Elektronischer Vertrag und Formvorschriften in Deutschland, England und den Vereinigten Staaten von Amerika

INAUGURAL-DISSERTATION

zur Erlangung des Doktorgrades

der Juristischen Fakultät
der Heinrich-Heine-Universität Düsseldorf

vorgelegt von
Daniel Michel, LL.M.
aus
Berlin

Dekan: Prof. Dr. Dirk Looschelders

1. Gutachter: Prof. Dr. Ulrich Noack

2. Gutachter: Prof. Dr. Jan Busche

Tag der mündlichen Prüfung: 7. September 2009

Danksagung

Diese Arbeit konnte nur durch das Zutun mehrerer Personen entstehen. Der größte Dank gebührt dabei meinem Doktorvater Prof. Dr. Ulrich Noack für Begleitung der Dissertation, seine konstruktive Kritik, die wertvollen Anregungen und die ausdauernde und wiederholte Korrektur der Entwürfe, sowie Prof. Dr. Jan Busche als Zweitgutachter und dem Dekanat der juristischen Fakultät der Heinrich-Heine-Universität Düsseldorf. Ich danke meiner gesamten Familie für das Fundament, auf dem meine Leistungen aufbauen, und meiner geliebten und verehrten Frau Dr. Charlotte Fechner für unendliche Geduld und Motivation. Folgende Personen haben mich in der Eigenschaft als Mentor in entscheidenden Phasen meiner akademischen und beruflichen Ausbildung maßgeblich und großzügig unterstützt und damit das Unternehmen Promotion und dessen erfolgreichen Abschluss letztlich erst möglich gemacht: dies sind Andreas und Jutta Barthel, Dr. Paul Ulrich Fechner und Dr. Peter Waltl.

Inhaltsverzeichnis

Einleitung

Ausgangspunkt für diese Arbeit sind die Veränderungen und Herausforderungen, denen Formvorschriften für vertragliche Rechtsgeschäfte durch digitalisierte Kommunikationsformen des Internets ausgesetzt sind. Die Digitalisierung von Information macht diese anfällig für vielfältige Manipulationen und Verfälschungen in Form und Inhalt. Folglich tauchen Probleme bei der Authentizität solcher Information auf. Ein wesentliches Bedürfnis des E-Commerce ist daher dasjenige nach Vertrauenswürdigkeit der elektronischen Kommunikation, unabhängig davon, ob die Integrität und Authentizität der Kommunikation gesetzlich verlangt oder nur von den Parteien gewünscht und vereinbart wird. Bei traditionellen Kommunikationsformen greifen dort, wo die Gültigkeit eines Rechtsgeschäftes von einer Authentifizierung abhängt, die Formerfordernisse oder Vereinbarungen der Schriftlichkeit und der Signierung, oft in Form der eigenhändigen Unterzeichnung. Diese Instrumente sind auf elektronische Kommunikationsformen nicht ohne weiteres übertragbar, insbesondere hinsichtlich der Erfüllung von Zweck und Funktionen der Formvorschriften. Formerfordernisse und Beweisregelungen etc. mussten folglich entsprechend geändert werden. Dabei war die Rechtsgültigkeit elektronischer Signaturen sowie die Erfüllung von Formerfordernissen durch diese zu regeln. Hinsichtlich der durch die digitale Technik bedingten Authentisierungsprobleme bot sich mit der digitalen Signatur eine vordergründig ebenfalls technische Lösung an, deren Einsatz für viele Gesetzgeber als Mittel der Erfüllung der den Formerfordernissen innewohnenden Funktionen gewählt wurde. Gegenstand der gesetzliche Regelung des Einsatzes der digitalen Signatur waren die Technologie und die an diese zu stellenden Anforderungen technisch-organisatorischer Art. Dies betrifft insbesondere die Ausgestaltung der Sicherheitsinfrastruktur für die elektronische Signatur und deren Verknüpfung mit Rechtsfolgeregelungen.
Hinsichtlich der Änderung und Angleichung von Formvorschriften und zur Signaturgesetzgebung entstanden nationale Gesetze und Rechtsvorschriften, Richtlinien der Europäischen Union sowie Konventionen, Modellgesetze und Richtlinien von UN, UNCITRAL und OECD. Die Arbeit ist rechtsvergleichend, wobei rechtliche Regelungen und einschlägige Rechtsprechung von Staaten und Organisationen untersucht werden, die in einem besonderen Verhältnis zueinander stehen. Dies sind die gesetzlichen Regelungen zu Formvorschriften, elektronischer Kommunikation und elektronischer Signatur in der Europäischen Union, in Deutschland und England sowie in den USA. Gegenüber gestellt werden zunächst die Richtlinien der Europäischen Union über den elektronischen Geschäftsverkehr und über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, sowie deren Umsetzung in deutsches und englisches Recht. In Deutschland wurden die Richtlinien durch die Gesetze über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr sowie über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr umgesetzt und nachfolgend teilweise weiter geändert und ergänzt. In England wurde die Richtlinien zunächst durch den Electronic Communications Act 2000 und nachfolgend durch The Electronic Commerce (EC Directive) Regulations

2002 und The Electronic Signatures Regulations 2002 implementiert. In den USA wurden erst nachdem bereits verschiedenste bundesstaatliche Signaturgesetze existierten zur Vereinheitlichung auf Bundesebene der Uniform Electronic Transactions Act, der Electronic Signatures in Global and National Commerce Act und der Uniform Computer Information Transaction Act erlassen. Die hier verglichenen Gesetzeswerke und Gerichtsurteile sind Teil zweier sehr unterschiedlicher Rechtssysteme, des *common* oder *case law* und des *code law*, die teilweise unterschiedlich auf die neuen technischen Herausforderungen reagieren. Die deutschen Regelungen zu elektronischen Verträgen sind dabei in ein sehr klar strukturiertes Gebilde eingebunden und damit ein idealtypischer Vertreter eines auf Kodifizierung fußenden Rechtssystems. Das englische und das deutsche Recht sind durch die Harmonisierungsbestrebungen der Europäischen Union miteinander verbunden, während das US-amerikanische Recht ohne „äußeren" Druck in seiner Rechtstradition Regelungen geschaffen hat. Das US-amerikanische und das englische Recht wiederum sind durch ihren gemeinsamen Ursprung als Richterrecht miteinander verbunden. Sie teilen eine Vielzahl an rechtlichen Regeln und Prinzipien, gerade im Privat- und Vertragsrecht. Urteilen eines Obersten Gerichts wird im jeweils anderen Land, wenn nicht als Präzedenzfall und damit als Rechtsquelle, so doch als gewichtige Meinung Beachtung geschenkt. Beiden ist gemeinsam, dass sie als Richterrecht prinzipiell sehr flexibel auf neue technische Änderungen reagieren. Dennoch haben auch England und die USA trotz einer sehr ähnlichen Philosophie sehr unterschiedliche Formen und Ausmaße der gesetzlichen Regulierung gewählt. Des Weiteren gehören die USA, Großbritannien und Deutschland zu denjenigen Ländern, die sowohl traditionell im Welthandel, als auch in Bezug auf Verbreitung und Nutzung des Internets eine führende Rolle spielen. England und Deutschland bilden hierbei Teil eines gemeinsamen europäischen Binnenmarktes. Folglich werden rechtliche Regelungen dieser Länder und der Europäischen Union den E-Commerce faktisch beeinflussen. Die EU-Kommission ist auf europäischer Ebene ein wichtiges und durchsetzungsfähiges Organ und Instrument der Harmonisierung. Andere internationale Organisationen wie die UNCITRAL üben ihrerseits einen wichtigen Einfluss auf die weltweite Harmonisierung auf diesem Rechtsgebiet aus, zum Beispiel indem sie als Leitlinien für die Signaturpolitik der USA auf Bundesebene dienten. Der Vergleich verdeutlicht, dass sowohl die Ausgangspunkte für die nationalen gesetzlichen Neuregelungen, als auch die dabei beschrittenen Wege teilweise sehr unterschiedlich ausfallen.

Durch die Untersuchung bestimmter Formtypen wie der elektronischen Form des § 126a BGB und insbesondere der Textform des § 126b BGB, der *writing*- und *signature*-Erfordernisse im englischen und US-amerikanischen Recht sowie deren Erweiterung durch richterliche Rechtsfortbildung, soll, unter Herausarbeitung von Gemeinsamkeiten und Unterschieden, die Möglichkeiten gegenseitiger Befruchtung eruiert werden. Die Einführung elektronischer und digitaler Signaturen führt dazu, dass nicht mehr das verkörperte Original eines Dokumentes oder einer Unterschrift für die Authentizität und Integrität des Dokumentes bzw. ihres Inhaltes bürgt. Vielmehr soll dies durch technische Verfahren ersetzt werden, die insbesondere die Authentizität des signierten elektronischen Dokumentes garantieren sollen. Dabei fokussieren der europäische und der deutsche Gesetzgeber sehr auf die Technik der digitalen Signatur auf Grundlage von

Zertifikaten vertrauenswürdiger Dritter. Insofern wird Originalität ersetzt durch die Sicherheit eines bestimmten Systems. Dieses System hat aber mehrere grundlegende Schwächen, die trotz ihrer prinzipiell hohen Vertrauenswürdigkeit und Zuverlässigkeit de facto zu Unsicherheiten führen können. Um Sicherheit zu gewährleisten, bedarf es sehr aufwändiger Prüf- und Kontrollmechanismen. Gängige Verfahren beruhen auf den Elementen Wissen und Haben, die keinen 100%-igen Schutz vor Missbrauch und Verfälschung bieten. Stark voneinander abweichende Regelungsansätze und divergierende Umsetzungen in den einzelnen Staaten verstärken zum Beispiel durch mangelnde Interoperabilität und fehlende gegenseitige Anerkennung die Schwächen des Einsatzes der digitalen Signatur. Vor allem aber leidet das insbesondere in Deutschland gesetzlich normierte und als einziges mit Rechtskraft und Beweiskraft versehene Verfahren der digitalen Signatur an dem Umstand, dass es in keinem der hier vorgestellten Staaten eine hinreichende Marktdurchsetzung erreicht hat. Tatsächlich ist vielmehr festzustellen, dass sich Verbraucher wie Unternehmen für die allermeisten rechtserheblichen Erklärungen mit dem niedrigen Sicherheitsstandard und der geringen Beweiskraft einfacher elektronischer Dokumente und Signaturen zufrieden geben. Dies berechtigt zur Frage nach alternativen Verfahren zur digitalen Signatur und deren rechtlichen Bewertung, um Authentizität und Integrität statt Originalität und einen pragmatischen und rechtssicheren Weg für den elektronischen Rechtsverkehr zu gewährleisten.

Ein solcher Weg könnte in einer Stärkung der Textform und damit vergleichbarer Kommunikation liegen, zumal sie den im *common law* Englands und der USA als rechtswirksam anerkannten Formen des *signed writing* gleicht. Die insbesondere vom Bundesgesetzgeber der USA durchgesetzte, aber auch von den übrigen Gesetzgebern zumindest angestrebte Technikneutralität in Bezug auf Verfahren der elektronischen Signatur schließt die digitale Signatur ein, andere Verfahren der Authentifizierung jedoch nicht aus. Vielfach wird in England und den USA als *writing* akzeptiert, was in Deutschland nicht die Definition der Urkunde und die Voraussetzungen der Schriftform erfüllt, wenn dort auch vereinzelt auf die Verkörperung der Erklärung abgestellt wird. Gleiches gilt für die *signature*, die dort zum Beispiel seit jeher auch in Form eines Stempels erfüllt werden kann. Dabei kommt es weniger auf die konkrete Form der Signatur an, als auf den so manifestierten Willen des Signierenden, das Dokument zu authentisieren, also auf die konkrete Funktion der jeweiligen Signatur. In England und den USA sind von den Gerichten in jüngster Zeit einfache Formen der elektronischen Kommunikation wie beispielsweise die mit Namensangaben versehene E-Mails als *signed writing* gemäß gesetzlicher Formerfordernisse wie den Statutes of Frauds anerkannt worden, mithin solchen Formvorschriften, denen insbesondere auch eine Beweisfunktion zukommt. Deutsche Gerichte wiederum verneinen insbesondere die Erfüllung jeglicher Beweisfunktion durch solche Kommunikationsformen. Kern dieses Beweisproblems für Verwender und Empfänger ist es, zu belegen, dass ein elektronisches Dokument vom angegebenen Absender stammt und dieser die darin enthaltene Erklärung dieses Inhalts abgegeben hat. Die technischen Grundlagen und Probleme der Manipulierbarkeit von zum Beispiel E-Mails sind in allen Rechtsordnungen gleich. Es könnten also Bewertungen und Regeln aus dem englischen und US-amerikanischen Recht entlehnt werden, die faktisch zu einer höheren Beweiswirkung elektronischer Dokumente

mit einfachen elektronischen Signaturen führen können. Insgesamt kann möglicherweise für bestimmte Rechtsgeschäfte ein geringerer Standard als der derzeit vom Gesetz geforderte genügen und so der Anwendungsbereich zum Beispiel der Textform und vergleichbarer Kommunikation ausgeweitet werden.
Eine Beweiskraftregel gibt es für die Textform in Deutschland nicht. Dergleichen ist über § 371a ZPO lediglich für die elektronische Form des § 126a BGB als Anscheinsbeweis für die Authentizität und Integrität des elektronischen Dokuments vorgesehen, wenn dieses mit einer auf einem qualifizierten Zertifikat beruhenden fortgeschrittenen elektronischen Signatur versehen wurde. Ein Anscheinsbeweis oder eine Beweisvermutungen für elektronische oder digitale Signaturen wurden in England und den USA, mit Ausnahme einzelner Bundesstaaten in den USA, nicht gesetzlich festgeschrieben. Solche können dort also nur im Wege der richterlichen Rechtsentwicklung gebildet werden. Einfache elektronische Signaturen und digitale Signaturverfahren werden insofern gleich behandelt. Die *common law*-Staaten können dabei bereits bestehende Rechtsgrundsätze leichter auf das elektronische Umfeld übertragen. Im Hinblick auf eine Übertragung in deutsches Recht ist zu fragen, ob und mit welchen Argumenten für welche Arten elektronischer Erklärungen und Dokumente solche Beweiskraftregelungen, gesetzliche Vermutungen und Anscheinsregelungen existieren. Rechtlich besteht die wesentliche Parallele darin, dass elektronische Dokumente und Signaturen als Beweisstück Augenscheinsobjekt sind und grundsätzlich der freien Beweiswürdigung des Gerichts unterliegen. Daher sollten die hier wie dort angeführten Argumente zu Beweiszulässigkeit und Beweiswert solcher Dokumente gleichermaßen Gültigkeit haben und insbesondere die Diskussion in Deutschland befruchten können.

1 Technische und rechtliche Grundlagen

1.1 Digitales Format und elektronischer Vertrag

Gegenstand dieser Arbeit sind elektronische Erklärungen und Methoden ihrer Authentifizierung. Elektronische Erklärungen können die Form elektronischer Dokumente, etwa einer E-Mail haben. Elektronischer Dokumente sind Informationen und Daten, die als Dateien auf elektronischen Speichermedien existieren. Solche (Computer-)Dateien sind elektronisch in *dots* und *bytes* auf diesen Speichermedien oder Datenträgern, zum Beispiel der Festplatte eines Computers, auf Disketten oder CD-ROMs, gespeichert. Diese digital gespeicherten Dateien haben die Eigenschaft, dass Kopien identisch sind mit der Ursprungsdatei. Eine digitale Datei und also das elektronische Dokument können beliebig oft kopiert werden, ohne dass ein Unterschied zum kopierten Dokument erkennbar wäre. Veränderungen sind sehr leicht möglich und ohne direkten Vergleich mit dem Ursprungsdokument nicht als solche erkennbar. Dies betrifft auch alle die einer Datei zugehörigen oder dieser beigefügten Daten.[1] Die bisher üblichen, für traditionelle, verkörperte Dokumente entwickelten Methoden der Authentifizierung sind wegen der digitalen und damit nicht verkörperten Form elektronischer Dokumente vor Probleme gestellt.

Solche elektronische Dokumente werden vielfach für rechtserhebliche Erklärungen und zum Vertragsschluss verwendet. Als Kommunikationsmedium dient dabei zumeist das Internet.[2] Dabei können digitale Dateien über die dort vernetzten Computer vom Absender zum Empfänger versendet werden, bei E-Mails vom E-Mail-Account des Absenders zu dem des Empfängers.[3] Eine andere Kommunikationsform stellt die von einer der beteiligten Parteien vorgehaltene Website dar, welche die andere Partei aufrufen und einsehen kann. Über das Internet abgeschlossene elektronische Verträge und die diesen zugrunde liegenden Erklärungen sind damit Spiegelbild der für dieses Medium typischen Kommunikationsformen.[4] Der reine E-Mail-Vertrag entspricht den traditionellen Vertragsverhandlungen durch Austausch von Angebots- und Annahme Erklärung mit-

---

[1] Redeker, „Schriftformerfordernisse im E-Commerce: In welcher Form können Schriftformerfordernisse den E-Commerce behindern?“, ITRB 2001, S. 46-48, S. 48.

[2] Für eine Einführung in die Themen Electronic Commerce und die Entstehung der Informationstechnologie und des Internet siehe: Lloyd, *Information Technology Law*, London 2000, S. XLIV-XLVI, 1-2, 5-11, 29-32. Zur Funktionsweise des Internet siehe auch Kennedy, *The Rough Guide To The Internet*, London 2000.

[3] Jede Kommunikation über das Internet wird nicht an einem Stück gesendet, sondern in mehrere kleine Pakete zerteilt, die einzeln und über verschiedene Wege zum Empfänger gelangen. Diesen Datenpaketen wird eine *check sum*, also eine Information über die Summe der gesamten versendeten Datenmenge, angehängt. Sollte nur eines der Datenpakete nicht beim Empfänger ankommen, erfährt dieser unmittelbar vom partiellen Kommunikationszusammenbruch und kann darauf unmittelbar reagieren. Siehe bei Murray, Andrew D. in Edwards, Lilian/Charlotte Walden, *Law & The Internet – A Framework for Electronic Commerce*, Oxford 2000, S. 25/26:

[4] Siehe hierzu die ausführliche Beschreibung von Mayer, „Recht und Cyberspace“, NJW 1996, S. 1782-1791, S. 1784f. Tatsächlich haben sich durch das Internet eine Vielzahl von Geschäfts- und Vertragsformen herausgebildet. Ausführlich z.B. Semdinghoff, „The Legal Requirements for Creating Secure and Enforceable Electronic Transactions“, www.bmck.com/ecommerce/article-electronic-transactions2.doc, S. 2.

tels Dokumenten auf dem Postweg.[5] Beim zweiten Typ, dem Webvertrag oder „Click-Wrap"-Vertrag, sind die auf einer Website enthaltenen Warenkataloge, Bestellformulare etc. interaktiv ausgestaltet. Durch ein Menü geführt kann dabei der Besteller Waren oder Dienstleistungen auswählen und rechtsverbindlich bestellen, beispielsweise durch das Betätigen eine „Ich akzeptiere"-Buttons. Der Webvertrag kann daher mit der traditionellen Postbestellung verglichen werden.[6]

Das Internet ist ein dem Prinzip nach offenes Kommunikationsmedium, auf das alle verbundenen Computer Zugang haben. Darüber versendete Nachrichten werden also nicht innerhalb eines begrenzten, von den Kommunikationsparteien beherrschten Mediums versendet. Nicht zuletzt werden solchermaßen online geschlossene vertragliche Vereinbarungen oder online übermittelte Erklärungen wiederum auf elektronischen Speichermedien gespeichert.[7] Geschäfte im Internet können zudem in Echtzeit getätigt werden, da die Übermittlung von Erklärungen in Sekundenbruchteilen abläuft und bestimmte Dienste sofort ausgeführt und angenommen werden.[8] Insbesondere beim Webvertrag lässt dies dem Nutzer wenig Zeit zum Nachdenken vor der Abgabe rechtserheblicher Erklärungen.[9] Außerdem kennt das Internet keine Grenzen, weder rechtliche noch geographische.[10]

---

[5] York/Tunkel, *E-Commerce – A guide to the Law of Electronic Business* London (2000), p. 85. Ein älterer Weg des online-Vertragsabschlusses aus der Zeit der Ursprünge des www stammt nutzte Business Data Interchange-Systeme, vorab vereinbarte *interchange agreements* oder *trading partner agreements*. Ausführlich siehe ebenda, S. 85.

[6] Dabei stellt die Bestellung das Angebot dar und die, häufig automatisch generierte und zum Besteller gesendete Bestätigung die Annahme, gegebenenfalls die Zusendung der Ware (auf dem normalen Postweg) oder die Durchführung der Dienstleistung (teilweise ebenfalls auf elektronischen Weg). Als problematisch wird teilweise die Aufgabe einer Bestellung durch die Auswahl einer Ware oder Dienstleistung auf einer Website und die anschließende Betätigung eines „Bestellen"- oder „Ich akzeptiere"-Buttons gesehen. Siehe hierzu Köhler/Arndt, *Recht des Internet*, Heidelberg 2003, S. 45; Ernst, „Der Mausklick als Rechtsproblem – Willenserklärungen im Internet", NJW-CoR 1997, S: 165-167, S. 165; Lloyd, S. 563; Maennel, „Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission", MMR 1999, S. 187-192, S. 191; York/Tunkel, S. 85; *Butler Machine Tool Co Ltd. v. Ex-Cell-O Co Corpn (England) Ltd.* [1979] 1 All ER 965; A.A. Boehme-Neßler, *Cyberlaw: Lehrbuch zum Internet-Recht*, München 2001, S. 142.

[7] Semdinghoff, „The Legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 3.

[8] Die Kommunikation über das Internet kann insofern verglichen werden mit der telefonischen. Siehe hierzu; Murray in Edwards/Walden, S. 25/26.

[9] Hörnle, „The European Union Takes Initiative in the Field of E-Commerce", JILT 2000, Vol. 3., http://elj.warwick.ac.uk/jilt/00-3/hornle.html.

[10] Die Bezüge zu fremden Rechtsordnungen erweitern sich; Sookman, „Legal Framework for E-Commerce Transactions", CLTR 2001, S. 85-95, S. 90; Vehslage, „Das geplante Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr", DB 2000, S. 1801-1805, S. 1801.

1.2 Zweck und Funktion von Formvorschriften

Viele der gesetzlichen Vorschriften, die auf den traditionellen „offline"-Handel Anwendung finden werden auch auf elektronische Erklärungen und Geschäfte des E-Commerce angewendet. Diese Regelungen umfassen vertragsrechtliche Vorschriften, etwa das Erfordernis von Angebots- und Annahmeerklärung für den wirksamen Vertragsschluss. Vorschriften zu rechtserheblichen Erklärungen sowohl im zivilrechtlichen als auch im prozessualen oder öffentlich-rechtlichen Bereich umfassen grundsätzlich auch Formerfordernisse für bestimmte Arten von Erklärungen und Vereinbarungen.[11] Formerfordernisse dienen jeweils einer bestimmten Funktion. Sofern also untersucht werden soll, ob und unter welchen Voraussetzungen elektronische Erklärungen diese Funktionen der Formerfordernisse, beispielsweise die Authentifizierung einer Erklärung, erfüllen können, sind diese Funktionen kurz darzustellen.

Hinsichtlich des Zwecks und der Funktion kann unterschieden werden zwischen dem Erfordernis der schriftlichen Form eines Dokuments und dem Erfordernis dessen Signierung.[12] Die schriftliche Form oder Schriftform dient der Fixierung des Erklärten. Rechtserhebliche Willenserklärungen werden so in körperlicher Form und damit dauerhaft bewahrt. Der Inhalt einer Vereinbarung wird fixiert und klargestellt. Neben dieser Traditions- und Klarstellungsfunktion erfüllt die schriftliche Fixierung insbesondere die Beweisfunktion bezüglich des Inhalts der Erklärung.[13] Dagegen ist die reine Dokumentationsfunktion von Formvorschriften, etwa eine Information dauerhaft verfügbar und abrufbar zu bewahren, ein Minus zur Beweisfunktion.[14] Die Signierung einer schriftlich fixierten Erklärung, insbesondere durch die eigenhändige Unterschrift, dient der Verifizierung der Identität des Erklärenden und der Authentifizierung der Erklärung. Sie symbolisiert und beweist den Willen des Unterzeichnenden, sich rechtlich durch die Erklä-

---

[11] Viele der auf elektronische Kommunikation und den E-Commerce anwendbaren rechtlichen Regeln sind von denjenigen abgeleitet, die für die herkömmlichen papiergebundenen Kommunikationsformen gelten; Cavanillas, „An Introduction to Web Contracts", in Walden/Hörnle (Hrsg.), *E-Commerce Law and Practice in Europe*, (ECLIP), Teil 2, Kap. 1, Cambridge 2001, S. 9. Siehe auch Sookman, CTLR 2001, S. 90, 91, der von *„Schriftform- und Unterschriftserfordernissen sowie notariellen und anderen Formalitäten"* spricht.

[12] Nachfolgend werden solche Formerfordernisse, die für Dokumente und Nachrichten die Verfasstheit in schriftlicher Form (*in writing*) verlangen, Schriftformerfordernis oder Erfordernis der schriftlichen Form genannt. Solche die die Unterzeichnung oder Signierung eines Dokuments oder einer Erklärung verlangen (*signature*, *signed* oder *signed writing*) werden Unterschriftserfordernis genannt. Diese Unterscheidung orientiert sich an der Unterscheidung beider Typen der Formerfordernisse im englischen und US-amerikanischen Recht. Diese Unterscheidung ist insbesondere bei der Betrachtung der Formvorschriften im deutschen Recht zu beachten, wo der Begriff des Schriftformerfordernisses des § 126 BGB sowohl die schriftliche Verkörperung als auch die Unterschrift umfasst, siehe nachfolgend 1.3.1.2.

[13] Cavanillas, (ECLIP), S. 9; Chissick, *Electronic Commerce: Law and Practice*, London 1999, S. 81; Einsele in Rebmann/Säcker/Rixeder, *Münchner Kommentar zum Bürgerlichen Gesetzbuch* (MüKo), München 2006, § 125, Rn. 8, 9; Jewell, *An Introduction to English Contract Law*, Baden-Baden 1997, S. 66, 67; Lloyd, S. 571; Mason, *Electronic Signatures in Law*, Haywards Heath, 2007, S. 8. Zu den Funktionen der Formerfordernisse (insbesondere in den USA) siehe auch Menna, „From Jamestown to the Silicon Valley, Pioneering a Lawless Frontier: The Electronic Signatures in Global and National Commerce Act", VJLT 2001, www.vjolt.net/vol6/issue2/v6i2-a12-Menna.html.

[14] Einsele in MüKo, § 125, Rn. 9.

rung zu binden.[15] Häufig wirkt die Einhaltung einer bestimmten Form konstitutiv, insbesondere das Unterschriftserfordernis.[16] Dieses wird eingesetzt, um das Rechtsgeschäft überhaupt erst rechtskräftig werden zu lassen. Teilweise dient die Einhaltung einer bestimmten Form insbesondere im *common law* nur der Durchsetzung eines vertraglichen Anspruches.[17] Die Unterschrift dient vor allem als Sicherheitselement. Sie kann ein Dokument authentifizieren die Feststellung ermöglichen, dass dieses Dokument vom Unterzeichner stammt. Ferner kann sie die Integrität, also die Vollständigkeit und Unverfälschtheit des Dokuments sicherstellen.[18] Schriftform- und Unterschriftserfordernis sollen dem Erklärenden die Rechtserheblichkeit ihrer Erklärungen und die besondere Bedeutung des beabsichtigten Rechtsgeschäfts vor Augen führen. Die Ausführung in schriftlicher verkörperter Form zusammen mit der eigenhändigen Unterschrift erfordert einen gewissen Zeitaufwand und verfügt über eine zeremonielle Komponente. Der dadurch bewirkte psychologische Effekt auf die Erklärenden dient der Warnung und soll den Unterzeichner veranlassen, die möglichen Gefahren des Vertrages abzuwägen.[19] Erfordernisse, die schriftliche unterschriebene Urkunden verlangen, haben damit die Funktion der Klarstellung und des Beweises, der Identitätsfeststellung, Echtheit, Verifikation und der Warnung.[20]

Bis zum Aufkommen des Computers und der elektronischen Kommunikation waren die Zivilrechtssysteme geprägt durch die Vorstellung des persönlichen Kontakts oder des Austauschs von geschriebenen, papiernen Erklärungen. Diese Kommunikation garan-

[15] Hoeren, „Electronic Commerce and Law", in Walden/Hörnle, Teil 1, Kap. 1, S. 9; auch Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 12. Im *common law* dient die Signatur als (zulassungsfähiger) Beweis für die Zustimmung und Akzeptanz des Inhalts eines Dokuments durch den Signierenden erbringen; Mason, *Electronic Signatures in Law*, Haywards Heath 2007, S. 20 und unten 1.3.2.3 und 1.3.3.3.

[16] Fringuelli/Wallhäuser, CR 1999, S. 93-101, S. 94; Semdinghoff, „The Legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 4.

[17] So wirken im Englischen und US-Amerikanischen Recht viele Formvorschriften nicht konstitutiv, hindern jedoch bei Nichterfüllung die Durchsetzung der ansonsten wirksamen Vertragsvereinbarung. Insbesondere Formvorschriften aus den Statutes of Frauds dienen häufig lediglich der Beweisbarkeit von Versprechen und sind gegen betrügerische Ansprüche gerichtet. Es soll vermieden werden, dass ein Gericht durch betrügerische Aussagen zu falschen Schlussfolgerungen hinsichtlich des Vertrages gebracht wird. Siehe hierzu: Reimann, *Einführung in das US-amerikanische Privatrecht*, München 2004, S.42, und Bernstorff, *Einführung in das englische Recht*, München 2000, S. 52, sowie 1.3.2.3 und 1.3.3.3.

[18] Mason, *Electronic Signatures in Law*, S. 2-4; Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 12.

[19] Cavanillas, ECLIP, S. 10; Chissick, S. 81, 84; Einsele in MüKo, § 125, Rn. 8; Fringuelli/Wallhäuser, „Formerfordernisse beim Vertragsschluss im Internet", CR 1999, S. 93-101, S. 94; Jewell, S. 65; York/Tunkel, p. 86. Zur Bedeutung des Aspekts Zeit für die Warnfunktion des Schrift- und Unterschriftserfordernissees siehe bspw. Hoeren, „Internet und Recht – Neue Paradigmen des Informationsrechts", NJW 1998, S. 2849-2954, S. 2852.

[20] Ferner Ausweisfunktion (auch Legitimationsfunktion), Informations-, Beratungs-, Instruktions-, Kontroll-, Schuldnerschutz- (auch Liberations-) sowie Wertpapier-, Umlauf- und Sperrfunktion; Heinrichs in Palandt, *Bürgerliches Gesetzbuch*, München 2008, § 125, Rn. 1-2d; Einsele in MüKo, § 125, Rn. 6-8; Nöcker, „Urkunden und EDI-Dokumente", CR 2000, S. 176/177; Die United Nations Commission on International Trade Law (UNCITRAL) hat in einem Bericht 1990 vier Gründe für Formvorschriften festgestellt: die Anzahl an Rechtsstreitigkeiten zu verringern, den Vertragsparteien die Folgen ihres Handelns zu verdeutlichen, Beweise über die Vertragsvereinbarungen zu schaffen, auf die sich Dritte stützen können, und Steuern, Buchführung und Kontrollwesen zu unterstützen. Siehe in: Lloyd, S. 575.

tiert ein Minimum an Authentizität und Integrität. Letztendliche Sicherheit über die Identität der Parteien kann dabei durch die Einschaltung eines Notars erreicht werden.[21] Auf digitale Dateien und Dokumente in elektronischen Speichermedien sowie auf die Kommunikation über das Internet sind vertrauensbildende Maßnahmen dieser Gestalt nicht anwendbar. Die digitalen und über das Internet übertragenen Dateien und Dokumente sind leicht zu manipulieren und – im Prinzip – uneingeschränkt zugänglich. Dadurch ist es nicht ohne weiteres gewiss, ob eine vorliegende Erklärung wirklich identisch ist mit ihrem ursprünglichen Inhalt, ob sie vom angegebenen Absender stammt oder der Inhalt der Erklärung nicht während der Übertragung vom Sender zum Empfänger verändert wurde.[22] Ein papierner Ausdruck einer Computerdatei ist zum Beispiel nur bedingt aussagekräftig in Bezug auf die im Arbeitsspeicher und auf den Bildschirm eines Computers geladene Datei. Eine eigenhändige Unterzeichnung eines digitalen Dokuments wiederum ist nicht vorstellbar.[23] Auch eine gescannte Unterschrift wird durch den Scanvorgang in digitale Daten zerlegt und dadurch manipulationsfähig.[24] Gesetzliche oder privat vereinbarte Erfordernisse der schriftlichen Form oder der (eigenhändigen) Unterschrift in ihrem traditionellen Verständnis sind daher auf das Internet nicht ohne weiteres zu übertragen.

[21] Hoeren, ECLIP, S. 9. Telefonisch übermittelten Willenserklärungen können durch sofortiges Nachfragen überprüft werden und auch eine per Telefax übermittelte Erklärung enthält zumeist eine Abbildung der handschriftlichen Signierung; Köhler/ Arndt, Fn. 90.

[22] Deville/Kalthegener, „Wege zum Handelsverkehr mit elektronischer Unterschrift“, NJW-CoR 1997, S. 168-172, S. 169; Hoeren, ECLIP, S. 10, siehe auch unter 3.2.1.5, 3.3.6 und 3.3.7.

[23] Zwar gibt es verschiedene technische Hilfsmittel, mit denen vergleichbares möglich ist, wie beispielsweise der „E-Pen“, mit dem auf einem Bildschirm eigenhändig signiert werden kann. Dabei geht jedoch auch das so geschaffene Abbild der eigenhändigen Unterschrift auf dem Bildschirm in ein digitales Format über. Dazu siehe Kröger/Gimmy, *Handbuch zum Internetrecht: Electronic Commerce – Informations-, Kommunikations- und Mediendienste*, Berlin/Heidelberg 2002, S. 26/26.

[24] Nöcker, CR 2000, S. 178/179.

1.3 Formvorschriften in Deutschland, England und den USA vor den Neuregelungen

Überall in Europa und den USA sind Verträge grundsätzlich formlos gültig. Die existierenden Vorschriften hinsichtlich der für bestimmte rechtserhebliche Erklärungen und Rechtsgeschäfte vorgeschriebenen Form sind von Rechtsordnung zu Rechtsordnung teilweise unterschiedlich.[25] Nachfolgend wird zunächst für die hier im Vergleich stehenden Rechtsordnungen dargelegt, inwieweit nach alter Rechtslage elektronische (digitale) Dokumente die oben genannten Funktionen der papiergebundenen schriftlichen Form und der Unterschrift erfüllen können. Es wird aufgezeigt, wo der Gesetzgeber Gesetzesänderungen vornehmen musste, um die Formvorschriften an die neuen Kommunikations- und Vertragsformen anzupassen, beziehungsweise Funktionsgleichheit zwischen papiernen und digitalen Dokumenten und Signaturen zu schaffen.

1.3.1 Formvorschriften im deutschen Recht

Nach deutschen Recht bedürfen Erklärungen wie Angebot und Annahme oder der Vertrag grundsätzlich nicht einer bestimmten Form, um rechtlich wirksam zu werden. Ein solches Formerfordernis kann jedoch in bestimmten Fällen aus dem Gesetz oder Parteivereinbarung folgen.

1.3.1.1 Regelungsort

Die Formvorschriften im deutschen Zivilrecht finden sich im Allgemeinen Teil des Bürgerlichen Gesetzbuchs (BGB). Der Allgemeine Teil des BGB behandelt die Rechtsgeschäfte in generell abstrakter Form. Das BGB nannte ursprünglich für die verschiedenen Arten von Rechtsgeschäften und je nach dem mit der Form verfolgten Zweck die Schriftform des § 126 BGB sowie die öffentliche Beglaubigung, § 129 BGB, und die notarielle Beurkundung, § 128.[26] In den §§ 125 ff. BGB, insbesondere § 126 BGB, ist allgemein festgelegt, welche Anforderungen an die Schriftlichkeit oder die Signierung einer Willenserklärung vom Gesetz gestellt werden. Auf diese Vorschriften beziehen sich alle im BGB im Besonderen Teil folgenden Formerfordernisse zu den einzelnen Rechtsgeschäfts- und Vertragstypen. In Nebengesetzen zum BGB sowie Gesetzen außerhalb des BGB gibt es weitere Vorschriften, welche die bestimmte Form für bestimmte Rechtsgeschäfte vorschreiben und sich auf die §§ 125 ff. BGB beziehen.[27] Die in den

---

[25] Siehe hierzu ausführlich Cavanillas, ECLIP, S. 9; Heinrichs in Palandt, § 125, Rn. 1; Einsele in MüKo, § 125 Rn. 1; Hay, *U.S.-Amerikanisches Recht:Ein Studienbuch* , München 2000, Rn. 263ff.; Reimann, S. 41; Jewell, Rn. 83; Murray in Edwards/Walden, S: 19.

[26] Einsele in MüKo, § 125, Rn. 2.

[27] Cavanillas, ECLIP, S. 9; Jansen, „Legal Aspects of Doing E-Commerce Business in Germany", *ICCLR* Spe. 1999, S. 39-42, S. 39; Niemann, „Electronic Transaction Bill – Germany", *CLSR* (2001), S. 28-31, S. 28, 29. Gesetzliche Formerfordernisse bestehen beispielsweise für Verträge über den Verkauf von Immobilien oder für Verbraucherkreditverträge. Eine ausführliche Auflistungen der Vorschriften des

§§ 125 ff. BGB genannten Formen werden wiederum teilweise in den auf die einzelnen Rechtsgeschäfte anwendbaren Formvorschriften modifiziert.[28] Keine Anwendung findet § 126 BGB auf schriftlich vorzunehmende Prozesshandlungen oder im öffentlichen Recht.[29] Im Falle der gesetzlich zwingend verlangten Form wird die Vereinbarung bei Missachtung des Formerfordernisses unwirksam, § 125 Satz 1 BGB. Im Falle des vertraglich vereinbarten Formerfordernisses ist für die Frage der Nichtigkeit der Vereinbarung der Wille der Parteien entscheidend. Wenn die bestimmte Form der Klarheit und zum Beweis dienen soll, so macht ein Mangel der Form die Vereinbarung nicht unwirksam.[30]

1.3.1.2 Schriftform

Gemäß § 126 BGB alter und neuer Fassung bedarf es zur Erfüllung des Schriftformerfordernisses zunächst der Verkörperung der Erklärung als Gedankenerklärung in Schriftzeichen, die auf einem gegenständlichen, räumlich abgrenzbaren Träger festgehalten ist und aus sich heraus wahrnehmbar ist – also einer Urkunde.[31] Fraglich war daher, ob eine digital gespeicherte Erklärung diese Voraussetzungen erfüllen kann. So war umstritten, ob sie die Voraussetzung der Verkörperung erfüllt, da diese ein Material voraussetzt, dass auf die optische Wahrnehmung durch den Adressaten abzielt und von einer bestimmten Dauer ist.[32] Digitale Dokumente sind nur als elektronische Impulse (*dots* und *bytes*) auf einem elektronischen Speichermedium ohne haptische Qualität vorhanden. Zur optischen Wahrnehmbarkeit muss die Computerdatei zumindest erst in den Arbeitsspeicher und auf den Bildschirm geladen werden.[33] In jedem Falle aber fehlt

---

BGB, die die Schriftform oder schriftliche Form verlangen, siehe bei Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, Bonn 2002, § 15, Rn. 6. Siehe Einsele in MüKo, § 126, Rn. 3, für eine Darstellung von Vorschriften in und außerhalb des BGB, die die Schriftform verlangen und sich auf § 126 BGB beziehen.

[28] So ist z.B. das Testament nicht nur schriftlich zu verfassen, sondern es verlangt auch die eigenhändige Abfassung der Erklärung, § 2247, muss aber andererseits nicht notwendig mit dem Namen unterzeichnet werden. Bei der Inhaberschuldverschreibung genügt ein bloßes Faksimile, § 793 Abs. 2 S. 2. Die Auflassung, § 925 BGB, oder der Ehevertrag, § 1410 BGB, bedürfen der gleichzeitigen Anwesenheit beider Teile bzw. die Mitwirkung eines Standesbeamten. Siehe bei Einsele in MüKo, § 125, Rn. 2.

[29] Im Zivilprozess sind von der Rechtsprechung zahlreiche Erleichterungen zugelassen worden, etwa die Einlegung bestimmender Schriftsätze, für die grundsätzlich die eigenhändige Unterzeichnung verlangt wird, durch Telefax oder mittels elektronischer Übertragung einer Textdatei mit eingescannter Unterschrift auf das Faxgerät des Gerichts. Siehe Darstellung bei Einsele in MüKo, § 126, Rn. 5.

[30] Heinrichs in Palandt, § 125, Rn. 10-13; Niemann, CLSR 2001, S. 28, 29.

[31] Der Begriff der Urkunde ist nicht legaldefiniert. Siehe Einsele in MüKo, § 126, Rn. 5 ff.; Fringuelli/Wallhäuser, CR 1999, S. 94; Heinrichs in Palandt, § 126, Rn. 2.

[32] Ausführliche Darstellung bei Fringuelli/Wallhäuser, CR 1999, S. 94/95, m.w.N. An die Dauerhaftigkeit der Fixierung können offenbar keine zu hohen Anforderungen gestellt werden, da dies selbst für ein Testament auf einer Schiefertafel angenommen wurde, siehe RG DJZ 15 (1910), S. 594 f.; Einsele in MüKo, § 126, Rn. 6.

[33] Zum Teil wird von einer Verkörperung ausgegangen, wenn die Erklärung auf Papier ausgedruckt ist, oder wenn sie in einem nicht-flüchtigen Speichermedium abgelegt ist, teilweise bereits dann, wenn die Erklärung wenigstens zeitweise in Form einer Datei vorliegt, in der sie auch transportiert werden kann. So bspw. Fringuelli/Wallhäuser, CR 1999, S. 94/95. Andere schließen deren Verkörperung grundsätz-

es an der Wahrnehmbarkeit aus sich selbst heraus. Für die Lesbarkeit eines digitalen Dokuments ist immer ein technisches Hilfsmittel notwendig und folglich das dann Lesbare nur ein Derivat.[34]

Daneben bedarf es zur Erfüllung der Schriftform auch der eigenhändigen Unterschrift des Ausstellenden. Aussteller der Urkunde ist derjenige, der die Erklärung in eigener Verantwortung abgibt.[35] Erklärung und Unterschrift müssen auf einer einheitlichen Urkunde vereint sein. Die Unterschrift muss auf die Urkunde aufgebracht werden und diese räumlich abschließen. Deshalb lässt die herrschende Meinung eine „Oberschrift" oder „Nebenschrift" nicht genügen.[36] Die Unterschrift nach § 126 BGB muss aber vor allem eigenhändig erfolgen. Dies schließt jede Form der mechanischen Vervielfältigung der Unterschrift durch Stempelaufdruck, Faksimile, mittels Schreibmaschine, Fernschreiber oder Telefax aus. Auch Telegramme sind nicht ausreichend für die gesetzliche Schriftform, auch nicht, wenn das Aufgabetelegramm eigenhändig unterzeichnet wurde.[37] So kann auch keine der mit Hilfe eines Computers zu erstellende „Unterschrift" dem § 126 BGB entsprechen.[38] Nur ausnahmsweise und laut einiger Sonderregelungen ist die vervielfältigte Unterschrift ausreichend[39] und nur vereinzelt hatten einige Regelungen bereits eine Abweichung von der Schriftform zugelassen.[40]

Gegenseitige, der Schriftform bedürfende Erklärungen müssen in Form eines eigenhändig unterschriebenen Dokuments übermittelt werden, § 126 Abs. 2 BGB. Eine Übermittlung in Form einer Kopie genügt hierfür nicht.[41] Für Verträge, für welche die Parteien die Schriftform vereinbart haben, gelten gemäß § 127 BGB nicht ohne weiteres die strengen Anforderungen des § 126 BGB. So war und ist anerkannt, dass auch der Austausch von Faxe ausreichte.[42] Für E-Mails war die Frage offen, auch hatte sich kein allgemeiner Brauch dahingehend entwickelt, dass Schriftformklauseln auch dann erfüllt sind, wenn die Verträge per E-Mail lediglich geändert werden.[43]

---

lich aus oder sehen sie spätestens durch die Übertragung der Erklärung aufgelöst, Deville/ Kalthegener, NJW-CoR 1997, S. 169.

[34] Fringuelli/Wallhäuser, CR 1999, S. 95.

[35] Einsele in MüKo, § 126, Rn. 12.

[36] Einsele in MüKo, § 126, Rn. 8, 9 und Rn. 10, nach der die Formwahrung durch eine „Ober-„ oder „Nebenschrift" nach der Verkehrssitte und nach den Gesamtumständen entschieden werden sollte.

[37] Einsele in MüKo, § 126, Rn. 14 m.w.N.

[38] Die Telefax-Rechtsprechung war hierauf nicht anwendbar; Fringuelli/Wallhäuser, CR 1999, S. 95/96.

[39] Z.B. § 793 Abs. 2 S. 2 BGB (Inhaberschuldverschreibungen), § 13 Aktiengesetz (AktG) (Aktien, Zwischenscheine), §§ 3 Abs. 1, 39 Abs. 1, 43 Nr. 4 Versicherungsvertragsgesetz (VVG) (Versicherungsschein, Mahnung, Prämienrechnung).

[40] So konnte z.B. gemäß § 408 Abs. 2 Handelsgesetzbuch (HGB) die eigenhändige Unterschrift durch Druck oder Stempel ersetzt oder die Schadensanzeige nach § 438 HGB auch mit Hilfe telekommunikativer Einrichtungen übermittelt werden. Die §§ 410 Abs. 1, 455 Abs. 1 und 468 Abs. 1 HGB verlangen Ausführung in Schriftform oder in sonst lesbarer Form, was die elektronische Form einschloss. Siehe Müglich, „Neue Formvorschriften für den E-Commerce", MMR 2000, S. 7-13, S. 9.

[41] Fringuelli/Wallhäuser, CR 1999, S. 96; Niemann, CLSR 2001, S. 29.

[42] Nach einer Entscheidung des OLG Frankfurt/M soll ein Fax-Schreiben sogar dann ausreichend sein, wenn vertraglich ein Einschreibebrief verlangt wird; Siehe bei Redeker, ITRB 2001, S. 47, m.w.N.

[43] Siehe bei Redeker, ITRB 2001, S. 48.

Aus den genannten Gründen können elektronisch erzeugte und übermittelte Erklärungen grundsätzlich die Voraussetzungen des § 126 Abs. 1 BGB nicht erfüllen. Elektronische Dokumente können zwar die Informations-, Kontroll- und Instruktionsfunktion unproblematisch erfüllen. Die Erfüllung der Warnfunktion aber wurde ihnen etwa wegen der schnellen Kommunikation über das Internet abgesprochen.[44] Ebenso die Fähigkeit, die Echtheits-, Identitäts- und Beweisfunktion unterschriebener Urkunden zu erfüllen, da es elektronischen Dokumenten oder Ausdrucken und Kopien von elektronischen Dokumenten an Originalität mangele.[45] Daher konnten nach deutschem Recht nur solche Verträge wirksam über das Internet geschlossen werden, die keiner besonderen Form bedürfen.[46] Entscheidungen der Rechtsprechung, in der ein „normales" E-Commerce-Geschäft betroffen und an Formvorschriften gescheitert ist, fehlen.[47]

1.3.1.3 Beweiszulassungs- und Beweiskraftregelungen

Die Darlegung und der Beweis der einen rechtlichen Anspruch stützenden Tatsachen sind entscheidend für dessen Durchsetzung. Die Frage der Beweislast richtet sich dabei nach dem materiellen Recht. Wie Beweis angeboten werden kann richtet sich für das Zivilrechtsverfahren nach der Zivilprozessordnung (ZPO).[48] Nach dem Grundsatz des Strengbeweises stehen den Parteien dabei vor Gericht nur bestimmte Beweismittel zur Verfügung, von denen der Urkundsbeweis einer ist.[49] Bei der Beurteilung der Beweismittel hat der Richter gemäß § 286 ZPO nach seiner freien Überzeugung zu entscheiden. Dieser Grundsatz der freien Beweiswürdigung wird nur durch bestimmte gesetzliche Beweisregeln beschränkt, § 286 Abs. 1 ZPO.[50] Solche Beweisregeln finden sich für Urkunden, weshalb deren Beweisfunktion von besonderer Bedeutung ist.[51] Der Urkundsbegriff der §§ 415 ff. ZPO ist ein anderer als der des BGB. Urkunden sind danach durch Niederschrift verkörperte Gedankenerklärungen, die geeignet sind, Beweis für streitiges Parteivorbringen zu liefern.[52] Besonderes Merkmal dieser Urkunde, auch Pri-

[44] Nöcker, CR 2000, S. 177, 179, 181.

[45] Nöcker, CR 2000, S. 179/181. Elektronische Dokumente können wegen der zwingenden schriftlichen Verkörperung auch keine Rechte verkörpern oder die Wertpapierfunktion übernehmen; ders., CR 2000, S. 181.

[46] Jansen, ICCLR Spe. 1999, S. 39. Tatsächlich sind für die typischen, geringwertigen Business-to-Consumer-Transaktionen (B2C-Commerce) kaum Formerfordernisse verlangt. Dies gilt für die große Mehrheit der im Internet geschlossenen Verträge; Niemann, CLSR 2001, S. 2; Redeker, ITRB 2001, S. 47.

[47] Siehe Redeker, ITRB 2001, S. 47, m.w.N., was heute noch Gültigkeit hat. Folglich muss die Behauptung, der E-Commerce sei ohne jegliche Änderung von Gesetzen erschwert, eingeschränkt werden. Derselbe, S. 46.

[48] Hoffmann, Mathis, „Der Beweiswert elektronischer Dokumente", DSWR 2006, S. 60-62, S. 60.

[49] Neben Augenschein, Zeugen, Sachverständigen und der Parteivernehmung, § 284 ZPO.

[50] Geimer, Reinhold in Zöller, *Kommentar zur ZPO*, 27. Auflage, 2007, vor § 415, Rn. 1; Hoffmann, DSWR 2006, S. 60.

[51] Fringuelli/Wallhäuser, CR 1999, S. 99.

[52] Geimer in Zöller, vor § 415, Rn. 2. Urkunde i.S.d. BGB ist die Verkörperung einer Gedankenerklärung in Schriftzeichen, die auf einem gegenständlichen, räumlich abgrenzbaren Träger festgehalten ist und aus sich heraus wahrnehmbar ist, siehe oben unter 1.3.1.2.

vaturkunde genannt, ist also wiederum die Verkörperung. Sofern Privaturkunden von ihren Ausstellern (eigenhändig) unterschrieben oder mittels notariell beglaubigten Handzeichens unterzeichnet sind, bieten diese Privaturkunden gemäß § 416 ZPO den vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen von den Ausstellern abgegeben sind. Auch eine Urkunde ohne Unterschrift taugt zum Beweis. Sie steht dann aber in ihrer Beweiskraft hinter der eigenhändig unterschriebenen zurück.[53] Ob die Urkunde echt ist, richtet sich nach den §§ 439, 440 ZPO.[54] Die Echtheit der Urkunde ist dabei vom Beweisführer zu beweisen. Ist sie bewiesen, heißt dies, dass der Aussteller den in der Urkunde verkörperten Inhalt erklärt hat. Die Beweislast für das Gegenteil trifft gemäß § 440 Abs. 2 ZPO dann die Gegenseite. Die Richtigkeit des Inhalts der Urkunde ist gemäß § 286 Abs. 1 ZPO durch das Gericht wie für jedes andere Beweismittel frei zu würdigen. Allerdings besteht eine tatsächliche Vermutung, dass die Erklärung richtig und vollständig ist. Voraussetzung hierfür ist wiederum die Echtheit des Dokuments, die gleichgesetzt wird mit der Echtheit der Unterschrift.[55]
Elektronische Dokumente weisen die genannten Urkundsmerkmale, insbesondere die Verkörperung der Gedankenerklärung, nicht auf. Sie können vor Gericht nur als Computerdatei auf einem entsprechenden Datenträger oder als papierner Ausdruck, mithin als Kopie, vorgelegt werden. Mangels Urkundseigenschaft i.S.d. §§ 415 ff. ZPO ist die Beweiskraftregelung des § 416 ZPO damit für sie ausgeschlossen.[56] Sie stellen gemäß § 371 ZPO lediglich Objekte des Augenscheins dar. Dieses Beweismittel Augenschein bezweckt die gegenständliche Wahrnehmung von Personen und Sachen.[57] Elektronische Dokumente, E-Mails oder die vorgenannten Kopien und Ausdrucke etc. sind damit als Beweismittel zugelassen, allerdings nur der freien Beweiswürdigung zugänglich. Es liegt im Ermessen des Gerichts über dessen Beweiswert zu befinden.[58]

1.3.1.4 Elektronische Dokumente und Signaturen im Rechtsverkehr vor den Neuregelungen

Nach herrschender Meinung und Rechtsprechung konnte nach alter Rechtslage keine mittels Computer erstellte „Unterschrift“, auch nicht die digitale Signatur, § 126 BGB genügen. Daran ändere auch die Einführung des Signaturgesetzes (SigG) a.F. nichts, da die Anwendung des Signaturverfahrens als tatsächlicher Vorgang mangels Verknüpfung der Sicherheitsstandards des SigG mit Rechtsfolgen und mangels Gleichsetzung mit der handschriftlichen Signatur nicht mit einer eigenhändigen Unterschriftsleistung gleichge-

[53] Redeker, ITRB 2001, S. 48. Darüber, ob der Inhalt der Urkunde wahr ist, trifft § 416 ZPO keine Aussage; Hoffmann, DSWR 2006, S. 60.

[54] Echt ist eine Privaturkunde, wenn sie von derjenigen Person stammt, von der sie nach der Behauptung des Beweisführers herrühren soll; Hoffmann, DSWR 2006, S. 60; Huber in Musielak, *Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz*, München 2007, §§ 439, 440.

[55] Huber in Musielak, § 440 Rn. 2, 3; Nöcker, CR 2000, S. 177.

[56] Hoffmann, DSWR 2006, S. 60; Nöcker, CR 2000, S. 177, 178; Redeker, ITRB 2001, S. 48.

[57] Die Abgrenzung des Augenscheinsobjekt zur Privaturkunde der §§ 415 ff. ZPO liegt im Merkmal der Verkörperung, die bei ersterem nicht gefordert ist; Geimer in Zöller, vor § 415, Rn. 2.

[58] Niemann, CLSR 2001, S. 28.

stellt werden konnte. Funktionsgleichheit zwischen elektronischer oder digitaler Signatur und der Unterschrift i.S.d. § 416 ZPO bestand nicht.[59] Über den Beweiswert digitaler Signaturen als Tatsachenbeweis[60] sollten ihre Qualitätsmerkmale entscheiden.[61]
Die Beweiseignung von elektronischen Dokumenten wie E-Mails veranschaulicht ein Urteil des Arbeitsgerichts Frankfurt a.M., in dem das Gericht mittels mehrerer zwischen den Parteien gewechselten E-Mails, die als Ausdruck vorgelegt worden waren, einen bestimmten Sachverhalt feststellte.[62] Allerdings waren der Austausch und der Inhalt der E-Mails hier nicht bestritten worden. Insgesamt wurde und wird die Beweiskraft elektronischer Dokumente und deren Ausdrucken als nicht besonders hoch eingestuft.[63] So zum Beispiel in einem Urteil des AG Bonn, das feststellte, dass E-Mail-Ausdrucke den Beweis für das Bestehen einer Vereinbarung in Abwesenheit weiterer Beweise nicht erbringen könnten, da E-Mail-Dateien manipulierbar seien.[64] Als Ausnahme kann ein Urteil des AG Hannover aus 1999 gelten, in dem die Vorlage einer Kopie der E-Mail, die das Sendeprotokoll erkennen lasse, sogar als Nachweis dafür genügen sollte, dass diese E-Mail von einer bestimmten Person versendet wurde.[65] Die ganz überwiegende Rechtsprechung verneinte dies jedoch schon damals. Die anfangs geäußerte Hoffnung, diejenigen, denen man Ausdrucke ihrer E-Mails präsentierte, würden deren Versand und Inhalt kaum bestreiten[66], hat sich als zumindest fraglich erwiesen. In einem Urteil aus 2001 wies das AG Erfurt[67] die Klage eines Verkäufers zurück, dessen angeblicher Kunde seine angebliche Bestellung bestritt. Dieser war über ein persönliches Passwort bei dem Verkäufer, einem Internetauktionshaus, gemeldet. Die Erklärung der Annahme des Vertragsangebots, hier das Gebot, erfolgte über eine E-Mail, deren angegebene Adresse dem Beklagten gehörte. Der Kläger habe keinen Anspruch auf den Kaufpreis, da er nicht habe beweisen können, dass es der Beklagte gewesen sei, der zum höchsten Gebot die Annahme erklärte. Der Ausdruck der fraglichen E-Mail, in der die E-Mail-Adresse des Beklagten genannt wurde, reiche zum Beweis nicht aus, eine Legitimationsprüfung könne hierüber nicht erfolgen. Auch die Tatsache, dass ein Passwort-Schutz

[59] Fringuelli/Wallhäuser, CR 1999, S. 95, 96; Nöcker, CR 2000, S. 178/179; Schumacher, CR 1998, S. 759,760. ausführliche Darstellung zum SigG a.F. siehe unten unter2.3.1 und 2.3.2.

[60] Tatsächlich hatten einzelne Gerichte Ausdrucke von elektronischen Dokumenten als Beweismittel akzeptiert; siehe bei Redeker, ITRB 2001, S. 48 und nachfolgend.

[61] Zur Beurteilung bedurfte es dabei eines Sachverständigen. Dumortier/van Eecke, CLSR 1999, S. 109, 110; Geis, MMR 2000, S. 669. Folglich wurde prognostiziert, digital signierte elektronische Dokumente würden von der Beweiskraft her wie unterschriebene Privaturkunden behandelt werden. Die freie Beweiswürdigung beschränkte sich dabei auf die Prüfung, ob in dem Gutachten von den richtigen Tatsachen ausgegangen, nicht offensichtlich die falsche digitale Signatur geprüft und ob die Vorschriften des Signaturgesetzes eingehalten wurden. Siehe bei Nöcker, CR 2000, S. 180/181.

[62] ArbG Frankfurt, Urt. v. 09.01.2002, 7 Ca 5380/01, JurPC Web-Dok. 125/2002, Abs. 1-10. Dieses sowie die nachfolgend hier genannten Urteile sind zumeist zu einem Zeitpunkt nach dem Erlass der unten (2.3) dargestellten Neuregelungen des SigG n.F. und der Formvorschriften ergangen, beziehen sich jedoch auf Sachverhalte die diesen zeitlich vorausgingen.

[63] Fringuelli/Wallhäuser, CR 1999, S. 99.

[64] AG Bonn, Urt. v. 25.10.2001, 3 C 193/01, NJW-RR 2002, S. 1363.

[65] AG Hannover, Urt. v. 20.12.1999, 518 C 13916/99, CR 2000, S. 854.

[66] so z.B. Redeker, ITRB 2001, S. 48.

[67] AG Erfurt, Urt. v. 14.09.2001, 28 C 2354/01, JurPC Web-Dok. 71/2002.

bestand, ändere die Beurteilung nicht. Ein Indiz dafür, dass es der Beklagte war, der das Gebot abgegeben habe, sei dies nicht. Als Grund wurde angeführt, dass jedermann an jedem Ort unter Verwendung der E-Mail-Adresse des Beklagten an der Internetauktion unter dem Namen des Beklagten teilnehmen könne, wenn ihm das Passwort bekannt sei.[68] Im vorliegenden Fall bestünden keine Hinweise auf Sicherheitskriterien für die Verwendung des Passworts. Grundsätzlich hätte dies also ein Dritter herausbekommen können. Das Internet selbst gewährleiste keine Sicherheit dergestalt, dass Dritte keinen Zugriff auf die entsprechenden Daten hätten. Das Gericht schloss daraus:

> *„Nach alledem ist davon auszugehen, dass eine ausreichende Legitimationsprüfung nicht stattgefunden hat, die es erlaubt, mit einer an Sicherheit grenzenden Wahrscheinlichkeit davon auszugehen, dass es der Beklagt gewesen ist, der das entsprechende Angebot abgegeben hatte."*

Nahezu zeitgleich entschied das LG Bonn[69] in einem vergleichbaren Fall, in dem ein Gebot per E-Mail über bei dem Internetanbieter „GMX" eingerichtete Adressen erfolgt war, bei denen der Beklagte mit Passwortschutz versehene E-Mail-Konten unterhielt. Unter Berufung auf die gleiche Begründung der Unsicherheit der elektronischen Kommunikation über das Internet urteilte das Gericht, die Klage sei abzuweisen,

> *„weil nicht feststeht, dass es der Beklagte war, der das Gebot ... unter der Bezeichnung ‚...' abgegeben hat. Die Beweislast hierfür liegt ... bei dem Kläger."*[70]

Hier wird das Prinzip der Beweislast deutlich: Bestreitet der angebliche Vertragspartner, hier der Bieter, dass die ihm zugeordnete E-Mail von ihm versandt beziehungsweise der Klick auf den entsprechenden Button von ihm gesetzt wurde, trifft den Anspruchsteller die Beweislast, den Nachweis für die bestrittene Tatsachenbehauptung zu erbringen. Ist dies nicht möglich und lassen sich die Tatsachen, etwa über ergänzende Beweise, nicht aufklären – sogenanntes non liquet –, treffen den Anspruchsteller die Nachteile der Beweislast und es droht der Prozessverlust. In der Literatur wurde und wird die Einschätzung zur mangelnden Beweiskraft elektronischer Dokumente ganz überwiegend geteilt.[71]

---

[68] Zutreffend hat es darauf hingewiesen, dass es bei vielen Anbietern in der Benutzermaske eine Voreinstellung gebe, in der der Verwender das Passwort, auch wenn es nicht lesbar ist, automatisch vermerken könne; AG Erfurt, JurPC Web-Dok. 71/2002.

[69] LG Bonn, Urt. v. 07.08.2001, 2 O 450/00, MMR 2002, S. 255, S. 256; bestätigt durch OLG Köln, Urt. v. 06.09.2002, 19 U 16/02, JurPC Web-Dok. 364/2002, Abs. 1-15.

[70] LG Bonn, MMR 2002, S. 256.

[71] Siehe Darstellung unten unter 2.3.2.

1.3.2 Formvorschriften im englischen Recht

Nach englischem Recht[72] bedarf es für einen rechtswirksamen Vertrag neben Angebot und Annahme[73] sowie dem Willen beider Parteien, sich rechtlich zu binden, in den allermeisten Fällen der *consideration*. Die vertraglich vereinbarte Leistung muss einem gewissen Gegenwert gegenüberstehen.[74] Die Bedeutung dieses Erfordernisses der *consideration* ist für die Frage der Wirksamkeit einer Vereinbarung vielfach größer als die der Form, die eine Vereinbarung hat.[75] Grundsätzlich sind Verträge nach englischem Recht formlos gültig. Formlose Verträge stellen die große Mehrzahl aller Verträge dar, einschließlich der meisten Kauf- und Miet-/Pachtverträge.[76] Ausnahmen von der Formfreiheit sind auch hier durch Gesetz festgeschrieben oder können vertraglich vereinbart werden.[77] Viele Verträge bedürfen der schriftlichen Form (*writing*) oder müssen andere Formvorschriften erfüllen, wie die Einfügung einer (handschriftlichen) Unterschrift oder Signatur (*signature*) oder die Bezeugung durch Dritte. Formvorschriften, insbesondere die schriftliche Form (*writing*), stellten in Bezug auf elektronische Kommunikation aber auch das englische Recht vor Probleme.[78]

1.3.2.1 Regelungsort und Ursprung

Das englische (Vertrags-)Recht ist als *common law* Richterrecht. Es beruht auf der Rechtsprechung der 1066 durch die Normannen eingerichteten kirchlichen Gerichte. Deren Zuständigkeit richtete sich nach der Wahl einer bestimmten Klageart. In hoch formalisierten Verfahren wurden Tatfragen erarbeitet und von einer Jury aus Laienrich-

---

[72] Grundlage dieses Vergleichs ist das Recht Englands. Soweit insbesondere in der Gesetzgebung vom Vereinigten Königreich (*United Kingdom*) die Rede ist, umfasst dies Großbritannien (bestehend aus England, Wales und Schottland) sowie Nordirland. England und Wales teilen eine gemeinsame Rechtsordnung, wobei für Wales seit 1998 eine eigene Nationalversammlung existiert, weshalb einzelne Gesetze (einschließlich des Electronic Communications Act, siehe unten 2.4.2) in Wales nur in geänderter Form zur Anwendung kommen. Die Gerichte in Schottland und Nordirland sind zwar, bei entsprechender Erstreckung der Gesetzgebung, durch die Gesetze des Parlaments des Vereinigten Königreichs (*United Kingdom Parliament*) gebunden. Die Rechtsordnungen Schottlands und Nordirlands sind aber, trotz vieler Übereinstimmungen, von der Englands und Wales verschieden. Das hier behandelte Recht findet daher in Schottland und Nordirland keine Anwendung. Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, Oceana Publications 2005, S. 639.

[73] Zur Besonderheit der Postal Rule, nach der es für eine wirksame Annahme genügt, wenn ein Annahmeschreiben ordnungsgemäß frankiert, adressiert und bei dem Beförderer (Post) abgegeben wird, ohne dass es darauf ankommt, ob der Anbieter die Annahme tatsächlich erhält (oder das Angebot in der Folge ablehnt), Downing/Harrington, „The Postal Rule in Electronic Commerce: A Reconsideration", Talley's Communications Law, Vol. 5, No. 2, 2000, S. 43-47.

[74] Für eine Einführung in das Vertragsrecht siehe: Bernstorff, S. 50 ff. Für eine ausführliche Darstellung des Erfordernisses und der Bedeutung der *consideration* siehe McKendrick, *Contract Law*, Basingstoke 2000, S. 79ff.

[75] McKendrick, S. 74, der ausführt, dass diese Regel der *consideration* – mehr noch als die Einhaltung einer bestimmten Form – der jeweiligen Vereinbarung das *„badge of enforceability"* verschaffe, sie also erst rechtlich durchsetzbar mache.

[76] Chissick, S. 54, 67; Murray in Edwards/Walden, S. 19.

[77] Chissick, S. 54, 67; McKendrick, S. 74 f.; York/Tunkel, S. 79, 80.

[78] Siehe nachfolgend 1.3.2.2 und Murray in Edwards/Walden, S. 19.

tern entschieden, wobei Beweisregeln die unangemessene Beeinflussung der Jury verhindern und eine gerechte Entscheidung sichern sollten. Das materielle Recht musste sich somit innerhalb dieser Formzwänge entwickeln, was eine Rezeption römischer Rechtsvorstellungen und damit eine Systematisierung des Rechts verhinderte. Als quasi Auflockerung des an vorangegangene Entscheidungen gebundene und damit teilweise zu ungerechten Entscheidungen führenden *common law* konnte ab dem 15. Jahrhundert in bestimmten Fällen der Kanzler (*Chancery*) angerufen werden, damit dieser kraft königlicher Prärogative dieses recht starre Recht lockerte und ergänzte, wo die Billigkeit dies erforderte (*equity*).[79] Auch die Einführung mehrerer *acts of parliament* hat diese Charakteristik nicht geändert, da Gesetze historisch betrachtet nur als zweitrangige Rechtsquelle angesehen werden.[80] Ein Gesetzeswerk, das – vergleichbar dem Allgemeinen Teil des BGB – Rechtsgeschäfte und damit auch die auf diese anwendbaren Formvorschriften allgemein gültig regelt, gibt es nicht. Vielmehr sind die Rechtsvorschriften, die für bestimmte Verträge eine besondere Form verlangen, und damit sowohl die Voraussetzungen von schriftlicher Form und Unterschrift als auch die Rechtsfolgen der Nichterfüllung, über mehrere Gesetzeswerke verstreut.[81] Zu beachten ist, dass es eine gesetzliche ausdrückliche Definition der *signature* bis zum Erlass der nachfolgend geschilderten neuen gesetzlichen Regelungen nicht gab.[82] Hinzu kommen durch die Rechtsprechung entwickelte Anforderungen, Definitionen, *rules* und *doctrines*. Das englische Recht als Richterrecht ist durch seine flexible und bisweilen schnelle Reaktion auf praktische Probleme geprägt, sowie durch die Betonung der Privatautonomie und Selbstständigkeit der Vertragsparteien. Folglich haben sich Formzwänge (ursprünglich) nur dort herausgebildet, wo sie sich als unabdingbar erwiesen. Es steht im vernünftigen Ermessen der Parteien, ob insbesondere ein schriftlicher Beweis nötig ist. Auch für den größten Teil des kommerziellen Handels ist dies eine Frage der Wahl.[83] Heutzutage finden sich deshalb nur dort Formerfordernisse, wo es neben der Warnung und dem Schutz der Parteien eines unbedingt sicheren Beweises bedarf.[84] Die Anzahl der Bezugnahmen in der Englischen Gesetzgebung auf Schriftform- und Unterschriftserfordernisse werden auf über 40.000 geschätzt, davon über 6.000, die eine *signature* verlangen.[85]

---

[79] Miedbrodt, „Unterschiede im Regulierungsverständnis der deutschen und der amerikanischen Rechtskultur“, in Bizer u.a. (Hrsg.), *Umbruch von Regelungssystemen in der Informationsgesellschaft, Freundesgabe für Alfred Büllesbach*, Stuttgart 2002, S. 273-282, S. 275, 276.

[80] Zum Beispiel der Sale of Goods Act 1893, nachträglich in abgeänderter Form erneut erlassen 1979 (er reguliert Aspekte des Verkaufs von Gütern und implizierter Garantien), Consumer Credit Act 1974 (er bietet eine Regelung für zwei- und dreiseitige Verbraucherkreditverträge), Unfair Contract Terms Act 1977 (um bestimmte unfaire Vertragsklauseln in Verbraucherverträgen zu vermeiden). Siehe York/Tunkel, S. 75; Miedbrodt in Bizer et al., S. 276, 280.

[81] Beispielsweise im Interpretation Act von 1978 oder dem Copyright, Designs and Patents Act von 1988.

[82] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 654.

[83] Dort seien schriftliche Beweise nahezu unvermeidbar vorhanden. Auch entschieden sich die Parteien dort, wo Verpflichtungen großen Werts eingegangen werden und damit Streitwerte großer Höhe entstehen, von sich aus für eine akkurate Aufzeichnung. Vergleiche bei Downes, S. 136/137.

[84] Downes, S. 136/137.

[85] Diese finden sich in so unterschiedlichen Gesetzen wie dem Statute of Frauds 1677, dem Bills of Exchange Act von 1882, dem Law of Property Act von 1925, dem Consumer Credit Act von 1974, dem Companies Act von 1985, dem Law of Property Act (Miscellaneous Provisions) Act von 1989 u.v.m. Lloyd, S. 578; York/Tunkel, S. 80; *Mason, Electronic Signatures in Law*, S. 14.

Die Unterschrift (*signature*) wird gesetzlich dort gefordert, wo nur signierte Dokumente als Beweis zugelassen sind oder sie eine Beweisvermutung schaffen, etwa hinsichtlich ihres Inhalts, ferner dort wo die Unterschrift zum Zwecke der Authentifizierung verlangt wird oder sie zur Durchsetzung eines gesetzlichen Rechts erforderlich ist.[86] Formerfordernisse zu missachten kann dazu führen, dass der Vertrag nicht durchsetzbar, weil vor Gericht nicht beweisbar, oder völlig nichtig ist.[87] Eine besondere Form des Vertrages beziehungsweise der Schriftlichkeit ist das *deed*, durch dessen besondere Form auch solche Vereinbarungen rechtswirksam werden, die keine *consideration* bieten, und das deshalb für bestimmte Verträge vorgeschrieben ist.[88]

1.3.2.2 Erfordernis, Definition und Formen des Writing

Es ist zu unterscheiden zwischen dem Erfordernis, dass ein Vertrag *in writing* abgeschlossen werden, und dem, dass er *in writing* bewiesen werden muss. Im ersten Fall betrifft dies die Wirksamkeit des Vertrages selbst[89], im zweiten Fall lediglich den Beweis seiner Existenz. Der Vertrag ist dann unter Umständen nicht durchsetzbar.[90] Wo das *in writing*-Erfordernis nur dem Beweis dient, braucht jedoch nicht ein einziges, den gesamten Vertragsinhalt enthaltendes Dokument vorgelegt werden. Vielmehr genügt es, eine Reihe von Dokumenten vorzubringen, die zum Beispiel über mündliche Zeugenaussagen miteinander verbunden sind.[91] Der Civil Evidence Act 1995 definiert Dokument (*document*) in § 13 als

> *„alles, in dem Informationen einer Beschreibung* [information of any description]* *aufgezeichnet sind, und ‚Kopie' bezeichnet in Bezug auf ein Dokument al-*

[86] Mason, *Electronic Signatures in Law*, S. 14.

[87] Chissick, S. 80, 81.

[88] Beispielsweise für die Verpachtung einer Immobilie für mehr als zehn Jahre, §§ 52 und 54 Abs. 2 Law of Property Act 1925. Die Hauptfunktion der Ausführung des Vertrages als deed war es, die consideration und den Rechtsbindungswillen der Parteien festzuhalten. Sofern also eine Vereinbarung die formellen Voraussetzungen eines deeds erfüllt, ist sie rechtlich verbindlich, auch ohne consideration, siehe bei York/Tunkel, S. 79, 80; Jewell, S, 65/66. Heutzutage dient das deed, ähnlich der notariellen Beurkundung im deutschen Recht, etwa dazu, den Parteien die rechtliche Verpflichtung vor Augen zu führen und Rechtssicherheit zu schaffen. Gemäß § 1 Law of Property (Miscellaneous Provisions) Act 1989 müssen folgende Voraussetzungen erfüllt werden: Das *deed* muss durch die Person oder Personen unterzeichnet werden, die es aufsetzt oder aufsetzen; es muss durch einen Zeugen bezeugt, auf seiner Vorderseite als deed gekennzeichnet und es muss ausgehändigt oder übergeben (*delivered*) werden. Unter *delivery* wird eine Handlung verstanden, durch die der Aussteller des deeds seinen Willen, durch das deed unwiderruflich gebunden zu sein, zum Ausdruck bringt. Jewell, S, 65.

[89] Z.B. Verträge über den Grundstücksverkauf, § 2 Law of Property (Miscellaneaous Provisions) Act 1989; bestimmte Verbraucherkreditverträge, § 62 Consumer Credit Act 1974; *bills of sale*, §§ 4 und 8 Bills of Sale Act 1878; Übertragung von Urheber- und anderen Rechten an geistigem Eigentum, § 90 Abs. 3 Copyright, Designs, and Patents Act 1988.

[90] Shears/ Stephenson, S. 227; Jewell, S. 70.

[91] Shears/Stephenson, S. 228.

* Begriffe und Erläuterungen in […]-Klammern kennzeichnen Einfügungen durch den Verfasser. Sie werden nachfolgend insbesondere in übersetzten Textpassagen eingesetzt. Sie sollen durch einen direkten Vergleich mit dem Originaltext oder dort, wo mehrere Begriffe als Übersetzung in Frage kommen, das Verständnis erleichtern.

> *les auf das die im Dokument aufgezeichnete Information kopiert wurde, ungeachtet der eingesetzten Mittel und der direkten oder indirekten Aufzeichnung oder Kopie.*[92]

Die Civil Procedure Rules 1998 enthalten eine Definition des *documents*, die nahezu identisch ist.[93] Die Betonung der Aufzeichnung eines Inhalts deutet dabei auf das (übliche) Anbringen eines Textes, also Schriftzeichen, auf Papier hin.[94] Weitere gesetzliche Definitionen bezeichnen Art und Material des Speichermediums[95], wobei der Finance Act 1993 ausdrücklich den Begriff Computer einführt:

> *„… 'Dokument' schließt Dokumente jedweder Art ein und insbesondere Aufzeichnungen, die mittels eines Computers aufbewahrt werden."*[96]

Im *common law* wurde die Bedeutung des Dokuments auf dessen Beweisfunktion beschränkt. Schon 1908 wurde in *R v. Daye* bestimmt, dass Begriff und Bedeutung des Dokuments nicht eng auszulegen seien:

> *„Ich möchte behaupten, dass jede geschriebene Sache* [written thing]*, die als Beweis taugt, zutreffend als Dokument zu beschreiben ist und dass es unerheblich ist, worauf die Schrift* [the writing] *aufgebracht ist."*[97]

Tonbänder wurden als *discoverable*[98] *documents* akzeptiert, wobei das Dokument über dessen Qualität, unabhängig von der Art der Informationsvermittlung des Speichermediums, definiert wurde[99], so dass heute jedes Medium darunter fällt.[100] Der Begriff Aufzeichnung wird in der Mehrzahl der gesetzlichen Vorschriften derart verwendet, dass er digitale Informationen einschließt, auch wenn einzelne Vorschriften die Aufbewahrung

---

[92] § 13 Civil Evidence Act 1995: *„… anything in which information of any description is recorded, and 'copy' in relation to a document, means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirect."*

[93] Teil 31, § 4: *„… anything in which information of any description is recorded, and a copy is, in relation to a document, … anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirect."*

[94] Mason, *Electronic Signatures in Law*, S. 9.

[95] Mason, *Electronic Signatures in Law*, S. 9, m.w.N.

[96] § 40 Finance Act 1993: *„… 'document' includes a document of any kind whatsoever and, in particular, a record kept by means of a computer."*

[97] *„I should myself say that any written thing capable of being evidence is properly described as a document and that it is immaterial on what the writing may be inscribed."* Richter Darling in *Re v. Daye*, [1908], 2 KB 333.

[98] *Discovery* bezeichnet die Offenlegung/Bekanntgabe von Urkunden, siehe Collin et al.; *PONS Fachwörterbuch Recht: Englisch-Deutsch, Deutsch-Englisch*, Stuttgart/Düsseldorf/Leipzig 1998, S. 110: Danach ist *discovery* die Eröffnung der Dokumente der beiden Parteien für die jeweils andere Partei bevor eine Verhandlung vor einem Zivilgericht beginnt.

[99] *Grant v. Southwestern and Country Properties Ltd.*, [1975] Ch 185.

[100] Mason, *Electronic Signatures in Law*, S. 10.

der Aufzeichnungen als *hard copy* verlangen.[101] Die Definitionen des *instrument* als einem Dokument oder einer Urkunde nehmen regelmäßig Bezug auf Dokumente, die wiederum nicht notwendig digitale Informationen ausschließen. Der Forgery and Counterfeiting Act 1981 bezieht sich in § 8 Abs. 1 sogar ausdrücklich auf digitale Informationen.[102]

Es gibt eine Reihe von gesetzlichen Vorschriften, die *evidence in writing* verlangen, so etwa das Statute of Frauds von 1677, welches in Teilen bis heute fort gilt. Durch das Erfordernis des schriftlichen Beweises soll vermieden werden, dass ein Gericht durch betrügerische Aussagen zu falschen Schlussfolgerungen gebracht wird.[103] Bezogen auf elektronische Kommunikation beschrieb Richter Pelling in *Mehta v. J. Perreira Fernandes SA* den Zweck des Statute of Frauds mit dem Schutz davor, an einer formlosen Erklärungen festgehalten zu werden, da diese ohne die notwendige Abwägung und *consideration* vorgenommen worden oder ausdrücklich mehrdeutig gewesen sein könne oder von der Gegenseite missbräuchlich behauptet werde.[104] Der Interpretation Act 1978 enthält in § 1 eine Definition der schriftlichen Form (*writing*). Danach umfasst *writing*

> *„Maschinenschreiben, Drucken, Lithographie und andere Verfahren, Worte in sichtbarer Form zu präsentieren oder zu vervielfältigen; auf die schriftliche Form Bezug nehmende* [referring to writing] *Ausdrücke sind entsprechend zu interpretieren"*[105]

Diese Betonung der sichtbaren Form (*visible form*) schließt zunächst Informationen in digitalem Format aus.[106] Sie konnten allenfalls einbezogen werden, wenn sie unter die genannten „*andere*[n] *Verfahren, Worte in sichtbarer Form zu präsentieren oder zu vervielfältigen"* fielen.[107] Fraglich war deshalb, ob nur in digitaler Form vorliegende Dokumente, wenn sie auf einen Computerbildschirm geladen und so sichtbar sind, diesen Voraussetzungen entsprechen.[108] Hier ist eine parallele zum deutschen Recht zu

---

[101] Siehe Mason, *Electronic Signatures in Law*, S. 12, und die in den vorgenannten § 13 Civil Evidence Act 1995 und Teil 31 § 4 Civil Procedure Rules enthaltenen Definitionen.

[102] Mason, *Electronic Signatures in Law*, S. 12, 13.

[103] Bernstorff, S. 52, Fn. 130. Heute wird insbesondere für den Garantievertrag der Beweis in schriftlicher Form verlangt. Der *Law Reform (Enforcement of Contracts) Act* von 1954 hat das Schriftformerfordernis für Warenverkaufverträge abgeschafft. Siehe Bernstorff, a.a.O.; Downes, S. 141.

[104] *Mehta v. J. Perreira Fernandes SA* [2006] 1 WLR 1543, [2006] EWHC 813 (Ch): *„The purpose of the statute of frauds is to protect people from being held liable on informal communications because they may be made without sufficient consideration of expressed ambiguously or because such a communication might be fraudulently alleged against the party to be charged."*

[105] Interpretation Act 1978, § 1: *„Writing includes typing, printing, lithography, photography and other modes of presenting or reproducing words in a visible form, and expressions referring to writing are construed accordingly."*

[106] York/Tunkel, S. 91, 92, die daher die Definitionen der schriftlichen Form (*writing*) und auch der Unterschrift (*signed*) als veraltet bezeichnen.

[107] Mason, *Electronic Signatures in Law*, S. 11.

[108] Siehe bei Griffith, David Hugh und Harrison, Jouel, in Campbell, Dennis, *E-Commerce and the Law of Digital Signatures*, Oceana Publications 2005, S. 644, 645, die ausführen, dass elektronische Kommunikation während der Übertragung nur vorübergehend und mittels elektronischen Impulsen bzw. mittels

erkennen, wo bei der Urkunde die Fähigkeit der Wahrnehmbarkeit aus sich selbst heraus für elektronische Dokumente abgelehnt wurde.[109] Vergleichbar wurde hier mehrheitlich eingewandt, dass digitale Kommunikation als Serie elektronischer Impulse nicht das vom Interpretation Act geforderte Kriterium der Sichtbarkeit oder Wahrnehmbarkeit erfülle.[110] Bis zum Inkrafttreten des Electronic Communications Act 2000 gab es auch kein einschlägiges Fallrecht zu diesen Problemfeldern, so dass die Rechtsunsicherheit diesbezüglich fortbestand.[111] In einem 2001 veröffentlichten Bericht äußerte die Law Commission[112] die Ansicht, dass E-Mail und der Handel über Websites (*website trading*) generell die im Interpretation Act enthaltene Definition des *writing* erfüllen können.[113] E-Mails und Websites seien beide für die Parteien sichtbar, und zwar über den Bildschirm des Computers. Es genüge, wenn die Datennachricht zu irgendeinem Zeitpunkt sichtbar sei.[114] Dagegen wird eingewandt, dass die Tatsache, dass die Information nur zu bestimmten Zeitpunkten sichtbar sei, zu anderen jedoch nicht, nämlich dann, wenn sie gerade nicht auf dem Bildschirm erscheinen, nicht mit dem Willen des Gesetzgebers vereinbar sei, wo dieser *„Verfahren, Worte in sichtbarer Form zu präsentieren“* gefordert habe.[115] Es sei auf die Funktion des writing abzustellen, eine gewisse Aufzeichnung der Information zu erreichen, die ein nur vorübergehendes Sichtbarmachen nicht erfülle.[116]

Lichtimpulsen bestünden und üblicherweise mittels magnetisch polarisiertem Material oder „pits“ auf optischen Medien gespeichert würden.

