Lutz Gollan, Christoph Meinel:
Elektronische Signaturen - eine amerikanische und europäische Perspektive
in Proceedings of the 7th Deutsche IT-Sicherheitskongress des BSI (BSI 2001), SecuMedia Press, Bonn, Germany, pp. 97-112, 5, 2001.

Elektronische Signaturen

– Eine amerikanische und europäische Perspektive -[1]

Lutz Gollan, Christoph Meinel[2]

Kurzfassung:

Der Beitrag stellt die verschiedenen gesetzlichen Ansätze der Rechtskreise der USA und der Europäischen Union sowie für letzteren beispielhaft die Gesetze der Bundesrepublik Deutschland zur Regelung und Förderung des Einsatzes elektronischer Signaturen vor. Neben den technischen Belangen der einzelnen Vorschriften werden die juristischen Anforderungen und die praktischen Auswirkungen der unterschiedlichen Herangehensweisen hinsichtlich des zukünftigen geschäftsmäßigen Einsatzes elektronischer Unterschriften kritisch beleuchtet.

Stichwörter: Elektronische Unterschriften, digitale Signaturen, E-Sign, EU-Richtlinie, SigG 2001, Akzeptanz, Haftung

Abstract:

This article introduces different legal approaches implemented for the regulation and promotion of electronic signatures by the American and European Union justice systems, the latter exemplified by the according German regulations. In addition to the technical requirements for the varying methods, the legal requirements, as well as the repercussions in their application, will be critically illustrated, keeping in regard the future marketable usage of electronic signatures.

Key-words: Electronic signatures, digital signatures, E-Sign, EC-Directive, SigG 2001, Acceptance, Liability

1. Einleitung

In jüngster Zeit wurden sowohl in den USA als auch in Europa Gesetze verabschiedet, die durch eine Gleichstellung sogenannter „elektronischer Signaturen[3]“ mit handschriftlichen Unterschriften den Weg für den rechtsverbindlichen E-Commerce ebnen sollen. Die EU-Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Si-

---

[1] Veröffentlicht in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): 2001-Odysee im Cyberspace, Ingelheim 2001, 97- 112.

[2] Institut für Telematik, Trier.

[3] Im folgenden ist die “elektronische Signatur” der Oberbegriff und beinhaltet die “digitale Signatur”, welche eine Gruppe von Protokollen bezeichnet, die auf asymmetrischen Verschlüsselungsverfahren beruhen und die Authentifizierung und Integrität elektronisch signierter Daten sicherstellen, vgl. AALBERTS, VAN DER HOF 1999; die hier besprochenen Vorschriften befassen sich ausschließlich mit dem elektronischen Signieren von Daten, nicht mit deren Verschlüsselung. Signierte Daten sind nicht notwendigerweise verschlüsselt, sie sind daher grundsätzlich frei lesbar.

Signaturen vom 13. Dezember 1999 und das entsprechende US-Bundesgesetz, verbreitet als “E-Sign” bezeichnet, beziehen hierbei unterschiedliche Positionen bezüglich der Anwendung der elektronischen Gegenstücke zu den herkömmlichen Unterschriften aus “Papier-und-Tinte” (und auch aus Kohle, wie weiter unten dargelegt wird). Dabei reflektiert das US-Gesetz die Technik-Neutralität des amerikanischen Ansatzes, während das deutsche Signaturgesetz 2001, das hier als nationales Umsetzungsgesetz der Richtlinie ebenfalls untersucht wird[4], nur bestimmte Zertifikate, die von einem (qualifizierten) Zertifizierungsdiensteanbieter ausgegeben werden, als Grundlage für die Gleichstellung elektronischer Signaturen mit herkömmlichen Unterschriften im Rahmen der gesetzlichen Formerfordernisse anerkennt.

Dieser Aufsatz beschreibt die Gemeinsamkeiten und Unterschiede bezüglich verschiedener Gesichtspunkte der US-amerikanischen, europäischen und deutschen Gesetze. Die jeweiligen technischen und rechtlichen Aspekte werden hierbei gleichgewichtet betrachtet. Innerhalb der juristischen Abschnitte wird die Frage der Haftung für elektronische Signaturen näher beleuchtet. Während die technische Sicherheit eine der herausragenden Säulen für das Vertrauen in die elektronischen Signaturen darstellt, ist anzunehmen, dass deren allgemeine Akzeptanz durch eine sorgfältig ausgearbeitete Haftungsstruktur seitens Anbieter und Nutzer gefördert wird.

2. US Electronic Signatures in Global and National Commerce Act

Am 30 Juni 2000 unterzeichnete der frühere Präsident der USA Bill Clinton „E-Sign“, den "Electronic Signatures in Global and National Commerce Act"[5]. Dieser trat weitestgehend am 01. Oktober 2000 in Kraft. Das Bundesgesetz soll den Gebrauch von elektronischen Unterschriften im Handel zwischen den einzelnen Bundesstaaten und dem Ausland erleichtern, indem es Rechtssicherheit für das Verwenden der elektronischen Signaturen schafft[6].

Dieses Gesetz ist nicht die erste US-amerikanische Vorschrift auf dem Gebiet der elektronischen Signaturen. Verschiedene Gesetze einzelner Bundesstaaten, wie z.B. der Utah Digital Signature Act (1995) oder der Washington Electronic Authentication Act (1996), wurden schon weit früher erlassen. Mittlerweile haben 46 Bundesstaaten Regelungen zur Wirksamkeit elektronischer Signaturen erlassen[7]. Gleichwohl bestand die Mehrzahl der Anwendungen, die auf elektronische Anwendungen zurückgreifen, noch im Jahr 1998 aus Server-Authentisierungs-Mechanismen, nicht etwa aus der eigentlichen Zielgruppe der sogenannten „Stranger-to-Stranger-Kommunikation“[8].

