Die elektronische Signatur im österreichischen Recht: ein Überblick

Veit Öhlberger

veit.oehlberger@utanet.at

Schlagworte: Elektronische Signatur, Zertifikat, Funktionsweise, Rechtswirkung, Anwendungsbereich

Abstract: Das Internet ist aus dem rechtsgeschäftlichen Bereich nicht mehr wegzudenken und stellt auch für den Verwaltungsapparat eine enorme Chance dar, Bürgernähe und rasche Erledigungen zu gewährleisten. Bei der Sicherstellung von Echtheit und Unverfälschtheit von übermittelten Informationen erlangt die elektronische Signatur immer größere Bedeutung. Nach Darstellung der Funktionsweise folgt eine Übersicht über Rechtsgrundlagen und Rechtswirkungen. Weiters werden einige Detailfragen des Signaturrechtes angesprochen und die diskutierten bzw bereits tatsächlichen Anwendungsbereiche des elektronischen Pendants zur eigenhändigen Unterschrift skizziert.

1. Vorbemerkung

Durch die weltumspannende Vernetzung interaktiver und multimedialer Dienste können grenzüberschreitende wirtschaftliche Transaktionen in kürzester Zeit abgewickelt werden. Online-Dienste ermöglichen nicht mehr nur die Anbahnung erster Kontakte und die Abwicklung von Geschäftstätigkeiten, sondern auch den direkten Bezug von Waren und Dienstleistungen. Es wird prognostiziert[1], dass bereits im Jahr 2004 insgesamt 6,8 Trillionen $ im Internet umgesetzt werden. Europa wird von diesem Umsatz 22 % leisten. In den nächsten fünf Jahren wird der Verkauf von Waren und Dienstleistungen über das Netz in Europa um 140 % pro Jahr steigen. 2004 werden 6 % aller Käufe in Europa über Internet durchgeführt werden. Doch nicht nur im Geschäftsverkehr sondern auch im Bereich der staatlichen Verwaltung soll das Internet immer größere Bedeutung erlangen. Durch die Beteiligungsmöglichkeit von jedem, der über Computer und Internetanschluss verfügt, werden kaum vorstellbare Dimensionen erreicht, worin gleichzeitig auch nicht zu unterschätzende Gefahren

[1] Umfassende Studien zu E-Commerce unter http://www.forrester.com.

liegen[2], da Fremdeinwirkungen leichter erfolgen können als bei anderen Kommunikationsmitteln. Um über Authentizität (Echtheit) und Integrität (Unverfälschtheit) der übermittelten Informationen sicher sein zu können, bedarf es also einer gewissen Kontrollmöglichkeit, ansonsten wäre das Internet für den rechtsgeschäftlichen Bereich und für die öffentliche Verwaltung unattraktiv. Diese Kontrollmöglichkeit liegt in der Versiegelung eines Textes durch eine elektronische Signatur, bei der es sich nicht um eine digitalisierte Version des Schriftzuges einer eigenhändigen Unterschrift handelt, sondern um eine Codierung.

2. Elekronische Signatur – digitale Signatur

2.1. Begriffsdefinitionen

Die beiden Begriffe bedeuten keineswegs dasselbe, denn nicht jede elektronische Signatur ist eine digitale Signatur. Bei der elektronischen Signatur handelt es sich um den Überbegriff, der alle Methoden der elektronischen Authentifizierung umfasst. Die digitale Signatur hingegen ist eine elektronische Signatur, die mit Hilfe asymmetrischer Kryptographie erstellt wird. Das asymmetrische Verschlüsselungsverfahren stellt derzeit die wichtigste eingesetzte Technologie dar und deshalb wird im Zusammenhang mit elektronischen Signaturen immer auch von digitalen Signaturen gesprochen. Doch im Sinne eines technologieneutralen Ansatzes wird sowohl in der Richtlinie als auch im SigG nur der Begriff elektronische Signatur verwendet.