[109] Siehe unter 1.3.1.4 und 2.3.2.

[110] Murray in Edwards/Walden, S. 20. Nach einer Ansicht konnte dies zwar noch einer weiten Auslegung dieser Definition entsprechen, da diese Vertragsvereinbarungen auf eine Diskette etc. gespeichert oder ausgedruckt werden könnten; so York/Tunkel, S. 80. Die gleichen Einwände gelten auch für den Click-Wrap-Vertrag wenn lediglich ein „Ich akzeptiere“-Button aktiviert wird und dabei diejenigen Links nicht beachtet und nicht aufgerufen werden, auf denen sich die (ausführlichen) Vertragsbedingungen befinden; siehe bei York/Tunkel, S. 80.

[111] Chissick, S. 81. Vorgeschlagen wurden u.a. zwei Herangehensweisen: nicht auf die Fixierung der Information auf einen Träger abzustellen, sondern zwischen informeller mündlicher Übermittlung und formell aufgezeichneter Information zu unterscheiden; oder das Erfordernis der Schriftlichkeit oder schriftlichen Form (*writing*) ausschließlich als Beweiserfordernis zu sehen. Siehe Darstellung bei Mason, *Electronic Signatures in Law*, S. 11, der einwendet, dass zum einen hinsichtlich der verwendeten Technologie keine Unterscheidung zwischen informeller und formeller Nutzung besteht, und zum anderen darauf hinweist, dass laut Rechtsprechung das Angebot mündlicher Beweise (*oral evidence*) den Mangel der Form nicht beheben kann.

[112] Die Law Commission wurde durch den Law Commissions Act 1965 ins Leben gerufen mit dem Ziel, die Reform des Rechts voranzutreiben.

[113] Nicht jedoch der elektronische Datenaustausch (electronic data interchange), siehe The Law Commission, „Electronic Commerce: Formal Requirements in Commercial Transactions – Advice from the Law Commission”, Dezember 2001, www.lawcom.gov.uk/docs/e-commerce.pdf, S. 8, 9.

[114] The Law Commission, „Electronic Commerce: Formal Requirements in Commercial Transactions – Advice from the Law Commission”, S. 9-11.

[115] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 645, 646.

[116] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 646. Ebenso wenig könne dies weitere Funktionen der schriftlichen Form erfüllen, wobei die Autoren auf die im Modellgesetz zum Elektronischen Geschäftsverkehr (siehe dazu oben 1.2 und unten 2.6.1 zum Modellgesetz) genannten Funktionen verweisen.

Eine Erweiterung der Definition von *writing*, um digitale Dokumente einzubeziehen, fand sich dagegen bereits im Copyright, Designs and Patents Act 1988, der *writing* definiert als:

> *„jede Form von Zeichen oder Code, ob handschriftlich oder auf andere Weise, und ohne Ansehung der Methode oder des Mediums durch die oder in dem es aufgezeichnet ist.“*[117]

1.3.2.3 Erfordernis und Definition der Signature

Grundsätzlich verlangt das englische Recht nicht das Signieren von Verträgen, auch nicht wenn sie der schriftlichen Form bedürfen. Dennoch werden signierte Verträge häufig genutzt und gefordert. Dies folgt aus dem Prinzip, dass der Unterzeichner eines Vertrages später nicht dessen Existenz oder Inhalt bestreiten kann.[118] Beispielsweise muss bei einem nicht signierten Vertrag der Kläger beweisen, dass die Gegenpartei um den tatsächlichen Vertragsinhalt wusste. Dies ist bei einem signierten Vertrag nicht nötig, da dann

> *„sofern kein Betrug oder... arglistige Täuschung vorliegt, die unterschreibende Vertragspartei gebunden ist, wobei es völlig unerheblich ist, ob sie das Dokument gelesen hat oder nicht.“*[119]

Als primäre (Beweis-)Funktion der Signatur gilt im englischen Recht ihre Funktion als verkörperter (*tangible*) und vertrauenswürdiger (*reliable*) Beweis von Zustimmung (*approval*) zum und Übernahme (*adoption*) des Inhalts eines Dokuments durch den Unterzeichnenden, ferner als Beweis des Rechtsbindungswillens des Unterzeichnenden in Bezug auf den Inhalt des Dokuments und der Erinnerung des Unterzeichnenden an die Bedeutsamkeit und Notwendigkeit des Akts der Unterzeichung.[120] Die Unterschrift kann, als sekundäre (Beweis-)Funktion, die Identität der unterzeichnenden Person authentifizieren, indem sie etwa die kausale Verbindung zwischen Unterschrift und dem auf einem Dokument angeführten Namen bestätigt. Daneben kann die Existenz eines (unterschriebenen) Dokuments unter anderem als Beweis einerseits des Willens des Unterzeichnenden, andererseits der Originalität und Vollständigkeit sowie der Unverfälschtheit des Dokumentes selbst dienen.[121]

---

[117] Copyright, Designs and Patents Act 1988, s.178: „*… any form of notation or code whether by hand or otherwise and regardless of the method by which, or medium in or on which, it is recorded.*“

[118] *Smit International Singapore Pte Ltd v. Kurnia Dewi Shipping SA (The Kurnia Dewi)* [1997] 1 Lloyd’s Rep 552.

[119] *„… in the absence of fraud, or … misrepresentation, the party signing is bound, and it is wholly immaterial whether he has read the document or not.*“ So Scrutton L.J. in *L’Estrange v. Graucob* [1934] 2 K.B. 394.

[120] Mason, *Electronic Signatures in Law*, S. 20.

[121] Mason, *Electronic Signatures in Law*, S. 20, 21.

Eine allgemeingültige gesetzliche Definition des Begriffs der Unterschrift oder Unterzeichnung (*signature*) gibt es im englischen Recht nicht[122], insbesondere nicht im Interpretation Act 1978. Existierende Definitionen der *signature* bezeichnen diese als Faksimiles einer Unterschrift oder Unterzeichnung, unabhängig vom Prozess der Wiedergabe. Dies umfasst Reproduktionen, Abschriften, Abdrucke, Ab- und Nachbildungen der Unterschrift, einschließlich der Wiedergabe der Unterschrift in einem elektronischen Format.[123] Insgesamt haben die Gerichte bei der Frage der Wirksamkeit der Unterschrift auf die Intention der Parteien abgestellt. Gleich welche Form eine Signatur hatte, haben die Gerichte die hinter der Verwendung der Signatur stehende Absicht für maßgeblich befunden. Folglich ist die Funktion, die eine Signatur ausübt, mindestens so bedeutsam, wenn nicht sogar bedeutsamer, als ihre Form. Aufgrund dieser Verschiebung der Bedeutsamkeit der Form einer Unterschrift zu deren Funktion wurden zunehmend andere Formen der Signatur als die handschriftliche Unterschrift als *signature* akzeptiert und ist die Bandbreite möglicher Formen der Signatur groß.[124]

1.3.2.4 Formen der Signature

Das Prinzip der Signierung geht aus vom Aufbringen des Namens oder einer Identifizierungsmarke beziehungsweise -zeichens (*identifying mark*) auf ein Dokument.[125] Dass die Signatur vertrauenswürdig oder schwer zu fälschen ist, ist dabei keine Voraussetzung.[126] So wurden in England beispielsweise Initialen als ausreichende Zeichen für, jedenfalls als Beweis für den Vertragsschluss, und als *signing* gemäß Statute of Frauds zugelassen.[127] Auch in juristischen Verfahren, für Testamente und für Rechtsgeschäfte über Grundeigentum wurden Initialen als *signature* anerkannt.[128] Ebenso der bloße Nachname in Bezug auf das Statute of Frauds, da sich der Unterzeichner durch seinen Nachnamen im Urkundstext identifiziert habe, siehe Lord Denham in *Lobb and Knight v. Stanley:*

> *„… ist es eine Unterschrift der Partei, wenn sie die Urkunde* [the instrument] *durch das Schreiben ihres* [Nach-]*Namens auf die Urkunde authentifiziert. … Ich denke, mehr ist nicht notwendig"*[129]

[122] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 654.

[123] Mason, *Electronic Signatures in Law*, S. 13, 14, m.w.N.

[124] Mason, *Electronic Signatures in Law*, S. 22, 25, 30.

[125] Mason, *Electronic Signatures in Law*, S. 30-33, m.w.N.

[126] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 654.

[127] *Phillimore v. Barry*, 1 Camp, S. 512; 170 ER, S. 1040 (bzgl. Beweis des Vertragsschlusses) und *Chichester v. Cobb* (1866), 14 L.T.N.S., S. 433 (bzgl. *signature*).

[128] *R v. Morais* [1988] 3 All ER, S. 161, CA (*judicial use*) und *R v. Avery*, 21 LJQB, S. 430 (*voting*); *Re Savory's Goods*, 15 Jur, S. 1042 (*wills*); *Hill v. Hill* [1947], 2 NZLR, S. 398 (CA) (*rights in property*).

[129] *„… it is a signature of the party when he authenticates the instrument by writing his* [sur-]*name in the body. … I think more is not necessary"*, *Lobb and Knight v. Stanley* (1844), 5 QB S. 574, S. 581.

Und bestätigend, unter Bezugnahme auf die Namensnennung am Beginn des Urkundstextes, Richter Coleridge:

> *„Ist es nicht ausreichend, wenn eine Partei am Anfang des Dokuments ihren Namen schreibt, damit es auf das Nachfolgende angewendet wird? Nutzt sie dann nicht ihren Namen als Unterschrift?“*[130]

Für Vertragszwecke wurde die Verwendung von Handelsnamen (*trade names*) als ausreichend angesehen, bei Testamenten (*wills*) auch unvollständige Unterschriften, etwa in einem Fall, in dem die Erblasserin während der Unterzeichnung verstarb[131], und andere Bezeichnungen als Namen, bspw. „Deine Mutter“.[132] Beide letztgenannten Entscheidungen stützten sich auf eine Aussage Lord Campbells in *Hindmarch v. Carlton*, wonach

> *„entweder der Name vorliegen muss oder ein Zeichen* [a mark]*, das* [nach dem Willen des Unterzeichnenden] *den Namen wiedergeben beziehungsweise repräsentieren soll.“*[133]

Gleiches soll für Abkürzungen von Namen[134] oder sonstige identifizierende Bezeichnungen[135] gelten:

> *„Unterschrift* [signature] *bedeutet nicht notwendig das Schreiben des Vor- und Zunamens, sondern ein Zeichen, das aufzeigt, dass es die Handlung dieser Partei ist.“*[136]

Auch die Verwendung geruckter (*printed*) Namen wurde als ausreichend zur Erfüllung der Erfordernis des *signing* des Statue of Frauds gewertet. Durch den Abdruck des Namens beispielsweise auf einer Rechnung[137] oder einem Auftragsbuch (*order book*)[138] sind die Partien hinreichend kenntlich gemacht worden, um dem Statute of Frauds zu entsprechen. Ein Grund hierfür liegt an der Berücksichtigung der Handelsbräuche und -

---

[130] *„Is it not enough if a party, at the beginning of a document, writes his name so as to govern what follows? Does he not then use his name as a signature?”*, S. 582.

[131] Wobei für die Formwirksamkeit von Testamenten gem. dem Wills Act 1837 die Bezeugung der Unterschrift durch Dritte notwendig ist, vorliegend also weitere (Zeugen-)Beweise vorlagen; *Re Chalcraft's Goods* [1948], P, S. 222.

[132] *Re Cook's Estate Murison v. Cook* [1960] 1 All ER, S. 689, wobei auch hier *additional evidence* vorhanden war. Siehe auch Mason, *Electronic Signatures in Law*, S. 51-54.

[133] *Hindmarch v. Carlton* (1861) 8 HL Cas, S. 160, 167.

[134] Siehe Darstellung bei Mason, *Electronic Signatures in Law*, S. 55, 56.

[135] Z.B. *Selby v. Selby* (1817) 3 Mer 2; 36 ER 1 (*„the most affectionate of mothers“*) in Bezug auf das Statute of Frauds.

[136] Richter Maule in *Morton v. Copeland* (1855) 16 C B, S. 516, 535: *„Signature does not necessary mean writing a person's Christian and surname, but a mark which indicates it as the act of the party.“*

[137] *Schneider v. Norris* (1814) 2 M & S, S. 237; 105 ER, S. 388.

[138] Sarl v. Bourdillon, 1 C.B. (N.S.), S. 188 ; 140 ER, S. 79.

gepflogenheiten durch die englischen Gerichte.[139] Auf der gleichen Grundlage wurde in *Tourret v. Cripps* auch ein nicht unterschriebenes, aber handschriftlich aufgesetztes Annahmeschreiben auf ein Pachtverlängerungsangebot auf einem mit einem Briefkopf des Verfassers versehenen Dokument für rechtswirksam erklärt. Es stand dabei zur Überzeugung des Gerichts fest, dass die Handschrift vom Verfasser stammte und dieser den Brief auch abgesendet hatte. Folglich schloss das Gericht daraus, dass der Verfasser die Absicht hatte, das Angebot anzunehmen und dass sein im Briefkopf gedruckter Name diese Absicht bestätigte (*to authenticate*).[140] Gleiches galt für das Unterschriftserfordernis gemäß § 266 Public Health Act 1875, die durch den Abdruck des Namens (*printed name*) des *town clerk* (etwa als Verwaltungspräsident zu übersetzen) auf einem gedruckten Formular als erfüllt beurteilt wurde. Auch wenn das Gesetz eine *signature* fordere, so sei eine handschriftliche Unterschrift dafür nicht erforderlich:

> *„… alles was erforderlich war, war dass die Mitteilung als vom* [town clerk] *stammend bestätigt* [authenticated] *wurde, und das geht aus der Mitteilung hinreichend hervor.“* [141]

Diese Beurteilung wurde in *Goodman v. J. Eban Limited* von Lord Justice Romer bekräftigt indem er weiter ausführt, dass der Empfänger der Nachricht die Authentizität der Mitteilung mittels Bestätigung dessen Inhalts durch den Absender (hier der *town clerk*) hätte feststellen können.[142] Dieser Entscheidung wurde in *Ringham v. Hackett* gefolgt, in dem ein Partner einer Gesellschaft einen Scheck unterschrieb, auf dem der Name der Gesellschaft gedruckt war. In dem Urteil über die Klage gegen den anderen Partner bemerkte Lord Justice Lawton:

> *„Ein von einer geschriebenen Unterschrift begleiteter gedruckter Name ist ein Beweis des ersten Anscheins* [prima facie evidence] *dafür, dass der Scheck von dem Konto abgezogen wurde, dass er angibt.“*[143]

In *Central Motors (Birmingham) Ltd. v. P.A. & S.N.P. Wadsworth* stellte Lord Justice Slade ebenfalls fest, dass eine Unterschrift nicht auf das handschriftliche Schreiben des Namens (*manuscript writing of the name*) beschränkt sei und dass es möglich sei, die Identität einer Firma aus deren gedrucktem (*printed*) Namen auf einem Scheck abzulei-

---

[139] Mason, *Electronic Signatures in Law*, S. 65.

[140] *Tourret v. Cripps* (1879) 48 L J Ch, S. 567; 27 WR, S. 706.

[141] *Bridges (Town Clerk of Cheltenham) v. Dix* (1890-91) 7 TLR, S. 215, 216(a): *„… all that was necessary was that the notice should be authenticated as coming from the town clerk, and that sufficiently appeared in this notice.”*

[142] *Goodman v. J. Eban Ltd.* [1954] 1 QB, S. 550, 564; [1954] 2 WLR, S. 581, CA.

[143] *„A printed name accompanied by a written signature was prima facie evidence that the checque was being drawn on the account it purported to be drawn on“*, *Ringham v. Hacket* (1980) 124 SJ, S. 201. Während angenommen werden könne, dass der auf dem Scheck gedruckte Kontoname das Konto der Gesellschaft (des Kontoinhabers) bezeichne, folge daraus jedoch nicht, dass die Unterschrift bestätigt (*authorized*) worden sei, S. 201.

ten.[144] Vergleichbar wurden auch Signaturen in Form lithographierter Namen (*lithographed names*) von den Gerichten anerkannt.[145] Insbesondere aber wurde in der Rechtsprechung der Gebrauch von (Gummi-)Stempeln zur Signierung unter den verschiedenen *signature*-Erfordernissen behandelt. Hier zeigen sich besonders die Unterschiede zum Schriftform und Unterschriftserfordernis des § 126 BGB, das jegliche mechanische Vervielfältigung oder Hilfsmittel ausschließt.[146] In England wurde im Fall einer Mittels Stempels signierten Urkunde zur Ergänzung (*codicil*) eines Testaments dies als hinreichende Signatur anerkannt:

> *„Ob das Zeichen* [the mark] *mittels Stift oder durch ein anderes Instrument erstellt wird, kann nun keinen Unterschied machen, noch kann es dem Grunde nach einen Unterschied machen, dass ein Faksimile des vollständigen Namens auf das Testament aufgebracht wird anstelle eines bloßen Zeichens oder eines X.“*[147]

Die Form der Signatur war unerheblich aufgrund vorliegender Beweise über die Umstände des Aufbringens des Stempels, die nachwiesen, dass der Erblasser sich durch den Inhalt der Ergänzungen (*codicils*) rechtlich binden wollte.[148] In einem Fall, in dem es um die Verwendung eines Stempels mit eingraviertem Faksimile der üblichen Unterschrift des Unterzeichnenden für Zwecke einer nach dem Voters Registration Act 1843 erforderlichen *signature* ging, wurde ähnlich argumentiert:

> *„Die übliche Art des Aufbringens einer Unterschrift* [signature] *auf ein Dokument ist nicht diejenige allein per Hand, sondern mittels mit einem Werkzeug* [instrument] *wie einem Stift oder Füllfederhalter verbundener Hand. Ich sehe keinen Unterschied zwischen dem Einsatz eines Stifts oder Füllfederhalters und dem Einsatz eines Stempels, sofern durch die eigene Hand des Unterzeichnenden ein Abbild auf das Papier aufgebracht wird.“*[149]

---

[144] *Central Motors (Birmingham) Ltd. v. P.A. & S.N.P. Wadsworth*, [1982] CAT 231, May 28, 1982; (1983) 133 NLJ 555 Court of Appeal (Civil Division).

[145] R v. Cowper (1890) 24 QBD 60, 533 CA, Firmenname in lithographierter Form auf einem *county court bill*.

[146] Siehe oben unter1.3.1.2.

[147] Sir Cresswell in *Jenkins v. Gainsford and Thring*, (1863) 3 Sw & Tr, S. 93, 96; 164 ER 1208; (1862-63) 11 WR 854: *„Now, whether the mark is made by a pen or by some other instrument cannot make any difference, neither can it in reason make a difference that a fac-simile of the whole name was impressed on the will instead of a mere mark or X.“*

[148] *Jenkins v. Gainsford and Thring*, (1863) 3 Sw & Tr, S. 93; 164 ER 1208; (1862-63) 11 WR 854; Mason, *Electronic Signatures in Law*, S. 73.

[149] *Bennett v. Brumfitt* (1867-68) 3 LRCP, S. 28, Richter Bovill, S. 31: *„The ordinary mode of affixing a signature to a document is not by the hand alone, but by the hand coupled with some instrument, such as a pen or pencil. I see no distinction between using a pen or a pencil and using a stamp, where the impression is put upon the paper by the proper hand of the party signing.“*

Entscheidend sei, dass ein persönliches Handeln des Unterzeichnenden vorliege. hinsichtlich der Einzigartigkeit (*genuineness*) einer Unterschrift sei nicht einzusehen, warum eine Unterschrift

> *„… durch eine per Stift angefertigte Signatur besser authentifiziert werde als durch die Abbildung des Stempels, der durch die eigene Hand des Unterzeichners aufgebracht wird.“*[150]

Auch für richterliche Unterschriften wurde der Gebrauch von Stempeln als Unterschrift auf richterlichen Beschlüssen grundsätzlich anerkannt.[151] Bemerkenswerte Urteile und Begründungen ergingen gerade auch zur Verwendung von Stempeln als Unterschrift hinsichtlich des *signature*-Erfordernis des Statute of Frauds. In *Goodman v. J. Eban Limited* wurde geurteilt:

> *„Wo ein Parlamentsgesetz verlangt, das ein bestimmtes Dokument durch eine Person ‚unterschrieben' werden muss, ist, prima facie, dieses gesetzliche Erfordernis erfüllt, wenn diese Person eine Darstellung ihrer Unterschrift mittels eines Gummistempels, auf dem diese eingraviert ist, auf das Dokument aufbringt. … Das wesentliche Erfordernis der Unterschrift ist es, seinen Namen oder seine ‚Signatur' anzufügen, ob durch das Schreiben mittels eines Füllfederhalters oder eines Stiftes oder ein sonstiges Einprägen auf das Dokument.“*[152]

Hintergrund war die Verwendung des Stempels mit einer Abbildung einer Unterschrift auf einer Kostenrechnung. Zwar sei die Unterschrift unter einer Kostenrechnung mittels eines Gummistempels grundsätzlich nicht wünschenswert, und ein solcher Gummistempel stelle nicht per se eine Unterschrift dar.[153] Unter Berücksichtigung der *authority* (Rechtsprechung) und der Funktion, die eine Unterschrift erfüllen soll, müsse jedoch die Verwendung des Gummistempels im Ergebnis als Unterschrift zum Zwecke der Authentifizierung des Schreibens gewertet werden. Ein Argument war, dass der Empfänger, hätte er die Authentizität der Unterschrift angezweifelt, er sich diese durch Nachfrage bestätigen lassen können.[154] Dieses Argument ist der Diskussion in Deutschland gänzlich fremd. Ein weiteres Argument, dass in diesen Fällen im *common law* vielfach für die Nutzung von Stempeln angeführt wird, ist die Erleichterung durch Zeiter-

---

[150] *Bennett v. Brumfitt* (1867-68) 3 LRCP, S. 28, Richter Keating, S. 32: *„… is better authenticated by a signature by means of a pen than by means of an impression of stamp affixed by the party's own hand."*

[151] *Blades v. Lawrence* (1873-74) 9 LRQB, S. 374 ; (1874) 43 LJR QB, S. 133.

[152] „*Where an Act of Parliament requires that any particular document be 'signed' by a person, then prima facie, the requirement of the Act is satisfied if the person himself places on the document an engraved representation of his signature by means of a rubber stamp… The essential requirement of signing is the affixing in some way, whether by writing with a pen or pencil or by otherwise impressing upon the document, one's name or 'signature' so as personally to authenticate the document.*" Lord Denning in *Goodman v. J. Eban Limited* [1954] 1 Q.B. S. 550, S. 557.

[153] Richter Evershed, S. 554, Lord Justice Romer, S. 563.

[154] Lord Justice Romer, S. 564.

sparnis und die Möglichkeit der einfachen Repetierbarkeit.[155] Dieses Bedürfnis nach Erleichterung des Rechtsverkehrs ist in Deutschland auch erkannt worden und war mit ausschlaggebend für die Einführung der Textform, wird jedoch nicht im Zusammenhang mit den Formerfordernissen der §§ 125 ff. BGB genannt. In *Re United Canso Oil & Gas Ltd.* wird dazu dagegen festgehalten:

> *„Heutige Geschäfte könnten nicht durchgeführt werden, wenn gestempelte Unterschriften nicht als rechtlich bindend anerkannt würden. Das Aufbringen eines Stempels vermittelt genauso wirksam die Absicht, durch das so ausgeführte Dokument gebunden zu sein, wie es die handschriftliche Unterschrift* [the manual writing of a signature by hand] *tut.“*[156]

Hier zeigt sich erneut die Bedeutung der Absicht zu authentifizieren, die, ihr Vorliegen zum Zeitpunkt des Signierens festgestellt, zur Wirksamkeit dieser Form der Signatur führen kann. Ähnlich fällt das Urteil bezüglich zu signierender Verwaltungsakte in *British Estate Investment Society Ltd. v. Jackson (H M Inspector of Taxes)* aus:

> *„… ist dies ein Fall, … in dem die Unterzeichnung mittels einer gestempelten Signatur korrekt* [proper] *ist, da jedermann weiß, dass diese Art von* [Commissioners] *mit einer großen Zahl an Dokumenten beschäftigt ist, und es wäre eine beschwerliche Bürde, wenn diese alle durch den* [Commissioner] *selbst unterschrieben werden müssten.“*[157]

Ebenfalls als Erleichterung verschaffendes technisches Mittel wurde die Schreibmaschine und damit Maschinen geschriebene Unterschriften von den Gerichten anerkannt. Dabei wird zudem die Bedeutung deutlich, die das *common law* den ergänzenden Beweisen zumisst. So wurde regelmäßig Beweis für die Tatsache verlangt, dass die Person, deren Name auf dem Dokument getippt (*typed*) wird, diesen Maschinen geschriebenen Namen als ihre Unterschrift anbringen beziehungsweise annehmen wollte.[158] Unterstützend könnte hier außerdem die sogenannte *authenticated signature fiction*, ein

---

[155] Lord Denning hatte dagegen gerade die Art der vielfache, wiederholte Verwendung des Stempels in *Goodman v. J. Eban Limited* aufgrund Bequemlichkeit und der Arbeitserleichterung kritisiert und darauf bestanden, dass die betreffende Person die Unterzeichnung (hier das Aufbringen durch den Stempel) eigenhändig vornehmen müsse, damit bewiesen sei, dass sie dem Dokument die nötige persönliche Aufmerksamkeit geschenkt hat. Kritisch: Mason, *Electronic Signatures in Law*, S. 78.

[156] Richter Hallett in *Re United Canso Oil & Gas Ltd.* (1980) 12 B.L.R. 130; 76 A.P.R. 282; 41 N.S.R. (2d), 282 (T.D.), S. 289: *„Today's business could not be conducted if stamped signatures were not recognized as legally binding. The affixing of a stamp conveys the intention to be bound by the document so executed just as effectively as the manual writing of a signature by hand.“*

[157] Richter Danckwerts in *British Estate Investment Society Ltd. v. Jackson (H M Inspector of Taxes)* (1954-1958) 37 Tax Cas, S. 79, S. 86; [1954] TR 397; 35 ATC 413; 50 R & IT 33: *„… this is a case, … in which the signing by means of a stamped signature is proper, because everybody knows that Commissioners of this kind have to deal with numerous documents, and it is an onerous duty if they have to be signed by the writing of the Commissioner himself.“* Siehe auch *Fitzpatrick v. Secretary of State for the Environment* [1990] 1 PLR 8, CA.

[158] Mason, *Electronic Signatures in Law*, S. 8-90, mit zahlreichen Hinweisen auf insbesondere Rechtsprechung in den USA (dazu nachfolgend unter 1.3.3.4 und 1.3.3.6).

aus dem neuseeländischen Recht stammendes Rechtsinstitut (*rule*), angeführt werden. Danach kann eine nur von einer Partei unterschriebene Urkunde dennoch als ausreichend signiert gelten, wenn die Namen beider Parteien, wenn auch in gedruckter oder Maschinen geschriebener Weise, im Urkundstext enthalten sind.[159] Auf das englische Recht bezogen soll diese Regel nur dann eingreifen, wenn die Partei, gegen die ein Anspruch geltend gemacht werden soll, oder ihr Vertreter den zugrunde liegenden Vertrag aufgesetzt hat und der Vertrag deren Name in geschriebener oder gedruckter Form enthält, durch diese Partei oder ihren Vertreter an die andere Partei zur Unterzeichnung zwecks Vertragsabschluss versendet wurde und entweder durch das Dokument oder durch begleitende Umstände bewiesen ist, dass das Dokument von niemandem anderen als derjenigen Partei unterschrieben werden sollte, der es zugesandt wurde.[160]
Die flexible Reaktion des *common law* auf den Einsatz neuer Technologien zeigt auch die Anerkennung von per Telegramm erstellten Unterschriften dar. Telegramme, deren Inhalt elektronisch per Morsecode über Kabel übermittelt wurde, waren seinerzeit auch für den Abschluss oder die Bestätigung von Verträgen gebräuchlich, ebenso wie später Telexe.[161] In *Godwin v. Francis* wurde entschieden, dass die Annahme eines Grundstückkaufangebots per Telegramm, zusammen mit weiterer Korrespondenz, ausreichend war, um die Voraussetzungen des Stature of Frauds zu erfüllen. Die Unterschrift des Telegrafensekretärs wurde dabei als ausreichende *signature* anerkannt. Richter Bovill:

> *„Ich bin bereit zu entscheiden, dass das bloße Telegramm,* [aus-]*geschrieben und unterschrieben wie vom Telegraphensekretär vorgezeigt, eine ausreichende Unterschrift gemäß dem Statute of Fraud ist."*[162]

In *McBlain v. Cross*, in dem eine in einem Telegramm enthaltene Unterschrift ebenfalls als ausreichend gemäß dem Statute of Fraud angesehen wurde, wurde dies im Hinblick auf neue Technologien und die Notwendigkeit, das Recht entsprechend auszulegen, wie folgt begründet:

> *„Wenn wir nicht dies als rechtswirksam* [to be the law] *ansähen, würde der Nutzen, den die elektronische Telegraphie der Menschheit geschenkt hat, in großem Maße untergraben."*[163]

---

[159] Illustriert im neuseeländischen Fall *Bilsland v. Terry*, [1972] NZLR 43, in dem eine Vereinbarung über den Verkauf von Land zwar beide Namen der Parteien im Urkundstext enthielt, jedoch nur die handschriftliche Unterschrift einer der Parteien – und dennoch als unterschrieben i.S.d. § 2 Contracts Enforcement Act 1956 galt. Ausführlich siehe Mason, *Electronic Signatures in Law*, S. 86, 87 m.w.N.

[160] So Richter Wilson im neuseeländischen Fall Stuart v. McInnes [1974] 1 NZLR 729, unter Verweis auf Rechtsprechung in England, u.a. auf *Tourret v. Cripps* (1879) 48 L J Ch, S. 567; 27 WR, S. 706 (s.o.).

[161] Mason, *Electronic Signatures in Law*, S. 90, 91.

[162] *„I am prepared to hold that the mere telegram written out and signed in the way indicated by the telegraph clerk, if done with the authority of the vendors, would have been a sufficient signature within the Statute of Frauds."*, *Godwin v. Francis* (1870) LR 5 CP 295; 22 LT Rep NS 338.

[163] *McBlain v. Cross* (1872) LT 804: *„If we did not hold such to be the law, the convenience which the modern invention of electric telegraph has bestowed upon mankind would be in a great measure subverted."*

Um also als unpraktikabel oder nicht wünschenswert erkannte Rechtssituationen zu vermeiden, wurde die Auslegung der *signature* von den Gerichten den tatsächlichen und wirtschaftlichen Gegebenheiten entsprechend ausgeweitet. Eine legislative Anpassung, wie es in kodifizierten Rechtssystemen erforderlich oder auch nur der Tradition entspräche, wurde verzichtet. Diese Herangehensweise bestimmt auch die Bewertung von Telex-Nachrichten. In *Clipper Maritime Ltd. v. Shirlstar Container Transport Ltd., The Anemone*, in dem es um einen Vertragsschluss ging, der teilweise in Telexen festgehalten war, wurde festgestellt, dass die Umstände, in denen die fraglichen Telexe ausgetauscht wurden, bewiesen, dass ein Vertrag bestand. In diesem Rahmen stellte Richter Staughton fest, dass die Rückantwort (*answerback*) des Versenders eines Telexes eine Unterschrift darstellt, während dies bei der Rückantwort des Empfängers nicht der Fall sei, da letztere lediglich das Dokument authentifiziere und nicht die Zustimmung zu dessen Inhalt ausdrücke.[164] Auch eine per Telefax übermittelte Kopie der Signatur erfülle das Unterschriftserfordernis, da es keinen Grund gebe, weshalb einigen Methoden des *„impressing the mark on paper"* eine größere Rechtswirkung zukommen solle als anderen, siehe *Re a debtor* aus dem Jahr 1995.[165] Dennoch wurde das Problem angesprochen, dass die Natur des Dokuments durch die Übermittlung verändert wird und diese Kommunikationsform die Möglichkeiten für Verfälschungen (*fraud*) erhöht. Zugrunde lag ein Fall, in dem eine Vollmachtsurkunde (*proxy form*), die gemäß § 8.2 Abs. 3 der Insolvency Rules 1986 unterschrieben werden muss, zum entscheidenden Zeitpunkt nur per Fax übermittelt worden war. Der Distriktrichter hatte die Formwirksamkeit der Urkunde verneint. Ohne sich auf direkte Präzedenzfälle (*direct authority*) stützen zu können, erkannte Richter Laddie in der nächsten Instanz:

> *„… in der überwiegenden Mehrheit der Fälle in denen der* [Vorsitzende] *... eine Vollmachtsurkunde* [proxy form] *erhält, wird das Formular eine Unterschrift aufweisen, die er nicht erkennen kann und die unleserlich sein mag. Authentizität könnte dann nur dadurch gefördert werden, dass der sich hinreichend identifizierende* [Gläubiger] *das Formular in Anwesenheit des* [Vorsitzenden] *unterschreibt. Selbst dann besteht die Möglichkeit der Irreführung."*[166]

Die Funktion der Unterschrift sei es dabei, *„zu zeigen, aber nicht notwendig zu beweisen, dass das Dokument vom* [Gläubiger, Unterzeichnenden] *persönlich geprüft und bestätigt wurde."*[167] Hierzu führt er weiter aus:

---

[164] *Clipper Maritime Ltd. v. Shirlstar Container Transport Ltd., The Anemone*, [1987] 1 Lloyd's Rep., S. 546, 556.

[165] *Re a debtor (No. 2021 of 1995), Ex p, Inland Revenue Commiccioners v. The debtor; Re a debtor (No. 2022 of 1995), Ex, Inland Revenue Commissioners v. The debtor* [1996] 2 All E.R. 1208, S. 345, 351

[166] *Re a debtor* (s.o.), S. 351 (b-c): *„… in the overwhelming majority of cases in which the chairman … received a proxy form, the form will bear a signature which he does not recognise and may well be illegible. Authenticity could only be enhanced if the creditor carrying suitable identification signed the form in person in the presence of the chairman. Even there the possibility of deception exists."*

[167] *Re a debtor* (s.o.), S. 351 (d): *„… the function of a signature is to indicate, but not necessarily prove, that the document has been considered personally by the creditor and is approved by him."*

> *„Man kann sagen, dass eine bestimmende* [qualifying] *Unterschrift aus zwei Bestandteilen besteht. Erstens enthält sie die erforderlichen Informationen, um den* [Gläubiger] *zu identifizieren … und, zweitens, die Unterschrift, die oben ausgeführte Funktionen erfüllt. Wenn der* [Vorsitzende] *eine Vollmachtsurkunde erhält, die eine angebliche Unterschrift enthält* [what purports to be a signature]*, so ist er berechtigt, diese als echt zu behandeln sofern nicht andere Umstände auf das Gegenteil hinweisen.“*[168]

Grund hierfür sei, dass durch die Übermittlung per Fax der Inhalt des Formulars übersandt wurde und damit auch die Unterschrift. Das Empfängerfaxgerät werde tatsächlich durch den Absender instruiert, dessen Unterschrift auf der Vollmachtsurkunde zu reproduzieren, die ihrerseits durch das Empfängergerät kreiert wird, mit der Folge, dass

> *„… nach meiner Ansicht das empfangene Fax eine vom* [Gläubiger] … *unterschriebene Vollmachtsurkunde ist.“*[169]

Selbst in Fällen, in denen die Signatur digitalisiert und danach dem Fax beigefügt wird, so dass das Fax die erste verkörperte Kopie dieses Dokuments darstellt, soll dieses Dokument als signiert gelten.[170] Im gleichen Jahr erging eine Entscheidung zur Verwendung von *tested telexes* zwischen Banken, bei denen immerhin eine Methode der Authentifizierung des Inhalts der Übermittlung angewendet wird. Auch hier wurden die so übermittelten Dokumente als echt und verlässlich (*authentic and reliable*) bewertet, solange der Empfänger nicht von Tatsachen Kenntnis habe, die auf das Gegenteil hinweisen.[171] In *PNC Telecom plc v. Thomas* wurde in 2003 eine per Telefax übermittelte Einladung zu einer außerordentlichen Gesellschafterversammlung, die laut § 368 Companies Act 1985[172] der Gesellschaft an ihrem Sitz in originaler, ursprünglicher Form (*to be genuine*) zugehen und dort aufbewahrt werden muss, als rechtswirksam beurteilt. Zur Vertrauenswürdigkeit dieser Übermittlungsmethode führt Richter Sir Andrew an:

> *„… ist dem Fax nichts eigen, das es mehr oder weniger verlässlicher machte als die* [Brief-]*Post. Es ist wahr, dass ein Fax durch Einfügungen und Löschun-*

---

[168] *Re a debtor* (s.o.), S. 352 (d-e): *„It may be said that a qualifying proxy form consists of two ingredients. First, it contains the information required to identify the creditor and … and, secondly, the signature performing the function set out above. When the chairman receives a proxy form bearing what purports to be a signature, he is entitled to treat it as authentic unless there are surrounding circumstances which indicate otherwise.“* Dabei bezog Richter Laddie dies ausdrücklich nur auf Teil 8 der Insolvency Rules 1986.

[169] *Re a debtor* (s.o.), S. 351 (h): *„The receiving fax is in effect instructed by the transmitting creditor to reproduce his signature on the proxy form which itself being created at the receiving station. It follows that, in my view, the received fax is a proxy form signed by the principal or…“*

[170] *Re a Debtor* (s.o.), S. 351.

[171] *Standard Bank London Ltd. v. Bank of Tokyo Ltd.* [1995] CLC 496; [1996] 1 C.T.L.R. T-17; Mason, *Electronic Signatures in Law*, S. 102.

[172] Der Companies Act 1985 wurde im Rahmen der Neuregelungen (siehe unten 2.4) durch den Companies Act 1985 (Electronic Communication) Order geändert, um elektronische Zustellungen u.a. zu ermöglichen. Diese Änderungen betrafen jedoch nicht § 368.

gen gefälscht werden kann, aber Betrug und Verfälschung ist, gewöhnlich durch andere Mittel, bei postalischer oder persönlicher Übermittlung gleichermaßen möglich.“[173]

Damit wurde die Idee der Signierung auf ihre Authentifizierungsfunktion reduziert. Leitbild ist die Bestätigung und Billigung, nicht die physische Manifestation der Unterschrift. Entscheidend ist demnach der Wille des Unterzeichnenden, zuzustimmen und zu authentifizieren.[174] Weitere Fälle im *case law* anderer *common law*-Staaten bestätigen diese Beurteilung in Bezug auf neue Technologien.[175] Die zu Telegramm, Telex und Telefax genannten Fälle zeigen jedoch, dass bei Verwendung solcher neuen Technologien nach dem *case law* zunehmend die Verantwortlichkeit des Empfängers eine Rolle spielt, die gesamten Umstände der zur Authentifizierung eingesetzten Mittel zu berücksichtigen.[176] Diese Bedeutung ergänzender Beweise in Bezug auf den Willen einer Partei zur Authentifizierung eines Dokumentes belegt auch die Bereitschaft englischer Gerichte, mündliche Bestätigungen beziehungsweise Authentifizierungen anstelle der Unterschrift als rechtswirksam gelten zu lassen. So wurde in *Smith v. Neale*[177] die mündliche Bestätigung eines schriftlichen Vertragsangebots, das nur von der anderen Partei unterzeichnet war, als wirksam gemäß § 4 des Statute of Frauds beurteilt. In *Ellis v. Smith* wurde, widerwillig, die mündliche Anerkennung der eigenen Handschrift auf einem Testament gegenüber einem Zeugen der Testamentsaufsetzung als der Unterschrift gleichwertig anerkannt.[178] Die Gerichte waren sogar bereit, Verträge, die der Unterschrift bedürfen aber von keiner Partei (handschriftlich) unterschrieben waren, als wirksam zu erklären. In *Rist v. Hobson*[179] kam das Gericht sogar zu der Einschätzung, dass es bei Vorliegen einer schriftlichen Vereinbarung vermutet werden könne, dass Dokument sei unterschrieben worden, solange nicht Beweis für das Gegenteil beigebracht würde. In *Bleakley v. Smith*[180] genügte ein allein von einer Partei aufgesetztes Vertragsdokument, um dem Statute of Frauds zu genügen, da es von dieser Partei eigenhändig geschrieben worden war und diese auch den Kaufpreis von der anderen Partei erhalten hatte. In all diesen Fällen waren hinreichende Beweise für den entsprechenden Willen der Parteien, den Inhalt der Dokumente anzunehmen (*to adopt*), vorhanden. Daher

---

[173] *PNC Telecom plc v. Thomas* [2003] BCC 202, [2004] 1 BCLC 88, [2002] EWHC 2848, 2002 WL 31676421: *„... there is nothing inherent in a fax transmission to make it more or less reliable than the post. It is true that a fax may be falsified by a cut and paste operation but forgery and falsification is equally possible, usually by other means, in connection with postal and personal transmission too.“*

[174] Chissick, S. 83.

[175] Siehe z.B. Darstellung bei Mason, *Electronic Signatures in Law*, S. 25 ff., m.w.N.

[176] Mason, *Electronic Signatures in Law*, S. 102, der dies insbesondere auch auf elektronisch übersendete Dokumente bezieht.

[177] *Smith v. Neale*, 2 C.B. (N.S.) 67; 140 ER 337.

[178] *Ellis v. Smith* (1754) 1 Ves Jun 11; 1 Ves Jun Supp 1; 30 ER 205; 34 ER 666; Präzedenzfall für *Ellis v. Smith*: *Gryle v. Gryle* (1741) 2 Atk 176; 26 ER 509, in dem allein ergänzende Beweise für die Authentifizierung des Testaments ausschlaggebend waren. Ähnlich im neueren Fall *Weatherhill v. Pearce* [1995] 2 All ER 492, Ch D.

[179] *Rist v. Hobson* (1824) 1 Sim & St 543; 57 ER 215.

[180] *Bleakley v. Smith* (1840) 11 Sim 149, 49 ER 831

konnte, obwohl die Formerfordernisse nicht erfüllt waren, der Inhalt der Dokumente als authentifiziert gelten.[181]

1.3.2.5 Beweiszulassungs- und Beweiskraftregelungen

Nach englischem Recht sind Beweismittel durch das Gericht zuzulassen. Die Bedeutung von Verfahrensvorschriften im *common law* wurde eingangs bereits dargestellt.[182] Das Verfahren der Einzelentscheidung muss danach geeignet sein, zu einem gerechten Ergebnis zu gelangen, was am besten dadurch erreichen lässt, indem man den Parteien gestattet in einer „kämpferisch-agitatorischen" Bemühung ihre jeweiligen Standpunkte bewusst einseitig geltend zu machen. Dabei soll der Richter im Wesentlichen nur über die Einhaltung der Verfahrensregeln wachen (*adversary procedure*).[183]
Was digitale Dokumente betrifft, so hat das Gericht in *Derby & Co. Ltd. v. Weldon* entschieden, dass eine Computerdatenbank (rechts-)gültiges Dokument der Offenlegung oder Bekanntgabe (*valid document for discovery*) ist, *„sofern sie Information enthält, die abgerufen und in lesbare Form gebracht werden kann"*[184] Danach ist ein Dokument in elektronischer Form in gleichem Maße als Beweis zulässig (*admissible*) wie jede andere Form des Beweises.[185] Eine weitere Erleichterung brachte der Civil Evidence Act 1995, mit dem das Erfordernis gestrichen wurde, ein Dokument müsse im Original, in schriftlicher Form, vorgelegt werden, um als Beweismittel zugelassen zu werden. § 8 zum Beweis von in Dokumenten enthaltenen Aussagen:

> *„(1) Wo eine in einem Dokument enthaltene Aussage als Beweis zugelassen werden soll, muss diese bewiesen werden:*
> *(a) durch die Vorlage dieses Dokuments, oder*
> *(b) unabhängig von der Existenz dieses Dokuments durch Vorlage einer Kopie dieses Dokuments oder seines wesentlichen Teils,*
> *durch eine vom Gericht bestimmte Methode authentifiziert.*
> *(2) Die Anzahl der Lücken auf der Kopie im Vergleich zum Originalist ist unbeachtlich."*[186]

---

[181] Mason, *Electronic Signatures in Law*, S. 115.

[182] 1.3.2.1

[183] Miedbrodt in Bizer et al., S. 280.

[184] „*… so far as it contains information capable of being retrieved and converted into readable form*." *Derby & Co. Ltd. v. Weldon (No. 9)* [1991] 1 WLR, S. 652, 654.

[185] *Derby & Co. Ltd. v. Weldon (No. 9)* [1991] 1 WLR, S. 652, 658A-B; Gemäß dem Civil Evidence Act 1995 ist eine Computerdatei als Beweismittel zugelassen, wenn *„es ein Teil der Aufzeichnungen eines Geschäfts ist und ein Organ dieses Geschäfts (oder Unternehmens) eine Bestätigung seiner Authentizität erbringt." („… forms part of the records of a business and an officer of the business provides certificate of its authenticity")*, siehe bei Hoeren, *Grundzüge des Internetrechts – E-Commerce/Domains/Urheberrecht*, München 2002, S. 201.

[186] § 8 Civil Evidence Act 1995, *„Proof of statements contained in documents. (1) Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved: (a) by the reproduction of that document, or (b) whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such manner as the court may*

Authentication (Authentifizierung) bezeichnet den Vorgang, in dem das Gericht davon überzeugt werden muss, dass ein Dokument dasjenige ist, was es zu sein vorgibt, in dem der Ursprung einer Signatur bewiesen wird und die Tatsache, dass das Dokument nicht nachträglich geändert wurde. Dies kann geschehen durch Beibringung von Zeugen- und anderen Beweisen wie etwa Beweise die Technologie der Aufzeichnung und Bearbeitung von Informationen betreffend.[187] Die Tatsache, dass eine Datennachricht nicht als Original vorliegt, kann dabei jedoch nach allgemeinen Beweisregeln des englischen Rechts dessen Beweiswert mindern.[188]
Sowohl handschriftliche als auch elektronische Signaturen sind hier als *factual evidence* anerkannt und nicht per se von der Beweiswürdigung ausgeschlossen.[189] Handschriftliche Unterschriften oder Signaturen (*manuscript signatures*) können nach englischem Recht nur in bestimmten Fällen angefochten werden (*to be disputed* oder *challenged*). Das ist zum Beispiel der Fall, wenn die Unterschrift eine Fälschung ist, sie aufgrund besonderer Umstände nicht als Handlung des Unterzeichners gelten kann, wenn eine der Parteien dem Schriftstück (*writing*) nach Unterzeichnung durch die andere Partei einseitig wesentliche Regelungen hinzufügt, oder wenn die signierende Partei keine Kenntnis davon hatte, ein Vertragsdokument zu unterzeichnen.[190] Die auf die Echtheit der Unterschrift vertrauende Partei muss dann zunächst beweisen, dass die auf dem entsprechenden Dokument aufgebrachte oder darin enthaltene Unterschrift diejenige des angeblichen Unterzeichnenden (*signatory*) ist.[191] Ist dieser Beweis, beziehungsweise der Beweis der Ähnlichkeit der Unterschrift mit der des Unterzeichnenden, erbracht, muss der (angebliche) Unterzeichnende beweisen, dass diese Unterschrift eine Fälschung ist.[192] Darüber hinaus muss der Beweis dafür geführt werden, dass der Unterzeichnende den Willen zur Unterzeichnung des Dokuments und zu dessen Authentifizierung und Annahme hatte.[193]

---

approve. (2) It is immaterial for this purpose how many removes there are between a copy and the original." Wobei Dokument gemäß § 13 Civil Evidence Act 1995 alles, auf dem Information jeder Beschreibung aufgezeichnet ist, bedeutet.

[187] Mason, *Electronic Signatures in Law*, S. 458.

[188] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S: 665. Vergleich das deutsche Recht hierzu: Da elektronische Dokumente keine Urkunde i.S.d. §§ 415ff. ZPO sind, kann nach deutschem Recht die Vorlage des „Originals" nicht verlangt werden, weshalb hier die Verwendung elektronischer Dokumente als Beweis im Gerichtsverfahren nicht durch ein etwaiges Erfordernis, das Original vorzulegen, behindert wird; Heydn, Truiken J. in Campbell, Dennis, *E-Commerce and the Law of Digital Signatures*,Oceana Publications, 2005, S. 259, 260.

[189] Geis, „Die elektronische Signatur: Eine internationale Architektur der Identifizierung im E-Commerce", MMR 2000, S. 667-674, S. 669; Dumortier/van Eecke, „Electronic Signatures – The European Draft Directive on a Common Framework for Electronic Signatures", CLSR, S. 106-112, S. 109.

[190] Mason, *Electronic Signatures in Law*, S. 16, m.w.N. zur Rechtsprechung.

[191] Hierfür ist ein Abgleich mit Referenz-/Vergleichsunterschriften des (angeblich) Unterzeichnenden erforderlich, u.U. mittels Sachverständigenschriftgutachten; Mason, *Electronic Signatures in Law*, S. 17, 18.

[192] Mason, *Electronic Signatures in Law*, S. 17, 18, der sich hierbei auf Saunders v. Anglia Building Society, [1971], AC 1004 stützt.

[193] Mason, *Electronic Signatures in Law*, S. 18, 19, mit Verweis auf *L'Estrange v. F.Graucob Limited* [1934] 2 KB 394 Divisional Court, und *Pryor v. Pryor* (1860) LJR 29 NS P, M & A 114, (bzgl. der Absicht zu unterzeichnen) sowie auf *Ringham v. Hackett* (1980) 124 SJ 201, und *Central Motors (Bir-*

Zur Vermutung hinsichtlich der Identität des Unterzeichnenden findet sich im oben genannten Fall *British Estate Investment Society Ltd. v. Jackson (H M Inspector of Taxes)* aus dem Jahr 1954 ein Beispiel. Dazu wurde bezüglich der mittels Stempel aufgebrachten Signatur, ausgeführt:

> *„… man sollte annehmen, dass ein Dokument, das eine Unterschrift aufweist, ordnungsgemäß von* [demjenigen] *unterschrieben wurde, der es zu unterzeichnen angibt, … Es scheint mir, dass die rechtliche Vermutung* [presumption in law] *dahin geht, dass dieses Dokument ordnungsgemäß unterschrieben wurde, solange nicht das Gegenteil bewiesen wird durch denjenigen, der diese Schlussfolgerung widerlegen will.“*[194]

1.3.2.6 Elektronische Dokumente und Signaturen im Rechtsverkehr vor den Neuregelungen

Elektronische Dokumente konnten das Erfordernis, etwas, zum Beispiel Informationen, müsse schriftlich (*written* oder *in writing*) vorliegen, nicht ohne weiteres erfüllen. Es war daher unüblich, dass eine gesetzliche Vorschrift eine Definition von *writing* bot, die auch auf Informationen in digitaler Form ausgedehnt werden konnte.[195] Vielmehr betonte die im Interpretation Act enthaltene Definition die Sichtbarkeit oder Wahrnehmbarkeit (*visibility*) der Information, was eindeutig ein elektronisches *writing*, also die Abfolge elektronischer Impulse, ausschloss.[196] Ausgehend vom oben dargestellten Streit um die Erfüllung des *writing*-Erfordernisses durch unter anderem E-Mail und Websiteverträge bestand aber letztlich hinsichtlich des Gebrauchs von E-Mails Einigkeit darüber, dass diese die Funktionen des *writing* erfüllen können. Dies wird in der Literatur entgegen der Ansicht der Law Commission für Websiteverträge abgelehnt.[197] Daran ändere auch die Tatsache nichts, dass letztere von den Parteien ausgedruckt und so ein zum späteren Beweis erstellt werden könne: dass etwas in Schriftform erbracht werden könne, bedeute nicht, dass es in schriftlicher Form bestehe. Allenfalls könnte dadurch das Erfordernis, nach dem ein Vertrag in *writing* bewiesen werden können

---

mingham) Ltd. v. P.A. & S.N.P. Wadsworth [1982] CAT 231, (1983) NLJ 555 Court of Appeal (Civil Division) (bzgl. der Absicht der Authentifizierung und Übernahme).

[194] Richter Danckwerts in *British Estate Investment Society Ltd. v. Jackson (H M Inspector of Taxes)* (1954-1958) 37 Tax Cas, S. 79, S. 86; [1954] TR 397; 35 ATC 413; 50 R & IT 33: *„… one would presume that when a document appears to be signed it has been duly signed by the officer who purports to sign it, … It seems to me that the presumption in law is that the document has been properly signed until the contrary has been shown by a person who desires to upset that conclusion.“*

[195] Siehe oben 1.3.2.2.

[196] Siehe Ausführungen oben unter 1.3.2.2 und DTI, „Building Confidence in Electronic Commerce – A Consultation Document".

[197] Ebenso für EDI, Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 648-650.

muss, erfüllt werden, nicht jedoch ein Erfordernis, nach dem der Vertrag in Schriftform geschlossen werden müsse.[198]

Wie oben beschrieben setzt das englische Recht aber der Nutzung elektronischer Kommunikationsformen und elektronischer Dokumente, insbesondere aber der Nutzung elektronischer Signaturen als Ersatz für die Unterschrift (*signature*), relativ niedrige Hürden entgegen. Das *common law* ist hier, wie oben gesehen, prinzipiell flexibler. Elektronische Signaturen wurden bereits vor dem Erlass spezieller Gesetze verwendet. Dabei wurden auf diese neuen Technologien bestehende Rechtsprinzipien angewandt und als ausreichend erkannt.[199] Folglich konnte das Unterschriftserfordernis sogar durch die Eingabe des Namens am Ende einer E-Mail über die Tastatur oder durch das automatische oder manuelle Anhängen einer Signatur-Datei an die E-Mail erfüllt werden, da diese die Funktion eines Briefkopfes und damit einer Unterschrift habe.[200] Die Signatur am Ende einer E-Mail, zu verstehen als die (bloße) Namensnennung des Signierenden, war in 1997 in *Hall v. Cognos Limited*[201] als ausreichende Unterschrift akzeptiert worden. Voraussetzung war auch hier, dass der Unterzeichner die Absicht hatte, das Dokument zu signieren und durch diese Unterschrift das Dokument zu authentifizieren. Festgestellt wurde, dass eine E-Mail in schriftlicher Form und durch die Partei(en) unterschrieben (*„in writing and signed"*) ist, sobald sie ausgedruckt ist. Die Tatsache, dass die Unterschriften nur (aus)gedruckt, nicht handschriftlich vorlagen, sei nicht entscheidend. Dies könne jedoch anders sein, wenn die E-Mail nur zeitweise auf der Festplatte des Computers gespeichert sei.

Zu beachten ist auch hier wieder die Bedeutung ergänzender Beweise. Wenn in solchen Fällen die Identität des Unterzeichners fraglich ist, so kann durch weitere Beweise der Nachweis darüber geführt werden, wer die Unterschrift auf das Dokument aufgebracht hat.[202] Aufgrund der leichten Verfälschbarkeit blieb es jedoch ungewiss, ob Gerichte elektronischen Signaturen großes Gewicht beimessen würden. Der tatsächliche Fortschritt in der Rechtsprechung war langsam.[203] In der Praxis konnten also, während elektronische Signaturen als gleichwertig angesehen werden mochten, Verträge, die der schriftlichen Form und oder der Unterschrift bedürfen, ohne entsprechende Gesetzesänderungen nicht auf elektronischem Wege abgeschlossen werden.[204]

---

[198] Ebenso EDI, siehe Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 649.

[199] Baker et al., ILPF 2000; Chissick, S. 53, 54; Mason, *Electronic Signatures in Law*, S. 280; York/Tunkel, S. 75.

[200] So Chissick, S. 83. Problematisch wurden Click-Wrap-Verträge gesehen, dass das bloße Anklicken eines „Ich akzeptiere"-Buttons nicht die Darstellung eines Namens oder eines sonstigen Identifizierungszeichens beinhaltet. Möglichen Gefahren oder rechtlichen Folgen können so nicht kommuniziert werden, insbesondere, wo Vertragsklauseln in Hyperlinks versteckt sind. Ders., S. 81, 84.

[201] *Hall v. Cognos Limited*, Industrial Tribunal Case No. 1803325/97.

[202] Mason, *Electronic Signatures in Law*, S. 186.

[203] Chissick, S. 83; York/Tunkel, S. 91, 92.

[204] Brooks, „E-Commerce Directive: The Task Ahead (Part 2)", ECLP 2001, S. 6-7, S. 6; Crichard, „UK Electronic Communications Act 2000: Take-Off Time for E-Business or a Missed Opportunity?", CLSR 2000, S. 397-399, S. 398.

1.3.3 Formvorschriften im US-amerikanischen Recht

Das US-amerikanische und das englische Vertragsrecht sind gleichen Ursprungs. Das US-amerikanische Recht, ebenfalls *case law*, hat seine Wurzeln größtenteils im englischen *common law*. Die USA und England gehören zu einer Rechtsfamilie. Insbesondere im Zivilrecht wurden viele juristische Grundsätze und Methoden übernommen und prägen das Zivilrecht in den USA insgesamt.[205] Die obigen grundsätzlichen Erläuterungen zum *common law*[206] gelten hier folglich gleichermaßen. Dabei ist das *common law* jedoch nicht auf einen Staatenbund, wie es die USA heute sind, übertragen worden, sondern von den verschiedenen Bundesstaaten jeweils übernommen und über deren bundesstaatlichen Rechtsprechung – teilweise unterschiedlich – fortentwickelt worden.[207] Die Regelung der meisten zivilrechtlichen Materien, so auch das Vertragsrecht, ist grundsätzlich Sache der Bundesstaaten.[208] Dieses *federal system* ist ein weiteres prägendes Merkmal. Um den Gefahren der Unübersichtlichkeit hinsichtlich der Rechtsentwicklung in 50 Bundesstaaten zu entgegnen, hat es verschiedene Initiativen zur Rechtsvereinheitlichung gegeben. Daneben wirkten die Bundesgerichtsbarkeit und der Bundesgesetzgeber Rechts vereinheitlichend.[209]
Vergleichbar dem englischen Recht verlangt das US-amerikanische Vertragsrecht für einen wirksamen Vertragsabschluss zwei übereinstimmende Willenserklärungen sowie das Vorliegen einer Gegenleistung, der *consideration*.[210] Grundsätzlich sind auch hier Verträge formlos gültig, können aber aufgrund Parteiwillens in einer bestimmten Form gehalten sein. Nur bestimmte Verträge bedürfen von Gesetzes wegen einer besonderen Form.[211] Auch hier findet sich in einigen Staaten mit dem *contract under seal*, also dem Versprechen in schriftlicher Form und Siegel, in Anlehnung an das englische *deed* die

[205] Das Common Law ist im Rahmen der Kolonialisierung nach Nordamerika gelangt und hat auch nach der Unabhängigkeit der USA weiter großen Einfluss ausgeübt; Reimann, S. 1, 5, 7; Hay, Rn. 1, 11, zum US-amerikanischen Recht als Richterrecht siehe dort ausführlich Rn. 16 ff.

[206] Siehe 1.3.2.

[207] Daneben erkennt man kontinentaleuropäische Einflüsse, in einigen westlichen und südwestlichen Staaten insbesondere französisch-spanische bzw. mexikanische Einflüsse, Reimann, S. 1, 5-6; Louisiana beispielsweise folgte auch nach seiner Aufnahme in den Bund der französischen Rechtstradition mit Kodifikationen nach französischem Vorbild, Siehe: Hay, Rn. 10.

[208] Hay, Rn. 246.

[209] Reimann, S. 7, 8. Zum Verhältnis des Bundes- zum einzelstaatlichen bzw. bundesstaatlichen Recht siehe ausführlich Hay, Rn. 13-15. Die Bundesverfassung (*Constitution*) bestimmt die Bundesgesetzgebungskompetenz, behält den verbleibenden Teil dem bundesstaatlichen Gesetzgeber vor und bestimmt, dass Bundesrecht bundesstaatlichen Recht vorgeht, ebenda Rn. 13. Die Bundesgerichte sind zuständig für alle zivilen Rechtssachen, die unter ein Gesetz des (Bundes-)Kongresses fallen und dem Schutz von Handel und Wirtschaft dienen, Staatsgerichte für staatliche Wirtschaftssachen. Beide teilen die Rechtsprechung über den E-Commerce abhängig vom Streitwert, der Art der Transaktion etc. Siehe bei Muenchinger, „E-Commerce – US – Proposed US Legal Solutions to Questions Concerning Electronic Commerce“, CLSR 2000, S. 378-385, S. 378.

[210] Siehe hierzu ausführlich: Reimann, S. 28-31.

[211] Reimann, S. 41, umfassend zu Formvorschriften im US-amerikanischen Recht in Bezug auf elektronische Kommunikation siehe Cordes, *Form und Zugang von Willenserklärungen im Internet im deutschen und US-amerikanischen Recht*, Münster 2000, S. 155-185.

Möglichkeit, dass die Form die Verbindlichkeit begründet.[212] Im Gegensatz zum englischen *deed* ist der *contract under seal* in keinem Fall als zwingend oder konstitutiv vorgeschrieben, sondern dient als Option zur Erreichung einer Bindungswirkung. Er geht aber ebenfalls von den vorgestellten Begriffen *writing* und *signature* aus, die nachfolgend geschildert werden. Wie das *seal* erzeugt die bloße schriftliche Form in manchen Staaten dabei eine (widerlegliche) Vermutung einer Gegenleistung.[213]

1.3.3.1 Regelungsort

Die meisten Ausnahmen von der Formfreiheit sind im Statute of Frauds[214] zusammengefasst. Zu diesem kommen noch die Bestimmungen des Uniform Commercial Code (UCC) und im Second Restatement of Contracts[215] sowie verstreute Formvorschriften für einzelne Vertragsarten[216], die gelegentlich ebenfalls als Statutes of Frauds bezeichnet werden.[217] Das Statute of Frauds regelt die für die Wirksamkeit eines Vertrages notwendigen Formalitäten, ist gegen betrügerische Ansprüche gerichtet und dient der Beweisbarkeit von Versprechen.[218] Seine Vorschriften sind vom *contract under seal* oder *in writing* und von der Parole Evidence Rule[219] unabhängig, gelten also für die betroffenen Vertragsarten immer.[220] Was genau unter die jeweiligen Kategorien fällt, ist Gegenstand umfangreicher Rechtsprechung. Dabei werden die jeweiligen Bestimmungen oft eng ausgelegt, um Versprechen nicht an fehlender schriftlicher Form scheitern zu lassen.[221] Weitere Formerfordernisse finden sich im UCC. Dieser gilt mit Ausnahme

[212] Der *contract under seal* entstammt wie das englische *deed* dem mittelalterlichen *writ of covenant*, der heute wie alle *common law writs*, abgeschafft ist. Beim *contract under seal* dient die Form quasi als Alternative zum Bindungsgrund der *consideration*, so dass die Vereinbarung selbst ohne Gegenleistung bindend ist. Er ist streng zu unterscheiden von den oben beschriebenen Formvorschriften des Statute of Frauds. Siehe: Reimann, S. 26, 27, 28.

[213] Ebenso macht die schriftliche Form Angebote – entgegen dem *common law* – beim Warenkauf gem. § 2-205 UCC u.U. unwiderruflich; siehe Reimann, S. 26, 27.

[214] Man verwendet diesen Begriff meist in der Einzahl, obwohl es sich bei den Formvorschriften um bundesstaatliches Recht handelt und es deshalb eigentlich 50 Stautes of Frauds gibt. Diese gehen alle auf das englische Statute of Frauds von 1677 zurück, das dort 1954 abgeschafft wurde. In den USA wurden sie Teil des *common law* der einzelnen Staaten oder durch die Staatsgesetzgebung aufgenommen. Sie sind noch in allen Bundesstaaten in Kraft. Siehe Reimann, S. 41, 42; Hay, Rn. 263; Muenchinger, CLSR 2000, S. 378, 379; und § 110 Restatement (Second) of Contracts.

[215] Cordes, S. 177; The American Law Institute, *The Restatement (Second) of Contracts*, 1981, Text bei www.okcu.edu/law/academics/pdfs/Excerpts-R2d.pdf. Das Restatement ist eine zwar nicht bindende, aber sehr bekannte und in der Rechtsprechung viel zitierte Abhandlung über das Vertrags- und Handelsrecht des anglo-amerikanischen *common law*.

[216] Insbesondere für Versicherungs- und Verbraucherverträge.

[217] Der Begriff kann daher auch schlicht jede gesetzliche Formvorschrift bezeichnen; So Reimann, S. 41, 42.

[218] Muenchinger, CLSR 2000, S. 378/379; Reimann, S. 42, 43.

[219] Sie schließt bei der Auslegung von schriftlichen Verträgen bestimmte Argumente aus. Reimann, S. 42.

[220] Anwendbar auf ca. ein halbes Dutzend Vertragsarten, z.B. über Garantie und Bürgschaft, Grundstückskauf; Reimann, S. 42.

Louisianas in allen Staaten und ist damit das erfolgreichste *uniform law*.[222] Art. 2 UCC findet auf alle Kaufverträge über bewegliche Waren, nicht nur auf Handelskäufe, Anwendung[223] und beinhaltet eine eigene Version der Statutes of Frauds. Daneben finden sich im US-amerikanischen Recht tausende von bundes- oder einzelstaatlichen und selbst lokalen gesetzlichen Vorschriften für eine Vielzahl anderer Rechtsgeschäfte, die für diese die schriftliche Form und die Unterschrift vorschreiben.[224]

1.3.3.2 Erfordernis, Definition und Formen des Writing

Das Statute of Frauds verweigert bestimmten Rechtsgeschäften die Durchsetzbarkeit, wenn der Vertrag nicht in schriftlicher Form und unterschrieben (*signed writing*) vorliegt.[225] Das praktisch wohl bedeutendste Schriftformerfordernis ist das des UCC für den Verkauf von Waren (*sale of goods*) zu einem Preis von mehr als 500 US-$.[226] Um digitale Formen einzuschließen, wurde bereits vor den nachfolgend dargestellten Gesetzesinitiativen die Definition von *writing* erweitert. Der UCC definiert *writing* als *„Drucken, Maschinenschreiben oder jede andere absichtliche Reduzierung auf eine greifbare Form“*.[227] Grundsätzlich soll es der UCC den Gerichten ermöglichen, das Recht kommerzieller Transaktionen *„im Licht unvorhergesehener und neuer Umstände und Praktiken zu entwickeln.“*[228] Der UCC verlangt nicht, dass der Vertrag selbst vorgelegt wird beziehungsweise das ganze Vertragswerk schriftlich niedergelegt worden ist.

---

[221] Hay, Rn. 263; Reimann, S. 42. Die Rechtsfolgen für die Nichterfüllung der Anforderungen des Statute of Frauds sind je nach Bundesstaat unterschiedlich, teilweise ist der Vertrag anfechtbar, teilweise ist er nichtig. Ausnahme ist dagegen beispielsweise die ordnungsgemäße Erfüllung. Ausführlich ders., Rn. 263, 265.

[222] Bei den 50 Bundesstaaten handelt sich um eigenständige Rechtsordnungen. Um Divergenzen zu überbrücken, gibt es für viele Rechtsgebiete bzw. Rechtsfragen *uniform laws*. Diese werden von der National Conference of Commissioners for Uniform Laws ausgearbeitet und den Bundesstaaten zur Annahme vorgeschlagen. Nur wenige gelten in der Mehrheit der Bundesstaaten. Siehe Hay, Rn. 15. Die bundesstaatlichen Gesetzgeber können vor der Einführung eines *uniform law* Änderungen einfügen und nachfolgend kann die Auslegung und Anwendung mangels einer übergeordneten Gerichtskompetenz mit der Zeit auseinander gehen; ders., Rn. 15.

[223] Art. 2 UCC hat das Vertragsrecht als Ganzes beeinflusst. Das Wiener UN-Übereinkommen über Verträge über den internationalen Warenkauf (CISG) ist in den USA seit dem 1.1.1988 in Kraft und verdrängt als Bundesrecht abweichendes bundesstaatliches Recht einschließlich des Art. 2 UCC. Dieser hat dann lediglich eine Lücken füllende Funktion. Siehe: Hay, Rn. 247. Die Bedeutung des Art. 2 UCC für das Vertragsrecht ist insoweit beschränkt, als das Gesetz den Warenkauf nicht abschließend regelt, sondern seine Vorschriften immer im Zusammenhang mit dem Fallrecht gesehen werden, § 1-103 UCC. Andererseits reicht seine Bedeutung wegen seines Einflusses auf das Vertragsrecht insgesamt über seinen eigentlichen Anwendungsbereich hinaus. Siehe: Hay, Rn. 246; Reimann, S. 24.

[224] So existieren in Illinois über 3000 gesetzliche Vorschriften, die solche Formerfordernisse enthalten, in Georgia über 5000 und in Ohio über 8000; siehe bei Smedinghoff/Hill Bro, „Moving With Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce”, JMJCIL 1999, S. 723, Kopie von www.bakerinfo.com/ecommerce, dort nummeriert von S. 1-41, S. 11; Semdinghoff, „The Legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 4.

[225] Menna, VJLT 2001; Miedbrodt, DuD 2000, S. 543.

[226] § 2-201 UCC; Borges, *Verträge im elektronischen Geschäftsverkehr*, München 2003, S. 539.

[227] § 1-201 (46) UCC: *„... printing, typewriting, or any other intentional reduction to tangible form.*”

[228] § 1-102 UCC, siehe dazu Smedinghoff/Hill Bro, JMJCIL 1999, S. 32.

Vielmehr genügt ein vom jeweiligen Beklagten unterzeichnetes Schriftstück, oft *memorandum* genannt, das die Abgabe des Versprechens bekundet und seinen Inhalt einigermaßen genau bezeichnet.[229] Auch braucht das Schriftstück nicht von beiden Parteien unterschrieben zu sein. Es muss sich lediglich aus einem von der in Anspruch genommenen Partei unterschriebenen Schriftstück ergeben, dass ein Vertrag geschlossen wurde.[230]

Die traditionelle Definition des *writing* ist nicht auf das Aufbringen von Tinte auf Papier beschränkt. Vielmehr ist entscheidend, dass die Mitteilung auf eine körperliche oder verkörperte (*tangible*) Form reduziert wird.[231] Auch hier zeigt sich die dem englischen *common law* vergleichbare Fähigkeit, neue Technologien aufzunehmen und das Recht entsprechend ohne legislative Änderungen anzupassen. Denn aufgrund dieses Erfordernisses wäre es schlüssig gewesen, den neuen Kommunikationsformen mangels Verkörperung die Schriftlichkeit im Sinne von § 2-201 UCC abzusprechen.[232] Allerdings wurde bereits 1869 in New Hampshire in *Howley v. Whipple* ein telegrafierter Vertrag als *writing* gemäß dem Statute of Frauds anerkannt:

> *„Es macht keinen Unterschied, ob* [der Erklärende] *das Angebot oder die Annahme... mit einem einen Inch langen, an einen einfachen Stifthalter angebrachten Metallstift schreibt, oder ob sein Stift ein tausend Kilometer langer Kupferdraht ist. In beiden Fällen wird der Gedanke durch den Einsatz des auf dem Stift ruhenden Fingers zu Papier gebracht. Auch macht es keinen Unterschied, dass in einem Fall gewöhnliche Tinte benutzt wird und im anderen Fall ein abstrakteres* [subtle] *Fluidum, als Elektrizität bekannt, diese Aufgabe übernimmt.“*[233]

Ebenso wurden Telexe, Telegramme, Telefaxe, Magnetbänder und magnetische Aufzeichnungen von Gerichten als *writing* gemäß UCC anerkannt.[234] Auch in den Federal Rules of Evidence wurde *writing* bereits definiert als

---

[229] §§ 1-206 Abs. 1, 2-201 Abs. 1 UCC. Es kann auch nach Vertragsschluss entstehen und muss keineswegs als Vertragsurkunde gedacht sein. Oft reicht eine Auftragsbestätigung, Quittung oder gar ein Scheck aus. Beim Warenkauf zwischen Kaufleuten genügt eine unwidersprochen gebliebene Auftragsbestätigung nach § 2-201 Abs. 2 UCC. Das Schriftstück muss nicht einmal an den Vertragspartner gerichtet gewesen sein, so dass selbst ein internes Memorandum genügen kann. Mitunter ist selbst ein solches Schriftstück verzichtbar, insbesondere dann, wenn andere verlässliche Anzeichen für den Vertragsschluss vorliegen. Siehe bei Reimann, S. 42, 43; Muenchinger, CLSR 2000, S. 379.

[230] Hay, Rn. 264; Muenchinger, CLSR 2000, S. 378/379.

[231] Smedinghoff/Hill Bro, JMJCIL 1999, S. 12.

[232] Siehe Cordes, S. 178.

[233] *Howley v. Whipple* 48 N.H. 487 (1869): *„It makes no difference whether the operator writes the offer or the acceptance in the presence of his principal and by the principal's express direction, with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by the use of the finger resting upon the pen. Nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office.”*

[234] *Joseph Denunzio Fruit Co. v. Crane*, 79 F. Supp. 117 (S.D. Cal. 1948) (Telexe), *McMillan Ltd. V. Weimer Drilling & Eng. Co.*, 512 So.2d 14 (Ala. 1986) (*mailgram*), *Ellis Canning Co. v. Bernstein*, 348 F. Supp. 1212 (D. Colo. 1972) und a.A. *Roos v. Aloi*, 127 Misc. 2d 864 (N.Y. Sup. Ct. 1985) (Magnet-

> *„Buchstaben, Wörter oder Zahlen, sowie deren Entsprechung, hervorgebracht* [set down] *durch Handschrift, Maschinenschreiben, Drucken, Fotokopieren, Fotografieren, magnetischen Impuls, mechanische oder elektronische Aufzeichnung oder eine andere Form der Zusammenstellung von Daten.*“[235]

1.3.3.3 Erfordernis und Definition der Signature

Die Statutes of Frauds setzen einen hohen Standard für die Durchsetzbarkeit von (elektronischen) Geschäftstransaktionen. Grundsätzlich wird diese verweigert, wenn der Vertrag nicht in schriftlicher Form und unterschrieben (*signed writing*) vorliegt.[236] Erfordernisse, nach denen ein Dokument signiert sein muss, damit es rechtswirksam oder durchsetzbar ist, bereiten grundsätzlich wenig Probleme. Für die Erfüllung des Unterschriftserfordernisses genügt das Vorliegen eines bloßen Symbols auf dem Dokument, das vom Signierenden mit dem Willen aufgebracht wurde, dieses Dokument zu unterschreiben, beziehungsweise zu authentifizieren und sich den Inhalt der Erklärung zurechnen lassen zu wollen.[237] Die Definition von *signed* im UCC umfasst

> *„… jedes Symbol, sofern als es durch eine Partei mit der vorhandenen Absicht, ein Schriftstück* [a writing] *zu authentifizieren, ausgeführt oder aufgebracht* [executed or adopted] *wird.“*[238]

Damit stellt auch hier die Authentifizierung (*authentication*), also die Bezeichnung eines Schriftstückes als eigenes durch den Unterzeichner, das wesentliche Element dar.[239] Zwar ist die (herkömmliche) Unterschrift (beziehungsweise Signatur) auf einem Dokument die wichtigste Methode der Feststellung eines solchen Willens. Sofern es der Ent-

---

bänder, *tape recording*); *Bazak International Co. v. Mast Industries, Inc. 73* N.Y.2d 111, 7 UCC Rep. Serv. 2d 1380 (1989), bzw. 535 N.E. 2d 633 (N.Y. 1989).

[235] „*… letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostatting, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.”* „Federal Civil Judicial Procedure and Rules”, Title 28, Federal Rules of Evidence, West Group, 1999.

[236] Menna, VJLT 2001; Miedbrodt, DuD 2000, S. 543.

[237] Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 13.

[238] Art. 1, § 1-201 UCC, auch § 2-201 UCC. Siehe hierzu auch Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 13. Auffällig sind die großen Unterschiede zum konstitutiven Schriftformerfordernis im deutschen Recht. So enthält § 2-201 UCC kaum eines der Merkmale des § 126 BGB, auch wenn die Voraussetzungen an Urkunden teilweise ähnlich sind. § 2-201 UCC und Stautes of Frauds betreffen allenfalls die gerichtliche Durchsetzbarkeit eines Vertrages, sind also als Einrede zu sehen, nicht als Wirksamkeitsvoraussetzung. Ausführlich Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 556, 557, 559-561.

[239] Mit einer anderen Bedeutung als im Prozessrecht, siehe Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 545.

wicklung des Handels förderlich war, haben die Gerichte jedoch eine flexible Interpretation der Unterschrifts- und Schriftformerfordernisse erlaubt.[240]

1.3.3.4 Formen der Signature

Im Vergleich zu England haben die Gerichte in den USA bei einer größeren Anzahl und Formen von *marks* oder *signs* zu deren rechtlicher Qualifikation als Unterschrift Stellung genommen. So wurden z.B. (Identifizierungs-)Marken oder Zeichen auf Rechnungen und *deeds* ebenso als für eine *signature* ausreichend angesehen wie Fingerabdrücke auf Versicherungsdokumenten, bloße Namensangaben auf Telegrammen, auf Telexen, Maschinen geschriebene Namen auf *mailgrams*, Namensangaben in Briefköpfen oder Firmenstempel sowie per Telefax übersendete Unterschriften und Firmenstempel.[241] Initialen wurden in auch den USA, hinsichtlich der Anforderungen des Statute of Frauds, in öffentlich-rechtlichen und juristischen Verfahren als *signature* anerkannt.[242] Auch für Rechnungen, Schecks, Treuhandvereinbarungen (*trusts*) und Testamente (*wills*) wurden Initialen als zulässiges Mittel der *authentication* bewertet.[243] Gleiches gilt für andere Bezeichnungen einer Person als deren Namen.[244] Hinsichtlich der Anerkennung gedruckter Namen als Unterschrift sind die Gerichte in den USA grundsätzlich der englischen Rechtsprechung gefolgt. Fälle zu gedruckten Namen auf Banknoten (*banknotes*)[245], Frachtbriefen (Konossemente, *bills of lading*)[246], verschiedenen Verträgen[247] oder gerichtlichen oder öffentlichen Dokumenten[248], und anderen, insbesondere

---

[240] Menna, VJLT 2001; Miedbrodt, „Das Signaturgesetz in den USA – Electronic Signatures in Global and National Commerce Act“, DuD 2000, S. 541-545, S. 542/543; Kommentar zu § 2 Nr. 7 UETA, www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm.

[241] Mason, *Electronic Signatures in Law*, S. 33, m.w.N.; Smedinghoff/Hill Bro, JMJCIL 1999, S. 12, m.w.N.

[242] Z.B. im *federal case* aus 1993 *George A. Ohl & Co. Vv. A.L. Smith Iron Works*, 288 U.S. 170, S. 170, 53 S.Ct. 340, 77 L.Ed. 681; in Illinois *Robertson v. Robertson*, 462 N.E.2d, S. 712, Ill.App. 5 Dist. 1984; oder in Nebraska *Griffith v. Bonawitz*, 73 Neb. 622, 103 N.W. S. 327; siehe auch Mason, *Electronic Signatures in Law*, S. 43, 44, m.w.N., auch über ablehnende Urteile.

[243] Z.B. in New York *Palmer v. Stevens*, 1 Denio, S. 471 (*bills*); *The Merchants' Bank v. Spicer*, 6 Wnd., S. 443 (*check*); als *federal cases* bzgl. Statute of Frauds *The Salmon Falls Manufacturing Company v. Goddard*, 55 U.S., 446, 14 How. 446, 1852 WL 6760 (U.S.Mass.), 14 L.Ed., S. 493; *Jones v. fox Film Corporation*, 6 F.2d, S. 116 und *Monetti, S.P.A. v. Anchor Hocking Corporation*, 931 F.2d, S. 1178 (7th Cir. 1991); in Kalifornien *Weiner v. Mullaney*, 59 Cal.App.2d, S. 620, 140 P.2d, S. 704 (trusts); in Virginia Pilcher v. Pilcher, 117 Va. 356, 84 S.E., S. 667, L.R.A. 1915D, S. 905; siehe auch Mason, *Electronic Signatures in Law*, S. 43, 44, m.w.N. für andere Staaten.

[244] Z.B. „Dad“ in *Brendan v. Brendan*, 103 P.2d, S. 622 (Kaliformien), siehe Mason, *Electronic Signatures in Law*, S. 43, 44, m.w.N. für andere Staaten.

[245] *Hill v. United States*, 288 F. 192.

[246] Pennsylvania: *Carna t/d/b/a/ T.C. Trucking Company v. Bessemer Cement Company*, 558 F.Supp. 706 (1983).

[247] *Pennington v. Baehr*, 48 Cal. 565, 1874 WL 1399 (Cal.) oder *Williams v. McDonald*, 58 Cal. 527, 8 P.C.L.J. 23, 58 Cal. 527, 1881 WL (Cal.) (beide Kalifornien, bzgl. *bonds*); *Berryman c. Childs*, 98 Neb. 450, 153 N.W. 486 (Nebraska, bzgl. *brokers contracts*); *Weston v. Myers*, 33 Ill. 424, 1864 WL 2948 (Illinois, zu *promissory notes*).

[248] Z.B. *State of North Carolina v. Watts*, 289 N.C. 445, 222 S.E.2d 289; *Potts v. Cooley*, 13 N.W.Rep. 682 (beide zu *public documents*); *Smith v. Ostly*, 53 Cal.2d 262, 1 Cal.Rptr. 340, 347 P.2d 684 (Kali-

hinsichtlich der Statutes of Frauds[249], sind positiv entschieden worden. Hinzuweisen ist dabei auch auf die zu Unterschriften in Briefköpfen ergangene Rechtsprechung, etwa bei einem standardisierten Formular[250] oder einer gedruckten Rechnung[251] mit Briefkopf des Verkäufers, oder dem Briefkopf des Käufers und dem Maschinen geschriebenen Namen des Verkäufers am Ende des Dokuments.[252] Ebenso wie in England wurden lithographierte Namen als rechtswirksame Signaturen anerkannt.[253] Auch finden sich im *case law* zahlreiche Fälle zur Verwendung von Stempeln beziehungsweise Faksimile-Unterschriften, z.B. bei deren Verwendung auf Banknoten[254], Ladepapieren[255], Schecks[256], Wahlen[257], Finanzmitteilungen (*finance statements*)[258], Briefen[259], öffentlichen Urkunden[260] oder Angelegenheiten in Bezug auf das Fifth Amendment[261]. Teil-

fornien); aber: *Ames v. Schurmeier*, 9 Minn. 221, 1864 WL 1409 (Minnesota), in dem der gedruckte Name als unwirksame Signatur abgelehnt wurde, wo handschriftliche Unterschrift (*manuscript signature*) gesetzlich verlangt wird. Siehe ausführliche Darstellung bei Mason, *Electronic Signatures in Law*, S. 69.

[249] Z.B. *Defur v. Westinghouse Electric Corporation*, 677 F.Supp. 622 (E.D.Mo. 1988) (Missouri); *Reich v. Helen Harper*, Inc., 3 UCC Rep.Serv. 1048, 1966 WL 8838 (New York); *Velie v. Osgood*, 8 Barb. 130 (New York, gedruckte Namen am Ende eines Vertragsdokuments); siehe ausführliche Darstellung bei Mason, *Electronic Signatures in Law*, S. 67, 68.

[250] *Troutt v. Nash AMC/Jeep*, Inc., 157 Ga.App. 399, 278 S.E.2d 54 (Georgia).

[251] *Alarm Device Manufacturing Company v. Arnold Industries*, Inc., 56 Ohio App.2d 256, Ohio App., 417 N.E.2d 1284 (Ohio).

[252] *Dawkins and Company v. L. & L. Planting Company*, 602 So.2d 838 (Miss. 1992) (Mississippi)

[253] Als Unterschrift auf *bonds*, siehe *Hewel v. Hogin*, 3 Cal.App. 248, 84 P. 1002 (Kalifornien); *McKee v. Vernon County*, 3 Dill. 210, 16 F.Cas. 188, No. 8851 (Missouri); Town Council of Lexington v. Union National Bank, 75 Miss. 1, 22 So. 291 (Mississippi).

[254] *Hill v. United States*, 288 F. 192.