---

[4] EU-Richtlinien bilden grundsätzlich nur einen Rahmen für die Umsetzung der jeweiligen gesetzlichen Normen der Mitgliedsländer der EU, daher sind Abweichungen vom deutschen Ansatz in den Nachbarstaaten denkbar. Das deutsche Signaturgesetz dient hier nur als Beispiel für eine Möglichkeit der Umsetzung der Richtlinie.

[5] Pub.L. 106-229,114 Stat. 464 (2000).

[6] vgl. White House Presseerklärung vom 30.06.2000 <http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/2000/7/3/5.text.2> am 04.01.2001.

[7] ZOELLICK 2000, 2; vgl. im Einzelnen MIEDBRODT 1998.

[8] MIEDBRODT 1998, 198.

Der Grund für die Verabschiedung eines entsprechenden Bundesgesetz erst im Jahr 2000, fünf Jahre nach dem Utah Act, beruht vornehmlich darauf, dass es kein einheitliches Vertragsrecht in den USA gibt, für das die elektronischen Unterschriften grundsätzlich von Belang sind. Vielmehr verfügen die Bundesstaaten über unterschiedliche Vertragsrechtsregelungen. Mittlerweile haben jedoch die meisten der Staaten ein *einheitliches* Vertragsrecht geschaffen, das an den Uniform Commercial Code (U.C.C.)[9] angelehnt ist. Dieser dient als Modellgesetz, so dass im Laufe der Jahre auch ein einheitliches Signaturgesetz sinnvoll wurde.

Mit der Internationalisierung des Handels und des Wachstums des Internets wurde der US-Regierung bewusst, dass die international und über die Bundesstaatengrenzen hinaus agierenden Unternehmen einheitliche und verlässliche Regeln zur elektronischen Unterschrift benötigen. E-Sign als Bundesgesetz soll diese (bundes-) staatenübergreifend liefern[10].

2.1. Technologische Aspekte

E-Sign verlangt keine bestimmte Technologie für den Einsatz elektronischer Signaturen, sondern überlässt dies der Entwicklung im Markt. Da das Gesetz weder auf die Voraussetzungen für den Widerruf einer geleisteten elektronischen Signatur noch auf andere für die Authentisierung des Absenders belangreiche Momente eingeht, muss das Gesetz hierzu auch nicht Stellung beziehen. Im übrigen ist E-Sign mit den bisherigen, herkömmlichen Regeln in Bezug auf die Definition, was eine Unterschrift eigentlich ist, vergleichbar.

In den Definitionen unterscheidet der Uniform Commercial Code zwischen den „Unterschriftsanforderungen"[11] und den „Schriftformanforderungen"[12] als Voraussetzungen für einen gültigen und durchsetzbaren Vertrag. Diese Differenzierung ist für das Verständnis der weiten Definition der Bestandteile einer elektronischen Signatur, wie sie E-Sign beinhaltet, von herausragender Bedeutung. Nach der Definition im U.C.C.[13] besteht eine Unterschrift aus jeglichem Symbol, das mit dem Willen zur Unterzeichung von einer Person angewendet wird. Die Unterschriftsanforderungen sind daher sehr offen und in der rechtlichen und gesellschaftlichen Geschichte der USA begründet. In der Fortführung dieser Tradition, und um die Akzeptanz des elektronischen Äquivalents zum Kohle-X zu steigern, findet sich eine ähnliche weite Definition zur (nun: elektronischen) Signatur in sec. 105 § 6 E-Sign, wo es heißt, dass hiermit jeder elektronische Klang, jedes elektronische Symbol oder jeder elektronische Prozess, der mit einem Vertrag oder einer anderen Willenserklärung verbunden oder assoziiert ist und von einer Person mit dem Willen zur Unterzeichnung der Willenserklärung angebracht wird, gemeint ist. GREENWOOD stellt daher fest, dass das "archetypische Wild-West-Szenario des Cowboys, der ein X mit einem

---

[9] vgl. <http://janus.state.me.us/legis/statutes/11/title11ch00sec0.html> am 04.01.2001.

[10] s. Fußnote 4.

[11] § 1-201 (39) U.C.C., Quelle s.o.

[12] § 1-201 (46) U.C.C., Quelle s.o.

[13] § 1-201 (39) U.C.C., Quelle s.o.

Stück Kohle macht, nicht fiktiv ist"[14], sondern auch heute noch bei den modernen Geschäftstransaktionen vorstellbar ist.

Neben dem Fehlen der Vorgabe von technischen Standards zur wirksamen und durchsetzbaren elektronischen Unterzeichnung schreibt E-Sign auch keinerlei technische *Infrastruktur* vor. Gemäß den Unterstützern von E-Sign dient das neue Bundesgesetz vornehmlich der Gleichstellung der elektronischen Unterschrift mit den herkömmlichen „Papier-und-Tinte"-Signaturen, und nicht der Förderung bestimmter Technologien[15]. Bundesstaatliche Abweichungen von E-Sign sind zwar auch weiterhin möglich[16], doch verlangt sec. 102 (a) (2) E-Sign bezüglich der Gültigkeit elektronisch signierter Verträge stets die strikte technische Neutralität der Ländergesetze.

2.2. Juristische Aspekte

2.2.1. Allgemeine Bemerkungen

E-Sign soll die Nutzung elektronischer Willenerklärungen und Unterschriften im zwischen-bundesstaatlichen und übernationalen Handel durch die Schaffung von Rechtssicherheit bei der Verwendung von digitalen Signaturen fördern[17]. Ebenso soll die Durchsetzbarkeit von elektronischen Dokumenten durch E-Sign erreicht werden[18]. Vor E-Sign waren nur Verträge und Willenserklärungen in herkömmlicher Schriftform rechtlich durchsetzbar[19].