Der österreichische Gesetzgeber[3] unterscheidet die Begriffe (einfache) elektronische Signatur und sichere elektronische Signatur. Der Begriff der (einfachen) elektronischen Signatur entspricht dem des technologieneutralen Überbegriffes. Die Merkmale einer sicheren elektronischen Signatur werden unter § 2 Z 3 SigG näher beschrieben. Sichere elektronische Signaturen sind demnach solche, die die Identifizierung des Signators sicherstellen, ausschließlich diesem zugeordnet und unter seiner alleinigen Kontrolle zu erstellen sind, nachträgliche Veränderungen unmöglich machen, auf einem qualifizierten Zertifikat (siehe 2.3.) beruhen und mit sicheren technischen Komponenten

---

[2] Über die Gefahren und deren Zurechnung: *Zib*, Electronic Commerce und Risikozurechnung im rechtsgeschäftlichen Bereich, ecolex 1999, 230.

[3] Siehe § 2 SigG: Begriffsbestimmungen.

erstellt wurden. Diese Unterscheidung ist für die Rechtswirkung der Signatur von Bedeutung (siehe 4.).

Ein Zertifikat wird von einer Zertifizierungsstelle (siehe 2.3.) ausgestellt und bestätigt, dass der Inhaber der Signatur tatsächlich auch derjenige ist, der als solcher aufscheint.

2.2. Funktionsweise[4]

Allgemein unterscheidet man in der Kryptographie zwei Verschlüsselungsverfahren. Beim symmetrischen Verfahren vereinbaren Sender und Empfänger einen gemeinsamen Code. Der Nachteil dieses Verfahrens liegt darin, dass der vorherige Austausch des Schlüssels ein Sicherheitsrisiko in sich birgt und dass für jeden Geschäftspartner ein eigener Code benötigt wird. Beim asymmetrischen Verschlüsselungsverfahren hingegen, und allein dieses wird zum Erstellen und Verifizieren von digitalen Signaturen herangezogen, bedarf es für alle Geschäfte eines Signators nur eines einzigen Schlüsselpaares, wobei der öffentliche Schlüssel für jedermann zugänglich ist. Da grundsätzlich nur das asymmetrische Verfahren zum Erstellen und Verifizieren von Signaturen herangezogen wird, ist allein dieses in Folge zu erläutern.

Die digitale Signatur selbst ist ein Zahlencode, der am Ende eines zu versendenden Dokumentes angebracht wird und sich mit den Dokumentdaten verknüpft. Sie erscheint beim Empfänger als besonders gekennzeichneter, unleserlicher Teil der übermittelten Daten. Eine Signatur lässt den Text selbst lesbar. Ein Unlesbarmachen des Textes scheint zur Sicherheit der Allgemeinheit nicht erstrebenswert[5] und ist nicht Gegenstand des SigG. Bei dieser Verknüpfung[6] der Signatur mit den Dokumentdaten wird eine Prüfsumme – eine für den Dokumentinhalt repräsentative Datenkombination (sog Hash-Wert) – gebildet, die verschlüsselt wird. Bei der Entschlüsselung durch den Empfänger wird wiederum eine Prüfsumme ermittelt und diese mit der entschlüsselten Prüfsumme des Senders verglichen. Sind die beiden Prüfsummen ident, so sind dies auch die Dokumentdaten – der Text ist also nicht verändert worden. Weiters wird durch das Entschlüsseln bestätigt, dass die

---

[4] Dazu ausführlich: *Brenn*, Signaturgesetz, 36ff; *Menzel*, Elektronische Signaturen, 25ff.

[5] *Brenn*, Signaturgesetz, 46.

[6] Die Verknüpfung erfolgt mit Hilfe mathematischer Algorithmen (genauer dazu die Literatur unter FN 4).

Nachricht vom angegebenen Absender stammt, da sonst der Schlüssel nicht gepasst hätte.

Das asymmetrische Verschlüsselungsverfahren arbeitet mit einem Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel, wobei letzterer jedermann zugänglich ist (zB durch Download von der firmeneigenen Homepage oder von speziellen Datenbanken, sog key-servern). Wenn der Sender eine Nachricht digital signieren will, so erfolgt dies mit seinem privaten Schlüssel. Der Empfänger prüft die Signatur mit dem öffentlichen Schlüssel, der keine Aufdeckung des privaten Signaturschlüssels ermöglicht, sondern lediglich – durch Vergleich der beiden Prüfsummen – bestätigt, das der Text unverändert ist und dass die Daten vom Unterzeichner stammen, da der öffentliche Schlüssel nur Verschlüsselungen des korrelierenden privaten Schlüssels entsperrt.