[255] *Carna t/d/b/a/ T.C. Trucking Company v. Bessemer Cement Company*, 558 F.Supp. 706 (1983) (Pennsylvania).

[256] *Robb v. The Pennsylvania Company for Insurance on Lives and Granting Annuities*, 40W.N.C. 129, 3 Pa.Super. 254, 1897 WL 3989 (Pa.Super. 1897), bestätigt durch 186 Pa. 456, 40 A969 (Pennsylvania).

[257] *Wurts v. Newsome*, 253 Ky. 38, 68 S.W.2d 448.

[258] Z.B. *In the Matter of Colorado Mercantile Co.*, 299 F.Supp. 55 (1969) (Colorado), in dem ein *financing statement* mit einer gestempelten Unterschrift akzeptiert wurde, obwohl das gesetzliche Formerfordernis die handschriftliche Unterzeichnung forderte; In *In re Bengston*, 1965 WL 8262 (Bankr.D.Conn.), 3 UCC Rep.Serv. 283 (Connecticut) wurde eine in Tinte gedruckte (gedeutet als mit einem Stempel gedruckte) Unterschrift auf einem Standardformular als *signed* akzeptiert; *In re Deep River National Bank*, 73 Conn. 341, 47 A. 675. Weitere Rechtsprechung zu vergleichbaren Fällen ist dargestellt bei Mason, *Electronic Signatures in Law*, S. 83.

[259] *Kocinski v. The Home Insurance Company*, 154 Wis.2d 56, 452 N.W.2d 360 (Wis. 1990) (Wisconsin), in dem eine mit einem Gummistempel aufgebrachte Faksimie-Unterschrift auf einem Dokument das Erfordernis der unterschrieben werden muss (*to be subscribed*); Federal 6th Circuit: *National Accident Society v. Spiro*, 78 F. 774, 24 C.C.A. 334 zu einer Faksimile-Unterschrift, die auf einem Briefkopf aufgedruckt wurde.

[260] Z.B. *State of Oklahoma ex rel. Independent School district Number One of Tulsa County v. Williamson*, 1960 OK 126, 352 P.2d 394 (Okla. 1960) (Oklahoma), in dem eine Faksimile-Unterschrift (die Uniform Facsimile Signature) auf Öffentliche Anleihen (*public bonds*) als rechtswirksam beurteilt wurde; *Moss v. Arnold*, 63 Okl.Cr. 343, 75 P. 491 (Oklahoma), nach dem eine Faksimile-Unterschrift die *authenticate requirements* erfüllt; Maricopa County v. Osborn, 60 Ariz. 290, 136 P.2d 270 (Arizona); smith v. Greenville County, 188 S.C. 349, 199 S.E. 416; weitere Rechtsprechung hierzu dargestellt bei Mason, *Electronic Signatures in Law*, S. 83, 84.

[261] Federal 2nd Circuit: *Biegeleisen v. Ross*, 158 F.3d 59 (2nd Cir. 1998), in dem festgestellt wurde, dass eine mit einem Unterschriftsstempel anstelle mit einer handschriftlichen Unterschrift unterzeichnete

weise wurden sie jedoch auch als nicht rechtswirksam abgelehnt, so in zwei Fällen zu Empfangsbestätigungen (*receipts*), in denen zum Beispiel ein ausreichender Beweis dafür fehlte, das der Stempel als Unterschrift aufgebracht und angewendet (*adopted*) wurde.[262] Hier wird erneut die Bedeutung der Einbeziehung aller Umstände der Signierung und der Berücksichtigung ergänzender Beweise deutlich. Grundsätzlich aber scheint man der Nutzung von Vervielfältigungsmechanismen der Unterschrift gegenüber aufgeschlossen. Ähnlich wie im Englischen Fall *Re United Canso Oil & Gas Ltd.*[263] wird in *State of North Carolina v. Watts*, in einem Fall über öffentliche Aufzeichnungen im Sinne von öffentlichen Urkunden (*public records*) zur Zeitersparnis und Praktikabilität gestempelter Unterschriften und damit als Argument für deren Verwendung und rechtliche Anerkennung festgehalten:

> *„Es ist offensichtlich, dass es extrem zeitaufwändig und kostspielig wäre, für* [öffentliche Aufzeichnung/Urkunde] *die handschriftliche Unterzeichnung zu verlangen.“*[264]

Die Verwendung von Stempeln in der Gerichtsbarkeit ist dagegen nur mit unterschiedlichem Erfolg rechtlich anerkannt worden.[265] Während sie in den Bundesstaaten weitgehend akzeptiert ist[266], wurde in *United States of America v. Juarez* von einem Bundesgericht in zweiter Instanz ein Durchsuchungsbefehl (*search warrant*) für unwirksam erklärt, der vom Amtsrichter (*magistrate*) mittels Stempel anstelle der handschriftlichen Unterschrift unterzeichnet wurde. Richter Tone begründet dies wie folgt:

> *„Seine* [des Stempels] *Verwendung erweckt den Eindruck, dass der Verwender die Sensitivität* [sensitivity] *vermissen lässt, die ein Bundesgerichtsbeamter den bedeutenden Werten entgegenbringen sollte, die der Durchsuchungsbefehl schützen soll.“*

Mitteilung nicht gegen die Due Process Clause des Fifth Amendment (Amendment V of the United States Constitution, Teil der Bill of Rights und damit der Verfassung) verstößt.

[262] So in Boardman *v. Spooner*, 13 Allen 353, 95 Mass. 353, 1866 WL 5009 (Massachusetts) zu einem *bill of sale of goods*. In *Bell Bros. v. Western & A.R. Co.*, 125 Ga. 510, 54 S.E. 532 wurde eine Unterschrift per Matritze (*stencil*) abgelehnt, da nicht hinreichender Beweis dafür vorlag, dass der Unterzeichnende die Empfangsbestätigung unterschrieben, die Unterschrift bestätigt (*adopted*) habe, oder es gebräuchlich war, seine Unterschrift auf diese Weise auf solche Dokumente aufzubringen.

[263] *Re United Canso Oil & Gas Ltd.* (1980) 12 B.L.R. 130; 76 A.P.R. 282; 41 N.S.R. (2d), 282 (T.D.), S. 289, siehe oben 1.3.2.4.

[264] Richter Branch in *State of North Carolina v. Watts*, 289 N.C. 445, 222 S.E.2d, S. 389, 392: *„It is ... obvious that to require the manual signing of every record certified from ... would be extremely time consuming and expensive.“*

[265] Mason, *Electronic Signatures in Law*, S. 82.

[266] Z.B. *State of Florida v. Hickman*, Fla., 189 So.2d 254, in dem die Unterschrift des Richters durch dessen Faksimile-Unterschrift mittels Gummistempel und durch den Büroleiter (*chief clerk*) aufgebracht wurde und als wirksame Unterschrift des Richters gewertet wurde. Siehe dazu auch Mason, *Electronic Signatures in Law*, S. 82-84 m.w.N.

Diese Argumentation scheint auf die Warnfunktion einer eigenhändigen Unterzeichnung anzuspielen, auch wenn es hier um einen öffentlich-rechtlichen beziehungsweise strafrechtlichen Sachverhalt geht. Auch hier wurden in der ersten Instanz die Umstände der Signierung und weitere Indizien berücksichtigt, denn Richter Tone führt weiter aus:

> *„Nichtsdestotrotz hat der Amtsrichter eindeutig ausgesagt, dass er sich daran erinnert, den Stempel auf den Durchsuchungsbefehl ausgebracht zu haben, und das Distriktsgericht hat diese Aussage für ihn gewertet."*[267]

Maschinen geschriebene Unterschriften wurden ebenfalls als *signature* akzeptiert[268], etwa mit der Begründung, das Recht verlange Unterschriften nur als ein Hinweis und Beweis für die Zustimmung der Parteien.[269] Allerdings wurde dabei vielfach ausdrücklich der (zusätzliche) Beweis dafür gefordert, dass die Person, dessen Namen als Unterschrift gedruckt oder getippt wird, diese Unterschrift aufgebracht hat.[270] Die Schwierigkeit, das Aufbringen des Maschinen geschriebenen Namens mit dem Beweis zu verbinden, dass dieser Name mit Absicht und Berechtigung (*authority*) aufgebracht wurde, wird illustriert in *Landecker v. Co-operative Bldg. Bank*:

> *„Die bloße Erstellung des Vertrages mit dem Maschinen geschriebenen Namen des Gebers ist ungenügend, um die Voraussetzungen des Gesetzes zu erfüllen, sofern nicht die Befugnis und der Wille beim Schreiben des Namens bewiesen werden."*[271]

Auch in den USA wurden früh die Voraussetzungen für den Beweis mit Telegrammen festgelegt[272] und bestimmt, dass diese ein adäquates *memorandum* eines Vertrages darstellen können und dass aus dem Vorliegen mehrerer Telegramme und Briefe auf das

---

[267] *United States of America v. Juarez*, 549 F.2d 1113 (1977): *„Its* [the stamp's] *use creates the appearance that the user lacks the sensitivity a federal judicial officer should have to the important values which the warrant is designed to protect. Nevertheless, in this case the magistrate testified unequivocally that he remembered placing the signature stamp on the warrant, and the District Court credited this testimony"*

[268] Z.B. hinsichtlich des Statute of Frauds: *In the Matter of Save-On-Carpets of Arizona*, Inc., 547 F.2d 1239 (1976) (in Bezug auf ein UCC *financing statement*); *A. & G. Construction Co., Inc., v. Reid Brothers Logging Co., Inc.*, Alaska 547 P.2d 1207 (Alaska) oder *Ashland Oil, Inc. v. Pickard*, Fla., 269 So.2d 714 (Florida), beide bzgl. eines getippten Namens am Ende eines Briefs; *Dawkins and Company v. L. & L. Planting Company*, 602 So.2d 838 (Miss. 1992) (Mississippi); *Watson v. Tom Growney Equipment, Inc.*, 721 P.2d 1302 (N.M. 1986) (New Mexico), u.a., siehe bei Mason, *Electronic Signatures in Law*, S. 89.

[269] *Ardery v. Smith*, 35 Ind.App. 94, 73 N.E. 840 (Indiana).

[270] *Roberts v. Johnson*, 212 F.2d 672; Tabas v. Emergency Fleet Corporation, 9 F.2d 648 *affirmed United States Shipping Board Emergency Fleet corporation v. Tabas*, 22 F.2d 398 (Pensylvania); oder *Estate of Moore*, 92 Cal.App.2d 120, 206 P.2d 413, wonach bei einer getippten Unterschrift auf einem Testament weitere Beweise dafür gegeben sein müssen, dass der Name vom Erblasser selsbt oder in dessen Anwesenheit von einem anderen getippt wurde.

[271] *Landecker v. Co-operative Bldg. Bank*, 130 N.Y.Supp. 780 (New York): *„The mere production of the contract with the typewritten name of the grantor is insufficient to meet the requirements of the statute, unless the authority and intent in signing the name is shown."*

[272] *Howley v. Whipple*, 48 N.H. 487 (1869) (New Hampshire).

Bestehen eines Vertrages geschlossen werden kann.[273] Auch in anderen Fällen wie Rechnungen, Justiz und in Bezug auf das Statute of Frauds wurden Telegramme für ausreichend erachtet.[274] In *Leesley Bros. v. A. Rebori Fruit Co.*, wurden Angebot und Annahme eines Kaufvertrags mittels zweier Telegramme als vollständig ausreichend im Sinne des Statute of Frauds beurteilt mit der Begründung:

> *„… anders zu urteilen würde mit Sicherheit gegenwärtige Geschäftsmethoden diskreditieren und die Kosten erhöhen und die Nützlichkeit des Telegraphen als notwendiges Instrument des modernen Handels beschädigen.“*[275]

In *La Mar Hosiery Mills, Inc., v. Credit and Commodity Corporation* wurde festgestellt, warum ein Name in einem Telegramm eine rechtswirksame Unterschrift darstellt:

> *„Das Telegramm mit der Maschinen geschriebenen Signatur des Namens des Beklagten stammt vom Beklagten, der für sie verantwortlich ist. Die Unterschrift auf dem hier in Frage stehenden Telegramm ist deshalb, obwohl sie im Büro der Telegraphengesellschaft geschrieben wurde, die autorisierte Unterschrift des Beklagten im Sinne der Voraussetzungen des Statute of Frauds. Im Hinblick darauf, wie heutzutage Geschäfte getätigt werden, würde jede andere Sichtweise unrealistisch sein und schädliche Konsequenzen hervorrufen, die die Durchführung von Geschäftstransaktionen verhinderten.“*[276]

In *Hessenthaler v. Farzin* wurde mittels *mailgram* der Verkauf eines Grundstücks bestätigt und vom Gericht mit Blick auf die bestehende Rechtsprechung als *signed writing* akzeptiert mit der Begründung:

---

[273] *Meek v. Briggs*, 80 Fla. 487, 86 So. 271 (Florida).

[274] Z.B. *Selma Savings Bank v. Webster County Bank*, 206 S.W. 870, 182 Ky. 604, 2 A.L.R. 1136 (Kentucky); *Blackburn v. City of Paducah*, 441 S.W.2d 395, (Ky. 1969) (Kentucky); insbesondere *MyMillan Ltd. v. Warrior Drilling and Engineering Company, Inc.*, 512 So.2d 14 (Ala. 1986) in Alabama, in dem ein Name in einem Telegramm eine ausreichende Unterschrift i.S.d. Statute of Frauds darstellte, oder *Ashland Oil, Inc. v. Pickard*, Fla., 269 So.2d 714, in dem ein Telegramm als *signed memorandum* galt; ähnlich *Yaggy v. The B.V.D. Company*, Inc., 70 N.C.App. 590, 173 S.E.2d 496, 72 Am.Jur.2d; in *Pike Industries, Inc. v. Middlebury Associates*, 398 A.2d 280 *affirmed on other grounds* 436 A.2d 725, *cert denied*, 455 U.S. 947, genügte ein Telegramm dem Statute of Frauds deshalb nicht, weil der Name der Partei überhaupt nicht in dessen Text aufgenommen war. Weitere Fälle siehe Darstellung bei Mason, *Electronic Signatures in Law*, S. 94, 95.

[275] *„… to hold otherwise would certainly embarrass present business methods and increase the expense and impair the usefulness of the telegraph as a necessary instrumentality in modern commerce.“ Leesley Bros. v. A. Rebori Fruit Co.*, 162 Mo.App. 195, 144 S.W. 138, Richter Nixon, vergleichbar dem englischen Fall *McBlain v. Cross* (siehe oben).

[276] *La Mar Hosiery Mills, Inc., v. Credit and Commodity Corporation*, 28 Misc.2d 764, 216 N.Y.S.2d 496, 72 Am.Jur.2d: *„The telegram with the typed signature of defendant's name emanated from the defendant which is responsible for it. The signature on the telegram in suit, although typed in the office of the telegraph company, is therefore defendant's authorized signature within the requirements of the statute of frauds. In view of the way in which business is done nowadays, any other view would be unrealistic and would produce pernicious consequences, impeding the conduct of business transactions.“*

> *„Wir stimmen mit diesen Urteilen darin überein, dass der richtige, realistische Ansatz in diesen fällen der ist, auf die Verlässlichkeit des* [memorandum] *abzustellen anstatt auf einer formellen Unterschrift zu bestehen.“*[277]

Das *mailgram* würde hinreichend die Absicht des Unterzeichnenden, das Geschriebene als von ihm stammend anzunehmen, darstellen und sei daher als unterschrieben (signed wiritng) für die Zwecke des Gesetzes.[278] Auch Telexe haben in der Rechtsprechung der USA eine weit reichende Anerkennung gefunden.[279] Danach kann der Austausch von Nachrichten via Telex die *merchants exception* der Statute of Frauds erfüllen.[280] In die Telex-Nachrichten aufgenommene Signaturen stellten Unterschriften dar, was wie folgt begründet wurde:

> *„… jede [Partei] hatte einen Teleschreiber in ihrem Büro und als die Maschine in einem Büro bedient wurde, schrieb sie die Nachricht oder* [das Memorandum] *gleichzeitig im anderen Büro; jede Partei war einfach zu identifizieren und der anderen Partei bekannt durch die verwendeten Symbole oder Codes und es gibt kein Hinweis darauf, dass die Nachrichten nicht vom Büro der einen Partei herrührten und im Büro der anderen endeten. … Das Gericht muss eine realistische Sicht auf die modernen Geschäftspraktiken haben.“*[281]

Ferner wurden wie in England im Fall *Re a debtor*[282] auch Telefaxe als rechtswirksam anerkannt.[283] So in *Madden v. Hegadorn*, in dem ein Fax eines Dokuments, das eine handschriftliche Unterschrift aufwies, als wirksam erklärt wurde.[284] Richter Troast bemerkte zur Technik des Faxes:

---

[277] *Hessenthaler v. Farzin*, 564 A.2d S. 990 (Pa.Super. 1989) (Pennsylvania): *„We agree with these authorities that the proper, realistic approach in these cases is to look to the reliability of the memorandum, rather to insist on a formal signature.“*

[278] *Hessenthaler v. Farzin*, 564 A.2d S. 990 (Pa.Super. 1989), S. 994.

[279] Siehe Darstellung bei Mason, *Electronic Signatures in Law*, S. 97-99.

[280] *Apex Oil Co., v. Vanguard Oil & Services Co.*, 760 F.2d 417 (1985).

[281] *Joseph Denunzio Fruit Co., v. Crane*, 79 F.Supp. 117 *reversed on other grounds upon rehearing* 89 F.Supp. 962: *„… each had a teletype machine in his office and as the machine was operated in one office, it would type the message or memorandum simultaneously in the other office; each party was readily identifiable and known to the other by the symbols or code letters used, and there is no contention that the messages did not originate in the office of one and terminate in the office of the other. … The court must take a realistic view of modern business practices.“*

[282] *Re a debtor (No. 2021 of 1995), Ex p, Inland Revenue Commiccioners v. The debtor; Re a debtor (No. 2022 of 1995), Ex, Inland Revenue Commissioners v. The debtor* [1996] 2 All E.R. 1208, S. 345, 351, siehe oben unter 1.3.2.4.

[283] Z.B. *Bazak International Corp., v. Mast Industries, Inc.*, 140 Ad.2d 211, 528 N.Y.S.2d 62, 6 UCC Rep.Serv.2d 375, *appeal granted by* 72 N.Y.2D 808, 529 N.E.2d 425, 533 N.E.2d 57 (N.Y. 1988), *Order reversed by* 73 N.Y.2D 113, 535 N.E.2d 633, 538 N.Y.2d 503, 57 USLW 2520, 82 A.L.R.4th 689, 7 UCC Rep.Serv.2d 1380 (N.Y. 1989) (New York). Allein der Übermittlungsakt und als Beweis dafür das Sendeprotokoll wurden dabei als ausreichend erachtet, siehe auch Cordes, S. 182.

[284] *Madden v. Hegadorn*, 565 A.2d, S. 725 (N.J. Sper.L 1989), 236 N.J.Super. 280, affirmed 571 A.2d 296 (N.J. 1989), 239 N.J. Super 268, wobei technische Mängel durch die spätere Einreichung des Originals geheilt wurden.

„Die Telefaxtechnologie ist relativ neu. Es ist allgemein bekannt, dass ‚Fax'-Geräte Dokumente elektronisch scannen, sie auf eine Serie digitaler Signale reduzieren und diese über das Telefonnetz an ein Empfängergerät übermitteln, das die Signale wieder zusammensetzt und dann das Originaldokument reproduziert."[285]

In anderen Fällen, in denen durch strikte *rules* ausdrücklich die handschriftliche Unterzeichnung gefordert wurde, konnten Fax-Dokumente diese Voraussetzung jedoch nicht erfüllen.[286] In *Parma Tile Mosaic & Marble Co., Inc. v. Estate of Fred Short, d/b/a Sime Construction Co.* wurde zudem die Frage behandelt, ob die Programmierung des Faxgeräts, bei jeder Sendung automatisch die Senderkennung mit dessen Namen am Anfang oder Ende jeder Seite zu drucken, das Schriftform- und Unterschriftserfordernis (*the writing to be subscribed*) erfüllen kann. Dies wurde abgelehnt:

„Der Akt des Identifizierens und Sendens eines Dokuments an eine bestimmte Adresse allein stellt keine Unterschrift dar, die den Inhalt des Dokuments im Sinne des Statute of Frauds authentifiziert… Wir weisen auch die Einlassung des Klägers zurück, schon allein die willentliche Programmierung des Faxgeräts weise gegenüber dem Empfänger hinreichend den offensichtlichen Willen des Versenders nach, alle nachfolgend gefaxten Dokumente zu authentifizieren. Der Wille zur Authentifizierung des einzelnen in Frage stehenden Schriftstücks muss nachgewiesen werden."[287]

Dennoch wird aus *Madden v. Hegadorn* gefolgert, dass eine als Unterschrift gedachte elektronische Aufzeichnung ebenfalls die Voraussetzungen der Unterschrift erfüllen würde.[288] Dabei ist der Ort, an dem die Signatur angebracht ist, unbeachtlich.[289]
In *Spevack, Cameron & Boyd v. National Community Bank of New Jersey*[290] wurde die einzigartige Kontonummer des Kontoinhabers als ebenso vollständige Signatur des Kontoinhabers qualifiziert wie dessen (hand-)geschriebener oder gedruckter Name. Eine

---

[285] *Madden v. Hegadorn*, S. 728: *„Facsimile technology is relatively new. It is common knowledge that "fax" machines electronically scan documents, reduce the documents to a series of digital signals and transmit them over telephone lines to a receiving machine which reassembles the signals and then reproduces the original documents."*

[286] Z.B. *Gilmore v. Lujan*, 947 F.2d 1409 (9th Cir. 1991).

[287] *Parma Tile Mosaic & Marble Co., Inc. v. Estate of Fred Short, d/b/a Sime Construction Co.*, 155 Misc.2d 950, 590 N.Y.S.2d 1019 (Supp. 1992), *motion for summary judgement affirmed*, 209 A.D.2d 495, 619 N.Y.S..2d S. 628 *reversed* 663 N.E.2d 633 (N.Y. 1996), 640 N.Y.S.2d 477 (Ct.App. 1996), 87 N.Y.2D 524, S. 635: *„The act of identifying and sending a document to a particular destination does not, by itself, constitute a signing authenticating the contents of the document for Statute of Frauds purposes… We also reject plaintiff's contention that the intentional act of programming a fax machine, by itself, sufficiently demonstrates to the recipient the sender's apparent intention to authenticate every document subsequently faxed. The intent to authenticate the particular writing at issue must be demonstrated."*

[288] Mason, *Electronic Signatures in Law*, S. 229.

[289] *Parma Tile Mosaic & Marble Co., Inc. v. Estate of Fred Short, d/b/a Sime Construction Co.*, s.o.

[290] *Spevack, Cameron & Boyd v. National Community Bank of New Jersey*, 677 A.2d, S. 1168, N.J.Super.A.D. 1996, 291 N.J.Super. 577.

Unterschrift (*signature*) könne viele Formen annehmen und es bestünde kein Grund, weshalb eine Kontonummer nicht eine dieser Formen darstellen könne:

> *„In diesem Computerzeitalter ist der Gebrauch von Nummern als Mittel der Identifikation allgegenwärtig geworden. Tatsächlich werden Nummern leichter* [more readily, auch im Sinne von geeignet] *anerkannt und genutzt als Signaturen* [Unterschriften]. *Die vom* [Kontoinhaber] *genutzte ‚Signatur' war seine Kontonummer bei* [der Bank]*... Diese ‚Signatur' hat den Einzahler korrekt identifiziert... In der Tat hätte die Bank, hätte der* [Kontoinhaber] *einen geschriebenen Namen ohne Kontonummer angegeben, die dazugehörende Nummer nachschlagen müssen. Es sind die Nummern, die im elektronischen Zeitalter die vornehmliche Bedeutung haben.‟*[291]

Ähnlich wie in den englischen Fällen, in denen bei Vorliegen hinreichender weiterer Beweise die mündliche Bestätigung u.U. die Unterschrift ersetzen konnte, wurden auch in den USA unübliche Methoden, Zustimmung zu einer Vereinbarung auszudrücken, anerkannt. So zum Beispiel bei einer Tonbandaufzeichnung einer Konversation.[292] Andererseits wurde in *Parshalle v. Roy* bezüglich einer Wahl die Autorisierung einer Vollmachtsurkunde per *datagram*, also per Telefonverbindung, als unwirksam erachtet, da nicht ausreichend Beweis für die Echtheit und Einzigartigkeit der Übertragungsmethode vorlag, um eine Verbindung zwischen Wähler und Votum herzustellen.[293]

1.3.3.5 Beweiszulassungs- und Beweiskraftregelungen

Zunächst ist darauf hinzuweisen, dass nur wenigen der Statutes of Frauds über den Beweiszweck hinausgehende Zwecke zukommen.[294] Die vorgenannten Erfordernisse stellen daher größtenteils solche an die bestimmte Form von Beweisen dar. Auch die Beweisregeln, die Rules of Evidence, nach denen das Gericht entscheidet, welche Beweise in einem Verfahren zugelassen werden, sind in den Bundesstaaten verschieden. Nur die Bundesgerichte folgen den Federal Rules of Evidence.[295] Zunächst wird verlangt, dass die Authentizität (*authenticity*) eines Dokuments oder einer Aufzeichnung bewiesen wird, bevor dies als Beweis angenommen wird.[296] *Authenticity* meint, dass es sich zum

---

[291] Richter Bilder, S. 1169: *„In this computer age the use of numbers as a means of identification has become pervasive. Indeed, numbers are more readily recognized and handled than signatures. The 'signature' used by* [the depositor] *was its account number at* [the bank]*,... That 'signature' accurately identified the payee... In fact, had* [the depositor] *written a name without the account number, the bank would have had to look up the number that correspond with the same. In keeping with the electronic age, it is the numbers which have the primary significance."*

[292] *Ellis Canning Company v. Bernstein*, 348 F.Supp. 1212 (1972) (Colorado).

[293] *Parshalle v. Roy*, Del. Ch. 567 A.2d 19 (1989).

[294] Zum Beispiel beim UCC 2-201, siehe Borges, *Verträge im elektronischen Geschäftsverkehr*, S, 554.

[295] Muenchinger, CLSR 2000, S. 380/381; Federal Rules of Evidence in ihrer aktuellen Fassung vom 31.12.2004, dort ab Art. IX, Rules 901 ff.

[296] Siehe *U.S. v. Eisenberg*, 807 F.2d 1446 (8th Cir. 1986); *U.S. v. Grande*, 620 F.2d 1026 (4th Cir. 1980).

Beispiel bei einer Urkunde tatsächlich um denjenigen Gegenstand handelt, der es nach der Behauptung des Beweisführers sein soll, also die Urheberschaft der Urkunde. Sie dient als Nachweis der Identität des Beweismittels, ohne mit der Echtheit (*genuineness*) identisch zu sein.[297] Eine Signatur, insbesondere die handgeschriebene auf papiernem Dokument, kann diesen Zweck erfüllen.[298] Von Bedeutung ist, dass die Authentifizierung einer Urkunde nicht nur durch direkten Beweis, sondern genauso durch Indizienbeweis (*circumstantial evidence*) erfolgen kann. Die Authentifizierung elektronischer Aufzeichnungen dürfte also auch bei solchen ohne elektronische Signatur meist möglich sein. Erst anschließend geht es um den eigentlichen beweis der Urheberschaft, der sehr aufwändig sein kann.[299]

Von besonderer Bedeutung ist die Best Evidence Rule (auch Original Document Rule genannt), von der eine Version allgemein in allen Staaten gilt.[300] Anders als in England, wo das gesetzliche Erfordernis der Vorlage des Originals eines Dokumentes zum Beweis in § 8 Civil Evidence Act 1995 ganz gestrichen worden war[301], muss hier dort, wo bestimmte Vertragsbestimmungen entscheidend sind, das Original des Schriftstückes (*original writing*) vorgelegt werden, um dessen Inhalt zu beweisen. Ein indirekter Urkundsbeweis (*secondary evidence*), beispielsweise mittels Kopien, ist danach nur möglich, wenn dargelegt wurde, dass das Original aus anderen Gründen als einem ernsthaften vorsätzlichen Fehlverhalten des Beweisführers nicht mehr vorhanden ist.[302] Gemäß den Federal Rules of Evidence kann anstelle des Originals ein Computerausdruck oder eine im Computer gespeicherte Erklärung als Beweismittel vorgelegt werden, sofern wiederum bewiesen ist, dass die Daten korrekt sind.[303] Hierbei gleichen sich die Anforderungen an den Beweis mittels elektronischer Dokumente im englischen und US-amerikanischen Recht wieder an. Im Vergleich dazu kann in Deutschland die Verwendung elektronischer Dokumente als Beweis im Gerichtsverfahren nicht durch ein etwaiges Erfordernis, das Original vorzulegen, behindert werden. Denn da elektronische Dokumente die Voraussetzungen der Urkunde gemäß §§ 415ff. ZPO nicht erfüllen, können weder das Gericht noch die gegnerische Partei die Vorlage dessen „Originals“ verlan-

[297] Authentifizierung (*authentication*) bezieht sich ebenfalls auf die Echtheit einer Urkunde, setzt jedoch nicht den Beweis der Urheberschaft oder der Echtheit im Sinne der vollen Überzeugung des Gerichts voraus. Ausführlich zu den Erfordernissen der Authentifizierung (*authentication*) und der Echtheit (*authenticity*) sowie zur Rule of Authentication siehe bei Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 374ff. und 378ff.

[298] Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 18.

[299] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 380, 410.

[300] Einheitliche Beweisregelungen, die *Uniform Rules of Evidence*, müssen z.T. noch von den Staaten angenommen werden; Muenchinger, CLSR 2000, S. 381.

[301] Siehe oben unter 1.3.2.5.

[302] Siehe dazu Semdinghoff, „The Legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 4. Beispielsweise muss im Falle eines Warenkaufs in Höhe von mehr als $ 500,- das original *signed writing* vorgelegt werden, siehe Muenchinger, CLSR 2000, S. 379.

[303] Federal Rules of Evidence, Art. X, Rules 1002 ff.; Miedbrodt, DuD 2000, S. 544. Dabei ist zu beachten, dass der Richter lediglich über sich die aus den Rules of Evidence ergebenden Rechtsfragen entscheidet, die Jury aber über alle Tatsachenfragen. Der Richter entscheidet, ob ein Schriftstück oder eine Aufzeichnung als Original bewertet wird, und die Jury, ob der dargebrachte Beweis den Inhalt des Originals korrekt wiedergibt; Muenchinger, CLSR 2000, S. 381.

gen.[304] Für die *authentication* nicht nur beim Zeugenbeweis, sondern auch für den Beweis mit Dokumenten, insbesondere von E-Mails bei denen vorhergegangene Nachrichten angehängt oder beigefügt werden, ist zudem die Hearsay Rule[305] bedeutend. Danach sind – ähnlich dem Begriff des „Hörensagen" – Bekundungen (*statements*), die nicht vom Erklärenden im Rahmen seiner Vernehmung im Gerichtsverfahren gemacht werden, kein zulässiges Beweismittel.[306] Die Aussage eines Zeugen, dass ein Dritter eine Aussage über eine streitige Tatsache gemacht habe, kann also nicht als Beweis dienen. Dadurch soll eine unsachliche Beeinflussung des Gerichts vermieden werden, da beim *hearsay* das für die Überprüfung des Wahrheitsgehalts im US-amerikanischen Prozessrecht so bedeutende Kreuzverhör (*cross examination*) entfällt.[307] Allerdings existieren eine Vielzahl von Ausnahmen vom *hearsay*-Verbot.[308]
Beweiskraftregeln wie die des § 416 ZPO existieren hier nicht. Für die Maschinen geschriebene Unterschrift (*typewritten signature*) wurde in *First Security Bank of Brookfield v. Fastwich* eine Vermutung ihrer Echtheit sowie dafür festgestellt, dass sie vom Aussteller autorisiert (*authorized*) ist.[309] In *Wurts v. Newsome* wurde zur Verlässlichkeit der Unterschrift mittels Stempel sogar ausgeführt:

> *„Die Möglichkeiten zum Betrug* [fraud] *sind bei der Verwendung eines Gummistempels nicht größer als die Möglichkeiten zum Betrug durch Fälschung* [einer handschriftlichen Unterschrift]*."* [310]

1.3.3.6 Elektronische Dokumente und Signaturen im Rechtsverkehr vor den Neuregelungen

Trotz der oben dargestellten Flexibilität in der Adaption des Rechts an neue Technologien stellten Formvorschriften wie in den Statutes of Frauds gesetzliche Hindernisse für die Rechtswirksamkeit und Durchsetzbarkeit elektronischer Aufzeichnungen und Dokumente (*records and documents*) dar.[311] Eine gesetzliche, generelle Feststellung, dass

---

[304] Heydn, Truiken J. in Campbell, Dennis, *E-Commerce and the Law of Digital Signatures*, Oceana Publications, 2005, S. 259, 260.

[305] Festgehalten in Art. VIII, Rules 801 ff. Federal Rules of Evidence. Sie wurde ursprünglich in England entwickelt, ist dort aber mittlerweile für Zivilverfahren abgeschafft, § 1 Civil Evidence Act.

[306] Definition in Rule 801 Lit. c).: *„"Hearsay" is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."*

[307] Ausführlichere Darstellung bei Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 369-373.

[308] Unter die unter bestimmten Umständen auch betroffene E-Mails fallen, siehe dazu auch unten 2.5.6.

[309] *First Security Bank of Brookfield v. Fastwich*, 612 S.W.2d 799 (Mo.App. 1981) (Missouri).

[310] Richter Clay in *Wurts v. Newsome*, 253 Ky. 38, 68 S.W.2d 448 (*„The opportunities for fraud when a rubber stamp is used are no greater than the opportunities for fraud by forgery."*), der weiter ausführt: *„Es wäre ebenso schwierig festzustellen, dass die Stimmzettel* [ballots] *nicht* [wirksam] *unterschrieben sind und einen Gummistempel herzustellen, als es schwierig wäre, jemanden zu beauftragen, die Unterschrift des Richters zu imitieren, der nicht unterschrieben hat."* (*„It would be just as difficult to ascertain that the ballots had not been signed, and have a rubber stamp prepared, as it would be to employ one to imitate the signature of the judge who failed to sign."*).

[311] Und in Vorschriften zur Speicherung solcher Aufzeichnungen (*record retention statutes*) oder bezüglich öffentlicher Registrierungen u.ä. (*governmental filing*); Miedbrodt, DuD 1998, S. 391; Prefatory

solche Schriftform- und Unterschriftserfordernisse durch elektronische Dokumente und elektronische Signaturen erfüllt werden können, gab es nicht. So bestanden insbesondere beim Einsatz elektronischer Signaturen Bedenken, zum Beispiel hinsichtlich deren Urkundsqualität und der strengen Anforderungen der Statutes of Frauds an das *signed writing*.[312] Wie bereits oben aufgezeigt waren allerdings in den USA – im Gegensatz zum englischen Recht – die Begriffe *in writing* oder *written* weiter gefasst beziehungsweise ausgelegt worden. Die Begriffe Urkunde (*writing*) und Unterschrift (*signature*) wurden vielfach durch Aufzeichnung (*record*) und Authentifizierung (*authentication*) ersetzt.[313] Aufgrund der erweiterten Definition des *writing* zum Beispiel im UCC und der Akzeptanz beispielsweise von Telexen und Telefaxen als *writing* war es daher wahrscheinlich, dass die Gerichte elektronische, auf einem körperlichen Medium gespeicherte Nachrichten ebenfalls als *writing* anerkennen.[314] In *Clyburn v. Allstate* hatte das Gericht hierzu entschieden, dass es

> *„in der heutigen ‚papierlosen' Gesellschaft mit von Computern geschaffener Information... , so lange eine gesetzliche Regelung oder dergleichen nicht vorliegt, nicht bereit ist festzustellen, dass eine Computer-Floppy-Diskette nicht schriftliche Form* [writing] *im Sinne der Vorschrift darstellte.*"[315]

In *CompuServe Inc. v. Patterson* war in 1996 ein elektronischer Vertrag zwischen einem Internet-Provider und seinem Kunden für wirksam erklärt worden.[316] Im Jahr 2000 wurde in *In re RealNetworks, Inc. Privacy Litig.* sogar festgestellt, dass ein Lizenzvertrag auf einer Website *writing* darstellt, wenn die Vereinbarung ausgedruckt und gespeichert werden kann.[317] Elektronische Dokumente können also Urkundseigenschaft haben. Ferner waren die Gerichte auch darum bemüht, die Statutes of Frauds im Lichte der Förderung von geschäftlichen Aktivitäten zu interpretieren.[318] Daher waren elektronische Signaturen bereits vor den neuen gesetzlichen Regelungen akzeptiert, auch in den einfachsten Formen der eingescannten Unterschrift oder der Namensnennung in der E-Mail. Auch in diesen Fällen wurde darauf abgestellt, dass allein der Wille des Signie-

---

Note (Einleitende Anmerkung) zum Uniform Electronic Transactions Act (1999), www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm.

[312] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 577; Menna, VJLT 2001; Miedbrodt, DuD 2000, S. 542, 543; Muenchinger, CLSR 2000, S. 379; Kommentar zu § 2 Nr. 7 UETA, www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm.

[313] Siehe ausführlich bei Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 153 ff., 154.

[314] Ausführlich Smedinghoff/Hill Bro, JMJCIL 1999, S. 12, m.w.N.

[315] *Clyburn v. Allstate* 826 F.Supp. 955 (D.S.C. 1993) (Kalifornien): *„... in today's 'paperless' society of computer generated information*", it is *„not prepared, in the absence of some legislative provision or otherwise, to find that a computer floppy diskette would not constitute a 'writing' within the meaning of [the Statute]*." Zur Erfüllung des Schriftformerfordernisses durch auf Computerdisketten gespeicherte Dokumente (hinsichtlich der Definition von *written instrument* im Colorado Forgery Statute): *People v. Avila*, 770 P.2d 1330, 1332 (Colo. Ct. App. 1988).

[316] *CompuServe Inc. v. Patterson*, 89 F.ed 1257 (6th Cir. 1996).

[317] *In re RealNetworks, Inc. Privacy Litig.*, 2000 U.S.Dist. LEXIS 6584 (N.D.Ill. 2000), 2000 WL 631341 (N.D.Ill. 2000) (Illinois).

[318] Menna, VJLT 2001; Miedbrodt, DuD 2000, S. 543.

renden, sich die Erklärung zurechnen lassen zu wollen, entschied.[319] Im Fall *Doherty v. Registry of Motor Vehicles* aus Massachusetts war ein verwaltungsrechtlicher Bericht, der per E-Mail versandt wurde, als rechtswirksam beurteilt worden:

> *„Ich schließe, dass ein Polizeibeamter, der einen Bericht, in dem sich eine aussage findet, die den Beamten als Aussteller identifiziert, mittels E-Mail oder einer anderen elektronischen Methode erstellt oder übermittelt, ... diesen ‚unterschrieben' hat ... auch wenn er keine handschriftliche Unterschrift enthält."*[320]

Auch Bundesgerichte hatten in Fällen, auf die die neuen Gesetze noch nicht anwendbar waren, Namensangaben in E-Mails als ausreichend für das Statute of Frauds erachtet. In *Cloud Corporation v. Hasbro, Inc.* war ein Vertrag mittels E-Mail-Kommunikation geändert worden. Der in der E-Mail enthaltene Name des Absenders wurde vom Gericht als Erfüllung des *signature*-Erfordernisses des Illinois Statute of Frauds angesehen.[321] Namen am Ende einer E-Mail wurden schon zuvor im Fall aus Massachusetts *Shattuk v. Klotzbach* als Unterschrift in einem Grundstückskaufvertrag anerkannt.[322] Andererseits ließen Gerichte der Bundesstaaten in einer Anzahl an Fällen vor Erlass der nachfolgend darzustellenden gesetzlichen Neuerungen E-Mails nicht für die Erfüllung der Formerfordernisse der Statutes of Frauds genügen.[323] Zur Unterschriftsqualität einer E-Mail-Adresse findet sich in *United States of America v. Siddiqui* ein bejahendes Urteil noch vor den Neuregelungen. Zu den zahlreichen Aspekten, die hier für die Annahme einer Authentifizierung durch den Absender der E-Mail sprachen, waren gerade auch die E-Mail-Adresse, die den Nachnahmen des Erklärenden enthielt, sowie sein in den Text eingefügter Spitznahme gezählt worden.[324] Ebenfalls weite Akzeptanz als *electronic signature* hatte das Anklicken eines „Ich akzeptiere"-Buttons bei US-Gerichten gefun-

---

[319] Siehe bei Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 577; Menna, VJLT 2001; Miedbrodt, „Das Signaturgesetz in den USA – Electronic Signatures in Global and National Commerce Act", DuD 2000, S. 541-545, S. 542/543; Kommentar zu § 2 Nr. 7 UETA, www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm.

[320] *Doherty v. Registry of Motor Vehicles*, No. 97/CV0050 (Suffolk, SS Massachusetts District Court, May 28, 1997): *„I conclude that a police officer who files or transmits ... a report ... by means of Email or some other electronic method in which there is a statement that identifies the officer making the report and ... has 'signed' the document ... even though the report does not contain a handwritten signature."*

[321] Wobei hier nicht deutlich wird, ob der Name des Unterzeichners im Text der E-Mail, an dessen Ende oder in der E-Mail-Adresse enthalten war; *Cloud Corporation v. Hasbro, Inc.*, 314 F.3d 289 (7th Cir. 2002) (*federal case*). Der Entscheidung in *Commonwealth Aluminum Corporation v. Stanley Metal Associates*, 186 F.Supp.2d 770 (W.D.Ky. 2001) (Kenttucky) ist zu entnehmen, dass ein Name in der E-Mail als Unterschrift gelten sollte.

[322] *Shattuk v. Klotzbach*, 14 Mass. L. Rptr. 360; 2001 WL 1839720 (Mass. Super.).

[323] So in *Bell Fuels, Inc. v. Chevron U.S.A. Inc.*, 2000 WL 305955 (N.D.Ill.) (Illinois); *Ballas v. Tedesco*, 41 F.Supp.2d 531 (D.N.J. 1999) (New Jersey); *In the Matter of Estate of Georgskey*, 2001 WL 824326 (Ohio App. 11 Dist.) (Ohio). *In Page v. Muze, Inc.*, 270 A.D.2d 401; 705 N.Y.S.2d 383; 2000 N.Y. Slip Op. (New York) wurde eine nicht unterschriebene E-Mail als ungenügend erachtet.

[324] *United States of America v. Siddiqui*, 235 F.3d 1318 (11th Cir. 200) (*federal*).

den.[325] Problematisch waren dennoch Beweisregelungen, nach denen zunächst die Authentizität eines Dokuments bewiesen werden musste, damit dessen Inhalt als Beweis vor Gericht taugte.[326] Auch wenn für elektronische Aufzeichnungen das Erfordernis der Vorlage des Originals der Best Evidence Rule ausgesetzt war[327], bildeten diese Bestimmungen teilweise Barrieren wie sie im deutschen Recht nicht zu finden sind.[328]

[325] Z.B. im *federal case CompuServe Inc. v. Patterson*, 89 F.ed 1257 (6th Cir. 1996); Ausführliche Darstellung der Rechtsprechung in den Bundesstaaten siehe bei Mason, *Electronic Signatures in Law*, S. 199, 300.

[326] Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 18. Gleiches galt für „Click-wrap"-Verträge oder elektronische Vertreter (*electronic agents*). Insbesondere Verbraucherschützern erhoben Zweifel an der Rechtsgültigkeit elektronischer Dokumente; Menna, VJLT 2001; Brennan/Barber, „Why Software Professionals Should Support The Uniform Computer Information Transactions Act" (And What Will Happen If They Don't)", www.2bguide.com/docs/proucita4.doc; Nimmer, „UCITA: A Commercial Contract Code", TCL 2000, S. 3 – 17, S. 7. Zur Zurechnung automatisiert generierter Willenserklärungen im deutschen Recht siehe Cornelius, „Vertragsabschluss durch autonome elektronische Agenten", MMR 2002, S. 353-358.

[327] Nach den Federal Rules of Evidence gelten alle Aufzeichnungen als Originale, siehe Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 513.

[328] Miedbrodt, DuD 1998, S. 391.

1.4 Digitale Signatur und ihre gesetzliche Regelung

Die oben geschilderten Probleme der Erfüllung herkömmlicher Formerfordernisse durch elektronische Kommunikations- und Speicherformen sind durch die Digitalisierung bedingt. Digitale Formate können nicht ohne weiteres die durch die traditionellen Authentifizierungsmethoden gebotene Rechtssicherheit liefern. Die Technologie der digitalen Signatur, Public Key Infrastruktur und der Verschlüsselungstechnik bietet technische Lösungen an, welche die Funktionen der Formvorschriften, insbesondere der eigenhändigen Unterschrift, erfüllen können sollen.[329] Da sie vielfach zur Grundlage der hier dargestellten gesetzlichen Signaturregelungen gemacht wurde, sollen Technik und Ansatzpunkte für eine rechtliche Regelung kurz dargestellt werden.

1.4.1 Technische Grundlagen, Funktionsweise und Vorteile

Der Gebrauch der Begriffe elektronische Signatur oder digitale Signatur stiftet bisweilen Verwirrung und führt zu irrtümlichen Annahmen bezüglich ihrer tatsächlichen und rechtlichen Qualität. Deshalb sollen beide Begriffe abgegrenzt und nachfolgend die Technik der digitalen Signatur erläutert werden.

1.4.1.1 Unterscheidung von elektronischer und digitaler Signatur

Die Begriffe elektronische und digitale Signatur sind nicht gleichbedeutend, auch wenn sie häufig synonym verwendet werden.[330] Als elektronische Signatur wird oft allgemein das elektronische Substitut für die Unterschrift bezeichnet. Ihr werden mehrere Technologien und Verfahren zugerechnet, beispielsweise die digitale Signatur, aber auch die bereits oben beschriebene Unterzeichnung elektronischer Daten auf einem Bildschirm (*screen*) oder einem E-Pad mit Hilfe eines E-Pen, das Anklicken eines „I accept"-Buttons oder die Namensnennung in einer E-Mail. Die digitale Signatur bezeichnet eine bestimmte Technologie, „*die darauf zielt, elektronische Daten derart zu sichern, dass es möglich wird, gleichzeitig die Herkunft und die Integrität dieser Daten zu überprüfen.*"[331] Damit bietet die digitale Signatur wesentlich mehr Anwendungsmöglichkeiten als nur als elektronisches Substitut der eigenhändigen Unterschrift zu dienen. Dennoch

---

[329] Die Frage ist, *„ob Antwort auf die Maschine in der Maschine selbst zu finden sein mag."* Eine Reihe von rechtlichen Fragen könnten im Internet obsolet werden durch die Einführung bestimmter technischer Verfahren wie der digitalen Signatur aber auch der digitalen Wasserzeichen, digitaler Fingerabdrücke oder andere Verschlüsselungstechniken; dazu Hoeren, ECLIP, Teil 1, Kap.1, S. 7. *„...wie sollten Technologie und Recht zusammenwirken, um eine digitale Signatur in einem Online-Umfeld zu ermöglichen und durchzusetzen?" („...how should technology and law work together to effect a digital signature in an online environment?")*, York/Tunkel, S. 87.

[330] Ausführlich hierzu: Dumortier/van Eecke, CLSR 1999, S. 106, 107.

[331] *„... designation of a cryptographic technique aiming at securing electronic date in such a way that it enables one to verify at the same time the origin and the integrity of the data."* , Dumortier/van Eecke, CLSR 1999, S. 106. Eine übersichtliche Darstellung der Funktion der digitalen Signatur bieten auch Kath/Riechert, Internet-Vertragsrecht, Berlin 2002, Rn. 109-116.

liegt es nahe, sie für diesen Zweck zu nutzen. Diese Anwendung ist die Schnittfläche zweier sich teilweise überlappender Bereiche. Der erste beschreibt alle möglichen Anwendungen der digitalen Signaturtechnik. Der zweite beinhaltet alle möglichen elektronischen Substituten für die eigenhändige Unterschrift. Nur in dem sich überlappenden Teil findet sich der Einsatzbereich der digitalen Signatur als elektronischer Ersatz für die eigenhändige Unterschrift. Zu erwähnen sind ferner Verfahren, die zur Identifizierung einzigartige biometrische Merkmale nutzen, sowie solche, die wiederum von der eigenhändigen Unterschrift ausgehen und auf elektronischem Weg die Art der Schriftführung auf einer flachen Oberfläche, dessen Geschwindigkeit, Druck, Größe, Winkel und anderes messen und die so ermittelten Daten der elektronischen Nachricht anfügen.[332] Tatsächlich aber ist es vor allem die Technologie der digitalen Signatur diejenige, die zum Gegenstand spezifischer gesetzlicher Regelungen mit technisch-organisatorischen Vorgaben, der Signaturgesetzgebung, wurde.[333]

1.4.1.2 Funktionsweise der digitalen Signatur

Das für die digitale Signatur übernommene Prinzip von öffentlichem und privatem Schlüssel kann an Beispiel der Kryptographie dargestellt werden. Die Kryptographie bei elektronischen Daten kann symmetrisch oder asymmetrisch erfolgen.[334] Bei der asymmetrischen Kryptographie werden zwei unterschiedliche Schlüsselpaare generiert und verwendet. Chiffrier- und Dechiffrierschlüssel sind hier nicht identisch und können für unterschiedliche Zwecke eingesetzt werden.[335] So kann der Chiffrierschlüssel des *Empfängers* öffentlich bekannt gemacht und der Dechiffrierschlüssel geheim gehalten werden. Der Absender verschlüsselt seine Botschaft mit dem öffentlichen Schlüssel (des Empfängers). Ausschließlich der Empfänger kann die Nachricht dann mit seinem privaten Schlüssel entschlüsseln und lesen. Damit kann die Nachricht während der Übertragung im Internet vor dem Einblick Dritter geschützt werden. Die zweite Möglichkeit ist, den *De*chiffrierschlüssel des *Absenders* öffentlich bekannt zu geben und den Chiffrierschlüssel geheim zu halten. Der Absender chiffriert seine Nachricht und schickt sie an den Empfänger, der sie dann mit dem öffentlichen Schlüssel entschlüsseln und feststellen kann, dass diese Nachricht nur vom Absender stammen kann. Durch diese Möglichkeit der Feststellung der Authentizität wirkt das Schlüsselpaar wie eine (digitale) Unterschrift. Aufgrund der Bekanntmachung des einen und der Geheimhaltung des anderen

[332] Bekannt unter dem Begriff Signature Dynamics.

[333] Smedinghoff/Hill Bro, JMJCIL 1999, S. 8.

[334] Symmetrische Verschlüsselung bedeutet, dass sowohl Chiffrierung als auch Dechiffrierung über einen einheitlichen Schlüssel erfolgen. Dieser ist ein in (geheimer) Absprache zwischen den Parteien vereinbartes, möglichst kompliziertes Muster der Verschlüsselung. Über das Internet sind solche geheime Absprachen schlecht möglich und daher nur innerhalb einer geschlossenen Nutzergruppe sinnvoll einsetzbar. Ausführlicher hierzu: Hoeren, *Grundzüge des Internetrechts: E-Commerce/Domains/Urheberrecht*, S. 204, 205; auch Hage/Hitzfeld, in Loewenheim/Koch, *Praxis des Online-Rechts*, München 2001, S. 53.

[335] Hierzu ausführlich: Hoeren, *Grundzüge des Internetrechts: E-Commerce/Domains/Urheberrecht*, S. 205, 206; Köhler/Arndt, Rn. 154, 155; Thot/Gimmy in Kröger/Gimmy, S. 26, 27.

Schlüssels wird diese Verschlüsselung auch als Public Key Cryptography oder, in Bezug auf die hierfür eingesetzte Infrastruktur, als Public Key Infrastructure (PKI[336]) bezeichnet. Dabei kann der öffentliche Schlüssel, je nach System und rechtlichem Rahmen, entweder vom Absender mit der Nachricht mitgeschickt, oder in einem öffentlichen Verzeichnis für jedermann zugänglich gemacht werden. Den privaten Schlüssel kann der Benutzer mit Hilfe einer entsprechenden Software selbst herstellen. Grundlage der Verschlüsselung ist die Manipulation der entsprechenden Computerdaten. Hierfür werden die verschiedensten mathematischen Regeln genutzt und miteinander variiert und verschachtelt.[337] Beispielsweise wird zur Schlüsselgenerierung der so genannte RSA-Algorithmus[338] verwendet. Dies ermöglicht eine schnelle Berechnung der Schlüssel in eine Richtung, nicht jedoch in umgekehrter Richtung. Sind die Qualität des Algorithmus und die Länge des verwendeten Schlüssels ausreichend sicher bestimmt worden, führt ein Angriff, also das Erraten des Schlüssels, in praktisch sinnvollen Zeiträumen nicht zum Erfolg.[339] Bei der digitalen Signatur wandeln gängige Anwendungen[340] die zu versendenden elektronischen Daten – das elektronische Dokument – in einen Zahlencode um. Dieser Hash-Wert ist ein individuelles stellvertretendes Extrakt des Originaltextes und fungiert als eine Art Fingerabdruck, da er für jede zu versendende Nachricht unterschiedlich ist.[341] Der Hash-Wert wird vom Absender verschlüsselt, der ebenfalls verschlüsselten Nachricht angehängt und dem Empfänger übersandt. Der Empfänger entschlüsselt mit dem öffentlichen Schlüssel den übermittelten Fingerabdruck und vergleicht ihn mit dem parallel übermittelten unverschlüsselten Hash-Wert. Stimmen beide überein, ist eine Zurechnung der übermittelten Nachricht möglich. Der Hash-Wert hat eine Beziehung derart zu dem Text, dass jede Veränderung des Textes auch zu einer Veränderung des Hash-Wertes führt. Der Empfänger, der über den Text und den Hash-Wert verfügt, kann durch Anwendung der Hash-Funktion auf den Text und den Vergleich mit dem Hash-Wert feststellen, ob der Text verändert wurde.[342] Beide Verfahren – Verschlüsselung des Textes und digitale Signierung – haben grundsätz-

[336] Die Begriffe Public Key Cryptography und Public Key Infrastructure werden offensichtlich häufig synonym gebraucht. Letzterer ist dabei der gebräuchlichere und seine Abkürzung PKI wird nachfolgend verwendet.

[337] Hage/Hitzfeld in Loewenheim/Koch, S. 50ff., m.w.N. u. ausführlicher Darstellung und Liste gängiger Methoden und Algorithmen.

[338] Benannt nach seinen Entwicklern Rivest, Shamir und Adleman. Hierbei werden sehr große Zahlen gebildet, die in Primzahlen zerlegt werden können und folglich mittels Primzahlen sehr schnell berechnet werden können. Da es jedoch sehr viele Möglichkeiten gibt, diese großen Zahlen aus Primzahlen zu berechnen, ist es für denjenigen, der nur die große Zahl kennt, unmöglich, die einzig korrekte Berechnung zu finden. Er kann diese nur erraten. Siehe hierzu Hoeren, *Grundzüge des Internetrechts*, S. 205, 206.

[339] Hierzu siehe Thot/Gimmy in Kröger/Gimmy, S. 27; Roßnagel, „Die Sicherheitsvermutung des Signaturgesetzes“, NJW 1998, S. 3312 – 3320, S. 3314.

[340] Zum Beispiel eTrust von der Deutschen Post.

[341] Dabei ist die mathematische Transformation so ausgelegt, dass die auch nur um 1 Bit veränderte Ausgangsinformation einen Hash-Wert erzeugt, bei dem sich ungefähr die Hälfte seiner 160 Bits ändert. Hoeren, *Grundzüge des Internetrechts*, S. 205, 206; Köhler/Arndt, Rn. 154, 155; ausführliche technische Darstellung bei Hage/Hitzfeld in Loewenheim/Koch, S. 54, 55.

[342] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 50.

lich nichts miteinander zu tun, können und werden aber vielfach miteinander kombiniert.
Es wird deutlich, dass neben ihrer herausragenden Bedeutung für den E-Commerce, die Technologie der digitalen Signatur diejenige ist, die in größerem Umfang von einer gewissen Infrastruktur (der PKI) und einer Vielzahl von technischen Spezifikationen abhängig ist.

1.4.1.3 Nutzungsmöglichkeiten und Vorteile der digitalen Signatur

Voraussetzung für die Erfüllung insbesondere der konstitutiven Formerfordernisse für Verträge ist, dass die digitale Signatur die Funktionen der Formvorschriften ebenso erfüllt wie papiergebundene Dokumente und eigenhändige Unterschriften beziehungsweise herkömmliche Signaturen. Hinsichtlich der Abschlussfunktion ist die digitale Signatur im Vorteil. Sie wird nicht an einen Text angehängt, sondern als mathematische Transformation auf das gesamte Dokument angewendet. Die digitale Signatur bezieht sich in Gegensatz zu einer handschriftlichen Unterschrift auf den gesamten Text, nicht nur auf eine Seite, da das gesamte elektronische Dokument als Datenmenge in den mathematischen Vorgang der Signaturberechnung eingeht. Der Text, auf den sich die Signatur bezieht, kann hier nicht mehr unbemerkt nachträglich verändert werden.[343] Auch multimedial zusammengesetzte elektronische Dokumente, bestehend aus Grafiken und Texten, Audio- und Videodaten, lassen sich so signieren.[344] Ferner kann die digitale Signatur bei der Kommunikation zwischen Maschinen, zur Kontrolle von Herkunft und Integrität eines Java-Scripts oder zur Authentifizierung einer Webpage eingesetzt werden. Siegel, Stempel, Geldnoten, Ausweise, Rechnungen und alle sonstigen Formen von Berechtigungen und Erklärungen lassen sich so elektronisch nachbilden. Insbesondere wird es möglich, den Faktor Zeit in die Signatur einzubeziehen und damit einen Zeitstempel zu schaffen. Damit reicht ihr Anwendungsbereich weit über den einer handschriftlichen Signatur hinaus.[345] Generell ist jeder Vertragstypus im Internet vorstellbar, auch solche, die zunächst wegen Formvorschriften vom E-Commerce ausgenommen waren.[346] Daneben existieren weitere Einsatzmöglichkeiten, zum Beispiel in der Kommunikation zwischen Behörden und Bürgern, bei Unternehmenspublikationen, im Verhältnis von Unternehmen und Ihren Aktionären, bei elektronischen Patientendaten oder sogar bei Wahlen.[347]

---

[343] Thot/Gimmy in Kröger/Gimmy, S. 27, m.w.N.; auch Cordes, S. 133.

[344] Noack in Dauner-Lieb et al., § 15, Rn. 31.

[345] Dumortier/van Eecke, S. 106; Roßnagel, K&R 2000, S. 313/314; York/Tunkel, S. 87; Redeker, ITRB 2001, S. 47; Oberndörfer, „Digitale Wertpapiere im Licht der neuen Formvorschriften des BGB“, CR 2002, S. 358-362.

[346] So Redeker, ITRB 2001, S. 47, der feststellt, dass die Tatsache, dass diese noch nicht praktiziert werden, nicht bedeute, dass dies nicht in der Zukunft möglich sei.

[347] Siehe z.B. Storr, „Elektronische Kommunikation in der öffentlichen Verwaltung – Die Einführung des elektronischen Verwaltungsakts“, MMR 2002, S. 579-584; Noack, *Unternehmenspublizität – Bedeutung und Medien der Offenlegung von Unternehmensdaten*, Bundesanzeiger Verlag, Köln 2002; ders., „Amtliche Unternehmenspublizität und digitale Medien“, Festschrift für Ulmer, S. 1245-1262, auch Heller et al., „Die Online-Hauptversammlung – Überlegungen zur unmittelbaren Ausübung der Aktio-

1.4.2 Anknüpfungspunkte einer rechtlichen Regelung

Für eine Vielzahl der im Internet bereits etablierten Handlungsformen ist das Vertrauen in diese, insbesondere auf die jeweilige Kommunikation oder Transaktion, von großer Bedeutung.[348] Ein solches Vertrauen bedarf der Feststellung der Identität des Vertragpartners und der Absicherung, dass die übermittelten Dokumente authentisch und unverfälscht sind, entsprechend geschützt aufbewahrt werden und zugänglich bleiben (Authentizität, Integrität und Vertraulichkeit).[349] Wesentlich erscheint auch die Einfachheit der Authentifizierung und die Wirtschaftlichkeit der Generierung sowie eine preiswerte Einführung und Nutzung der Technologie.[350] Um die Funktionsgleichheit zwischen handschriftlicher und elektronischer beziehungsweise digitaler Signatur zu erreichen, ist zunächst die tatsächliche Ausgestaltung der Signaturverfahren und der Sicherungsinfrastruktur bedeutsam. Dies erlaubt eine rechtliche Einrahmung durch gesetzliche technisch-organisatorische Vorgaben oder Haftungsregelungen, um die erforderliche Sicherheit und Vertrauenswürdigkeit der Verfahren zu gewährleisten. Da zum Beispiel gängige digitale Signaturverfahren nicht biometrisch an Personen gebunden sind, könnten theoretisch Dritte diese unbefugt einsetzen. Da neben Nutzer und Empfänger weitere Personen in die Zertifizierungsstruktur eingebunden sind, können Fehlerquellen entstehen, die so bei der eigenhändigen Unterschrift nicht existieren.[351] Insofern ergeben sich gewisse Anforderungen an eine gesetzliche Regelung bereits aus der Technologie der digitalen Signatur. Ferner muss die digitale Signatur in praktikabler Weise sowohl als rechtlich gleichwertig als auch als Beweismittel akzeptiert werden.[352]

1.4.2.1 Anforderungen an digitale Signaturtechnik und Infrastruktur

Bei der digitalen Signatur erfolgt die Schlüsselgenerierung mittels einer von einem Signaturdiensteanbieter bereitgestellten Soft- und Hardware. Die Echtheitsfunktion wird dabei durch die Benutzung des individuellen privaten Signaturschlüssels gewährleis-

närsrechte via Internet“, CR 2002, S. 592-598; Blobel/Pharow, „Wege zur elektronischen Patientenakte“, DuD 2006, S. 164-169; Will, „Wahlen und Abstimmungen via Internet und die Grundsätze der allgemeinen und gleichen Wahl“, CR 2003, S. 126, 131f.

[348] Moritz, „Quo vadis elektronischer Geschäftsverkehr“, CR 2000, S. 61-72, S. 72.

[349] Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 17, 19; Semdinghoff/Hill Bro, JMJCIL 1999, S. 28.

[350] Einfachheit der Herstellung heißt dabei, dass die Technologie einfach zu bedienen und zu dem selben Zweck eingesetzt werden kann, wie heutzutage üblicherweise die eigenhändige Unterschrift. Siehe York/Tunkel, S. 87, 88, die ferner anführen die Einzigartigkeit der elektronischen Signatur dergestalt, dass sie nur durch den Inhaber hergestellt werden kann; die Unmöglichkeit der Fälschung dadurch, dass unautorisierte Nutzer sich unüberwindbaren mathematischen, zeitlichen und materiellen Schwierigkeiten gegenübersieht; die Einfachheit der Authentifizierung, die es dem Empfänger einer Information ermöglicht, den Absender oder Autor auch nach einigem Zeitablauf identifizieren; die Unmöglichkeit der Ablehnung der Urheberschaft durch den Autor, beispielsweise aufgrund von Fälschungen, auch nach einem gewissen Zeitablauf.

[351] Noack in Dauner-Lieb et al., § 15, Rn. 4.

[352] Roßnagel, K&R 2000, S. 314; Thot/Gimmy in Kröger/Gimmy, S. 28.

tet.[353] Diese Soft- und Hardware muss dem technischen Standard entsprechen, einwandfrei funktionieren und rechtzeitig aktualisiert werden.[354] Die Erfüllung der Identitätsfunktion durch die Public-Key-Cryptography bedingt eine weit reichende Infrastruktur. Ein vertrauenswürdiger Dritter muss bestätigen, dass es sich tatsächlich um den persönlichen Schlüssel des Erklärenden handelt, durch den der Schlüsselinhaber eindeutig feststellbar ist.[355] Diese Funktion übernehmen so genannte Trusted Third Parties (TTP) in Form einer Zertifizierungsinstanz. Die von ihr abgegebene Bestätigung, das sogenannte Zertifikat, ist ein Computerdokument, das die Zertifizierungsstelle sowie den Schlüsselinhaber identifiziert und dessen öffentlichen Schlüssel enthält.[356] Der öffentliche Schlüssel muss bei einer vertrauenswürdigen Stelle hinterlegt sein. Der geheime private Schlüssel wiederum darf während seiner Erzeugung, während der Übertragung auf einen Datenträger und anschließend von diesem aus nicht ausgeforscht und nicht kopiert werden können. Unberechtigte dürfen, auch wenn sie im Besitz des Datenträgers sind, nicht auf den geheimen Schlüssel zugreifen können.[357] Der private Schlüssel kann dabei für den Schlüsselinhaber auf einem vom Inhaber genutzten PC gespeichert werden (sogenannte softwarebasierte Lösung) oder er ist, wie aktuell üblich, auf einer Chipkarte gespeichert und an diese dergestalt gebunden, dass die digitale Signierung nur über sie durchgeführt werden kann (hardwarebasierte Lösung).[358] Die Zertifizierungsstelle muss dabei die Funktionen der Sicherungsinfrastruktur übernehmen, also Schlüsselerzeugung, Zertifizierung, Personalisierung der Datenträger des geheimen Schlüssels, die Ausgabe des Datenträgers, gegebenenfalls einen Zeitstempeldienst sowie die Verwaltung der ausgegebenen Zertifikate, Verzeichnis- und Sperrdienst.[359]

---

[353] Thot/Gimmy in Kröger/Gimmy, S. 26, 27; Nöcker, CR 2000, S. 180.

[354] In der Folge können durch Zeitablauf und technischen Fortschritt z.B. Probleme bei der Beweisbarkeit, genauer bei der längerfristigen Aufbewahrung von elektronisch signierter Dokumente, auftauchen. Dazu ausführlich siehe Roßnagel et al., „Erneuerung elektronischer Signaturen – Grundfragen der Archivierung elektronischer Dokumente“, CR 2004, S. 301-306, m.w.N.

[355] Durch den Einsatz dieser *indirect signature authentication* kann der Erklärende beispielsweise nicht freiwillig seinen privaten Schlüssel bekannt machen, um so später seine Autorenschaft der Erklärung zu leugnen (im Gegensatz zur *direct signature authentication* durch den Empfänger). Dazu siehe York/Tunkel, S. 89.

[356] Das Zertifikat wird seinerseits digital signiert, Roßnagel, K&R 2000, S. 313; Thot/Gimmy in Kröger/Gimmy, S. 26, 27. In das Zertifikat können auch zusätzliche Informationen, wie z.B. das Geburtsdatum, der Beruf und sogar die Vertretungsmacht für natürliche und juristische Personen aufgenommen werden, Hörnle, JILT 2000: *„… der Zertifizierungsdiensteanbieter stellt die Verbindung her zwischen der Signatur und der Identität des Absenders.“* (*„… the certification service provider makes the link between the signature and the identity of the sender.“*).

[357] Noch weiter gehend Müglich, MMR 2000, S.13, der auf die Schaffung von Organisationsstrukturen abstellt, die eine unberechtigte Kenntnisnahme bzw. einen unberechtigten Zugang möglichst weitgehend ausschließen. Denkbar sei die Ausgabe von Schlüsseln nur an signaturberechtigte Personen, die Protokollierung der Benutzung des Rechners in einem „Fahrtenbuch“ und besondere Türschließmechanismen u.ä.

[358] Die Hardwarelösung mit einer Chipkarte bedeute sogar hochgradige Sicherheit, da der auf ihr gespeicherte private Schlüssel niemals die Karte verlasse, während er auf der Speicherplatte für Unberechtigte zugänglich sei; Geis, MMR 2000, S. 668, m.w.N. Ein Beispiel und ein in Deutschland gängiges System ist das der SmartCard.

[359] Roßnagel, NJW 1998, S. 3314; Nöcker, CR 2000, S. 179, 180; Für lange bestehende Verträge muss sichergestellt sein, dass weder der Vertragsinhalt noch eine möglicherweise angewandte elektronische Signatur im Zeitablauf verändert werden; Rennie, “ „EU Electronic Commerce Directive: August 1999 – Amendments still avoid consumer protection”, CTLR 1999, S. 239-242, S. 241.

Für eine legislative Regelung ergeben sich daraus mehrere Anknüpfungspunkte. Dies sind zunächst Regelungen hinsichtlich der Technologie und der Infrastruktur. So kann eine bestimmte Technologie vorgeschrieben oder ausschließlich diese im Gesetz mit einer Rechtswirkung verknüpft werden. Hierzu kann etwa die Festlegung gehören, ob ein Verfahren der Public-Key-Infrastructure genutzt und ob überhaupt ein privatrechtlicher Gebrauch und Handel von (bestimmten) Verschlüsselungsverfahren erlaubt sein soll[360], sowie die Entscheidung für eine hardware- oder softwarebasierte Speicherung der privaten Schlüssel.[361] Bedeutender Regelungsgegenstand ist die technische und personelle Sicherheitsinfrastruktur. Die Zertifizierungsstelle muss technisch auf neuestem Stand und zuverlässig sein und ihre Mitarbeiter integer und vertrauenswürdig arbeiten. Die vom Zertifikataussteller verlangten Überprüfungsmaßnahmen bei der Identitätsfeststellung des Antragsstellers müssen konkretisiert werden.[362] Die Zuverlässigkeit der Zertifizierungsstelle kann durch eine vorgeschriebene Kontrolle und/oder gar Genehmigung ihres Tätigwerdens rechtlich gesichert werden. Daneben kann, um die Sicherheit der Schlüssel und ihrer Generierung sicherzustellen, eine Prüfung der technischen Komponenten vorgeschrieben werden.[363] Unter dem Blickwinkel der Rechtssicherheit, Vorhersehbarkeit der rechtlichen Beurteilung der Vertrauenswürdigkeit des eingesetzten Verfahrens und damit der Rechtsdurchsetzung kann ein solches vorab geprüftes Verfahren im Vorteil sein. So können hiermit beweisrechtliche Vorteile verbunden werden.

1.4.2.2 Anforderungen an die Ausgestaltung der Signaturverfahren

In einem Gerichtsverfahren zur Bestimmung der Rechtswirksamkeit einer elektronischen oder digitalen Signatur wird auf die Authentizität und Integrität des signierten Dokuments abgestellt. Um Funktionsgleichheit herzustellen, muss die digitale Signatur jedoch auch die Warnfunktion erfüllen.[364] Wegen der schnellen Kommunikation – digitale Signaturen werden automatisch erstellt und in Sekundenbruchteilen gesendet[365] – und der Abstraktheit des Unterschreibevorgangs kommt es daher wesentlich auf die Ausgestaltung des Signiervorganges an, da das Ausdrucksvermögen elektronischer und digitaler Signaturen je nach ihrer technischen Ausgestaltung erhöht oder gemindert

[360] So bestand beispielsweise in den USA ein Exportverbot wonach Verschlüsselungstechnik militärisches Gut ist. Siehe Hage/Hitzfeld, S. 52 f. m.w.N. und ausführlich Beucher/Schmoll, „Kryptotechnologie und Exportbeschränkungen“, CR 1999, S. 529-534.

[361] Geis, MMR 2000, S. 668, m.w.N.

[362] Hier ist ein Ausgleich zu finden zwischen dem für die notwendige hohe Sicherheit unabdingbaren Aufwand einer Überprüfung und deren Zumutbarkeit für den Diensteanbieter; Neuser, MMR 1999, S. 69.

[363] Roßnagel, NJW 1998, S. 3314.

[364] Darstellung der Ansichten über die Erfüllung der Warnfunktion durch die elektronische Form des § 126a BGB bei Steinbeck, „Die neuen Formvorschriften im BGB“, DStR 2003, S. 644-650, S. 648/649.

[365] Der Faktor Zeit wird nur nachfolgend, beispielsweise in einem Mailing-Protokoll, verzeichnet. Sofern ausführliche Regelungen zur Rückbestätigung fehlen, verschwände jegliche durch den traditionellen üblichen zeitlichen Kontext gebotene Möglichkeit der Rückversicherung und des Schutzes; Hoeren, ECLIP, Teil 1, Kap.1, S. 7.

ist.[366] Der Signiervorgang darf deshalb nicht automatisiert, sondern muss in mehrere zu durchlaufende Schritte unterteilt werden.[367] Vor dem Signieren dürfen keine anderen als die gewünschten Daten angezeigt werden und beim Prüfen keine falschen oder nicht signierten Daten generiert oder angezeigt werden.[368] Für die Autorisierung des Nutzers sind Verfahren gängig, die mit einer in ein Lesegerät einzuführenden Chipkarte und/oder der Autorisierung mittels einer PIN arbeiten. Die Warnung muss im Zusammenhang der Erklärung erfolgen und sich aus Umständen ergeben, die unmittelbar mit der Erklärung zusammenhängen. Sie darf nicht antizipiert, zeitlich lange zuvor erfolgen und/oder für eine nicht bestimmbare Anzahl von Erklärungen gelten.[369] Entscheidend ist die Verwendung und der konkrete Einsatz einer PIN, die ihrerseits durch das Verfahren nicht gespeichert (*cachen*) werden darf, sondern vor jedem Aufrufen des Signierprogramms ihre erneute Eingabe fordert.[370] Im Rahmen einer rechtlichen Regelung können entsprechende Mindestanforderungen an die Verfahren gestellt werden hinsichtlich eines bestimmten Ablaufs der Signaturprogramme und des vom Nutzer zu durchlaufenden Menüs, sowie hinsichtlich der Methode des Zugriffsschutzes. Diese können im Rahmen der Regelungen zu Genehmigungs- und Kontrollverfahren festgeschrieben werden.

1.4.2.3 Haftungsregime

Bei der Errichtung eines rechtlichen Rahmens für digitale Signaturen sind eine Benennung der Pflichten der Parteien und ein sachgerechtes Haftungsregime von besonderer

---

[366] Cavanillas, ECLIP, Teil 2, Kap.1, S. 11; Hoeren, ECLIP, Teil 1, Kap.1, S. 7; Hörnle, JILT 2000; Wright, 1999, S. 401; Noack in Dauner-Lieb et al., § 15, Rn. 13; Nöcker, CR 2000, S. 179;

[367] Vgl. Fringuelli/Wallhäuser, CR 1999, S. 100.

[368] Vgl. Roßnagel, NJW 1998, S. 3314.

[369] Roßnagel, NJW 1998, S. 3314. So kann eine bloße allgemein gehaltene Belehrung durch die Zertifizierungsstelle über die rechtliche Bedeutung des digitalen Signiervorganges als Warnung nicht genügen. Vgl. Scheffler/Dressel, „Vorschläge zur Änderung zivilrechtlicher Formvorschriften und ihre Bedeutung für den Wirtschaftszweig E-Commerce“, CR 2000, S. 378-384, S. 382. Der bloße Gebrauch einer Chipkarte wird diesbezüglich kritisiert, da das Einlegen der Chipkarte in ein Lesegerät ein völlig wertungsfreier Vorgang sei, bzw. die Karte möglicherweise in dem Gerät steckengelassen werde; Scheffler/Dressel, CR 2000, S. 382.

[370] Scheffler/Dressel, CR 2000, S. 382. Dem hier vorauszusetzenden Personenkreis, der sich ausdrücklich für die Nutzung dieser Technologie entschieden hat, sind Wesen und Zweck einer PIN als persönlicher Identifikationsnummer und der Zusammenhang zu Wesen und Zweck der Unterschrift bekannt. Siehe auch Noack in Dauner-Lieb et al., § 15, Rn. 13. Als problematisch wird bewertet, dass der gesamte beschriebene Vorgang und damit die für die Warnfunktion entscheidenden Handlungen ihrer Natur nach mehrdeutig sind. Die Eingabe (oder Markierung) von Daten, die Eingabe einer PIN und die Absendung der Daten durch das Drücken einer Return-, Enter- oder Bestätigungstaste wiederholen sich so in den unterschiedlichsten und eben auch in unverbindlichen Lebenssituationen. So zutreffend Scheffler/Dressel, CR 2000, S. 382/383, die jedoch zu dem Schluss kommen, dass einem Vorgang (Eingabe der PIN), der derart häufig in unterschiedlichen Lebenslagen abläuft (Abheben von Geld am Geldautomaten, Anmelden bei einem Computer etc.) und dem jeweils eine unterschiedliche Bedeutung zukommt, die der Verwender erst werten muss, nicht die Warnfunktion im Sinne der Schriftform oder schriftlichen Form zukommen kann. Dem ist entgegenzuhalten, dass ein solches Verfahren nicht zufällig oder beiläufig ausgeführt wird, sondern dann, wenn der Nutzer beabsichtigt, einer Erklärung eine besondere Bedeutung beizumessen.

Bedeutung. Die vorgenannten technisch-organisatorischen und persönlichen Anforderungen an die Zertifizierungsinstanz lassen sich im Rahmen von Genehmigungs- oder Kontrollverfahren festschreiben. Daneben muss ein entsprechend ausgestaltetes Haftungsregime treten. Dahinter steht die Annahme, dass sachgerechte und durchsetzungsfähige Haftungsregelungen die erforderliche Sicherungsinfrastruktur durch ihren präventiven Effekt absichern können.[371]

Anknüpfungspunkt für die konkreten Haftungstatbestände sind zunächst die Verkehrssicherungspflichten des Diensteanbieters. Folglich ist die Bestimmung verhaltensbezogener Anforderungen und damit der Sorgfaltspflichten entscheidend.[372] Zu unterscheiden ist dabei zwischen der Haftung für die im Zertifikat enthaltenen Informationen und der Haftung für die Nichteinhaltung technisch-organisatorischer Anforderungen. Hinsichtlich der Haftung für Angaben im Zertifikat kann weiter unterschieden werden zwischen der Haftung für Angaben des Zertifizierungsdiensteanbieters selbst und derjenigen für Angaben des Zertifikatsinhabers.[373] Bezüglich der Informationen über den Zertifikatinhaber kann der Zertifikataussteller nur dann haften, wenn ihm eine zuverlässige Überprüfung der Informationen des Antragstellers möglich ist. Eine Konkretisierung von Prüfumfang und Inhalt der Dokumentationspflicht ist hier sinnvoll. Der Charakter als Verkehrssicherungspflichten spräche für eine Haftung in Form des vermuteten Verschuldens mit der Möglichkeit des Entlastungsbeweises.[374] Eine andere Möglichkeit sind zertifikatimmanente Haftungsausschlüsse, die dem Diensteanbieter ermöglichten, darüber hinaus nicht für Fehler im Zertifikat haften zu müssen, die auf Informationen des Zertifikatinhabers beruhen. Bezüglich der Haftung bei Nichteinhaltung der technisch-organisatorischen Anforderungen durch den Zertifizierungsdiensteanbieter muss klargestellt werden, ob ein Sicherungserfolg oder lediglich eine Sicherungstätigkeit geschuldet sein soll. Eine verschuldensunabhängige Ausgestaltung der Haftung kann dabei deren Durchsetzungschancen erhöhen.[375] Von Bedeutung ist hier auch die Regelung von Kausalitätsfragen. Sofern die Beweislast beim Geschädigten liegt, muss dieser

[371] Fraglich ist, ob und inwieweit Haftungsregelungen diese Sicherungsinfrastruktur sogar gewährleisten und damit die Sicherheitserwartungen des Rechtsverkehrs in gleichem Maße wie ordnungsrechtliche Vorgaben und Kontrollen erfüllen können und ggf. die staatliche Sicherheitsgewährleistung und ordnungsrechtliche Maßnahmen kompensieren können und sollen. Diese Konzeption „Haftung statt Aufsicht“ will Regelungsziele durch die Aktivierung von Marktmechanismen erreichen, welche über die Haftung als durchsetzungsorientiertes Rechtsinstrument ausgelöst werden. Hierzu ausführlich Neuser, MMR 1999, S. 67, 71, 74 m.w.N.

[372] Ein Haftungsregime kann als Verschuldens- oder als Gefährdungshaftung ausgestaltet werden. Diese Frage ist jedoch von untergeordneter Bedeutung. Die Gefährdungshaftung birgt ein größeres Haftungsrisiko und verfügt über eine größere präventive Wirkung. Hierzu ist richtig festgestellt worden, dass bei entsprechender Ausgestaltung des Verschuldensnachweises beide Regelungsformen einen gerechten Schadensausgleich in vergleichbarer Weise erfüllen können. Siehe Neuser, MMR 1999, S. 72, 73.

[373] Aus diesen Angaben soll sich für einen Dritten die Identität des Nutzers sowie dessen Adresse oder Ort der Niederlassung ergeben. Probleme ergeben sich, wenn das Zertifikat zwar gültig ist, der so ausgewiesene Nutzer jedoch nicht wirklich existiert. Gleiches gilt, wenn die Prüfung des Zertifikats im Verzeichnisdienst nicht verlässlich ist, der Diensteanbieter nicht ermittelt werden kann oder aber der Kunde die Existenz des auf seinen Namen ausgestellten Zertifikats bestreitet. Darstellung bei Neuser, MMR 1999, S. 68.

[374] Etwa der Nachweis der ausreichenden, d.h. ihm zumutbaren Überprüfung der Identität des Antragsstellers; Neuser, MMR 1999, S. 69, 74.

[375] Neuser, MMR 1999, S. 70.

nachweisen, dass eine technisch-organisatorische Anforderung nicht eingehalten wurde und dass der Schaden gerade auf der Nichteinhaltung beruht. Gerade dies kann sich im Dreiecksverhältnis Empfänger, Zertifikatinhaber und Zertifizierungsdiensteanbieter schwierig gestalten, wenn die schädigende Ursache aus dem Bereich des Zertifikatinhabers oder auch des Diensteanbieters herrührt.[376] In Fällen, bei denen der Anspruch gegen den Zertifikatinhaber nicht durchgesetzt werden kann, weil Sicherungsmaßnahmen des Diensteanbieters unzureichend waren, kann eine sachgerechte Risikoverteilung durch eine Kausalitätsvermutung zugunsten des Geschädigten mit der Möglichkeit des Entlastungsbeweises geschaffen werden.[377] Grundsätzlich besteht das Problem der Unzugänglichkeit entscheidungserheblicher Tatsachen für den Geschädigten für im Verantwortungsbereich des Schädigers liegende Ursachen – zutreffend als „Informationsasymmetrie“ bezeichnet.[378] Lösungen böten hier entsprechende Beweiserleichterungen oder ein selbständiger Auskunftsanspruch des Geschädigten. Ferner ist zu bestimmen, welcher Zeitpunkt für die Einhaltung technisch-organisatorischen und anderer sicherheitsrelevanter Pflichten zugrunde gelegt werden soll. Dies kann der Zeitpunkt der Erstellung des Zertifikats[379] oder der Moment der Verwendung der Signatur sein, da das Vertrauen des Dritten als Zurechnungsgrund für die Haftung des Diensteanbieters sich in diesem Moment konkretisiert. Hinsichtlich der im Zertifikat enthaltenen Informationen sollte letzteres zutreffen für die Angaben des Diensteanbieters. Anders ist dies bei Angaben, die vom Zertifikatinhaber stammen, da diese sich außerhalb des Verantwortungsbereichs des Diensteanbieters vollziehen und er also nicht für deren fortbestehende Richtigkeit haften kann.[380] Er sollte ferner dafür haften, dass er zum Zeitpunkt der Erstellung von Zertifikat und Schlüssel bestehende und bekannte Sicherheitsrisiken ausschließt. Möglich ist auch eine Haftung für Schäden durch solche Sicherheitslücken, die zum Zeitpunkt der Zertifikatsverwendung erkennbar waren.[381] Eine mögliche Begrenzung des Transaktionswertes, aufgenommen in die Zertifikate, erleichterte die Kalkulation des Haftungsrisikos für den Diensteanbieter und hätte auch Auswirkungen auf die Versicherbarkeit dieses Risikos.[382] Andererseits kann eine Verpflichtung der Dienstean-

[376] Die Verantwortlichkeit des Zertifikatinhabers kann ggf. nicht auszuschließen sein, der Geschädigte also zwei mögliche Schuldner haben, die sich jeweils mit dem Hinweis auf den nicht auszuschließenden Kausalbeitrag des anderen entlasten können.