E-Sign als Ergänzung des herkömmlichen Rechts im neuen digitalen Zeitalter verbietet dabei grundsätzlich abweichende bundesstaatliche Regelungen[20]. Die existierenden gesetzlichen Regelungen sind an das neue Gesetz anzupassen. Hierdurch wird u.a. die Vorgabe einer bestimmten technischen Form von elektronischen Unterschriften als Voraussetzung für deren Gültigkeit, wie z.B. noch im ursprünglichen Utah Act geregelt, ausgeschlossen[21]. Wenn sich gleichwohl ein Bundesstaat dafür entscheidet, bestimmte *Wirkungen*, die über die bloße Tatsache, dass nach E-Sign elektronisch signierte Verträge und Willenserklärungen ebenso wirksam sind wie die herkömmlichen, an bestimmte technische Anforderungen zu knüpfen, so wird dies von E-Sign nicht ausgeschlossen. Ein Beispiel für eine entsprechende Regelung lässt sich bei NIMMER 2000 finden. Dieser geht davon aus, dass ein Ländergesetz, nach dem nur dann eine elektronische Unterschrift nicht abstreitbar und der Unterzeichner hieran entsprechend gebunden sei, wenn sie mit einer

---

[14] GREENWOOD 2000.

[15] US-Repäsentant BLILEY, 146 Congressional Records H4352 am 14.06.2000.

[16] vgl. unten 2.2.1.

[17] s.o.

[18] sec. 102 (a) 2 E-Sign.

[19] MIEDBRODT 2000a, 543.

[20] sec. 102 (c) E-Sign.

[21] NIMMER 2000, 5.

bestimmten Technologie angefertigt wurde, nicht gegen das Bundesgesetz verstößt. Dass der Vertrag ursprünglich wirksam war, wir von dieser Regelung ja gerade nicht berührt.

Eine grundsätzliche Ausnahme zum Variationsverbot bietet jedoch sec. 102 (a) (1) E-Sign, wonach ein Bundesstaat von E-Sign abweichen darf, wenn er das Modellgesetz „Uniform Electronic Transactions Act (UETA)“ in sein Vertragsrecht inkorporiert hat. UETA kann nach diesem Paragrafen das Bundesgesetz modifizieren, beschränken oder erweitern. Diese Modellvorschriften zur Verwendung von elektronischen Unterschriften gelten allerdings nur dann, wenn die Parteien eines Vertrages sich auf die Möglichkeit des Einsatzes von elektronischen Unterschriften geeinigt haben[22]. UETA schreibt den Einsatz von elektronischen Signaturen nicht vor und regelt auch nicht die Konsequenzen von deren Verwendung[23]. Seit 1999 haben ca. 22 Bundesstaaten der USA das Modellgesetz übernommen[24].

2.2.2. Haftung

Da E-Sign keinerlei Anforderungen an die für elektronische Unterschriften einzusetzende Technik stellt oder den Aufbau einer bestimmten Infrastruktur im Sinne einer PKI für die Authentisierung des Verwenders verlangt, berührt das Gesetz konsequenterweise auch nicht Fragen Haftung beim Einsatz von elektronischen Signaturen. Während einzelne bundesstaatliche Gesetze, wie z.B. der Utah Act, den Verwender digitaler Signaturen bislang vollständig haftbar für den Einsatz der elektronischen Unterschrift machte, sieht das Bundesgesetz keine vergleichbare Regelung vor.

Dies könnte sich als Hindernis für den Gebrauch von elektronischen Signaturen herausstellen. Da es auf Basis von E-Sign völlig unklar ist, wer für den Missbrauch bzw. Sicherheitsmängel beim Einsatz elektronischer Unterschriften für einen daraus resultierenden Schaden verantwortlich ist, wenn diese beispielsweise betrügerisch verwendet wird, wird die Verbreitung der neuen Technologie im Geschäftsverkehr möglicherweise nur zögernd voranschreiten.

Nach ZOELLICK sind jedoch die sehr weiten Haftungsregelungen, wie z.B. im Utah Act, nicht notwendigerweise die Lösung des Problems[25]. Dieses Gesetz könnte aufgrund der umfassenden Haftung des Verwenders diesen eher abschrecken, als zum Einsatz elektronischer Signaturen animieren, da er die volle Verantwortung für jeglichen technischen Defekt und betrügerischen Einsatz seiner elektronischen Unterschrift trägt.

Während andere US-Gesetze beispielsweise beim Einsatz von Kreditkarten die Haftung des Karteninhabers bei Betrug durch einen Dritten auf $50 beschränken, wurde dem Inhaber einer elektronischen Signatur in Utah bislang vom Gesetzgeber keinerlei Haftungserleichterung im Form einer Höchstsummenbeschränkung zuteil. Da aber die technischen

---

[22] vgl. § 9405 sec. 2 in den Main Revised Statutes <http://janus.state.me.us/legis/statutes/10/title10sec9405.html> am 04.01.2001.

[23] GREENWOOD 2000.

[24] vgl. im Einzelnen FRY 2000 and GREENWOOD 2000; zu Maine s.o. FN 20.

[25] ZOELLICK 2000, 6.

Gegebenheiten nicht vollständig unter der Kontrolle des Unterzeichners liegen und aufgrund der Komplexität und Kompliziertheit der technischen Komponenten und Verfahren auch nicht von diesem vollständig beherrscht werden können, dürfte diese weite Regelung für den durchschnittlichen Anwender abschreckend, nicht motivierend sein.

ZOELLICK kommt daher zum Ergebnis, dass ein Anstieg des Einsatzes elektronischer Signaturen nach dem Inkrafttreten von E-Sign vornehmlich im B2B-Bereich zu verzeichnen sein wird, da dort Vertrauens- und Authentifikationsmechanismen zum Teil schon vorhanden sind und Haftungsfragen ohne weiteres zwischen Gleichberechtigten vertraglich geregelt werden[26]. Darüber hinaus argumentiert ZOELLICK, dass verschiedene Geschäftssysteme verschiedene, z.T. proprietäre Authentifikationsmechanismen in geschlossenen Benutzergruppen einsetzen werden. Nach ZOELLICK werden daher verschiedene Geschäftsbereiche verschieden digitale Signatursysteme bereitstellen[27]. Ein Beispiel für Deutschland ist der HBCI-Standard der Banken, der mit einer Public-Key-Verschlüsselung den Kontenzugriff von zu Hause nur mit der eigenen Bank ermöglicht[28].