Der Zweck der digitalen Signatur liegt somit darin, die Unverfälschtheit der übermittelten Nachricht sicherzustellen und dem Empfänger zu ermöglichen, iVm einem Zertifikat die Identität des Absenders zweifelsfrei festzustellen.

2.3. Sicherheit durch Zertifikate

Der Nachteil des symmetrischen Verschlüsselungsverfahrens – die notwendige persönliche Kontaktaufnahme zum Austausch des Schlüssels – hat auch einen Vorteil: man erhält Informationen über die Identität des Geschäftspartners. Bei dem asymmetrischen Verfahren ist aufgrund des öffentlichen Schlüssels keine Kontaktaufnahme notwendig. Das Schlüsselpaar selbst kann aber nicht gewährleisten, dass deren Inhaber tatsächlich jene Person ist, für die er sich ausgibt. Daher bedarf es eines Dritten, der die Identitätsangaben des Schlüssels sicher ihrem Inhaber zuordnet. Die Zuordnung erfolgt durch Zertifikat einer Zertifizierungsstelle, welches unterschiedliche Sicherheitsstufen aufweisen kann: angefangen bei einem Zertifikat niedrigster Sicherheit, das durch E-Mail erworben wird, über Absicherungen durch telefonische Überprüfung oder Faxen einer Ausweiskopie, bis zur höchsten Stufe, bei der eine Zertifizierung nur nach persönlicher Vorsprache und Ausweisleistung erfolgt.

Im Moment gibt es vier Zertifizierungsstellen, die der Telekom-Control-Kommission[7] die Aufnahme der Tätigkeit angezeigt haben; nämlich die Generali Office-Service und Consulting AG, die Datakom Austria GmbH, die Arge Daten – Österreichische Gesellschaft für Datenschutz und das Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie. Die Kosten eines Zertifikates, deren Nutzung durch die Anbieter auf ein bis zwei Jahre beschränkt wird, betragen derzeit zwischen 0,- ATS für Demo-Zertifikate mit niedrigster Sicherheit („zum Ausprobieren"), über 260,- ATS (Euro 18,90) bis 690,- ATS (Euro 50,14) für solche „mittlerer" Sicherheit, bis hin zu 4.405,- ATS (Euro 320,00) für Software-Entwickler-Zertifikate.

Da das System der sicheren Zuordnung von Schlüsseldaten zu einer natürlichen Person nicht mehr funktioniert, wenn die Zertifizierungsstellen nicht „sicher" genug arbeiten, sind diese gem § 13 SigG einer Aufsichtsstelle[8] unterstellt: der Telekom-Control-Kommission.

Hingegen wird die Einhaltung technischer Sicherheitsstandards bei der Erstellung sicherer elektronischer Signaturen (Mindestkriterien werden im Anhang III zur Signaturrichtlinie festgelegt) von einer sog Bestätigungsstelle (§ 18 Abs 5, § 19 SigG) überwacht. Durch die Ausführungsverordnung zum SigG BGBl II 2000/31 stellte der Bundeskanzler im Einvernehmen mit dem Bundesminister für Justiz gem § 19 Abs 4 SigG die Eignung des Vereines „Zentrum für sichere Informationstechnologie – Austria (A-SIT)" als Bestätigungsstelle fest.[9]

Wie bereits erwähnt, ist für eine sichere elektronische Signatur ein qualifiziertes Zertifikat notwendig, welches hohen Sicherheitsanforderungen entspricht (Identitätsnachweis durch Lichtbildausweis gem § 7 Abs 1 Z 4 und § 8 Abs 1 SigG). Weiters muss das qualifizierte Zertifikat ausreichend Information über den Inhaber enthalten (§ 5 SigG) und auch die Zertifizierungsstellen selbst haben

---

[7] Nähere Informationen über die Telekom-Control-Kommission, die einzelnen Zertifizierungsstellen und deren Angebote unter http://www.tkc.at.

[8] Über Vor- und Nachteile der hierarchischen Struktur: *Forgó*, Was sind und wozu dienen digitale Signaturen?, ecolex 1999, 235.