[377] Aufgrund einer solchen widerlegbaren Vermutung der technisch-organisatorische Mängel im Bereich des Diensteanbieters haftete dieser nur für vorhandene eigene Mängel; Neuser, MMR 1999, S. 70, 73.

[378] Der Geschädigte benötigt interne Informationen über die betrieblichen Abläufe und die realisierten Sicherheitsstandards. Neuser, MMR 1999, S. 70.

[379] Die Verantwortlichkeit des Diensteanbieters resultiert daraus, dass er das Zertifikat in den Rechtsverkehr gebracht hat. Dieser Ansatzpunkt (Produktbezug) entspräche dem der Produkthaftung. siehe Neuser, MMR 1999, S. 70, 72.

[380] Eine Haftungslücke kann hier durch einen eigenständig durchsetzbaren Sperrungsanspruch gegen die Zertifizierungsstelle vermieden werden; Neuser, MMR 1999, S. 73.

[381] Dies entspräche einem Haftungsausschluss für Entwicklungsrisiken, wobei das jeweils realisierte Sicherheitsniveau mit der dynamischen technischen Entwicklung Schritt halten könne. So Neuser, MMR 1999, S. 74.

[382] Dabei kommen absolute oder relative Haftungshöchstgrenzen in Betracht. Erstere kämen nach Erreichen der Haftungshöchstgrenze einem vollständigen Haftungsausschluss gleich. Bei einer relativen Haftungshöchstgrenze erhöht sich das Haftungsrisiko des Diensteanbieters mit jeder Transaktion, was zu einer schlechteren Kalkulierbarkeit des Haftungsrisikos führte. eine solche Lösung wird als für die

bieter zur Bereitstellung ausreichender Finanzmittel, um das Haftungsrisiko tragen zu können, das Vertrauen der Nutzer und Dritter fördern.[383]
Ein weiterer Aspekt ist die Frage des Mitverschuldens des Empfängers und des Zertifikat- und Signaturschlüsselinhabers. Wesentliches Element für die rechtliche Wirksamkeit der digitalen Signatur ist die Tatsache, dass der Signaturschlüsselinhaber den geheimen Signaturschlüssel unter seiner ausschließlichen Kontrolle hält. Das hierzu gegenwärtig angewendete Mittel ist das Modell des Wissens und Habens im Sinne von Besitz der Signaturkarte und der Kenntnis einer geheimen Information, hier üblicherweise der PIN.[384] Sofern also der Zertifikatinhaber die Geheimhaltung dieser Elemente schuldhaft nicht ausreichend gewährleistet und diese Sorgfaltspflichtverletzung zu einem Schaden führt, so haftete er nach den allgemeinen Regeln. Problematisch ist allerdings auch im Verhältnis des Geschädigten zum Zertifikatinhaber die oben beschriebene Informationsasymmetrie, das heißt die mangelnde Kenntnis von den tatsächlichen, den Verlust der Geheimhaltung konkret bedingenden Umständen, insbesondere da auch Dritteingriffe, etwa in Form von Angriffen mittels sog. Trojanischer Pferde, nicht ausgeschlossen werden können.[385] Ferner sollte auf Seiten des Empfängers bestimmt werden, wann ein schutzwürdiges Vertrauen in das Zertifikat nicht mehr gegeben ist. Dieser Vertrauensschutz könnte auf nicht offensichtlich vorliegende Sicherheitsmängel oder Verfälschungen beschränkt werden. Daraus ergäbe sich eine Mitwirkungspflicht für den Dritten, beispielsweise dahingehend, einen entsprechenden Prüfungsdienst des Diensteanbieters zu nutzen.[386]

1.4.2.4 Feststellung der Formwirksamkeit

Eine so erreichte Funktionsgleichheit zwischen digitaler Signatur und eigenhändiger Unterschrift[387] kann sich in einer gesetzlichen Gleichstellung beider Handlungsformen ausdrücken, ob durch Rechtsprechung oder Gesetz. Hier muss unterschieden werden zwischen der Formerfüllung durch (einfache) elektronische und digitale Signaturen und deren rechtlicher Beurteilung in Deutschland und in den *common law*-Staaten England und den USA. In letzteren diente eine solche generelle Feststellung der Rechtsgültigkeit elektronischer Signaturen nach dem oben zu Formen der *signature* und zur Akzeptanz elektronischer Signaturen auch bei *signature*-Erfordernissen Festgestellten[388] haupt-

Marktgängigkeit von Zertifikaten unerlässlich angesehen, siehe Blum, K&R 2000, S. 67; Neuser, MMR 1999, S. 71.

[383] Neuser, MMR 1999, S. 71.

[384] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 50, 51.

[385] Dazu ausführlich unten unter 3.2.1.5 und 3.3.7.

[386] So wäre ein schutzwürdiges Vertrauen dann nicht mehr gegeben, wenn ein zwischenzeitlich widerrufenes Zertifikat verwendet würde, der Dritte sich von der aktuellen (Un-)Gültigkeit des Zertifikats überzeugen könnte. Neuser, MMR 1999, S. 71.

[387] Funktionsgleichheit ist nur gegeben, wenn sowohl die Sicherheitsanforderungen an digitale Signaturen als auch das tatsächlich gewährleistete Sicherheitsniveau der Signaturverfahren vergleichbar sind, Roßnagel, K&R 2000, S. 314

[388] Siehe 1.3.2.4 und 1.3.3.4.

sächlich der Klarstellung und Vereinheitlichung. Hinsichtlich der digitalen Signatur bliebe zunächst eine wie oben geschilderte gesetzliche Ausgestaltung deren Anwendung. An diese Signaturgesetzgebung könnte dann auch dort für bestimmte Formerfordernisse, die zum Beispiel zwingend eine eigenhändige Unterzeichnung erfordern, eine Gleichstellung erfolgen. In Deutschland hingegen ist die Gleichstellung der elektronischen Signatur mit dem Unterschriftserfordernis des § 126 BGB im Sinne einer vollen Funktionsgleichstellung nur im Rahmen eines wie vorgehend beschriebenen Regelungssystems mit der digitalen Signatur möglich. Ähnlich ist dies hinsichtlich einiger Formerfordernisse in England und den USA, beispielsweise die Aufbewahrung von Dokumenten oder deren notarielle Beglaubigung betreffend.

1.4.2.5 Beweisregelungen

Beweisfragen ergeben sich wie vorgehend dargestellt bereits innerhalb des Haftungsregimes in Bezug auf die Beweisbarkeit haftungsbegründender Tatsachen. Anspruch der digitalen Signatur ist es, ein ebenso zuverlässiger und unbestreitbarer Beweis für die Authentizität, Integrität, Abgabe und Inhalt einer rechtserheblichen Erklärung zu sein, wie dies bei eigenhändig unterzeichneten Dokumenten der Fall ist. Hier geht es um die Zulassung der digital signierten elektronischen Daten als Beweismittel sowie um die Beurteilung ihres Beweiswertes durch die Rechtsordnung. Hinsichtlich des ersten Aspekts käme eine allgemeine Regel in Betracht, nach der bestimmte elektronische Signaturen grundsätzlich als Beweismittel zuzulassen sind, unabhängig davon, ob sich dies aus dem Gesetz ergeben oder im Einzelfall vom Gericht zu entscheiden ist.[389] Eine Gleichstellung von elektronischen Signaturen und eigenhändiger Unterschrift hinsichtlich der Zulassung als Beweismittel wird zwar dort für überflüssig erachtet, wo jedes Beweisangebot als *factual evidence* angesehen wird und der Beweiswürdigung des Gerichts unterliegt.[390] Auch gibt es in kaum einer Rechtsordnung ein spezifisches Verbot hinsichtlich der Zulassung von elektronischen Daten und die Privatautonomie erlaubt ohnehin eine dahingehende vertragliche Festlegung.[391] Eine Feststellung der generellen Beweistauglichkeit erscheint dennoch zweckmäßig, ebenso eine entsprechende Regelung zur Anerkennung digitaler Signaturen ausländischer Herkunft.

---

[389] Siehe bei Dumortier/van Eecke, CLSR 1999, S. 109,110. Nach englischem und US-amerikanischem Recht sind Beweismittel durch das Gericht zuzulassen. Sowohl handschriftliche als auch digitale Signaturen sind hier als *factual evidence* anerkannt; Geis, MMR 2000, S. 669; Dumortier/van Eecke, CLSR 1999, S. 109. Digitale Signaturen unterliegen nach deutschem Recht als Augenscheinsbeweis der freien Beweiswürdigung und bezüglich (papierner) Urkunden gibt es sogar Beweis*kraft*regeln; Deville/Kalthegener, NJW-CoR 1997, S. 172; Dumortier/van Eecke, CLSR 1999, S. 109. siehe auch oben unter 1.3.1.3.

[390] Geis, MMR 2000, S. 669; Dumortier/van Eecke, CLSR 1999, S. 109.

[391] Eine generelle Vorschrift sei nicht notwendig, da entweder überflüssig oder ohne Substanz, sofern restriktive Traditionen gegen eine dahingehende Gleichstellung mit der traditionellen Urkunde sprechen. Ziel solle vielmehr die freie Beweiswürdigung der in einer elektronischen Authentifizierung vermuteten qualifizierenden Merkmale und folglich eine Regelung ohne materiellen Einfluss auf die Beweiswürdigung sein. So z.B. Gravesen/Dumortier/van Eecke, „Die europäische Signaturrichtlinie – Regulative Funktion und Bedeutung der Rechtswirkung“, MMR 1999, S. 577-585, S. 581.

Die Beweiskraft einer digitalen Signatur ist allein abhängig von ihrer Sicherheit. Sie muss sich nach der tatsächlichen faktischen Sicherheit der zugrunde liegenden Technik zum Zeitpunkt des Rechtstreits bemessen. Entscheidend ist, dass die oben genannten technisch-organisatorischen Anforderungen erfüllt sind.[392] Der Beweiswert einer digitalen Signatur kann mit ihrem Alter abnehmen[393] und es besteht grundsätzlich die Gefahr, dass die jeweilige digitale Signatur, zum Beispiel von einem Sachverständigen, als materiell unzureichend beurteilt wird, etwa aufgrund der ständigen Fortentwicklung insbesondere der Kryptographietechnik.[394] Andererseits kann einer digitalen Signatur aufgrund ihrer faktischen Fälschungssicherheit im Zuge der freien Beweiswürdigung auch ein größerer Beweiswert als einer traditionellen Unterschrift zugesprochen werden.[395] Dies spräche für einen Ansatz, der die freie Beweiswürdigung zum Kern hat, und gegen eine starre, unwiderlegbare Beweiskraftregel.[396] Allein die Möglichkeit der richterlichen Beweiswürdigung digitaler Signaturen garantiert jedoch nicht den tatsächlichen Beweis hierüber. Aus Sicht des Zertifikatinhabers oder Empfängers kann die Beweislast für das Funktionieren der Sicherungsinfrastruktur ein nahezu unüberwindbares Hindernis darstellen.[397] Will man dies vermeiden, müssten sie von der Last befreit werden, die Einhaltung der Sicherheitsanforderungen beweisen zu müssen[398], oder ihnen müsste die Beweisführung erleichtert werden, etwa durch eine gesetzliche Sicherheitsvermutung. Tatsächlich kann die Beweiskraft der digitalen Signatur über die Einführung von Beweiskraftregeln wie einer gesetzlichen Vermutung oder Anscheinsbeweisen, oder gar der Erstreckung von für die traditionelle Schriftform und handschriftliche Urkunde etwaig bestehenden Beweisregeln auf die digitale Signatur, unterstützt werden.[399] Möglich sind starre, nicht widerlegbare Beweisregeln oder durch Vollbeweis widerlegbare Beweisvermutungen.[400] Der Beweiswert einer digitalen Signatur hängt immer auch vom Grad der Wahrscheinlichkeit des Vorliegens eines Missbrauchsfalles ab.[401] Eine absolute Fälschungssicherheit wird auch die digitale Signatur nicht bieten können. Da im Rahmen der freien Beweiswürdigung nach § 286 Abs. 1 BGB letztlich allein der Grad der

[392] Nöcker, CR 2000, S. 178/179. Hier ist jedoch auch anzumerken, dass die Echtheit jeder einem Gericht als Beweis vorgelegten Unterschrift bestritten werden kann und der Beweis ihrer Echtheit dann vom graphologischen Gutachten abhängt, weshalb deren Bedeutung im Beweisrecht auch nicht überschätzt werden sollte, so Redeker, ITRB 2001, S. 48. Siehe dazu auch unten unter 3.2.2.1 ff.

[393] Köhler/Arndt, Rn. 169; Redeker, ITRB 2001, S. 48.

[394] Gravesen/Dumortier/van Eecke, MMR 1999, S. 581.

[395] Fringuelli/Wallhäuser, CR 1999, S. 100.

[396] Roßnagel, NJW 1998, S. 3318; Gravesen/Dumortier/van Eecke, MMR 1999, S. 581.

[397] Siehe oben unter 1.4.2.3 zur Informationsasymmetrie. Beweisprobleme und -kosten könnten für die Nutzung von Signaturverfahren zum entscheidenden Hindernis werden; so zutreffend Roßnagel, K&R 2000, S. 318.

[398] Roßnagel, „Europäische Signatur-Richtlinie und Optionen ihrer Umsetzung“, MMR 1999, S. 261-266, S. 265.

[399] Roßnagel, NJW 1998, S. 3314.

[400] Zu gesetzlichen Vermutungen siehe ausführlich Smedinghoff/Hill Bro, JMJCIL 1999, S. 26 ff., die diesen drei Eigenschaften zuweisen: die Übertragung der Beweispflicht auf diejenige Partei, die in der besseren Lage ist, den Beweis zu erbringen; die Förderung einer gerichtlichen Entscheidung; und die Tatsache, dass das Vermutete mit dem übereinstimmt, was höchstwahrscheinlich tatsächlich zutrifft.

[401] Siehe dazu auch unten 3.2.1.

Wahrscheinlichkeit zählt, sind unwiderlegliche Beweisregeln im Sinne des § 286 Abs. 2 BGB, bei denen allein durch eine technische Verifikation die Echtheit einer Willenserklärung bestätigt wird, nicht ratsam.[402]
Eine rechtliche Regelung könnte über eine Vermutung der Sicherheit der digitalen Signatur auf die Bejahung einer generellen Beweiskraft hinsichtlich der Authentizität und Integrität der Erklärung abzielen. Eine solche Vermutungsregel kann den Vertragsparteien Rechtssicherheit und Vorhersehbarkeit rechtlicher Beurteilungen bieten[403] und Grundlage für eine Echtheitsvermutung für elektronische Dokumente sein. Allerdings muss für die Grundlagen einer solchen Vermutung, also für die Sicherheitsinfrastruktur und ihre Kontrolle, zum Beispiel die Vorabprüfung der Sicherheit von Diensteanbieter und eingesetzten Komponenten, erheblicher Aufwand betrieben werden. Ob sie tatsächlich zu einer prozessual zuverlässigen Einschätzung der Erfolgsaussichten führen wird, wird teilweise wegen der Probleme bei der Ermittlung der den Entlastungsbeweis tragenden Tatsachen als nicht sicher eingeschätzt.[404]

1.4.2.6 Technikneutralität und technische Standards

Die obigen Feststellungen beruhen auf der Annahme, dass die digitale Signatur die derzeit sicherste und damit wohl einzige wirkliche Alternative zur eigenhändigen Unterschrift darstellt. Die Computertechnik bewegt sich jedoch in schnellen Schritten vorwärts. Für eine rechtliche Regelung kann es deshalb sinnvoll sein, eine gewisse Technikoffenheit oder -neutralität zum Ziel zu haben. Die Beschränkung auf den Einsatz einer bestimmten Technologie kann den unbeabsichtigten Ausschluss anderer ebenfalls angemessener Authentifizierungsmethoden implizieren. Die Entwicklung anderer gleichwertiger oder sogar überlegener Technologien könnte damit verhindert werden. Andererseits ist fraglich, ob diese Technikneutralität der Erreichung der oben genannten Ziele dient. Technikneutralität eines Signaturgesetzes sollte folglich bedeuten, eine bestimmte Technologie nicht gegenüber anderen unfair und unbegründet zu favorisieren. Solange andere Technologien nicht diskriminiert werden, würden dadurch legislative Lösungen für rechtliche Probleme einer bestimmten Technologie, hier der digitalen Signatur, nicht verhindert.[405] Wie oben dargelegt, ist es für die Sicherheit der digitalen Signatur sinnvoll, spezifische technisch-organisatorische Bedingungen und somit Details hinsichtlich der Verfahrensweise und Verwendung der Technik festzulegen.[406]

---

[402] Jungermann, „Der Beweiswert elektronischer Signaturen“, DuD 2003, S. 69-72, S. 70.

[403] Smedinghoff/Hill Bro, JMJCIL 1999, S. 27, 29; a.A. Müglich, MMR 2000, S.13, der unter Hinweis auf den erheblichen Aufwand zur Aufrechterhaltung einer Sicherheitsvermutung bezweifelt, ob die Einführung solcher gesetzlicher Vermutungsregeln tatsächlich zu einer zuverlässigen Einschätzung der Erfolgsaussichten einer Klage führt. Problematisch blieben hier Schwierigkeiten bei der Ermittlung der den Entlastungsbeweis tragenden Tatsachen, wie oben dargestellt (siehe 1.4.2.3 und 1.4.2.4).

[404] Müglich, MMR 2000, S.13, der sogar den Beweis durch Augenschein als hinreichende prozessuale Grundlage bezweifelt. Mangels ausreichender Judikatur ließen sich lediglich Einschätzungen, aber keine belastbaren Prognosen abgeben.

[405] Zutreffend Smedinghoff/Hill Bro, JMJCIL 1999, S. 35, 36.

[406] Dumortier/van Eecke, CLSR 1999, S. 107; Smedinghoff/Hill Bro, JMJCIL 1999, S. 36, 37.

Eine gesetzliche Ausgestaltung dieser Bedingungen der Anwendung digitaler Signaturen sollte vor dem Hintergrund der Eröffnung der mit dieser Technologie verbundenen vorteile daher nicht unter Hinweis auf eine erforderliche Technikneutralität unterbleiben. Es gilt, was *Smedinghoff* und *Hill Bro* gesagt haben:

> *„Bei der Erarbeitung von Gesetzen zur elektronischen Signatur müssen wir acht geben, die* [Technik-]*Neutralität nicht als Entschuldigung dafür zu nehmen, neue legitime und durch eine neue einzigartige Technologie aufgeworfene Themen nicht anzugehen oder – noch schlimmer – die Neutralität als Mittel der Diskriminierung solcher Technologien und ihrer Entwicklung einzusetzen, die von den meisten als für einen sicheren E-Commerce förderlich angesehen werden.“*[407]

Gegenstand der Signaturgesetzgebung ist auch die Erstellung technischer Standards. Gerade bei der Regulierung technischer Produkte und Anwendungen spielen technische Spezifikationen und Standards eine bedeutsame Rolle.[408] In Frage kommen Standardisierungen für die Festlegung und fortwährende Anpassung der technisch-organisatorischen Anforderungen an die Sicherheitsinfrastruktur. So kann die Rechtssicherheit des Diensteanbieters erhöht werden, indem eine verlässliche Grundlage zur Beurteilung des Sorgfaltsmaßstabes existiert.[409] Standards können bindenden Charakter haben, nicht bindende Standards wiederum können die Entwicklung eines bestimmten Marktes entscheidend fördern oder als Innovationshemmnis wirken. Einen bindenden Effekt bekommen Standards im Zusammenspiel mit dem Recht, etwa wenn sie direkt in ein Gesetz eingefügt werden, die Regelung selbst konkrete Vorgaben enthält, oder sie durch Verweise in der gesetzlichen Regelung auf außerrechtliche Technikstandards inkorporiert werden.[410]

---

[407] Smedinghoff/Hill Bro, JMJCIL 1999, S. 6: *„… we must be careful as we draft electronic signature legislation not to let neutrality become an excuse to avoid addressing legitimate new issues raised by a unique technology, or worse, use neutrality as a means to discriminate against the development of those technologies seen by most as facilitating secure e-commerce.”*

[408] Dazu ausführlich Dumortier/van Eecke, CLSR 1999, S. 107 u. 108.

[409] Neuser, MMR 1999, S. 73.

[410] Letztere, die so genannte „Neue Konzeption“, führt zur Verbindlichkeit außerrechtlicher Techniknormen. Insgesamt habe sich das Verhältnis von Recht und Standards gewandelt und kompliziert. So Dumortier/van Eecke, CLSR 1999, S. 107, m.w.N., die insbesondere auf das Deutsche Signaturgesetz verweisen (siehe dazu unten 2.3.1 und 2.3.3.6); Neuser, MMR 1999, S. 73.

2. Vergleich der Gesetzgebung

2.1 Überblick über die verschiedenen Regelungsansätze

In Anbetracht der sich ständig wandelnden und weiterentwickelnden digitalen Geschäftsanbahnungs- und Geschäftsabwicklungsumgebung sei, so *Müglich*, eine vernünftige und dauerhaft beständige Regelung schwierig:

> *„Nur allzu leicht entsteht die Gefahr, dass man in diesem Sektor dem Hase-und-Igel-Syndrom erliegt. Auf der anderen Seite ist der rechtliche Entwicklungs- und Klarstellungsbedarf evident.“*[411]

Diese Einschätzung aus dem Jahr 2000 war für den Zeitpunkt der Einführung neuer gesetzlicher Regelungen richtig – und sie ist es auch heute noch. Andererseits mag fraglich erscheinen, warum Internet-spezifische Regelungen überhaupt notwendig sein sollen. Der Nutzen einer solchen Regelung liegt in der Schaffung von Rechtssicherheit, besonders hinsichtlich solcher Aspekte, die andere rechtliche Lösungen als der Offline-Handel erfordern.[412] Die Alternative wäre ein Abwarten auf die Entwicklungen in der Rechtsprechung, und tatsächlich war auch eine solche *wait and see*-Einstellung bei einigen Gesetzgebern festzustellen.[413] Die nachfolgend dargestellten Gesetzesinitiativen greifen viele der oben unter 1.4.2 aufgeführten Aspekte und Anknüpfungspunkte einer gesetzlichen Regelung auf. Besonders umfassende Regelungswerke sind diesbezüglich die Richtlinien der EU sowie das deutsche Signaturgesetz (SigG) alter und neuer Fassung. Die Neuregelungen in England und den USA sind beschränkter und nach dem Willen der Gesetzgeber technikneutraler. Dabei wird deutlich, dass – wie es *Geis* formulierte – im internationalen E-Commerce *„zwei Konzepte zur Wahl stehen“*: das Konzept des EU-Binnenmarkts mit der Signatur-Richtlinie und das US-amerikanische Konzept mit den Bundesgesetzen zur elektronischen Signatur[414], beides Vertreter unterschiedlicher Rechtskulturen. Hilfreich ist eine kurze Darstellung der Ansätze der verschiedenen internationalen Regelungsinitiativen. Inhalt dieser Regelungen sind beispielsweise Aufsichts- und Kontrollregelungen hinsichtlich der Sicherheitsinfrastruktur der Signier- und Verschlüsselungstechnologien, nationale und internationale Standards für elektronische Authentifizierungsprodukte und -dienste, aber auch *best practices* und ähnliches. Gesetzgeber und Regulierungsbehörden haben zahlreiche und verschiedene Ansätze gewählt.[415] Diese werden häufig in drei voneinander zu unterscheidende Ansätze unterteilt:

---

[411] Müglich, MMR 2000, S. 12, 13.

[412] Hörnle, JILT 2000.

[413] Siehe die Zusammenfassung internationaler Regelungsinitiativen bei Baker et al., ILPF 2000.

[414] Geis, MMR 2000, S. 669.

[415] Baker et al., ILPF 2000, begründeten diese Unterschiede damit, dass sich die Technik der elektronischen/digitalen Signatur erst noch voll entwickeln müsse.

Der minimalistische, auch technologieneutral genannte Ansatz[416] beschränkt sich auf die Erleichterung der Nutzung von elektronischen Signaturen und die Beseitigung bestehender rechtliche Hindernisse für die Verwendung elektronischer oder digitaler Signaturen, ohne Befürwortung einer bestimmten Technologie. Teilweise wird festgestellt, dass (alle) elektronische(n) oder digitale(n) Signaturen die bestehenden rechtlichen Erfordernisse der Signatur erfüllen können. So werden beispielsweise fakultative Gesetze erlassen, um elektronische Aufzeichnungen in ihrer Rechtswirkung schriftlichen Aufzeichnungen und elektronisch authentifizierte Aufzeichnungen den eigenhändig unterzeichneten Aufzeichnungen gleichzustellen.[417] Diese Gleichstellung steht dabei im Vordergrund, auch wenn zumeist noch weitere Aspekte geregelt werden.[418] Teilweise werden lediglich bestehende Regelungen so erweitert, dass sie auch elektronische Transaktionen umfassen und auf eine Beschreibung der Voraussetzungen an eine elektronische Signatur wird vollständig verzichtet. Was eine rechtsgültige elektronische Signatur ausmacht, wird nicht bestimmt.[419] Zum Teil definieren die Gesetze Umstände, unter denen diese Anforderungen erfüllt werden. Teilweise wird auch ein Beweisstandard eingeführt.[420]

Unter dem beschreibenden, auch technologiespezifisch genannten Ansatz[421] wurden Gesetze verabschiedet, die bestimmte Authentifizierungstechnologien und Infrastrukturen regeln. Er verlangt für die Rechtsgültigkeit elektronischer Signaturen, dass diese bestimmte Eigenschaften besitzen oder bestimmte Anforderungen erfüllen, macht also die Gleichstellung mit der handschriftlichen Unterschrift von bestimmten technischen und sonstigen Voraussetzungen abhängig.[422] In einer Ausprägung wird nicht so sehr auf die Eigenschaften der Signatur abgestellt, als vielmehr auf die verwendete Technologie, und es wird ein rechtlicher Rahmen für die Tätigkeit der TTP (innerhalb der PKI) erstellt. Oft auf Grundlage der asymmetrischen Kryptographie als genehmigte Möglichkeit der elektronischen Signatur werden technisch-organisatorische Anforderungen gestellt, die Rechte des Schlüsselinhabers festgeschrieben und definiert, wann Vertrauen in eine elektronische Signatur gerechtfertigt ist. Er ermöglicht dem Gesetzgeber und den Regulierungsbehörden, direkt Standards für die Technik zu setzen und die Richtung der neuen Technik zu beeinflussen.[423] *Borges* unterscheidet daher in Gesetze zur elektronischen Signatur und Gesetze zum elektronischen Geschäftsverkehr. Bei ersteren liege der Schwerpunkt auf der Regelung der Komponenten des Signaturverfahrens. Bei letzteren

[416] Siehe bei Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 72.

[417] Sookman, CTLR 2001, S. 85; Baker et al., ILPF 2000; Smedinghoff/Hill Bro, JMJCIL 1999, S. 14 ff.

[418] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 70.

[419] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 72; Sookman, CTLR 2001, S. 85; und Smedinghoff/Hill Bro, JMJCIL 1999, S. 18, die auf die US-Staaten Connecticut, Minnesota, Wyoming u.a. verweisen.

[420] Baker et al., ILPF 2000.

[421] Siehe bei Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 71, 72.

[422] Baker et al., ILPF 2000; Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 71; Smedinghoff/Hill Bro, JMJCIL 1999, S. 15-18; Sookman, CTLR 2001, S. 85.

[423] Sookman, CTLR 2001, S. 85; Baker et al., ILPF 2000; Smedinghoff/Hill Bro, JMJCIL 1999, S. 18.

liege der Schwerpunkt auf der Anpassung der rechtlichen Bestimmungen an die Bedürfnisse des E-Commerce.[424]

Der dritte, vermittelnde Ansatz stellt eine Konvergenz und Synthese der vorherigen Ansätze dar. Hierbei werden Gesetze erlassen, die Standards festsetzen für die Tätigkeit von TTP und denen eine weite Auslegung der rechtsgültigen elektronischen Signatur für rechtliche Zwecke zugrunde liegt. Sie erreichen eine technologische Neutralität dadurch, dass sie wenigstens eine minimale rechtliche Anerkennung der meisten Authentifizierungstechniken beinhalten, sowie durch die Schaffung eines besser definierten und vorhersehbaren rechtlichen Rahmens durch die Einbeziehung von Regelungen für eine Authentifizierungstechnik der Wahl.[425] Hier wird bei der Gleichstellung von handschriftlicher Unterschrift und elektronischen Äquivalenten nach Merkmalen des Signaturverfahrens differenziert. Die volle Gleichstellung bleibt nur solchen Signaturverfahren vorbehalten, die bestimmte Voraussetzungen erfüllen und deshalb eine hohe Sicherheit garantieren.[426]

Zu erwähnen ist, dass fast alle hier dargestellten Gesetze, Richtlinien und Rechtsverordnungen in einem Zeitraum ab dem Jahr 2000 verabschiedet wurden. Davor gab es in den hier verglichenen Rechtsordnungen nur in Deutschland mit dem Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste und dem Signaturgesetz vom Juli 1997 sowie, angefangen mit dem Signaturgesetz des Staates Utah im Jahr 1995, in einzelnen Staaten der USA gesetzliche Regelungen zur elektronischen beziehungsweise digitalen Signatur. Zwar regelte die Fernabsatzrichtline der EU vom Februar 1997 bereits einige auch den E-Commerce betreffenden Aspekte, nicht jedoch den Einsatz elektronischer Signaturen. Erst im Dezember 1999 und im Juni 2000 sorgte auch die EU mit der Signaturrichtlinie und der E-Commerce-Richtlinie für eine EU-weit harmonisierende Regelung dieses Rechtsgebiets. Im Mai 2000 wurde zunächst in England der EC Act erlassen, im Mai und Juli 2001 wurden in Deutschland mit dem EGG, dem Signaturgesetz n.F. und dem Formanpassungsgesetz die Vorgaben der EU-Richtlinien umgesetzt. Erst nach Ablauf der von der Kommission gesetzten Frist zur Umsetzung wurden danach in England im Februar und Juli 2002 die Electronic Signatures Regulations 2002 und die Electronic Commerce (EC Directive) Regulations verabschiedet. Zwischen dem Erlass von Signatur- und E-Commerce-Richtlinie hat im Jahr 2000 auch der US-amerikanische Bundesgesetzgeber mit dem Uniform Electronic Transactions Act im April, dem Electronic Signature in Global and National Commerce Act im Juni und dem Uniform Computer Information Transactions Act im September gesetzliche Bestimmungen geschaffen, die den E-Commerce und den Einsatz elektronischer Signaturen regeln.

[424] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 70, 71.

[425] Baker et al., ILPF 2000.

[426] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 73

2.2 Richtlinien der Europäischen Union zu E-Commerce und elektronischen Signaturen

Internet und elektronischer Geschäftsverkehr sind grenzüberschreitend. Sofern es nicht ausdrücklich auf der jeweiligen Website oder E-Mail kenntlich gemacht wird, lässt sich der E-Commerce nicht auf ein Staats- und Rechtsgebiet und einen Markt beschränken. Vielmehr schafft er einen gemeinsamen Markt und kann damit das Prinzip und Ziel des europäischen Binnenmarkts fördern und diesen stärken.[427] Es ist daher folgerichtig, dass die Europäische Union angesichts der vielen verschiedenen Rechtsordnungen in Europa diesen Bereich einer harmonisierenden Regelung zuführte. Der wirksame Abschluss von Verträgen über das Internet sollte unter anderem nicht an Formvorschriften des nationalen Rechts scheitern.[428] Hier sind die Richtlinie über den elektronischen Geschäftsverkehr (E-Commerce-Richtlinie)[429] und die Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (Signatur-Richtlinie) als Harmonisierungsinstrument zu nennen[430] Sie sollten von den Mitgliedstaaten der Europäischen Gemeinschaft[431] in nationales Recht umgesetzt werden.

2.2.1 E-Commerce-Richtlinie

Die Richtlinie über den elektronischen Geschäftsverkehr[432], hier E-Commerce Richtlinie (oder kurz RLeC[433]) genannt, stellt den ersten Baustein für eine gemeinschaftsweite Regelung des elektronischen Geschäftsverkehrs dar. Sie bietet Definitionen und stellt wichtige Prinzipien auf.

---

[427] Siehe York/Tunkel, S. 459.

[428] Hoeren, *Grundzüge des Internetrechts*, S. 194.

[429] 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 Geschäftsverkehr), L178/1.

[430] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingung für elektronische Signaturen, L 13/12; Jansen, ICCLR 1999, S. 39.

[431] Der Begriff des Mitgliedstaates bezeichnet solche Staaten, die Mitglied der Europäischen Union (EU) sind.

[432] 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 Geschäftsverkehr“).

[433] Diese Abkürzung wird von vielen Autoren verwendet und wird hier übernommen.

2.2.1.1 Zielsetzung und Anwendungsbereich

Die RLeC wurde initiiert von der Europäischen Kommission[434], da die Diensteanbieter international und auch innerhalb der Europäischen Union differierenden rechtlichen Grundlagen gegenüber standen. Ihnen sollte eine sichere rechtliche Grundlage für ihre Tätigkeiten bereitet, die geschäftliche Nutzung der Online-Dienste erschwerende Unsicherheiten beseitigt und grenzüberschreitende elektronische Transaktionen gefördert werden.[435] Unter anderem sollten die Diensteanbieter aufgrund der geschaffenen rechtlichen Grundlage ein möglichst breites Angebot in einem kompetitiven Umfeld schaffen, was letztlich den Verbrauchern zu gute kommen soll.[436] Die RLeC stellt fest, dass der E-Commerce sich nicht voll entwickeln kann, solange der Abschluss von Online-Verträgen behindert wird durch bestimmte formelle oder andere rechtliche Erfordernisse, die nicht den Bedürfnissen des Online-Businesses angepasst sind. Deshalb sollte sichergestellt werden, dass der elektronische Vertragsschluss gemeinschaftsweit möglich ist.[437]
Die RLeC hat zunächst den freien Verkehr von Diensten der Informationsgesellschaft in der Europäischen Union zum Gegenstand.[438] Gemäß Art. 1 Abs. 2 sorgt die RLeC

> *„für eine Angleichung bestimmter für die Dienste der Informationsgesellschaft geltender innerstaatlicher Regelungen, die* [neben anderem] *elektronische Verträge,... betreffen."*

In Art. 2 lit. a) wird neben anderen der Begriff der Dienste der Informationsgesellschaft (DIG)[439] definiert: dies ist *„jede in der Regel gegen Entgelt elektronisch im Fernabsatz*

---

[434] Siehe hierzu: Mitteilung der Europäischen Kommission „Eine europäische Initiative im elektronischen Geschäftsverkehr", KOM [97] 157 vom 16.4.1997; Vorschlag der Kommission zur Richtlinie, KOM [1998] 586 endg., vom 18.11.1998; Entschließung des Parlaments vom 15.4. 1998 (A4-0173/98); Moritz, CR 2000, S. 68.

[435] Erwägungsgrund 1 RLeC: *„... Die Weiterentwicklung der Dienste der Informationsgesellschaft in dem Raum der ohne Binnengrenzen ist ein wichtiges Mittel, um die Schranken die die europäischen Völker trennen, zu beseitigen."*; Erwägungsgrund 3: *„... Diese Richtlinie zielt daher darauf ab, ein hohes Niveau der rechtlichen Integration in der Gemeinschaft sicherzustellen, ..."*; Erwägungsgrund 5: *„... Die Hemmnisse bestehen in Unterschieden der innerstaatlichen Rechtsvorschriften sowie in der Rechtsunsicherheit hinsichtlich der auf Dienste der Informationsgesellschaft jeweils anzuwendenden nationalen Regelungen."*; Erwägungsgrund 6: *„... gilt es, die genannten Hemmnisse durch Koordinierung bestimmter innerstaatlicher Rechtsvorschriften und durch Klarstellung von Rechtsbegriffen auf Gemeinschaftsebene zu beseitigen,..."*; siehe auch Erwägungsgrund 2 und 10. Siehe hierzu: Pullen/Logan, „The European Union Proposed Legal Framework for E-Commerce" *ICCLR* Spe (1999) S. 21, 22; York/Tunkel, S. 81; Maennel, „Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission"; MMR 1999, S. 187-192, S. 187.

[436] Erwägungsgrund 7 RLeC: *„Um Rechtssicherheit zu erreichen und das Vertrauen der Verbraucher zu gewinnen, muss die Richtlinie einen klaren allgemeinen Rahmen für den Binnenmarkt bezüglich bestimmter rechtlicher Aspekte des elektronischen Geschäftsverkehrs festlegen."*; auch Erwägungsgrund 41 und 65. Siehe Maennel, MMR 1999, S. 187, 188.

[437] Siehe Erwägungsgründe 5, 6, 34 bis 39 RLeC; Maennel, MMR 1999, S. 188, 190; Pullen/Logan, „The European Union Proposed Legal Framework for E-Commerce", ICCLR Spe 1999, S. 21-28, S. 21, 22; York/Tunkel, S. 81. Ferner soll der Verbraucher die notwendigen Informationen zur Art und Weise des Vertragsschlusses und über diejenigen Umstände, die Rechtswirkungen haben können, erhalten.

[438] Art. 1 Abs. 1 RLeC.

und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung". Gemeint sind Dienstleistungen, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht werden.[440] Dies umfasst einen Teil der oben unter 1.1 dargestellten online getätigten Geschäfte, Transaktionen und Verträge mittels Websites, aber auch bestimmte Zertifizierungsdienste. Ferner definiert die RLeC für ihren Anwendungsbereich die Begriffe Diensteanbieter, Nutzer und Verbraucher.[441]

2.2.1.2 Diensteanbieter

Die RLeC regelt wesentliche, den E-Commerce betreffende Aspekte grundsätzlich. Regelungen zum elektronischen Vertrag sind nur ein Teil des Gesamten. Zunächst ist die Binnenmarktregel des Art. 3 RLeC zu nennen. Sie schreibt das Herkunftslandprinzip fest, wonach Diensteanbieter gemeinschaftsweit tätig werden können und in ihrer Tätigkeit nicht eingeschränkt werden dürfen, wenn sie den Regeln ihres Herkunftslandes entsprechen, auch wenn das Empfängerland oder der Ort des Abrufens der Dienstleistung andere Regeln vorsehen sollte, Art. 3 Abs. 1 und 2 i.V.m. Art. 2 lit. h).[442] Das Einschränkungsverbot der Binnenmarktregel bezieht sich dabei auf Gründe, die in den koordinierten Bereich Fallen. Dieser umfasst

> *„die für die Anbieter von* [DIG] *in den Rechtssystemen der Mitgliedstaaten festgelegten Anforderungen,... einschließlich der auf... Verträge anwendbaren Anforderungen..."*[443]

Dies betrifft auch die Regelung der Tätigkeit von Zertifizierungsstellen. Das Herkunftslandprinzip erwächst aus einem grundlegenden europarechtlichen Prinzip. Grund dafür ist unter anderem, dass im Internet tätige Unternehmen nicht wissen können, wer von wo ihren Dienst abrufen wird und nicht in der Lage oder bereit sind, 15 verschiedene Rechtsordnungen zu kennen und zu beachten. Dennoch ist die getroffene Regelung

---

[439] Abgekürzt DIG; In der englischen Entsprechung *information society services* (ISS abgekürzt).

[440] Dabei wird die Dienstleistung mittels Geräten für die elektronische Verarbeitung und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen und sie wird vollständig über Draht oder Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen. Der Begriff Dienst entspricht der Dienstleistung i.S.d. Art. 60 des Vertrages zur Gründung der Europäischen Gemeinschaft vom 25.3. 1957 (EGV) und ist weit auszulegen. Die Abgrenzung zum Rundfunk erfolgt durch das Merkmal „auf Abruf". „Im Fernabsatz" beschreibt die räumliche Trennung der Parteien, die dank der technischen Hilfsmittel wie unter Anwesenden handeln können. Siehe dazu: Maennel, MMR 1999, S. 188.

[441] Gemäß Art. 2 lit. b) ist Diensteanbieter *„jede natürliche oder juristische Person, die einen Dienst der Informationsgesellschaft anbietet"*, gemäß lit. d) Nutzer *„jede natürliche oder juristische Person, die zu beruflichen oder sonstigen Zwecken einen* [DIS] *in Anspruch nimmt, ..."* und gemäß lit. e) Verbraucher *„jede natürliche Person, die zu Zwecken handelt, die nicht zu ihren gewerblichen, geschäftlichen oder beruflichen Tätigkeiten gehören."*

[442] Siehe auch Pullen/Logan, ICCLR 1999, S. 22.

[443] Art. 2 lit. h) RLeC.

nicht unumstritten.[444] Im Anhang der RLeC sind diejenigen Rechte aufgelistet, die ausdrücklich von der Anwendung des Art. 3 Abs. 1 und 2 RLeC und damit dem Einschränkungsverbot ausgenommen sind. Dies ist unter anderem die

> *„formale Gültigkeit von Verträgen, die Rechte an Immobilien begründen oder übertragen, sofern diese Verträge nach dem Recht des Mitgliedstaates, in dem sich die Immobilie befindet, zwingenden Formvorschriften unterliegen".*[445]

In Art. 4 Abs. 1 stellt die RLeC fest, dass der Zugang zur Tätigkeit für einen Anbieter von DIG nicht zulassungspflichtig sein soll.[446] Art. 5 Abs. 1 RLeC bestimmt verschiedene Informationspflichten der Diensteanbieter. Art. 2 lit. f) RLeC definiert kommerzielle Kommunikationen.[447] Ausgenommen vom Anwendungsbereich sind beispielsweise bestimmte Tätigkeiten wie die Notartätigkeit oder das Auftreten vor Gericht.[448] Der Anwendungsbereich der RLeC erfasst keine DIG, die von einem in einem Drittland niedergelassenen Diensteanbieter bereitgestellt werden. Dennoch erkennt die RLeC die Notwendigkeit der internationalen Harmonisierung, für die ein einheitlicher Rechtsrahmen für die Europäische Union ein erster wichtiger Schritt sei.[449]

---

[444] So beinhaltet sie die Verpflichtung der Mitgliedstaaten für die Einhaltung der Rechtsvorschriften des Staates ihrer Niederlassung zu sorgen, Art. 2 lit. c) i.V.m. Art. 3 Abs. 1 RLeC. Für die Niederlassung kommt es auf den Schwerpunkt der tatsächlichen Aktivität an, siehe Urteil des Europäischen Gerichtshofs vom 25.07.1991, Rs. C-221/89 und Erwägungsgrund 19 RLeC: *„... Erbringt ein Unternehmen Dienstleistungen über eine Web-Site des Internets, so ist es weder dort niedergelassen, wo sich die technischen Mittel befinden, die diese Web-Site beherbergen, noch dort, wo die Web-Site zugänglich ist, sondern an dem Ort, an dem es seine Wirtschaftstätigkeit ausübt... Ist im Falle mehrerer Niederlassungsorte schwierig zu bestimmen, von welchem Ort aus ein bestimmter Dienst erbracht wird, so gilt als solcher der Ort, an dem sich der Mittelpunkt der Tätigkeiten des Anbieters in Bezug auf diesen bestimmten Dienst befindet."* Unter Umständen sind die Dienstanbieter dennoch gezwungen, sich auch nach dem Recht des Abrufortes zu richten. Ausführlich und kritisch hierzu Pullen/Logan, ICCLR 1999, S. 21, 25-28 (mit vielen weiteren Nachweisen) und Moritz, CR 2000, S. 70f.; des weiteren Hörnle, JILT 2000 (u.a. mit Entscheidungsnachweisen); Lloyd, S. 567, 568; Maennel, MMR 1999, S. 188, 189; Murray in Edwards/Walden, S. 32 f.; Nazerali/Cowan, „E-Commerce and Cross-Border Shopping – Can the EU Untangle the Web?", BLR 2000, S. 117-118, S. 117; York/Tunkel, S. 456.

[445] Letzteres entspricht der in Art. 9 Abs. 2 lit. a) RLeC aufgeführten Ausnahme (dazu 2.2.3). Daneben ergeben sich weitere Ausnahmen dadurch, dass es den Mitgliedstaaten gemäß Art. 3 Abs. 4 RLeC unter bestimmten Voraussetzungen gestattet ist, entgegen dem Einschränkungsverbot Maßnahmen gegen einzelne DIG zu ergreifen. Kritisch hierzu Rennie, CTLR 1999, S. 240.

[446] Art. 4 Abs. 1 RLeC: *„Die Mitgliedstaaten stellen sicher, dass die Aufnahme und die Ausübung der Tätigkeit eines Anbieters von [DIS] nicht zulassungspflichtig ist und keiner sonstigen Anforderung gleicher Wirkung unterliegt."*; Die Mitgliedstaaten können demnach keine Lizenzpflicht mehr für solche Dienste vorschreiben. Unberührt bleiben dagegen allgemeine Zulassungsverfahren, also solche, die nicht speziell und ausschließlich DIG betreffen. Siehe Maennel, MMR 1999, S. 189.

[447] Kommerzielle Kommunikationen sind danach *„alle Formen der Kommunikation, die der unmittelbaren oder mittelbaren Förderung des Absatzes von Waren und Dienstleistungen oder des Erscheinungsbilds eines Unternehmens, einer Organisation oder einer natürlichen Person dienen, die eine Tätigkeit in Handel, Gewerbe oder Handwerk oder einen reglementierten Beruf ausübt; ..."* Siehe auch Art. 6 lit. a) und b) RLeC; ausführlich Rennie, CTLR 1999, S. 240f.

[448] Zu weiteren Ausnahmen zu Art. 3 RLeC: Maennel, MMR 1999, S. 192 und den Anhang der RLeC.

[449] In den Erwägungsgründen 58 bis 61 RLeC heißt es dazu: *„... Angesichts der globalen Dimension des elektronischen Geschäftsverkehrs ist... dafür Sorge zu tragen, dass die gemeinschaftlichen Vorschriften mit den internationalen Regeln in Einklang stehen. Die Ergebnisse der Erörterungen über rechtliche Fragen in internationalen Organisationen (unter anderem WTO, OECD, UNCITRAL) bleiben von die-*

2.2.1.3 Elektronischer Vertrag – Ermöglichungsgrundsatz, Art. 9 RLeC

Um den insbesondere im grenzüberschreitenden elektronischen Geschäftsverkehr auftauchenden Problemen des Vertragsschlusses über das Internet entgegenzuwirken, will die RLeC auch im Bereich der für den Vertragsschluss geltenden Rechtsvorschriften eine gewisse Harmonisierung erreichen. Kernvorschrift des dritten, sich mit dem Abschluss von Verträgen auf elektronischen Weg beschäftigenden Abschnitts der RLeC ist Art. 9 Abs. 1. Hier verpflichtet die RLeC die Mitgliedstaaten wie folgt:

> *„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 zustande gekommen sind, keine rechtliche Wirksamkeit oder Gültigkeit haben."*

Danach muss ein auf elektronischem Weg geschlossener Vertrag grundsätzlich die gleiche Gültigkeit und Rechtskraft haben wie ein Vertrag, der auf konventionellem Weg geschlossen wurde. Vorschriften, die für die Gültigkeit bestimmter Verträge die Schriftform beziehungsweise schriftliche Form oder die (handschriftliche) Signatur voraussetzen, müssen so geändert werden, dass auch ein elektronischer Weg des Abschlusses möglich ist.[450] Damit wird der in Art. 9 Abs. 1 aufgestellte Ermöglichungsgrundsatz zum Kern und Ausgangspunkt für die Anpassung der Formvorschriften an den elektronischen Geschäftsverkehr.[451] Erwägungsgrund 34 RLeC präzisiert diesen Auftrag an die Mitgliedstaaten:

> *„Jeder Mitgliedstaat hat seine Rechtsvorschriften zu ändern, in denen Bestimmungen festgelegt sind, die die Verwendung elektronischer Verträge behindern könnten; dies gilt insbesondere für Formerfordernisse. Die Prüfung anpassungsbedürftiger Rechtsvorschriften sollte systematisch erfolgen und sämtliche*

---

ser Richtlinie unberührt." „Trotz der globalen Natur elektronischer Kommunikationen ist eine Koordinierung… auf der Ebene der Europäischen Union notwendig,... Diese Koordinierung sollte auch zur Herausbildung einer gemeinsamen und starken Verhandlungsposition in internationalen Gremien beitragen." „Im Sinne der ungehinderten Entwicklung des elektronischen Geschäftsverkehrs muss dieser Rechtsrahmen klar, unkompliziert und vorhersehbar sowie vereinbar mit den auf internationaler Ebene geltenden Regeln sein, um… innovative Maßnahmen in diesem Sektor nicht zu behindern." „Damit der elektronische Markt in einem globalisierten Umfeld wirksam funktionieren kann, bedarf es einer Abstimmung zwischen der Europäischen Union und den großen nichteuropäischen Wirtschaftsräumen..."

[450] Erwägungsgrund 37 RLeC begrenzt diese Verpflichtung der Mitgliedstaaten: *„Die Verpflichtung der Mitgliedstaaten, Hindernisse für die Verwendung elektronisch geschlossener Verträge zu beseitigen, betrifft nur Hindernisse, die sich aus rechtlichen Anforderungen ergeben, nicht jedoch praktische Hindernisse, die dadurch entstehen, dass in bestimmten Fällen elektronische Mittel nicht genutzt werden können."* Auch Erwägungsgrund 38.

[451] Hierzu Maennel, MMR 1999, S. 190.

Phasen bis zum Vertragsabschluss umfassen,... Diese Änderung sollte bewirken, dass es möglich ist, elektronisch geschlossene Verträge zu verwenden...“

Für die Mitgliedstaaten bedeutete dies, dass sie Vorschriften zurücknehmen mussten, die die Nutzung elektronischer Medien zum Vertragsschluss *ausdrücklich* untersagen oder beschränken, dass sie kein zweistufiges System errichten oder aufrechterhalten durften, nach dem elektronischen Verträgen weniger Rechtswirkung zukommt als papiernen Verträgen, und dass sie insbesondere solche Formerfordernisse für Verträge aufheben mussten, die durch elektronische Hilfsmittel nicht erfüllt werden können oder die, wenn auf elektronische Verträge angewandt, Mehrdeutigkeiten hervorrufen. Vorschriften wie das Erfordernis der Schriftlichkeit, oder solche, die verlangen, dass ein Dokument eine bestimmte Form haben muss, um bei Gerichtsverfahren präsentiert (*presented*) werden zu können, oder dass ein Vertrag im Original oder als Ausdruck vorgelegt werden muss, mussten geändert werden. Ferner mussten beispielsweise Erfordernisse, nach denen ein Vertrag nur bei Anwesenheit beider Vertragsparteien oder nur zwischen natürlichen Personen abgeschlossen werden kann, ebenfalls geändert werden.[452] Die Richtlinie verlangt dabei nicht nur eine Gleichstellung hinsichtlich des rechtlichen Status und die Aufhebung spezifischer Verbote des elektronischen Vertragsabschlusses. Vielmehr darf, im Zusammenspiel aller einschlägigen Regelungen, im Ergebnis keine allein auf den elektronischen Vertrag beschränkte Behinderung mehr gegeben sein.[453] Dennoch erlaubt die RLeC den Mitgliedstaaten gemäß Erwägungsgrund 35 RLeC

„... allgemeine oder spezifische rechtliche Anforderungen für Verträge, die auf elektronischem Wege erfüllt werden können, insbesondere Anforderungen für sichere elektronische Signaturen, aufrecht zu erhalten oder festzulegen.“[454]

Das Ziel, elektronische Verträge den papiernen und handsignierten Verträgen gleichzustellen, kann nur über die elektronische beziehungsweise digitalen Signatur erreicht werden. Die RLeC steht daher in engem Zusammenhang mit der nachfolgend dargestellten sogenannten Signaturrichtlinie (hier kurz RLeS genannt[455]), die die rechtliche Grundlage und Funktionieren dieses Hilfsmittels regelt. Auch wenn die Harmonisierung von Formvorschriften für privatrechtliche elektronische Verträge Aufgabe des Art. 9 der RLeC ist, behandelt die RLeC nicht die Vorschriften bezüglich der Wirksamkeit elekt-

[452] Siehe hierzu Pullen/Logan, ICCLR 1999, S. 23; auch Hoeren, *Grundzüge des Internetrechts*, S. 195 und Hörnle, JILT 2000.

[453] Maennel, MMR 1999, S. 191, nennt den Fall, dass eine den elektronischen Geschäftsverkehr hindernde Regelung nur „pro forma“ geändert werde, andere Vorschriften aber nach wie vor die alltägliche Nutzung behindern.

[454] Siehe dazu Kye, „E-Commerce in the EU: Bringing Businesses and Consumers Aboard“, CLSR 2001, S. 25-27, S. 27.

[455] Diese Abkürzung wird von vielen Autoren verwendet und hier übernommen. Zur Signaturrichtlinie siehe nachfolgend unter 2.2.2.

ronischer Signaturen. Diese sind in der RLeS geregelt, die festlegt welche Arten von elektronischen Signaturen als Form der Erfüllung von Formvorschriften genügen.[456]
Die RLeC enthält jedoch auch einige Abweichungen vom Ermöglichungsgrundsatz des Art. 9 Abs. 1 RLeC. Abs. 2 listet bestimmte Verträge auf, die von den Mitgliedstaaten von der Regelung des Abs. 1 ausgenommen werden können. Dies sind:

> *„a) Verträge, die Rechte an Immobilien mit Ausnahme von Mietrechten begründen oder übertragen;*
>
> *b) Verträge, bei denen die Mitwirkung von Gerichten, Behörden oder öffentliche Befugnisse ausübenden Berufen gesetzlich vorgeschrieben ist;*
>
> *c) Bürgschaftsverträge und Verträge über Sicherheiten, die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit eingegangen werden;*
>
> *d) Verträge im Bereich des Familienrechts oder Erbrechts....“*[457]

2.2.1.4 Umsetzung

Die RLeC sollte von den Mitgliedstaaten bis zum 16. Januar 2002 in nationales Recht umgewandelt werden.[458] Die Mitgliedstaaten sind verantwortlich für die Regulierung der Aktivitäten im E-Commerce und müssen beispielsweise sicherstellen, dass die Aktivitäten der innerhalb ihrer Grenzen etablierten ISP den Regelungen der Richtlinie in Form ihrer Umsetzung in nationales Recht entsprechen.[459]

2.2.2 Signaturrichtlinie

Der zweite bedeutende Baustein für eine europaweite Regelung des elektronischen Geschäftsverkehrs ist die Schaffung eines einheitlichen Rechtsrahmens für die Erstellung, Nutzung und die Sicherheitsinfrastruktur elektronischer Signaturen. Bereits vor der Verabschiedung der RLeC hatten das Europäische Parlament und der Rat die Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen[460] (Signaturrichtlinie, RLeS) verabschiedet.

---

[456] Erwägungsgrund 34 RLeC. Hierzu Pullen/Logan, ICCLR 1999, S. 23; Roßnagel, K&R 2000, S. 321. Beide Richtlinien ergänzen sich gegenseitig und sind aufeinander angewiesen. Maennel, MMR 1999, S. 190.

[457] Art. 9 Abs. 2 lit. a) bis d) RLeC. Siehe dazu auch Erwägungsgrund 35 (oben zitiert). Für diese Fälle müssen die Mitgliedstaaten der Kommission vollständige Listen der ausgeschlossenen Vertragstypen einreichen; Siehe hierzu York/Tunkel, S. 81. Dazu Hoeren, *Grundzüge des Internetrechts*, S. 195: Diese Vorschrift erstaune insofern, als dass sich in der RLeC der Geist des Binnenmarktes widerspiegele, nun aber Gedanken zu einer Reform des Zivilrechts auftauchten (z.B. Familien und Erbrecht).

[458] Art. 19; Maennel, MMR 1999, S. 192.

[459] Art. 2 RLeC; Pullen/Logan, ICCLR 1999, S. 22.

[460] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingung für elektronische Signaturen, Abl. EG Nr. L 13/12.

2.2.2.1 Zielsetzung und Anwendungsbereich

In Erwägungsgrund 4 stellt die RLeS fest, dass *„elektronische Kommunikation und elektronischer Geschäftsverkehr... ‚elektronische Signaturen' und entsprechende Authentifizierungsdienste für Daten"* erfordere. Zielsetzung der RLeS ist es daher, die Verwendung elektronischer Signaturen zu erleichtern und zu ihrer rechtlichen Anerkennung beizutragen.[461] Hierzu stellt sie fest, dass divergierende Regeln über die rechtliche Anerkennung elektronischer Signaturen und die Akkreditierung von Zertifizierungsanbietern in den Mitgliedstaaten *„ein ernsthaftes Hindernis... darstellen"* können.[462] Folglich sollen die grenzüberschreitende rechtliche Anerkennung elektronischer Signaturen sichergestellt, harmonisierte und *„klare gemeinschaftliche Rahmenbedingungen für elektronische Signaturen"* und für bestimmte Zertifizierungsdienste geschaffen und die Interoperabilität von Produkten für elektronische Signaturen gefördert werden.[463] Über die RLeS soll gemeinschaftsweit sichergestellt werden, dass Zertifizierungsstellen bestimmte Anforderungen erfüllen und kontrolliert werden und dass die elektronische beziehungsweise digitale Signatur bestimmten Sicherheitsstandards genügt. Hierfür setzt die Richtlinie einen europaweiten Standard fest. Kern ihrer Regelungen ist die Gleichstellung mit der Unterschrift. Der Anwendungsbereich der RLeS bleibt hierauf beschränkt und erstreckt sich ausdrücklich nicht auf

> *„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"* oder auf *„im einzelstaatlichen Recht oder im Gemeinschaftsrecht vorgesehene Regeln und Beschränkungen für die Verwendung von Dokumenten"*.[464]

---

[461] Art. 1 Abs. 1 RLeS.

[462] Erwägungsgrund 4 RLeS, auch Erwägungsgrund 7 RLeS.

[463] Art. 1 Abs. 1 RLeS und Erwägungsgrund 4 RLeS: *„... Klare gemeinschaftliche Rahmenbedingungen... stärken demgegenüber das Vertrauen und die allgemeine Akzeptanz hinsichtlich der neuen Technologien."* Ferner Erwägungsgrund 5: *„... Es sind grundlegende Anforderungen zu erfüllen, die speziell für Produkte für elektronische Signaturen gelten, um so den freien Verkehr im Binnenmarkt zu gewährleisten und das Vertrauen in digitale Signaturen zu fördern. ..."*; Hoeren, *Grundzüge des Internetrechts*, S. 194.

[464] Art. 1 Abs. 2 RLeS. Im Gegensatz zur RLeC gelten Regelungen der RLeS, die die Rechtswirkung elektronischer Signaturen betreffen, nicht nur für das Privatrecht, sondern für alle Rechtsbereiche, auch für den öffentlichen Bereich, Art. 5 RLeS. Da der EU die Regelungskompetenz für das Angleichen des nationalen Verwaltungsrechts fehlt, ist der Einsatz elektronischer Signaturen im öffentlichen Bereich aus dem Anwendungsbereich ausgenommen. Für diesen Bereich können die Mitgliedstaaten weitergehende Anforderungen stellen, Roßnagel, K&R 2000, S. 321/322. Ausgenommen vom Anwendungsbereich der RLeS sind auch Signaturverfahren in so genannten geschlossenen Systemen. Den Vertragsparteien steht es insofern im Rahmen des nationalen Rechts frei, im Rahmen der Vertragsfreiheit die für sie günstigsten Lösungen zu vereinbaren (Erwägungsgrund 16). Eine Haftung der Zertifizierungsstellen dürfte in einem geschlossenen System nicht greifen. Siehe Blum, K&R 2000, S. 69; Müglich, „Neue Formvorschriften für den E-Commerce: Zur Umsetzung der EU-Signaturrichtlinie in deutsches Recht", MMR 2000, S. 7-13, S. 8; Rossnagel, MMR 1999, 261, 263.

Aufgrund ihrer Entstehungsgeschichte ist die RLeS durch differierende Regelungsansätze und divergierende Regelungsziele geprägt. Die Kommission verfolgte ursprünglich ein marktorientiertes Regelungskonzept, stieß damit aber bei der Mehrheit der Mitgliedstaaten auf Widerstand.[465] Sie verbindet in ihrer Sicherheitsinfrastruktur für elektronische Signaturen nun eine Mischung aus Marktfreiheit[466] mit Marktkorrektiven[467], technisch-organisatorischen Anforderungen an Zertifizierungsdienste und technische Komponenten[468] und der Etablierung von Überwachungssystemen[469]. Sie ist damit dem dritten Ansatz zuzuschreiben, da sie minimalistische und beschreibende Merkmale enthält.[470] Ausdruck des für das Zustandekommen der RLeS notwendigen Kompromisses ist es, dass die Richtlinie den Mitgliedstaaten teilweise explizit einen eigenen Gestaltungsspielraum lässt.[471]

2.2.2.2 Fortgeschrittene elektronische Signatur, Signaturerstellung und Signaturüberprüfung

Art. 2 der RLeS definiert die Schlüsselbegriffe der der elektronischen Signatur zugrunde liegenden technologischen Basis und ihrer Sicherheitsinfrastruktur. Die RLeS versucht dabei, eine möglichst neutrale, das heißt nicht auf eine bestimmte Verschlüsselungs- oder Signierungstechnologie bezogene Sprachregelung beizubehalten. Dabei etabliert die RLeS ein System der abgestuften Sicherheit und Zuverlässigkeit der eingesetzten Signaturen und Infrastruktur. Je nachdem, ob bestimmte qualifizierende Anforderungen erfüllt werden, bestimmt sich die Rechtswirkung. Der Begriff digitale Signatur wird nicht verwendet. Stattdessen unterscheidet sie zwischen zwei verschiedenen Typen der elektronischen Signatur, unterschiedlichen Sicherheitsstandards und Rechtsfolgen.[472] Der erste Typ ist die (einfache) elektronische Signatur, die gemäß Art. 2 Nr. 1 definiert wird als:

> *„Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“.*

Diese grundlegende Begriffsbestimmung wird dabei von den eingangs dargestellten Merkmalen einer elektronischen Signatur im Sinne eines einfachen Substituts für die Signatur[473] erfüllt. So umfasst der Begriff beispielsweise Methoden wie die eingescann-

[465] Dazu Roßnagel, K&R 2000, S. 315.

[466] Art. 3 Abs. 1 (Marktzugang) und Art. 4 RLeS (Binnenmarktgrundsätze), siehe nachfolgend 2.2.2.9.

[467] Art. 6 RLeS (Haftung), siehe nachfolgend 2.2.2.5.

[468] Anhang I bis IV, siehe nachfolgend 2.2.2.3 und 2.2.2.4.

[469] Art. 3 Abs. 3 und 4 RLeS, siehe nachfolgend 2.2.2.5.

[470] Siehe oben 2.1; Baker et al., ILPF 2000.

[471] So in Art. 3 Abs. 2 und 7 RLeS, siehe Roßnagel, K&R 2000, S. 315.

[472] Dazu York/Tunkel, S. 90.

[473] Siehe oben 1.4.1.1.

te Unterschrift[474], aber auch geheime Codes wie PIN oder biometrische Verfahren in elektronischem Format[475], also auch Merkmale der digitalen Signatur. Der Begriff Authentifizierung selbst wird von der RLeS nicht definiert oder erklärt.[476] Die Definition der elektronischen Signatur versäumt es dabei, die Notwendigkeit der Authentifizierung der Daten, denen sie beigefügt oder mit denen sie verknüpft wird, herauszustellen.[477] Um zweifelsfrei die Herkunft und Integrität der elektronischen Daten feststellen zu können, müssen zudem weitere Anforderungen erfüllt sein. Diese Anforderungen stellt die RLeS in Art. 2 Nr. 2 in der Definition der fortgeschrittenen elektronischen Signatur fest. Die (einfache) elektronische Signatur wird zur fortgeschrittenen elektronischen Signatur, sofern sie folgendes erfüllt:

> *„a) Sie ist ausschließlich dem Unterzeichner zugeordnet;*
>
> *b) sie ermöglicht die Identifizierung des Unterzeichners;*
>
> *c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;*
>
> *d) sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann;“*[478]

Die einzige Form der elektronischen Signatur, die das letztgenannte Element erfüllen kann, ist die digitale Signatur.[479] Den zur Erstellung einer elektronischen Signatur durch den Nutzer beziehungsweise Unterzeichner[480] erforderlichen Komplex der Soft- und Hardware unterscheidet und bezeichnet die RLeS als Signaturerstellungsdaten[481], beispielsweise private kryptographische Schlüssel, und Signaturerstellungseinheiten[482]. Die technischen Komponenten werden jedoch nicht umfassend geregelt. An diese Komponenten werden weder Anforderungen gestellt noch an ihre Verwendung Rechtsfolgen geknüpft. Funktionale Sicherheitsanforderungen werden nur in Anhang III der RLeC für sichere Signaturerstellungseinheiten erhoben.[483] Signaturerstellungseinheiten

---

[474] Geis, MMR 2000, S. 669. Siehe dazu auch unten 3.3.2.

[475] Mason, *Electronic Signatures in Law*, S. 147.

[476] Dumortier/van Eecke, CLSR 1999, S. 110.

[477] Mason, *Electronic Signatures in Law*, S. 147.

[478] Art. 2 Nr. 2 lit. a) bis d) RLeS. Diese Anforderungen werden zum Beispiel durch frei verfügbare Implementierungen wie Pretty Good Privacy (PGP) erfüllt, die aus dem Netz herunter geladen werden können und bei denen die Signierschlüssel auf Diskette, Festplatte oder anderen lesbaren Datenträgern gespeichert werden können, Geis, MMR 2000, S. 669.

[479] Mason, Electronic Signatures in Law, S. 151, siehe auch oben 1.4.1.2 und 1.4.1.3.

[480] Art. 2 Nr. 3 RLeS: Unterzeichner ist *„eine Person, die eine Signaturerstellungseinheit besitzt und die entweder im eigenen Namen oder im Namen der von ihr vertretenen Stelle oder juristischen oder natürlichen Person handelt“*.

[481] Art. 2 Nr. 4 RLeS: Signaturerstellungsdaten sind *„einmalige Daten wie Codes oder private kryptographische Schlüssel, die vom Unterzeichner zur Erstellung einer elektronischen Signatur verwendet werden“*.

[482] Art. 2 Nr. 5 RLeS: Signaturerstellungseinheit ist *„eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturerstellungsdaten verwendet wird“*.

[483] Zutreffend Roßnagel, K&R 2000, S. 316, 317.

qualifizieren sich als sicher dadurch, dass sie die im Anhang III enthaltenen zusätzlichen Anforderungen erfüllen. So wird verlangt, dass sie durch geeignete Technik und Verfahren zumindest gewährleisten, dass:

> *„a) die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten praktisch nur einmal auftreten können und dass ihre Geheimhaltung hinreichend gewährleistet ist;*
>
> *b) die... Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die Signatur vor Fälschungen bei Verwendung der jeweils verfügbaren Technologie geschützt ist; ...“*[484]

Des Weiteren dürfen sie die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass diese Daten dem Unterzeichner vor dem Signaturvorgang dargestellt werden. Beachtlich ist, dass die RLeS für sichere Signaturerstellungseinheiten eine Vorabprüfung vorsieht. Ihre Konformität mit Anhang III soll nach Art. 3 Abs. 4 RLeS von geeigneten privaten oder öffentlichen Stellen festgestellt werden, die von den Mitgliedstaaten benannt werden.[485] Und in Satz 2: *„Die Kommission legt nach dem Verfahren des Artikels 9* [Ausschuss für elektronische Signaturen, siehe 2.2.2.10 zur Umsetzung der RLeS] *Kriterien fest, anhand deren die Mitgliedstaaten bestimmen, ob eine Stelle zur Benennung geeignet ist.“*[486] Die Kommission lässt sich hierdurch die Möglichkeit einräumen, wesentliche Elemente anstelle der Mitgliedstaaten zu regeln, obwohl diese zunächst zur Konkretisierung des Tatbestands der elektronischen Signatur berufen sind.[487] Die nach diesen Kriterien festgestellte Übereinstimmung der sicheren Signaturerstellungseinheiten mit den Anforderungen des Anhangs III muss dann von allen Mitgliedstaaten akzeptiert werden.[488] Hier zeigt sich, dass die RLeS dem Konzept des Verweises auf verbindliche außerrechtliche Technikstandards folgt.[489]

---

[484] Anhang III Nr. 1 lit. a) und b) RLeS.

[485] Art. 3 Abs. 4 S. 1 RLeS.

[486] Die Kommission kann dabei Referenznummern für allgemein anerkannte Normen festlegen. Sofern ein Produkt diesen Normen entspricht, wird davon ausgegangen, dass es die Anforderungen von Anhang II lit. f) und Anhang III erfüllt, Art. 3 Abs. 5 RLeS.

[487] Siehe Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 109.

[488] Art. 3 Abs. 4 RleS.

[489] Anhang III Nr. 2 RLeS. Anhang III liegt ein Streit einiger Mitgliedstaaten zu Grunde. So wollte Deutschland nur solchen elektronischen Signaturen eine rechtliche Wirksamkeit zusprechen, die durch Produkte hergestellt werden, die ein Minimum an technischer Sicherheit gewährleisten. Andere Staaten wie Großbritannien widersprachen obligatorischen Produkterfordernissen; siehe Dumortier/Van Eecke, CLSR 1999, S. 111/112. Die Einhaltung der Sicherheitsanforderungen überließ die RLeS-V der jeweiligen Zertifizierungsstelle, eine ausreichende Sicherheit sollte sich über den Markt herausbilden, die Einhaltung der Anforderungen durch Drohung und Belohnung unterstützt werden. Der Entwurf sah eine vom Verschulden des Zertifizierungsdienstanbieters unabhängige Haftung vor. Die Mitgliedstaaten konnten sich nicht darauf einigen, ob die Richtlinie überhaupt technische Sicherheitsanforderungen enthalten sollte. Letztlich wurde das Regelungskonzept weitgehend beibehalten, die RLeS um technische Anforderungen ergänzt. Zum anderen wurden Kontrollverfahren vorgesehen. Außerdem sollen die Mitgliedstaaten ein Aufsichtssystem über die Zertifizierungsdiensteanbieter aufstellen. Schließlich wurde mit Art. 6 RLeS eine Haftungsregelung vorgesehen. Siehe bei Roßnagel, MMR 1999, S. 262.

Das Pendant zu Signaturerstellungsdaten und -einheiten stellen Signaturprüfdaten und -einheiten dar.[490] Für die Signaturprüfung stellt die RLeS keine Anforderungen, lediglich in Anhang IV Empfehlungen für die sichere Signaturprüfung.[491] Danach soll mit hinreichender Sicherheit unter anderem gewährleistet sein, dass die Echtheit und die Gültigkeit des zum Zeitpunkt der Überprüfung der Signatur verlangten Zertifikats zuverlässig überprüft[492] und dass sicherheitsrelevante Veränderungen erkannt[493] werden können.[494] Die RLeS hat sich nicht für oder gegen die hardware- oder softwarebasierte Installation des privaten Schlüssels beim Nutzer entschieden. Damit bleibt ein entscheidendes Qualitätsmerkmal für elektronische Signaturen offen.[495] Die fortgeschrittene elektronische Signatur betreffende Vorschriften lassen jedoch darauf schließen, dass eine solche Signatur nur mit einem privaten Schlüssel erstellt werden kann, der auf sich auf einem Medium befindet, über das der Signierende totale physische Kontrolle besitzt.[496]

2.2.2.3 Zertifizierungsanbieter und qualifizierte Zertifikate

Zentrales Merkmal der von der RLeS vorausgesetzten Sicherungsinfrastruktur sind Zertifikate für elektronische Signaturen.[497] Die RLeS definiert Zertifikate Art. 2 Nr. 9 als

> *„elektronische Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und die Identität einer Person bestätigt wird“.*

Auch hier wird unterschieden zwischen (einfachen) Zertifikaten, an die keine weiteren Anforderungen gestellt werden, und qualifizierten Zertifikaten. Letztere zeichnen sich dadurch aus, dass sie die in Anhang I RLeS bestimmten Anforderungen erfüllen und von einem Zertifizierungsdiensteanbieter bereitgestellt werden, der seinerseits die in Anhang II RLeS bestimmten Anforderungen erfüllt, Art. 2 Nr. 10 RLeS. Zertifizie-

---

[490] Art. 2 Nr. 7 RLeS: Signaturprüfdaten sind *„Daten wie Codes oder öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden“*. Art. 2 Nr. 8 RLeS: Signaturprüfeinheit ist *„eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturprüfdaten verwendet wird“*. Ferner definiert Art. 2 Nr. 12 RLeS Produkte für elektronische Signaturen als *„Hard- oder Software bzw. deren spezifische Komponenten, die von einem Zertifizierungsdiensteanbieter für die Bereitstellung von Diensten für elektronische Signaturen verwendet werden sollen oder die für die Erstellung und Überprüfung elektronischer Signaturen verwendet werden sollen“*.

[491] Weil sich die Mitgliedstaaten nicht auf verbindliche Anforderungen einigen konnten; Roßnagel, K&R 2000, S. 316, 317.

[492] Anhang IV lit. d) RLeS.

[493] Anhang IV lit. g) RLeS.

[494] Daneben bezieht sich Anhang IV auf eher selbstverständlich erscheinende Aspekte und auf technische Kriterien an die Überprüfung, etwa dass mit hinreichender Sicherheit gewährleistet sein soll, dass: *„a) die zur Überprüfung der Signatur verwendeten Daten den Daten entsprechen, die dem Überprüfer angezeigt werden, b) die Signatur zuverlässig überprüft wird und das Ergebnis dieser Überprüfung korrekt angezeigt wird,…*[etc.]*“*

[495] Zutreffend Geis, MMR 2000, S. 668.

[496] Etwa die SmartCard, siehe Mason, *Electronic Signatures in Law*, S. 247.

[497] Siehe z.B. Erwägungsgrund 20 RLeS: *„… Zertifikate können dazu dienen, die Identität einer elektronisch signierenden Person zu bestätigen.“*

rungsdienstanbieter erbringen dabei vielfältige Dienstleistungen der Infrastruktur für Signaturverfahren.[498] Sie werden nicht allein durch ihre Tätigkeit des Zertifizierens definiert, sondern die RLeS erfasst unter diesem Begriff alle Funktionen der Sicherungsinfrastruktur. Die RLeS ermöglicht dadurch (theoretisch) unterschiedliche organisatorische Strukturen von Sicherungsdienstleistungen. Zur Zertifikatshierarchie enthält die Richtlinie keine Vorgaben, insbesondere ist keine Wurzelzertifizierungsinstanz vorgesehen. Die Zertifizierungsdiensteanbieter müssen sich also selbst zertifizieren und beispielsweise versuchen, durch vielfältiges Cross-Zertifizieren für eine europaweite faktische Anerkennung ihrer Zertifikate zu sorgen.[499] Besondere Anforderungen an (einfache) Zertifizierungsdiensteanbieter stellt die Richtlinie nicht. Dagegen enthält Anhang II einen Katalog von zwölf allgemeinen funktionalen Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen. Danach haben diese sowohl Sicherheitsmaßnahmen für die einzelnen Stellen zu gewährleisten, als auch für die Infrastruktur notwendige Pflichtdienstleistungen zu erbringen. Gemäß Anhang II RLeS müssen diese Zertifizierungsdiensteanbieter hinsichtlich ihres Betriebs und der dafür verwendeten Technik:

> *„... die erforderliche Zuverlässigkeit... nachweisen;*[500]
>
> *... den Betrieb eines schnellen und sicheren Verzeichnisdienstes und eines sicheren und unverzüglichen Widerrufsdienstes gewährleisten;...“*[501]
>
> *„... vertrauenswürdige Systeme und Produkte einsetzen, die vor Veränderungen geschützt sind und die die technische und kryptographische Sicherheit... gewährleisten;“*[502] und
>
> *„... vertrauenswürdige Systeme für die Speicherung von Zertifikaten in einer überprüfbaren Form verwenden, so dass nur befugte Personen Daten eingeben und ändern können; die Angaben auf ihre Echtheit hin überprüft werden können; Zertifikate nur in Fällen öffentlich abrufbar sind, für die die Zustimmung des Inhabers des Zertifikats eingeholt wurde; technische Veränderungen, die die Einhaltung dieser Sicherheitsanforderungen beeinträchtigen, für den Betreiber klar ersichtlich sind.“*[503]

Auch die oben dargestellten Anforderungen aus Anhang III RLeS an sichere Signaturerstellungseinheiten sind hier zu berücksichtigen. Dies gilt insbesondere in dem Fall, in

[498] Sie werden in Art. 2 Nr. 11 RLeS definiert als Stellen oder juristische oder natürliche Personen, die Zertifikate ausstellen oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellen.

[499] Roßnagel, K&R 2000, S. 316; Neuser, MMR 1999, S. 68, der auf mögliche negative Auswirkungen dieser Konzeption, bei der die Diensteanbieter ihrerseits nicht in eine Zertifizierungsstruktur eingebunden sind, hinweist. Die Durchsetzung von Haftungsansprüchen gegen den Diensteanbieter könne scheitern, sollte dieser nicht ermittelt werden können.

[500] Anhang II lit. a) RLeS.

[501] Anhang II lit. b) RLeS.

[502] Anhang II lit. f) RLeS.

[503] Anhang II lit. l) RLeS.

dem der Zertifizierungsdiensteanbieter auch für die zur Signaturerstellung benötigte und beim Nutzer zum Einsatz kommende Hard- und Software verantwortlich ist. Auch implizieren die Anforderungen der Anhänge II und III[504] die Forderung, eine hinreichend sichere Technik zu konfigurieren, zu zertifizieren, zu verwenden und gegebenenfalls bereitzustellen. Hinreichende Sicherheit kann nur die jeweils letzte Entwicklungsstufe einer solchen Technologie bieten. Dies kommt einem Auftrag zur ständigen Aktualisierung und Modifizierung der angewendeten Hard- und Software gleich, insbesondere wo Anhang II lit. l) RLeS den Einsatz funktional näher umschriebener vertrauenswürdiger Systeme und Produkte verlangt. Für die Darstellungskomponenten oder die Komponenten, in denen Signaturerstellungseinheiten zum Einsatz kommen, sieht die RLeS keine Regelungen vor. Dies kann Sicherheitslücken eröffnen.[505] Neben Signaturerstellungseinheiten, deren Hersteller (lediglich) behaupten, sie seien sicher, sieht die RLeS auch für diese vertrauenswürdigen Systeme und Produkte keine Vorabprüfung vor. Ob diese tatsächlich die Anforderungen des Anhangs II erfüllen, muss daher bis zum entscheidenden Rechtsstreit offen bleiben.[506]
Zertifizierungsdiensteanbieter müssen gemäß Anhang II RLeS ferner:

> *„… mit geeigneten Mitteln nach einzelstaatlichem Recht die Identität und gegebenenfalls die spezifischen Attribute der Personen überprüfen, für die ein qualifiziertes Zertifikat ausgestellt wird;“*[507]
>
> *„… bevor sie in Vertragsbeziehungen mit einer Person eintreten, die von ihnen ein Zertifikat zur Unterstützung ihrer elektronischen Signatur wünscht, diese Person mit einem dauerhaften Kommunikationsmittel über die genauen Bedingungen für die Verwendung des Zertifikats informieren,... Diese Angaben müssen schriftlich – gegebenenfalls elektronisch übermittelt – in klar verständlicher Sprache vorliegen. …“*[508]
>
> *„… Maßnahmen gegen Fälschungen von Zertifikaten ergreifen und... die Vertraulichkeit während der Erzeugung* [der Signaturerstellungsdaten] *gewährleisten;“*[509] sowie
>
> *„… alle einschlägigen Informationen über ein qualifiziertes Zertifikat über einen angemessenen Zeitraum aufzeichnen, um insbesondere für Gerichtsverfahren die Zertifizierung nachweisen zu können... “*[510]

Ferner dürfen die Zertifizierungsdiensteanbieter die privaten Schlüssel (Signaturerstellungsdaten) nicht speichern, Anhang II lit. j). Die RLeS verpflichtet die Diensteanbieter

[504] Siehe 2.2.2.4 und 2.2.2.5.

[505] Siehe dazu ausführlich unten unter3.2.1.4.

[506] Roßnagel, K&R 2000, S. 317.

[507] Anhang II lit. d) RLeS. Die Richtlinie präzisiert die Identitätsfeststellung des Nutzers nur unter datenschutzrechtlichen Aspekten, Art. 8 Abs. 2 RLeS.

[508] Anhang II lit. k) RLeS.

[509] Anhang II lit. g) RLeS.

[510] Anhang II lit. i) RLeS.

nicht zur Einrichtung eines Prüfungsdienstes für Dritte. Allerdings ist der Diensteanbieter wegen seines ansonsten unbegrenzten Haftungsrisikos faktisch dazu gezwungen, einen solchen vorzuhalten und garantiert störungsfrei zu betreiben.[511] Als weitere persönliche und sachliche Voraussetzung der Diensteanbieter sieht Anhang II RLeS vor, diese müssten:

> *„... Personal mit den... erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen beschäftigen;...*[512] sowie
>
> *„... über 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... ;"*[513]

Sofern Zertifizierungsdiensteanbieter die Anforderungen des Anhangs II RLeS erfüllen, können sie qualifizierte Zertifikate ausstellen. Diese qualifizierten Zertifikate müssen folgendes enthalten:

> *„a) die Angabe, dass das Zertifikat als qualifiziertes Zertifikat ausgestellt wird;*
>
> *b) die Angabe des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist;*
>
> *c) den Namen des Unterzeichners oder ein Pseudonym,...*
>
> *d) Platz für ein spezifisches Attribut des Unterzeichners, das gegebenenfalls je nach Bestimmungszweck des Zertifikats aufgenommen wird:*
>
> *e) Signaturprüfdaten, die den vom Unterzeichner kontrollierten Signaturerstellungsdaten entsprechen;*
>
> *f) Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikats;*
>
> *g) Identitätscode des Zertifikats;*
>
> *h) die fortgeschrittene elektronische Signatur des ausstellenden Zertifizierungsdiensteanbieters;..."*[514]

sowie gegebenenfalls Beschränkungen des Geltungsbereichs des Zertifikats und Begrenzungen des Werts der über das Zertifikat ausführbaren Transaktionen.[515]

---

[511] Neuser, MMR 1999, S. 71 und unter 2.2.2.5.

[512] Anhang II lit. e) RLeS.

[513] Anhang II lit. h) RLeS. Die RLeS nennt in Anhang II lit. h) exemplarisch den Abschluss einer entsprechenden Versicherung, um dieser Deckungsvorsorgeverpflichtung nachzukommen Ein solcher Versicherungsschutz auch für Vermögensschäden ist grundsätzlich auch für die Risiken elektronischer Signaturen möglich; Neuser, MMR 1999, S. 71.

[514] Anhang I lit. a) bis j) RLeS.

[515] Anhang I lit. i) und j) RLeS, siehe unter 2.2.5.