2.2.3. Verbraucherschutz

Eine beachtliche Zahl der Regelungen in E-Sign beschäftigt sich mit dem Verbraucherschutz. Das Ziel von E-Sign ist neben den oben genannten Stimulationseffekten auch das Verhindern der Verringerung von Verbraucherrechten beim Einsatz der neuen Technologien. In der herkömmlichen schriftlichen Form verschiedener Verträge diente die Einhaltung der Schriftform auch dem Verbraucherschutz. Durch die Perpetuierung und das förmliche „Vor-Augen-Führen“ konnte die Bedeutung eines Vertrages stärker herausgestellt werden als in einer flüchtigen, beispielsweise mündlichen Form. Daneben werden durch eine Papier-Version eines Vertrages auch die Beweismöglichkeiten für den Vertragsinhalt erleichtert.

Das Gesetz unternimmt den Verbraucherschutz vornehmlich mit drei bedeutenden Vorschriften: Zum ersten soll er dadurch gewährleistet werden, dass der Verbraucher vor dem rechtsverbindlichen Erhalt von elektronischen Willenserklärungen sein Einverständnis hierzu elektronisch dem zukünftigen Vertragspartner mitteilt, um so seine entsprechende technische Kapazität und seine Bereitschaft zu zeigen[29]. Zum zweiten muss der Verbraucher die Möglichkeit haben, sein Einverständnis jederzeit widerrufen zu können, um etwaige Mitteilungen und Willenserklärungen zukünftig in Papierform erhalten zu können[30]. Hierfür können jedoch Gebühren verlangt werden.

Drittens können Willenserklärungen in bestimmten Bereichen nicht elektronisch abgegeben werden. Die entsprechenden Rechtsgebiete umfassen vornehmlich das Familien- und

---

[26] ZOELLICK 2000, 8.

[27] ZOELLICK 2000, 9.

[28] vgl. <http://www.hbci.de/index.html> am 04.01.2001.

[29] sec. 101 (c) 1 (B) (ii) E-Sign.

[30] sec. 101 (c) 1 (B) (i) (II) E-Sign.

Erbrecht oder Versorgungsverträge mit Wasser, Wärme, Elektrizität etc., und hier insbesondere die Kündigungen von laufenden Verträgen[31].

2.3. Auswirkungen

Während E-Sign grundsätzlich alle technischen Standards zum Signieren von elektronischen Daten erlaubt, ist fraglich, ob die geschäftsmäßigen Verwender, die sich an zum Teil strenge Verbraucherschutzregelungen nach diesem Gesetz halten müssen, den als förderungswürdig erachteten Einsatz von elektronischen Unterschriften entsprechend unterstützen werden. Die Frage der Haftung beim Einsatz elektronischer Unterschriften ist darüber hinaus für sowohl die gewerblichen Nutzer wie auch die Verbraucher von herausragender Bedeutung und dürfte noch zu bemerkenswerten Erscheinungen im Markt und auch vor den Gerichten führen.

Letztendlich dürfte von einer angemessenen Haftungsregelung die Verbreitung der elektronischen Unterschriften in großem Maße abhängen. Sollte eine Lösung ähnlich wie beim Einsatz von Kreditkarten mit einer großzügigen Haftungsbeschränkungen zumindest für den Verbraucher gefunden werden, würde dieser sicherlich öfter elektronisch seine Geschäfte tätigen.

3. EU-Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

Am 13. Dezember 1999 wurde die Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (EU-Richtlinie) verabschiedet. Der Zweck der Richtlinie ist nach deren offizieller Begründung die Förderung des Gebrauchs von elektronischen Signaturen und die Unterstützung von deren rechtlicher Anerkennung[32]. Die EU-Richtlinie muss bis zum 19. Juli 2001 jeweils in nationales Recht umgesetzt werden, den Anforderungen der Richtlinie widersprechende nationale Regelungen müssen angepasst werden.

Im Vergleich zu anderen EU-Richtlinien ist die hier besprochene verhältnismäßig detailliert. Grundsätzlich kann eine Richtlinie nur Rahmenbedingungen für einen bestimmten Regelungsbereich vorgeben, so wie es auch der Titel der Richtlinie hier vermuten lässt. Die Signaturrichtlinie geht jedoch über einen Rahmen hinaus. Neben den eigentlichen Artikeln enthält sie vier Anhänge, die zum Teil äußerst genau die Anforderungen an die technischen Komponenten und Verfahren vorschreiben. Diese beziehen sich u.a. auf die sogenannten qualifizierten Zertifikate (Anhang I), die entsprechenden Anbieter (Anhang II) sowie die „sichere Signaturerstellungseinheiten“ (Anhang III).

---

[31] sec. 103 (a), (b) E-Sign.

[32] Art. 1 EU-Richtlinie.

3.1. Technologische Aspekte

Die EU-Richtlinie unterscheidet drei verschiedene Arten von elektronischen Signaturen: (a) (einfache) elektronische Signaturen[33], (b) fortgeschrittene elektronische Signaturen[34], und (c) fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und von einer sicheren Signaturerstellungseinheit erstellt wurden[35]. Eine elektronische Signatur (a) können jegliche Daten in elektronischer Form sein, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen. Ein gutes Beispiel für eine solche Unterschrift ist die eingescannte händische Unterschrift durch ein Faxgerät.