[9] Informationen über A-SIT unter: http://www.a-sit.at; Verfassungsrechtlich bedenklich scheint, dass die Verordnung gem § 19 Abs 4 SigG (vor der Novelle: § 19 Abs 3 SigG) *nur* auf Antrag der betreffenden Einrichtung erlassen werden kann, womit eine Bindung eines obersten Organes der Vollziehung im Raum steht. Dazu: *Schimak*, Ist § 19 Abs 3 Signaturgesetz verfassungskonform?, juridikum 2000, 185.

vorgegebene Zuverlässigkeits- und Sicherheitsanforderungen (§ 7 SigG) zu erfüllen.

3. Rechtsgrundlagen

3.1. Signaturrichtlinie[10]

Am 16. April 1997 verwies die Europäische Kommission in ihrer Mitteilung über eine „Europäische Initiative für den elektronischen Geschäftsverkehr" auf die elementare Bedeutung der elektronischen Signaturen für die Gewährleistung der Sicherheit und des Vertrauens im offenen Netz. Ein Jahr später, am 13. Mai 1998, wurde ein Richtlinienvorschlag über gemeinsame Rahmenbedingungen für elektronische Signaturen durch die Kommission vorgelegt. Das Ergebnis der danach folgenden Lesungen und eines gemeinsamen Standpunktes ist die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. Verkürzt dargestellt lassen sich die Grundsätze der RL wie folgt skizzieren:

- Technologieneutralität: Die RL geht von einem technologieneutralen Ansatz aus und spricht daher von elektronischen (nicht digitalen) Signaturen.
- Nichtdiskriminierung: Elektronische Signaturen dürfen nicht – etwa weil sie elektronisch sind und nicht handschriftlich – als rechtlich unbeachtlich qualifiziert werden. Weiters werden sog fortgeschrittene elektronische Signaturen (diese entsprechen den im SigG als sichere elektronische Signaturen bezeichneten Signaturen) in ihrer Rechtswirkung grundsätzlich der eigenhändigen Unterschrift gleichgestellt.
- Freier Marktzugang: Die Mitgliedsstaaten dürfen für die Aufnahme der Tätigkeit als Zertifizierungsstelle keine Lizenz vorsehen.
- Gegenseitige Anerkennung: Aufgrund der alltäglichen grenzüberschreitenden Transaktionen müssen Zertifikate innerhalb der EU ohne weitere Voraussetzungen sowie jene von Drittstaaten unter gewissen Bedingungen anerkannt werden.

---

[10] RL 1999/93/EG; dazu: *Schlechter*, Ein gemeinschaftlicher Rahmen für elektronische Signaturen, in: *Schweighofer/Menzel*, E-Commerce und E-Government (2000) 35.

3.2. Signaturgesetz[11]

Durch dieses Gesetz hat Österreich die Richtlinie noch vor deren Inkrafttreten umgesetzt. Man konnte sich bis zur Beschlussfassung an dem Richtlinienentwurf orientieren und hat somit weitgehend den Verpflichtungen aus der späteren Richtlinie entsprochen. Letzte Änderungen und redaktionelle Anpassungen wurden innerhalb der Umsetzungsfrist durch die Novelle zum SigG[12] vorgenommen. Staaten, die schon seit längerem über ein Signaturgesetz verfügen, wie die BRD und Italien, mussten bzw müssen einige Gesetzesanpassungen durchführen[13]. Das SigG übernimmt weitgehend die Grundgedanken der Richtlinie. Das Gesetz regelt ua:

- die Zulassung und die Nichtdiskriminierung von elektronischen Signaturen im Geschäfts- und Rechtsverkehr (§ 3 SigG),
- die weitgehende Gleichstellung der sicheren elektronischen Signatur mit der eigenhändigen Unterschrift (§ 4 SigG),
- ein Aufsichtssystem über Zertifizierungseinrichtungen und ein System der freiwilligen Akkreditierung (§§ 13-17 SigG),
- Haftungsregelungen für Zertifizierungseinrichtungen[14] (§ 23 SigG),
- und die Voraussetzungen der Anerkennung ausländischer elektronischer Signaturen (§ 24 SigG).