2.2.2.4 Freiwillige Akkreditierung und Überwachung der Zertifizierungsdiensteanbieter

Eine Überprüfung der Anforderungen des Anhangs II ist weder vor der Aufnahme eines Zertifizierungsdienstes vorgesehen, noch für die Zeit des Betriebes konkretisiert. Vielmehr verbietet es die RLeS den Mitgliedstaaten, das Angebot von Zertifizierungsdiensten von einem Zulassungsverfahren abhängig zu machen.[516] Den Mitgliedstaaten steht es jedoch frei, bestimmte freiwillige Akkreditierungssysteme einzuführen oder beizubehalten.[517] Ihr Gestaltungsspielraum umfasst sowohl das Ob als auch das Wie der Etablierung von Akkreditierungssystemen.[518] Die Lizenzierung durch die freiwillige Akkreditierung mit dem Charakter einer öffentlichen Dienstleistung ist gedacht als Angebot an die EU-Mitgliedstaaten.[519] Aber auch das Tätigwerden ohne freiwillige Akkreditierung soll erlaubt werden.[520] Die Begrenzungen des grundsätzlich großen Gestaltungsspielraums der Mitgliedstaaten sind in Art. 3 Abs. 2 RLeS beschrieben. Sie beziehen sich ausschließlich auf die Anforderungen der Akkreditierung, nicht auf die an die Akkreditierung geknüpften Rechtsfolgen.[521] Die Verfasser der RLeS rechnen in der Ausgestaltung von Akkreditierungssystemen mit unterschiedlichen nationalen Lösungen zwischen denen ein Wettbewerb entfacht werden soll.[522] Insoweit nach einem bereits be-

[516] Erwägungsgrund 10 RLeS stellt dazu fest: *„... Um das gemeinschaftsweite Anbieten von Zertifizierungsdiensten über offene Netze zu fördern, sollten Anbieter von Zertifizierungsdiensten diese ungehindert ohne vorherige Genehmigung bereitstellen können."* Siehe auch Erwägungsgrund 10: *„Vorherige Genehmigung bedeutet nicht nur eine Erlaubnis, wonach der betreffende Zertifizierungsdiensteanbieter einen Bescheid der einzelstaatlichen Stellen einholen muss, bevor er seine Zertifizierungsdienste erbringen kann, sondern auch alle sonstigen Maßnahmen mit gleicher Wirkung."* Und Erwägungsgrund 21 RLeS: *„Die rechtliche Anerkennung elektronischer Signaturen sollte auf objektiven Kriterien beruhen und nicht mit einer Genehmigung für den betreffenden Zertifizierungsdiensteanbieter verknüpft sein."*

[517] Art. 3 Abs. 2 S. 1 RLeS. Akkreditieren heißt beglaubigen oder auch „Kredit verschaffen". Die freiwillige Akkreditierung wird in Art. 2 Nr. 13 RLeS definiert als *„eine Erlaubnis, mit der die Rechte und Pflichten für die Erbringung von Zertifizierungsdiensten festgelegt werden und die auf Antrag des betreffenden Zertifizierungsdiensteanbieters von der öffentlichen oder privaten Stelle… erteilt wird…"*

[518] Roßnagel, K&R 2000, S. 319.

[519] Sie bietet Vorteile insbesondere im öffentlichen Bereich, siehe Art. 3 Abs. 7 RLeS; Schumacher, CR 1998, S. 761; Geis, MMR 2000, S. 699, 670. Diese zusätzlichen Anforderungen *„müssen* [u.a.] *objektiv, transparent, verhältnismäßig und nicht diskriminierend sein und dürfen sich nur auf die spezifischen Merkmale der betreffenden Anwendung beziehen"*, Art. 3 Abs. 7 S. 2 und 3 RLeS. Nicht von der Einschränkung betroffen sind somit Zertifizierungsdienste für die Verwaltung. Ausführlich Roßnagel, K&R 2000, S. 322.

[520] Erwägungsgrund 12 RLeS. Die RLeS räumt freiwilligen Akkreditierungssystemen, *„die auf eine Steigerung des Niveaus der erbrachten Zertifizierungsdienste abzielen,"* den Vorrang ein. Sie könnten *„den geeigneten Rahmen für die Weiterentwicklung ihrer Dienste bieten, um das... geforderte Maß an Vertrauen, Sicherheit und Qualität zu erreichen"* und sollten die Entwicklung von *best practices* fördern; Erwägungsgrund 11 RLeS. Art. 3 Abs. 2 S. 2 RLeS verlangt, das alle mit diesen Systemen verknüpften Anforderungen objektiv, transparent, verhältnismäßig und nicht diskriminierend sein müssten. Die RLeS geht davon aus, dass freie Akkreditierungssysteme im Gegensatz zur obligatorischen Vorabprüfung einen freien Marktzugang gewährleisten; Schumacher, CR 1998, S. 761; Geis, MMR 2000, S. 668/669.

[521] Erwägungsgrund 21 RLeS; Roßnagel, K&R 2000, S. 318. Neben den genannten Aspekten gibt die Richtlinie hierfür nur wenige Rahmendaten vor; Ausführlich Roßnagel, K&R 2000, S. 319; Erwägungsgrund 12 S. 3, 13 S. 3 RLeS; Art. 3 Abs. 2 S. 3 RLeS.

[522] Siehe Art. 3 Abs. 2 S. 1 RLeS und Roßnagel, K&R 2000, S. 319.

stehenden Akkreditierungs- oder Prüfsystem genehmigte Zertifizierungsstellen existieren, die den hier gestellten Anforderungen entsprechen, soll ihnen die Fortführung ihrer Tätigkeit ermöglicht werden. Die Mitgliedstaaten sollen ein Überwachungssystem über die in ihrem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter einrichten, das die Einhaltung der Bestimmungen der Richtlinie stichprobenartig und anlassbezogen prüfen kann.[523]

2.2.2.5 Haftung der Zertifizierungsdiensteanbieter

An einfache Zertifizierungsdiensteanbieter (sofern keine qualifizierten Zertifikate ausgestellt werden) stellt die RLeS keine Anforderungen. Sie unterliegen folglich auch nicht der in Art. 3 Abs. 3 RLeS geforderten Überwachung. Schon dies macht deutlich, dass das europäische System der freiwilligen Akkreditierung um eine Haftung für falsche Zertifizierungen ergänzt werden musste.[524] Folglich enthält die RLeS einige Regelungen zur Haftung und zur Begrenzung der Haftung von Zertifizierungsdiensteanbietern.[525] Die RLeS verfolgt die Grundidee der Privatisierung der Sicherungsinfrastruktur. Dabei geht die RLeS davon aus, dass harmonisierte Haftungsregelungen die Vertrauensbasis bei den Beteiligten stärken und damit zur breiten Akzeptanz elektronischer Signaturen beitragen. Die Regelungsziele sollen durch die Aktivierung von Marktmechanismen erreicht werden. Die Haftung der Diensteanbieter ist dabei das einzige durchsetzungsorientierte Rechtsinstrument der RLeS.[526] Für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate öffentlich ausstellen, oder für diese öffentlich einstehen, fordert Art. 6 Abs. 1 RLeS als Mindestregelung, dass die Mitgliedstaaten eine Verschuldenshaftung mit Umkehr der Beweislast einführen. So soll der Anbieter gegenüber jedem, der vernünftigerweise auf das Zertifikat vertraut, dafür haften, dass

> *„a) alle Informationen in dem qualifizierten Zertifikat zum Zeitpunkt seiner Ausstellung richtig sind und das Zertifikat alle für ein qualifiziertes Zertifikat vorgeschriebenen Angaben enthält,*
>
> *b) der... angegebene Unterzeichner zum Zeitpunkt der Ausstellung des Zertifikats im Besitz der Signaturerstellungsdaten war, die den im Zertifikat angegebenen beziehungsweise identifizierten Signaturprüfdaten entsprechen,...“*

Ferner soll der Anbieter dafür haften, dass, wenn

---

[523] Art. 3 Abs. 3 RLeS. Dabei können die Mitgliedstaaten entscheiden, wie sie das Überwachungssystem ausgestalten, etwa privatwirtschaftlich; Roßnagel, K&R 2000, S. 316.

[524] Geis, MMR 2000, S. 668/669; Roßnagel, K&R 2000, S. 316; Siehe auch oben 1.4.2.3.

[525] Erwägungsgrund 22 RLeS stellt dazu zunächst nur fest: *„Diensteanbieter, die ihre Zertifizierungsdienste öffentlich anbieten, unterliegen den einzelstaatlichen Haftungsregelungen.“* Siehe auch Geis, MMR 2000, S. 669.

[526] Neuser, MMR 1999, S. 67.

> *„der Zertifizierungsdiensteanbieter sowohl die Signaturerstellungsdaten als auch die Signaturprüfdaten erzeugt, beide Komponenten in komplementärer Weise genutzt werden können,...“*[527]

sowie dafür, dass ein Widerruf des Zertifikats rechtzeitig registriert wird.[528] Liegt ein Fehler vor, muss danach der Anbieter nachweisen, dass er nicht fahrlässig gehandelt hat. Die Haftung des Diensteanbieters bezieht sich zunächst auf *„alle Informationen* [im] *qualifizierten Zertifikat“*[529], unterscheidet also nicht zwischen solchen Informationen von oder über den Zertifikatinhaber und solchen von oder über den Diensteanbieter. Letzterer haftet für Schäden, *„es sei denn,* [er] *weist nach, dass er nicht fahrlässig gehandelt hat.“*[530] Diese Regelung stellt lediglich einen Haftungsausschluss mit einer entsprechenden Beweisregel dar. Der Hinweis auf die Fahrlässigkeit verweist auf die Anforderungen an den Diensteanbieter, nach denen dieser *„mit geeigneten Mitteln die Identität und... die spezifischen Attribute“* des Zertifikatinhabers überprüfen muss.[531] Der Begriff geeignete Mittel wird nicht weiter konkretisiert, ist aber wohl vergleichbar mit dem vielfach verwendeten Rechtsbegriff der Zumutbarkeit der Überprüfungsmaßnahmen.[532] Dies wird regelmäßig als ein Hinweis auf bestehende Verkehrssicherungspflichten zu werten sein. In der RLeS finden sich nun diese wenigen, genau definierten Haftungstatbestände. Ob der Zertifizierungsdiensteanbieter die Anforderungen des Anhanges II erfüllt, ist dagegen für seine Haftung ohne Belang.[533] Die Haftungsregelungen stellen laut Art. 6 Abs. 1 (am Anfang) RLeS nur eine Mindestregelung dar. Trotz der Harmonisierungsbemühungen ist es dennoch den Mitgliedstaaten überlassen, weitere Haftungstatbestände aufzustellen, etwa gestützt auf Anhang II, sofern ein Verstoß gegen die dort aufgeführten Anforderungen zu einem schadensursächlichen Fehler im Zertifikat oder ähnlichem führen.

Bezüglich der Nichteinhaltung technisch-organisatorischer Anforderungen sind zu Kausalitätsfragen und deren Nachweispflicht in der RLeS keine speziellen Regelungen enthalten. Grundsätzlich liegt folglich die Beweislast beim Geschädigten, was diesen mitunter vor erhebliche Probleme stellen kann.[534] Denn weder sind Regelungen zur Beseitigung der Informationsasymmetrie, zur sachgerechten Risikoverteilung für den Fall, dass eine mögliche Verantwortlichkeit des Zertifikatinhabers nicht auszuschließen ist,

---

[527] Art. 6 Abs. 1 lit. c) RLeS.

[528] Art. 6 Abs. 2 RLeS.

[529] Art. 6 Abs. 1 lit. a) RLeS.

[530] Art. 6 Abs. 1 a.E. RLeS.

[531] Anhang II RLeS, insbesondere lit. d).

[532] Wie auch noch im ursprünglichen Richtlinienvorschlag (RLeS-V), Art. 6 Abs. 2 RLeS-V, also als Haftung für vermutetes Verschulden mit der Möglichkeit des Entlastungsbeweises; Ausführlich bei Neuser, MMR 1999, S. 69. Im RLeS-V war ursprünglich eine Haftung dafür vorgesehen, dass *„alle Anforderungen dieser Richtlinie... eingehalten“* werden, Art. 6 Abs. 1 lit. b) - d) RLeS-V. Die Einhaltung der Sicherheitsanforderungen überließ der RLeS-V der jeweiligen Zertifizierungsstelle. Hierzu Roßnagel, MMR 1999, S. 262.

[533] Dumortier/van Eecke, CLSR 1999, S. 111.

[534] Siehe dazu oben 1.3.1.3, 1.3.2.5, 1.3.3.5 und unten 3.2.2.

noch ein Sperrungsanspruch des Geschädigten vorgesehen.[535] Ferner wird auf außerrechtliche Standards verwiesen.[536] Für die Sorgfaltspflichten des Diensteanbieters folgt hieraus, dass eine Haftung ausscheidet, sofern die verwendeten technischen Komponenten den im Amtsblatt der EG veröffentlichten technischen Normen entsprechen, auch wenn Teile der Sicherungsinfrastruktur wegen aktueller Manipulationsmöglichkeiten mittlerweile unsicher geworden sein sollten. Dies führt zwar zu einer größeren Rechtssicherheit des Diensteanbieters. Nachfolgend entdeckte Sicherheitslücken bei den Signaturprodukten könnten jedoch nicht rechtzeitig, also kurzfristig, im Wege eines europäischen Normsetzungsverfahrens geschlossen werden.[537] Unter Umständen besteht also keine Haftung für Schäden durch Sicherheitslücken, die im Zeitpunkt der Zertifikatverwendung erkennbar waren. Dies entspricht im Ergebnis einem Haftungsausschluss für Entwicklungsrisiken.[538] Maßgeblicher Zeitpunkt für die Haftung des Diensteanbieters (für die im Zertifikat enthaltenen Informationen und für den Besitz der Signaturerstellungsdaten) soll der Zeitpunkt der Ausstellung des Zertifikats sein. Damit fällt die Pflicht zur Sicherstellung der Richtigkeit der Informationen zum Zeitpunkt der Verwendung des Zertifikats aus dem Haftungsbereich. Nur die Haftung für die komplementäre Nutzungsmöglichkeit von Signaturerstellungs- und Signaturprüfdaten und für den Widerrufsdienst verweisen auf den durch die Gültigkeits- und Nutzungsdauer des Zertifikats vorgegebenen Zeitraum auch nach der Ausstellung des Zertifikats.[539] Eine gewisse Einschränkung der Haftung erfolgt dadurch, dass ein schutzwürdiges Vertrauen des Dritten nur anerkannt wird, wenn dieser *„vernünftigerweise* [auf das Zertifikat] *vertraut“* hat. Eine weitere Konkretisierung findet nicht statt, allerdings ist damit, im Rahmen einer sinnvollen Risikoverteilung, eine Mitwirkungspflicht hinsichtlich der Nutzung der Prüfdienste festgeschrieben. Des Weiteren wird die Möglichkeit einer Beschränkung der Verwendungsmöglichkeit des Zertifikats sowie einer relativen Haftungsbegrenzung hinsichtlich des Werts der mit der zertifizierten fortgeschrittenen elektronischen Signatur durchgeführten Transaktionen gegeben.[540] Ein Haftungsausschluss hinsichtlich der im Zertifikat enthaltenen Informationen ist nicht vorgesehen. Eine Rechtsfolgeregelung für den Fall eines Verstoßes gegen die Deckungsvorsorgepflicht aus in Anhang II lit. h) RLeS findet sich nicht.[541]

---

[535] So gefordert von Neuser, MMR 1999, S. 70, 73, siehe auch oben 1.4.2.3 und 1.4.2.4.

[536] Siehe dazu 1.4.2.6.

[537] So zutreffend Neuser, MMR 1999, S. 73.

[538] Neuser, MMR 1999, S. 73.

[539] Hiermit wird der Vertrauensschutz des Dritten abgedeckt, da die Haftung greift, wenn sich dessen Vertrauen auf das Zertifikat realisiert. Im Unterschied zum RLeS-V, nach dem zunächst die Einhaltung aller technisch-organisatorischen Anforderungen nur bei Erstellung des Zertifikats haftungsbewehrt sein sollte. Siehe Neuser, MMR 1999, S. 70.

[540] Art. 6 Abs. 3 und 4 RLeS; Roßnagel, K&R 2000, S. 318. Durch Angaben im Zertifikat kann die Haftung auf bestimmte Verwendungen der Zertifikate oder einen bestimmten Wert der Transaktionen begrenzt werden. Sofern diese Beschränkung oder Grenze für Dritte erkennbar ist, haftet der Anbieter nicht für darüber hinaus gehenden Schäden, Art. 6 Abs. 3 und 4 RLeS.

[541] Anhang II lit. h) RLeS fordert ausreichende Finanzmittel zur Absicherung des Haftungsrisikos, zum Beispiel durch Abschluss einer entsprechenden Versicherung. Eine Bezugnahme auf diese Regelung erfolgt lediglich über die Definition des qualifizierten Zertifikats sowie der Aufgaben des Ausschusses, Art. 2 Nr. 10, Art. 10 RLeS. Sie sind nicht ausdrücklich in die Haftungsregelungen des Art. 6 RLeS

2.2.2.6 Rechtsgültigkeit und Gleichstellung elektronischer Signaturen

Neben den Definitionen und Anforderungen an elektronische Signaturen und deren Sicherungsinfrastruktur ist die rechtliche Anerkennung ihrer Nutzung als zulässige Handlungsform auch für formgebundene Willenserklärungen wesentlicher Regelungsinhalt der RLeS. Die Gleichstellung dieser *„Identifizierungsarchitektur der Informationsgesellschaft"* mit der Unterschrift wird als Kern der Richtlinie bezeichnet.[542] Hier berührt eine europaweite Regelung die Formvorschriften der Mitgliedstaaten und damit voneinander teilweise sehr unterschiedliches nationales Recht. Die RLeS beschränkt sich daher auf die Schaffung eines Rechtsrahmens für die Einführung und Nutzung der elektronischen Signatur, also auf eine gemeinschaftlich einheitliche rechtliche Grundlage zum Anbieten von Zertifizierungsdiensten.[543] Nur sofern sich aus der Nutzung der elektronischen Signatur deren Funktionsgleichheit mit der eigenhändigen Unterschrift ergibt, soll dies in den Formvorschriften der Mitgliedstaaten auch zum Ausdruck kommen.[544] Die wesentliche Regelung hinsichtlich der Formvorschriften findet sich in Art. 5 RLeS. Zwar beschränkt die RLeS die Wirksamkeit der einfachen elektronischen Signatur auf formfreie Erklärungen.[545] Die fortgeschrittene elektronische Signatur soll aber unter gewissen Umständen mit einer weiter gehenden Rechtsfolge versehen werden. Gemäß Erwägungsgrund 20 RLeS können sie, wenn sie von einer sicheren Signaturerstellungseinheit erstellt werden, gegenüber handschriftlichen Unterschriften als rechtlich gleichwertig angesehen werden, wenn die Anforderungen für handschriftliche Unterschriften erfüllt sind[546], mithin Funktionsgleichheit besteht. Art. 5 Abs. 1 lit. a) RLeS:

> *„Die Mitgliedstaaten tragen dafür Sorge, dass fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und die von einer sicheren Signaturerstellungseinheit erstellt werden,... 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,..."*

Diese Signaturen sind also in ihrer rechtlichen Wirksamkeit den eigenhändigen Unterschriften auf Papier rechtlich gleichzustellen und treten neben diese als rechtlich gleichwertige Handlungsform. Hierbei muss unterschieden werden zwischen Schrift-

---

aufgenommen und auch im Anhang II RLeS findet sich keine Rechtfolgeregelung für den Verstoß gegen das Gebot. Dies wird als problematisch angesehen; so Roßnagel, K&R 2000, S. 318.

[542] Geis, MMR 2000, S. 668.

[543] Erwägungsgrund 20 RLeS: *„Durch harmonisierte Kriterien im Zusammenhang mit der Rechtswirkung elektronischer Signaturen lässt sich gemeinschaftsweit ein kohärenter Rechtsrahmen aufrechterhalten. In den einzelstaatlichen Rechtsvorschriften sind verschiedene Anforderungen für die Rechtsgültigkeit handschriftlicher Unterschriften niedergelegt."*

[544] Erwägungsgrund 28 erklärt, das Ziel der Schaffung harmonisierter rechtlicher Rahmenbedingungen könne besser durch die Gemeinschaft verwirklicht werden, ginge dabei aber *„nicht über das zur Erreichung dieses Ziels erforderliche Maß hinaus"*, Erwägungsgrund 28 RLeS.

[545] Geis, MMR 2000, S. 669; Mehr hierzu nachfolgend zu Art. 5 Abs. 2 RLeS.

[546] Erwägungsgrund 20 RLeS.

formerfordernissen, die verlangen, dass eine Willenserklärung in einer Urkunde verkörpert ist, und Unterschriftserfordernissen, nach denen sie vom Erklärenden eigenhändig unterschrieben werden muss. Hier sind nur letztere Erfordernisse gemeint.[547] Die Anforderungen an die handschriftliche Unterschrift, von denen Erwägungsgrund 20 spricht, werden von der RLeS nicht festgelegt. Der Vergleich mit dem rechtlichen Status der handschriftlichen Unterschrift muss also nach dem jeweiligen nationalen Recht für jeden Mitgliedstaat vorgenommen werden. Dabei werden einige Rechtsordnungen in den Mitgliedstaaten hinsichtlich der Anforderungen an die handschriftliche Unterschrift je nach dem Zeck der Unterschrift unterscheiden. Um die Voraussetzungen der handschriftlichen Unterschrift zu erfüllen, wird die fortgeschrittene elektronische Signatur die Funktionen der jeweiligen handschriftlichen Unterschrift erfüllen müssen.[548] Ziel der RLeS ist es zunächst, dass die Mitgliedstaaten die für die Bildung der Sicherungsinfrastruktur der elektronischen Signatur notwendigen Rechtsvorschriften und Haftungsregelungen erlassen. In der Vorschrift des Art. 5 RLeS wird nur die sich aus der somit garantierten Verlässlichkeit der fortschrittlichen elektronischen Signatur abgeleitete rechtliche Verwertbarkeit, also oben genannte Funktionsgleichheit festgestellt. Die Mitgliedstaaten werden verpflichtet, dies auch in den entsprechenden Gesetzen und Vorschriften zum Ausdruck zu bringen, indem sie diesen elektronischen Signaturen die gleiche Rechtswirkung wie der eigenhändigen Unterschrift zukommen lassen. Eine positive Verpflichtung zur Gleichstellung ist mit dieser Regelung nicht verbunden.[549] Vielmehr setzt Art. 5 Abs. 1 RLeS eine bereits vorliegende rechtliche Anerkennung voraus.[550] Von der rechtlichen Gleichstellung sollen die einfachen elektronischen Signaturen ausgenommen sein. Dennoch schreibt die RLeS auch ihre rechtliche Beachtlichkeit fest. Für sie bestimmt Art. 5 Abs. 2 RLeS, dass die Mitgliedstaaten dafür Sorge tragen, dass ihr

> *„die rechtliche Wirksamkeit... 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."*

Verlangt ist folglich eine konkrete inhaltliche Bewertung der elektronischen Signatur, ihrer Technologie und faktischen Sicherheit etc. im Einzelfall. Dies gilt sowohl im Hin-

[547] Art. 5 Abs. 1 lit. a) RLeS; Roßnagel, K&R 2000, S. 321

[548] Mason, Electronic Signatures in Law, S. 151.

[549] Roßnagel, K&R 2000, S. 318

[550] Gravesen/Dumortier/van Eecke, MMR 1999, S. 579: Hinsichtlich der Regelung der RLeS müsse unterschieden werden zwischen „eigentlichen" Schriftformerfordernissen und sekundären Formerfordernissen, die bestimmte Unterschriftsformen nicht vorschreiben, aber faktisch voraussetzen können. Neue Erfordernisse zur Schriftform könnten nur sehr beschränkt eingeführt werden, da sie der RLeS widersprächen.

blick auf eine gerichtliche Überprüfung als auch für regulierende Institutionen. Diese sind nicht zur Anerkennung der Rechtsgültigkeit der elektronischen Signatur an sich verpflichtet. Die gerichtliche oder regulative Anerkennung darf ihr aber nur aufgrund mangelnder Sicherheit nach einer konkreten Bewertung verweigert werden.[551] Einfache elektronische Signaturen sind folglich nicht per se rechtsunwirksam. Für sie wird die Beweislast umgekehrt. Die auf sie vertrauende Person muss ihre Zuverlässigkeit nachweisen, wie dies den allgemeinen Regeln zur Beweispflicht aller hier vorgestellten Rechtsordnungen entspricht.[552]

Eine darüber hinausgehende Harmonisierung nationaler vertragsrechtlicher Formvorschriften im Sinne von Wirksamkeitsvoraussetzungen beabsichtigt die RLeS ausdrücklich nicht. Formvorschriften werden nicht erfasst.[553] Die Regelungen über die rechtliche Wirksamkeit elektronischer Signaturen sollen unbeschadet einzelstaatlicher Formvorschriften gelten, die den Abschluss von Verträgen betreffen.[554] Dies bedeutet zum einen, dass Art. 5 RLeS nur anwendbar ist, wenn einzelstaatliche Formvorschriften die Anwendung der elektronischen Authentifizierung nicht ausschließen. Insoweit fällt damit die Frage der Rechtswirkung elektronischer Signaturen faktisch in einzelstaatliche Kompetenz.[555] Auch Erwägungsgrund 21 weist ergänzend darauf hin, dass die Festlegung der Rechtsgebiete, in denen elektronische Dokumente und elektronische Signaturen verwendet werden können, einzelstaatlichem Recht unterliegt.[556] Zum anderen wird deutlich, dass die Harmonisierung von Formvorschriften für privatrechtliche elektronische Verträge in den Regelungsbereich von Art. 9 RLeC fällt. Die rechtliche Wirksamkeit elektronischer Signaturen regelt die RLeS[557] über die Differenzierung nach ihrem Sicherheitsgrad, so dass die Mitgliedstaaten nur zur Anerkennung von fortgeschrittenen elektronischen Signaturen im Sinne des Art. 5 Abs. 1, Art. 2 Nr. 2 RLeS verpflichtet sind und gerade nicht jegliche elektronische Form als Formerfüllung genügen lassen müssen.[558] Dabei macht die Regelung des Art. 9 RLeC die des Art. 5 RLeS – oder umgekehrt – nicht überflüssig. Beide Regelungen haben eigenständige Regelungsbereiche und ergänzen sich insofern, als sie zusammengenommen dazu führen, dass eine mit einer solchen fortschrittlichen elektronischen Signatur gemäß der RLeS signierte Willens-

[551] Gravesen/Dumortier/van Eecke, MMR 1999, S. 579. Diese Regelung wird auch als de minimis-Gebot und eigentliche Grundregel des Art. 5 RLeS bezeichnet.

[552] Hörnle, JILT 2000 und oben 1.3.1.3, 1.3.2.5 und 1.3.3.5.

[553] Art. 1 Abs. 2 RLeS, auch oben 2.2.2.1.

[554] Auch gemäß Erwägungsgrund 17 zielt die RLeS *„... nicht darauf ab, nationales Vertragsrecht, insbesondere betreffend den Abschluss und die Erfüllung von Verträgen, oder andere, außervertragliche Formvorschriften bezüglich der Unterschriften zu harmonisieren."*

[555] So Gravesen/Dumortier/van Eecke, MMR 1999, S. 579.

[556] Ausführlicher zu Erwägungsgrund 21 RLeS siehe 2.2.2.4 und nachfolgend 2.2.2.6.

[557] Erwägungsgrund 34 RLeC: *„... Die rechtliche Wirksamkeit elektronischer Signaturen ist bereits Gegenstand der* [RLeS]*."*

[558] Die RLeS bestimmt auch nicht, wo diese Anerkennung zu erfolgen hat. Bezüglich der Differenzierung gemäß Art. 5 Abs. 1 lit. a) RLeS, siehe Erwägungsgrund 35 RLeC: *„Diese Richtlinie lässt die Möglichkeit der Mitgliedstaaten unberührt, allgemeine oder spezifische rechtliche Anforderungen für Verträge, die auf elektronischem Wege erfüllt werde können, insbesondere Anforderungen für sichere elektronische Signaturen aufrechtzuerhalten oder festzulegen."*; Siehe auch Roßnagel, K&R 2000, S. 321.

erklärung sowohl Schriftform- als auch Unterschriftserfordernissen entspricht.[559] Hierbei ist nochmals darauf hinzuweisen, dass Art. 9 RLeC nur für Privatverträge, Art. 5 RLeS auch für den öffentlichen Bereich gilt.[560]

2.2.2.7 Beweiszulassung elektronischer Signaturen

Ein weiterer bedeutsamer Punkt ist die Einführung elektronischer Signaturen als Beweismittel, wobei die RLeS lediglich deren Nichtdiskriminierung und ihre Zulassung als Beweis regelt.[561] Regelungen zu ihrem Beweiswert finden sich wie auch in der RleC in der RLeS nicht. Art. 5 Abs. 1 RLeS bestimmt:

> *„Die Mitgliedstaaten tragen dafür Sorge, dass fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und die von einer sicheren Signaturerstellungseinheit erstellt werden,...*
>
> *b) in Gerichtsverfahren als Beweismittel zugelassen sind."*

Diese Anerkennung ist also gleichfalls nur für auf qualifizierten Zertifikaten beruhende elektronische Signaturen vorgesehen. Die Regelung zielt auf Prozessordnungen, nach denen Beweismittel zuzulassen oder für den Nachweis des Abschlusses bestimmter Verträge nur schriftliche Dokumente zugelassen sind. In Deutschland beispielsweise sind sie ohnehin Objekt der freien Beweiswürdigung.[562] Wie bei deren rechtlicher Wirksamkeit darf jedoch auch der (einfachen) elektronischen Signatur die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie die oben genannten Voraussetzungen nicht erfüllt.[563] Die RLeS lässt das nationale Beweisrecht in seiner vollen Unterschiedlichkeit von Mitgliedstaat zu Mitgliedstaat unberührt. Über die genannten expliziten Regelungen hinaus strebt sie gerade keine Harmonisierung des Beweisrechts zu elektronischen Signaturen an.[564] Die RLeS trifft weder Regelungen zum Beweiswert fortschrittlicher oder einfacher elektronischer Signaturen noch zum Beweisverfahren, zum Beispiel über die freie Würdigung von Beweismitteln, und sie unterstützt nicht die Beweisführung durch eine Beweisvermutung

---

[559] Nach Art. 9 Abs. 1 RLeC ist die elektronische Präsentation der Willenserklärung mit der Urkunde gleichzusetzen und nach Art. 5 Abs. 1 lit. a) RLeS die dort genannte elektronische Signatur der eigenhändigen Unterschrift gleichzustellen; Roßnagel, K&R 2000, S. 321.

[560] Wie bereits dargestellt fehlt für die RLeS eine Vorschrift, die wie die RLeC für die Verkörperung der Willenserklärung in einer Urkunde eine Gleichstellung anordnet. Daraus erwächst den Mitgliedstaaten ein erweiterter Handlungsspielraum; Roßnagel, K&R 2000, S. 321/322; siehe auch unten 3.1.1.

[561] Erwägungsgrund 21 RLeS: *„... ist zu gewährleisten, dass elektronische Signaturen in allen Mitgliedstaaten in Gerichtsverfahren als Beweismittel verwendet werden können."*

[562] Geis, MMR 2000, S. 669; oben 1.3.1.3 und 1.3.1.4.

[563] Art. 5 Abs. 2 RLeS. Auch elektronischen Signaturen aus so genannten geschlossenen Systemen sollte gemäß Erwägungsgrund 16 RLeS die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel nicht abgesprochen werden.

[564] Roßnagel, K&R 2000, S. 320.

oder -erleichterung.[565] Dies ist im Zusammenhang mit der Entscheidung gegen Vorabprüfungen der Signaturverfahren oder Genehmigungen der Zertifizierungsdienste zu sehen.[566] Eine Sicherheitsvermutung als Grundlage einer Beweisvermutung ist nur möglich in Verbindung mit einer solchen Vorabprüfung. Folglich muss der Nutzer die Erfüllung der in den Anhängen I bis III RLeS aufgeführten Anforderungen im Streitfall vor Gericht nachweisen. Hier besteht wiederum das Problem der Informationsasymmetrie; der Nutzer wird schwerlich zum Nachweis der Sicherheit des gesamten Signaturverfahrens in der Lage sein.[567] Hier greift daher die Möglichkeit der Mitgliedstaaten, freie Akkreditierungssysteme einzuführen oder beizubehalten.[568] Nur indem einmalig Prüf- und Bestätigungsstellen die angewandte Technologie, Verfahren und Verlässlichkeit der Zertifizierungsstelle feststellen, kann hierauf im Wege einer Sicherheitsvermutung Bezug genommen werden. Den Mitgliedstaaten ist das Recht belassen, den Nachweis der Sicherheit der angebotenen Verfahren für ihre eigenen Rechtsverfahren unterschiedlich zu bewerten und insbesondere das Beweisverfahren durch das Angebot einer Sicherheitsvermutung praktikabel zu machen.

2.2.2.8 Technikneutralität der RLeS

Die RLeS erkennt zutreffend, dass ein gemeinschaftsweites Rechtsgültigkeitsprivileg dann eine Behinderung marktorientierter Innovationsfreiheit zur Folge hätte, wenn es einer einzelnen spezifischen Technologie Exklusivität einräumte.[569] Eigene Vorgaben werden vermieden, insbesondere soll die Signaturtechnologie sich nicht allein auf die Zertifizierung beschränken.[570] Tatsächlich setzen elektronische und fortgeschrittene elektronische Signatur nicht notwendig die Sicherheitsqualität der PKI voraus.[571] Ihre beabsichtigte regulatorische Technikoffenheit versucht die RLeS über offene und abs-

[565] Siehe Erwägungsgrund 21. Art. 5 RLeS ist im Zusammenhang mit Art. 1 Abs. 2 RLeS zu sehen, oben 2.2.2.1. Hierzu auch Roßnagel, K&R 2000, S. 318.

[566] Art. 3 Abs. 1 RLeS und oben 2.2.2.4. Dazu auch Erwägungsgrund 21 RLeS: *„Die rechtliche Anerkennung elektronischer Signaturen sollte auf objektiven Kriterien beruhen und nicht mit einer Genehmigung für den betreffenden Zertifizierungsdiensteanbieter verknüpft sein."*

[567] So richtig Roßnagel, K&R 2000, S. 318, siehe oben 1.4.2.4 und unten unter 3.2.2, 3.2.2.4.

[568] Art. 3 Abs. 2 RLeS erlaubt ausdrücklich, Akkreditierungssysteme beizubehalten. Die Beibehaltung der Sicherheitsvermutung für Signaturverfahren von bereits akkreditierten Zertifizierungsstellen ist europarechtlich zulässig. Ein Verstoß gegen den Binnenmarktgrundsatz des Art. 4 Abs. 1 S. 2 RLeS ist nicht gegeben. Danach dürfen *„die Mitgliedstaten die Bereitstellung von Zertifizierungsdiensten, die aus anderen Mitgliedstaaten stammen, in den unter diese Richtlinie fallenden Bereichen nicht einschränken."* Die Sicherheitsvermutung stellt kein solches Markthindernis dar. Zutreffend Roßnagel, K&R 2000, S. 318 bis 320

[569] Nur Italien hatte bereits vor der RLeS das Signaturverfahren generell auf bestimmte Technologien begrenzt, siehe Gravesen/Dumortier/van Eecke, MMR 1999, S. 578. Erwägungsgrund 8 und 9 RLeS. Die Austauschbarkeit der verwendeten Technologie soll gesichert werden, so dass die jeweilige technologische Entwicklung und der globale Charakter der Internet-Technik sich das gesetzliche Rechtsgültigkeitsprivileg zunutze machen kann; Gravesen/Dumortier/van Eecke, MMR 1999, S. 578.

[570] *„ ...sondern sollte auch alle sonstigen Dienste und Produkte einschließen, die elektronische Signaturen verwenden oder mit ihnen zusammenhängen"*, Erwägungsgrund 9:

[571] Geis, MMR 2000, S. 669.

trakte Definitionen und Begriffsbildungen auszudrücken.[572] Allerdings macht die Anerkennung eines Rechtgültigkeitsprivilegs der Signaturverfahren eine möglichst präzise Festlegung der Sicherheitsanforderungen erforderlich, wie dies in Art. 5 Abs. 1 und in den Anhängen der RLeS geschieht.[573] Dabei macht bereits der Begriff Signaturerstellungsdaten die Orientierung an der asymmetrischen Kryptographie deutlich. Ebenso ist das Erfordernis eines Zertifikats tatsächlich eine aus der PKI stammende Komponente.[574] Ferner ist offensichtlich, dass nur diejenigen Reglungen der RLeS praktisch relevant sind, die sich in ihren Anforderungen und Folgen faktisch allein auf die Technik digitaler Signaturverfahren beziehen. Die Anforderungen aller vier Anhänge können nur von Public-Key-Infrastrukturen und technischen Komponenten für digitale Signaturen erfüllt werden.[575] Es wird kritisiert, dass somit eine unbeabsichtigt restriktive Wirkung erzielt werde und für zukünftige andere technologische Verfahren spezifische Anforderungen formuliert werden müssten.[576]

2.2.2.9 Binnenmarkt, gemeinschaftsfremde elektronische Signaturen

Das Grundprinzip der EU des freien Zuganges zum gemeinsamen Binnenmarkt wird auch in der RLeS für die Zertifizierungsdiensteanbieter festgeschrieben:

> *„Die Mitgliedstaaten dürfen die Bereitstellung von Zertifizierungsdiensten, die aus anderen Mitgliedstaaten stammen, in dem unter diese Richtlinie fallenden Bereich nicht einschränken.“*[577]

Produkte für elektronische Signaturen müssen, soweit sie den Anforderungen der RLeS entsprechen, frei im Binnenmarkt verkehren können.[578] Daneben regelt die RLeS die Anerkennung von Zertifikaten aus Drittstaaten. Danach sind qualifizierte Zertifikate, die von einem Zertifizierungsdiensteanbieter eines Drittlandes öffentlich ausgestellt werden, den von einem in der EU niedergelassenen Diensteanbieter ausgestellten Zertifikaten rechtlich gleichzustellen, wenn sie eine dieser drei Voraussetzungen erfüllen: Der Anbieter hat sich einem freiwilligen Akkreditierungssystem eines Mitgliedstaats der Europäischen Union unterworfen, oder ein in der EU niedergelassener Zertifizierungsdiensteanbieter steht für das Zertifikat eines internationalen Partners in gleichem Umfang ein wie für seine eigenen Zertifikate, oder das Zertifikat oder der Zertifizierungsdiensteanbieter ist im Rahmen einer bilateralen oder multilateralen Vereinbarung zwi-

[572] Z.B. Signaturerstellungs- und -Prüfdaten, Signaturerstellungs- und Signaturprüfeinheit.

[573] Siehe oben 2.4.2.

[574] Gravesen/Dumortier/van Eecke, MMR 1999, S. 578.

[575] Roßnagel, K&R 2000, S. 317.

[576] So Gravesen/Dumortier/van Eecke, MMR 1999, S. 578.

[577] Art. 4 Abs. 1 Satz 2.

[578] Art. 4 Abs. 2 RLeS.

schen der EU und Drittländern oder internationalen Organisationen anerkannt.[579] Ziel ist die Gleichbehandlung mit innereuropäischen Zertifikaten. Unklar hierbei sind die Pflichten der garantierenden Zertifizierungsstelle.[580]

2.2.2.10 Umsetzung

Die Mitgliedstaaten waren gemäß Art. 13 Abs. 1 RLeS dazu verpflichtet, die Richtlinie durch den Erlass der erforderlichen Rechts- und Verwaltungsvorschriften bis zum 19. Juli 2001 in nationales Recht umzusetzen.[581] Dabei sollte die Festlegung der Rechtsgebiete, in denen elektronische Dokumente und elektronische Signaturen verwendet werden können, einzelstaatlichem Recht unterliegen.[582] Die somit erlassenen innerstaatlichen Bestimmungen werden von den einzelnen Mitgliedstaaten *„auf die in* [ihrem] *Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter und deren Dienste“* angewendet.[583] Ferner können die Mitgliedstaaten entscheiden, wie sie die Überwachung der Einhaltung der Bestimmungen dieser Richtlinie gewährleisten.[584] Die Kommission ihrerseits soll von einem Ausschuss für elektronische Signaturen unterstützt werden, der die festgelegten Anforderungen, Kriterien und die allgemein anerkannten Normen und Sicherheitsstandards für Produkte für elektronische Signaturen präzisieren soll.[585]

2.2.3 Zusammenfassung und Kritik

Die RLeS gestaltet nur einige wichtige Anforderungen insbesondere an Zertifizierungsdiensteanbieter verpflichtend aus, andere als Empfehlungen. Eine Pflicht zur regelmäßigen Anpassung der Verfahren und Komponenten an den technologischen Fortschritt ist nicht ausdrücklich genannt. Auch finden sich keine vorgeschriebenen Angaben zum praktischen Verfahrensablauf der Signierung, die eine Warnfunktion etc. übernehmen könnten. Die Anforderungen an die Identitätsprüfung des Zertifikatsinhabers (beziehungsweise des Antragsstellers) sind ungenügend. Die Regelungen für die technisch-organisatorischen Anforderungen in den Anhängen enthalten keine Rechtsfolgerege-

[579] Art. 7 Abs. 1 lit. a), b), c).

[580] Blum, K&R 2000, S. 70.

[581] Darstellung der Umsetzung in den Mitgliedsstaaten siehe bei Mason, *Electronic Signatures in Law*, S. 247-249.

[582] Erwägungsgrund 21 RLeS.

[583] Art. 4 Abs. 1 S. 1 RLeS.

[584] Erwägungsgrund 13.

[585] Art. 9 Abs. 1 und Art. 10 RLeS. Gemeint sind Anforderungen qualifizierte Zertifikate, an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, und an sichere Signaturerstellungseinheiten, Anhänge I bis III RLeS, sowie Kriterien anhand derer die Mitgliedstaaten bestimmen, ob eine Überprüfungsstelle zum Verfahren nach Art. 3 Abs. 3 und 4 S. 1 RLeS geeignet ist, Art. 3 Abs. 4 S. 2 RLeS. Soweit ein Produkt diesen Normen entspricht können die Mitgliedstaaten davon ausgehen, dass es den Anforderungen des Anhangs II lit. f) und des Anhangs III entspricht, Art. 3 Abs. 5 S. 2 RLeS. Solche Verfahren werden Komitologieverfahren genannt. Der Ausschuss ist aus Vertretern der Mitgliedstaaten zusammengesetzt. Siehe bei Roßnagel, K&R 2000, S. 317.

lung. Die RLeS verzichtet auf eine Haftungsregelung für die Einhaltung aller in den Anhängen aufgeführten Anforderungen. Das bedeutet grundsätzlich eine Verschlechterung der Durchsetzungschancen für die Sicherheitsanforderungen.[586]
Rechtsfolgen sind nur für die niedrigste und die höchste Form der Kombinationsmöglichkeiten, die fortgeschrittene elektronische Signatur auf Grundlage eines qualifizierten Zertifikats, erstellt mittels sicherer Signaturerstellungsprodukte, festgelegt. Letztere soll gleichwertig sein mit der eigenhändig unterzeichneten papiernen Urkunde. Möglich ist dies, neben den diesbezüglichen zwingenden technisch-organisatorischen Anforderungen, aufgrund und im Falle der möglichen freiwilligen Vorabprüfung der Einhaltung dieser Anforderungen durch den Zertifizierungsdiensteanbieter und seiner Verfahren und Produkte im Rahmen der freiwilligen Akkreditierung. Teilweise wurde aber bezweifelt, ob das Konzept der EU, die Gründung von Zertifizierungsstellen durch Private und ohne vorherige Lizenzierung zu erlauben und diese nur indirekt über die Haftung für Fehler zur Verantwortung zu ziehen, tatsächlich Vertrauen begründen würde.[587] Der Verzicht auf eine Sicherheitsvermutung, selbst für die fortgeschrittenen elektronischen Signaturen auf Grundlage qualifizierter Zertifikate, ist zwar konsequent, da diese nur bei einer solchen Vorabprüfung der Sicherheit möglich ist. Grundsätzlich stellt dies jedoch ein praktisches Handicap für die Signaturverfahren nach der RLeS dar.[588] Trotz einer Beweislastregelung zu Lasten des Diensteanbieters besteht zudem die Informationsasymmetrie zwischen Diensteanbieter, Nutzer und Drittem fort. Beweiskraftregeln, Beweisvermutungen oder -erleichterungen werden nicht eingeführt. Die Harmonisierung entsprechender nationaler Vorschriften ist nicht bezweckt. An zahlreichen Stellen bleibt die konkrete Ausfüllung der Vorschriften der der RLeS Rechtsprechung vorbehalten und bestehende Unsicherheiten werden gerade nicht beseitigt.[589] Aufgrund der Orientierung an der PKI ist nur die bekannte und bereits eingeführte Technologie der digitalen Signatur rechtlich ausgestaltet.[590] Für zukünftige neue Verfahren müssten neue Regelungen geschaffen werden, ebenso für viele weitere Anwendungsbereiche der digitalen Signatur-Technik. Aufgrund dieser PKI-Orientierung übt die RLeS eine restriktive Wirkung auf andere Signaturtechnologien aus.[591]
Die EU-Richtlinien beschränken sich insgesamt auf einige wenige grundlegende Bereiche einer rechtlichen Einrahmung elektronischer Signaturen. Die Regeln der RLeS zum Tatbestand der elektronischen Signatur bedürften der Konkretisierung durch die Mitgliedstaaten.[592] Den Mitgliedstaaten ist ein Freiraum bei der Bestimmung der vom elektronischen Vertragsschluss ausgeschlossenen Rechtsgeschäfte und bei der Ausgestal-

[586] So zutreffend Neuser, MMR 1999, S. 70.

[587] Denn danach können Zertifizierungsstellen beispielsweise allein durch die Wahl ihrer Rechtsform ihr Haftungsrisiko begrenzen. Hoeren, ECLIP, Teil 1, Kap.1, S. 10.

[588] So zutreffend Roßnagel, K&R 2000, S. 318; a.A. Müglich, MMR 2000, S. 13.

[589] Zutreffend Müglich, MMR 2000, S. 13; Roßnagel, K&R 2000, S. 317, 323..

[590] Siehe auch Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 109.

[591] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 109; Gravesen/Dumortier/van Eecke, MMR 1999, S. 578. Für zukünftige andere Technologien und für viele weitere Anwendungsgebiete müssen daher neue, spezifische Standards und Anforderungen formuliert werden; Hoeren, *Grundzüge des Internetrechts*, S. 195; Roßnagel, K&R 2000, S. 317.

[592] Siehe Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 102-104, 109.

tung der Formvorschriften belassen. Zahlreiche unbestimmte Rechtsbegriffe und die erstrebte Technologieneutralität lassen Raum für unterschiedliche Interpretationen divergierende Anforderungen an Signaturverfahren.[593] Sie wurden daher teilweise als insgesamt nicht weit reichend beurteilt.[594]

[593] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 109.

[594] Z.B. Moritz, CR 2000, S. 72; Rennie, CLRT 1999, S. 242.

2.3 Signaturgesetz und Änderungen der Formvorschriften in Deutschland

Vor dem Hintergrund der oben dargestellten Rechts- und Gesetzeslage in Bezug auf Formerfordernisse[595] war es bereits früh Ziel des deutschen Gesetzgebers, einen rechtlichen Rahmen für die Verwendung digitaler Signaturen zu schaffen. Formfreien Willenserklärungen in Form elektronischer Dateien und Dokumente sollte so zu einer gewissen abgesicherten Beweiskraft verholfen werden.[596] Eine Änderung der Formvorschriften, um elektronischen Dokumenten die Möglichkeit zu eröffnen, gesetzliche Formerfordernisse, insbesondere das der Schriftform, zu erfüllen, erfolgte zunächst jedoch nicht.

2.3.1 Das Signaturgesetz von 1997

Vor der Verabschiedung von RLeC und RLeS hatte der deutsche Gesetzgeber 1997 das Informations- und Kommunikationsdienstegesetz[597] erlassen. Es umfasste unter anderem das Gesetz zur digitalen Signatur.[598] Hier sollen einige Merkmale des SigG a.F. kurz dargestellt werden, um das ursprüngliche Regelungskonzept zu verdeutlichen.
Der rechtliche Rahmen für digitale Signaturen im SigG a.F. beschränkte sich auf den administrativen Rahmen für die digitale Signatur. Es enthielt keine materiellen Regelungen[599], berührte nicht die Formerfordernisse des BGB und sollte auch keine rechtliche Gleichstellung von digitaler Signatur und eigenhändiger Unterschrift bewirken. Zweck des SigG a.F. war es gemäß § 1 Abs. 1:

> *„… Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können."*

Schon durch die Begriffsbestimmungen zeigt sich, dass der Anwendungsbereich des SigG a.F. beschränkter war als derjenige der RLeS. So sprach das SigG a.F. ausschließlich von digitalen, nicht von elektronischen Signaturen. Das SigG a.F. war auf eine einzige Technologie zugeschnitten. Als gesetzliche digitale Signatur war diejenige der PKI bestimmt[600], jedoch enger als der Begriff der elektronischen Signatur der RLeS.[601] Da-

---

[595] Siehe 1.3.1.

[596] Scheffler/Dressel, CR 2000, S. 379.

[597] Informations- und Kommunikationsdienstegesetz (IuKdG) vom 22.7.1997 (in Kraft seit 1.8.1997), BGBl. I, S. 180.

[598] Gesetz zur digitalen Signatur (Signaturgesetz) vom 22. Juli 1997 (BGBl. I S. 1870). Es wird nachfolgend SigG a.F. abgekürzt. Eine Zusammenfassung zu IuKdG und SigG a.F. bei: Köhler/Arndt, *Recht des Internet*, Heidelberg 2003, S. 47ff.; Schumacher, CR 1998, S. 759. Ausführliche Darstellung der Gesetzgebung bei Köhler/Arndt, S. 60, und Jansen, ICCLR 1999, S. 39.

[599] Müglich, „Neue Formvorschriften für den E-Commerce – Zur Umsetzung der EU-Signaturrichtlinie in deutsches Recht", MMR 2000, S. 7-13, S. 8; Schumacher, CR 1998, S. 759.

[600] Chissick, S. 83; Schumacher, CR 1998, S. 759.

[601] Schumacher, CR 1998, S. 760.

bei blieb sie auf die Nutzung durch natürliche Personen zum Zwecke der Authentifizierung beschränkt.[602] Eine Abstufung digitaler Signaturen nach ihrer Qualität und Sicherheit oder eine Diversifizierung der Zertifikate[603] nach deren Qualität erfolgte nicht. Die faktische Sicherheit digitaler Signaturen sollte durch fünf ineinander greifende Regelungselemente gewährleistet werden: Geprüfte Zertifizierungsstellen, eingebunden in eine einfache und klare Zertifizierungsstruktur, sollten alle erforderlichen Sicherheitsdienstleistungen anbieten, nur geprüfte technische Komponenten verwenden und überwacht werden von einer Kontrollinfrastruktur.[604] Wesentliche Merkmale des Regelungskonzepts waren folglich die Genehmigungspflicht der Zertifizierungsstellen, deren Einbindung in eine Zertifizierungsstruktur mit einer Wurzelzertifizierungsinstanz[605] sowie die Feststellung der Anforderungen an die Sicherheitsinfrastruktur. Die Genehmigung wurde erteilt, wenn die Zertifizierungsstelle die erforderliche Zuverlässigkeit besaß, fachkundiges Personal einsetzte und die technisch-organisatorischen Sicherheitsanforderungen des SigG erfüllte.[606] Um die organisatorische Sicherheit zu gewährleisten, mussten die Zertifizierungsstellen zum Beispiel für eine korrekte Schlüsselerzeugung sorgen, den Antragsteller für ein Zertifikat zuverlässig identifizieren, die Zuordnung zu seinem öffentlichen Schlüssel per Zertifikat bestätigen, ihn über Sicherungsmaßnahmen und anderes unterrichten, das Zertifikat in einen öffentlich zugänglichen Verzeichnisdienst aufnehmen, einen Sperrdienst unterhalten und Zeitstempel anbieten.[607] Um die technische Sicherheit zu gewährleisten, durfte sie nur geprüfte technische Komponenten einsetzen, die über Sicherheitsvorkehrungen insbesondere gegen Verfälschungen verfügen.[608] Die Kontrolle der Erfüllung dieser Verpflichtungen oblag der damaligen Regulierungsbehörde.[609] Da nur Grundzüge der technisch-

[602] § 2 SigG a.F. liest sich wie eine kurze Funktionserklärung der Signaturtechnik der digitalen Signatur. Abs. 1: *„Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüsseln erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle... versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt."* Siehe auch Dumortier/van Eecke, CLSR 1999, S. 108.

[603] § 2 Abs. 2 SigG a.F.: *"Eine Zertifizierungsstelle… ist eine natürliche oder juristische Person, die die Zuordnung von öffentlichen Signaturschlüsseln zu natürlichen Personen bescheinigt..."* § 2 Abs. 3 SigG a.F.: *„Ein Zertifikat… ist eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person..."* Diesbezüglich spricht das SigG a.F. von Signaturschlüssel-Zertifikat, neben dem es noch das so genannte Attribut-Zertifikat, Abs. 3 2. HS, gab.

[604] Roßnagel, K&R 2000, S. 314.

[605] Die Zertifizierungsstellen bedurften zur Aufnahme ihrer Tätigkeit einer Genehmigung der damaligen Regulierunsgbehörde für Telekommunikation und Post (heute Bundesnetzagentur, siehe 2.3.1) als zuständige Behörde im Sinne des SigG a.F., welches auf § 66 Telekommunikationsgesetz (TKG) verwies.

[606] § 2 Abs. 2 a.E. SigG a.F. und § 4 Abs. 1: *„Der Betrieb einer Zertifizierungsstelle bedarf einer Genehmigung ... Diese ist auf Antrag zu erteilen."* Genehmigungsverfahren und Anforderungen an die Zertifizierungsstelle waren in den Absätzen 2 bis 5 geregelt.

[607] § 5 Abs. 1 und § 6 SigG a.F. Siehe auch Nöcker, CR 2000, S. 179; Roßnagel, K&R 2000, S. 314.

[608] § 14 SigG a.F.

[609] §§ 3 und 13 SigG a.F. i.V.m. § 66 TKG.

organisatorischen Anforderungen geregelt waren, wurde mit der Signaturverordnung ein gesetzeskonkretisierender Unterbau normativer Regelungen geschaffen.[610]
Sofern alle technisch-organisatorischen Anforderungen erfüllt wurden, galt eine so erstellte digitale Signatur gemäß § 1 Abs. 1 SigG a.F. als sicher. Die gewerbe- und technikrechtlichen Rahmenbedingungen für die Sicherungsinfrastruktur waren allerdings nicht verbindlich, die Anwendung anderer Verfahren war freigestellt, so dass auch solche Signaturverfahren angeboten werden konnten, die nicht die hohen Anforderungen des Gesetzes erfüllten, dann aber auf die Sicherheitsvermutung des § 1 Abs. 1 SigG a.F. verzichteten.[611] Tatsächlich war und ist der Beweisantritt mit digitalen Signaturen grundsätzlich schwierig bis unmöglich oder, insbesondere unter Zuhilfenahme von Sachverständigen, sehr aufwendig und kostspielig. Im Rahmen der gerichtlichen Überprüfung musste die Sicherheit eines Signaturverfahrens im Einzelfall jeweils neu festgestellt werden. Das SigG a.F. schuf hier eine wesentliche Erleichterung mit der Sicherheitsvermutung des § 1 Abs. 1 SigG[612], einer *„versteckten aber ausreichenden*“ Beweisregelung[613] aufgrund der Vorabprüfung im Genehmigungsverfahren.[614]
Auf spezielle Haftungstatbestände verzichtete das SigG a.F. Aufgrund der Anwendbarkeit der allgemeinen deliktsrechtlichen Vorschriften war die Haftung der Zertifizierungsstellen eine Verschuldenshaftung, wobei einzelne Regelungen des SigG a.F.

[610] Am 1.11.1997 trat die in § 16 SigG a.F. vorgesehene Signaturverordnung (SigV, hier SigV a.F.) in Kraft, am 30.10.1998 wurden Maßnahmenkataloge für Zertifizierungsstellen und technische Komponenten veröffentlicht. Siehe Roßnagel, K&R 2000, S. 315; Schumacher, CR 1998, S. 759. Der deutsche Gesetzgeber bedient sich damit zur weiteren Spezifizierung der Rechte und Pflichten der Beteiligten sowie der technisch-organisatorischen Voraussetzungen der Möglichkeit des Erlasses einer Rechtsverordnung durch die Bundesregierung. Eine Rechtsverordnung ist eine allgemein verbindliche Anordnung, die nicht im förmlichen Gesetzgebungsverfahren ergeht, sondern von Organen der vollziehenden Gewalt gesetzt wird. Die Art des Zustandekommens unterscheidet die Rechtsverordnung vom formellen Gesetz. Da sie Rechtsnormen enthält, ist sie jedoch Gesetz im materiellen Sinn. Ein formelles Gesetz (wie das SigG) kann die vollziehende Gewalt zum Erlass von Rechtsverordnungen ermächtigen, Art. 80 Grundgesetz (GG). Rechtsverordnungen dürfen nur zur Durchführung und zur inhaltlich bereits vorgezeichneten Ausfüllung und Ergänzung des formellen Gesetzes ergehen. Sie haben große Bedeutung erlangt, weil es den zeitraubenden Weg der Gesetzgebung erspart und schnellere Anpassung der Rechtslage an veränderte Verhältnisse ermöglicht. Aus Creifelds/Kaufmann, *Rechtswörterbuch*, München 1992. Siehe zum Vergleich die Rechtsform der Neuregelungen in England (unten 2.4.2.4). In Deutschland ist so ein nicht bindender Standard festgeschrieben worden, allerdings über Prozeduren, die normalerweise dem Gesetzgebungsverfahren vorbehalten sind. Dem oben (1.4.2.6) beschriebenen Zusammenhang von Standards und rechtlichen Vorschriften hat das SigG *„eine neue Dimension hinzugefügt“; s*o Dumortier/van Eecke, CLSR 1999, S. 108. Es wird eingewandt, dass zu sehr belastenden technischen Spezifikationen des SigG als Sicherheitsstandard das Risiko der Markterdrückung anhaftet. Andererseits sei eine detaillierte Beschreibung typisch ist für technische Standards. Insgesamt wird der gesamte Prozess beschleunigt, größerer Einfluss und eine größere Wirkung erzielt. Allerdings trüge die erst nachfolgende detaillierte Ausgestaltung das das Risiko der Auslassung bestimmter Aspekte in sich. Darstellung bei Dumortier/van Eecke, a.a.O.

[611] § 1 Abs. 2 SigG a.F.; Roßnagel, K&R 2000, S. 314

[612] Roßnagel, K&R 2000, S. 318

[613] So zutreffend Schumacher, CR 1998, S. 759.

[614] Die Sicherstellung der Erfüllung aller Voraussetzungen ermöglichte es, die digitale Signatur nach dem SigG als fälschungssicher einzustufen und digital signierte Daten in praktikabler Weise als Beweismittel zu verwenden. So Roßnagel, K&R 2000, S. 315

Schutzgesetzcharakter hatten.[615] Ausländische Zertifikate wurden nur anerkannt, wenn diese aus Mitgliedstaaten der EU oder anderen Vertragsstaaten des Europäischen Wirtschaftsraums stammten und nur, wenn sie eine gleichwertige Sicherheit boten, im Ausstellungsland also vergleichbare Sicherheitsvorschriften vorlagen.[616]

2.3.2 Umsetzungsbedarf hinsichtlich der EU-Richtlinien

Auch nach Einführung des SigG a.F. war es umstritten, ob die rechtliche Gleichwertigkeit zwischen digitaler Signatur und eigenhändiger Unterschrift bereits gegeben war und ob diese noch gesetzlich festgestellt werden sollte, etwa durch eine Beweiskraftregel. Nach einer Ansicht entsprach die prozessuale Beweiskraft digitaler Dokumente derjenigen unterschriebener Privaturkunden – auch bei der freien Beweiswürdigung nach § 286 Abs. 1 ZPO. Unter Umständen hätten sie sogar einen höheren Beweiswert, der allein auf der faktischen Fälschungssicherheit beruhe und nicht auf einer gesetzlichen Regelung. Folglich sei Funktionsgleichheit gegeben und es bedürfe keiner Gesetzesänderung durch Einführung einer separaten Beweisvorschrift.[617] Der deutsche Gesetzgeber hatte bei Verabschiedung des SigG a.F. keine Notwendigkeit für eine Gleichstellung von digitaler Signatur und eigenhändiger Unterschrift gesehen.[618] Dadurch waren weite Anwendungsbereiche ausgeschlossen. Nach wie vor war auch mit der digitalen Signatur nach dem SigG a.F. ein digitales Ausweisen dort nicht möglich, wo das Original eines Dokuments präsentiert werden musste. Mangels Originalität konnte eine Kopie inklusive einer digitalen Signatur oder eines digitalen Zeitstempels weder die Legitimations- noch die Liberationsfunktion erfüllen, mangels schriftlicher Verkörperung auch keine Rechte verkörpern oder die Wertpapierfunktion übernehmen.[619] Dies wurde erst durch die später erfolgten Änderungen der Formvorschriften und weiterer

[615] Die Haftung der Zertifizierungsdiensteanbieter erfolgte über das Rechtsinstitut des Vertrags zu Gunsten Dritter oder über § 823 Abs. 2 BGB. Siehe Geis, MMR 2000, S. 671 und Neuser, MMR 1999, S. 72.

[616] Digitale Signaturen anderer Staaten benötigten für ihre Wirksamkeit überstaatliche oder zwischenstaatliche Vereinbarungen, was beispielsweise bei US-Bundesstaaten nicht gegeben war, § 14 SigG a.F. Siehe auch Jansen, ICCLR 1999, S. 40; Schumacher, CR 1998, S. 760.

[617] Die digitale Signatur sei fälschungssicherer als die handschriftliche und erfülle auch die Warnfunktion. Die Richtigkeit und Vollständigkeit eines so signierten Textes stünde bereits fest. Eine andere Meinung lehnte eine der eigenhändigen Unterschrift vergleichbare Behandlung der elektronischen Signatur ab, da diese eine relativ unbekannte Größe sei. Eine weitere Meinung verneinte die Notwendigkeit eines eigenen gesetzlichen „elektronischen Dokumentenbeweises“ und einer Anpassung der ZPO mit dem Hinweis auf die Sicherheitsvermutung des § 1 Abs. 1 SigG. Diese biete eine vergleichbare Rechtssicherheit wie der Urkundsbeweis. Die herrschende Meinung in der Literatur hielt einen Bruch mit dem „überkommenen“ Urkundsbegriff nicht für notwendig, da die digitale Signatur im Einzelfall als gleichwertiges Beweismittel des Augenscheins diene, §§ 371 ff. ZPO. So auch Roßnagel, K&R 2000, S. 315 und Müglich, MMR 2000, S. 12. Siehe ausführliche Darstellung bei Dumortier/van Eecke, CLSR 1999, S. 109, 110 m.w.N., Fringuelli/Wallhäuser, CR 1999, S. 97, 100, m.w.N. und Nöcker, S. 181.

[618] Dies wurde mit mangelnden Erfahrungen mit der digitalen Signatur begründet, jedoch bestritten wegen der langen Existenz nicht lizenzierter digitaler Signaturen. Schumacher, CR 1998, S. 759, 760 m.w.N.

[619] Nöcker, CR 2000, S. 181.

gesetzlicher Regelungen im Zivilrecht und den Prozessordnungen[620] möglich. Das Fehlen materieller Regelungen wurde damals als Hemmschuh für die Entwicklung des E-Commerce kritisiert, ebenso die Exklusivität einer bestimmten Technik, die die marktorientierte Innovationsfreiheit behindere.[621] Daneben existierten die oben bereits benannten Probleme bezüglich einfacher elektronischer Signaturen und elektronischer Dokumente.[622]

Änderungsbedarf ergab sich vor allem aus der Verabschiedung von RLeS und RLeC. Neben vielen Abweichungen im Einzelnen, fanden sich bei RLeS und SigG a.F. in wesentlichen Punkten divergierende Regelungsansätze, auch wenn Vorstellungen des deutschen Gesetzgebers deutlichen Einfluss auf die Ausgestaltung von RLeC und RLeS genommen hatten. Eine der Folgen des deutschen Einflusses ist die Regelung der RLeS zur freiwilligen Akkreditierung, die allein auf das Genehmigungsverfahren des deutschen SigG bezogen ist, welches als einziges Signaturgesetz in den EU-Mitgliedstaat eine solche Vorabprüfung von Zertifizierungsstellen etabliert hatte.[623] Unterschiede im Regelungskonzept bestanden auch bezüglich der technischen Verfahren und der Haftung der Zertifizierungsstellen.[624] Andererseits hatte das SigG insbesondere hinsichtlich der von den Zertifzierungsdiensteanbietern zu erfüllenden Voraussetzungen hohe Standards gesetzt.[625] Im Übrigen ging die RLeS mit ihrer elektronischen Signatur weiter als das deutsche SigG a.F. indem sie technikoffener ist und insbesondere eine Rechtsfolgeregelung beinhaltete.[626] Wie *Schumacher* richtig anmerkt sind Regelungen über die digitale Signatur letztlich Sicherheitsstandards, die nur dann Sinn machen, wenn auch gleichzeitig Rechtsfolgen geregelt werden.[627] Dies nachzuholen war die Hauptaufgabe bei der Novellierung des SigG. Die Formwirksamkeit elektronischer Erklärungen ohne gesetzliche Neuregelungen anzuerkennen, war nicht möglich. Die allgemein geltenden gesetzlichen Bestimmungen für die gesetzlichen Formvorschriften mussten geändert werden.[628] Zudem war die Gesetzeslage zu Formvorschriften und ihrem Verhältnis zur elektronischen beziehungsweise digitalen Signatur aufgrund der Vielzahl von Ausnahmeregelungen geprägt durch eine Zersplitterung dieser Vorschriften. Ausnahmerege-

[620] Siehe nachfolgend unter 2.3.4.

[621] Siehe bei Schumacher, CR 1998, S. 759/760; Gravesen/Dumortier/van Eecke, MMR 1999, S. 577 ff., a.A. Noack in Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 7.

[622] Siehe unter 1.3.1.4.

[623] Art. 2 Abs. 2 RLeS sollte es ermöglichen, den Regelungsansatz des SigG fortzuführen; Hoeren. ECLIP, Teil 1, Kap. 1, S. 10; Roßnagel, K&R 2000, S. 319.

[624] So musste die Haftung der Zertifzierungsstellen nach allgemeinem Recht nun in eine Haftung aufgrund vermuteten Verschuldens mit der Möglichkeit der Exkulpation geändert werden; Geis, MMR 2000, S. 671; Müglich, MMR 2000, S. 8; Neuser, MMR 1999, S. 68, 71.

[625] Hoeren, ECLIP, Teil 1, Kap.1, S. 10.

[626] Art. 5 Abs. 2 RLeS. Müglich, MMR 2000, S. 8; Schumacher, CR 1998, S. 760/761.

[627] Schumacher, CR 1998, S. 760/761.

[628] Fringuelli/Wallhäuser, CR 1999, S. 99. In Anbetracht des geschilderten Meinungsstreits zur rechtlichen Wirksamkeit und Gleichstellung elektronischer Signaturen war herrschende Meinung, dass eine rechtliche Neubewertung dem Gesetzgeber überlassen bleiben sollte; Siehe dieselben, CR 1999, S. 97, die dort äußern: *„Bei den gesetzlichen Formerfordernissen ist die Grenze erreicht, an der der Ruf nach dem Gesetzgeber gerechtfertigt ist."*

lungen zu den Formerfordernissen fanden sich nicht nur in einzelnen Vorschriften des BGB, sondern auch in weiteren Gesetzeswerken, was deren Überschaubarkeit und Handhabung zunehmend erschwerte.[629] Die mit der Verabschiedung des IuKdG eingeleitete Entwicklung wurde daher zunächst weitergeführt durch das Inkrafttreten des Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz)[630], insbesondere aber mit dem Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz, SigG)[631], dem Gesetz zur Anpassung des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr (Formvorschriftenänderungsgesetz)[632] und später dem Ersten Gesetzes zur Änderung des Signaturgesetzes (Signaturänderungsgesetz)[633] und dem Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz)[634]. Die Änderungen des Signaturgesetzes und der gesetzlichen Formvorschriften stellen dabei eine Mischung aus Regelungselementen der EU-Richtlinien und des zuvor bestehenden SigG a.F. dar.

2.3.3 Das Signaturgesetz von 2001

Das SigG wurde der RLeS über weite Teile angeglichen und erfüllt deren Umsetzungsauftrag vollumfänglich. Viele Begrifflichkeiten und Definitionen wurden angeglichen. Insbesondere wurde das Regelungskonzept der lizensierungsfreien Tätigkeit der Zertifizierungsdiensteanbieter eingeführt. Dabei wurden jedoch viele aus dem Genehmigungsverfahren des SigG a.F. stammenden Anforderungen übernommen.

2.3.3.1 Anwendungsbereich und Begriffsbestimmungen

Die wesentlichen Begrifflichkeiten und Ziele des SigG entsprechen nun denen der RLeS.[635] Das SigG unterscheidet ebenfalls zwischen (einfacher) elektronischer und

[629] Ausführlich Vehslage, DB 2000, S. 1801.

[630] Text entnommen dem „Entwurf eines Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr“ (im Folgenden EGG abgekürzt) vom 17. Mai 2001, BT-Drucks. 14/6098. Eine ausführliche Auflistung zum Umsetzungsbedarf aufgrund der RLeC ist in der Begründung zum EGG, S.12 ff. enthalten.

[631] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001, BGBl. I Nr. 22, S.876, vom 21.05.2001, BT-Drucks. 14/4662 vom 16. 11.2001. Das so genannte Signaturgesetz (neuer Fassung) wird nachfolgend – in Abgrenzung zum Signaturgesetz alter Fassung (SigG a.F.) - als SigG abgekürzt.

[632] Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom13.7.2001, BGBl. I S. 1542 ff.

[633] Erstes Gesetzes zur Änderung des Signaturgesetzes, im Folgenden 1. SigÄndG abgekürzt, vom 4.1.2005, BGBl. I, S. 2

[634] Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz, im Folgenden JKomG abgekürzt, vom 22.3.2005, in Kraft seit 1.4.2005, BGBl. I, S. 837.

[635] Siehe § 1 Abs. 1 SigG: Das SigG bezieht sich nun auf elektronische Signaturen, nicht mehr auf digitale Signaturen. Auch fehlt die Sicherheitsvermutung des § 1 Abs. 1 SigG a.F – § 15 Abs. 1 S. 4 SigG.

fortgeschrittener elektronischer Signatur, die ebenso wie der Begriff des Zertifikats gemäß der RLeS definiert wurden.[636] Der Begriff Zertifizierungsstelle wurde durch Zertifizierungsdiensteanbieter aus Art. 2 Nr. 11 RLeS ersetzt.[637] Auch qualifizierte Zertifikate werden im SigG vergleichbar wie in der RLeS definiert.[638] Daneben führt das SigG aber noch eine weitere begriffliche Differenzierung ein. Qualifizierte elektronische Signaturen i.S.d. § 2 Nr. 3 SigG entsprechen, in gleicher Definition, den fortgeschrittenen elektronischen Signaturen der RLeS, die entsprechend Art. 5 Abs. 1 RLeS auf einem qualifizierten Zertifikat beruhen und von einer sicheren Signaturerstellungseinheit erstellt werden.[639] Anstatt von Signaturerstellungs- und Signaturprüfdaten spricht das SigG von Signaturschlüssel und Signaturprüfschlüssel, definiert diese aber wie die RLeS.[640] Der Begriff der sicheren Signaturerstellungseinheit ist in SigG und RLeS identisch, § 2 Nr. 10 SigG verweist dabei aber auf Anforderungen, die mit denen des Anhang III RLeS nicht völlig übereinstimmen.[641] Leicht unterscheiden sich die Definitionen des Unterzeichners in der RLeS, den es so im SigG nicht gibt, und des Signaturschlüssel-Inhabers.[642] Ferner definiert das SigG die Begriffe Signaturanwendungskomponenten, technische Komponenten für Zertifizierungsdienste, Produkte für qualifizierte elektronische Signaturen sowie den qualifizierten Zeitstempel[643] und die freiwillige Akkreditierung[644], was in der RLeS nicht oder anders geschieht. Die Definition der technischen Komponenten für Zertifizierungsdienste im SigG entspricht ungefähr derjenigen der Produkte für elektronische Signaturen aus der RLeS.[645] Signaturanwen-

[636] Art. 2 Nr. 1 und Nr. 2 lit. a) bis d) sowie Art. 2 Nr. 9 RLeS. Auch hier wird der Bereich der elektronische Signatur-Technologie verwendet, der sich mit demjenigen der digitalen Signatur überlappt. Dumortier/van Eecke, CLSR 1999, S. 107. Auch eine automatisiert erstellte elektronische Signatur erfüllt die Anforderungen des § 2 Nr. 1 SigG, siehe hierzu ausführlich Roßnagel/Fischer-Dieskau, „Automatisiert erzeugte elektronische Signaturen", MMR 2004, S. 133-139.

[637] Wobei dieser nach § 2 Nr. 8 SigG nun ausschließlich Zeitstempel neben den Zertifkaten ausstellt.

[638] Qualifizierte Zertifikate sind gemäß § 2 Nr. 7 SigG solche Zertifikate, *„... die die Voraussetzungen des § 7* [über den Inhalt von qualifizierten Zertifikaten] *erfüllen und von Zertifizierungsdiensteanbietern ausgestellt werden, die mindestens die Anforderungen nach den §§ 4 bis 14* [Allgemeine Anforderungen und Pflichten und Haftung der Zertifizierungsdiensteanbieter]*... und der Vorschriften der* [SigV] *erfüllen."*

[639] § 2 Nr. 3 SigG. Die fortgeschrittene elektronische Signatur gem. § 2 Nr. 2 SigG stellt also eine geminderte Stufe der Signatur dar, an die keine Rechtsfolgen geknüpft sind; siehe bei Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 37.

[640] § 2 Nr. 4 und 5 SigG.

[641] § 2 Nr. 10 SigG bezieht sich auf die Anforderungen des § 17 SigG.

[642] Letzterer ist gemäß § 2 Nr. 9 SigG, wer die Signaturschlüssel besitzt. Nach Änderung des § 2 Nr. 9 SigG durch Art. 1 des 1. SigÄndG ist nun bestimmt, dass bei qualifizierten elektronischen Signaturen dem Signaturschlüssel-Inhaber die zugehörigen Signaturprüfschlüssel durch ein qualifiziertes Zertifikat zugeordnet sein müssen.

[643] Ein qualifizierter Zeitstempel wird gemäß § 2 Nr. 14 SigG definiert als *„elektronische Bescheinigung eines Zertifizierungsdiensteanbieters, der* [die gleichen Voraussetzungen erfüllt wie derjenige, der qualifizierte Zertifikate ausstellt]*, darüber, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben."*

[644] Die Definition in § 2 Nr. 15 SigG ist nur im ersten Halbsatz ähnlich der des Art. 2 Nr. 13 RLeS. Freiwillige Akkreditierung stellt nach dem SigG lapidar ein *„Verfahren zur Erteilung einer Erlaubnis für den Betrieb eines Zertifizierungsdienstes* [dar]*, mit der besondere Rechte und Pflichten verbunden sind."*

[645] § 2 Nr. 12 SigG: *„Software- oder Hardwareprodukte, die dazu bestimmt sind, a) Signaturschlüssel zu erzeugen und in eine sichere Signaturerstellungseinheit zu übertragen, b) qualifizierte Zertifikate öf-*

dungskomponenten definiert § 2 Nr. 11 SigG als Software- und Hardwareprodukte, die dazu bestimmt sind,

> *„a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder*
>
> *b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen.“*

2.3.3.2 Zertifizierungsstruktur

Die Zertifizierungsstruktur mit der Bundesnetzagentur[646] als Regulierungsbehörde und Wurzelzertifizierungsinstanz aus dem SigG a.F. wurde beibehalten. Dies ergibt sich aus § 3 SigG, aber auch aus den in sonstigen Aufgaben der Bundesnetzagentur als zuständige Behörde.[647] Ihr werden durch die Zertifizierungsdiensteanbieter die Maßnahmen zur Erfüllung der Sicherheitsanforderungen in einem Sicherheitskonzept sowie deren Erfüllung angezeigt.[648] Die Bundesnetzagentur stellt die (qualifizierten) Zertifikate für die Zertifizierungsdiensteanbieter aus, wobei für sie die Anforderungen hinsichtlich der Ausstellung von qualifizierten Zertifikaten entsprechend gelten.[649] Sie muss die Namen der angezeigten Zertifizierungsdiensteanbieter und derer, die ihre Tätigkeit eingestellt haben oder denen der Betrieb untersagt wurde, sowie mögliche Widerrufe einer Akkreditierung etc. abrufbar halten.[650] Ihr obliegt die Aufsicht über die Einhaltung der Vorschriften des SigG und der SigV.[651] Sie kann eigene Maßnahmen zur Sicherstellung deren Einhaltung treffen, Zertifikate sperren oder den Betrieb von Zertifizierungsdiensteanbietern untersagen.[652] Die Bundesnetzagentur ist insbesondere für die Akkreditierung der Zertifizierungsdiensteanbieter verantwortlich.[653] Außerdem ist sie zustän-

---

fentlich nachprüfbar und gegebenenfalls abrufbar zu halten oder c) qualifizierte Zeitstempel zu erzeugen.“ Technische Komponenten für Zertifizierunsdienste, Signaturanwendungskomponenten und sichere Signaturerstellungseinheiten sind Produkte für qualifizierte elektronische Signaturen, § 2 Nr. 13 SigG.

[646] Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen ist zuständige Behörde gemäß § 3 des SigG, siehe unter http://www.bundesnetzagentur.de/enid/544082aaae77d4ca6a62b5266848f50e,0/Sachgebiete/Elektronische_Signatur_gz.html.

[647] Aufgeführt in den §§ 4 Abs. 2 bis 4, 13, 15, 16, 17 Abs. 4, 18 Abs. 1, 19 Abs. 1 bis 4 und Abs. 6 sowie § 20 Abs. 1 SigG.

[648] § 4 Abs. 2 a.E. und Abs. 4 SigG. Ebenso wird ihr der Betrieb, die Einstellung der Tätigkeit oder die Insolvenz angezeigt, §§ 4 Abs. 3, 13 Abs. 1 und 3.

[649] § 16 Abs. 1 S. 1 und 2, § 5 SigG.

[650] §§ 19 Abs. 4, 16 Abs. 2 SigG.

[651] § 19 Abs. 1 S. 1 1. HS SigG. Nach Abs. 1 S. 1 2. HS kann sie *„sich bei der Durchführung der Aufsicht privater Stellen bedienen.“*

[652] §§ 19 Abs. 1 bis 4, 15 Abs. 6 SigG. Unter Umständen muss sie sogar dessen Tätigkeit oder dessen Dokumentation über die von diesem ausgestellten Zertifikate übernehmen. Sie kann von den Zertifizierungsdiensteanbietern zum Beispiel Auskünfte oder die Duldung einer Durchsuchung verlangen.

[653] Diese muss sie auf Antrag bei Vorliegen der Voraussetzungen erteilen, kann sie aber unter Umständen auch versagen und widerrufen oder mit Nebenbestimmungen versehen, § 15 Abs. 1, Abs. 3 bis 5 SigG. Die Bundesnetzagentur verleiht auch das „Gütezeichen“ (siehe dazu anschließend), § 15 Abs. 1 S. 3.

dig für die Ernennung der Prüf- und/oder Bestätigungsstellen.[654] Diese sind wiederum verantwortlich für die Prüfung (und eine entsprechende Bestätigung)

a) der von den Zertifizierungsdiensteanbietern, die eine Akkreditierung beantragen, vorgelegten Sicherheitskonzepte auf deren Eignung und praktische Umsetzung[655] und

(b) der Produkte für qualifizierte elektronische Signaturen auf die Erfüllung der an Signaturerstellungseinheiten, Signaturanwendungskomponenten und technische Komponenten für Zertifizierungsdienste gestellten Anforderungen.[656]

2.3.3.3 Anforderungen an Signaturverfahren und Signaturtechnik

Qualifizierten Zertifikate müssen gemäß § 7 SigG einen bestimmten Inhalt haben. Das SigG lehnt sich auch hier an die RLeS an. Die wesentlichen Vorgaben sind identisch.[657] Gemäß § 7 Abs. 1 S. 1 SigG aber muss ein qualifiziertes Zertifikat eine qualifizierte elektronische Signatur des ausstellenden Zertifizierungsdiensteanbieters tragen, gemäß der RLeS lediglich dessen fortgeschrittene elektronische Signatur.[658] Darüber hinaus muss ein qualifiziertes Zertifikat im Sinne des SigG diejenigen Algorithmen bezeichnen, mit denen der Signaturprüfschlüssel des Signaturschlüssel-Inhabers sowie der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann.[659] Sichere Signaturerstellungseinheiten, die für die Speicherung von Signaturschlüsseln und die Erzeugung qualifizierter elektronischer Signaturen eingesetzt werden, müssen mindestens die Anforderungen nach § 17 SigG und der SigV erfüllen. Danach müssen sie Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen[660], was am ehesten mit den Anforderungen aus Anhang III Nr. 1 lit. b) RLeS vergleichbar ist. Ferner müssen sie die signierten Daten gegen unberechtigte Nutzung der Signaturschlüssel schützen, was der Reglung des Anhangs III Nr. 1 lit. a) RLeS entspricht.

---

[654] § 18 Abs. 1 SigG. Diese können natürliche oder juristische Personen sein, müssen die *„für die Tätigkeit erforderliche Zuverlässigkeit, Unabhängigkeit und Fachkunde“* nachweisen und sollen unparteiisch, weisungsfrei und gewissenhaft arbeiten.

[655] Bezogen auf die allgemeinen Anforderungen des § 4 Abs. 2 S. 4, § 15 Abs. 2 S. 1 SigG. Gemäß Satz 2 ist diese Prüfung *„nach sicherheitserheblichen Veränderungen sowie in regelmäßigen Zeitabständen zu wiederholen.“*

[656] Bezogen auf die Anforderungen des § 17 Abs. 1 bis 3 SigG und der SigV. Ebenfalls im Zusammenhang mit der freiwilligen Akkreditierung des betreffenden Zertifizierungsdiensteanbieters. § 15 Abs. 2 und 7, § 17 Abs. 4 SigG.

[657] § 7 Abs. 1 Nr. 2 SigG entspricht Anhang I lit. e) RLeS, Nr. 4 entspricht inhaltlich lit. g), die Nr. 5, 6, 7 und 8 entsprechen den lit. f), b), i)/j) und a), Nr. 9 entspricht lit. d). Attribute können in ein qualifiziertes Attributs-Zertifikat aufgenommen werden, § 7 Abs. 2 SigG.

[658] Anhang I lit. h) RLeS.

[659] § 7 Abs. 1 Nr. 3 SigG.

[660] § 17 Abs. 1 S. 1 SigG.

Was in der RLeS in Anhang IV nur als Empfehlungen formuliert ist, wird im SigG als verpflichtende und haftungsbewehrte Vorschrift verfasst. § 17 Abs. 1 bis 3 SigG regeln die Voraussetzungen an die bei Erstellung und Prüfung qualifizierter elektronischer Signaturen eingesetzten Signaturerstellungseinheiten, Signaturanwendungskomponenten und der technischen Komponenten für Zertifizierungsdienste. So müssen Signaturanwendungskomponenten, also die Software, die für die Erzeugung qualifizierter elektronischer Signaturen eingesetzt wird, gewährleisten, dass sie die Erzeugung dieser Signatur eindeutig anzeigen, und ebenso, auf welche Daten diese sich bezieht,[661] was den lit. a) und b) des Anhangs IV der RLeS entspricht. Hinsichtlich der Überprüfung signierter Daten beim Einsatz einer qualifizierten elektronischen Signatur muss sich feststellen lassen, auf welche Daten sich die Signatur bezieht und welchem Signaturschlüssel-Inhaber sie zuzuordnen ist[662], entsprechend den Vorgaben des Anhang IV RLeS.[663] Ferner müssen, entsprechend den lit. c) und g) des Anhangs IV der RLeS, etwaige Veränderungen der signierten Daten und die Inhalte des qualifizierten Zertifikats feststellbar sein[664], sowie die Zuordnung eines Signaturschlüssels durch den Zertifizierungsdiensteanbieter nachvollziehbar sein.[665] Bei qualifizierten elektronischen Signaturen eingesetzte technische Komponenten für Zertifizierungsdienste müssen gemäß § 17 SigG bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel gewährleisten, Abs. 3 Nr. 1 1. HS, der wiederum mit Anhang III Nr. 1 lit. a) RLeS vergleichbar ist. Darüber hinaus müssen sie eine Speicherung außerhalb der sicheren Signaturerstellungseinheit ausschließen, Abs. 3 Nr. 1 2. HS, was so in der RLeS nicht gefordert wird. Zudem müssen sie qualifizierte Zertifikate vor unbefugter Veränderung und unbefugtem Abruf schützen, § 17 Abs. 3 Nr. 2, am ehesten vergleichbar mit Anhang II lit. l) 1. Fall RLeS, und bei der Erzeugung qualifizierter Zeitstempel Fälschungen und Verfälschungen ausschließen.[666]
Die Novellierung des SigG durch das 1. SigÄndG im Jahr 2005 betraf die Signaturanwendungskomponenten und stellte neben die Prüfung und Bestätigung durch unabhängige Stellen das Mittel der Herstellererklärung, ohne den Regelungscharakter in seinem Wesen zu berühren.[667] Zur Erfüllung der Anforderungen nach den § 17 Abs. 2 und 3 Nr. 2 und 3 genügt danach nun eine Erklärung durch den Hersteller des Produkts für qualifizierte Signaturen. Der Hersteller hat spätestens zum Zeitpunkt des Inverkehrbringens des Produkts eine Ausfertigung seiner Erklärung in schriftlicher Form bei der

[661] § 17 Abs. 2 S. 1 SigG.

