richtlinie 97/7/EG des Europäischen Parlaments und des Rates vom 20.5.1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz, ABl. L 144 vom 4.6.1997

Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L 13 vom 19.1. 2000

Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Rechtsverkehr"), ABl. L 178/1 vom 17.7.2000

Stellungnahme des Ausschusses der Regionen zur Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen „Europäische Initiative für den Elekronischen Geschäftsverkehr, Brüssel, 12. März 1998, KOM (97) 157 endg.

Stellungnahme des Ausschusses der Regionen zu dem „Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen", ABl. C 93 vom 6.4.1999

Stellungnahme des Wirtschafts- und Sozialausschusses, ABl. C 40 vom 15.2.1999

Telekommunikationsgesetz - TKG, dt. BGBl. I Nr. 100/1997 samt Novellen, http://www.tkc.at/www/RechtsD.

Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf, BGBl. 1988/96

Übereinkommen vom 19. Juni 1980 über das auf vertragliche Schuldverhältnisse anzuwendende Recht, BGBl. III Nr. 208/1998 (EVÜ)

Übereinkommen von Rom über das auf vertragliche Schuldverhältnisse anzuwendende Recht von 1980 (konsolidierte Fassung), ABl 1998 C 27/34 ff, auch Europäisches Vertragsrechtsübereinkommen (EVÜ) genannt.

Verordnung des Bundeskanzlers über die Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie–Austria (A-Sit)“ als Bestätigungsstelle, BGBl. II 31/2000.

Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV), BGBl. II Nr. 30/2000

Verordnung zur digitalen Signatur (dtSignaturverordnung - SigV) in der Fassung des Beschlusses der Bundesregierung vom 8. Oktober 1997, veröffentlicht im dt. BGBl. I vom 22.10.1997, S 2498

Vertrag von Amsterdam zur Änderung des Vertrags über die Europäische Union, der Verträge zur Gründung der Europäischen Gemeinschaften sowie einiger damit zusammenhängender Rechtsakte samt Schlussakte (Vertrag von Amsterdam), BGBl. III Nr. 83/1999

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen, Brüssel, den 13.5.1998, KOM (1998) 297 endg.

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen, ABl. C 325 vom 23.10.1998

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, ABl. C 30 vom 5.2.1999

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen, ABl C 104 vom 14.4.1999

Wohnungseigentumsgesetz BGBl III GNr. 403-1 idgF

Kommentare

Dittrich/Tades, Das Allgemeine bürgerliche Gesetzbuch: ABGB, 35. Auflage, Wien 1999

Fasching, Hans W., Lehrbuch des Österreichischen Zivilprozeßrechts, 2. Auflage, Wien 1990

Fitz, Hanns/*Purtscheller*, Meinhard/*Reindl*, Peter, Produkthaftung, Wien 1998
Harrer, Praxiskommentar zum ABGB samt Nebengesetzen², Bd. 7

Kosesnik-Wehrle/Lehofer/Mayer, Konsumentenschutzgesetz: KSchG, Wien 1997

Koziol, Helmut, Österreichisches Haftpflichtrecht, Bd. II, Besonderer Teil, Wien 1975

Nitsche, Gunther/ *Nowotny*, Christian/ *Zetter*, Peter, Handelsgesetzbuch, 13. Auflage, Wien 1994
Rechberger, Walter H., Kommentar zur ZPO: Jurisdiktionsnorm und Zivilprozeßordnung samt den Einführungsgesetzen, Wien 1994

Rechberger, Walter H./ *Simotta*, Daphne-Ariane, Grundriß des österreichischen Zivilprozeßrechts, 4. Auflage, Wien 1994

Rummel, Peter, Kommentar zum Allgemeinen bürgerlichen Gesetzbuch, 2. Auflage, Wien 1992

Schönherr, Fritz/ *Nitsche*, Gunter, Handelsgesetzbuch, 27. Auflage, Wien 1981

Stohanzl, Rudolf, Jurisdiktionsnorm und Zivilprozeßordnung, 14. Auflage, Wien 1990

*Stohanz*l, Rudolf, Zivilprozeßgesetze, 7. Auflage, Wien 1995

Straube, Manfred, Kommentar zum Handelsgesetzbuch, Wien 1987

Würth, Helmut/ *Zingher*, Karl , Miet- und Wohnrecht, 20. Auflage, Wien 1997