3.3. Signaturverordnung[15]

Gem § 25 SigG hat der Bundeskanzler im Einvernehmen mit dem Bundesminister für Justiz die für die Durchführung des SigG erforderlichen Vorschriften zu erlassen. Die SigV regelt unter anderem die Höhe pauschaler Entgelte für die Aufsichtstätigkeiten, die finanziellen und personellen Anforderungen an die Zertifizierungsdiensteanbieter und

---

[11] BGBl I 1999/190, idF BGBl I 2000/137; Kommentarliteratur: *Brenn*, Signaturgesetz.

[12] BGBl I 2000/137; dazu *Thaler*, Endlich erste Novelle zum SignaturG!, ecolex 2000, 862.

[13] Überblick und links zur Situation in anderen Rechtsordnungen: *Van der Hof*, Digital Signature Law Survey, http://rechten.kub.nl/simone/ds-lawsu.htm.

[14] Ausführlich dazu: *Menzel*, Haftung von Zertifizierungsdiensteanbietern, in: *Schweighofer/Menzel*, E-Commerce und E-Government (2000) 55.

[15] BGBl II 2000/30; Kommentarliteratur: *Brenn/Posch*, Signaturverordnung, 2000.

die erforderlichen Maßstäbe technischer Komponenten und Verfahren der Aufsichtsstelle und Zertifizierungsdiensteanbieter von qualifizierten Zertifikaten. Weiters normiert die Verordnung die näheren Umstände der Prüfung der technischen Komponenten und Verfahren durch die Bestätigungsstellen und legt die betriebsorganisatorischen Abläufe für die Erbringung vertrauenswürdiger Signatur- und Zertifizierungsdienste fest, wozu auch Regelungen über die Gültigkeitsdauer qualifizierter Zertifikate, die näheren Umstände der Ausstellung dieser, die Vorgangsweise beim Nachsignieren und Bestimmungen über Verzeichnis- und Widerrufsdienste gehören.

Im Bezug auf die Bestimmungen über die finanziellen Anforderungen an die Zertifizierungsdiensteanbieter wird kritisiert[16], dass staatliche Anbieter gegenüber nichtstaatlichen Mitbewerbern bevorrechtet werden. Grundsätzlich müssen nach § 2 SigV die Anbieter qualifizierter Zertifikate ein Mindestkapital von 300.000,- Euro und als Haftungsfonds eine Mindestversicherungssumme von 1 Million Euro der Aufsichtsstelle nachweisen. Doch § 2 Abs 3 SigV nimmt Bund, Länder, Gemeindeverbände und Ortsgemeinden mit nicht mehr als 50.000 Einwohnern von diesem Nachweis aus.

4. Rechtswirkungen der elektronischen Signatur

4.1. Allgemeine Wirkung

Der in § 3 SigG verwirklichte Grundsatz der Nichtdiskriminierung spricht jeder Form von elektronischer Signatur eine „allgemeine Rechtswirkung" zu. Signaturen sind somit kraft Gesetz rechtlich existent. Ihr völliger Ausschluss aus dem Geschäftsverkehr ist nicht mehr möglich. Auch als Beweismittel dürfen diese nicht ausgeschlossen werden.

4.2. Besondere Rechtswirkung der sicheren elektronischen Signatur

§ 4 SigG fingiert für sichere elektronische Signaturen (siehe 2.1.) Schriftlichkeit iSd § 886 ABGB. Diese Form der Signatur entfaltet somit die selbe Rechtswirkung wie die eigenhändige Unterschrift. Damit diese Fiktion aber keinen Mangel an Schutz bedeutet, muss die sichere

---

[16] *Mayer-Schönberger*, Bedauerlich: Signatur-Dienstleister nach der SigV, ecolex 2000, 130.

elektronische Signatur auch die besonderen Zwecke der Unterschrift – nämlich einerseits Identitätsfunktion und Identifizierungsfunktion und andererseits auch die allgemeinen Gründe für Formvorschriften wie zB Schutz vor Übereilung – erfüllen. § 2 Z 3 lit e SigG verlangt, dass die Signatur auf einem qualifizierten Zertifikat beruht. Dadurch ist die Identität sicherstmöglich festgestellt. Die Identifizierung des Signators mit dem Inhalt des unterzeichneten Textes soll vor allem dadurch gewährleistet sein, dass der Zertifizierungsdiensteanbieter nach § 20 Abs 3 SigG den Zertifikatswerber über die möglichen Rechtswirkungen des Signaturverfahrens zu belehren hat. Weiters ist gem § 4 Abs 3 SigG die Bestimmung des § 294 ZPO (Vermutung der Echtheit des Inhaltes einer unterschriebenen Privaturkunde) auch auf sichere elektronische Signaturen anzuwenden[17].