[662] § 17 Abs. 2 S. 2 Nr. 1 und Nr. 3 SigG.

[663] Anhang IV lit. a) und e) RLeS.

[664] § 17 Abs. 2 S. 2 Nr. 2 und Nr. 4 SigG. Dies gilt auch für zugehörige qualifizierte Attribut-Zertifikate, § 17 Abs. 2 S. 2 Nr. 4 a.E.

[665] § 17 Abs. 2 S. 2 Nr. 5 SigG, der sich auf de Nachprüfung gemäß § 5 Abs. 1 S. 2 SigG bezieht. Des Weiteren müssen, entsprechend den Anforderungen der RLeS, diese Signaturanwendungskomponenten nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten „*hinreichend erkennen lassen*“, § 17 Abs. 2 S. 3 SigG, entsprechend Anhang IV lit. c) RLeS.

[666] § 17 Abs. 3 Nr. 3 SigG.

[667] Ausführlich Fischer-Dieskau/Steidle, „Die Herstellererklärung für Signaturanwendungskomponenten – Eine Erleichterung zur Verbreitung elektronischer Signaturen?“, MMR 2006, S. 68-73.

Bundesnetzagentur zu hinterlegen.[668] Weitere Anforderungen an die Signaturverfahren nach dem SigG sind, dass der Antragsteller im Besitz der zugehörige Signaturerstellungseinheit ist,[669] was so in der RLeS nicht gefordert wird, und dass eine Speicherung von Signaturschlüsseln außerhalb der sicheren Signaturerstellungseinheit nicht vorgenommen wird,[670] ebenfalls in der RLeS so nicht verlangt.[671]

2.3.3.4 Zertifizierungsdiensteanbieter – Haftung

§ 4 SigG stellt allgemeine Anforderungen auf, die von allen Zertifizierungsdiensteanbietern erfüllt werden müssen. Insbesondere dürfen Zertifizierungsdiensteanbieter nach Abs. 1 S. 1 einen Zertifizierungsdienst nur betreiben, wenn sie die für den Betrieb erforderliche Zuverlässigkeit und Fachkunde sowie eine Deckungsvorsorge nachweisen, wie dies auch in Anhang II RLeS[672] verlangt wird. Im Gegensatz zur RLeS werden diese Anforderungen im SigG jedoch weiter spezifiziert: Die erforderliche Zuverlässigkeit besitzt, wer die Gewähr dafür bietet, als Zertifizierungsdiensteanbieter die für den Betrieb maßgeblichen Rechtsvorschriften einzuhalten, Abs. 1 S. 2. Die erforderliche Fachkunde liegt vor, wenn die im Betrieb tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen, Abs. 1 S. 3, entsprechend lit. e) des Anhang II RLeS. Ferner muss der Zertifizierungsdiensteanbieter die weiteren Voraussetzungen des SigG und der SigV gewährleisten[673], also geeignete Maßnahmen zur Erfüllung der Sicherheitsanforderungen von SigG und SigV der Bundesnetzagentur in einem Sicherheitskonzept aufzeigen und diese auch praktisch umsetzen.[674] Die vorgenannten Voraussetzungen des § 4 Abs. 2 SigG müssen über die gesamte Zeitdauer der Tätigkeit sichergestellt werden,[675] was in der RLeS nicht verlangt wird.[676]
Sofern der Zertifizierungsdiensteanbieter qualifizierte Zertifikate ausstellt, muss er weitere Voraussetzungen und Anforderungen erfüllen. Qualifizierte Zertifikate müssen zunächst die in § 7 SigG (oben 2.3.3.3) genannten Angaben enthalten, wie es weitestge-

[668] Durch das 1. SigÄndG neu eingefügter Satz 3 des § 17 Abs. 4 SigG. Gem. Abs. 4 S. 4 werden Herstellererklärungen, die den Anforderungen der SigV entsprechen, im Amtsblatt der Bundesnetzagentur veröffentlicht.

[669] § 5 Abs. 6 SigG.

[670] § 5 Abs. 4 S. 2 SigG.

[671] §§ 10 und 19 SigG. Ferner müssen Zertifikate, Akkreditierungen und Sicherheitsmaßnahmen dokumentiert werden und es muss ein Sperrdienst bestehen, § 8 SigG.

[672] Anhang II lit. a), e) und h) RLeS. Ferner wird von ihm wie auch von der RLeS eine Deckungsvorsorge verlangt, § 12 SigG (i.H.v. 250.000,00 Euro), Anhang II lit. h) RLeS.

[673] § 4 Abs. 1 S. 1 SigG.

[674] § 4 Abs. 1 S. 4 SigG, eine Ausgestaltung des in Art. 3 RLeS geforderten Überwachungssystems.

[675] § 4 Abs. 4 SigG. Daneben müssen die Betriebsaufnahme und -einstellung sowie eine Insolvenz angezeigt, §§ 4 Abs. 3, 13 Abs. 1 S. 1 und Abs. 3 SigG, und die Sicherheitsmaßnahmen zur Einhaltung der Vorschriften von SigG und SigV dokumentiert werden, § 10 Abs. 1 SigG.

[676] Datenschutzrechtliche Vorschriften sind einzuhalten und dem Signaturschlüssel-Inhaber ist Einblick in die ihn betreffenden Daten zu gewähren, §§ 14 und 10 Abs. 2 SigG, auch in Art. 8 RLeS verlangt.

hend der RLeS entspricht.[677] Vor der Vergabe eines qualifizierten Zertifikats muss der Zertifizierungsdiensteanbieter den Antragsteller zuverlässig identifizieren, anhand des Personalausweises oder Reisepasses oder auf *„andere geeignete Weise“*, und die Zuordnung eines Signaturschlüssels zu dieser Person bestätigen.[678] Damit hat der deutsche Gesetzgeber die Identitäts- und sonstige Überprüfung der Angaben des Antragsstellers näher bestimmt als die RLeS.[679] Sicherheitsrelevante Anforderungen stellen § 5 Abs. 4 SigG. Satz 1 und 2 SigG:

> *„Der Zertifizierungsdiensteanbieter hat Vorkehrungen zu treffen, damit Daten für qualifizierte Zertifikate nicht unbemerkt gefälscht oder verfälscht werden können. Er hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der Signaturschlüssel zu gewährleisten.“*

Diese Anforderungen sind vergleichbar mit denen der lit. f), j) und insbesondere g) des Anhang II RLeS. Des Weiteren muss der Zertifizierungsdiensteanbieter zuverlässiges Personal und Produkte für qualifizierte elektronische Signaturen einsetzen[680], was Anhang II lit. e) und Anhang III RLeS entspricht. Darüber hinaus darf er die Signaturschlüssel nicht außerhalb der sicheren Signaturerstellungseinheit speichern[681] und muss sich *„in geeigneter Weise“* davon überzeugen, dass der Antragssteller im Besitz der zugehörigen Signaturerstellungseinheit ist,[682] diesen in Textform über seine Maßnahmen zur Sicherheit und zuverlässigen Prüfung sowie unter anderem darüber unterrichten,

> *„dass eine qualifizierte elektronische Signatur im Rechtsverkehr die gleiche Wirkung hat wie eine eigenhändige Unterschrift...“*.[683]

---

[677] § 7 Abs. 1 Nr. 1, 2, 4, 5, 6, 7 und 8 SigG entsprechen den lit. c), e), g), f), b), i) / j) und a) des Anhang I RLeS, wobei das SigG in Nr. 1 genauere Angaben fordert. Darüber hinaus verlangt das SigG *„die Bezeichnung der Algorithmen, mit denen der Signaturschlüssel des Signaturschlüssel-Inhabers sowie der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann“, s*owie *„nach bedarf Attribute des Signaturschlüssel-Inhabers“*, § 7 Abs. 1 Nr. 3 und 9 SigG.

[678] § 5 Abs. 1 S. 1 und 2 SigG i.V.m. § 3 Abs. 1 *SigV*.

[679] Siehe Art. 2 Nr. 9 und Anhang I lit. d) RLeS, die eine Identitätsprüfung mit geeigneten Mitteln verlangen. Bei Vertretung für einen Dritten muss der Zertifizierungsdiensteanbieter dessen Einwilligung überprüfen, berufsbezogene Angaben etc. zur Person muss er bestätigen lassen, § 5 Abs. 2 S. 2 und 3, Abs. 3 S. 2 SigG.

[680] § 4 Abs. 5 SigG. Diese müssen mindestens den Anforderungen der §§ 4 bis 14 SigG und der SigV entsprechen, § 5 Abs. 5 SigG. Anforderungen zum Personal finden sich in § 4 Abs. 2, solche zu den Produkten für qualifizierte elektronische Signaturen in § 2 Nr. 13 und damit in den Nr. 10, 11 und 12, sowie § 15 Abs. 7 SigG bezüglich der freiwilligen Akkreditierung (siehe dazu nachfolgend).

[681] § 5 Abs. 4 S. 2 SigG.

[682] § 5 Abs. 6 SigG.

[683] § 6 Abs. 1 S. 1 und Abs. 2 SigG. Die Unterrichtung ist dem Antragssteller in Textform zu übermitteln und deren Kenntnisnahme vom Antragsteller ebenfalls in Textform zu bestätigen, § 6 Abs. 3 SigG in seiner durch das 1. SigÄndG geänderten Fassung, ebenfalls nicht in der RLeS verlangt.

Letzteres ist in der RLeS ebenfalls so nicht geregelt, allenfalls in Anhang II lit. k) angedeutet. Die qualifizierten Zertifikate muss der Zertifizierungsdiensteanbieter gemäß § 10 Abs. 1 SigG so dokumentieren, dass sie jederzeit nachprüfbar aber nicht veränderbar sind, vergleichbar Anhang II lit. i) und l) RLeS. Ferner muss er wie auch nach der RLeS einen Prüfdienst sowie einen Sperrdienst vorhalten.[684] Der Signaturschlüsselinhaber seinerseits soll für die Erstellung einer qualifizierten elektronischen Signatur Signaturanwendungskomponenten einsetzen, die die Anforderungen des § 17 Abs. 2 SigG erfüllen, oder *„andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen."* Eine explizite Rechtsfolge für die Nichteinhaltung dieser Sollensvorschrift nennt das SigG nicht. Erstmals nimmt das SigG aber auch einen speziellen Haftungstatbestand hinsichtlich der Verantwortlichkeit des Zertifizierungsdiensteanbieters auf.[685] Dieser ist entsprechend der Vorgabe der RLeS[686] als Haftung aufgrund vermuteten Verschuldens mit der Möglichkeit der Exkulpation ausgestaltet. § 11 Abs. 1 S. 1 SigG:

> *„Verletzt ein Zertifizierungsdiensteanbieter die Anforderungen dieses Gesetzes oder der* [SigV] *oder versagen seine Produkte für qualifizierte elektronische Signaturen oder sonstige technische Sicherungseinrichtungen, so hat er einem Dritten den Schaden zu ersetzen, den dieser dadurch erleidet, dass er auf die Angaben in einem qualifizierten Zertifikat, einem qualifizierten Zeitstempel oder einer Auskunft nach § 5 Abs. 1 Satz 2* [über die Zuordnung eines Signaturprüfschlüssels zu einer Person] *vertraut."*

Anknüpfungspunkt ist also auch hier das schutzwürdige Vertrauen des Dritten, das nach Abs. 1 S. 2 dann nicht mehr gegeben ist, wenn der Dritte die Fehlerhaftigkeit der Angabe kannte oder kennen musste. Die Ersatzpflicht scheidet auch dann aus, wenn der Zertifizierungsdiensteanbieter nicht schuldhaft handelte, beziehungsweise ist beschränkt, sofern eine Beschränkung der Nutzung des Signaturschlüssels in das Zertifikat eingetragen war.[687] Der deutsche Gesetzgeber hat alle im SigG genannten Anforderungen in den Haftungstatbestand aufgenommen und nicht nur einzelne wenige Haftungsfälle bezeichnet, wie es die RLeS tut. Die Verantwortlichkeit des Zertifizierungsdiensteanbieters steigt also, je nach dem, ob er nur einfache Zertifikate oder qualifizierte Zertifikate ausgibt oder er sich sogar freiwillig akkreditieren lässt.

---

[684] § 5 Abs. 1 S. 2 SigG. Die Sperrung des qualifizierten Zertifikats hat zu erfolgen, wenn dies vom Signaturschlüssel-Inhaber verlangt oder sie angeordnet wird, es aufgrund falscher Angaben ausgestellt wurde, § 8 Abs. 1 S. 1 SigG, oder es nach Beendigung der Tätigkeit des Diensteanbieters nicht übernommen wird, § 13 Abs. 1 S. 2 SigG. Vergleich Anhang II lit. b) RLeS. Gem. dem durch das 1. SigÄndG neu eingefügten Satz 2 des § 8 Abs. 1 können weitere Sperrungsgründe vertraglich vereinbart werden.

[685] Siehe eine ausführliche Darstellung zu § 11 SigG bei Thomale, „Die Haftungsregelung nach § 11 SigG", MMR 2004, S. 80-86.

[686] Art. 6 RLeS.

[687] § 11 Abs. 2 und 3 SigG. Für beauftragte Dritte sowie für das Einstehen für ausländische Zertifikate haftet der Zertifizierungsdiensteanbieter wie für eigenes Verschulden, § 11 Abs. 4 SigG.

2.3.3.5 Freiwillige Akkreditierung der Zertifizierungsdiensteanbieter

Das SigG macht von der in der RLeS vorgesehenen Möglichkeit Gebrauch, freiwillige Akkreditierungssysteme einzusetzen und diese gesetzlich zu regeln. Kern der Regelung ist es, dass alle Zertifizierungsdiensteanbieter die in den §§ 4 ff. SigG aufgeführten Anforderungen erfüllen müssen. Sie erhalten darüber hinaus jedoch die Möglichkeit, ihre Zuverlässigkeit und ihr Sicherheitskonzept vorab prüfen und bestätigen zu lassen:

> *„Akkreditierte Zertifizierungsdienste erhalten ein Gütezeichen der* [Bundesnetzagentur]. *Mit diesem wird der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen (qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung) zum Ausdruck gebracht.“*
>
> *„Die Akkreditierung ist zu erteilen, wenn der Zertifizierungsdiensteanbieter nachweist, dass die Vorschriften nach dem SigG und der SigV erfüllt sind.“* [688]

Dafür muss der Zertifizierungsdiensteanbieter insbesondere die Erfüllung der Anforderungen[689] durch eine Prüf- und Bestätigungsstelle bestätigen lassen. Er darf nur die so geprüften und bestätigten Produkte verwenden[690] und auch nur für solche Personen Zertifikate ausstellen, die geprüfte und bestätigte Signaturerstellungseinheiten besitzen.[691]
Für die Rechtssicherheit der bereits in Deutschland tätigen Zertifizierungsdiensteanbieter (Zertifizierungsstellen nach SigG a.F.) war bedeutend, dass Zertifizierungsstellen, die ihre Tätigkeit noch nach dem SigG a.F. hatten genehmigen lassen, gemäß § 25 Abs. 1 SigG als akkreditiert im Sinne von § 15 SigG galten.[692] Die von diesen Zertifizierungsdiensteanbietern gemäß § 5 SigG a.F. ausgestellten Zertifikate sind danach qualifizierten Zertifikaten gleichgestellt.[693]
Am 3. April 2003 gründeten Staat und Wirtschaft zur Förderung der elektronischen Signatur das „Signaturbündnis“, dessen Geschäftstelle beim Bundesamt für Sicherheit in der Informationstechnik angesiedelt ist. Die Bündnispartner einigen sich darin unter anderem auf gemeinsame technische Standards und einheitliche Sicherheitsvorgaben.[694]

---

[688] § 15 Abs. 1 S. 3 und 4 sowie Abs. 1 S. 2 SigG.

[689] Aus § 17 Abs. 1 bis 3 SigG und der SigV, gemäß § 15 Abs. 7 SigG; oben unter 2.3.3.2 und 2.3.3.3 dargestellt.

[690] Abs. 7 Nr. 1 SigG.

[691] § 15 Abs. 7 Nr. 2.

[692] Sie mussten nur binnen drei Monaten nach Inkrafttreten des SigG einen Deckungsnachweis vorlegen.

[693] Deren Inhaber mussten innerhalb von sechs Monaten nach Inkrafttreten des SigG unterrichtet werden, § 25 Abs. 2 S. 1 SigG. Gleiches wie für die Genehmigung von Zertifizierungsdiensteanbietern und für deren Zertifikate nach dem SigG a.F. gilt auch für die Anerkennungen von Prüf- und Bestätigungsstellen durch die Bundesnetzagentur sowie für die Bestätigung der Erfüllung der Anforderungen des SigG a.F. an technische Komponenten, die damit Produkten für elektronische Signaturen i.S.d. SigG gleichgestellt sind.

[694] Siehe www.signaturbuendnis.de, u.a. auch mit ausführlichen Darstellungen zum Signatureverfahren.

2.3.3.6 Ausländische Signaturen

Für ausländische elektronische Signaturen und deren Produkte bestimmt § 23 Abs. 1 1. HS SigG, in Umsetzung der Vorgabe des Art. 4 RLeS:

> *„Elektronische Signaturen, für die ein ausländisches qualifiziertes Zertifikat aus einem anderen Mitgliedstaat der Europäischen Union... vorliegt, sind, soweit sie Artikel 5 Abs. 1 der* [RLeS] *... entsprechen* [also fortgeschrittene elektronische Signaturen sind, die von einer sicheren Signaturerstellungseinheit erstellt wurden]*, qualifizierten elektronischen Signaturen gleichgestellt."*

In nahezu wortgetreuer Umsetzung der Vorgabe des Art. 7 Abs. 1 RLeS stellt sie elektronische Signaturen im Sinne von Art. 5 RLeS aus Drittstaaten qualifizierten elektronischen Signaturen gleich, wenn das Zertifikat dort öffentlich als qualifiziertes Zertifikat ausgestellt und die oben genannten Voraussetzungen[695] erfüllt sind. Dies gilt insbesondere, wenn der Zertifizierungsdiensteanbieter in einem Mitgliedstaat der Europäischen Union akkreditiert ist, ein solcher Zertifizierungsdiensteanbieter aus der EU für das Zertifikat einsteht oder bilaterale oder multilaterale Vereinbarungen greifen. Aufgrund der Einführung eines freiwilligen Akkreditierungssystems sind elektronische Signaturen nach § 23 Abs. 1 qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung gleichzustellen, wenn sie nachweislich gleichwertige Sicherheit aufweisen. Auch Produkte für elektronische Signaturen, bei denen in einem anderen Mitgliedstaat festgestellt wurde, dass sie den Anforderungen der RLeS entsprechen, werden anerkannt.[696] Sie werden auch den nach dem SigG geprüften Produkten für qualifizierte elektronische Signaturen gleichgestellt, wenn sie nachweislich eine gleichwertige Sicherheit aufweisen.[697]

2.3.4 Änderungen der Formvorschriften

Mit dem Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr (FormG)[698] setzte der deutsche Gesetzgeber insbesondere die Vorgabe des Art. 9 RLeC um, rechtliche Hindernisse für den Abschluss elektronischer Verträge, wie es die in § 126 Abs. 1 und 2 BGB a.F. allgemein aufgestellten Formerfordernisse darstellen, abzuschaffen. Folglich musste das allgemeine Schriftformerfordernis des BGB sowie weitere aus den jeweiligen Regelungen zu

[695] Siehe unter 2.2.2.2 und 2.2.2.3.

[696] § 23 Abs. 3 S. 1 SigG.

[697] § 23 Abs. 3 S. 2 SigG.

[698] Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr (Formvorschriftenänderungsgesetz, im Folgenden FormG abgekürzt) vom 13.07.2001, in Kraft seit 1.8.2001, BGBl. I, S. 1542.

den einzelnen Rechtsgeschäften, angepasst werden.[699] Die §§ 126 ff. BGB wurden weitest gehend in ihrer alten Fassung belassen, aber um entscheidende Regelungen ergänzt. Sonstige Formvorschriften wurden nur in sehr geringem Umfang geändert. Das FormG stellte den bisherigen allgemeinen Formvorschriften die „elektronische Form" und die „Textform" zur Seite, die von unterschiedlicher Qualität sind und unterschiedliche Rechtsfolgen gewähren. Die elektronische Form dient als Abbild und Substitut der Schriftform des § 126 Abs. 1 BGB, indem sie die qualifizierte elektronische Signatur als Äquivalent zur eigenhändigen Unterschrift nutzt. Die Textform soll als neuer Formtyp *„den Rechtsgedanken der unterschriftslosen Erklärung aus bislang verstreuten Einzelvorschriften* [zusammenfassen]*."*[700] Flankiert wurde diese Neuerung durch die Einführung neuer Regelungen unter anderem in die ZPO, mit denen ein Anscheinsbeweis für die qualifizierte elektronische Signatur nach dem SigG eingeführt und die Möglichkeit eröffnet wurde, Schriftsätze und Erklärungen bei Gericht auch als elektronisches Dokument einzureichen.

2.3.4.1 Elektronische Form, §§ 126 Abs. 3, 126a BGB

§ 126 BGB (in seiner alten Fassung) wurde folgender dritter Absatz angefügt:

> *„Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich aus dem Gesetz nichts anderes ergibt."*[701]

Im neu eingefügten anschließenden § 126a wird die elektronische Form definiert als Erklärung in Form eines elektronischen Dokuments, dem der Name des Erklärenden hinzugefügt wurde und das mit einer qualifizierten elektronischen Signatur nach dem SigG versehen wurde.[702] Die generelle Bezugnahme auf die qualifizierte elektronische Signatur wie definiert im SigG sorgt für die automatische Aufnahme der diesbezüglichen Voraussetzungen des SigG in das BGB.[703] Sofern also die besonderen Formvorschriften für das einzelne Rechtsgeschäft die elektronische Form nicht ausschließen,

---

[699] *„Die auf das Medium „Papier" fixierten Formvorschriften des Bürgerlichen Gesetzbuchs tragen den Entwicklungen des modernen Rechtsgeschäftsverkehrs nicht ausreichend Rechnung. ... Die entsprechenden privatrechtlichen Vorschriften bedürfen daher der Anpassung... unter Berücksichtigung der Anforderungen, die sich aus den [RLeS] und [RLeC] ergeben."* Beschlussempfehlung und Bericht des Rechtsausschusses zu dem Gesetzentwurf der Bundesregierung – Drucksache 14/4987 -, BT-Drucks. 14/5561, vom 14.03.2001. Siehe auch die Begründung zum Entwurf des Elektronischer Geschäftsverkehr-Gesetz (EGG), BT-Drucks. 14/6098, S. 13, zum Umsetzungsbedarf im nationalen Recht.

[700] Beschlussempfehlung und Bericht des Rechtsausschusses zu dem Gesetzentwurf der Bundesregierung – Drucksache 14/4987 -, BT-Drucks. 14/5561, vom 14.03.2001.

[701] Art. 1 Nr. 2 lit. a) FormG; lit. b): *„Der bisherige Absatz 3 wird Absatz 4."*

[702] Art. 1 Nr. 3 FormG. Um der Abschlussfunktion zu genügen, reicht z.B. eine Nachbildung der Namensunterschrift; Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 59. Als anzufügender Name genügen der Nachnahme, ein Wahlname oder beim Kaufmann auch die Firma (§ 17 HGB); ders. Rn. 28, 29. Die signierfähigen digitalen Daten (elektronisches Dokument) können auch multimedialer Natur sein; ders. Rn. 31. Zum Erklärungsträger siehe ders., Rn. 50 ff.

[703] Niemann, CLSR 2001, S. 29.

kann sie die Schriftform mit eigenhändiger Unterschrift nach § 126 Abs. 1 ersetzen, wenn sie den vorgenannten Anforderungen genügt. Damit ist die elektronische Form eine gleichwertige Option wo die Parteien die elektronische Kommunikation mittels ausdrücklicher oder stillschweigender Vereinbarung wählen.[704] Ausgeschlossen ist die elektronische Form zum Beispiel bei der Beendigung von Arbeitsverhältnissen, der Erteilung von Leibrentenversprechen, Bürgschaftserklärungen, abstrakten Schuldversprechen und Schuldanerkenntnissen.[705] Sie kann ausgeschlossen werden, wo Formvorschriften der Warnung der Parteien dienen, also das hergebrachte Schriftformerfordernis ausdrücklich verlangt wird.[706] Insgesamt beschränkt der deutsche Gesetzgeber die Möglichkeit, die eigenhändige Unterschrift durch ein elektronisches Substitut zu ersetzen also allein auf die digitale Signatur in ihrer Ausformung der qualifizierten elektronischen Signatur nach dem SigG. Der tatsächliche Anwendungsbereich des § 126a BGB beschränkt sich zudem auf nur wenige Vertragstypen.[707] Damit wird gesetzlich festgelegt, dass die Funktionen der eigenhändigen Unterschrift allein durch diese Technik erfüllt werden können sollen – und auch dies nur in einigen, keinesfalls jedoch allen Fällen. Der Gesetzgeber hat also die Vorgabe der RLeS, nach der sich die Rechtswirksamkeit einer elektronischen Signatur nach den nationalen Formvorschriften bemessen soll, insofern entsprochen, dass er für diese Fälle, in denen die eigenhändige Unterzeichnung gemäß § 126 BGB vorgeschrieben ist, diese Beurteilung vorweggenommen hat. Eine solche gesetzliche Festlegung ist in England und den USA nicht erfolgt.

2.3.4.2 Textform, § 126b BGB

Auch vor den Neuregelungen gab es vereinzelte Vorschriften, die zwar eine schriftliche Erklärung forderten, auf die eigenhändige Unterschrift aber verzichteten, sofern die Er-

[704] Müglich, MMR 2000, S. 10. Das Schriftformerfordernis kann grundsätzlich durch die elektronische Form ersetzt werden in §§ 32 Abs. 2, 37 Abs. 1, 81 Abs. 1, 111 S. 2, 368 S. 1, 410 Abs. 2, 416 Abs. 2 S. 2, 550 S. 1, 557a Abs. 1, 557b Abs. 1, 568 Abs. 1, 574b Abs. 1, 577 Abs. 3, 581 Abs. 2 i.V.m. 550 S. 1, 585a, 594f, 1154 Abs. 1 BGB, außerhalb des BGB z.B. bei §§ 32 Abs. 1, 108 Abs. 3, 122 Abs. 1 S. 1 Aktiengesetz, § 38 Abs. 2 und 3 ZPO; Einsele in MüKo, § 126, Rn. 21, 22. Abzustellen ist hierbei auf den Willen der Parteien, in ihrer konkreten Rechtsbeziehung elektronische Form zu gebrauchen, ohne dass diese einer Partei aufgedrängt wird. Nicht verlangt ist eine Vereinbarung über den Formgebrauch, siehe Noack in Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 18. Gemäß § 126a Abs. 2 BGB, eingeführt gem. Art. 1 Nr. 3 FormG, müssen im Falle des Vertragsschlusses beide Parteien je ein identisches Dokument mit einer qualifizierten elektronischen Signatur versehen.

[705] §§ 623, 761 S. 2, 766 S. 2, 780 S. 2, 781 S. 2 BGB, ferner beim Abschluss von Teilzeit-Wohnrechteverträgen und Verbraucherdarlehnsverträgen, §§ 484 Abs. 1 S. 2, 492 Abs. 1 S. 2 BGB, siehe Einsele in MüKo, § 126, Rn. 23. Teilweise erfolgt der Ausschluss insbesondere aufgrund mangelnder Warnfunktion, Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 22, 23.

[706] Siehe Art. 1 Nr. 7 bis 11 FormG, nach dem in die §§ 623, 630, 761, 766, 780 und 781 S. 1 BGB ein ausdrücklicher Ausschluss der elektronische Form aufgenommen wurde. Dies sei sinnvoll, wo die Formerfordernisse besondere Schutzfunktionen übernehmen, Niemann, CLSR 2001, S. 29. Müglich, MMR 2000, S. 10, führt aus, ein Verzicht hierauf sei nur möglich bei besonderer Vertrautheit mit dem entsprechenden Rechtsgeschäft, etwa bei Kaufleuten gemäß § 350 HGB.

[707] Darlehnsvermittlungsvertrag und bestimmte befristete Miet- und Pachtverträge, Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 40.

klärung mit Hilfe automatischer Einrichtungen erstellt worden war. Hier knüpft der deutsche Gesetzgeber an und führt zusätzlich die Textform in die allgemeinen, für alle Rechtsgeschäfte geltenden Vorschriften ein. Die Textform bündelt damit zuvor existierende Vorschriften aus verschiedenen Gesetzen, die Ausnahmen von diesen strengen Formerfordernissen erlaubten und schafft so ein einheitliches zentrales Formerfordernis.[708] Der Gesetzgeber erkannte ein Verkehrsbedürfnis nach Erleichterung der strengen Schriftform, weshalb er eine Erweiterung der Formvorschriften für geboten hielt, in denen, wie es in der Gesetzesbegründung heißt, die eigenhändige Unterschrift entbehrlich beziehungsweise unangemessen und Verkehrs erschwerend ist.[709] Dies solle unabhängig von der Art und Weise der Erstellung der Erklärung gelten. Welche Formerfordernisse und Formzwecke notwendig seien, müsse sich an dem betreffenden Rechtsvorgang und nicht an der Art und Weise der Anfertigung der Erklärung orientieren.[710] § 126b BGB lautet:

> *„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."*

Dieses reduzierte Formerfordernis verlangt keine Verkörperung, keine eigenhändige Unterzeichnung und keine qualifizierte elektronische Signatur und ist damit sowohl für papierne und elektronische Dokumente geeignet. Es muss nur den Namen des Erklärenden enthalten, damit der Empfänger dessen Herkunft erkennen kann, etwa durch ein Faksimile oder eine eingescannte eigenhändige Unterschrift. Lesbar gemacht wird die Erklärung zum Beispiel bereits durch das Laden auf den Bildschirm.[711] Die Textform soll den Erklärungsempfänger nicht nur mittels einer flüchtigen, zum Beispiel mündlich zugegangenen Erklärung informieren, sondern in einer Form, in der sie dauerhaft in Schriftzeichen wiedergegeben werden kann. Sie soll dort ausreichen und eingesetzt werden können, wo die Informations- und Dokumentationsfunktion im Verhältnis zur Beweisfunktion überwiegen und die Warnfunktion für den Erklärenden keine oder eine untergeordnete Rolle spielt[712], die potenzielle Gefährdung der Rechtssicherheit als ge-

---

[708] Art. 1 Nr. 3 FormG; BT-Drucks. 14/4987, S. 18; Einsele in MüKo, § 126b, Rn. 1; Niemann, CLSR 2001, S. 29.

[709] BT-Drucks. 14/4987, S. 18, 19; Einsele in MüKo, § 126b, Rn. 1; Geis, MMR 2000, S. 671.

[710] BT-Drucks. 14/4987, S. 18, 19; Einsele in MüKo, § 126b, Rn. 1.

[711] So erlaubt es die Textform, automatisierte Massenerklärungen einzusetzen und diese z.B. über Computer wirksam zu kommunizieren; Einsele in MüKo, § 126b, Rn. 2, Niemann, CLSR 2001, S. 29, 30; Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 45. Bspw. kann für die Mitteilung über eine Beteiligungsquote gem. § 20 Abs. 1 Aktiengesetz (AktG) mittels elektronischer Form oder Textform erfolgen, siehe Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 8. Telefax oder sonstige telekommunikative Einrichtungen sind nun – in diesen Anwendungsbereichen – zweifelsfrei als rechtswirksam bestimmt. Geis, MMR 2000, S. 671.

[712] BT-Drucks. 14/4987, S. 19; Einsele in MüKo, § 126b, Rn. 1; Geis, MMR 2000, S. 671; Müglich, MMR 2000, S. 10, 12; Niemann, CLSR 2001, S. 29, 30; Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 46, 47, mit Hinweis auf die bereits anerkannte vervielfältig-

ring zu beurteilen ist und die Echtheitsfunktion einer Form somit regelmäßig leer liefe.[713]

Die in Textform verfasste Erklärung muss, um zur dauerhaften Wiedergabe in Schriftzeichen geeignet zu sein, zunächst irgendwie in Schriftzeichen lesbar zu machen sein. Nicht verlangt ist die unmittelbare Lesbarkeit oder eine Speicherung in Schriftzeichen. Der Empfänger muss die Erklärung aber mit einem Hilfsmittel wiedergeben und dadurch deren durch Schriftzeichen wiedergegebenen Sinn optisch wahrnehmen können.[714] Bei der Nennung des Namens des Erklärenden ist es gleichgültig, wo dessen Name genannt wird, etwa im Kopf oder im Inhalt der Erklärung.[715] Einer Unterschrift bedarf es zur Autorisierung nicht.[716] Es geht um die Erkennbarkeit der Person, die die Erklärung in eigener Verantwortung abgibt. Die sprachliche Unterscheidung zwischen dem in § 126b BGB genannten Erklärenden und dem Aussteller aus §§ 126 Abs. 1, 126a Abs. 1 BGB scheint daher unbeachtlich zu sein. Jedenfalls aber soll der Begriff des Erklärenden nicht anders als der des Ausstellers bestimmt werden.[717] Sofern im konkreten Fall auf Grund der zwischen den Parteien bestehenden Beziehungen die Person des Erklärenden mit hinreichender Deutlichkeit erkennbar ist, genügt die Nennung des Vor- oder Spitznamens beziehungsweise eines Pseudonyms.[718] Es ist daher schlüssig, der Textform auch eine Identifizierungsfunktion zuzubilligen.[719] Der Abschluss der Erklärung muss zudem erkennbar gemacht werden. Dies kann durch Nachbildung der Namensunterschrift oder anders, also durch die Nennung des Namens am Ende des Textes, durch Faksimile, eingescannte Unterschrift, Datierung, eine Grußformel oder andere

te Unterschrift z.B. in Vorschriften im Versicherungsvertragsgesetz und § 13 AktG. Die Textform wird verlangt für Erklärungen nach §§ 312c Abs. 2 (Verbraucherinformation in Fernabsatzverträgen), 355 Abs. 1 S. 2 (Widerruf bei Verbraucherverträgen), 356 Abs. 1 Nr. 3 (Einräumung eines Rückgaberechts bei Verbraucherverträgen), 357 Abs. 3 (Hinweis an Verbraucher über Wertersatzpflicht), 477 Abs. 2, (Garantieerklärung in Textform auf Verbraucherverlangen) 493 Abs. 1 S. 5 (Bestätigung und Unterrichtung bei Überziehungskrediten), 502 Abs. 2, 505 Abs. 2 (Ratenlieferungsvertrag), 554 Abs. 3 (Mietermitteilung über Erhaltungs- und Modernisierungsmaßnahmen), 556a Abs. 2 (Vermietererklärung bzgl. Betriebskostenabrechnung), 556b Abs. 2 (Aufrechnungserklärung des Mieters), 557b Abs. 3 (Mieterhöhungsverlangen bei Indexmiete), 558a Abs. 1 (Mieterhöhungsverlangen), 559b Abs. 1 (Mieterhöhungsverlangen), 560 Abs. 1 und 4 (Erklärung über Betriebskostenerhöhung), 613a Abs. 5 (Arbeitnehmerunterrichtung bei Betriebsübergang), 651g Abs. 2, 665b Abs. 1 S. 4 BGB, sowie außerhalb des BGB z.B. in § 24 Abs. 4 Wohnungseigentumsgesetz, §§ 410 Abs. 1, 438 Abs. 4, 455 Abs. 1, 468 Abs. 1 HGB, oder generell bei formbedürftigen Handlungen des Versicherungsunternehmers gemäß dem Gesetz über den Versicherungsvertrag (VVG) bzw. für die Widerrufserklärung des Versicherungsnehmers (§ 8 Abs. 1); siehe Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 48, und Heinrichs in Palandt, § 126b, Rn. 2.

[713] So Gotthard/Beck, Elektronische Form und Textform im Arbeitsrecht: Wege durch den Irrgarten", NZA 2002, S. 876-883, S. 879.

[714] Weshalb gesprochene und dann digitalisierte Worte nicht der Textform genügen, siehe bei Noack/Kremer, *Anwaltkommentar BGB*, § 126b, Rn. 11, 12.

[715] Einsele in MüKo, § 126b, Rn. 5; Heinrichs in Palandt, § 126b, Rn. 4.

[716] OLG Hamm, Urt. v. 8.8.2006, 19 U 2/06, NJW-RR 2007, S. 852-853, S. 852.

[717] Einsele in MüKo, § 126b, Rn. 5.

[718] Einsele in MüKo, § 126b, Rn. 5, der auf die Verwendung des Namens, unter dem der Betreffende tatsächlich auftritt und bekannt ist, bei § 126 BGB verweist; Heinrichs in Palandt, § 126b, Rn. 4; siehe auch BT-Drucks. 14/4987, S. 20; Noack/Kremer, *Anwaltkommentar BGB*, § 126b, Rn. 18.

[719] So Mankowski, „Textform und Formerfordernisse im Miet- und Wohnungseigentumsrecht", ZMR 2002, S. 481-489, S. 483, siehe auch unten 3.3.

Zusätze wie *„diese Erklärung ist nicht unterschrieben“* geschehen. Es muss das Ende der Erklärung kenntlich gemacht werden, um sie als rechtlich bindende Erklärung vom nicht bindenden Entwurf abzugrenzen.[720]
Erklärungen in Textform sind Information des Empfängers durch ein Medium, dass die Erklärung, in Abgrenzung zum flüchtig gesprochenen Wort, stets abrufbar und dauerhaft verfügbar hält. Sie erfüllt daher die Dokumentations- und Informationsfunktion.[721]
Aufgrund der Dokumentationsfunktion ist das Element der dauerhaften Wiedergabemöglichkeit von besonderer Bedeutung. Dennoch können an die dauerhafte Wiedergabemöglichkeit etwa elektronischer Speichermedien keine allzu hohen Anforderungen gestellt werden. Sie setzt nicht voraus, dass die Schriftzeichen wirklich langfristig festgehalten werden müssen[722], jedoch soll die Erklärung für eine den konkreten Umständen nach angemessene Zeit durch den Empfänger zur Kenntnis genommen werden können.[723] Der Empfänger soll die Erklärung mit verkehrsüblichen technischen Mitteln inhaltlich unverändert reproduzieren und gegebenenfalls speichern können. Es genügt die Verkörperung der Erklärung auf einer Festplatte, auf Diskette oder CD-ROM. Auf ein eventuelles Ausdrucken des elektronischen Dokuments kommt es dann nicht mehr an. Allerdings ist ein bloßes Zugänglichmachen der Erklärung in einem vom Erklärenden exklusiv beherrschten Medium oder die Ablage in einem flüchtigen Speicher nicht ausreichend.[724] Der Zugang als Fax, Computerfax, Kopie oder – jedenfalls bei Speicherung auf dem eigenen Server oder PC – E-Mail genügt daher für den formgerechten Zugang der Erklärung.[725]
Umstritten ist allerdings, ob die Textform bei Darstellung einer Erklärung auf einer Website gewahrt wird, was in Rechtsprechung und Literatur insbesondere an der Frage der wirksamen und rechtzeitigen Widerrufsbelehrung beim Fernabsatzgeschäft über das Internet diskutiert wird.[726] Nach einer Ansicht genügen Erklärungen auf Websites nicht

[720] Einsele in MüKo, § 126b, Rn. 6; Noack/Kremer, *Anwaltkommentar BGB*, § 126b, Rn. 19; OLG Hamm, NJW-RR 2007, S. 852.

[721] Einsele in MüKo, § 126b, Rn. 7; siehe bspw. auch Ulmer, „Online Vertragsschluss – ein Verfahren wird populär?“, CR 2002, S. 208-213, S. 211, der das Integritätsprinzip – die Sicherung des Inhalts und des Umfanges der Erklärung –durch die Textform des § 126b BGB gefördert sieht.

[722] Einsele in MüKo, § 126b, Rn. 4 mit Verweis auf RG, DJZ 15 (1910), S. 594 f., in dem ein dauerhaftes Festhalten von Schriftzeichen für ein Testament auf einer Schiefertafel angenommen wurde.

[723] Noack/Kremer, *Anwaltkommentar BGB*, § 126b, Rn. 13, die auf einen Zeitraum z.B. bis zur vollständigen Abwicklung des betroffenen Rechtsgeschäfts abstellen.

[724] Einsele in MüKo, § 126b, Rn. 4; Heinrichs in Palandt, § 126b, Rn. 3; Noack/Kremer, *Anwaltkommentar BGB*, § 126b, Rn. 13.

[725] Die Verkörperung der Widerrufsbelehrung in einer E-Mail wahrt das Textformerfordernis des § 126b BGB, weil die Botschaft dem Empfänger übermittelt wird und er sie jederzeit von seinem eigenen Server abrufen und speichern kann, LG Berlin, Urt. v. 24.05.2007, 16 O 149/07, CR 2008, S. 198. Für die Formerfüllung des § 48 Abs. 2 GmbHG (Einverständniserklärung der Gesellschafter in Textform zum Verzicht auf die Gesellschafterversammlung oder zur schriftlichen Abgabe der Stimmen) durch Erklärungen mittels SMS Mayer, „Nichtige Gesellschafterbeschlüsse einer GmbH“, NZG 2007, S. 448-450, S. 450. Zu Computerfax siehe auch unten 3.3.12

[726] Darstellung des Streitstandes nachfolgend. Nur für die Frage der Anforderungen an die Widerrufsbelehrung von Belang, hier jedoch wegen der Darstellung der RLeC erwähnt die Schlussfolgerung von Lejeune in „Die Reform der Widerrufsbelehrung für den Online Handel“, CR 2008, S. 226-231, S. 229, 230: Gemäß den Anforderungen des Art. 10 Abs. 3 RLeC müssten Vertragsbestimmungen und AGB dem Nutzer nur so zur Verfügung gestellt werden, dass dieser sie speichern und reproduzieren könne.

der Anforderungen der Dauerhaftigkeit, da es dem Betreiber jederzeit möglich ist, diese zu verändern oder ganz vom Netz zu nehmen. Tatsächlich können Dateien bei erneutem Aufruf der Website durch zwischenzeitlich veränderte Onlineversion aktualisiert und auf diese Weise ersetzt werden. Da dem Nutzer dadurch die Einsichtnahme in die unveränderte Erklärung willkürlich verwehrt werden kann, sei deren Dauerhaftigkeit nicht gegeben.[727] Websites seien nicht per se geeignet, vom Empfänger dauerhaft wiederhergestellt zu werden. Dazu bedürfe es des wesentlichen und vom Empfänger eigenhändig zu veranlassenden Zwischenschritts der Speicherung. Die bloße Möglichkeit dazu erfülle das Textformerfordernis jedoch nicht.[728] Die Textform sei nur dann gewahrt, wenn es tatsächlich zur Perpetuierung der Erklärung beim Abrufenden komme.[729] Nach der Gegenansicht müsse sich die Website als Datenträger nur zur dauerhaften Wiedergabe in Schriftzeichen eignen, was der Fall sei, wenn der Empfänger die darauf enthaltene Erklärung herunter laden oder ausdrucken könne.[730] Zutreffend ist, dass Texte in HTML-Dateien[731] ohne weiteres dauerhaft lesbar sind beziehungsweise über Speicherung und Ausdruck lesbar gemacht werden können. Es komme, so diese Ansicht weiter, folglich auf die Eignung dazu an und nicht darauf, ob der Empfänger davon Gebrauch mache.[732] Zutreffend ist ferner, dass auch E-Mails als Textdateien, insbesondere aber als HTML-

Der Verbraucher müsse gemäß Art. 5 RLeC die Informationen über das Bestehen eines Widerrufsrechts nach Art. 4 Abs. 1 lit. f) RLeC rechtzeitig vor Vertragsabschluss schriftlich oder auf einem für ihn verfügbaren dauerhaften Datenträger verfügbar haben. Deshalb bestünde bei der Widerrufsbelehrung aufgrund der RLeC kein Erfordernis für die Textform. Und daher reiche es aus, dass der Verbraucher die vorgenannten Informationen vor Vertragsschluss von der Website des Unternehmers herunterladen könne.

[727] Buchmann, „Die Widerrufsbelehrung im Spannungsfeld zwischen Gesetzgebung und Rechtsprechung – Vorschlag für ein Muster für Fernabsatzgeschäfte mit Waren im Internet“, MMR 2007, S. 347-353, S. 349; Bonke/Gellmann, „Die Widerrufsfrist bei eBay-Auktionen – Ein Beitrag zur Problematik der rechtzeitigen Belehrung des Verbrauchers in Textform“, NJW 2006, S. 3169-3173, S. 3170; Schirmbacher, „Von der Ausnahme zur Regel: Neue Widerrufsfristen im Online-Handel? – Zugleich Anmerkungen zu den Urteilen des KG v. 18.7.2006 – 5 W 156/06 und des OLG Hamburg v. 24.8.2006 – 3 U 103/06“, CR 2006, S. 673-677, S. 677; OLG Köln, Urt. v. 24.8.2007, 6 U 60/07, CR 2008, S. 44-49, S. 45, m.w.N. aus der Rechtsprechung.

[728] Bonke/Gellmann, NJW 2006, S. 3170; Hoffmann, „Anmerkung zu OLG Hamburg, Urt. v. 24.8.2006 – 3 U 103/06 – Dauer der Widerrufsfrist bei eBay-Auktionen“, MMR 2006, S. 676-677, S. 677.

[729] KG, Beschl. v. 18.7.2006, 5 5 W 156/06, MMR 2006, S. 678-679, S. 679; OLG Hamburg, Urt. v. 24.8.2006, 3 U 103/06, MMR 2006, S. 675-676, S. 676; OLG Köln, CR 2008, S. 45; Beschl. v. 5.12.2006, 5 W 295/06, MMR 2007, S. 185-186, S. 186.

[730] Einsele in MüKo, § 126b, Rn. 9; Heinrichs in Palandt, § 126b, Rn. 3; Noack, DStR 2001, S. 1897; Steinbeck, „Die neuen Formvorschriften im BGB”, DStR 2003, S. 644-650, S. 649; auch Kaufmann, „Das Online-Widerrufsrecht im Spiegel der Rechtsprechung – Eine Bestandsaufnahme zur Fortentwicklung des Online-Widerrufsrechts durch die Judikative“, CR 2006, S. 764-770, S. 766, der ausgehend von der Prämisse, Manipulationen seien durch Ausdruck oder Speicherung der online bereitgestellten Erklärung ausgeschlossen, feststellt, dass nicht ersichtlich sei, warum sich im Falle der Widerrufsbelehrung diese zu Gunsten des Empfängers verlängern solle, wenn er dies unterlasse – was freilich allenfalls dann als zutreffend bewertet werden könnte, wenn man Websites hier genügen ließe.

[731] HTML (Hypertext Markup Language oder deutsch Hypertext-Auszeichnungssprache), oft kurz als Hypertext bezeichnet, ist eine textbasierte Auszeichnungssprache zur Strukturierung von Inhalten wie Texten, Bildern und Hyperlinks in Dokumenten. HTML-Dokumente sind die Grundlage des www und werden von einem Webbrowser dargestellt.

[732] Stadler, „Widerrufsfrist bei eBay-Auktionen – Können Webseiten die Voraussetzungen der Textform nach § 126b BGB erfüllen?“, JurPC Web-Dok. 136/2006, Abs. 1-26, Abs. 15, 16.

Mails ebenso leicht abänderbar sind wie HTML-Seiten.[733] Verbleiben solche HTML-Mails auf dem Server des Anbieters und werden nicht auf dem eigenen Rechner gesichert und hat daher der Nutzer lediglich die Möglichkeit der Speicherung oder des Ausdrucks, so ist die Situation der bei einer Website – insoweit – vergleichbar.[734] Die fehlende Änderbarkeit beziehungsweise Manipulierbarkeit sei auch gerade kein vom Gesetzgeber vorgesehenes Kriterium, da die Textform keine Beweisfunktion erfülle.[735] Die Veränderungsmöglichkeit spiele daher für die Formwirksamkeit keine Rolle.[736] Diese Argumentation ist stichhaltig. Besonderes Gewicht bekommt vor diesem Hintergrund das Argument, dass es zu erheblichen Wertungswidersprüchen käme, wenn man auf der einen Seite E-Mails – auch mit dynamischem Inhalt – generell als zur dauerhaften Wiedergabe geeignet ansähe, andererseits aber eine – wenn auch zeitlich befristete – Speicherung von Internetseiten in unveränderbarer Form mit der Möglichkeit des individuellen Abrufs durch den Nutzer als nicht dauerhaft erachte.[737] Die undifferenzierte Unterscheidung zwischen E-Mail einerseits und Internetseite andererseits scheint daher im Rahmen der Frage der Dauerhaftigkeit der Wiedergabe tatsächlich nicht mehr tauglich.[738] Zu holzschnittartig ist jedoch die Folgerung, dass, wolle man nicht allen Arten von elektronischen Erklärungen die Textform versagen, man es immer genügen lassen müsse, dass dem Empfänger eine dauerhafte Speicherung oder ein Ausdruck ermöglicht werde.[739] Vielmehr muss hier gerade differenziert werden nach Art und Form (zum Beispiel HTML- oder einfache Textdatei) der digitalen Erklärung. Für den besonderen Fall der auf der Website enthaltenen Widerrufsbelehrung auf eBay, die dort zusammen mit dem jeweiligen Angebot für 90 Tage unveränderlich gespeichert wird, haben Gerichte angenommen, dass der Verbraucher ohne besonderen Aufwand die Möglichkeit hat, diese zu speichern und auszudrucken, weshalb seinem Schutzbedürfnis hinreichend Rechnung getragen sei und diese Darstellung auf der Website ausnahmsweise der Textform genügen soll.[740]

Es bleibt das Problem des Zugangs bei lediglich auf Websites dargestellten und herunterladbaren Erklärungen, sowie des Beweises desselben. Das *OLG Köln* hat, ebenfalls in einem die Widerrufsbelehrung betreffenden Fall, entschieden, dass in der Speicherung

[733] Stadler, JurPC Web-Dok. 136/2006, Abs. 10. Denn auch E-Mails können mittlerweile dynamischen HTML-Inhalt enthalten dergestalt, dass im Rahmen der empfangenen E-Mail eine Grafik oder sonstiger HTML-Inhalt abgerufen und dargestellt wird. Der Inhalt der E-Mail kann demgemäß durch Änderungen der auf dem Server lagernden Grafik ohne Weiteres verändert werden. Für den Nutzer ist dies umso unsicherer, als er nicht damit rechnet, dass eine einmal in sein E-Mail-Postfach gelangte Nachricht nachträglich verändert werden kann. Siehe bei Dietrich/Hofmann, „3... Gerichte, 2... Wochen, 1... Monat? – Konfusion um die Widerrufsfristen bei eBay", CR 2007, S. 318-322, S. 319, 320.

[734] Dietrich/Hofmann, CR 2007, S. 319, 320.

[735] Stadler, JurPC Web-Dok. 136/2006, Abs. 10.

[736] Noack, „Digitaler Rechtsverkehr: elektronische Signatur, elektronische Form und Textform", DStR 2001, S. 1893-1897, S. 1897

[737] Dietrich/Hofmann, CR 2007, S. 319.

[738] Dietrich/Hofmann, CR 2007, S. 319.

[739] Stadler, JurPC Web-Dok. 136/2006, Abs. 16.

[740] LG Potsdam, Urt. v. 30.09.2004, 11 S 27/04, MMR 2007, S. 191; LG Flensburg, Urt. v. 23.8.2006, 6 O 107/06, MMR 2006, S. 686. Für diesen Sonderfall sei dem LG Flensburg zugegeben, dass diese Betrachtungsweise eine klare Abgrenzung ermöglicht und bestimmte Schwierigkeiten vermeidet.

durch den Plattformbetreiber gerade keine gezielte Mitteilung an den jeweiligen Empfänger liege. Dies sei bei E-Mails, die mit ihrer Speicherung auf dem als virtueller Briefkasten fungierenden Server des Providers gezielt in den Machtbereich des Nutzers gelangt seien, anders.[741] Von einer Abgabe der Erklärung an den Empfänger im Sinne einer zielgerichteten Entäußerung kann – besondere Einzelfälle ausgenommen – bei Websites in der Tat grundsätzlich nicht die Rede sein.[742] Erklärungen auf einer Website gingen dem Empfänger deshalb nicht im Sinne von § 130 BGB zu, wenn dieser die Informationen lediglich lese.[743] Dagegen wird eingewandt, dass die Textform auch dann erfüllt werde, wenn der Empfänger die Information im Sinne eines Pull selbst abrufen könne, weil der Erklärende die Erklärung lediglich abzugeben habe. Entscheidend sei also die Abgabe durch den Erklärenden und nicht der tatsächliche Empfang.[744] Diese Annahme kann jedoch schon für die Widerrufsbelehrung und somit für vergleichbare empfangsbedürftige Erklärungen nicht zutreffen. Nach dem Sinn der Belehrung ist ein Erfolg geschuldet, nicht bloßes Tätigwerden des „Erklärenden", bei dem es letztlich allein auf das Verhalten des „Erklärungsempfängers" ankommt, ob eine Belehrung oder ein Zugang tatsächlich erfolgt. Auf eine gewisse Zielgerichtetheit bei Abgabe der Erklärung kann also nicht verzichtet werden. Auf die Textform allgemein bezogen widerspräche diese Annahme zunächst auch deren Informationsfunktion, da es bei den Anwendungsbereichen der Textform – auch bei Massenerklärungen – immer einen bestimmten, konkretisierten Adressatenkreis gibt, auf die eine Entäußerung hinzielen muss. Andernfalls kann der Erklärende auch nicht sicher sein, ob ein Zugang und damit eine dauerhaften Wiedergabe gewährleistet oder überhaupt, wie hier gefordert, nur ermöglicht wird. Und auch die Dokumentationsfunktion wäre dabei nicht gewährleistet, da aus Sicht des Erklärenden vom Verhalten des Empfängers abhängig. Der Ansicht, die in Schriftzeichen lesbare Erklärung sei mit dem Aufruf der Website in den Machtbereich des Empfängers gelangt und die Tatsache, ob der Empfänger die Möglichkeit der Speicherung oder des Ausdrucks im Einzelfall nutze oder nicht, habe mit der Frage nach Einhaltung der Form nichts zu tun[745], kann daher – in dieser Pauschalität zumindest – nicht zugestimmt werden. Schwierig bis unmöglich würde auch der durch den Absender zu erbringende Beweis, dass der Empfänger die Erklärung gespeichert beziehungsweise ausgedruckt hat.[746] Auch wenn diese Frage unabhängig von der Frage der Formerfüllung gesehen werden muss[747], so wird doch hier letztlich der praktische

[741] OLG Köln, CR 2008, S. 46.

[742] So richtig Buchmann, MMR 2007, S. 349.

[743] Buchmann, MMR 2007, S. 349.

[744] Stadler, JurPC Web-Dok. 136/2006, Abs. 11, 16.

[745] Sobald der Empfänger die Internetseite lädt, sei die in Textform abzugebende Erklärung wirksam geworden. Die Erklärung werde schon automatisch für eine gewisse Zeit gespeichert (Festplatten-Cache), doch komme es darauf nicht an. So Noack, DStR 2001, S. 1897.

[746] Auch weil ein Anscheinsbeweis wie bei der Sendebestätigung eines Fax oder einer E-Mail nicht besteht, siehe Buchmann, MMR 2007, S. 349; a.A. Waltl in Loewenheim/Koch, *Praxis des Online-Rechts*, München 2001, S. 184, der Empfangsbestätigungen bei E-Mails eine starke Beweiskraft zuerkennt.

[747] Noack, DStR 2001, S. 1897, der auch auf die Bedeutung der Reformulierung einer Website-Erklärung bei Streit um die zum Zugangszeitpunkt maßgebliche Fassung und auf den Umstand hinweist, dass der

Grund dafür liegen, Informationen allein auf Websites nicht für Erklärungen, die der Form des § 126b BGB bedürfen, zu nutzen.
Die Funktionen der Warnung und der Beweissicherung sowie eine Identitäts- und Echtheitsfunktion soll die Textform dagegen nicht übernehmen können. Grund hierfür sei, dass der Erklärende zwar seinen Namen nennen, sich zu der Erklärung jedoch nicht in der unverwechselbaren Weise der Unterschrift oder der digitalen Signatur bekennen müsse.[748] Die mit einer Erklärung in Textform verbundenen Rechtsfolgen sollen grundsätzlich nicht erheblich oder aber leicht rückgängig zu machen sein.[749] Die der Textform unterliegenden Erklärungen lösten in der Regel zumindest nicht unmittelbar und typischerweise vertragliche Verpflichtungen des Erklärenden gegenüber dem Erklärungsempfänger aus.[750] Hier ist zu unterscheiden von denjenigen Erklärungen, für die das Gesetz die Textform vorschreibt und also genügen lässt. Angesichts des begrenzten Anwendungsbereichs[751] ist dies für die davon umfassten Rechtsgeschäfte und Erklärungen zutreffend. Gleichwohl wird eine Großzahl der im elektronischen Geschäftsverkehr vorkommenden elektronischen Kommunikationsformen die oben genannten Voraussetzung der Textform erfüllen.[752] Wie richtig angemerkt wird, ist der Gesetzgeber mit der Einführung der Textform der Rechtswirklichkeit gefolgt, die insbesondere bei Massenerklärungen zum Verzicht auf die eigenhändige Unterzeichnung zwecks Vereinfachung des Rechtsverkehrs gedrängt habe.[753] Dabei ist zum einen nicht ausgeschlossen, dass sich der Erklärende durch die Nennung seines Namens zum Beispiel in einer E-Mail durchaus zu der betreffenden Erklärung bekennt, diese also authentifizieren will. Neben Willenserklärungen können auch geschäftsähnliche Handlungen in Textform vorgenommen werden.[754] Zum anderen ist vor diesem Hintergrund fraglich, ob die Beschränkung auf Erklärungen und damit Rechtsgeschäfte, deren Rechtsfolgen nicht erheblich oder leicht rückgängig zu machen sein sollen, sinnvoll ist beziehungsweise in der derzeitigen restriktiven Form durchzuhalten ist. Danach stellt die Textform zunächst nur dort, wo der Zweck einer die Schriftlichkeit vorsehenden Vorschrift nicht zur Ein-

Erklärende schon im eigenen Interesse den Abruf der Seite durch Bestätigungsanforderungen, Registrierungen oder durch Kontrollprogramme dokumentieren werde.

[748] Einsele in MüKo, § 126b, Rn. 7; Geis, MMR 2000, S. 671; Heinrichs in Palandt, § 126b, Rn. 1, nachdem die Textform keine der klassischen Formzwecke erfüllt; Müglich, MMR 2000, S. 10, 12; Niemann, CLSR 2001, S. 29, 30; Steinbeck, DStR 2003, S. 649; Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 46, 47, mit Hinweis auf die bereits anerkannte vervielfältigte Unterschrift z.B. in Vorschriften im Versicherungsvertragsgesetz und § 13 AktG. In Bezug auf die Warnfunktion a.A. Mankowski, ZMR 2002, S. 483, unter Hinweis auf die vielfach nur minimale Warnfunktion bei der traditionellen Schriftform, insbesondere bei vorformulierten Erklärungen.

[749] Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 46.

[750] Einsele in MüKo, § 126b, Rn. 5.

[751] Insgesamt wurde die Textform nur äußerst zurückhaltend eingesetzt. Dazu Scheffler/Dressel, CR 2000, S. 380. So wird sie lediglich in für die §§ 554 Abs. 3, 556a Abs. 2, 556b Abs. 2, 557b Abs. 3, 558a Abs. 1, 559b Abs. 1, 560 Abs. 1 und 4, sowie in § 651g Abs. 2 BGB gesetzlich für ausreichend erklärt. Eine Aufzählung der Vorschriften des BGB, auf die die Textform Anwendung findet siehe in Heinrichs in Palandt, § 126b, Rn. 2.

[752] Siehe 2.3.4.2 und auch unten unter 3.3.1 und 3.3.2.

[753] So Noack/Kremer in Dauner-Lieb et al., *Anwaltkommentar BGB*, § 126b, Rn. 2.

[754] Noack/Kremer in Dauner-Lieb et al., *Anwaltkommentar BGB*, § 126b, Rn. 9.

haltung von § 126 BGB zwingt, eine Alternative dar.[755] Es ist jedoch fraglich, ob die Textform im Einzelfall auch bei Fehlen einer ausdrücklichen gesetzlichen Anordnung die Schriftform ersetzen kann. Dies ist durch Auslegung zu ermitteln.[756] Möglich ist, dass der Begriff „schriftlich" lediglich den Ausschluss der bloß mündlichen Erklärung oder Information meint.[757] Daneben kann die Einhaltung zum Beispiel der Schriftform unter Berücksichtigung des Formzwecks als entbehrlich angesehen werden und das Rechtsgeschäft daher dennoch als rechtswirksam anzusehen sein.[758] Oder der Normzweck der jeweiligen Formvorschrift gebietet gar eine Erleichterung gegenüber der gesetzlichen Schriftform durch die Verwendung der Textform, etwa dann wenn erstere wegen der untergeordneten Bedeutung der Warn- und Beweisfunktion nicht erforderlich ist.[759]

Die Einführung der Textform wurde aus mehreren Gründen kritisiert. Sie passe nach ihrer Art und ihrem Sinn nicht in das bisherige System der Formvorschriften des Zivilrechts. Die Änderung des Schriftformerfordernisses in Textform möge allenfalls theoretisch sinnvoll sein, wo bereits vorher keine Warn- oder Beweisfunktion der Schriftform mehr vorhanden war, aber nicht wirklich notwendig. Denn dort wo keine Schriftform mit ihren typischen Funktionen erforderlich sei, genügte im Zweifel die Aufhebung des Formerfordernisses. Bestenfalls werde sie sich als überflüssige aber unschädliche „Form" erweisen.[760] Der Bundesrat prägte den Begriff der „qualifizierten Formlosigkeit".[761] Andere dagegen erblicken in der Textform unter Hinweis auf deren Perpetuierungs- und Identifizierungsfunktion, die die Einhaltung einer gewissen „Mindestform" gebieten, eine geeignete und keineswegs überflüssige Formstufe.[762]

2.3.4.3 Vereinbarte Form - Änderungen des § 127 BGB

Wird die Formbedürftigkeit rechtsgeschäftlich zwischen den Parteien vereinbart, können diese selbst bestimmen, welche Anforderungen sie an die rechtsgeschäftlich vereinbarte Form stellen. Für den Fall, dass die Parteien keine anderweitige Regelung treffen, enthält § 127 BGB eine Auslegungsregel dahingehend, dass die Regelungen der §§ 126, 126a und 126b BGB auch bei vertraglich frei vereinbarten Formerfordernissen Anwendung finden, wenn diese Zweifel aufwerfen bezüglich der Form des Vertrages. Die

[755] Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 49.

[756] Einsele in MüKo, § 126b, Rn. 2.

[757] Einsele in MüKo, § 126b, Rn. 2; Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 49.

[758] Einsele in MüKo, § 126b, Rn. 2.

[759] Noack/Kremer in Dauner-Lieb et al., *Anwaltkommentar BGB*, § 126b, Rn. 6, mit Verweis auf die schriftlichen Erklärungen nach § 626 Abs. 2 S. 3 BGB, § 99 Abs. 3 S. 1 BetrVG und § 20 Abs. 1 S. 1 AktG, die Einreichung vorbereitender oder bestimmender Schriftsätze im Zivilprozess oder auf die durch Tarifvertrag begründeten.

[760] Hähnchen, Susanne, "Das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr", NJW 2001, S- 2831-2834, S. 2832, 2833.

[761] BR-Begr., BT-Drucks. 14/6044, S. 1.

[762] Mankowski, ZMR 2002, S. 483.

rechtsgeschäftlich vereinbarte schriftliche Form kann durch die elektronische Form ersetzt werden.[763] Die Bezugnahme auf die neuen §§ 126a, 126b und 127 Abs. 1 BGB ergänzt und ersetzt die veraltete Wortwahl telegraphische Übertragung durch telekommunikative Übermittlung und öffnet den Anwendungsbereich für alle telekommunikativen Mittel.[764] Ferner verzichtet § 127 Abs. 1 BGB zwar auf das Erfordernis der eigenhändigen Unterschrift, nicht jedoch generell auf die Schriftform im Sinne einer textlich verkörperbaren Erklärung.[765] § 127 Abs. 2 und Abs. 3 BGB sehen jeweils Erleichterungen für die Wahrung der vereinbarten Form vor. So bestimmt § 127 Abs. 3 BGB, dass bei der Wahl der elektronischen Form im Zweifel „*eine andere als die in § 126a bestimmte Signatur*" genügt. Es genügt also sowohl eine einfache als auch eine fortgeschrittene elektronische Signatur nach § 2 Nr. 1 und Nr. 2 SigG.[766] Dies wird als ein Zugeständnis an die Tatsache gewertet, dass auch digitale Signaturen, die nicht den Erfordernissen des Signaturgesetzes entsprechen, ein gewisses Maß an Sicherheit bieten, das über dem von Fax oder Telegramm liegt.[767]
Eine weitere bedeutende Änderung bei vertraglich vereinbarten Formerfordernissen ist, dass nurmehr Angebot und Annahme jeweils elektronisch signiert werden müssen und nicht mehr *ein* Dokument mit dem gesamten Vertragsinhalt durch beide Parteien elektronisch signiert werden muss.[768]

2.3.5 Änderungen der Beweisvorschriften

2.3.5.1 Beweisantritt mit elektronischem Dokument, § 371 Abs. 1 S. 2 ZPO

Mit § 371 Abs. 1 S. 2 ZPO wurde die Beweismittelfähigkeit elektronischer Dokumente ausdrücklich festgestellt. Sollen sie als Beweis verwendet werden, sind sie dem Gericht als Datei und nicht lediglich als Ausdruck vorzulegen. Sie unterliegen damit der freien Beweiswürdigung durch das Gericht.[769] Auch der neue § 371 Abs. 1 S. 2 ZPO bestätigt

[763] Steinbeck, DStR 2003, S. 647; Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 63, 65. Ebenso kann von der vereinbarten Textform auf die Schriftform übergegangen werden; ders. Rn. 71.

[764] Eingeführt durch Art. 1 Nr. 4 FormG in § 127 Abs. 2 Satz 1 BGB. Folglich genügt auch ein Fax oder eine E-Mail, Heinrichs in Palandt, § 127, Rn. 2.; Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 66.

[765] Das bedeutet, dass nunmehr jede E-Mail oder Computerfax genügt, nicht jedoch die allein mündliche Erklärung; Heinrichs in Palandt, § 127, Rn. 2.

[766] Steinbeck, DStR 2003, S. 647; Heinrichs in Palandt, § 127, Rn. 5. Die Privatautonomie bleibt über § 127 Abs. 3 S. 2 BGB erhalten, der eine Rückfallposition für einvernehmliche, nachträgliche Vereinbarungen bietet; Müglich, MMR 2000, S. 12.

[767] Niemann, CLSR 2001, S. 30.

[768] § 126 Abs. 3 BGB, eingeführt durch Art. 1 Nr. 4 FormG, Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 67.

[769] § 286 ZPO, Hoffmann, DSWR 2006, S. 61. Ausführliche Darstellung bei Berger, „Beweisführung mit elektronischen Dokumenten", NJW 2005, S. 1016-1020.

nun gesetzlich, dass elektronische Dokumente den Regeln über den Augenscheinsbeweis unterliegen (siehe nachfolgend).[770]

2.3.5.2 Anscheinsbeweis bei elektronischer Form, § 371a Abs. 1 S. 2 ZPO

Im Gegensatz zu § 1 Abs. 1 SigG a.F. besteht nunmehr lediglich die Möglichkeit der freiwilligen Akkreditierung des Zertifizierungsdiensteanbieters. An diese ist eine Beweis- und Sicherheitsvermutung gerade nicht mehr geknüpft, da dies im Hinblick auf die Binnenmarktregelungen der Art. 3 und 4 RLeS ein Hindernis für den freien Binnenmarkt darstellte.[771] Mit der freiwilligen Akkreditierung weist der Zertifizierungsdiensteanbieter (lediglich) nach, dass seine technische und administrative Sicherheit hinsichtlich der auf qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen umfassend geprüft wurde.[772] Das FormG führte nun darauf aufbauend eine Vermutungsregel zu Gunsten des Empfängers ein. Diese, ausschließlich für die elektronische Form des § 126a BGB geltende und damit nur auf die qualifizierte elektronische Signatur anwendbare Regelung, findet sich in den Beweisvorschriften der ZPO.[773] Ursprünglich wurde sie neu als § 292a ZPO eingeführt. Dieser lautete:

> *„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 ernstliche Zweifel daran begründen, dass die Erklärung mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist.“*

Damit begründete § 292a ZPO den gesetzlich normierten Anscheinsbeweis für die Echtheit der elektronischen Willenserklärung, also dafür, dass die Willenserklärung tatsächlich von dem in ihr benannten Absender stammte. Durch das Justizkommunikationsgesetz[774] wurde § 292a ZPO aufgehoben und durch § 371a ZPO ersetzt. Abs. 1 lautet:

---

[770] Berger, NJW 2005, S. 1016; Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 512, 513. Dabei gibt es mangels körperlicher Identität kein Erfordernis zur Vorlage des elektronischen Dokuments im Original wie für den Urkundsbeweis, ders. S. 513. Anders ist dies für Datenträger, auf die § 420 ZPO Anwendung findet, ders. ebenda. Hoffmann, DSWR 2006, S. 62. Siehe hierzu auch die Beweisvorschriften in England und den USA zur Vorlage des Originals (1.3.2.4 und 1.3.3.5).

[771] Geis, MMR 2000, S. 672.

[772] Diese Tatsache, ist dann Gegenstand der freien Beweiswürdigung des Gerichts; Geis, MMR 2000, S. 672.

[773] Die RLeS sieht eine solche Vermutungsregel nicht vor. Sie verlangt lediglich, dass elektronische Signaturen, die den qualifizierten elektronischen Signaturen des SigG entsprechen, die rechtlichen Anforderungen an die eigenhändige Unterschrift in gleicher Weise erfüllen, bzw. definiert die fortgeschrittene elektronische Signatur so, dass an sie (unter Erfüllung weiterer Aspekte) eine Sicherheitsvermutung geknüpft werden kann, Art. 5 Abs. 1 lit. a) und 2 Nr. 2 RLeS

[774] Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (JKomG), BGBl. I, S. 837.

„Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist."

Damit ist die Beweisfunktion der elektronischen Form zu Gunsten des Empfängers bekräftigt worden. Auf private elektronische Dokumente, die nicht mit einer qualifizierten elektronischen Signatur versehen sind, soll § 371a nicht, auch nicht analog, anwendbar sein.[775] Soweit aber ein elektronisches Dokument also mit einer qualifizierten elektronischen Signatur erstellt worden ist, kommt ihm die Beweiskraft der Privaturkunde, § 416 ZPO, zu, womit § 371a ZPO einen Schritt weiter geht als § 292a ZPO.[776] Wie die Privaturkunde beweist das elektronische Dokument mit qualifizierter elektronischer Signatur dabei zunächst nur, dass der in ihr enthaltene Text beziehungsweise die Erklärung in dieser Form von dem benannten Aussteller stammt.[777] Ob damit auch bewiesen ist, dass das Dokument willentlich vom Aussteller in den Verkehr gebracht wurde, ist nur dann bewiesen, wenn die Abgabe beziehungsweise Übermittlung des Dokuments zwingend mit dessen digitaler Signierung erfolgt.[778] Keinen Beweis per se liefert es hingegen für die Wahrheit der enthaltenen Information.[779] Für die qualifizierte elektronische Signatur wird damit aber – anders als bei der eigenhändigen Unterschrift – vermutet und muss nicht zwingend bewiesen werden, dass sie vom Aussteller herrührt.[780] Dabei handelt es sich bei § 371a ZPO nicht um eine Beweislastumkehr, sondern eine Beweiserleichterung. Der Empfänger soll, entsprechend den für den Beweis des ersten Anscheins von der Rechtsprechung entwickelten Grundsätzen[781], den Nachweis, dass die Erklärung von dem Signaturschlüssel-Inhaber abgegeben worden ist, grundsätzlich schon durch eine Überprüfung der Signatur nach dem SigG durch die Überprüfung der Zuordnung des Signaturprüfschlüssels erbringen können.[782] Hier geht es allerdings nicht um einen, wie bei dem von der Rechtsprechung begründeten Anscheinsbeweis, für die zu bewei-

[775] Klein, „Die Beweiskraft elektronischer Verträge", JurPC Web-Dok. 198/2007, abs. 1-71, Abs. 57; siehe auch unten 3.3.10.2.

[776] Hoffmann, DSWR 2006, S. 61; Huber in Musielak, § 371a, Rn. 1.

[777] Hoffmann, DSWR 2006, S. 61.

[778] So zutreffend Hoffmann, DSWR 2006, S. 61, der sich für eine Bindung des Gerichts auch dahingehend ausspricht, sofern der Automatismus „Verschlüsselung = Versand" sich aus dem elektronischen Dokument selbst ergebe. A.A. Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 514 f., der die Abgabe des elektronischen Dokuments hier als bewiesen ansieht, sich dabei auf den alten § 291a ZPO bezieht. Zum Nachweis des Zugangs: Schneider, *Handbuch des EDV-Rechts*, Köln 2003, B Rn. 779-793, S. 311 ff.

[779] Hoffmann, DSWR 2006, S. 61.

[780] Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 12.

[781] So die Gesetzesbegründungen für § 292a, BT-Drucks. 14/4987, S. 24, und § 371a ZPO, BT-Drucks. 15/4067, S. 34.

[782] Huber in Musielak, § 371a, Rn. 6.

sende Tatsache nach der Lebenserfahrung typischen Geschehensablauf. Der hier geregelte Anschein beruht nicht auf Erfahrungswissen, sondern auf einer gesetzlichen Vorgabe und ist Beweisregel im Sinne des § 286 Abs. 2 ZPO.[783]
Die Vorschrift soll den Erklärungsempfänger als die regelmäßig beweispflichtige Partei vor unbegründeten Einwänden des Signaturausstellers schützen. Der Signaturaussteller könnte nämlich behaupten, die Erklärung stamme nicht von ihm, sei ohne sein Wissen abgesandt oder während der Übermittlung verfälscht worden.[784] Das Risiko liegt folglich beim Inhaber der elektronischen Signatur.[785] Ob aber eine qualifizierte elektronische Signatur eingesetzt wurde, muss der Erklärungsempfänger beweisen, was ihm vor allem bei vorliegender Akkreditierung des Zertifizierungsdiensteanbieters, also der sog. „akkreditierten" Signatur, gelingen dürfte.[786] Es genügt die Erschütterung des durch § 371a ZPO angeordneten Anscheins durch den Beweisgegner, die signierte Erklärung stamme vom vermeidlich Erklärenden.[787] „Ernstliche Zweifel" können sich insbesondere aus einer unbefugten Verwendung des Signaturschlüssels oder aus dem Signieren anderer Daten als die eigentlich gewollten ergeben. Da die Erzeugung der Signatur neben dem Wissen der PIN auch den Besitz der Signaturerstellungseinheit (Haben) voraussetzt, ist also beispielsweise der Nachweis deren Abhandenkommens erforderlich.[788]
Eine weitergehende Auseinandersetzung mit § 371a ZPO erfolgt unten unter 3.2.2.4.
Gemäß § 371a Abs. 2 ZPO[789] finden auf „öffentliche elektronische Dokumente", §§ 3a, 33, 37 Verwaltungsverfahrensgesetz (VwVfG), § 130 ZPO, die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Dies sind die allgemeinen Beweiskraftregeln der §§ 415, 417 und 418 ZPO sowie diejenigen zum gerichtlichen Protokoll, § 165 ZPO) und Urteilstatbestand, § 314 ZPO.[790] Öffentliche Dokumen-

[783] Huber in Musielak, § 371a, Rn. 7.

[784] Huber in Musielak, § 371a, Rn. 6.

[785] Geis, MMR 2000, S. 672.

[786] Geis, „Die neue Signaturverordnung: Das Sicherheitssystem für die elektronische Kommunikation", K&R 2002, S. 59-61, S. 61; Huber in Musielak, § 371a, Rn. 9; Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 12, 36. Zur Zurechnung der Signatur bei der elektronischen Form bei Nutzung durch den legitimierten oder unbefugten Dritten (Handeln unter fremden Namen, Haftung wegen fahrlässig verursachten Rechtsscheins) aufgrund der Beweiserleichterung des § 292a ZPO siehe ders., Rn. 14, 15; Greger, Reinhard in Zöller, § 292a, Rn. 3. Dazu ausführlicher unten unter 3.2.2., insbesondere 3.2.2.4.

[787] Greger in Zöller, § 292a, Rn. 2; Siehe auch Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 515, 516, der anzweifelt, ob sich nach den allgemeinen, von der Rechtsprechung und der Literatur entwickelten Grundsätzen über den Anscheinsbeweis aus der Verwendung eines geheimen Signaturschlüssels ein Anscheinsbeweis für die Urheberschaft des Schlüsselinhabers ergibt (dazu auch unten ausführlich unter 3.2.2.4).

[788] Huber in Musielak, § 371a, Rn. 10; Roßnagel, Alexander / Fischer-Dieskau, Stefanie, „Elektronische Dokumente als Beweismittel - Neufassung der Beweisregelungen durch das Justizkommunikationsgesetz", NJW 2006, S. 806-808, S. 807.

[789] § 371a Abs. 2 ZPO: *„Auf elektronische Dokumente, die von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden ist (öffentliche elektronische Dokumente), finden die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Ist das Dokument mit einer qualifizierten elektronischen Signatur versehen, gilt § 437 [ZPO] entsprechend."*

[790] Huber in Musielak, § 371a, Rn. 11.

te, die mit einer qualifizierten elektronischen Signatur versehen ist, soll durch entsprechende Anwendung des § 437 ZPO die Vermutung der Echtheit gewährt werden.[791]

2.3.6 Weitere Gesetzesänderungen

Weitere Gesetzesänderungen betreffen die vorsichtige Öffnung von Grundbuchordnung, mehreren Gerichtsordnungen, des Handelsgesetzbuchs etc.[792] sowie insbesondere des öffentlichen Rechts für die neuen Kommunikationsformen.[793] Über das 2005 verabschiedete JKomG findet die qualifizierte elektronische Signatur unter anderem Anwendung als Prozesshandlung im Sinne eines Äquivalents zu schriftlichen Mitteilungen.[794] In Gerichtsverfahren wurde die Möglichkeit geschaffen, Erklärungen etc. in elektronischer Form abzugeben. Der neu eingefügte § 130a Abs. 1 ZPO lautet:

> *„Soweit für vorbereitende Schriftsätze und deren Anlagen, Anträge und Erklärungen der Parteien sowie für Auskünfte, Aussagen, Gutachten und Erklärungen Dritter die Schriftform vorgesehen ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn dieses für die Bearbeitung durch das Gericht geeignet ist. Die verantwortende Person soll das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.“*[795]

Hierbei handelt es sich um eine „Soll“-Vorschrift, die jedoch nach dem Willen des Gesetzgebers ein zwingendes Erfordernis darstellt, das im Interesse des Absenders gewährleisten soll, dass das Dokument nicht spurlos manipuliert werden kann[796] – wobei bezweifelt werden darf, wie wahrscheinlich und aufgrund welcher Motivation eine solche Manipulation insbesondere bei Gericht ist.
Auch die Verwaltungsverfahrensgesetze (VwVfG) des Bundes wurden für die elektronische Kommunikation auf der Basis qualifizierter elektronischer Signaturen geöffnet

[791] Huber in Musielak, § 371a, Rn. 12.

[792] Zum Beispiel die Beschwerde nach § 73 Abs. 2 Grundbuchordnung, Art. 5a Nr. 1 FormG und § 73 Abs. 2 S. 2 GBO n.F.

[793] Einführung der qualifizierten elektronischen Signatur in § 3a VwVfG, § 77a Abs. 1 Finanzgerichtsordnung, § 108a Abs. 1 Sozialgerichtsgesetz. Im Steuerrecht verlangt § 14 Abs. 3 Nr. 1 Umsatzsteuergesetz die Verwendung der akkreditierten elektronischen Signatur.

[794] Umfangreiche Gesetzesänderungen aufgrund des Justizkommunikationsgesetzes (JKomG), z.B. in §§ 130a, 130b, 298, 298a, 299, 371a, 416a, 758a, 829 ZPO sowie des Ordnungswidrigkeitengesetz u.a., siehe umfassende Darstellung in Viefhues, „Referentenentwurf des Justizkommunikationsgesetz (JKomG)“, CR 2003, S. 541-548.

[795] Näheres bestimmen die Bundesregierung und die Landesregierungen durch Rechtsverordnungen, Abs. 2. Gleiches wurde auch für die anderen Gerichtswege eingeführt. Siehe auch Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 9, der im Prozess- und öffentlichen Recht das Hauptanwendungsfeld der elektronischen Form sieht; Splittgerber, CR 2003, S.26, 27. Siehe auch § 86a Verwaltungsgerichtsordnung, § 46b Arbeitsgerichtsgesetz.

[796] Stadler in Musielak, § 130a, Rn. 3.

und entsprechend angepasst (Stichwort „elektronischer Verwaltungsakt“).[797] Gemäß dem neu eingefügten § 3a Abs. 1 VwVfG ist die Übermittlung elektronischer Dokumente durch die Behörde zulässig, soweit der Empfänger hierfür einen Zugang eröffnet. Eine durch Rechtsvorschrift angeordnete Schriftform kann laut Abs. 2, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Laut dem geänderten § 37 Abs. 2 S. 1 VwVfG soll ein Verwaltungsakt schriftlich, elektronisch, mündlich oder in anderer Weise, zum Beispiel als elektronischer Verwaltungsakt, erlassen werden, wobei mit letzterem ein neuer Verwaltungsaktstypus eingeführt wurde. Laut § 37 Abs. 2 S. 2 VwVfG soll ein mündlich ergangener Verwaltungsakt von der Behörde schriftlich oder elektronisch bestätigt werden, wenn hieran ein berechtigtes Interesse besteht und der Betroffene dies unverzüglich verlangt. Dabei ist eine qualifizierte elektronische Signatur gerade nicht erforderlich. Das Gesetz unterscheidet dabei also zwischen elektronischer Form und elektronischen Dokumenten, die jedoch nicht definiert werden.[798]

2.3.7 Zusammenfassung und Kritik

Die Gesetzgebung zur Regelung der digitalen Signatur übernahm sämtliche Vorgaben der RLeS und ergänzte und erweiterte sie hinsichtlich der technisch-organisatorischen Anforderungen an Signaturverfahren und Komponenten, Zertifizierungsdienste und Sicherheitsinfrastruktur. Das SigG n.F., aufbauend auf den SigG a.F., nutzte dabei den durch die EU-Richtlinien gewährten Freiraum in der Ausgestaltung der Signaturregelungen.[799] Das SigG n.F. ging zum Beispiel regulativ über die RLeS hinaus indem es die bereits zuvor bestehende Bundesnetzagentur als Wurzelzertifizierungsinstanz vorsieht und alle in der RLeS und ihren Anhängen genannten technisch-organisatorischen Anforderungen als allgemein verpflichtend und haftungsbewehrt ausgestaltete. Die Haftungsregelungen nahmen alle sicherheitsrelevanten Anforderungen als Tatbestände auf, zudem wurden weitere Anforderungen hinzugefügt. Verschlüsselungsdienste wurden in eine umfassende, gesetzlich festgelegte Prüf- und Überwachungsstruktur eingebunden. Anstelle der vormals geforderten, nun aber durch die RLeS ausgeschlossene Vorabprüfung der Diensteanbieter und ihrer Verfahren und Komponenten trat die freiwillige Akkreditierung der Zertifizierungsdienste. Folge der Abkehr von der zwingenden Vorabprüfung war allerdings eine Abstufung minderer Sicherheit, die sich in unterschiedlichen Qualitäten von Zertifizierungsstellen und Signaturen widerspiegelt.[800] Trotz dieser Neuregelungen wurde bezweifelt, ob die qualifizierte elektronische Signatur tatsächlich

[797] Ausführliche Darstellung zum sog. 3. Verwaltungsverfahrens-Änderungsgesetz z.B. bei Storr, „Elektronische Kommunikation in der öffentlichen Verwaltung – Die Einführung des elektronischen Verwaltungsakts“, MMR 2002, S. 579-584.