An dieser Stelle zeigt sich schon ein erster erheblicher Unterschied zum amerikanischen E-Sign. Das Ziel der *Authentifikation* des Unterzeichners ist im US-Gesetz nicht geregelt. Der Unterzeichner, egal wer er oder sie ist, muss nur Daten unterzeichnen und dies auch wollen. Ob er oder sie später anhand der Signatur authentifiziert oder sogar identifiziert werden kann, ist hierbei unerheblich[36].

Die fortgeschrittene elektronische Signatur (b) verlangt die Zuordnung der Signatur zum Unterzeichner mit der Möglichkeit, diesen zu identifizieren. Hierzu reicht eine flache Public-Key-Infrastruktur, wie sie z.B. bei Pretty-Good-Privacy (PGP[37]) Verwendung findet. Ein sogenanntes qualifiziertes Zertifikat im Sinne von (c), auf dem eine fortgeschrittene Signatur (b) basieren kann, darf nur von einem Zertifizierungsdiensteanbieter ausgestellt werden, der die technischen Anforderungen, wie im Anhang II der EU-Richtlinie aufgeführt, erfüllt und zuverlässiges Personal zur Durchführung seiner angebotenen Dienste einsetzt. Als Zusatzqualifikation, quasi als vierte Signaturkategorie, kann sich der Zertifizierungsdiensteanbieter in den Mitgliedsstaaten der EU von der jeweiligen zuständigen nationalen Einrichtung akkreditieren lassen. Dieser strenge Prozess umfasst neben der Prüfung der eingesetzten technischen Komponenten auch die Kontrolle der eingesetzten Verfahren.

Im Unterschied zu E-Sign ist die EU-Richtlinie folglich nicht technikneutral. Zwar schreibt die Richtlinie nicht den Einsatz bestimmter Algorithmen oder gewisser Zertifikatsstandards vor, gleichwohl wird durch die Anhänge des Regelwerks deutlich, dass die Europäische Kommission einen anderen Standpunkt hinsichtlich der Gewährleistung der technischen und administrativen Sicherheit der elektronischen Signaturen einnimmt als die USA.

Obwohl die Richtlinie jegliche Art von elektronischen Unterschriften zulässt, wird nur die Benutzung der Signaturen nach (c), also jener, die auf Zertifikaten beruhen, die von sicheren Zertifizierungsdiensteanbietern unter Verwendung von sicheren Signaturerstellungs-

---

[33] Art. 2 (1) EU-Richtlinie.

[34] Art. 2 (2) EU-Richtlinie.

[35] Art. 5 (1) (a) EU-Richtlinie.

[36] vgl. GREENWOOD 2000.

[37] <http://www.pgp.com>

einheiten ausgestellt wurden, maßgeblich durch die Vorgabe von Sicherheitsanforderungen gefördert. Nur diese digitalen Signaturen müssen den Anforderungen entsprechen, die an die herkömmlichen handschriftlichen Unterschriften gestellt werden[38].

Der PGP-Standard mit seiner flachen Hierarchie und fehlenden Anbietern von Zertifikaten kann die von der Richtlinie geforderten *qualifizierten* Zertifikate mangels sicherer Zertifizierungsdiensteanbieter nicht liefern. Zwar verlangt die Richtlinie nicht den Aufbau nationaler Root-CAs, die qualifizierten Zertifikate müssen aber neben anderen Angaben auch die Signatur des ausstellenden Zertifizierungsdiensteanbieters enthalten[39], und diese wiederum müssen beispielsweise die erforderliche Zuverlässigkeit für die Bereitstellung von Zertifizierungsdiensten nachweisen und den Betrieb eines schnellen und sicheren Verzeichnisdienstes und eines sicheren und unverzüglichen Widerrufsdienstes für die ausgestellten Zertifikate gewährleisten, auch wenn sie sich gar nicht akkreditieren lassen wollen[40]. Darüber hinaus muss dieser Anbieter vor der Ausstellung des Zertifikats die Identität des Kunden überprüfen und die erhobenen Daten für eventuell später anfallende Überprüfungen speichern[41]. Die de-facto-Voraussetzung für ein Äquivalent einer elektronischen Signatur zur „Papier-und-Tinte"-Unterschrift ist daher die Existenz einer zertifikatbasierten PKI mit Zertifizierungsdiensteanbietern, die den Sicherheits- und Infrastrukturanforderungen der Richtlinie entsprechen.

3.2. Rechtliche Aspekte

3.2.1. Allgemeine Bemerkungen

Zweifellos kann festgestellt werden, dass das Ziel der Verbreitung des Gebrauchs von elektronischen Signaturen durch strenge Sicherheitsanforderungen gefördert wird, wenn das Vertrauen der Anwender in die Technik und die eingesetzten Verfahren gestärkt wird. Neben der Zulassung von bestimmten digitalen Signaturen parallel zur herkömmlichen Schriftform für bestimmte Rechtsgeschäfte ist auch die in der Richtlinie verlangte Anerkennung elektronischer Unterschriften als Beweismittel in Gerichtsverfahren hierzu förderlich.

Wie E-Sign billigt die Richtlinie diesen Unterschriften keinen bestimmten Beweiswert zu, es wird nur verlangt, *dass* elektronische Signaturen im Rechtsstreit vor Gericht als Beweismittel zulässig sind[42]. Die genaue Bedeutung der elektronischen Unterschrift in Gerichtsprozessen, egal ob es sich um Signaturen nach (a), (b) oder (c) handelt, wird vollständig den Mitgliedsstaaten unter Berücksichtigung der dortigen, zum Teil stark abweichenden, prozessualen Regelungen überlassen. Wenn daher ein Mitgliedsstaat elektronische Unterschriften zwar als Beweismittel zulässt, an diese aber nur eine sehr geringe

---

[38] Art. 5 (1) (a) EU-Richtlinie.

[39] Anhang I (h) EU-Richtlinie.

[40] Anhang II (a), (b) EU-Richtlinie.

[41] Anhang II (d), (i) EU-Richtlinie.

[42] Art. 5 I (b) EU-Richtlinie.