4.3. Ausnahmen

In § 4 Abs 2 SigG werden folgende Bereiche von der Rechtswirkung iSd § 886 ABGB ausgenommen:

- Z 1: Formgebundene Rechtsgeschäfte des Familien- und Erbrechts
  Die Rechtfertigung[18] der Ausnahme liegt in der besonderen Sensibilität dieser Bereiche, da diese häufig vermögensrechtliche Belange besonders schutzbedürftiger Personen betreffen.
- Z 2: Willenserklärungen und Rechtsgeschäfte, die einer öffentlichen Form bedürfen
  Soweit davon auch bloße Beglaubigungen von Unterschriften erfasst sind, scheint diese Bestimmung über den Normzweck hinauszugehen. Diese Ausnahme steht nicht im Einklang mit dem Artikel 9 Abs 2 lit b der E-Commerce-RL[19].
- Z 3: Willenserklärungen, Rechtsgeschäfte und Eingaben, die zur Eintragung in ein öffentliches Register einer öffentlichen Form bedürfen
- Z 4: Bürgschaftserklärungen

---

[17] Hier wäre eine widerlegbare Vermutung der Echtheit wünschenswert. Dazu: *Schumacher*, Sichere Signaturen im Beweisrecht, ecolex 2000, 860.

[18] Sowohl zur Begründung der Ausnahme der Z 1 als auch der Weiteren siehe EB zu § 4 Abs 2 SigG.

[19] Dazu: *Huemer*, Bundesgesetz über elektronische Signaturen, AnwBl 1999, 392.

Die letztere Ausnahme wurde bereits von mehreren Seiten kritisiert[20]. Die Begründung in den EB stellt auf die besondere Warnfunktion der eigenhändigen Unterschrift ab, die die Gefahren und Nachteile verstärkt vor Augen führen soll. Es wird also davon ausgegangen, dass der Bürge durch eigenhändige Unterschrift zu einer gründlicheren Überlegung angehalten wird, als durch elektronische Signierung. Doch ist die Vornahme der elektronischen Signierung zweifellos aufwändiger als die eigenhändige Unterfertigung und außerdem müsste der Signator über die Rechtswirkungen von elektronischen Signaturen durch den Zertifizierungsdiensteanbieter gem § 20 Abs 3 SigG gesondert belehrt worden sein.

5. Verbraucherschutz- und finanzrechtliche Aspekte

Nachdem das SigG seit mittlerweile über einem Jahr in Geltung steht, haben sich schon einige Detailfragen eröffnet, worüber im Folgenden ein kurzer Überblick gewährt werden soll.

Der Gesetzgeber hat durch das SigG die Möglichkeit geschaffen, zahlreiche gesetzliche Formvorschriften nicht nur in Papierform durch Leistung einer eigenhändigen Unterschrift sondern auch durch elektronische Dokumente mit sicherer elektronischer Signatur zu erfüllen. Durch diese Wahlmöglichkeit stellt sich die Frage, ob der ausschließliche Einsatz sicherer elektronischer Signaturen als formwahrend wirksam vereinbart werden kann[21]. Vor allem könnte § 6 Abs 1 Z 4 KSchG einer solchen Vereinbarung entgegenstehen, obwohl dieser nur gewillkürte Formerfordernisse für ansonsten formlose Erklärungen erfasst. Als gewillkürte Form wäre eine Verpflichtung zum Einsatz elektronischer Signaturen auf jeden Fall als zu streng zu werten, da dies einhellig schon bei Telegramm, Telefax und eingeschriebenem Brief angenommen wird. Doch scheint dieses Verbot auch im Zusammenhang mit der Auswahl