[798] Storr, MMR 2002, S. 581, der als solche elektronischen Dokumente solche ansehen will, die nicht papierbezogen sind und bei denen zumindest kein automatischer Papierausdruck erfolgt.

[799] Siehe dazu auch 3.1.1.

[800] So Scheffler/Dressel, CR 2000, S. 382, nach denen dies daraus folgen könne, dass bereits nach dem SigG a.F. genehmigte Zertifizierungsdiensteanbieter jetzt als akkreditiert nach dem SigG n.F. gelten.

allein den Beweis für die Unverfälschtheit des elektronischen Dokuments und für die Urheberschaft erbringen kann.[801]

Die deutsche Signaturgesetzgebung ist ein klassischer Vertreter eines sehr stark regulativen Ansatzes. Aus rein deutscher Sicht mag das neue SigG als tragfähige Grundlage für den elektronischen Rechtsverkehr angesehen werden. Der Vergleich mit den Signaturregelungen des Bundesgesetzgebers in den USA und insbesondere mit den englischen Neuregelungen zur elektronischen Signatur und der Änderung von Formerfordernissen wird zeigen, wie umfassend, regulativ und letztlich auch auf eine Technologie beschränkt das deutsche Signaturrecht ist. Schon vor dem Hintergrund der zum Beispiel mit RLeC und RLeS beabsichtigten Harmonisierung war der Ruf nach weiterer Ergänzung des SigG[802] deshalb nicht verständlich und nicht förderlich. Parallel wird dabei die digitale Signatur als auf der qualifizierten elektronischen Signatur fußenden elektronischen Form als einziges Substitut für die gesetzlich geforderte Schriftform gemäß § 126 BGB definiert. Gesetzliche Form- und Beweiskraftregelungen sind ebenfalls ausschließlich auf diese bezogen. Allein in der Einführung der Textform versucht der Gesetzgeber dem Bedarf nach geringerer Formenstrenge im Rechtsverkehr nachzukommen. Vor dem Hintergrund der zuvor bereits existierenden teilweisen Aufweichungen der strengen Schriftform für bestimmte Rechtsgeschäfte oder rechtserhebliche Erklärungen war die Einführung der Textform als einer besonderen Form nicht notwendig, aber doch zweckmäßig und klärend. Zum einen ist hier festzuhalten, dass die qualifizierte und unter Umständen auch die akkreditierte elektronische Signatur trotz des enormen sicherheitstechnischen und organisatorischen Aufwandes, der für sie betrieben werden muss, nicht immer und nicht notwendig die ihr zugesprochene Vertrauenswürdigkeit aufweist.[803] Einfacheren elektronischen Kommunikationsformen, etwa der Kommunikation mittels E-Mail über das Internet, wird außer über den § 127 BGB, durch diese Gesetzgebung die Möglichkeit der Formerfüllung genommen. Die Rechtsprechung verweigert ihr zudem jeglichen Beweiswert. Zum anderen ist auffällig, wie begrenzt der Anwendungsbereich der Textform nach dem ursprünglichen Willen des Gesetzgebers im Jahr 2001 sein sollte. Dabei ist aber in noch stärkerem Maße als bei der elektronischen Form zu bemängeln, dass die Textform nicht auf weitere Arten von Rechtsgeschäften ausgeweitet wurde.[804] Auch ohne den Blick auf die Bewertung vergleichbarer Kommunikationsformen durch die englischen und US-amerikanischen Gesetzgeber und Gerichte stellt sich daher die Frage, ob diese legislative Begrenzung und Einengung

[801] Sie bekomme aber im Zusammenspiel mit anderen Merkmalen eine hohe Beweiswirkung; Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 515. Siehe dazu auch unten ausführlich unter 3.2.

[802] Z.B. Lüdemann, „Die elektronische Signatur in der Rechtspraxis", K&R 2002, S. 8-12, S. 12; Roßnagel, K&R 2000, S. 323; Ulmer, CR 2002, S. 213. Siehe auch Peters, „E-Government – eine kleine Tour d´horizon", VR 2003, S. 68-74, S. 73, der aufgrund der verschiedenen Signaturstufen Verwirrung beim potentiellen Nutzer erkennt.

[803] Siehe unten unter 3.2.

[804] So auch Scheffler/Dressel, CR 2000, S. 380 u. 382 bis 384, die auch kritisierten, dass der Gesetzgeber die Warnfunktion durch sie erfüllt sehe, diese Einschätzung jedoch bezüglich einiger Vorschriften wieder zurücknehme. Auch wurde kritisiert, dass zwischen HGB und BGB unterschiedliche Formulierungen der Schriftform und der „lesbaren Form" entstanden, so Müglich, MMR 2000, S. 9/10. Siehe zum sehr eingeschränkten Anwendungsbereich der „elektronischen Form": Noack in Noack in Dauner-Lieb et al., *Das neue Schuldrecht in der anwaltlichen Praxis*, § 15, Rn. 40.

tatsächlich, jedenfalls aber in diesem Maße notwendig war und insbesondere, ob sie auch heute noch sachgerecht ist. Darüber hinaus zeigt schon der bisherige Vergleich[805], dass Erklärungen, die das Formerfordernis des § 126b BGB erfüllen, nach englischem und US-amerikanischem Recht vielfach (gesetzliche) Erfordernisse des *writing* und der *signature* erfüllten. Diesen wird aber zumeist die Erfüllung weiter reichender Formfunktionen als der Textform zugebilligt. Deshalb soll die legislative und judikative Reaktion in England und USA nachfolgend dargestellt werden. Eine nähere kritische Betrachtung zu den Schwächen der digitalen Signatur gerade auch unter deutschem Recht und zu einer möglichen Stärkung der Textform durch Übernahme von entsprechenden Rechtsregeln aus dem englischen und US-amerikanischen Recht folgt unter 3.2 und 3.3.

[805] Vergleiche oben 1.3.2.4 und 1.3.3.4.

2.4 Signaturregelungen und Änderungen der Formvorschriften in England

Grundsatz der Gesetzgebung in England war es, rechtlich nicht zwischen Geschäften auf traditioneller und auf elektronischer Weise zu unterscheiden, um den E-Commerce zu fördern.[806] Dennoch mussten die Vorgaben der RLeS und der RLeC über Gesetzgebung in nationales englisches Recht umgesetzt werden. Dies erfolgte zunächst mit dem Electronic Communications Act im Jahre 2000, der die Vorgaben der RLeS und RLeC nur teilweise aufnahm. Er sollte dennoch bereits eine ausreichende gesetzliche Basis für die Nutzung elektronischer Signaturen schaffen, vertraute aber im Übrigen auf Marktmechanismen und Selbstregulierungsinitiativen der Industrie – typisch für das *common law*. Im Jahre 2002 wurden weitere Rechtsverordnungen erlassen, die die zuvor noch nicht geregelten Teile der EU-Richtlinien umsetzten.[807] Erst damit bot nun auch England einen umfassenden gesetzlichen Rahmen. In 2003 folgten mit dem Communications Act 2003 einzelne Änderungen. Anschließend ergingen zur Umsetzung der vorgenannten Regelungen eine Vielzahl an Gesetzen und Rechtsverordnungen, um entsprechende Änderungen der betreffenden Vorschriften vorzunehmen.[808] Der hier favorisierte Regelungsansatz unterscheidet sich von demjenigen der RLeC und RLeS und insbesondere der deutschen Regelungen.

2.4.1 Umsetzungsbedarf hinsichtlich der EU-Richtlinien

Einen Umsetzungsbedarf hinsichtlich der Regelung des Art. 5 Abs. 1 lit. a) RLeS zur Gleichsetzung mit eigenhändigen Unterschriften auf Papier erkannte das Department Of Trade And Industry (DTI) zum damaligen Zeitpunkt zwar nicht[809], da elektronische Signaturen verschiedenster Formen, wie oben dargestellt (1.3.2.6), bereits in der Lage waren, (bestimmte) Signaturerfordernisse zu erfüllen.[810] Trotz der dargestellten großen Akzeptanz verschiedenster Formen der Unterschrift – auch der elektronischen Signatur – durch die englischen Gerichte, gab es Umstände, unter denen es fraglich war, ob elektronische Signaturen gesetzliche Unterschriftserfordernisse erfüllen konnten.[811] Veraltete Definitionen der Unterschrift (*signed*) und der schriftlichen Form (*writing*) waren hinderlich und ob *digitale* Signaturen Unterschriftserfordernisse wie etwa beim *deed* erfüllen konnten, war nicht geklärt.[812] Aufgrund der leichten Verfälschbarkeit wurde

---

[806] Und eine in diesem Sinne technikneutrale rechtliche Regelung zu bieten. Department Of Trade And Industry (DTI), „Building Confidence in Electronic Commerce – A Consultation Document", www.dti.gov.uk/cii/ecommerce/ukecommercestrategy/archiveconsultationdocs/index.shtml.

[807] Um dies herauszustellen und aufgrund der zeitlichen Verzögerung zwischen der Verabschiedung der genannten Gesetze soll die Darstellung chronologisch erfolgen.

[808] Ausführliche Auflistung der Rechtsverordnungen und Gesetze bei Mason, *Electronic Signatures in Law*, S. XXV ff.

[809] DTI, „Electronic Signatures & Associated Legislation", www.dti.gov.uk/cii/datasecurity/electronicsignatures/esd_note.shtml.

[810] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 658.

[811] DTI, „Building Confidence in Electronic Commerce – A Consultation Document".

[812] York/Tunkel, S. 79, 80, 91, 92.

auch in England als ungewiss angesehen, ob Gerichte elektronischen Signaturen großes Gewicht beimessen würden.[813] Der Bedarf an sicheren elektronischen Signaturen wurde als groß eingeschätzt und damit auch der Zwang, diesen Bereich gesetzlich zu regeln.[814] Die britische Regierung begrüßte daher die Verabschiedung der RLeS,[815] auch wenn das Department for Trade and Industry (DTI) die Auswirkungen der RLeS auf die Entwicklung von Authentifizierungsdiensten skeptisch einschätzte. Insgesamt wurde die RLeS in einem positiven Licht gesehen und sollte daher auch umgesetzt werden, allerdings mittels eines nur leichten regulativen Ansatzes, um den E-Commerce zu fördern anstatt ihn einzuschränken.[816] Dabei musste gesetzlich geregelt werden, dass elektronische Signaturen generell als Beweismittel zuzulassen sind (Art. 5 Abs. 1 lit. b) RLeS) und ihnen die Rechtswirkung nicht abgesprochen wird (Art. 5 Abs. 2 RLeS). Insbesondere die Regelungen des Art. 9 RLeC und Art. 3 Abs. 3 RLeS hinsichtlich des Überwachungssystems für Zertifizierungsdiensteanbieter waren in englisches Recht umzusetzen. Das bestehende Recht bot auch keine Haftungsregelung für Zertifizierungsdiensteanbieter wie die der RLeS.[817]

2.4.2 Electronic Communications Act 2000

Am 25 Mai 2000 erhielt der Electronic Communications Act 2000 (EC Act) die „königliche Genehmigung“ (*Royal Assent*) als Parlamentsgesetz.[818] Er besteht aus drei Teilen[819], von denen der erste und der zweite Teil hier dargestellt werden. Der erste, nie in

[813] Chissick, S. 83.

[814] Diesen Bedarf an sichereren digitalen Signaturen veranschaulicht *Standard Bank London v. The Bank of Tokyo Ltd.* [1995] CLC 496; [1996] 1 C.T.L.R. T-17: Danach durfte ein Empfänger eines *validated telex* (ein Telex mit einem geheimen Code) auf dieses vertrauen solange er nicht vom Gegenteil Kenntnis erlangte oder Grund für Zweifel an der Redlichkeit des Vertragspartners bestand. Diese Entscheidung bürdet dem Versender eine entscheidende Verantwortung dafür auf, die Codes oder Schlüssel zu sichern.

[815] DTI, „Building Confidence in Electronic Commerce – A Consultation Document”.

[816] DTI, „Discussion Document on Electronic Signatures Directive Implementing Regulations“, www.dti.gov.uk/cii/datasecurity/electronicsignatures/signatures.shtml; ausführlich hierzu Worthy/Anderson, „E-Commerce UK: UK Moves Towards Electronic Communications Bill”, CLSR 1999, S. 397-400, S. 398.

[817] DTI, „Electronic Signatures & Associated Legislation”; DTI, „Consultation Document on the Implementation of the EU Electronic Signatures Directive“, Absatz Nr. 40. www.dti.gov.uk/cii/ecommerce/europeanpolicy/esigncondoc.pdf;.

[818] Electronic Communications Act 2000, 2000 Chapter c. 7, vom 25.05.2000, entnommen aus: www.hmso.gov.uk/acts/acts2000/20000007.htm. Der Begriff *act* bezeichnet in England ein Gesetz, das durch ein gesetzgebendes Organ, d.i. hier das Parlament, gebilligt oder genehmigt wurde (*approved*) und damit zum Recht wird. Zum Gesetzgebungsverfahren in England (respektive Großbritannien) siehe ausführlich von Bernsdorff, S. 11 ff. Die Abkürzung „EC Act“, die nachfolgend verwendet wird, ist keine „offizielle“ oder in der einschlägigen Gesetzgebung oder Literatur gebräuchliche Abkürzung (wie beispielsweise der Begriff FormG in Deutschland). Sie dient hier lediglich der Vereinfachung.

[819] Teil I, Kryptographiediensteanbieter (§§ 1 bis 6) (Part I, „Cryptography Service Providers“), Teil II, „Erleichterung für den elektronischen Geschäftsverkehr, Datenspeicherung, etc.“ (§§ 7 bis 10) (Part II, „Facilitation of Electronic Commerce“), sowie Teil III, „Telekommunikationslizenzen und Anhang“ (§§ 11-16, wobei §§ 11 und 12 in 2003 aufgehoben wurden) (Part III, „Telecommunicatios Licenses and Supplemental“), der hier, mit Ausnahme der Darstellung einiger in ihm enthaltener Definitionen, nicht dargestellt wird.

Kraft getretene und mittlerweile aufgehobene Teil beschäftigt sich mit Kryptographie- oder Verschlüsselungsdiensteanbietern (*cryptography service providers*), deren Genehmigung und den damit zusammenhängenden Pflichten des Secretary of State, der zweite mit der rechtlichen Wirksamkeit und Beweistauglichkeit elektronischer Signaturen und der Änderung von Formvorschriften sowie mit den hiermit zusammenhängenden Ermächtigungen der Regierung.[820]

2.4.2.1 Regelungsziel und Begriffsbestimmungen

Ziel des englischen Gesetzgebers war es, den elektronischen Geschäftsverkehr zu erleichtern.[821] Wie bereits die Explanatory Notes zum Gesetzestext ausführen, sollen mit dem EC Act *„bestimmte Regelungen“* der RLeS, mithin nicht alle, in englisches Recht umgesetzt werden.[822] Dies ergibt sich neben dem oben Gesagten auch aus der Vorstellung über den Charakter einer entsprechenden rechtlichen Regelung, die von der der RLeS zugrunde liegenden verschieden ist.[823] Dennoch wurde die Bedeutung und Notwendigkeit des Vertrauens der Nutzer in die Sicherheit und Rechtmäßigkeit von Signatur- und Verschlüsselungsdiensten erkannt. Dieses Vertrauen sollte aufgebaut werden durch die Einführung einer Genehmigungsregelung (*approvals scheme*) für Verschlüsselungsdienste, die rechtliche Anerkennung elektronischer Signaturen und die Beseitigung von rechtlichen Hindernissen für die Nutzung elektronischer Kommunikation und Speicherung anstelle derjenigen in Papierform.[824]
Der englische Gesetzgeber bietet im EC Act in verschiedenen Teilen und Paragraphen des Gesetzes ebenfalls Bestimmungen von Begriffen, die im Rahmen der Kommunikation auf elektronischem Weg sowie der Signierung, Verschlüsselung und Speicherung von elektronischen Daten von Bedeutung sind. Im Vergleich zu den EU-Richtlinien und dem deutschen SigG sind diese Begriffsbestimmungen nicht erschöpfend hinsichtlich der Sicherheitsinfrastruktur und Funktionsweise elektronischer beziehungsweise digitaler Signaturen, wie dies die vorgenannten Regelungswerke zumindest anstreben. Insbesondere aber differieren sie vielfach im Vergleich zu denen der RLeS, RLeC und des

[820] Siehe eine Kurzzusammenfassung in: DTI, „The Guide to The Electronic Communications Act 2000” (Guide to EC Act), www.dti.gov.uk/cii/docs/e-com_guide.pdf. Einzelne nachfolgende Änderungen des EC Act betreffen größtenteils hier nicht relevante Regelungen.: § 4 Abs. 2 EC Act wurde durch den Regulation of Investigatory Powers Act 2000 geändert, der Communications Act 2003 änderte § 15 Abs. 1 EC Act und hob §§ 11 und 12 EC Act auf; Darstellung bei Mason, *Electronic Signatures in Law*, S. 185, 186.

[821] DTI, „Explanatory Notes to Electronic Communications Act 2000” (Explanatory Notes EC Act), Einleitung, www.hmso.gov.uk/acts/en/2000en07.htm; DTI, „Building Confidence in Electronic Commerce – A Consultation Document”.

[822] Explanatory Notes, Absatz Nr. 19; DTI, „Building Confidence in Electronic Commerce – A Consultation Document”.

[823] So stellt das DTI in den Explanatory Notes EC Act, Absatz Nr. 20, fest, dass das Ziel des EC Acts *„im Großen und Ganzen“* (*the broad aim*) ähnlich denen der RLeC sei, es jedoch in den einzelnen Vorschriften keine Übereinstimmung gebe. Ferner erkannte das DTI sogar einen gewissen Vorteil darin, auf diesem Gebiet unilateral zu handeln, anstatt zunächst internationale Abkommen anzustreben, „Building Confidence in Electronic Commerce – A Consultation Document”.

[824] Explanatory Notes, Absatz Nr. 6 und 7.

SigG und sind regelmäßig weiter gefasst. Dies deutet bereits auf den Regelungsansatz des englischen Gesetzgebers hin. Am Ende des EC Act werden die Begriffe Dokument, elektronische Mitteilung und Aufzeichnung bestimmt. Unter den Begriff Dokument (*document*) sind auch (Land-)Karten, Pläne, Designs (oder Muster), Zeichnungen etc. zu subsumieren.[825] Mitteilungen umfassen danach auch Geräusche und Töne (*sounds*), aber auch Bilder oder beides sowie die Anweisung von Zahlungen.[826] Diese Ausweitung der traditionellen Vorstellung von Dokumenten soll es ermöglichen, alle auch zukünftig sich ergebenden Möglichkeiten des *„information age"* zu nutzen.[827] Elektronische Mitteilung umschreibt solche mittels elektronischer Kommunikationsnetzwerke oder anderer, jedenfalls aber elektronischer Formen, die zwischen Personen, zwischen einem Gerät und einer Person oder sogar ausschließlich zwischen Geräten stattfinden.[828] Aufzeichnungen im Sinne des EC Act umfassen generell auch elektronische Aufzeichnungen. Ferner stellt der EC Act fest, was im Rahmen dieses Gesetzes unter einem Verweis auf die Authentizität beziehungsweise die Integrität von Mitteilungen und Daten zu verstehen ist. Ersteres seien Bezugnahmen unter anderem darauf,

> *„(i) ob eine Mitteilung oder Daten von einer bestimmten Person oder von einer anderen Quelle stammen;*
>
> *(ii) ob sie genau zeitlich bestimmt und datiert sind;*
>
> *(iii) ob sie rechtlich wirksam sein soll;...*"[829]

Bezugnahmen auf die Integrität von Mitteilungen und Daten sind solche auf eine etwaige Verfälschung oder Manipulation diese Mitteilungen oder Daten.[830] Sofern dabei und bei der Verschlüsselung von Daten etwas in lesbare Form gebracht werden soll, so ist darunter auch zu verstehen, dass etwas in den Zustand zurückgeführt wird, in dem es sich befand bevor es verschlüsselt wurde oder ein anderer Prozess darauf angewandt wurde.[831] Im Zusammenhang mit elektronischen Daten ist ein Schlüssel (*key*)

---

[825] § 15 Abs. 1 (am Anfang) EC Act: *„...'document' includes a map, plan, design, drawing, picture or other image;"*

[826] § 15 Abs. 1 EC Act: *„... 'communication' includes a communication comprising sounds or images or both and a communication effecting a payment;"*

[827] DTI, „Building Confidence in Electronic Commerce – A Consultation Document".

[828] § 15 Abs. 1 EC Act: *„... 'electronic communication' means a communication transmitted (whether from one person to another, from one device to another or from a person to a device or vice versa, (a) by means of a electronic communications network; or (b) by other means but while in an electronic from;"* Elektronisch ist sie, wenn sie über ein Telekommunikationssystem, oder über andere Mittel, jedoch in elektronischer Form, geschieht.

[829] § 15 Abs. 2 lit. a) EC Act: *„... references to the authenticity of any communication or data are references to any one or more of the following, (i) whether the communication or data comes from a particular person or other source; (ii) whether it is accurately timed and dated; (iii) whether it is intended to have legal effect;"*

[830] § 15 Abs. 2 lit. b) EC Act: *„... references to the integrity of any communication or data are references to whether there has been any tampering with or other modification of the communication or data."*

[831] § 15 Abs. 3 EC Act: *„References in this Act to something's being put into an intelligible form include references to its being restored to the condition in which it was before any encryption or similar process was applied to it."*

„jeder Code, Passwort, Algorithmus, Schlüssel oder Daten, deren Einsatz (mit oder ohne andere Schlüssel)

a) Zugang zu diesen elektronischen Daten gewährt, oder

b) es erleichtert, diese elektronischen Daten in lesbare Form zu bringen;“[832]

Diese Definition ist nicht identisch mit der der Signaturerstellungsdaten der RLeS, vor allem wird kein Bezug genommen auf die elektronische (oder digitale) Signatur, sondern allein auf die Verschlüsselung elektronischer Daten abgestellt. Dennoch gebraucht auch der EC Act den Begriff der elektronischen Signatur, der hier ebenfalls weiter ist als in der RLeS[833], § 7 Abs. 2 EC Act:

„Für die Zwecke dieses Paragraphen ist eine elektronische Signatur alles in elektronischer Form, das

a) in eine elektronische Mitteilung oder in elektronische Daten aufgenommen oder anders logisch mit ihnen verknüpft ist; und

b) vorgibt, so aufgenommen oder verknüpft zu sein, um der Feststellung der Authentizität der Mitteilung oder Daten, der Integrität der Mitteilung oder Daten, oder beidem zu dienen.“[834]

Beachtlich ist, dass die elektronische Signatur nach dieser Definition nicht nur zur Feststellung der Authentizität der Mitteilung oder Daten, sondern auch zur Feststellung deren Integrität dienen soll. Durch dieses zusätzliche Element wird ein engerer Fokus beschrieben als in der RLeS.[835] Der EC Act verlangt oder bezeichnet keine bestimmte Methode oder Format der elektronischen Signatur, soll somit technikneutral sein und alle Arten der elektronischen Signatur umfassen.[836] Unter § 7 Abs. 2 EC Act fällt z.B. auch die bloße Namensnennung in einer E-Mail, solange dies nach dem Willen des Unterzeichners als Mittel der Authentifizierung dienen soll, da dieser eingetippte Name dann zum Zwecke der Authentifizierung mit dem Inhalt des entsprechenden elektronischen Dokuments verbunden ist.[837] Der nachfolgende Abs. 3 des § 7 EC Act definiert, was unter Zertifizieren zu verstehen ist, gibt also eine Definition des Zertifikats:

---

[832] § 14 Abs. 3 S. 1 EC Act: *„In this section 'key', in relation to electronic data, means any code, password, algorithm, key or other data the use of which (with or without other keys), (a) allows access to the electronic data, or (b) facilitates the putting of the electronic data into an intelligible form;…"*

[833] Dort Art. 2 Nr. 1.

[834] § 7 Abs. 2 EC Act: *„For the purposes of this section an electronic signature is so much of anything in electronic form as (a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and (b) purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both."*

[835] Mason, *Electronic Signature in Law*, S. 189.

[836] Solche, die auf dem schlichten Austausch von E-Mails beruhen, die PKI zur Grundlage haben oder biometrischen Verfahren einsetzen; DTI, „The Guide to The Electronic Communications Act 2000".

[837] Mason, *Electronic Signature in Law*, S. 195, siehe auch unten unter 2.4.5.

> *„Im Sinne dieses Paragraphen ist eine elektronische Signatur* [nach Maßgabe des Abs. 2]*... durch eine Person zertifiziert, wenn diese Person (entweder vor oder nach der Abgabe der Mitteilung) bestätigt hat, dass*
>
> *a) die Signatur,*
>
> *b) ein Mittel der Herstellung, Übermittlung und Überprüfung der Signatur, oder*
>
> *c) ein auf die Signatur angewandtes Verfahren,*
>
> *(entweder einzeln oder in Kombination mit anderen Faktoren) ein gültiges Mittel der Feststellung der Authentizität der Mitteilung oder der Daten, der Integrität der Mitteilung oder der Daten, oder beidem, ist.“*[838]

Dies entspricht ebenfalls nicht der Definition aus Art. 2 Nr. 9 RLeS.[839] Teil 1 des EC Act sprach auch nicht von Zertifizierungsdiensteanbietern wie es das SigG und die RLeS tun. Als Kernelement der Infrastruktur der elektronischen Signatur war hier der Kryptographie-(oder Verschlüsselungs-)Unterstützungsdienst (*cryptography support service*), in § 6 Abs. 1 des 1. Teils des EC Act definiert als:

> *„… jeder Dienst, der den Absendern oder Empfängern elektronischer Mitteilungen oder denjenigen gegenüber geleistet wird, die elektronische Daten speichern, und der zur Nutzung von Verschlüsselungstechniken zu folgenden Zwecken geschaffen ist:*
>
> *a) der Gewährleistung, dass auf solche Mitteilungen oder Daten nur durch bestimmte Personen zugegriffen werden oder sie nur von bestimmten Personen in lesbare Form gebracht werden kann;*
>
> *b) der Gewährleistung, dass die Authentizität oder Integrität solcher Mitteilungen oder Daten festgestellt werden kann.“*

Dies ist ein sehr weiter Begriff,[840] vor allem weiter als der des Art. 2 Nr. 11 RLeS. Allerdings entsprechen die hier genannten Zwecke, zu denen diese Dienste eingesetzt werden sollten, den Anforderungen, die die RLeS an fortgeschrittene elektronische Signaturen stellt.[841] Ebenso wie die anderen Vorschriften des 1. Teils des EC Act ist dieser § 6 jedoch nie in Kraft getreten, siehe nachfolgende Darstellung.

---

[838] § 7 Abs. 3 EC Act: *„For the purposes of this section an electronic signature… is certified by any person if that person (whether before or after the making of the communication) has made a statement confirming that (a) the signature, (b) a means of producing, communicating or verifying the signature, or (c) a procedure applied to the signature, is (either alone or in combination with other factors) a valid means of establishing the authenticity… , the integrity…, or both.”*

[839] Wenn auch die lit. b) und c) sich an die Nr. 4 (Signaturerstellungsdaten) und 7 (Signaturprüfdaten), die wiederum in Bezug zu Nr. 9 (Zertifikat) stehen, anzulehnen scheinen.

[840] Crichard, CLSR 2000, S. 397.

[841] Dort Art. 2 Nr. 2 lit. c) sowie b) und d) RLeS.

2.4.2.2 Teil 1 EC Act – Zertifizierungsdiensteanbieter

Auch der englische Gesetzgeber hatte mit der Verabschiedung von Teil 1 des EC Act zunächst die Möglichkeit vorgesehen, ein Genehmigungs- oder Lizenzierungssystem (*licensing scheme*) einzuführen und Kriterien aufzustellen, die von genehmigten (*approved*) Kryptographie-Service-Providern erfüllt werden müssen.[842] Eine dahingehende Verpflichtung wurde jedoch abgelehnt.[843] Gesetzliche Akkreditierungsregelungen sollten vielmehr in Form eines selbstregulativen, freiwilligen, Gütezeichen verleihenden (*kite-market*) Verfahrens geschaffen werden mit einem Verzeichnis genehmigter Kryptographie-Service-Povider.[844] Dieser Teil 1 des EC Act ist mittlerweile, ohne jemals in Kraft getreten zu sein, aufgehoben worden. Seine Regelungen sollen hier jedoch trotzdem kurz dargestellt werden.[845]

§ 1 Abs. 1 des ersten Teils des EC Act verpflichtete den Secretary of State[846], für solche genehmigte *cryptography support services* ein Verzeichnis (*register*) aufzustellen und zu unterhalten.[847] Darunter ist nicht ein Genehmigungsverfahren wie nach dem SigG a.F. zu verstehen, sondern es ist eher im Sinne von Billigung, Zustimmung oder Akkreditierung (*approved*) zu deuten. Die Aufnahme in dieses Verzeichnis sollte freiwillig und kein Diensteanbieter verpflichtet sein, eine solche Genehmigung zu beantragen. Auch nicht derart akkreditierte Diensteanbieter sollten frei sein, Verschlüsselungsdienste anzubieten.[848] Ziel war es, ein öffentliches Verzeichnis vorzuhalten, aus dem sich ersehen lässt, dass bestimmte *cryptography support services* von einer unabhängigen Stelle nach bestimmten Standards geprüft wurden.[849] Diese Vorabprüfung sollte es den Anbietern ermöglichen, Zertifikate zur Unterstützung elektronischer Signaturen anzubieten, die vertrauenswürdig genug sind, um sie als gleichwertig zur (hand-) schriftlichen (*written*) Signatur anzuerkennen.[850] Folglich sollte das Genehmigungsverfahren so ausgestaltet werden, dass eine elektronische Signatur, die auf einem solchen Zertifikat beruht, die an ein Äquivalent zur (hand-)schriftlichen Signatur zu stellenden Anforderungen erfüllt. Im Gerichtsverfahren sollte es dann einer Überprüfung der Erfüllung der technischen Anforderungen im Einzelfall nicht mehr bedürfen.[851] Im Übrigen aber setz-

[842] Der EC Act sollte dabei sogar bewusst weiter gehen als von der RLeS verlangt, DTI „Building Confidence in Electronic Commerce – A Consultation Document".

[843] DTI, „Consultation Document on the Implementation of the EU Electronic Signatures Directive", Absatz Nr. 6.

[844] Crichard, CLSR 2000, S. 397, 398; Frühere Vorschläge für eine gesetzliche freiwillige Lizenzierung wurden durch ein Genehmigungs-System ersetzt, dessen Einzelheiten durch Rechtsverordnungen festgesetzt werden sollen (siehe nachfolgende Darstellung), Worthy/Anderson, CLSR 1999, S. 398.

[845] Am 25. Mai 2005, näheres siehe nachfolgend.

[846] Der Begriff Secretary of State bezeichnet in Großbritannien einen Minister i.S. eines Leiters eines Ministeriums und Mitglieds der Regierung. In den USA bezeichnet der Begriff Secretary of State auf Bundesebene regelmäßig das Amt des Außenministers. Auf bundesstaatlicher Ebene ist damit der Leiter eines Ministeriums gemeint; PONS, *Fachwörterbuch Recht*, S. 326f., 102.

[847] § 1 Abs. 1 EC Act.

[848] Explanatory Notes EC Act, Absatz Nr. 24.

[849] Explanatory Notes EC Act, Absatz Nr. 22.

[850] DTI, „Building Confidence in Electronic Commerce – A Consultation Document".

[851] DTI, „Building Confidence in Electronic Commerce – A Consultation Document".

te der englische Gesetzgeber auf die Marktkräfte. Elektronischen Signaturen, die nicht von akkreditierten Anbietern stammen, soll gemäß der Maßgabe der RLeS die Rechtswirksamkeit nicht abgesprochen werden. Es sollte den Parteien überlassen sein, ob sie das höhere Risiko tragen wollen.[852] Eine Wurzelzertifizierungsinstanz war, wie auch in der RLeS, nicht vorgesehen.[853]
§ 1 EC Act sollte ferner regeln, welche Angaben über diese Dienste in dem Verzeichnis für die Zeit der Genehmigung enthalten sein müssen[854], sowie welche Anforderungen an das Verzeichnis und das Genehmigungsverfahren zu stellen seien.[855] Dies sollte ebenfalls in Form der Ermächtigung und Verpflichtung des Secretary of State geschehen, diese Vorgaben zu regeln. Bestimmungen sollten geschaffen werden über die Genehmigung der Diensteanbieter, die *cryptography support services* anbieten oder dies beabsichtigt, sowie über die hierfür zu erfüllenden Bedingungen.[856] Danach sollte der Antragsteller

> *„… a) bei der Leistung seiner Dienste, für die er die Genehmigung erhalten hat, die* [durch den Secretary of State] *vorgeschriebenen technischen oder anderen Anforderungen* [erfüllen]*;*
>
> *b) den* [so] *vorgeschriebenen Anforderungen an seine Person jetzt und zukünftig* [entsprechen]*;*
>
> *c) jetzt und zukünftig in der Lage und willens* [sein]*, alle Anforderungen, die der Secretary of State ihm in Form von Bedingungen der Genehmigung auferlegt, zu erfüllen; und*
>
> *d) auch sonst eine geeignete und fähige Person* [sein]*, um eine Genehmigung für solche Dienste zu erhalten.“*[857]

---

[852] DTI, „Building Confidence in Electronic Commerce – A Consultation Document".

[853] Coyle, „Still Waiting for a Critical Mass", ECLP 2001, S. 8-9, S. 8.

[854] Etwa zu Personalien, Dienstleistungen und Bedingungen der Genehmigung, § 1 Abs. 2 EC Act; und Abs. 3: *„The particulars that must be recorded in every entry in the register relating to an approved person are (a) the name and address of that person; (b) the services in respect of which that person is approved; and (c) the conditions of the approval."* Explanatory Notes EC Act, Absatz Nr. 21.

[855] § 1 Abs. 4 sowie § 2 EC Act.

[856] § 2 Abs. 1 EC Act: Explanatory Notes EC Act, Absatz Nr. 26. So müssen die Bestimmungen ferner zum Beispiel sicherstellen, dass die Genehmigung an Bedingungen geknüpft werden kann. § 2 Abs. 2 lit. c) EC Act: *„The arrangements must… (c) provide for an approval granted to any person to have effect subject to such conditions… as may be contained in the approval;…"*; lit. b) EC Act.

[857] § 2 Abs. 3 EC Act: *The condition that must be fulfilled before an approval is granted to any person is that the Secretary of State is satisfied that that person (a) will comply in providing the services in respect of which he is approved, with such technical and other requirements as may be prescribed; (b) is a person in relation to whom such other requirements as may be prescribed are, and will continue to be, satisfied; (c) is, and will continue to be, able and willing to comply with any requirements that the Secretary of State is proposing to impose by means of conditions of the approval; and (d) is otherwise a fit and proper person to be approved in respect of those services."* Eine Genehmigung kommt danach nicht in Betracht, wenn der Antragsteller gegen Bestimmungen des EC Act verstoßen hat, wegen Betrugs oder unredlichen Verhaltens verklagt wurde oder betrügerische oder unlautere Geschäftspraktiken anwendet. Explanatory Notes EC Act, Absatz Nr. 28. § 2 Abs. 4 erlaubt es, die Bedingungen der Erfüllung der Anforderungen an die Meinung einer zu bestimmenden Person zu knüpfen; Explanatory Notes EC Act, Absatz Nr. 29.

Darüber hinaus sollte der Secretary of State gemäß Abs. 3 ermächtigt sein, in Form von *regulations* (Satzungen, Rechtsvorschriften)[858] Anforderungen an den Antragsteller und die eingesetzte Technik zu bestimmen.[859] Die Genehmigung sollte letztlich abhängig sein von der Erfüllung dieser Anforderungen.[860] Ferner sollte der Secretary of State über *arrangements* Möglichkeiten der Einsichtnahme in das Verzeichnis und der Feststellung Rücknahme oder Modifizierung einer Genehmigung sicherstellen.[861] Er müsse Vorkehrungen für die Handhabung u.a. von Modifizierungen und Rücknahmen treffen.[862]

Nach dem Willen des Gesetzgebers sollte dieser Genehmigungsprozess zurücktreten hinter ein von der Industrie geführtes Verfahren. Hauptziel einer jeden privaten Initiative sei es, innerhalb bestehender Marktstandards zu funktionieren und in diese nur dort einzugreifen, wo es erforderlich scheint.[863] Auch die Industrie hatte sich für einen solchen selbstregulativen Ansatz ausgesprochen.[864] Die Regierung entschied sich folglich dafür, diesen ersten Teil des EC Act zunächst nicht in Kraft treten zu lassen und abzuwarten, wie die Versuche der Industrie zur Selbstregulierung verlaufen.[865] Zu diesem Zweck war von der Alliance for Electronic Business ein solches industriegeführtes Verfahren mit dem Namen tScheme ins Leben gerufen worden.[866] Zum Zeitpunkt der Ver-

---

[858] Hier muss unterschieden werden zwischen *statutory instrument*, *order* und *regulations*. *Regulations* ist ein Oberbegriff für Gesetze oder Vorschriften, die ein Minister erlässt und die anschließend dem Parlament zur Genehmigung übergeben werden. Ein *statutory instrument* ist eine Rechts- oder Ausführungsverordnung, genauer ein order, der Gesetzeskraft hat und durch einen Minister erlassen wurde, der hierzu in einem Parlamentsgesetz (*Act of Parliament*) ermächtigt wurde. Ein *order* ist eine solche Rechtsverordnung, die ihrerseits, wie die *regulations*, dennoch durch das Parlament beschlossen werden muss, um Rechtskraft zu erlangen. Siehe PONS, *Fachwörterbuch Recht*, S. 244, 302/303, 342.

[859] Explanatory Notes EC Act, Absatz Nr. 28. Abs. 5 bestimmt weiter, welcher Art die an eine Genehmigung möglicherweise zu knüpfenden Bedingungen sein können. Beispielsweise, bestimmte Informationen bereit zu stellen, § 2 Abs. 5 lit. a); Explanatory Notes, Absatz Nr. 30, siehe auch Nr. 31.

[860] Explanatory Notes EC Act, Absatz Nr. 34. Der Secretary of State ist ermächtigt, die in den §§ 1 und 2 EC Act genannten Genehmigungsaufgaben an ein öffentliches Gremium oder eine Behörde zu delegieren. § 3 Abs. 1 und 2 bis 4 EC Act, Abs. 5 ermächtigt den Secretary of State, gesetzliche Bestimmungen zu diesen Gremien oder Behörden durch Rechtsverordnungen (*order*) zu ändern und über das Parlament beschließen zu lassen. Siehe auch § 5 EC Act, der die Ermächtigung zum Erlass von untergeordneter Gesetze (*subordinant legislation*) regelt, sowie Explanatory Notes, Absatz Nr. 35 und 38.

[861] § 1 Abs. 4 EC Act: *„It shall be the duty of the Secretary of State to ensure that such arrangements are in force as he considers appropriate for (a) allowing the members of the public to inspect the contents of the register; and (b) securing that such publicity is given to any withdrawal or modification of an approval as will bring it to attention of persons likely to be interested in it."* § 2 Abs. 2 lit. e) und f) EC Act: *„The arrangements must… (e) make provisions for the handling of complaints and disputes…; (f) provide for the modification and withdrawal of approvals."*.

[862] § 2 EC Act; Explanatory Notes EC Act, Absatz Nr. 25.

[863] Siehe bei York/Tunkel, S. 92.

[864] Dazu Worthy/Anderson, CLSR 1999, S. 398.

[865] Crichard, CLSR 2000, S. 397, 398.

[866] tScheme ist ein mitgliedschaftlich organisiertes Projekt (*scheme*) für Kryptographieunterstützungsdienste, oder „electronic trust services", das Mindeststandards für deren Akkreditierung und Dienstleistungen sicherstellen soll; Explanatory Notes, Absatz Nr. 10. Es ist eine in Großbritannien eingetragene Aktiengesellschaft, die unter anderen durch die Alliance for Electronic Business, der Confederation of British Industry, der Federation of Electronics Industry und der Computer Services and Software Industry (CSSA) gegründet wurde. Siehe hierzu: DTI, „Electronic Signatures & Associated Legislation: tScheme", www.dti.gov.uk/cii/datasecurity/electronicsignatures/tscheme.html.

abschiedung des EC Acts hatte die Regierung nicht die Absicht, tatsächlich ein freiwilliges Akkreditierungssystem wie in der RLeC vorgeschlagen einzuführen. Vielmehr sollte tScheme die Ziele der RLeS und der durch die Mitgliedstaaten eingeführten Verfahren erfüllen.[867] Solange dies erreicht würde, sollte Teil 1 des EC Act nicht in Kraft treten.[868] Unterdessen wurde Teil 1 des EC Act, die §§ 1 bis 6 umfassend, am 25. Mai 2005 aufgehoben, da innerhalb des in § 16 Abs. 4 genannten Fünf-Jahres-Zeitraums kein für das Inkrafttreten dieses Teils erforderlicher *order* des Secretary of State ergangen war.[869]

2.4.2.3 Zulassung elektronischer Signaturen als Beweismittel

Teil 2 des EC Act regelt die Zulassung elektronischer Signaturen und Zertifikate vor den Gerichten sowie die Beseitigung rechtlicher Hemmnisse für elektronische Verträge. Für die oben definierten elektronischen Signaturen und Zertifikate[870] gilt gem. § 7 Abs. 1 EC Act:

> *„In jedem Gerichtsverfahren sollen*
>
> *a) elektronische Signaturen, die in eine bestimmte elektronische Mitteilung oder Daten integriert oder mit diesen logisch verknüpft sind und*
>
> *b) die durch eine Person vorgenommene Zertifizierungen dieser elektronischen Signaturen,*
>
> *sowohl hinsichtlich der Authentizität als auch der Integrität dieser Mitteilung oder Daten, als Beweismittel zugelassen sein.“*[871]

Im Sinne des EC Act bezieht sich die Bedeutung der *authenticity* auf den einzigen Aspekt der Verifizierung der Person wie in § 15 Abs. 2 EC Act aufgeführt.[872] Diese Regelung entspricht zwar nicht der Vorgabe der RLeS, da der EC Act nicht auf eine fortgeschrittene elektronische Signatur oder eine Signatur mit vergleichbaren Eigenschaften

---

[867] DTI, „Consultation Document on the Implementation of the EU Electronic Signatures Directive“, Absatz Nr. 8.

[868] Diese Möglichkeit des Rückgriffs auf ein gesetzliches Verfahren, falls die Selbstregulierung nicht funktioniere, garantiere die Qualität elektronischer Signaturen und anderer Verschlüsselungsunterstützungsdienste; DTI, „The Guide to The Electronic Communications Act 2000”, Explanatory Notes, Absatz Nr. 10.

[869] Mason, *Electronic Signatures in Law*, S. 185.

[870] Siehe oben 2.4.2.2.

[871] § 7 Abs. 1 EC Act: *„ In any legal proceedings (a) an electronic signature…, and (b) the certification by any person of such signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data.”* Hiermit wird zunächst die in Art 5 Abs. 2 RLeS verlangte Zulassung als Beweismittel geregelt; Explanatory Note zu den Electronic Signatures Regulations 2002, www.legislation.hmso.gov.uk/si/si2002/20020318.htm. DTI, „Electronic Signatures & Associated Legislation”, www.dti.gov.uk/cii/datasecurity/electronicsignatures/esd_note.shtml.

[872] Siehe oben 2.4.2.1; Mason, *Electronic Signatures in Law*, S. 468.

abstellt. Dennoch sind danach elektronische Signaturen als Beweis in Bezug auf die Authentizität und/oder Integrität der Kommunikation zuzulassen. § 7 Abs. 1 EC Act behandelt dabei allein die Zulassung elektronischer Signaturen als Beweis und regelt gerade nicht, ob sie ein gesetzliches Formerfordernis erfüllten.[873] Die RLeS stellt in Art. 5 Abs. 2 dagegen auf deren rechtliche Wirksamkeit ab. Dabei ist jedoch zu beachten, dass nach englischem Recht eine elektronische Signatur zunächst als Beweis zuzulassen ist bevor sie rechtswirksam werden kann. Auch behandelt § 7 Abs. 1 EC Act nicht die Frage der Echtheit der elektronischen Signatur und überlässt die Frage deren Beweiswerts den Gerichten.[874] Der Gesetzgeber erkannte folglich hinsichtlich Art. 5 Abs. 1 lit. a) RLeS auch keinen Umsetzungsbedarf, da dessen Regelung der bereits bestehenden Rechtslage entsprach. Denn Erfordernisse hinsichtlich der Signatur einer Erklärung (oder ähnlichem) konnten bereits durch elektronische Signaturen, einschließlich der fortgeschrittenen und qualifizierten elektronischen Signaturen, erfüllt werden.[875] Dennoch wurde vermutet, dass durch diese Regelung (neben weiteren, siehe nachfolgend) die Rechtsprechung die Integrität und Authentizität eines Dokuments aufgrund der digitalen Signatur als verifiziert ansehen werde.[876] Letztlich muss nach wie vor im Einzelfall anhand der vorliegenden Beweise entschieden werden, ob eine elektronische Signatur korrekt benutzt wurde und welcher Wert ihr zugemessen werden soll. Damit sollte sie mit der eigenhändigen Unterschrift insofern gleichgestellt sein, als über deren Beweiswert ebenfalls das Gericht im Einzelfall entscheidet.[877] Eine Sicherheitsvermutung wurde daher nicht eingeführt.[878] Grundsätzlich enthält die Regelung aber die Möglichkeit, eine widerlegbare Vermutung zu schaffen „*... sowohl hinsichtlich der Authentizität, als auch der Integrität...*“.[879] Voraussetzung ist allerdings, dass weitere Anforderungen an die elektronische Signatur gestellt werden, was erst nachfolgend mit den Electronic Signatures Regulations erfolgte.[880] Eine solche gesetzliche Vermutungsregel wurde letztlich bislang nicht eingeführt. Hinsichtlich der Beurteilung des Beweiswerts elektronischer Dokumente und Signaturen wird jedoch in direkter Bezugnahme auf das

[873] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 658; Mason, *Electronic Signatures in Law*, S. 193.

[874] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 658; Mason, *Electronic Signatures in Law*, S. 190.

[875] DTI, „Discussion Document on Electronic Signatures Directive Implementing Regulations“, www.dti.gov.uk/cii/datasecurity/electronicsignatures/signatures.shtml.; Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 658.

[876] York/Tunkel, S. 90.

[877] DTI, „The Guide to The Electronic Communications Act 2000”, Explanatory Notes, Absatz Nr. 10; Explanatory Notes EC Act, Absatz Nr. 44; York/Tunkel, S. 92. Das Recht der Parteien zu Vereinbarungen über die Bewertung der eingesetzten elektronischen Signaturen blieb unangetastet; Explanatory Notes EC Act, Absatz Nr. 44.; Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 658.

[878] Dieser Verzicht wurde in der Literatur teilweise als nicht weit reichend genug kritisiert, da somit die Existenz einer elektronischen Signatur nur *einer* der im Gerichtsverfahren in Betracht zu ziehenden Faktoren sei; so Crichard, CLSR 2000, S. 398. Das Konzept einer widerlegbaren Vermutung der rechtlichen Anerkennung für elektronische Signaturen aus den ersten Gesetzentwürfen war aufgegeben worden, ausführlich Worthy/Anderson, CLSR 1999, S. 398.

[879] DTI, „Building Confidence in Electronic Commerce – A Consultation Document”.

[880] DTI, „Building Confidence in Electronic Commerce – A Consultation Document”.

Modellgesetz der United Nations Commission on International Trade Law (UNCITRAL) zum Elektronischen Geschäftsverkehr (MLeC[881]) angenommen, dass die in Art. 9 Abs. 2 MLeC genannten Aspekte der Vertrauenswürdigkeit der Art und Weise der Generierung, Speicherung oder Übermittlung der Datennachricht berücksichtigt werden.[882] Die British Standards Institution hat in 2004 einen *Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically* herausgebracht, in dem unter anderem Mittel aufgezeigt werden, wie gegenüber den Gerichten in einer für diese akzeptablen Form nachgewiesen werden kann, dass die Inhalte bestimmter auf Computersystemen gespeicherten Dokumenten seit ihrer Aufzeichnung oder Speicherung nicht mehr verändert wurden, etc.[883]

2.4.2.4 Änderungen gesetzlicher Formvorschriften

§ 8 EC Act sollte es ermöglichen, Vorschriften anderer Gesetze, welche die Nutzung elektronischer Kommunikation oder elektronischer Speicherung behinderten, zu beseitigen sowie dort, wo elektronische Kommunikation und Speicherung bereits erlaubt waren, diese gesetzlich zu regeln.[884] Schriftform- und Unterschrifterfordernisse hatten sich über einen langen Zeitraum durch Recht und Gewohnheit gebildet, weshalb nicht mit einem einzigen Schritt die Gleichwertigkeit von traditionellen und elektronischen Mitteln der Kommunikation festgeschrieben werde sollte.[885] Die bestehenden gesetzlichen Formerfordernisse mittels einer allumfassenden Klausel zu ändern war also weder möglich noch erwünscht.[886] Die Law Commission for England and Wales hatte 2001 für das *writing*-Erfordernis sogar festgestellt, dass ein elektronisches Dokument dieses zwar möglicherweise nicht erfülle, wohl aber die Darstellung eines Dokuments auf dem Computerbildschirm. Die Tatsache, dass dieses Dokument unter Umständen gar nicht gelesen werde, berühre dessen Wirksamkeit nicht[887], was eine interessante Parallele aufweist zur Diskussion in Deutschland, ob die Textform durch eine Internetseite erfüllt werden kann.[888] Auch wird deutlich, dass zunächst die Entwicklung des elektronischen Geschäftsverkehrs und des Rechts hinsichtlich der Problematik der Formerfüllung beobachtet, keine unnötigen Hindernisse bereitet und die betroffenen Wirtschafts- und Verbraucherverbände konsultiert werden sollten. Hinsichtlich der Übersendung eines Dokuments in körperlicher Form (*physical transmission*), der Übertragung, Aushändi-

[881] Siehe unten unter 2.6.1.

[882] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 665.

[883] Siehe bei Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 665.

[884] Explanatory Notes EC Act, Absatz Nr. 47.

[885] DTI, „Building Confidence in Electronic Commerce – A Consultation Document". Auch gäbe es Fälle, in denen es nicht angebracht sei, elektronische Mittel neben den traditionellen zu erlauben.

[886] Mason, *Electronic Signatures in Law*, S. 193.

[887] The Law Commission, „Electronic Commerce: Formal Requirements in Commercial Transactions – Advice from the Law Commission", S. 9-11. Diese Sichtweise stimmt überein mit der in den USA herrschenden Ansicht, dass ein Dokument, das leicht ausgedruckt und gespeichert werden kann, *writing* darstellt, siehe bei Christensen/Low, ALJ 77:416, 2003, S. 3.

[888] Siehe oben 2.3.4.2, sowie unten

gung oder Veröffentlichung von Dokumenten in schriftlicher Form schien es dem Gesetzgeber dagegen angemessen, unter Berücksichtigung einiger Sicherheitsvorkehrungen, dies auch im Wege der elektronischen Kommunikation zu ermöglichen.[889] Der zuständige Minister (*appropriate Minister*) kann folglich durch Rechtsverordnungen (*order made by statutory instrument*) die Vorschriften

> *„a) jeder gesetzlichen Bestimmung oder untergeordneter Gesetzgebung oder*
>
> *b) jeder gemäß einer gesetzlichen Bestimmung oder eines untergeordneten Gesetzes ausgestellte, gewährte oder abgegebene Regelung, Lizenz, Genehmigung oder Bewilligung*
>
> *derart* [ab]*ändern, wie es ihm zur Authentifizierung oder Erleichterung der Nutzung elektronischer Kommunikation oder elektronischer Speicherung (an Stelle anderer Kommunikation oder Speicherung)... geeignet erscheint."*[890]

Diese Bestimmung ist enger als die des § 7 EC Act.[891] Die Ermächtigung des Ministers ist auf bestimmte Zwecke der elektronischen Kommunikation und Speicherung beschränkt. Dies sind

(a) Handlungen (*the doing of anything*), die in schriftlicher Form (*writing*) beziehungsweise mit Hilfe eines Dokuments, einer Notiz oder einer Urkunde ausgeführt oder bewiesen werden müssen;

(b) Mitteilungen, die auf dem Postwege oder mittels besonderer Zustellungsformen erfolgen müssen;

(c) solche, die mittels Unterschrift oder einem Siegel (*seal*, auch Stempel) authentifiziert oder in Form des deed ausgeführt (*delivered*) oder bezeugt werden müssen;

(d) Erklärungen, die unter Eid oder als eidesstattliche Versicherung abgegeben werden müssen; sowie

(e) die Aufbewahrung von Rechnungen, Aufzeichnungen, Notizen, Dokumenten oder anderer Dokumente gemäß bestimmter Rechtsverordnungen.[892]

---

[889] DTI, „Building Confidence in Electronic Commerce – A Consultation Document".

[890] § 8 Abs. 1 EC Act: *„... the appropriate Minister may by order made by statutory instrument modify the provisions of (a) any enactment or subordinate legislation, or (b) any scheme, licence, authorisation or approval issued, granted or given by or under any enactment or subordinate legislation, in such manner as he may think fit for the purpose of authorising or facilitating the use of electronic communications or electronic storage (instead of other forms…)…"*

[891] Explanatory Notes EC Act, Absatz Nr. 47. Die Befugnis könne selektiv genutzt werden, um die elektronische Option denjenigen anzubieten, die dies wünschen, Explanatory Notes EC Act, Absatz Nr. 47.

[892] § 8 Abs. 2 lit. a) bis e) EC Act. § 8 Abs. 1: *„... may... modify the provisions of... for the purpose of authorising or facilitating the use of electronic communications… for the purpose mentioned in subsection (2)."*, Abs. 2: *„Those purposes are (a) the doing of anything which under any such provisions is required to be or may be done or evidenced in writing or otherwise using a document, notice or instrument; (b)… is required to be or may be done by post or other specified means of delivery; (c) … is required to be or may be authorised by a person's signature or seal, or is required to be delivered as a deed or witnessed; (d) the making of any statement or declaration which under any such provisions is*

Insgesamt fällt eine große Anzahl von Bestimmungen in Gesetzen verschiedener Rechtsgebiete, die die Benutzung von Papier verlangen oder dahingehend interpretiert werden können, in diesen Anwendungsbereich.[893] Die Ermächtigung ist dabei beschränkt durch die Verpflichtung, solche Rechtsverordnungen nur zu erlassen, wenn die elektronische Kommunikation oder Speicherung nicht eine weniger zufrieden stellende Lösung darstellt.[894] Eine solche Rechtsverordnung darf zudem nicht den Gebrauch elektronischer Kommunikation oder elektronischer Speicherung vorschreiben.[895] Damit soll sichergestellt werden, dass zum Beispiel der elektronische Vertragsschluss nur denjenigen angeboten wird, die dies wollen[896] – ebenfalls ein strikter *opt-in*-Ansatz. Papierform und Postbrief bleiben die *„default option"* falls von dieser Option kein Gebrauch gemacht wird.[897] Diese Rechtsverordnungen können ferner Vorschriften zur Form der elektronischen Kommunikation, Mitteilung oder Speicherung enthalten[898], zum Beispiel gemäß § 8 Abs. 4 lit. (g):

> *„Vorschriften, in Bezug auf Fälle in denen die Verwendung elektronischer Kommunikation oder elektronischer Speicherung so autorisiert ist, für die Bestimmung der in Abs. 5 genannten Umstände oder der Art in der sie in Gerichtsverfahren bewiesen werden;"*[899]

Ebenso dürfen die Rechtsverordnungen an die elektronische Kommunikation, Mitteilung oder Speicherung Bedingungen stellen, die Nutzung elektronischer Kommunikationen in Bezug auf deren Authentizität und Integrität regeln sowie diesbezüglich weitere

---

required to be made under oath or to be contained in a statutory declaration; (e) the keeping, maintenance or preservation, for the purposes or in pursuance of any such provisions, of any account, record, notice, instrument or other document; (f) the provision, production or publication under any such provisions of any information or other matter; (g) the making of any payment that is required to be or may be made under any such provisions." Diese Ermächtigung ist nicht beschränkt auf die Bestimmungen zu schriftlicher Information (siehe oben die Definition von Dokument und Kommunikation), Explanatory Notes EC Act, Absatz Nr. 48.

[893] Explanatory Notes EC Act, Absatz Nr. 48, 49. Die Mehrzahl der Vertragstypen fällt hingegen nicht in diese Kategorie.

[894] Entsprechende Rechtsverordnungen sollten nicht erlassen werden, solange eine zuverlässige Speicherung möglich ist, § 8 Abs. 3 EC Act; Explanatory Notes, Absatz Nr. 52; York/Tunkel, S. 81.

[895] § 8 Abs. 6 lit. a) EC Act, Explanatory Notes, Absatz Nr. 55.

[896] York/Tunkel, S. 81; § 8 Abs. 6 EC Act.

[897] Lloyd, S. 556ff., der einwandte, es sei abzuwarten, ob diese Grundregel sich umkehren werde.

[898] § 8 Abs. 4 EC Act: *„... the power to make an order under this section shall include power to make an order containing any of the following provisions, (a) provision as to the electronic form to be taken by any electronic communications or electronic storage...; (b) provision imposing conditions subject to which the use of electronic communications or... storage is so authorised;... (e) provision, in connection with any use of electronic communications so authorised,... for the transmission of any data or for establishing the authenticity or integrity of any data; (f) provision, in connection with any use of electronic storage so authorised, for persons satisfying such conditions... ; (j) provision requiring persons to prepare and keep records in connection with any use of electronic communications or electronic storage which is so authorised;..."*

[899] § 8 Abs. 4 lit. g) EC Act: *„provision, in relation to cases in which the use of electronic communications or electronic storage is so authorised, for the determination of any of the matters mentioned in subsection (5), or as to the manner in which they may be proved in legal proceedings;"*

Bereiche und Fragestellungen regeln.[900] Diese beiden Abs. 4 und 5 des § 8 EC Act zusammen geben dem Minister die Möglichkeit darüber zu bestimmen, wie elektronische Mitteilungen behandelt werden und welche Vermutungen bei ihrer Verwendung Anwendung finden sollen. Sie erlauben es dem Minister zum Beispiel, widerlegbare oder unwiderlegbare Vermutungen aufzustellen, die das Risiko von der auf die elektronische Mitteilung vertrauenden Partei auf den angeblichen Unterzeichner verlagern.[901]
Zuständig ist der Leiter des jeweiligen Ministeriums (*appropriate Minister*), in dessen Aufgabenbereich das jeweilige Rechtsgebiet fällt. Gegebenenfalls sollen mehrere Ministerien diese Ermächtigung gemeinschaftlich ausüben.[902] Auch hier wird wieder deutlich, dass es keine allgemeinen Formerfordernisse gibt, sondern alle relevanten Vorschriften einzeln abgeändert werden müssten. Der EC Act beschränkt sich darauf, diese Aufgabe den Ministerien anzuvertrauen, die dies nach eigener Erwägung durchführen, Rechtsverordnungen jedoch durch beide Kammern des Parlaments beschließen lassen sollen.[903] Diese Ermächtigung wurde favorisiert gegenüber der Möglichkeit, Formvorschriften durch Parlamentsgesetze einzeln zu ändern. Diese Regelung der teilweisen und graduellen Änderung sollte weniger zeitaufwendig sein und maßgeschneiderte Lösungen für einzelne Formvorschriften ermöglichen.[904] Beispiele dafür, wie die Ermächtigung der Minister genutzt wird, sind unter anderem im Companies Act 1985 zu finden, der noch im Jahre 2000 durch den Companies Act 1985 (Electronic Communications) Order 2000 (EC Order) geändert wurde.[905]

---

[900] Z.B. ob etwas mittels elektronischen Mitteilung oder Speicherung ausgeführt wurde; den Zeitpunkt oder das Datum, an dem dies ausgeführt wurde; den Ort wo... [dies] ausgeführt wurde; die Person durch die dies erfolgte oder den Inhalt, die Authentizität oder Integrität elektronischer Daten, § 8 Abs. 5 EC Act: *The matters referred to in subsection (4) (g) are (a) whether a thing has been done using an electronic communication or electronic storage; (b) the time at which, or date on which, a thing done using any such communication or storage was done; (c) the place where a thing done using such communication or storage was done; (d) the person by whom such a thing was done; and (e) the contents, authenticity or integrity of any electronic data."*

[901] Mason, *Electronic Signatures in Law*, S. 195.

[902] § 9 Abs. 1 und 2 EC Act. Genannt sind das Department of the Secretary of State, so dass dann dieser zuständig wäre, sowie the Treasury. Die Regierung verpflichtete sich, für ein koordinierten Vorgehen der verschiedenen Ministerien (*departments*) und entsprechende Vorgaben zu sorgen; Explanatory Notes, Absatz Nr. 50.

[903] § 9 Abs. 3 EC Act; Explanatory Notes, Absatz Nr. 58. Beachte die Differenzierung *statutory instrument*, *order* und *regulation* (in 2.4.2.2). § 9 EC Act enthält weitere Vorschriften, wie sie üblicherweise an solche Ermächtigungen zum Erlass nachrangiger Gesetze geknüpft werden, beispielsweise die Möglichkeit, ergänzende Vorschriften zu erlassen, Explanatory Notes, Absatz Nr. 57.

[904] DTI, „Building Confidence in Electronic Commerce – A Consultation Document". Es bestanden durchaus Zweifel an so weit reichenden Ermächtigungen zur nachrangigen Gesetzgebung. Skeptisch wurde beobachtet, in welchem Maß davon Gebrauch gemacht wurde, insbesondere hinsichtlich der erlaubten Ausnahmen für bestimmte Rechtsbereiche und Vertragstypen; siehe Brooks, ECLP 2001, S. 6.

[905] Statutory Instrument 2000 No. 3373, The Companies Act 1985 (Electronic Communications) Order 2000, vom 21. Dezember 2000, in Kraft seit dem 22. Dezember 2000, Text aus: www.legislation.hmso.gov.uk/si/si2000/2000333.htm. Eine Zusammenfassung siehe in York/Tunkel, S. 82, sowie in Hollywood (Steptoe & Johnson), „E-Communications Order 2000", www.steptoe.com/webdoc.nsf/Files/E-Commerce-order/$file/E-Comm-order.pdf. Eine ausführliche Auflistung der Rechtsverordnungen und Gesetze bei Mason, *Electronic Signatures in Law*, S. XXV ff. Die Abkürzung „EC Order" wird, wie auch die Abkürzung „EC Act", nur hier verwendet. Unternehmen ist es nun unter anderem erlaubt, Kapitalgesellschaften auf elektronischem Wege zu gründen, die Anmeldung zum Handelsregister, Kopien ihrer Jahresberichte etc. in elektronischer Form zu fassen und zu versenden oder elektronische Medien zur Kommunikation mit ihren Mitgliedern einzusetzen (Zur

2.4.3 Electronic Signatures Regulations 2002 und Electronic Commerce (EC Directive) Regulations 2002

Die Electronic Signatures Regulations 2002 (ES Reg.)[906], in Kraft seit dem 8. März 2002, sollten die RLeS in englisches Recht umsetzen. Die Art. 3, 5 bis 7 Abs. 1, 10 bis 14, 18 Abs. 2 und 20 RLeC werden dabei durch die Electronic Commerce (EC Directive) Regulations (EC Reg.)[907], größtenteils in Kraft seit dem 21. August 2002, umgesetzt.[908]

2.4.3.1 Begriffsbestimmungen

Die ES Reg. führten für ihren Anwendungsbereich die Begriffe elektronische Signatur und fortgeschrittene elektronische Signatur, Signaturerstellungs- und Signaturprüfdaten, Signaturerstellungs- und Signaturprüfeinheit, Zertifikat und qualifiziertes Zertifikat sowie die Begriffe Unterzeichner und Zertifizierungsdiensteanbieter ein und definieren diese nahezu identisch wie die RLeS.[909] Signaturerstellungsdaten (*signature-creation data*) sind dabei ausdrücklich nicht auf Codes oder private Schlüssel der PKI beschränkt.[910] Bezüglich der qualifizierten Zertifikate sind die Anhänge I und II der RLeS[911] wortgleich von den ES Reg. übernommen und ihr als Schedule 1 und Schedule 2 angehängt worden. Entsprechend verweist die Definition des qualifizierten Zertifikats auf diese Anforderungen. Auch den Begriff der freiwilligen Akkreditierung wie er in der RLeS definiert wird übernehmen die ES Reg.[912] Nicht übernommen worden sind

---

Unternehmenspublizität im deutschen Recht siehe ausführlich Noack, *Unternehmenspublizität: Bedeutung der Offenlegung von Unternehmensdaten*, Köln 2002, S. 58 f.).

[906] Statutory Instrument 2002 No. 318, „The Electronic Signatures Regulations 2002", vom 14. Februar 2002, Text aus: www.legislation.hmso.gov.uk/si/si2002/20020318.htm. Auch die Abkürzung „ES Reg." findet sich nur in vorliegendem Text.

[907] Statutory Instrument 2002 No. 2013, „The Electronic Commerce (EC Directive) Regulations 2002", vom 31. Juli 2002, Text aus: www.hmso.gov.uk/si/si2002/20022013.htm. Auch die Abkürzung „EC Reg." findet sich nur in vorliegendem Text.

[908] DTI, „Explanatory Note" zur ES Reg., www.legislation.hmso.gov.uk/si/si2002/20020318.htm; „Explanatory Note" zur EC Reg., www.hmso.gov.uk/si/si2002/20022013.htm. Die „Explanatory Note[s]" zu den EC Reg., www.hmso.gov.uk/si/si2002/20022013.htm, raten dazu, die EC Reg. im Zusammenhang mit der RLeC zu lesen, bzw. diese zur Auslegung heranzuziehen (*„These regulations should be read with the...* [RLeC]*..."*).

[909] § 2 ES Reg. Definiert *electronic signatures* und *advanced electronic signatures*, *signature-creation data* und *signature verification data*, *signature-creation device* und *signature-verification device*, *certificate* und *qualified certificate*, *signatory* und *certification-service-provider* wie es auch Art. 2 Nr. 1, 2, 4, 7, 5, 8, 9, 10, 3 und 11 RLeS tun.

[910] § 2 ES Reg.: *„... 'signature-creation data' means unique data (including, but not limited to, codes or private cryptographic keys) which are used by the signatory to create an electronic signature;..."*

[911] Siehe Art. 2 Nr. 10 und Anhänge I und I RLeS.

[912] § 2 ES Reg. Die ES Reg. übernahmen unter anderem die Bestimmungen der RLeC über allgemeine Informationspflichten und kommerzielle Kommunikation, §§ 6, 7 und 8 EC Reg. Bereits nach altem Recht bestanden die meisten dieser Informationspflichten, siehe Brooks, „E-Commerce Directive: The Task Ahead (Part 2)", ECLP 2001, S. 6-7, S. 6. Dazu kommen Informationspflichten etc. aus §§ 10 und 11 EC Reg. (Art. 10 und 11 RLeC), oder Vorschriften zur Verantwortlichkeit von Diensteanbietern in befassten §§ 17 bis 19 EC Reg. (Art. 12 bis 14 RLeC). Die in den §§ 6, 7, 8, 9 Abs. 1 und § 11 Abs. 1

die Begriffe der sicheren Signaturerstellungseinheit sowie der Produkte für elektronische Signaturen aus der RLeS.[913] Ebenfalls nicht übernommen wurden unter anderem die Bestimmungen der RLeS zur Anerkennung von qualifizierten Zertifikaten ausländischer, also nicht in England (beziehungsweise in Großbritannien) niedergelassener Zertifizierungsdiensteanbieter.[914] Allerdings unterscheidet das englische Recht nicht zwischen inländischen und ausländischen qualifizierten Zertifikaten.[915]

2.4.3.2 Überwachung und Haftung der Zertifizierungsdiensteanbieter

§ 3 ES Reg. erfüllt die Vorgabe des Art. 3 Abs. 3 RLeS und bestimmt wie die Zertifizierungsdiensteanbieter zu überwachen sind.[916] Hierzu wird wieder der Secretary of State verpflichtet, die Tätigkeit der Zertifizierungsdiensteanbieter, die (öffentliche) qualifizierte Zertifikate ausstellen, und der beteiligten Personen zu überprüfen.[917] Daneben soll er ein Verzeichnis einrichten und unterhalten für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen:[918]

> *„Der Secretary of State soll dabei die ihm zur Kenntnis gebrachten Beweise für Handlungen von... Zertifizierungsdiensteanbietern berücksichtigen, die seiner Ansicht nach die Interessen derjenigen Personen schädigen, die solche Zertifikate nutzen oder auf sie vertrauen, und er soll diese Beweise in einer ihm zweckmäßig erscheinenden Weise veröffentlichen."*[919]

EC Reg. dem Diensteanbieter auferlegten Pflichten sind durch den betroffenen Nutzer gerichtlich einklagbar im Wege der Schadensersatzklage aufgrund Verstoßes gegen eine gesetzliche Pflicht, § 13 EC Reg.

[913] Dort Art. 2 Nr. 6 und 12 RLeS. § 2 Abs. 1 EC Reg. seinerseits übernimmt die Begriffsbestimmungen des Art. 2 RleC, so die kommerzielle Kommunikation, Verbraucher, Diensteanbieter, Nutzer (hier *recipient of the service*), sowie koordinierter Bereich.

[914] Art. 7 RLeC. Auch hierfür besteht laut DTI kein Anlass, da dies gemäß der Definition des qualifizierten Zertifikats nicht davon abhinge, wo der Zertifizierungsdiensteanbieter, der es ausgestellt hat, niedergelassen sei; DTI, „Electronic Signatures & Associated Legislation". Ebenfalls kein Umsetzungsbedarf wurde hinsichtlich Art. 4 RLeS gesehen, da keine der im EC-Act enthaltenen Regelungen ein Binnenmarkthindernis o.ä. aufwerfen; DTI, „Consultation Document on the Implementation of the EU Electronic Signatures Directive", Absatz Nr. 35. www.dti.gov.uk/cii/e-commerce/europeanpolicy/esigncondoc.pdf.

[915] Dumortier et al., „The legal and market aspects of electronic signatures", DuD 2004, S. 141-146, S. 143.

[916] DTI, „Electronic Signatures & Associated Legislation".

[917] Etwa auf ihre Identität und die näheren Umstände ihres Tätigseins; § 3 Abs. 1 ES Reg.: *„It shall be the duty of the Secretary of State to keep under review the carrying on of activities of certification service providers… who issue qualified certificates to the public and the persons by whom they are carried on with a view her to* [/him] *becoming aware of the identity of those persons and the circumstances relating to the carrying on of those activities."*

[918] § 2 Abs. 2 ES Reg. In diesem Verzeichnis sollen deren Namen und Adressen aufgenommen und es soll in geeigneter Weise öffentlich zugänglich gemacht werden, § 3 Abs. 3: *„… of whom she*[/he] *is aware who are established in the* [UK] *and who issues qualified certificates…"* und Abs. 4 ES Reg.: *„… shall publish the register in such manner as she considers appropriate."*

[919] § 3 Abs. 5 ES Reg.: *„The Secretary of State shall have regard to evidence becoming available to her*[/him] *with respect to any course of conduct of a certification-service-provider… and who issues*

Offensichtlich hat sich letztlich die Ansicht durchgesetzt, dass der Wert der qualifizierten Signaturen davon abhängt wie strikt die Einhaltung der Anforderungen der Anhänge I und II der RLeS (hier Schedule 1 und 2 ES Reg.) sichergestellt wird und dass dies im Rahmen eines freiwilligen Genehmigungs- oder Akkreditierungssystems gewährleistet werden kann.[920] Elektronische Signaturen von Zertifizierungsdiensteanbietern, die (sichere) Signaturerstellungseinheiten ausgeben und nutzten, die ihrerseits nach den im Verfahren nach Art. 3 Abs. 5 RLeS aufgestellten Standard geprüft sind, werden als fortgeschrittene elektronische Signaturen anerkannt. Die Einführung von unabhängigen Prüf- oder Festlegungssystemen gemäß der in der RLeS genannten Standards war jedoch nicht vorgesehen.[921] Die Regierung selbst wollte nicht die Führung bei der Erarbeitung der Standards übernehmen, sondern dies einer industrie- oder nutzergeführten Initiative überlassen.[922]

Erstmalig wurde in den ES Reg. die Haftung der Zertifizierungsdiensteanbieter gesetzlich geregelt. Damit korrigierte man die kritisierte (vorläufige) Entscheidung, die Verantwortlichkeit der *trust service providers* dem bestehenden Recht und vertraglichen Vereinbarungen zu überlassen.[923] Die ES Reg. folgen dabei den Vorgaben der RLeS[924], gehen aber auch etwas darüber hinaus. Entsprechend der Regelung des Art. 6 Abs. 1 RLeS bestimmt § 4 Abs. 1 ES Reg. für den Fall, dass der Zertifizierungsdiensteanbieter entweder ein Zertifikat als ein qualifiziertes öffentlich ausstellt oder für ein derartiges Zertifikat öffentlich einsteht und

---

qualified certificates to the public and which appears to her[/him] *to be conduct detrimental to the interests of those persons who use or rely on those certificates with the view to making any of this evidence as she*[/he] *considers expedient available to the public in such manner as she considers appropriate."*

[920] In seinem „Consultation Document on the Implementation of the EU Electronic Signatures Directive" hatte das DTI diese Frage noch offen gelassen, Absatz Nr. 11. Es sollte der Gedanke des *„fit the remedy to the risk"* (das Rechtsmittel dem Risiko anzupassen) herrschen. Dem *high risk scenario* mit aktiv handelnden Überwachungssystems und zwingender, strafbewehrter Meldepflicht für qualifizierte Zertifikate wurde das *low risk scenario* vorgezogen. Der Markt sollte beobachtet und nur die so in Erscheinung tretenden oder freiwillig informierende Diensteanbieter sollten aufgenommen werden In beiden Fällen sollte erst aufgrund eines auslösenden Moments, beispielsweise verbraucherschädlichen Verhaltens, eingeschritten werden. Absätze Nr. 13 bis 16, 21, 22.

[921] Dort Art. 3 Abs. 5 RLeS, hinsichtlich Anhang III. DTI, „Consultation Document on the Implementation of the EU Electronic Signatures Directive", Absatz Nr. 31.

[922] Die Anerkennung der Standards über die Kommission sei nicht der einzige gangbare Weg; DTI, „Discussion Document on Electronic Signatures Directive Implementing Regulations".

[923] Siehe Coyle, ECLP 2001, S. 9; Worthy/Anderson, CLSR 1999, S. 398.

[924] DTI, „Electronic Signatures & Associated Legislation", www.dti.gov.uk/cii/datasecurity/electronicsignatures/esd_note.shtml. Nicht gesetzlich eingeführt wurde die Möglichkeit für Zertifizierungsdiensteanbieter, ihre Haftung für bestimmte Anwendungen der Zertifikate auszuschließen oder sie zu beschränken. Hierfür bestand laut des Department of Trade and Industry (DTI) kein Grund, da Zertifizierungsdiensteanbieter dies bereits nach den bestehenden Regeln des Deliktsrechts und des *tort* erreichen könnten. Der Begriff des *tort* lässt sich am besten mit deliktischem Handeln übersetzen, stimmt mit dem Begriff der unerlaubten Handlung des BGB jedoch nicht überein und steht dem des *contract* gegenüber. Siehe ausführlich: von Bernstorff, S. 96 ff. Ursprünglich hatte das DTI in seinem „Consultation Document on the Implementation of the EU Electronic Signatures Directive", Absatz Nr. 42, einen dahingehenden Umsetzungsbedarf noch bejaht. Dieser wurde aber anschließend verneint, DTI, „Discussion Document on Electronic Signatures Directive Implementing Regulations", www.dti.gov.uk/cii/datasecurity/electronicsignatures/signatures.shtml.

„… b) eine Person vernünftiger Weise auf dieses Zertifikat hinsichtlich folgender Tatsachen vertraut

(i) dass jegliche Informationen in dem qualifizierten Zertifikat zum Zeitpunkt seine Ausstellung richtig sind,

(ii) dass das qualifizierte Zertifikat alle in Schedule 1 [entspricht Anhang I der RLeS] *aufgeführten Angaben enthält,*

(iii) dass der in dem qualifizierten Zertifikat angegebene Unterzeichner zum Zeitpunkt der Ausstellung des Zertifikats im Besitz der Signaturerstellungsdaten war, die den im Zertifikat angegebenen oder identifizierten Signaturprüfdaten entsprechen, oder

(iv) dass in Fällen, in denen der Zertifizierungsdiensteanbieter sowohl die Signaturerstellungsdaten als auch die Signaturprüfdaten erzeugt, beide in komplementärer Weise genutzt werden können,[925]

c) diese Person aufgrund dieses Vertrauens einen Verlust [loss] *erleidet*[926] *und*

d) der Zertifikationsdiensteanbieter zum Schadensersatz in voller Höhe des Verlustes verpflichtet wäre

i) sofern eine Sorgfaltspflicht des Zertifizierungsdiensteanbieters gegenüber der in lit. b) genannten Person bestünde und

(ii) sofern der Zertifizierungsdiensteanbieter fahrlässig gehandelt hätte,

so soll der Zertifizierungsdiensteanbieter dementsprechend in gleichem Maße verpflichtet sein, gleichwohl ein Beweis seiner Fahrlässigkeit nicht vorliegt, es sei denn der Zertifizierungsdiensteanbieter weist nach, dass er nicht fahrlässig gehandelt hat.“[927]

Lit. d) entspricht ungefähr dem Regelungsgehalt des Art. 6 Abs. 1 RLeS. Er ist eine Ausprägung des englischen Schadensersatzrechts, nimmt allerdings, im Vergleich zur üblichen Regel, eine Umkehr der Beweislast vor.[928] Zusammen mit Abs. 2, der hinsichtlich der in Abs. 1 lit. b) genannten Aspekte eine Sorgfaltspflicht des Zertifizierungsdiensteanbieters gegenüber der auf das qualifizierte Zertifikat vertrauenden Person nochmals feststellt, sichert er die Umsetzung in englisches Recht. Einen weiteren, zweiten Haftungstatbestand regelt § 4 Abs. 3 ES Reg., wonach der ein qualifiziertes Zertifikat öffentlich ausstellende Zertifizierungsdiensteanbieter in gleicher Weise[929] haftet, wenn der Dritte auf dieses Zertifikat vertraut[930] und *„… diese Person in Folge einer*

[925] § 4 Abs. 1 ES Reg., dessen Ziffern (i) bis (iv) den lit. a) bis c) des Art. 6 Abs. 1 RLeS entsprechen.

[926] Auch dies entspricht dem Art. 6 Abs. 1 RLeS.

[927] § 4 Abs. 1 lit. d) ES Reg.: *„„„ the certification-service-provider would be liable in damages in respect of any extend of the loss (i) had a duty of care existed between him and the person…, and (ii) had the certification-service-provider been negligent, then that certification-service-provider shall be so liable to the same extent notwithstanding that there is no proof that the certification-service-provider was negligent, unless the certification-service-provider proves that he was not negligent.”*

[928] Mason, *Electronic Signatures in Law*, S. 192.

[929] § 4 Abs. 3 lit. d) ES Reg., Haftungsfolge des § 4 Abs. 2 lit. d) ES Reg.

[930] Abs. 3 lit. a) und b).

vom Zertifizierungsdiensteanbieter unterlassenen Eintragung eines Widerrufs des Zertifikats einen Verlust erleidet..."[931]

2.4.4 Zusammenfassung und Kritik

Die Englischen Gesetzesänderungen in Erfüllung der Umsetzungspflicht aus RLeC und RLeS zeigen das Spannungsfeld zwischen minimalistischem und beschreibendem Ansatz auf. Grundsätzlich ist die bloße allgemeine Feststellung der generellen Beweiszulassung elektronischer Signaturen und Verträge in Anbetracht der geringeren rechtlichen Hürden, insbesondere der bereits bestehenden rechtlichen Anerkennung im Sinne der Rechtswirksamkeit elektronischer Signaturen, hier ein sinnvoller Ansatz. Auch wenn erst mit den ES Reg. wesentliche Regelungsinhalte der RLeS übernommen wurden, ist hinsichtlich der Signaturgesetzgebung hervorzuheben, dass die der RLeS angelehnten Haftungsregelungen wie in Deutschland über die Vorgaben der RLeS hinausgehen und auch Sorgfaltspflichten des Zertifikatsinhabers festgeschrieben wurden. Mit Ausnahme dieser Regelungen und der Ermöglichung eines Genehmigungsverfahrens für Zertifizierungsdiensteanbieter und mit Ausnahme umfangreicherer Haftungstatbestände für diese, gehen die englischen Neuregelungen aber nicht über die Mindestvorgaben der RLeS hinaus. Die englischen Gesetze und Rechtverordnungen haben auch keine detaillierten Standards ausgebildet. Die Regelungen des EC Act allein waren für die Umsetzung der EU-Richtlinien völlig ungenügend, schon da mit ihm keine Änderungen von Formvorschriften einhergingen.[932] Im Ergebnis hat sich die Gesetzeslage für elektronische Verträge und formbedürftige Erklärungen in elektronischer Form nur geringfügig geändert. Zum Beispiel besteht die Diskussion um die Erfüllung von Schriftformerfordernissen, nach denen Verträge *in writing* abgeschlossen werden (nicht bloß beweisbar sein) müssen, durch elektronische Dokumente und Datennachrichten daher zunächst einmal fort.[933] Solche *in writing* abzuschließenden Verträge[934] gehören weiter zu den bestehenden rechtlichen Hindernissen für den Einsatz elektronischer Verträge, die nach Ansicht des DTI auf einer *case by case*-Basis nach und nach beseitigt werden sollten. Um das Problem der Authentizität und Integrität zu lösen, wurden zwar die verpflichtenden Vorgaben der EU-Richtlinien umgesetzt. Hinsichtlich der Erfüllung von Formvorschriften hat der EC Act aber die bereits bestehende Flexibilität der Bedeutung der *signature* im englischen Recht nicht geändert. Eine elektronische Signatur muss nicht die besondere Form der digitalen Signatur haben, um als Unterschrift akzep-

[931] Abs. 3 lit. c): *„that person suffers loss as a result of any failure by the certification-provider to register revocation of the certificate..."* Auch hierfür bestimmt Abs. 4 eine Sorgfaltspflicht des Zertifizierungsdiensteanbieters gegenüber dem Dritten.

[932] Zutreffend Crichard, CLSR 2000, S. 399. Die Industrie ihrerseits begrüßte dessen Regelungsansatz des EC Act; Siehe bei Worthy/Anderson, CLSR 1999, S. 399.

[933] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 667.