Beweiskraft knüpft, werden die Bemühungen der EU konterkariert. So kann beispielsweise in einem Staat die Beweislast für den Nachweis der Unverfälschtheit einer elektronischen Nachricht beim Unterzeichner liegen, während im Nachbarstaat der Empfänger die Verfälschung der E-Mail nachweisen muss.

3.2.2. Haftung

Ein weiterer bedeutsamer Unterschied zwischen der EU-Richtlinie und E-Sign ist die im Gegensatz zum US-Gesetz in Europa geregelte Frage der Haftung des Zertifizierungsdiensteanbieters. Unter bestimmten Voraussetzungen haftet dieser für Schäden, die durch den Gebrauch von qualifizierten Zertifikaten entstehen, auch gegenüber Dritten, die auf die Inhalte der Zertifikate vertrauen[43]. Dies dürfte geeignet sein, den Gebrauch von entsprechenden Zertifikaten zu unterstützen. Sowohl der Verwender als auch der Empfänger können in diesen Fällen davon ausgehen, dass eine zumindest teilweise Kompensation von Schäden erfolgt, wenn beispielsweise der Zertifizierungsdiensteanbieter gleichwohl eine unsichere Technik einsetzt, um die Zertifikate zu erzeugen oder abrufbar zu halten. Eine Mindestversicherungssumme wird jedoch von der Richtlinie nicht vorgeschrieben.

3.3. Auswirkungen

Die EU-Richtlinie dürfte aufgrund der technischen Anforderungen ein beachtliches Vertrauen der Verwender und Empfänger in ein mit einer (c)-Signatur unterzeichnetes Dokument bewirken. Durch die Notwendigkeit sicherer technischer Komponenten, Verfahren und den Einsatz geschulten und verlässlichen Personals kann von einer Mindestsicherheit der entsprechenden elektronischen Signaturen ausgegangen werden. Den sicher signierten Dokumenten wird aber durch die Richtlinie kein besonderer rechtlicher (Beweis-) Wert zuteil. Die Mitgliedsstaaten der EU müssen bei der Umsetzung der Richtlinie in nationales Recht lediglich sicherstellen, dass die (c)-Signaturen die rechtlichen Anforderungen an eine Unterschrift in bezug auf in elektronischer Form vorliegende Daten in gleicher Weise erfüllen wie handschriftliche Unterschriften in bezug auf Daten, die auf Papier vorliegen, und in Gerichtsverfahren als Beweismittel zugelassen werden[44].

Durch die Richtlinie wird daher nicht gewährleistet, dass diese Unterschriften in den Mitgliedsstaaten gleich behandelt und vor einem Gericht gleich bewertet werden. Die Anwender im übernationalen Geschäftsverkehr können folglich nicht von einer einheitlichen Bewertung ihrer Rechtsgeschäfte ausgehen. Es ist daher zu erwarten, dass es in den verschiedenen Ländern Europas nicht nur wegen der infrastrukturellen Unterschiede, sondern auch aufgrund des unterschiedlichen Prozessrechts zu unterschiedlichen Akzeptanzraten der elektronischen Unterschriften kommen wird.

---

[43] Art. 6 EU-Richtlinie.

[44] Art. 5 (1) (b) EU-Richtlinie.

4. Deutsche Umsetzungsgesetze

Die Übertragung der EU-Richtlinie in nationales Recht wird in Deutschland im wesentlichen durch drei Gesetze geregelt: durch das Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (SigG 2001)[45], die Signaturverordnung 2001 (SigVO 2001) und das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr (AnpassungsG 2001), die sich allerdings noch alle im Gesetz- bzw. Verordnungsgebungsverfahren befinden. Eine Verabschiedung der Vorschriften wird voraussichtlich im Frühsommer 2001 erfolgen.

Die beiden erstgenannten Regelwerke haben Vorgänger aus dem Jahr 1997. Es handelte sich um die ersten Vorschriften dieser Art in Europa, die für zwei Jahre als eine Art Pilotprojekt gedacht waren. Die Erfahrungen mit den Vorschriften wurden genutzt, um die neuen Regelungen vorzubereiten. Das SigG und die SigVO regeln die technischen, personellen und infrastrukturellen Vorgaben, die Frage der Beweiskraft elektronischer Unterschriften und die Anpassung der zivilrechtlichen Formvorschriften wird durch das AnpassungsG 2001 adressiert.

4.1. Technologische Aspekte

Wie von der EU-Richtlinie vorgegeben und oben geschildert, unterscheidet das SigG 2001 drei Formen der elektronischen Signaturen: (a) elektronische Signaturen[46], (b) fortgeschrittene elektronische Signaturen[47], und (c) fortgeschrittene elektronische Signaturen, die zum Zeitpunkt ihrer Erzeugung auf einem gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt wurden, (qualifizierte elektronische Signaturen)[48]. Bezüglich der qualifizierten *Zertifikate* kann auf die obigen Ausführungen unter 3.1. verwiesen werden. Zertifizierungsdiensteanbieter können per Akkreditierung durch die Regulierungsbehörde für Telekommunikation und Post (RegTP[49]), ein Gütesiegel für staatliche überprüfte Sicherheit erhalten. Im übrigen müssen die Anbieter von qualifizierten Zertifikaten ihre Tätigkeit der RegTP unaufgefordert anzeigen und ihre personelle, technische und verfahrensbezogene Sicherheit und Übereinstimmung mit dem SigG 2001 und der SigVO 2001 nachweisen. Dies war nach SigG 1997 sogar die Voraussetzung für das Anbieten entsprechender Dienste nach dem Gesetz. Die entsprechende Akkreditierung hatten bis Januar 2001 lediglich drei Anbieter beantragt und erhalten: Telesec[50], Signtrust[51], und die deutsche Notarkammer, die allerdings auf die Technik und in weiten Teilen die Infrastruktur von Signtrust zurückgreift[52].