---

[20] So: *Jud/Högler-Pracher*, Die Gleichsetzung elektronischer Signaturen mit der eigenhändigen Unterschrift, ecolex 1999, 610; *Forgó*, Sicher ist sicher? – das Signaturgesetz, ecolex, 1999, 607; Weiters eröffnet sich durch diese Ausnahme die Frage, ob der Bereich der Sicherungsgarantie – der OGH hat sich nun der Auffassung angeschlossen, dass für diese die Bürgschaftsform gelten soll (siehe *Koziol/Welser*, Bürgerliches Recht II[11], 135 mwN) – auch von der Schriftlichkeitsfiktion des § 4 Abs 1 SigG ausgenommen werden soll.

[21] Unter anderem auch dazu: *Vonkilch*, Der Einsatz elektronischer Signaturen aus versicherungs- und verbraucherschutzrechtlicher Perspektive, VR 2001, 25.

zwischen mehreren Möglichkeiten zur Erfüllung gesetzlicher Formvorschriften anwendbar. Denn eine Vereinbarung des obligatorischen Einsatzes einer bei weitem aufwendigeren Übermittlungsform dürfte sich iSd § 6 Abs 1 Z 4 KSchG verbieten, wenn zur Wahrung der gesetzlichen Form gem § 886 ABGB bloße Unterschrift genügen würde. Dies sollte wohl auch für die Verpflichtung gelten, Empfangsvorrichtungen für den Eingang von E-Mails, die mit sicherer elektronischer Signatur versehen sind, bereit halten zu müssen.

Im Bereich Finanzrecht liegt ua die Frage nahe, ob der Abschluss von gebührenpflichtigen Rechtsgeschäften durch elektronisch signierte E-Mails eine Gebührenschuld nach dem Gebührengesetz auslöst. Da aber eine elektronische Nachricht kein Schriftstück iSd Gebührengesetzes darstellt, wird eine Gebührenschuld aufgrund eines elektronischen Dokumentes grundsätzlich zu verneinen sein[22]. Auch für den Vorsteuerabzug scheint das Signaturrecht neue Möglichkeiten zu eröffnen. Obwohl nach der derzeitigen Meinung des BMF und der Judikatur des VwGH als Rechnung iSd § 11 UStG immer nur ein Schriftstück (Papier) verstanden werden kann, soll die Verwendung sicherer elektronischer Signaturen eine neue Betrachtungsweise erlauben[23]. Zumindest befürwortet die europäische Kommission in einem Richtlinienvorschlag[24] den Einsatz und die Anerkennung von elektronischen Rechnungen in Verbindung mit elektronischen Signaturen für MwSt-Zwecke.

6. Anwendungsbereiche

Hier soll nur ein kurzer Überblick über die zahlreichen tatsächlichen und möglichen Anwendungsbereiche der elektronischen Signatur gegeben werden. Aufgrund der Unsicherheit über Integrität und Authentizität elektronischer Daten wurde das Internet im rechtsgeschäftlichen Bereich bisher überwiegend nur zum Informationsaustausch verwendet. Nun bietet aber die elektronische Signatur aufgrund ihrer Eigenschaften für

---

[22] Dazu: *Walzel*, Signaturgesetz und gebührenrechtliche Unterschrift, SWK 2001, S 256; *Lang*, Elektronisch signierte E-Mails und Gebührenschuld, SWK 2000, S 441.

[23] So: *Kutschera*, Berechtigt eine „elektronische Rechnung" zum Vorsteuerabzug?, SWK 2000, S 32; *Lang*, Rechnungen im E-Commerce, SWK 2000, S 353.

[24] Vorschlag für eine Richtlinie des Rates zur Änderung der Richtlinie 77/388/EWG mit dem Ziel der Vereinfachung, Modernisierung und Harmonisierung der mehrwertsteuerlichen Anforderungen an die Rechnungstellung, Dokument 500PC0650.

den Vertragsabschluss über Internet nicht nur ausreichende Sicherheit, sondern es erfolgt zusätzlich aufgrund eines Zeitstempels iSd § 2 Z 12 SigG eine Bestätigung darüber, dass bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Dies wäre zB bei der Abwicklung von Börsengeschäften hilfreich.