---

[45] Die folgenden Ausführungen beziehen sich auf den Gesetzentwurf vom 16.08.2000, der in erster Lesung im Bundestag verabschiedet wurde.

[46] § 1 Nr. 1 SigG 2001.

[47] § 1 Nr. 2 SigG 2001.

[48] § 1 Nr. 3 SigG 2001.

[49] <http://www.regtp.de>

[50] <http://www.telesec.de>

Die deutschen Regelungen definieren keine bestimmten technischen Vorgaben für die Zertifizierungsdiensteanbieter. Durch die Forderung nach anspruchsvollen Technologien, die hohen Sicherheitsstandards (nach ITSEC und Common Criteria) genügen müssen, die Notwendigkeit von PKIs mit zuverlässigen Zertifizierungsdiensteanbietern und die Komplexität der Verfahrensabläufe von der Identifizierung der Kunden bis zur mehrjährigen Online-Verfügbarkeit von abgelaufenen oder widerrufenen Zertifikaten in entsprechenden Verzeichnissen, soll jedoch eine anspruchsvolle Sicherheit erreicht werden, die über die herkömmlichen Standards, wie z.B. PGP, hinausgeht und so – ob gewollt oder ungewollt - die einsetzbaren Techniken einschränkt.

4.2. Rechtliche Aspekte

Das SigG 2001 soll die Nutzung des elektronischen Äquivalents zur händischen Unterschrift auf papiergebundene Willenserklärungen ermöglichen. Nach geltendem Recht (§ 126 Abs.1 Bürgerliches Gesetzbuch) entsprechen bislang nur die zuletzt genannten Unterschriften dem Schrifterfordernis, dass verschiedene gesetzliche Regelungen für bestimmte Rechtsgeschäfte verlangen. Ein Beispiel hierfür sind die Bürgschaftserklärungen nach § 766 I BGB. Tatsächlich dürften jedoch die mündlich oder konkludent geschlossenen Verträge des täglichen Lebens, wie z.B. beim Einkaufen im Supermarkt, die häufigste Form von Rechtsgeschäften darstellen. Um jedoch die Unabstreitbarkeit, Dauerhaftigkeit und Beweisfunktion von Willenserklärungen zu bewirken, wird oft auch freiwillig die Schriftform gewählt. Auch hierfür muss es in der digitalen Kommunikationswelt eine befriedigende Lösung geben.

Das AnpassungsG 2001 lässt qualifizierte elektronische Unterschriften nach (c) den Formerfordernissen nach einer Unterschrift im herkömmlichen Sinn genügen (§ 126a BGB) und gewährt diesen einen gesteigerten Beweiswert im Zivilprozessrecht (§ 292a ZPO)[53]. Eine vollständige Gleichstellung des Beweiswertes dieser digitalen Signaturen mit den traditionellen schriftlichen Dokumenten und Unterschriften wird vom AnpassungsG 2001 nicht vorgenommen, dies wird allerdings von der EU-Richtlinie auch nicht verlangt. Dort wird lediglich gefordert, dass elektronische Unterschriften als Beweismittel grundsätzlich zulässig sind. Alle elektronischen Unterschriften sind schon heute zum Abschluss von formfreien Rechtsgeschäften zulässig, haben aber im Beweisrecht keine gesteigerte Bedeutung und werden diese auch nicht erhalten. Es wird daher in Literatur gemutmaßt, dass die Regelung der einfachen und lediglich fortgeschrittenen elektronischen Signaturen überflüssig sind[54].

Durch die rechtliche Anpassung der Formvorschriften an die modernen Medien und die Gewähr einer praktischen, sicheren Lösung für die eben genannten „freiwilligen“ Anfor-

---

[51] <http://www.signtrust.de>

[52] <http://www.bnotk.de>

[53] <http://www.bmj.bund.de/ggv/bgbrege1.pdf>

[54] REDEKER 2000, 456.

derungen durch die Vorgabe von technischen Minimum-Standards ist das SigG 2001 geeignet, den verbreiteten Gebrauch der neuen Technologien zu fördern.

5. Zusammenfassung

Neben anderen nationalen Unternehmungen, wie z.B. in Singapur, versuchen auch die USA und Europa den Gebrauch von elektronischen Signaturen im Interesse des nationalen und internationalen Handels zu fördern und den Anforderungen an eine rechtlich verbindlich und sichere Alternative zur bisherigen Form von Unterschriften durch entsprechende gesetzliche Regelungen gerecht zu werden. Obwohl die beiden hier betrachteten Rechtskreise das selbe Ziel verfolgen, wurden zwei verschiedene Wege eingeschlagen. Das amerikanische E-Sign überlässt die Verwendung der Techniken und Infrastrukturen für elektronische Signaturen, einschließlich deren Sicherheit, vollständig dem Markt und beschränkt schon bestehende, technisch konkretisierende bundesstaatliche Regelungen.

Die EU-Richtlinie und insbesondere die deutsche Gesetzgebung unterscheiden sich hiervon erheblich durch die Tatsache, das diese die sichere Möglichkeit einer Identifikation des Unterzeichners, zumindest für bestimmte, herkömmlichen Unterschriften anzunähernde elektronische Signaturen verlangen. Da dies nur in einer Infrastruktur mit zuverlässigen Zertifizierungsdiensteanbietern sinnvoll möglich ist, verlangen die Richtlinie und in der Folge die nationalen Umsetzungsgesetze, wie z.B. das deutsche SigG 2001 die Erfüllung bestimmter Infrastruktur- und Technikanforderungen. Sie sind daher de facto im Gegensatz zu E-Sign nicht technik-neutral.

Die Hauptfunktion der EU-Richtlinie besteht darin, den Abschluss der Rechtsgeschäfte, die die händische Unterschrift unverzichtbar voraussetzen, durch elektronische Signaturen ebenfalls rechtsgültig zu ermöglichen. Konsequenterweise verlangt die Richtlinie, dass die elektronischen Unterschriften auch als Beweismittel anerkannt werden müssen. Den qualifizierten elektronischen Signaturen wird in Deutschland sogar aufgrund der hohen technischen Anforderungen auch ein höherer Beweiswert als den einfachen und fortgeschrittenen Signaturen zugebilligt, obwohl dies von der EU-Richtlinie nicht verlangt wird. Neben dieser rechtlichen Ausdehnung der Anwendbarkeit von elektronischen Unterschriften auf bestimmte Rechtsgeschäfte, die unter einem Formvorbehalt stehen, ist ein zu erwartender Nebeneffekt der verbreitete Einsatz zumindest von qualifizierten elektronischen Signaturen zur (freiwilligen) sicheren Perpetuierung von Willenserklärungen und Daten für die Archivierung und die Beweisführung bei späteren möglichen Auseinandersetzungen.

Gleichwohl bestehen Zweifel daran, ob sowohl der amerikanische als auch der europäische bzw. deutsche Weg zum angestrebten Ziel führen. Während E-Sign durch einen technik-neutralen Ansatz versucht, den Markt zu stimulieren, ist es möglich, dass gerade aufgrund dieser Offenheit die Unsicherheit für die Anwender hinsichtlich der Verlässlichkeit und technischen Sicherheit der eingesetzten Verfahren zu einem nur zögerlichen Einsatz der elektronischen Unterschriften führt.

Der Ansatz der EU-Richtlinie und insbesondere des SigG 2001 setzen hingegen auf eine anspruchsvolle Infrastruktur mit kostspieligen technischen Komponenten, um den An-

wendern qualifizierter elektronischer Signaturen die erwartete (Rechts-) Sicherheit zu geben und das Vertrauen in die Technik zu stärken. Gleichzeitig kann aber davon ausgegangen werden, dass die Hemmschwelle für die Anbieter durch die technischen und damit auch finanziellen Anforderungen sehr hoch liegt und dies auch an die Anwender weitergeben wird, auch wenn die Gebühren für die Anwender in Deutschland mit heute ca. 100-200 DM pro Jahr als durchaus moderat bewertet werden können. Die komplexen Infrastrukturen und anspruchsvollen technischen Komponenten führen gleichermaßen dazu, dass es zu Interoperabilitätsproblemen zwischen verschiedenen Anbietern kommt, wie z.B. derzeit zwischen Telesec und Signtrust.

Es ist daher sowohl in den USA als auch in Europa fraglich, ob wir eine schnelle und erfolgreiche Ausbreitung des Einsatzes von elektronischen Signaturen auch für sensible Rechtsgeschäfte erleben werden. Derzeit scheinen sich die Vor- und Nachteile der verschiedenen Ansätze in Europa und in Übersee die Waage zu halten. In beiden Rechtskreisen wird der Markt die Entscheidung für die Verbreitung der elektronischen Signaturen fällen und faktisch bestimmen, welche Technologien für welche Zwecke eingesetzt werden. Rechtsgeschäfte, die unter keinem Formvorbehalt stehen, können schon jetzt sowohl in den USA als auch in Deutschland durch *jede* Art von Willenserklärung, auch von elektronischen, getätigt werden. Eine Haftungserleichterung für die Anwender, wie bei dem Einsatz von Kreditkarten im heutigen Zahlungsverkehr wäre zur Steigerung der Akzeptanz der elektronischen Signaturen sicher hilfreich.

Insgesamt kann es aber sowohl durch Über- als auch durch Unterregulierung zur Existenz von verschiedenen geschlossenen Benutzergruppen kommen, bei denen die geschäftlichen Verwender die Technik diktieren und die Interoperabilität zwischen den Gruppen gefährden.

Literatur

AALBERTS, B.P., VAN DER HOF, S.: Digital Signature Blindness, Analysis of legislative approaches toward electronic authentication, November 1999 <http://cwis.kub.nl/~frw/people/hof/ds-fr.htm>.

BECKER, T., DUSEMUND, B., GOLLAN, L., ENGEL, T., MEINEL, CH.: Trust Centre: Infrastructure, Specifications and Standards. Trier 2000.

DUSEMUND, B., BECKER, T., GOLLAN, L., ENGEL, T., MEINEL, CH.: Security in Open Networks: The Functionality of a Public Key Infrastructure. Trier 2000.

FRY, P.B.: A Preliminary Analysis of Federal and State Electronic Commerce Laws. 25. September 2000, <http://www.bmck.com/ecommerce/ueta-esign.doc>

GREENWOOD, D.: Federal and State Electronic Signatures and Records Legislation: Legal Infrastructure for E-Commerce. 6. Oktober 2000, <http://civics.com/esign/>

HASTENTEUFEL, M., MEINEL, CH.: Digitale Zertifikate – Standards und Anwendungen. Trier 1999.

MEINEL, CH., LOSEMANN, F.: Warum Zertifikate? Trier 1998.

MIEDBRODT, A.: Anwendungserfahrungen ausgewählter US-amerikanischer Signaturgesetze. Datenschutz und Datensicherheit 1998, 194-198.

MIEDBRODT, A.: Das Signaturgesetz in den USA. Datenschutz und Datensicherheit 2000a, 541-545.

MIEDBRODT, A.: Signaturregulierung im Rechtsvergleich. Baden-Baden 2000.

NIMMER, R.T.: Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws. Discussion Draft. 10. November 2000 <http://www.bmck.com/ecommerce/ueta-esign-2.doc>

REDEKER, H.: EU-Signaturrichtlinie und Umsetzungsbedarf im deutschen Recht. Computer und Recht 2000, 455-460.

ZOELLICK, B.: Electronic Signatures. Commentary on the Electronic Signatures in Global and National Commerce Act 2000. 9. Januar 2001

<http://www.fastwater.com/Library/B2BEconomy/DigitalSigs/DigSig-Commentary-fr.php3>