Die Identifikationsfunktion der elektronischen Signatur könnte auch zu reinen Legitimationszwecken verwendet werden und PIN/TAN-Kundennummern ablösen, was im Bereich des Mobilfunk-Banking bereits diskutiert wird.[25] Für das Immaterialgüterrecht bedeutet diese Zuordnungsfunktion die Möglichkeit, die Verbindung zwischen Werk und Verwertungsbefugtem sicherzustellen und, durch Aufbau von sog Copyright-Management-Systemen, Transaktionskosten zu senken.[26] Weiters könnte man von der Nutzung von Standleitungen Abstand nehmen, da abgeschirmte Datenleitungen aufgrund der Echtheits- und Unverfälschtheitsgarantie der elektronischen Signatur nicht mehr notwendig wären.

Vor allem im E-Government wird der elektronischen Signatur eine große Bedeutung vorhergesagt. Verschiedene Dienste sind schon seit längerem über Internet verfügbar wie zB Firmenbuch und Grundbuch. Auch verkehren die Behörden untereinander schon verstärkt über Internet. Aufgrund der Sicherheit über Absenderdaten und unverfälschten Inhalt könnten viele Behördenwege und innerbehördliche Korrespondenzen vereinfacht werden. So könnte zB bei FINANZ*Online*[27], dem hauptsächlichen Kommunikationsmedium zwischen Finanzverwaltung und Wirtschaftstreuhändern, die erforderliche Identifizierung viel einfacher als bisher, nämlich durch elektronische Signatur, erfolgen. Derzeit wird dies durch Abgleich der von den Kammern mitgeteilten Informationen mit den bei der Abgabenbehörde gespeicherten Personendaten des Teilnehmers erreicht.

Auch bei der im Moment viel diskutierten Bürgerkarte[28] wird an den Einsatz von elektronischen Signaturen gedacht. Hier soll neben der

---

[25] *Gerpott/Knüfermann*, Mobilfunk-Banking Eine neue Variante des Tele-Banking, ÖBA 2000, 956.

[26] Ua auch dazu: *Mayer-Schönberger*, Das Immaterialgüterrecht in der Informationsgesellschaft – Ein Essay, ÖBl 2000, 51.

[27] Allgemein dazu: *Weninger*, FINANZ*Online* in der zweiten Ausbaustufe, ÖstZ 2000/699.

[28] Umfassende Informationen unter: http://www.buergerkarte.at; siehe auch den Beitrag von *Posch* in diesem Band.

Sozialversicherungskartenfunktion ein zusätzlicher Speicherplatz für andere Dokumente elektronischer Form zur Verfügung stehen, dessen Inhalt mit elektronischer Signatur vor Veränderungen und Fälschungen geschützt werden soll.

Sogar bei den Rechtsinformationssystemen wird ein potenzieller Anwendungsbereich gesehen. So hat sich der deutsche Bundesverfassungsgerichtshof bereits entschieden, um auch bei der Internetveröffentlichung höchste Verlässlichkeit zu bieten, seine neuesten Entscheidungen durch elektronische Signatur zu authentifizieren.

7. Abschließende Bemerkung

Um die Errungenschaften der Technik möglichst erfolgreich und gewinnbringend ausnützen zu können, muss die Manipulationsmöglichkeit elektronischer Daten ausgeschaltet werden, müssen „sicheren" elektronischen Dokumenten gewisse Rechtswirkungen zuerkannt werden und vor allem muss Rechtssicherheit gewährleistet sein. Diese Ziele verfolgen die Regelungen zur elektronischen Signatur. Doch stellt das Signaturgesetz nicht nur einen großen Schritt zur Weiterentwicklung des elektronischen Rechtsverkehres dar. Es werden dadurch Grundlagen für einen neuen Dienstleistungssektor geschaffen, was auch positive Effekte auf die Beschäftigung und den Wirtschaftsstandort Österreich erwarten lässt. Die Europäische Kommission rechnet in den nächsten Jahren mit 500.000 neu geschaffenen Arbeitsplätzen im Zusammenhang mit dem elektronischen Geschäftsverkehr[29]. Ebenso eröffnen sich für die rechtsberatenden Berufe neue Möglichkeiten und Betätigungsfelder.

---

[29] *Brenn*, Signaturgesetz, 36.