[934] Z.B. Verträge über den Grundstücksverkauf, § 2 Law of Property (Miscellaneaous Provisions) Act 1989; bestimmte Verbraucherkreditverträge, § 62 Consumer Credit Act 1974; *bills of sale*, §§ 4 und 8 Bills of Sale Act 1878; Übertragung von Urheber- und anderen Rechten an geistigem Eigentum, § 90 Abs. 3 Copyright, Designs, and Patents Act 1988.

tiert zu werden. Sofern dazu zum Beispiel der Name in einem elektronischen Dokument geschrieben (getippt) wird, ist dazu lediglich erforderlich, dass die betreffende Person beabsichtigt, dass dieser Name als Mittel der Authentifizierung dient und vom Empfänger erwartet, sich gemäß dem Inhalt des Dokuments zu verhalten. Weitere Voraussetzungen sind nicht zu erfüllen.[935] Auch mit der Definition der elektronischen Signatur in § 7 Abs. 2 EC Act und der hinsichtlich der Feststellung der Authentizität zu berücksichtigenden Aspekte gemäß § 15 Abs. 2 Ziffer (a) (i) bis (iii) EC Act wird, wo das Vorliegen einer elektrischen Signatur streitig ist, die jeweils beweisbelastete Partei nach wie vor Beweis für diese Aspekte erbringen müssen.[936] Diese Rechtslage wird auch durch neuere, nachfolgend dargestellte Urteile bestätig.

2.4.5 Formen der elektronischen Signatur

Nach Erlass der vorgenannten gesetzlichen Neuregelungen ist festzustellen, dass diese für die Beurteilung, ob eine rechtsgültige Unterschrift vorliegt, offenbar ohne große Bedeutung sind. Vielmehr bauten die Neuregelungen auf dem bisherigen *case law* wie es oben dargestellt wurde[937] auf. Die Frage, ob eine elektronische Signatur in der Lage ist ein Unterschriftserfordernis zu erfüllen, hängt dabei vom jeweiligen Formerfordernis ab.[938] Solange jedoch der erforderliche Wille zu signieren vorhanden ist, können grundsätzlich auch einfache Formen der elektronischen Signatur, zum Beispiel der eingescannten Version einer handschriftlichen Unterschrift in einem Dokument, ausreichen.[939] Bemerkenswert ist, dass in der Rechtsprechung digitale Signaturen, entsprechende Zertifikate und Verfahren der PKI praktisch nicht vorkommen. Vorausgesetzt, dies spiegelt wider, welche Arten der Signatur im elektronischen Umfeld tatsächlich eingesetzt werden, so wird deutlich, dass digitale Signaturen bei der elektronischen Kommunikation und der Abgabe rechtserheblicher und sogar formbedürftiger Erklärungen keine große Rolle spielen.

Eine mittlerweile von der Rechtsprechung in einzelnen Fällen akzeptierte Form der elektronischen Signatur ist die bloße Namensangabe wie sie in der E-Mail-Adresse enthalten ist. So wurde zunächst in *J. Perreira Fernandes SA v. Mehta*[940] in Bezug auf das Statute of Frauds entschieden. Entscheidend war allerdings, dass die Beweise in Form weiterer E-Mail-Kommunikation von derselben Adresse ausreichend waren, um die Authentizität der in Frage stehenden E-Mail zu belegen. Vor allem aber hatte hier der Versender der E-Mail die Versendung der E-Mail nicht bestritten. Gestützt wurde dieses

[935] Mason, *Electronic Signatures in Law*, S. 195; siehe bspw. die nachfolgend dargestellte Rechtsprechung zu Namen in E-Mails etc.

[936] Mason, *Electronic Signatures in Law*, S. 190.

[937] Siehe 1.3.2.3 und 1.3.2.4.

[938] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 659.

[939] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 659.

[940] *J. Perreira Fernandes SA v. Mehta* [2006] 1 WLR 1543; [2006] 2 All ER 891; [2006] 1 All ER (Comm) 885; [2006] All ER (D) 264; [2006] IP & T 546; The Times, 16. Mai 2006; [2006] EWHC 813 Ch.)

Urteil auch auf den Fall *Caton v. Caton* von 1867, in dem Lord Westbury zur Stelle auf dem Dokument, an der die Signatur aufgebracht werden müsse, ausführt, diese müsse

> *„… so platziert sein, dass sie zeigt, dass sie sich auf jeden Teil der Urkunde beziehen soll und tatsächlich bezieht. … sie muss jeden Teil der Urkunde bestimmen* [govern]. *Sie muss zeigen, das jeder Teil der Urkunde von der so unterzeichnenden Person herrührt und dass die Unterschrift diese Wirkung haben sollte. Daraus folgt, dass wenn eine Unterschrift nur zufällig in einer Urkunde auftaucht oder sich nur auf einen Teil der Urkunde bezieht, diese Unterschrift nicht die rechtliche Wirkung haben kann, die sie haben muss, um dem Gesetz zu entsprechen und dem gesamten Vertragswerk Authentizität zu verleihen.“*[941]

Dies wird bestätigt durch frühere Fälle, die ebenfalls vor allem auf die Absicht des Unterzeichnenden abstellten, nicht auf die Stelle, an der sie aufgebracht wird.[942] Es wird angeführt, dass die in der E-Mail-Adresse enthaltenen Informationen die gleichen Funktionen erfüllten, wie der Briefkopf auf einem papiernen Dokument.[943] Diese Überlegung wurde auch im 2005 entschiedenen Fall *SM Integrated Transware Ltd. v. Schenker Singapore (Pte) Ltd.* für die Akzeptanz der E-Mail-Adresse als *signature* zugrunde gelegt, in dem der Versender der E-Mails darauf verzichtet hatte seinen Namen in den Text der E-Mail aufzunehmen:

> *„Es besteht kein Zweifel, dass er zum Zeitpunkt des Absendens* [der E-Mails] *die Empfänger wissen lassen wollte, dass diese von ihm stammten. Des weiteren fand er es nicht notwendig, sich durch das Anfügen seines Namens am Ende jeder dieser E-Mails als Absender zu identifizieren … Ich kann nur annehmen, dass er dies deshalb unterließ, weil er wusste, dass sein Name so deutlich im Kopf jeder Nachricht neben seiner E-Mail-Adresse erschien, so dass kein Zweifel daran bestehen kann, dass er als Absender identifiziert werden wollte.“*[944]

---

[941] *Caton v. Caton* (1867) LR 2 HL 127: *„… be so placed as to shew that it was intended to relate and refer to, and that in fact it does relate and refer to, every part of the instrument. … it must govern every part of the instrument. It must shew that every part of the instrument emanates from the individual so signing, and that the signature was intended to have that effect. It follows, that if a signature be found in an instrument incidentally only, or having relation and reference only to apportion of the instrument, the signature cannot have legal effect and force which it must have I order to comply with the statute, and to give authenticity to the whole of the memorandum.“*

[942] *Stokes v. Moore* (1786) 1 cox. 219; 29 ER 1137; *Ogilvie v. Foljambe*, (1817) 3 Mer. 53; 36 ER 21; *Holmes v. Mackrell*, (1858) 3 C.B. (N.S.) 789; 140 ER 953.

[943] So schlüssig unter Berufung auf den oben unter 1.3.2.4 dargestellten Fall *Tourret v. Cripps* Mason, *Electronic Signatures in Law*, S. 317.

[944] *SM Integrated Transware Ltd. v. Schenker Singapore (Pte) Ltd.* [2005] 2 SLR 651, [2005] SGHC 58, 92: *„There is no doubt that at the time he sent [the emails] out, he intended the recipients of the various messages to know that they had come from him. Despite that, he did not find it necessary to identify himself as the sender by appending his name at the end of any of the mails … I can only infer that his omission to type in his name was due to his knowledge that his name appeared at the head of every message next to his email address so clearly that there could be no doubt that he was intended to be identified as the sender of such message.“*

In der zweiten Instanz wurde das Urteil zu *J. Perreira Fernandes SA v. Mehta* im Fall *Mehta v. J. Perreira Fernandes SA* dagegen aufgehoben und festgestellt, dass die E-Mail-Adresse keine elektronische Signatur darstelle, da nicht angenommen werden könne, dass die automatisch eingestellte Adresse als Signatur des Absenders gewollt war.[945] Unterstützt wird die Sichtweise, eine E-Mail-Adresse könne eine wirksame *signature* darstellen, aber auch durch § 7 Abs. 2 EC Act, nachdem eine elektronische Signatur beziehungsweise deren Daten in eine elektronische Mitteilung oder in elektronische Daten aufgenommen oder anders logisch mit ihnen verknüpft sein müssen. Denn sofern eine E-Mail-Adresse nicht so in das elektronische Dokument E-Mail aufgenommen oder mit dieser verknüpft wäre, würde ihr Inhalt weder versendet noch seinen Empfänger erreichen. Eine E-Mail-Adresse entspricht damit in im Prinzip der Voraussetzungen der elektronischen Signatur des EC Act.[946] Wie an den vorgenannten Fällen ersichtlich, geht es im Beweisverfahren dann darum, die entsprechende Absicht des Versenders, zu signieren, festzustellen. Hinsichtlich einer eingescannten handschriftlichen Unterschrift, die dann in digitaler Form einem elektronischen Dokument beigefügt wird, ist auf den oben dargestellten Fall *Re a debtor*[947] zur Faxübertragung zu verweisen. Danach soll das Mittel der Kommunikation den rechtlichen Effekt nicht beeinflussen.

Bezüglich solcher Formerfordernisse, die insbesondere die handschriftliche Unterschrift verlangen, wird in der Literatur angenommen, dass sie allein durch eine elektronische Signatur, die schwierig zu fälschen ist und die Echtheit des betreffenden Dokuments wie eine eigenhändige Unterschrift garantiert, erfüllt werden könnten. Die Unsicherheit hinsichtlich der Wirksamkeit der elektronischen Signatur in Anbetracht eines Unterschriftserfordernisses bestünde fort.[948] Dieser Einschätzung kann zumindest insoweit zugestimmt werden, als auch nach den Neuregelungen gerade nicht für jedes Formerfordernis deren Erfüllung durch elektronische Substitute gesetzlich festgestellt wird. Dennoch ist hier vor allem festzuhalten, dass viele der in den vorgenannten Urteilen als *signature* akzeptierte und zum Teil entsprechende Formerfordernisse erfüllende Formen der Signatur in elektronischen Mitteilungen den Anforderungen entsprechen, die § 126b BGB an Form und Inhalt der Textform stellen.[949]

[945] *Mehta v. J. Perreira Fernandes SA* [2006] 1 WLR 1543, [2006] EWHC 813 (Ch).

[946] Zutreffend Mason, *Electronic Signatures in Law*, S. 317, 318.

[947] *Re a debtor (No. 2021 of 1995), Ex p, Inland Revenue Commiccioners v. The debtor; Re a debtor (No. 2022 of 1995), Ex, Inland Revenue Commissioners v. The debtor* [1996] 2 All E.R. 1208, S. 345, 351

[948] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 659.

[949] Dazu ausführlich unten unter 3.3.1 und 3.3.2.

2.5 Signaturgesetze und Änderungen der Formvorschriften in den USA

Die USA prägten die technische Entwicklung; Produkte und Dienstleistungen für den E-Commerce kamen dort schneller und in größerem Umfang zur Anwendung. Sie sind auf dem globalen Internetmarkt stark vertreten, haben einen großen Anteil an Internet-Nutzern und üben damit einen nachhaltigen Einfluss auf die sogenannte „Netzgemeinde" aus.[950] Vielfach stehen Neuregelungen nationaler Gesetzgeber in einem globalen Kontext. So sind auch die RLeS und RLeC an internationalen Initiativen, insbesondere den UNCITRAL-Modellgesetzen, orientiert, die ihrerseits Richtschnur auch für bundeseinheitliche Signaturgesetze in den USA waren. Die USA wiederum beeinflussen durch ihre Gesetzgebung und Rechtsprechung das Recht anderer Staaten.[951] Ausländische Entwicklungen animieren ihrerseits nur gelegentlich die Rechtsentwicklung in den USA[952], weshalb die Bundesstaaten[953] und der Bundesgesetzgeber das *common law* und gesetzliche Vorschriften – im Unterschied zu England – ohne eine verpflichtende Harmonisierungsinitiative wie die EU-Richtlinien anpassen konnten.[954] Wie auch in England sollte die legislative Tätigkeit – wiederum typisch für das *common law* – grundsätzlich zurückhaltend und die Rechtsentwicklung dem Markt und dem relativ flexiblen *common law* überlassen bleiben. Grundsätzlich stand man auf dem Standpunkt, dass der Gesetzgeber erst dann eingreifen sollte, wenn das sich entwickelnde Ungleichgewicht der Marktkräfte dies gebiete.[955] Dennoch wurden auf regionaler Ebene früh diverse Gesetze erlassen, mit dem Ziel, ein möglichst günstiges regulatorisches Umfeld zu schaffen.[956] Die rechtliche Beurteilung elektronischer Signaturen zeichnete sich bereits durch die oben dargestellten Urteile hierzu ab.[957] Auch vor diesem Hintergrund sind die nachfolgend beschriebenen Gesetze zu sehen.

---

[950] Kochinke/Geiger, K&R 2000, S. 594; Schumacher, CR 1998, S. 59.

[951] Über den United States Trade Representative tragen sie ihre Rechtsvorstellung in internationale Gremien, damit, *„andere Länder ihr nationales Recht an das der USA anpassen ... oder dieses ... aus ökonomischer Notwendigkeit als exterritoriale Ausstrahlung dulden."* So Kochinke/Geiger, K&R 2000, S. 594. Nicht nur wegen der Vorreiterrolle der USA, auch wegen des sich ständig verdichtenden Netzes der Zuständigkeiten sollen die US-Regelungen hier berücksichtigt werden. Die gerichtliche Zuständigkeit von US-Gerichten kann leicht gegeben sein bei im Ausland getätigten Handlungen, solange ein Minimum an Kontakten zum Gerichtsstaat vorliegt, etwa vertragliche Beziehungen, auch E-Mails, jedenfalls interaktive Websites mit Bestellmöglichkeit; Kochinke/Geiger, K&R 2000, S. 602.

[952] Kochinke/Geiger, K&R 2000, S. 594, 595.

[953] Bundesstaat(en) bezeichnet hier die einzelnen, die Vereinigten Staaten bildenden Staaten. Der Begriff des Bundesstaates ist nicht gleichzusetzen mit dem des Mitgliedstaates der EU.

[954] Was aufgrund der gemeinsamen Herkunft und Rechtstradition schon einen Vergleich mit den englischen Neuregelungen rechtfertigte. Hinzu kommen große Unterschiede zum *civil law*, z. B. die Doctrine of Consideration im stark wirtschaftlich geprägten amerikanischen Vertragsrecht, das die Freiheit des Marktes betont, Hay, Rn. 245.

[955] Miedbrodt in Bizer et al., S. 277, die diesen Ansatz als „Bottom-up-Ansicht" bezeichnet, im Gegensatz zu einer „Top-down-Herangehensweise" z.B. des deutschen Gesetzgebers.

[956] Daneben spielt auch der Handlungsbedarf gegen Kriminalität eine bedeutende Rolle. Siehe Kochinke/Geiger, „Trends im US-Computer- und Internetrecht", K&R 2000, S. 594-602, S. 594, 602.

[957] Siehe unter 1.3.3.6.

2.5.1 Rechtslage vor den Neuregelungen

2.5.1.1 Bundesstaatliche Signaturgesetze

Der Bundesgesetzgeber agierte zunächst zurückhaltend in Bezug auf eine Regelung der Verwendung bestimmter Signaturtechnologien, der Tätigkeit von Verschlüsselungs- und Zertifizierungsdiensteanbietern oder zur Rechtswirksamkeit elektronischer Signaturen.[958] Entsprechende Vorschriften waren dafür von den meisten Einzel- oder Bundesstaaten erlassen worden, ohne dabei große Übereinstimmung auszubilden.[959] Diese bundesstaatlichen Gesetze[960] divergierten und divergieren stark in ihren Regelungsansätzen, im Umfang ihres Anwendungsbereichs und ihren Rechtsfolgen.[961] Sie alle beschränkten sich zunächst darauf, Behinderungen für den E-Commerce zu beseitigen.[962] Hinsichtlich der Signaturgesetzgebung folgte die Mehrheit der Bundesstaaten einem technologieneutralen Ansatz, der die rechtliche Gleichstellung von elektronischer und handschriftlicher Unterschrift festschreibt und auf Anforderungen an die Signaturverfahren verzichtet.[963] Dennoch hatten und haben viele Regelungen die PKI als technische Grundlage der elektronischen beziehungsweise digitalen Signatur. Häufig wurden Zulassungs- und Untersuchungsverfahren als Mittel der Gewährleistung der Sicherheit der Systeme eingesetzt, deren Maßstäbe und Standards jedoch nur zum Teil ausgestaltet. Eine Kategorie dieser Gesetze regelte viele der für den Einsatz der PKI typischen Aspekte.[964] Hier zeigt sich vielmals eine weitgehende Übereinstimmung mit dem Regelungsansatz der EU. Im Übrigen wurde und wird dem Zertifikatinhaber eine große Eigenverantwortung aufgebürdet.[965] Unterschiede bestehen auch hinsichtlich des Anwen-

[958] Dreben/Werbach, „Senators versus Governors: State and Federal Regulation of E-Commerce", TCL 2000, S. 3-15, S. 12; Schumacher, CR 1998, S. 59.

[959] Dreben/Werbach, TCL 2000, S. 12.

[960] Die Bezeichnung „bundesstaatliches Gesetz" bezieht sich auf ein von einem einzelnen (Bundes-)Staat der USA erlassenen Gesetz, im Unterschied zu Bundesgesetzen, welche im Rahmen einer Rechtsvereinheitlichung innerhalb der USA von Bundesorganen erlassen oder den (Einzel- oder) Bundesstaaten zur Übernahme empfohlen werden (Zu den *uniform laws* siehe Reimann, S.7 ff.).

[961] Es wurden weit über dreißig Gesetze oder Gesetzgebungsinitiativen der Bundesstaaten gezählt; siehe ausführlich Miedbrodt, „Regelungsansätze und -strukturen US-amerikanischer Signaturgesetzgebung", DuD 1998, S. 389-394, S. 389, und „Das Signaturgesetz in den USA – Electronic Signatures in Global and National Commerce Act", DuD 2000, S. 541, die versuchte, diese in verschiedene Ansätze zu unterscheiden, den beschreibenden Ansatz (*prescriptive approach*), den eigenschaftsbasierten Ansatz (*criteria-based*), den unterschriftsgleichstellenden Ansatz (*signature-enabling approach*) und einen Mischansatz. Einige seien nur auf bestimmte Kommunikationsbeziehungen anwendbar, andere auf jede Kommunikationsbeziehung, wiederum unterteilt in den technikrechtlichen, den marktwirtschaftlichen und einen hybriden Ansatz. Siehe auch Smedinghoff/Hill Bro, JMJCL 1999, S. 5 und oben 1.4.3.

[962] Siehe Miedbrodt, DuD 1998, S. 389.

[963] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 73.

[964] Bspw. Verpflichtungen der Zertifikatinhaber, z.B. wahrheitsgemäße Angaben machen, das Zertifikat überprüfen und ausdrücklich bestätigen, den privaten Schlüssel unter Kontrolle und geheim halten, oder der u.U. auch nicht lizenzierten Zertifizierungsdiensteanbieter, z.B. ein vertrauenswürdiges System einsetzen, die Identität der Antragssteller korrekt feststellen, die Gewähr für die Ausgabe des Zertifikats übernehmen etc.; Smedinghoff/Hill Bro, JMJCIL 1999, S. 30. Beispiele sind die Signaturgesetze der Bundesstaaten Minnesota, Missouri, Utah und Washington.

[965] Er selbst soll anhand bestimmter Angaben (*certification practice statements*) einschätzen, ob eine dem Zweck seiner Transaktion genügende Sicherheit geboten wird. Miedbrodt, DuD 1998, S. 394.

dungsbereiche, die sich zum Beispiel nur auf die Kommunikation mit öffentlichen Behörden und nur zum Teil auch auf den privaten Sektor erstreckten[966], teilweise wird nach der Art der Transaktionen unterschieden.[967] Einige Gesetze regelten und regeln lediglich die technisch-organisatorischen Voraussetzungen der Infrastruktur für die digitale Signatur, damit diese den Nachweis der Integrität und Authentizität erbringen kann.[968] Einige Signaturgesetze hatten Sicherheitsanforderungen des U.S. Comptroller General übernommen[969], die denen der RLeS und den deutschen und englischen gesetzlichen Regelungen sehr ähnlich waren. Manche Regelungen überlassen die Spezifizierung solcher Anforderungen den Marktkräften, andere verbinden die vorgenannten Regelungselemente.[970] Um den Einsatz von besonders vertrauenswürdiger Signaturverfahren zu fördern, wurden diese zum Teil mit einer gesetzlichen Vermutungsregel hinsichtlich der Identität des Absenders und der Integrität des Dokuments verbunden.[971]

2.5.1.2 Bedarf bundeseinheitlicher Regelungen

Die Zweckmäßigkeit einer bundesweiten Harmonisierung war in Anbetracht der Vielzahl verschiedener Gesetze und Regelungsansätze offensichtlich. Die dargestellte Rechtslage barg die Gefahr einer heterogenen Regelungslandschaft.[972] Auch wenn die Zielsetzung der Gesetzeswerke grundsätzlich gleich war, mangelte es offenbar an der Abstimmung der Bundesstaaten untereinander und an der Bereitschaft, (bundes-) staatsübergreifende Regelungen zu treffen. Eine Klarstellung war geboten, da zusätzliche Anforderungen an die Gleichstellung zwischen herkömmlicher und elektronischer Signatur in einigen Gesetzen den Schluss nahe legen, nur eine bestimmte Technologie könne die *signature requirements* erfüllen, beziehungsweise dass ausschließlich die digitale Signatur vertrauenswürdig sei.[973] So waren die Rechtswirksamkeit elektronischer Ver-

[966] Miedbrodt, DuD 1998, S. 389.

[967] Smedinghoff/Hill Bro, JMJCIL 1999, S. 18 m.w.N.

[968] Es wurden unterschiedliche Standards für die Authentifizierung elektronischer Dokumente aufgestellt, z.B. in den Gesetzen aus Utah, Washington und dem Electronic Signatures in Global and National Commerce Act (siehe 5.3); Dreben/Werbach, TCL 2000, S. 13. Geregelte Bereiche betreffen u.a. die Herstellung und Kontrolle von Signaturerstellungseinheiten und -daten. Smedinghoff/Hill Bro, JMJCIL 1999, S. 30, 31.

[969] Danach ist eine elektronische Signatur rechtswirksam, wenn sie einzig dem Nutzer zugewiesen ist (*„unique to the person using it"*), eine Überprüfung ermöglicht, unter der alleinigen Kontrolle des Nutzers steht und so mit den Daten verknüpft ist, dass durch jede Veränderung die Signatur ungültig wird. So zum Beispiel in Alaska, Kalifornien, Kentucky, Nebraska, Idaho und anderen. Siehe bei Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 23.

[970] Etwa die Signaturgesetze von Illinois oder auch die RLeS.

[971] So der Illinois Electronic Commerce Security Act, siehe nachfolgend und Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 23.

[972] Miedbrodt, DuD 2000, S. 541.

[973] Miedbrodt, DuD 2000, S. 542/543 ; Smedinghoff/Hill Bro, JMJCIL 1999, S. 20, 28. Hier wurde erkannt, dass für die im Internet üblichen Verträge nur wenige Schriftform- oder Unterschriftserfordernisse bestanden; Prefatory Note zum UETA, www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm.

träge und die Durchsetzbarkeit elektronischer Signaturen teilweise streitig.[974] Alle genannten Signaturgesetze enthalten, um dieses rechtliche Hindernis zu beseitigen, die Feststellung, dass elektronische Signaturen und Dokumente gesetzliche Signatur- und Schriftformerfordernisse erfüllen (können). Tatsächlich aber sind bei der Umsetzung dieses Zieles die gesetzlichen Regelungen uneinheitlich ausgefallen.[975] Außerdem lösten zahlreiche bundesstaatliche Signaturgesetze nicht das Authentifizierungsproblem elektronischer Signaturen.[976] Insgesamt bestand entgegen dem Willen der Gesetzgeber die Gefahr, dass durch die vielen verschiedenen Signaturgesetze gerade Vertrauen und die Vorhersehbarkeit des Rechts unterminiert würden.[977]
Den Bundesstaaten ist dabei zwar die grundsätzliche Gesetzgebungskompetenz zur Regelung des Vertragsrechts und des Handels innerhalb eines Bundesstaates zugewiesen, so dass sich die vorgenannten bundesstaatlichen Signaturgesetze und übrigen gesetzlichen Regelungen in den Bundesstaaten darauf stützen.[978] Die Bundesregierung besitzt jedoch die Kompetenz und Verantwortung dafür, Gesetze zur Regulierung des Handels zwischen den verschiedenen Bundessstaaten, mit anderen (ausländischen) Staaten und mit den in den USA ansässigen Indianerstämmen zu schaffen. Die Bundesstaaten können Gesetze erlassen, welche die Kompetenz des Bundesgesetzgebers über zwischenstaatlichen Handel berühren, vorausgesetzt, dieser hat kein entsprechendes, das bundesstaatliche Gesetz ausschließendes Gesetz erlassen.[979] Seit 1892 erarbeitet die National Conference of Commissioners on Uniform State Law (National Conference) Modellgesetze, die der Rechtsvereinheitlichung vor allem des Privatrechts dienen sollen.[980] Der Uniform Electronic Transactions Act und der Uniform Computer Information Transactions Act waren die ersten von der National Conference vorgeschlagenen bundesweiten Gesetze zu dieser Materie.[981]

2.5.2 Uniform Electronic Transactions Act

Der Uniform Electronic Transactions Act (UETA)[982] wurde im Juli 1999 durch die National Conference verabschiedet und im April 2000 angenommen. Er ist als Modellge-

[974] Siehe bei Collier/Shannon/Scott, „Electronic Signatures Legislation“ (Memo des NACS Counsel), Juni 2000, www.nacsonline.com/NACS/Resource/Government/electronic_sig_070500_ir.htm.

[975] Smedinghoff/Hill Bro, JMJCIL 1999, S. 14, der darauf hinweist, dass es teilweise unterschiedliche Ansätze sogar innerhalb ein und desselben Bundesstaates gibt.

[976] Auch hatte außer dem Utah Digital Signature Act keines der bundesstaatlichen Signaturgesetze das Problem der Anerkennung von aus anderen Bundesstaaten der USA (geschweige denn aus dem Ausland) stammenden elektronischen (oder digitalen) Signaturen aufgegriffen; ebenso wenig die Rechtswahl durch die Parteien; Dreben/Werbach, TCL 2000 S. 13.

[977] Smedinghoff/Hill Bro, JMJCIL 1999, S. 6.

[978] Dreben/Werbach, TCL 2000, S. 12.

[979] Mason, *Electronic Signatures in Law*, S. 230.

[980] So z.B. den Uniform Commercial Code (UCC, siehe oben 1.3.3.1), Reimann, S. 7.

[981] Dreben/Werbach, TCL 2000 S. 12.

[982] Uniform Electronic Transactions Act (1999), Text aus www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm, offiziell als „UETA” abgekürzt, so dass dieses Kürzel auch hier nachfolgend verwendet wird.

setz konzipiert, das von den Bundesstaaten in bundesstaatliche Gesetze umgesetzt werden sollte.[983]

2.5.2.1 Zielsetzung, Anwendungsbereich und Regelungskonzept

Der UETA sollte bundesweit aus Formvorschriften erwachsende rechtliche Hindernisse für die Wirksamkeit elektronischer Aufzeichnungen und Dokumente beseitigen, ohne die zugrunde liegenden Vorschriften und rechtlichen Regelungen zu Verträgen zu berühren. Elektronische Aufzeichnungen und Signaturen sollten ermöglicht und ihre Rechtsgültigkeit festgestellt werden.[984] Der UETA muss abgegrenzt werden vom Vertragsrecht und den oben aufgeführten Signaturgesetzen:

> *„... die wesentlichen Regeln* [und/oder Vorschriften] *des Vertragsrechts bleiben vom UETA unberührt. Er ist auch kein Gesetz zur digitalen Signatur. Insoweit ein* [Bundes-]*Staat über ein Digitale-Signaturgesetz verfügt, soll der UETA dieses unterstützen und ergänzen.*[985]

Vielmehr sollte das Gesetz unter Verweis auf bestehendes Recht eine minimalistische und vor allem lediglich prozessuale Regelung schaffen. So soll zum Beispiel die Frage, ob eine Aufzeichnung (oder Urkunde) einer bestimmten Person zugeordnet werden kann

> *„... dem außerhalb dieses Gesetzes bestehenden Recht überlassen sein. Ob eine elektronische Signatur irgendeine rechtliche Wirksamkeit entfaltet, ergibt sich aus den sie umgebenden Umständen und anderem Recht.“*[986]

Der Anwendungsbereich des Gesetzes beschränkt sich auf Rechtsgeschäfte (*transactions*). Dabei findet das Gesetz

---

[983] Den Bundesstaaten sollte ihre Rechtssetzungsbefugnis im Bereich des Vertragsrechts belassen werden und dennoch einheitliche Standards für den innerstaatlichen Geschäftsverkehr sichergestellt werden. Collier/Shannon/Scott, „Electronic Signatures Legislation“. Dem UETA wurde eine hohe Wahrscheinlichkeit der Umsetzung in den Bundesstaaten zugesprochen; Dreben/Werbach, TCL 2000 S. 13.

[984] § 6 UETA; Prefatory Note zum UETA und Kommentar Nr. 1 lit. a) und b) zu § 6 UETA. Der UETA sollte u.a. das Recht vereinfachen, modernisieren, seine Einheitlichkeit hinsichtlich der Nutzung elektronischer Medien (*means*) fördern, das Vertrauen in deren Rechtsgültigkeit und Integrität sowie die Schaffung der notwendigen rechtlichen und geschäftlichen Infrastruktur fördern; Kommentar Nr. 1 lit. c), e) bis g) zu § 6 UETA.

[985] Prefatory Note zum UETA: *„... the substantive rules of contracts remain unaffected by the UETA. Nor is it a digital signature statute. To the extend that a State has a Digital Signature Law, the UETA is designed to support and compliment that statute.”*

[986] *„The Act’s treatment of records and signatures demonstrates best the minimalist approach that has been adopted. Whether a record is attributed to a person is left to law outside this Act. Whether an electronic signature has any effect is left to the surrounding circumstances and other law.”* Siehe „Prefatory Note“ zum UETA und nachfolgend 5.2.3. Die Vorschriften sind so gestaltet, dass sie auch auf neue, noch nicht abzusehende Technologien anwendbar sind, Kommentar Nr. 2 zu § 6 UETA.

> *„… nicht auf alle Schrift*[form]*en und Signaturen* [Unterschriften] *Anwendung, sondern nur auf elektronische Aufzeichnungen und Signaturen in Zusammenhang mit Rechtsgeschäften, definiert als solche Interaktionen zwischen Personen in Bezug auf geschäftliche sowie Handels- und Regierungsangelegenheiten.“*[987]

Rechtsgeschäfte wie Testamente (*wills*) sind ausgenommen, ebenso Treuhandverhältnisse (*trusts*) und vor allem Verfügungen über Rechte an Immobilien[988], wobei der UETA den Abschluss dieser Rechtsgeschäfte in elektronischer Form jedoch nicht verbietet.[989] Daneben sollen insbesondere auch diejenigen Rechtsgeschäfte ausgenommen sein, auf die der Uniform Computer Information Transactions Act[990] und – mit Ausnahmen – der UCC Anwendung findet.[991] Der UETA bezieht sich lediglich auf das Medium in welchem Informationen, Aufzeichnungen und Signaturen präsentiert und aufbewahrt werden müssen. Seine rechtsgestaltenden Bestimmungen (*operative provisions*) beziehen sich auf Formerfordernisse aus anderen gesetzlichen Vorschriften.[992] Die Ausnahme bestimmter Vorschriften des Uniform Commercial Code (UCC) vom Anwendungsbereich des UETA erklärt sich mit der speziellen Regelung elektronischer Rechtsgeschäfte in Art. 5, 8, 9 UCC.[993] Er soll jedoch ausdrücklich Anwendung finden auf die von den Art. 2 und 2A UCC geregelten Rechtsgeschäfte Kauf und Miete.[994] Fer-

---

[987] § 3 lit. a) UETA; Prefatory Note zum UETA: *„The Act does not apply to all writings and signatures, but only to electronic records and signatures relating to a transaction, defined as those interactions between people relating to business, commercial and governmental affairs.”*; Kommentar Nr. 1 zu § 3 UETA. Einseitig generierte elektronische Aufzeichnungen (*records*, Begriffsbestimmung nachfolgend unter 2.5.2.2) und Signaturen sind folglich ebenfalls nicht umfasst; Kommentar Nr. 1 zu § 3 UETA; Kommentar Nr. 12 zu § 2 UETA.

[988] Ebenso Testamentsnachträge (*codicils*) oder Testamentstreuhandsverhältnisse (*testamentary trusts*), § 3 lit. b) Nr. 1 UETA. Diese Aufzählung ausgenommener Rechtsgeschäfte ist nicht abschließend, sondern repräsentativ für diejenigen Rechtsgeschäfte, in denen der Einsatz elektronischer Medien unangebracht erscheint; Kommentar zu § 3 UETA. Hinsichtlich der *real estate transactions* unterscheidet der Kommentar zwischen ihrer Rechtswirkung zwischen den Vertragsparteien und in Bezug auf Dritte, aus der sich regelmäßig die Verpflichtung einer öffentlichen Registrierung (*governmental filing*) ergebe, welche nach bundesstaatlichem Recht papierne Urkunden (genauer *deeds*) und die notariell beurkundete eigenhändige Unterschrift verlangen. Siehe Kommentar zu § 3 UETA.

[989] Die generelle Frage der Rechtswirksamkeit entsprechender Verträge überlässt der UETA anderen Gesetzen und Rechtsvorschriften. Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 8. Kritisch zu möglichen formgerechten Rechtsgeschäften über Immobilien per Mausklick aufgrund der weiten Definition der elektronsichen Signatur (hier im E-SIGN, siehe nachfolgend 2.5.3), Randolph, „Has Congress Murdered the Statute of Frauds?“, http://dirt.umkc.edu/files/sof.htm.

[990] Dazu ausführlich unten unter 2.5.4.

[991] Der UETA ist somit anwendbar auf die §§ 1-107 und 1-206 sowie der Art. 2 und 2A UCC, § 3 lit. b) Nr. 2 und 3 UETA.

[992] Folglich beziehen sich die vorgenannten Ausnahmen auf Schriftform- und Unterschriftserfordernisse, die nicht vom UETA berührt werden. Kommentar Nr. 2 zu § 3 UETA.

[993] Hinsichtlich der Art. 2 und 2A UCC soll der UETA Gesetzeslücken schließen; Prefatory Note zum UETA; Prefatory Note zum UETA; Kommentar Nr. 4 und 5 zu § 3 UETA.

[994] Kommentar Nr. 7 zu § 3 UETA. Diese Rechtsgeschäfte verlangten keine umfassenden Systeme oder Strukturen außerhalb der Rechtsbeziehungen zwischen den Parteien und sie hätten auch keine weit reichenden Auswirkungen auf die Rechte Dritter. Vielmehr sei der E-Commerce in diesem Bereich am

ner soll der UETA grundsätzlich nur dort Anwendung finden, wo die Vertragsparteien dem Einsatz elektronischer Medien zur Abwicklung des Rechtsgeschäfts zugestimmt haben.[995]

2.5.2.2 Begriffsbestimmungen

In § 2 definiert der UETA für seinen Anwendungsbereich beispielsweise die Begriffe Computerprogramm, Information und Informationsverarbeitungssystem[996], aber auch die Begriffe Aufzeichnung (*record*, auch als Akte oder Unterlage zu übersetzen) und elektronische Aufzeichnung (*electronic record*), elektronische Signatur und Sicherheitsverfahren (*security procedure*). Auch hierdurch wird der Anwendungsbereich des UETA näher bestimmt. Gemäß § 2 Nr. 5 UETA bezeichnet der Begriff elektronisch in Bezug auf eine Technologie, dass diese elektrische, digitale, magnetische, drahtlose, optische, elektromagnetische oder ähnliche Eigenschaften oder Fähigkeiten aufweist.[997] Hiermit soll sichergestellt werden, dass er sich auf die jeweils aktuelle Technologie bezieht:

> *„Der Begriff muss im Licht der sich entwickelnden Technologie weit ausgelegt werden, um den Zweck dieses Gesetzes, die Anerkennung* [validation] *geschäftlicher Transaktionen unabhängig vom… genutzten Medium, zu erfüllen. Derzeitige rechtliche Erfordernisse der ‚schriftlichen Form'* [writings] *können durch nahezu jedes körperliche Medium erfüllt werden, sei es Papier, andere Fasern oder selbst Stein. Der Zweck und der Anwendungsbereich dieses Gesetzes umfassen nicht-körperliche Medien, die aufgrund ihrer Technologie in der Lage sind, Informationen in für den Menschen verständlicher* [bzw. lesbarer] *Form* [perceivable] *zu speichern, zu übertragen und zu reproduzieren, jedoch des körperlichen Aspekts des Papiers, Papyrus oder des Steins entbehren.*[998]

Als *record* werden Informationen bezeichnet, die auf einem körperlichen, elektronischen oder anderem Medium gespeichert werden und in verständlicher (im Sinne von

---

weitesten verbreitet, so dass die Ausnahme dieser Rechtsgebiete dem Zweck dieses Gesetzes widerspräche; Kommentar Nr. 7 zu § 3 UETA.

[995] Prefatory Note zum UETA. § 5 lit. a) und b) S. 1 UETA.

[996] § 2 UETA, dort z.B. Nr. 3, 10 und 11.

[997] § 2 Nr. 5 UETA: *„'Electronic' means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities."*

[998] Kommentar zu § 2 Nr. 5 UETA, www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm: *„… The term must be construed broadly in light of developing technologies in order to fulfil the purpose of this Act to validate commercial transactions regardless of the medium used by the parties. Current legal requirements for 'writings' can be satisfied by almost any tangible media, whether paper, other fibres, or even stone. The purpose and applicability of this Act covers intangible media which are technologically capable of storing, transmitting and reproducing information in human perceivable form, but which lack the tangible aspect of paper, papyrus or stone."* Der Begriff elektronisch wird als der derzeit zur Bezeichnung der meisten gängigen Technologien am besten geeignet umrissen.

lesbarer) Form abgerufen werden können.[999] *Electronic record* sind Aufzeichnungen, die über oder durch elektronische Mittel generiert, gesendet, kommuniziert (oder übertragen), empfangen oder gespeichert werden.[1000] Eine elektronische Signatur (*electronic signature*) ist

> *„jeder elektronische Ton, jedes elektronische Symbol oder jedes elektronische Verfahren, der oder das einer elektronische Aufzeichnung* [record] *beigefügt oder mit dieser logisch verknüpft ist und von einer Person mit dem Willen, diese Aufzeichnung zu unterschreiben* [oder zu signieren]*, ausgeführt oder gebilligt wurde.“*[1001]

Diese Definition ist äußerst weit gefasst und enthält keine nennenswerten inhaltlichen Anforderungen.[1002] Entsprechend der anfangs dargestellten Definition der Signatur im US-amerikanischen Recht[1003] umfasst diese jede Art von Symbol und nunmehr auch Töne und (Signatur-)Verfahren. Neben diesem verlangt der UETA[1004] für alle elektronischen Signaturen zwei weitere Elemente. Dies ist zunächst die Absicht zu signieren. Die elektronische Signatur muss also auf ein bestimmtes Dokument bezogen sein und den Willen des Signierenden kenntlich machen.[1005] Unter welchen Voraussetzungen diese Absicht vorliegt bleibt eine Tatsachenfrage. Eine wesentliche Änderung des herkömmlichen Verständnisses der Unterschrift soll und wird damit nicht herbeigeführt. [1006] Wie auch in den vorgenannten Neuregelungen soll sie zudem mit der elektronischen Aufzeichnung verbunden werden. Diese Definition umfasst die Verwendung von PIN, digitalen Signaturen oder eines getippten Namens.[1007] Das Aufzeichnungsverfahren muss den Beweis ermöglichen, dass eine bestimmte Signatur in Verbindung mit einem bestimmten Dokument eingesetzt wurde.[1008]

> *„Ob eine bestimmte Aufzeichnung ‚unterschrieben‘* [bzw. signiert] *wurde, ist eine Tatsachenfrage* [question of fact]*. Der Beweis dieser Tatsache muss gemäß anderem anwendbaren Recht erfolgen. Dieses Gesetz stellt lediglich sicher,*

---

[999] § 2 Nr. 13 UETA: *„‘Record’ means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.“*

[1000] Gemeint ist damit ein Unterbegriff zur Aufzeichnung in herkömmlichen Medien, § 2 Nr. 7 UETA; Kommentar zu § 2 Nr. 7 UETA.

[1001] § 2 Nr. 8 UETA: *„‘Electronic Signature’ means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.“*

[1002] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 563.

[1003] Siehe 1.3.3.3.

[1004] Gleiches gilt auch für den E-SIGN, siehe nachfolgend 2.4.3.1.

[1005] Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 13.

[1006] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 563/564.

[1007] Mason, *Electronic Signatures in Law*, S. 231.

[1008] Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 13.

dass die Signatur durch elektronische Mittel erfolgen kann. Es muss keine spezifische Technologie eingesetzt werden, um eine rechtsgültige Signatur zu schaffen.“[1009]

Hier setzt die Kritik an, das Statute of Frauds verlange, dass eine Löschung der Unterschrift von oder deren irrtümliche Aufbringung auf einem Dokument sowie ihre Fälschung oder die Änderung des Inhalts des Dokuments leicht zu erkennen sei, die Erfüllung dieser Funktionen aber in Art. 2 Nr. 8 UETA nicht gefordert werde. Außerdem werde – anders als es das Statute of Frauds tue – nicht ausdrücklich verlangt, dass die Signatur die Person, welche die Signatur aufgebracht hat, identifizieren könne, es sei denn der Passus in Nr. 8 *„von einer Person ... ausgeführt oder gebilligt“* könne entsprechend ausgelegt werden.[1010] Die Funktionen der Unterschrift gemäß Statute of Frauds werde erst durch eine elektronische Signatur erfüllt, die den Voraussetzungen der fortgeschrittenen elektronischen Signatur der RLeS entspreche.[1011] Anders als die englischen Neuregelungen nennt der UETA die Technik der digitalen Signatur jedoch nicht. Hinsichtlich elektronischer Signaturen nimmt er aber auf ein Sicherheitsverfahren Bezug, also ein Verfahren, …

„das eingesetzt wurde, um zu bestätigen [verifizieren, to verify]*, dass eine elektronische Signatur, Aufzeichnung oder Handlung* [i.S.v. Erfüllung einer (vertraglichen) Verpflichtung] *von einer bestimmten Person stammt, oder um Änderungen oder Fehler der in einer elektronischen Aufzeichnung enthaltenen Information festzustellen. Der Begriff umfasst auch Verfahren, die den Einsatz von Algorithmen oder anderen Codes, Identifikationswörtern oder Identifikationsnummern, von Verschlüsselungs-, Rückruf-* [i.S.v. telefonischer Rückbestätigung] *oder sonstiger Bestätigungsverfahren voraussetzen.“*[1012]

Eine bestimmte Technologie für diese Verfahren ist nicht festgelegt, was Vereinbarungen der Parteien über ein Verfahren ihrer Wahl und den Einsatz des (möglicherweise) jeweils vorgeschriebenen Verfahrens ermöglichen soll.[1013] Es wird differenziert zwischen der weiten Definition der elektronischen Signatur und einem Sicherheitsverfah-

[1009] Kommentar zu § 2 Nr. 7 UETA, www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm: *„ Whether any particular record is ‘signed’ is a question of fact. Proof of that fact must be made under other applicable law. This act simply assures that the signature may be accomplished through electronic means. No specific technology need be used in order to create a valid signature.”*

[1010] Christensen/Duncan/Low, „The Statute of Frauds in the Digital Age – Maintaining Integrity of Signatures“, Murdoch University Electronic Journal of Law, Vol. 10, No. 4, December 2003, www. Murdoch.edu.au/elaw/issues/v10n4/christensen104_ text.html, Abs. 67, 68.

[1011] Christensen/Duncan/Low, Murdoch University Electronic Journal of Law, December 2003, Abs. 73.

[1012] § 2 Nr. 14 UETA: *„ ’Security Procedure’ means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The Term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or call-back or other acknowledgment procedures.”*

[1013] Kommentar zu § 2 Nr. 11 UETA.

ren, das Teil einer elektronischen Signatur sein kann und hier lediglich seiner Funktion nach definiert ist. Dieses Verständnis der elektronischen Signatur lässt neben der auf der PKI fußenden digitalen Signatur beispielsweise bereits jede Namensnennung, den Mausklick oder auch biometrische Verfahren etc. genügen. Es ist zudem ausdrücklich weiter gefasst als der in anderen Regelungen vielfach verwendete Begriff der Authentifizierung.[1014] Anforderungen sicherheitsinfrastruktureller oder technisch-organisatorischer Natur finden sich nicht, da der UETA gerade kein Signaturgesetz sein soll.[1015] Bereits existierende Signaturanbieter können ihre Verfahren weiterhin anbieten, ohne diese technisch nachrüsten zu müssen.[1016]

2.5.2.3 Rechtswirksamkeit elektronischer Signaturen, Aufzeichnungen und Verträge

Die rechtliche Wirkung einer elektronischen Aufzeichnung oder Signatur bestimmt sich nach dem UETA und anderem anwendbarem Recht.[1017] Daran anknüpfend stellt § 7 UETA allgemeine Rechtsgültigkeitsregelungen auf:

> *„a) Einer Aufzeichnung oder Signatur soll nicht allein deshalb die Rechtswirksamkeit oder Durchsetzbarkeit abgesprochen werden, weil sie in elektronischer Form vorliegt.*
>
> *b) Einem Vertrag soll nicht allein deshalb die Rechtswirksamkeit oder Durchsetzbarkeit abgesprochen werden, weil zu seiner Gründung eine elektronische Aufzeichnung eingesetzt wurde.*[1018]

Dies galt bereits für die meisten Rechtsgeschäfte in den USA.[1019] Anschließend geht der UETA aber darüber hinaus[1020]:

[1014] Kommentar zu § 2 Nr. 7 UETA. Umfasst ist auch die existierende Signature Dynamics-Technologie, bei der eigenhändige Unterschriften eingescannt werden. Dass der getippte Name am Ende einer nicht digital signierten Mail genügt, ist gerichtlich bestätigt worden, siehe Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 13/14; *Shattuck v. Klotzbach*, 2001 Mass. Super., LEXIS 642 (Urt. V. 11. Dezember 2001), Menna, VJLT 2001.

[1015] Einzig entscheidender Punkt ist hier der *Wille* des Erklärenden oder Handelnden, seine Willensäußerung oder die Aufzeichnung zu signieren. Kommentar zu § 2 Nr. 7 UETA (zur *electronic signature*): *„In jedem Falle ist der Wille entscheidend, den Ton, das Symbol oder das Verfahren zum Zweck der Signierung dieser Aufzeichnung auszuführen oder zu billigen.“* (*„In any case the critical element is the intention to execute or adopt the sound or symbol or process for the purpose of signing the related record.”)*; siehe auch Kommentar Nr. 5 zu § 9 UETA.

[1016] Menna, VJLT 2001.

[1017] § 5 lit. e) UETA.

[1018] § 7 lit. a) und b) UETA: *„(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form. (b) A contract may not… solely because an electronic record was used in its formation.”*

[1019] Siehe oben unter 1.3.3.2 und 1.3.3.6; Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 13.

[1020] Insbesondere auch im Vergleich zum E-SIGN (siehe nachfolgend 2.5.3.2); Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 6.

„c) Sofern ein Gesetz verlangt, dass eine Aufzeichnung in schriftlicher Form [in writing] *gestaltet sein soll, so erfüllt eine elektronische Aufzeichnung dieses Gesetz.*

d) Sofern ein Gesetz die Unterschrift [signature] *verlangt, so erfüllt eine elektronische Signatur dieses Gesetz.“*[1021]

Hierdurch wird die Prämisse festgeschrieben, dass das Medium einer Aufzeichnung, Signatur etc. dessen rechtliche Bedeutung nicht berührt.[1022] Die Gleichstellung elektronischer Dokumente mit einem Schriftstück zielt insbesondere auf die Zwecke des Statute of Frauds. Allerdings setzt der UETA dafür voraus, dass alle seine Voraussetzungen erfüllt werden.[1023] Elektronische Aufzeichnungen und Signaturen sollen als Äquivalent zu schriftlichen, papiernen Aufzeichnungen und Signaturen (*signatures*, also nicht ausschließlich im Sinne der eigenhändigen Unterschrift) etabliert werden.[1024] Des Weiteren muss ein entsprechender Wille oder eine Vereinbarung zur Ausführung des Rechtsgeschäfts auf elektronischem Wege feststellbar sein.[1025] Die Frage nach der rechtlichen Bedeutung einer elektronischen Aufzeichnung ist zu trennen von der, ob diese Aufzeichnung eine elektronische Signatur enthält.[1026]
Der UETA beschäftigt sich in der Folge ausführlich mit der Feststellung, welche Arten von Formerfordernissen unter welchen (weiteren) Voraussetzungen durch elektronische Aufzeichnungen und Signaturen erfüllt werden können. So bestimmt § 8 UETA hinsichtlich weiterer, aus anderen gesetzlichen Bestimmungen folgenden Schriftform- (und Informations-)Erfordernissen, dass sie mittels einer elektronischen Aufzeichnung erfüllt werden können, wenn diese zum Zeitpunkt ihres Empfanges durch den Empfänger gespeichert werden können.[1027] Die elektronische Aufzeichnung soll gegen deren Empfänger nicht durchsetzbar sein, wenn der Absender verhindert, dass ersterer sie speichert oder ausdruckt.[1028] Damit schafft der UETA eine im US-amerikanischen Recht einzigartige gesetzliche Einrede (*defence*) gegen den elektronischen Vertrag.[1029]
Gemäß § 11 UETA kann eine elektronische Signatur auch die Erfordernisse der notariellen Beurkundung *(to be notarized*), Anerkennung (beziehungsweise Bestätigung, *to*

[1021] § 7 lit. c) und d) UETA: *„(c) If a law requires a record to be in writing, an electronic record satisfies the law. (d) If a law requires a signature, an electronic signature satisfies the law.”*

[1022] Kommentar Nr. 1 zu § 7 UETA. Diese Prämisse ist allerdings auf gesetzliche Vorschriften beschränkt, die die schriftliche Form oder die Unterschrift verlangen. Andere Vorschriften, etwa hinsichtlich bestimmter zu erteilender Informationen, bleiben unberührt; Kommentar Nr. 3 zu § 7 UETA.

[1023] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 564, 577.

[1024] Hinsichtlich aller die Wirksamkeit solcher schriftlichen Formen betreffender Vorschriften, sofern diese nicht durch die spezielleren Vorschriften des UETA geändert werden; Kommentar Nr. 3 S. 5 zu § 7 UETA.

[1025] Kommentar Nr. 2 zu § 7 UETA.

[1026] Kommentar Nr. 5 zu § 7 UETA.

[1027] § 8 lit. a) UETA. Andere Erfordernisse hinsichtlich der Darstellung der Information o.ä. bleiben hiervon unberührt, lit. b) bis d) und Kommentar Nr. 1 zu § 8 UETA.

[1028] § 8 lit. c) UETA.

[1029] Mason, *Electronic Signatures in Law*, S. 235.

be acknowledged), Überprüfung *(to be verified*) oder der eidesstattlichen Erklärung *(to be made under oath*) erfüllen, wenn

> *„die elektronische Signatur der zur Durchführung dieser Handlungen autorisierten Person, zusammen mit allen anderen für diese Handlungen erforderlichen Informationen, der Aufzeichnung oder Signatur beigefügt oder logisch mit ihr verknüpft wird.“*[1030]

Erfordernisse hinsichtlich des Einsatzes von (öffentlichen) Stempeln oder Siegeln (*stamps* und *seals*) werden dadurch beseitigt.[1031] Der Unterschied zum europäischen Recht, wo hierfür die aufwändige Konstruktion der fortgeschrittenen (oder qualifizierten) elektronischen Signatur geschaffen wurde, ist groß.[1032] Gesetzliche Erfordernisse (oder Verpflichtungen) bezüglich der Aufbewahrung bestimmter Aufzeichnungen ([requirement] *that a record be retained* oder *record keeping requirements*), Urkunden oder Dokumente können unter bestimmten Voraussetzungen durch elektronische Aufzeichnungen erfüllt werden, sofern diese

> *„(1) die in der Aufzeichnung dargestellten Informationen akkurat wieder*[geben] *nachdem diese erstmals in ihrer letzten* [oder letztgültigen] *Form als elektronische Aufzeichnung oder anderweitig generiert wurde*[n]*; und*
> *(2) zum Zwecke der späteren Referenz zugänglich* [bleiben]. *“*[1033]

Weitere Anforderungen werden nicht gestellt. Unter denselben Voraussetzungen kann damit auch gesetzlichen Erfordernissen entsprochen werden, die verlangen, dass bestimmte Aufzeichnungen im Original *(in its original form*) vorgelegt (*presented*) oder aufbewahrt werden müssen.[1034] Hierbei soll nicht mehr die Originalität einer Aufzeichnung im Blickpunkt stehen, sondern deren Integrität.[1035] § 18 UETA gestattet es öffent-

---

[1030] § 11 UETA: *„If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.”*

[1031] Kommentar zu § 11 UETA; Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 29. Allerdings hat ein Notar nach US-amerikanischem Recht eine andere Funktion und auch andere, weniger weit reichende Befugnisse, als ein Notar nach deutschem Recht, siehe dazu Miedbrodt, DuD 2000, S. 544, und unter 1.3.3.1.

[1032] Siehe hierzu auch Geis, MMR 2000, S. 673.

[1033] § 12 lit. a) UETA: *„If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which: (1) accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and (2) remains accessible for later reference.“*

[1034] § 12 lit. d) UETA. Gleiches soll für Schecks oder Aufzeichnungen gelten, die als Beweis (*for evidentiary purposes*), zur Überprüfung (*audits*) o.ä. dienen, lit. e) und f).

[1035] Dabei wird das Erfordernis der Genauigkeit (*accuracy*) des § 12 lit. a) Nr. (1) UETA aus den Uniform and Federal Rules of Evidence entliehen. Das der Zugänglichkeit (*accessibility*) aus Nr. (2) soll sicherstellen, dass die Aufzeichnung nicht dadurch verloren geht, dass die ihr zugrunde liegende Technologie obsolet wird, Kommentar Nr. 2 und 3 zu § 12 UETA. Die Rechtsgültigkeit elektronischer Aufzeichnungen und elektronischer Informationen als Original entspricht auch den Uniform Rules of Evidence;

lichen Behörden festzulegen, ob und welche Art elektronischer Aufzeichnungen und Signaturen in der Kommunikation mit ihnen eingesetzt werden können. § 19 UETA stellt sicher, dass Vorschriften der Behörden einer Interoperabilität der in den Bundesstaaten eingesetzten Verfahren nicht im Wege stehen.[1036]

2.5.2.4 Zuordnung elektronischer Aufzeichnungen und Signaturen

In § 13 enthält der UETA ebenfalls eine Beweisregelung dahingehend, dass

> *„in einem Gerichtsverfahren der Beweis mittels einer Aufzeichnung oder Signatur nicht allein deshalb ausgeschlossen werden darf, weil diese in elektronischer Form vorliegt.“*[1037]

Dennoch muss die beweisführende Partei nach wie vor die sonstigen Grundlagen für die Zulassung einer elektronischen Aufzeichnung belegen.[1038] Ein wesentlicher Punkt ist die Zurechnung oder Zuordnung (*attribution*) einer elektronischen Signatur zu einer bestimmten Person. Hier wird der Ansatz des US-amerikanischen Gesetzgebers hinsichtlich elektronischer Dokumente und Signaturen deutlich. Der UETA stellt keine technisch-organisatorischen oder sonstige Anforderungen an den Einsatz elektronischer Signaturen und die ihnen zugrunde liegende Technologie und Infrastruktur. Ob ein bestimmtes Verfahren als (elektronische) Signatur zu werten ist, hängt vom Willen des Signierenden ab. Dabei wäre durchaus zu fragen, ob beispielsweise eine per E-Mail geäußerte Zustimmung zu einem Rechtsgeschäft gleichzeitig auch diesen Willen zu signieren umfasst.[1039] Dieser Wille sowie die Sicherheit und Vertrauenswürdigkeit und damit die Beweiskraft einer elektronischen Signatur sind Tatsachen, die ihrerseits dargelegt werden müssen – wobei eine besondere Vereinbarung der Parteien dienlich sein kann. Dem Ziel der Beweisbarkeit soll dabei das Erfordernis dienen, dass die elektronische Signatur in die Aufzeichnung eingefügt oder mit ihr logisch verknüpft sein muss.[1040] Diese Signaturverfahren können auch die eingangs genannten Sicherheitsver-

---

Kommentar Nr. 6 zu § 12 UETA, der auf die §§ 1001 (3), 1002, 1003 und 1004 Uniform Rules of Evidence verweist.

[1036] Siehe auch Muenchinger, CLSR 2000, S. 380.

[1037] § 13 UETA: *„In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.”* Hier sei nochmals darauf hingewiesen, dass alle Aufzeichnungen, auch elektronische, nach den Federal Rules of Evidence als Originale gelten, was durch die Regelungen des UETA nochmals ausdrücklich bestätigt wird; Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 513.

[1038] Nach den Uniform Rules of Evidence 1001 (3), 1002, 1004 and 1004; Kommentar zu § 13 UETA.

[1039] So Randolph, http://dirt.umkc.edu/files/sof.htm.

[1040] Bei der zweiten Alternative wird das Verfahren der Signatur unabhängig von der zu signierenden Aufzeichnung so gespeichert, dass sie zwecks Beweisführung mit einander in Verbindung zu bringen sind. Siehe dazu Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 13.

fahren umfassen, die dann bei der Darlegung zur *attribution* und Beweiskraft von großer Bedeutung sind.[1041] Allerdings ist an

> *„den Einsatz eines Sicherheitsverfahrens ... durch dieses Gesetz keine rechtliche Wirkung, beispielsweise in Form einer gesetzlichen Vermutung, geknüpft. Gemäß dieses Gesetzes ist der Einsatz eines Sicherheitsverfahrens lediglich eine Methode, den Ursprung oder den Inhalt einer elektronischen Aufzeichnung oder Signatur zu beweisen."*[1042]

Die *attribution* oder Zurechnung ist nicht identisch und nicht zu verwechseln mit der Authentifizierung einer Erklärung, die eine besondere Handlung und einen entsprechenden Willen voraussetzt. Die Zurechnung bestimmt nur den Anspruchsgegner, ist aber ausreichend, um eine Person an eine Transaktion zu binden.[1043] Hinsichtlich der *attribution* stellt § 9 UETA einige Grundsätze auf für die Darlegung oder Beweisführung. Danach ist eine elektronische Aufzeichnung oder elektronische Signatur einer bestimmten Person zuzuordnen, wenn sie eine Handlung (*act*) dieser Person darstellt. Dass es sich um eine Handlung dieser Person handelt, …

> *„kann auf jede Weise dargelegt werden, einschließlich der Darlegung der Wirksamkeit eines Sicherheitsverfahrens, das zum Zweck der Feststellung derjenigen Person eingesetzt wurde, der die elektronische Aufzeichnung oder Signatur zugeordnet werden sollte."* [1044]

Für diese Zurechnung ist bei herkömmlichen papiernen Medien die Unterschrift vielfach die Methode der Wahl. Gleiches soll nun auch für Signaturen im elektronischen Umfeld gelten. Ist eine elektronische Signatur einer Person zugeordnet, gilt dies auch für die signierte elektronische Aufzeichnung.[1045] Dennoch kann auch die übrige, neben der elektronischen Signatur in der elektronischen Aufzeichnung enthaltene Information

---

[1041] Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 21, 22, der dazu ausführt, dass das Recht die Bedeutung von Sicherheitsverfahren für die Feststellung der Wirksamkeit elektronischer Rechtsgeschäfte zunehmend anerkennt. Auch der neue Art. 4A UCC regelt die elektronische Übertragung von Fonds, für die demnach Sicherheitsverfahren eingesetzt werden müssen. Banken können Unterschriften durch diese Verfahren ersetzen.

[1042] Kommentar zu § 2 Nr. 11 UETA: *„The use of a security procedure is not accorded operative legal effect, through the use of presumptions or otherwise, by this Act. In this Act, the use of security procedures is simply one method for proving the source or content of an electronic record or signature."* Die Vergabe eines Gütezeichens wie es durch die Akkreditierung nach dem deutschen Recht ermöglicht wird, ist danach hier nicht nur nicht ausgeschlossen, sondern wäre sogar eine beweiskräftige Tatsache.

[1043] Durch die Zuordnung – gemäß Parteivereinbarung oder Gesetz – wird eine Partei als verantwortlich für eine elektronische Erklärung identifiziert, Muenchinger, CLSR 2000, S. 382.

[1044] § 9 lit. a) UETA: *„An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable."*

[1045] Es sei denn, diese vermeintliche Urheber beweist das Vorliegen von Verfälschungen, Betrug o.ä., wie dies auch bei papiernen Medien der Fall wäre, Kommentar Nr. 1 bis 3 zu § 9 UETA.

genügen, um eine Zuordnung zu begründen.[1046] Diese Regelung berührt andere bestehende Regelungen der *attribution* nicht, sondern soll lediglich sicherstellen, dass sie auch in einem elektronischen Umfeld anwendbar sind.[1047]
Die in den europäischen, deutschen und englischen, aber auch in einigen bundesstaatlichen Signaturregelungen vorgenommenen Typisierungen und Sicherheitsabstufungen der verschiedenen elektronischen und digitalen Signaturen können hier in Form der Sicherheitsverfahren eine bedeutende Rolle spielen, da sie der Authentifizierung dienen können.[1048] Dennoch wurde diese bestimmte Technologie nicht aufgenommen und ihr keine herausgehobene Stellung bei der Zurechnung zugeschrieben. Damit hat es der US-amerikanische Bundesgesetzgeber unterlassen, die behauptete oder angenommene Fälschungssicherheit dieser Verfahren zu einem eindeutig gesetzlich festgestellten rechtlichen Vorteil, beispielsweise einer gesetzliche Sicherheitsvermutung (also Risikoverteilung), zu nutzen.[1049] Die Mühen und Risiken der Beweisführung, auch hinsichtlich der sicherheitsrelevanten Aspekte des eingesetzten Sicherheitsverfahrens, bleiben damit dem Nutzer beziehungsweise dem Dritten überlassen. Dem gegenüber steht allenfalls die Möglichkeit der Parteien, den Einsatz elektronischer Medien abzulehnen oder sich im Rahmen einer Parteivereinbarung auf den Einsatz eines bestimmten Verfahrens zu einigen, im Rahmen der bundesstaatlichen Gesetze auch über Vermutungen hinsichtlich der Authentizität einer elektronischen Aufzeichnung. Daneben bietet der UETA im Unterschied zu den Gesetzen in England, Deutschland und der EU Regelungen zur rechtlichen Behandlung von Fehlern, die beim Einsatz elektronischer Medien auftreten. Ein bestimmtes Verfahren zur Fehlererkennung wird nicht verlangt. Vielmehr regelt § 10 UETA ausführlich die Verantwortlichkeit für bestimmte Fehler, beispielsweise für Veränderungen elektronischer Informationen während der Übermittlung. Auch hier spielt der Einsatz oder das Fehlen von bestimmten Sicherheitsvorkehrungen eine bedeutende Rolle.[1050]

[1046] § 9 UETA lit. b): *„Die* [Rechts-]*Folge einer, gemäß Buchstabe a) einer Person zugeordneten, elektronischen Aufzeichnung oder Signatur bestimmt sich aus dem Kontext und den Umständen zum Zeitpunkt ihrer Generierung, Ausführung oder Annahme, einschließlich Parteivereinbarungen, andernfalls aus Gesetz." („The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law.")* Siehe auch Kommentar Nr. 3 zu § 9.

[1047] Dies soll beispielsweise rechtswirksame computergenerierte Erklärungen ermöglichen, Kommentar Nr. 1 zu § 9 UETA.

[1048] Kommentar Nr. 4 zu § 9 UETA; Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 18, 19.

[1049] Immerhin erklärt der Kommentar zu § 9 UETA, die Aufnahme der Bezugnahme auf Sicherheitsverfahren als ein Mittel der Zurechnung sei hilfreich aufgrund der einzigartigen Bedeutung von Sicherheitsverfahren, Kommentar Nr. 4 zu § 9 UETA: *„Die Bezugnahme auf Sicherheitsverfahren soll nicht zu der Annahme führen, dass andere Formen, eine Zurechnung zu beweisen, weniger Überzeugungskraft haben." („The reference to security procedures is not intended to suggest that other forms of proof of attribution should be accorded less persuasive effect.")*

[1050] Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 23, 24. Auch Fehler durch so genannte *electronic agents*.

2.5.2.5 Transferable Records

Die einzigen weiteren funktionalen Anforderungen an ein Verfahren der Speicherung und Authentisierung elektronischer Aufzeichnungen finden sich in § 16 UETA zu einem besonderen Typ der schriftlichen Form, den übertragbaren Aufzeichnungen (*transferable records*), beziehungsweise übertragbaren Wertpapieren und Dokumenten (*paper negotiable instruments and documents*). Ähnlich der traditionellen Vorstellung vom Original(dokument) kommt es hier auf das Vorliegen eines verkörperten Symbols (*tangible token*) an, der immaterielle Rechte und Verpflichtungen symbolisiert[1051]:

> *„Die extreme Schwierigkeit der Herstellung einzigartiger elektronischer Symbole* [oder Zeichen, *token*]*, welche die besonderen Merkmale eines übertragbaren Wertpapiers oder Dokuments aufweisen, führt dazu, dass die Regeln bezüglich solcher übertragbaren Dokumente und Wertpapiere nicht einfach dahingehend geändert werden können, den Gebrauch elektronischer Aufzeichnungen an Stelle der erforderlichen papiernen schriftliche Form zu verwenden.“*[1052]

Da dennoch der Einsatz elektronischer Mitteilungen und Dokumente ermöglicht werden soll, stellt § 16 UETA an diese und die ihnen zugrunde liegenden Verfahren der Generierung und Übertragung bestimmte Voraussetzungen. Diese Regelungen und Anforderungen stellen die einzige Ausnahme vom oben dargelegten Regelungsansatz des UETA dar, schlicht die Rechtsgültigkeit elektronischer Medien festzustellen.[1053] Sein Anwendungsbereich ist beschränkt auf solche elektronischen Aufzeichnungen, die übertragbare Aufzeichnungen (*transferable records*) ersetzen sollen.[1054] Dies ist nur bei papiernen, schriftlichen Schuldscheinen (*paper promissory notes*) und papiernen Eigentumsurkunden (*paper documents of title*) möglich.[1055] An die Stelle des Besitzes eines solchen papiernen Dokuments tritt die Kontrolle über die elektronische Aufzeichnung. Diese dient gleichzeitig als Substitut für die Übertragung und Übergabe (*delivery*) des immateriellen Rechts (beziehungsweise der entsprechenden, dieses verkörpernde papiernen Urkunde).[1056] Kontrolle einer Person über eine übertragbare (elektronische) Aufzeichnung ist gegeben, wenn

---

[1051] Kommentar Nr. 1 zu § 16 UETA.

[1052] Kommentar Nr. 1 zu § 16 UETA: *„... The extreme difficulty of creating a unique electronic token which embodies the singular attributes of paper negotiable document or instrument dictates that the rules relating to negotiable documents and instruments not be simply amended to allow the use of an electronic record for the requisite paper writing.”*

[1053] Kommentar Nr. 1 und 9 zu § 16 UETA.

[1054] Schriftliche Mitteilungen (*notes*) i.S.d. Art. 3 UCC oder Dokumente i.S.d. Art. 7 UCC, siehe § 16 lit. a) Nr. 1) UETA.

[1055] Kommentar Nr. 2 zu § 16 UETA. Ferner muss der Aussteller ausdrücklich diesem elektronischen Ersatz zugestimmt haben; § 16 lit. a) Nr. 2) UETA.

[1056] Oder auch des Indossaments (*endorsement*), Kommentar Nr. 3 zu § 16 UETA.

„ein Verfahren, das zum Beweis der Übertragung von Rechten durch die übertragbare Aufzeichnung eingesetzt wurde, zuverlässig nachweist [reliably establishes]*, dass diese Person mit derjenigen übereinstimmt, für die die übertragbare Aufzeichnung ausgestellt oder an die diese übermittelt wurde.“*[1057]

Um diesen zuverlässigen Nachweis zu erbringen, muss das Verfahren bestimmte Anforderungen erfüllen. Die übertragbare Aufzeichnung muss dergestalt geschaffen sein, gespeichert und übertragen werden, dass

„1) eine einzige autorisierte [oder zuverlässige, authoritative] *Kopie der übertragbaren Aufzeichnung existiert, die einzigartig, identifizierbar und, mit Ausnahme der Regelungen der Nr. 4), 5) und 6)* [siehe nachfolgend]*, unveränderbar ist;*

2) die autorisierte Kopie diejenige Person, die die Kontrolle für sich beansprucht [asserting control[1058]]*, wie folgt identifiziert:*

A) als diejenige Person für die die übertragbare Aufzeichnung ausgestellt wurde; oder

B) sofern aus der autorisierten Kopie hervorgeht, dass sie übertragen wurde als diejenige Person, der die übertragbare Aufzeichnung zuletzt übermittelt wurde;

3) die autorisierte Kopie derjenigen Person, die die Kontrolle für sich beansprucht, oder ihrem ernannten Vertreter [designated custodian]*, übermittelt und von dieser aufbewahrt wird* [maintained]*;*

4) Kopien oder Veränderungen, die die Angaben zum benannten Abtretungsempfänger [identified assignee] *ändern oder einen weiteren hinzufügen, ausschließlich mit Zustimmung derjenigen Person vorgenommen werden können, die die Kontrolle für sich behauptet;*

5) jede Kopie der autorisierten Kopie und jede Kopie einer Kopie ohne weiteres als solche, mithin als nicht identisch mit der autorisierten Kopie, erkennbar ist; und

6) jede Veränderung der autorisierten Kopie ohne weiteres als selbst autorisiert oder nicht autorisiert erkennbar ist.“[1059]

[1057] § 16 lit. b) UETA: *„A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.“*

[1058] „To assert“ bedeutet behaupten oder beteuern, i.S.v.: *„to state in a strong way“* oder *„to insist“*, siehe PONS *Fachwörterbuch Recht*, S. 22.

[1059] § 16 lit. c) UETA: *„A system satisfies subsection (b), and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that: (1) a single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in paragraphs (4), (5), and (6), unalterable; (2) the authoritative copy identifies the person asserting control as: (A) the person to which the transferable record was issued; or (B) if the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred; (3) the authoritative copy is communicated to*

Sofern diese Anforderungen erfüllt sind und einer Person die Kontrolle über eine übertragbare Aufzeichnung zuerkannt werden kann, ist diese gemäß UETA als Inhaber (*holder*) dieser übertragbaren Aufzeichnung anzusehen und hat damit dieselben Rechte wie ein Inhaber einer vergleichbaren papiernen Urkunde.[1060] Diese Anforderungen können nach Ansicht des Bundesgesetzgebers am wahrscheinlichsten durch den Einsatz eines Trusted-Third-Party-Verzeichnissystems erfüllt werden. Entscheidend sei, dass jedes eingesetzte Verfahren sicherstellt, dass es nur einen Inhaber gibt.[1061] Hier zeigt sich erneut, dass sich der Gesetzgeber durchaus der sehr hohen Sicherheit der PKI-Signaturverfahren bewusst war. Sein Wille, das Gesetz so technologieneutral und offen wie möglich zu halten, und der Zwang, auf bestehende und sehr verschiedene bundesstaatliche Signaturgesetze Rücksicht nehmen zu müssen, verhinderte aber eine Aufnahme dieser Verfahren in den UETA im Sinne einer Ausgestaltung der technisch-organisatorischen Anforderungen. Die Erfüllung der Voraussetzung der einzigen autorisierten (*authoritative*) Aufzeichnung hängt allein davon ab, dass die eingesetzte Technik genau dies sicherstellen kann. Teilweise wird bezweifelt, dass derzeit eine Technik existiert, die dazu in der Lage ist.[1062]

2.5.2.6 Umsetzung

Der UETA war Modell für bundesstaatliche Gesetzgebung zum Vertragsrecht. Ende 2001 hatten 38 Staaten den UETA umgesetzt[1063], im März 2007 47 Bundesstaaten eine Form des UETA eingeführt.[1064] Zwar haben also tatsächlich viele Bundesstaaten den UETA übernommen. In der Umsetzung in den einzelnen Staaten ist jedoch nicht einheitlich, da viele bundesstaatliche Versionen des UETA zahlreiche Ausnahmen und Änderungen aufweisen. Signaturgesetze einzelner Bundesstaaten gehen über den Regelungsbereich des UETA hinaus. Tatsächlich sind so die Bundesgesetze sehr unterschiedlich umgesetzt worden und vielfachen Änderungen unterworfen.[1065]

---

and maintained by the person asserting control or its designated custodian; (4) copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control; (5) each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and (6) any revision of the authoritative copy is readily identifiable as authorized or unauthorized." Diese unbedingten Anforderungen sind aus dem § 105 des geänderten Art. 9 des UCC entnommen, siehe Kommentar Nr. 3 zu § 16 UETA.

[1060] § 16 lit. d) UETA; *holder* gemäß § 1-201(20) des UCC.

[1061] Kommentar Nr. 3 zu § 16 UETA. Siehe den Vergleich zum deutschen Recht in Bezug auf digitale Wertpapiere bei Oberndörfer, CR 2002, S. 358-362.

[1062] Siehe bei Mason, *Electronic Signatures in Law*, S. 232.

[1063] In 2002 hatten Kalifornien und Hawaii ihre bestehenden UETA-Gesetze angepasst, wobei das kalifornische Gesetz dem E-SIGN (siehe nachfolgend unter 2.5.3) entspricht; siehe bei Mason, *Electronic Signatures in Law*, S. 234.

[1064] Siehe bei Mason, *Electronic Signatures in Law*, S. 234.

[1065] Eine stets aktualisierte Aufstellung der bundesstaatlichen Gesetzgebung zur Umsetzung des UETA wurde in 2003 deswegen aufgegeben, siehe Mason, *Electronic Signatures in Law*, S. 233, 235.

2.5.3 Electronic Signature in Global and National Commerce Act

Der Electronic Signature in Global and National Commerce Act (E-SIGN)[1066] vom 30. Juni 2000 ist seit dem 1. Oktober 2000 in Kraft. Er ist in vier Teile unterteilt, dessen erster Rechtsfragen im Zusammenhang mit elektronischen Dokumenten und Signaturen, der zweite Teil elektronische Wertpapiere und der dritte Fragen zu deren internationalen Nutzung behandelt. Der E-SIGN[1067] war als reines Interims-Gesetz konzipiert für die Zeitspanne bis zur Übernahme des UETA.

2.5.3.1 Zielsetzung, Anwendungsbereich und Begriffsbestimmungen

Der E-SIGN sollte für diese Übergangszeit einen einheitlichen rechtlichen Standard für elektronische Signaturen und Dokumente (*records*, Aufzeichnungen) schaffen.[1068] Wie auch der UETA ist der E-SIGN kein Signaturgesetz im eigentlichen Sinne. Ergänzend zum UETA sollte die Nutzung elektronischer Kommunikationsmittel als rechtswirksamer Weg für den Abschluss und die Ausführung von Rechtsgeschäften innerhalb der USA und im Handel mit dem Ausland ermöglicht werden. Hinsichtlich elektronischer Signaturen treffen UETA und E-SIGN nahezu identische Regelungen.[1069] Auch der E-SIGN ist, auf Grundlage des *opt-in*-Ansatzes, allein auf Rechtsgeschäfte bezogen.[1070] Gesetzliche oder rechtliche Vorschriften, die für Verträge und andere Aufzeichnungen die schriftliche Form (*written*) oder die Unterschrift (*signed*) erfordern oder die für diese die nicht-elektronische Form (*non-electronic form*) verlangen, werden nicht eingeschränkt beziehungsweise geändert.[1071] Wie auch beim UETA sind vom Anwendungsbereich des E-SIGN bestimmte Verträge und Aufzeichnungen über Testamente etc., sowie die meisten der unter den Anwendungsbereich des UCC fallenden Rechtsgeschäfte ausgenommen.[1072] Ebenso wie beim UETA wird der Abschluss dieser Rechtsge-

---

[1066] Electronic Signatures in Global and National Commerce Act (2000), Text aus: www.nabl.org/government/106/senate/s761.htm. Die Abkürzung „E-SIGN" findet sich vielfach in der Literatur und wird hier übernommen.

[1067] Einen Überblick bietet Luigs, „The United States Electronic Signatures law (E-SIGN)", K&R 2002, S. 533-537.

[1068] Collier/Shannon/Scott, „Electronic Signatures Legislation".

[1069] Collier/Shannon/Scott, „Electronic Signatures Legislation".

[1070] § 101 lit. b) Nr. 2 E-SIGN. Er *„verlangt von niemandem, der Nutzung und Akzeptanz elektronischer Aufzeichnungen oder elektronischer Signaturen zuzustimmen..."* Auch verlangt der E-SIGN, dass die Vertragsparteien den Willen haben und, anders als vom UETA verlangt, auch tatsächlich bekunden, das Rechtsgeschäft auf elektronischem Wege abzuschließen, und keinesfalls durch die gesetzlichen Vorschriften dazu gezwungen werden; Mason, *Electronic Signatures in Law*, S. 234. Der Wille zum und die Übereinkunft über das elektronische Geschäft kann jedoch auch konkludent geäußert werden; Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 10, 11.

[1071] § 101 lit. b) Nr. 1) E-SIGN.

[1072] Mit Ausnahme der §§ 1-107 und 1-206 und der Art. 2 und 2A; § 103 lit. a) Nr. 1) und Nr. 3) E-SIGN, die dem § 3 lit. b) Nr. 1) und 3) UETA entsprechen. Ferner sind bestimmte, vom UETA umfasste, familienrechtliche Verträge und Aufzeichnungen (§ 103 lit. a) Nr. 2) E-SIGN), gerichtliche Verfügungen

schäfte auf elektronischem Wege dadurch nicht ausdrücklich verboten.[1073] Auch die Begriffsbestimmungen[1074] des E-SIGN stimmen weitestgehend überein mit denen des UETA, so die Begriffe Aufzeichnung und elektronische Aufzeichnung sowie insbesondere die elektronische Signatur als

> „*jede*[r] *elektronische Ton, jedes elektronische Symbol oder jedes elektronische Verfahren, der oder das einem elektronischen Vertrag oder einer elektronischen Aufzeichnung beigefügt oder mit diesem oder dieser logisch verknüpft ist und von einer Person mit dem Willen, diese Aufzeichnung zu signieren, ausgeführt oder gebilligt wurde.*“[1075]

Eine bestimmte Form der elektronischen Signatur wird auch hier nicht bestimmt, ebenso wenig weitere Anforderungen technischer oder organisatorischer Art.[1076] Auch hier genügt also beispielsweise eine PIN, eine digitale Signatur oder der getippte Name. Entscheidend ist, ob die elektronische Signatur der unterzeichnenden Person zugeordnet und insbesondere der entsprechenden Aufzeichnung beigefügt werden kann.[1077]

2.5.3.2 Rechtswirksamkeit elektronischer Signaturen und Verträge

Auch dem E-SIGN liegen als Prinzipien die Anerkennung der Rechtswirksamkeit elektronischer Schriftstücke und elektronischer Signaturen, die Parteiautonomie hinsichtlich des Vertragsschlusses mittels vereinbarter Verfahren oder Prozesse sowie die Nicht-Diskriminierung zu Gunsten spezieller Technologien (oder Provider) zugrunde.[1078] Die zentrale Bestimmung des ersten Teils ist § 101 E-SIGN. Er regelt wie der UETA die Gültigkeit von elektronischen Signaturen, Dokumenten und Verträgen, die Voraussetzungen für die elektronische Aufbewahrung von Dokumenten und die Voraussetzungen für elektronische Beurkundungen und Bestätigungen.[1079] Entsprechend dem UETA be-

---

oder Beschlüsse sowie offizielle Gerichtsurkunden (§ 103 lit. b) E-SIGN) ausgenommen. Gemäß § 103 lit. c) Nr. 1) soll der „Secretary of Commerce" (Wirtschaftsminister) innerhalb von drei Jahren nach Inkrafttreten des E-SIGN diese Ausnahmen überprüfen.

[1073] Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 8

[1074] Neben anderen findet sich z.B. die Definitionen des Verbrauchers, die der in der EU, in England und Deutschland gebräuchlichen entspricht, § 106 Nr. 1 E-SIGN.

[1075] § 106 Abs. 5 E-SIGN: *„…an electronic sound, symbol or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record"*, vgl. auch § 2 Nr. 8 UETA.

[1076] Miedbrodt, DuD 2000, S. 542; Muenchinger, CLSR 2000, S. 380. Eine mündliche Mitteilung oder deren Aufzeichnung soll i.R.d. § 101 (siehe nachfolgend 5.3.2) keine solche Aufzeichnung darstellen, § 106 Nr. 9, 4 und 5 E-SIGN, die dem § 2 Nr. 13, 7 und 8 UETA entsprechen.

[1077] Mason, *Electronic Signatures in Law*, S. 231.

[1078] Muenchinger, CLSR 2000, S. 380.

[1079] Im Zusammenwirken mit dem Statute of Frauds ist es damit möglich, Signaturen und Dokumente auch elektronisch notariell beurkunden und bestätigen zu lassen oder unter Eid abzugeben, dazu Menna, VJLT 2001.

stimmt § 101 lit. a) E-SIGN, dass ungeachtet anderer Gesetze, Rechtsvorschriften oder Rechtsregeln bezüglich Rechtsgeschäften, die den zwischenstaatlichen (im Sinne von zwischen Bundesstaaten der USA) oder Außenhandel betreffen, einer Signatur, einem Vertrag oder einer anderen Aufzeichnung (oder Dokument, *record*) die Rechtswirksamkeit, rechtliche Durchsetzbarkeit und – im Unterschied zum UETA ausdrücklich genannt – die Rechtsgültigkeit nicht allein deshalb verwehrt werden darf, weil diese(s/r) in elektronischer Form vorliegt. Gleiches gilt für einen Vertrag zu dessen Gründung elektronische Dokumente (*electronic records*) genutzt wurden. Auch hier wird lediglich klargestellt, was nach der alten Rechtslage bereits galt.[1080] Gemäß E-SIGN sind also unter Umständen das Anklicken eines „Ich-akzeptiere"-Buttons oder die Verwendung einer digitalen Signatur gleichermaßen rechtlich bindend wie die handschriftliche Unterzeichnung mit Tinte[1081], letztlich sogar auch für verbindliche Rechtsgeschäfte über Immobilien.[1082] Wie auch gemäß UETA kann einer solchen elektronischen Aufzeichnung die rechtliche Wirksamkeit, Gültigkeit oder Durchsetzbarkeit aber dann verweigert werden, wenn sie durch die berechtigte Person nicht aufbewahrt werden und sie den Inhalt nicht akkurat wiedergeben (lesen) kann.[1083]
Die Behörden sind ermächtigt, einzelne Arten von Mitteilungen aus dem Anwendungsbereich auszunehmen. Regelungen zur Erfüllung von Formerfordernissen wie der notariellen Beurkundung etc. durch elektronische Aufzeichnungen sind identisch mit den Bestimmungen des UETA[1084], ebenso die Bestimmungen zur Aufbewahrung von Verträgen und Dokumenten sowie Originalurkunden als elektronische Aufzeichnung.[1085] Behörden können verlangen, dass eine Aufzeichnung gemäß einem bestimmten Standard oder Format eingereicht wird.[1086] Grundsätzlich aber ist es den Behörden untersagt, Rechtsverordnungen oder Richtlinien zu erlassen, die nicht mit § 101 E-SIGN übereinstimmen und insbesondere den Einsatz einer bestimmten Technologie verlangen oder einer bestimmten Technologie eine größere rechtliche Wirkung zumessen.[1087] Da

[1080] Miedbrodt, DuD 2000, S. 542, 543; siehe auch 1.3.3.2 und 1.3.3.6.

[1081] Mason, *Electronic Signatures in Law*, S. 230.

[1082] So kritisch Randolph, http://dirt.umkc.edu/files/sof.htm.

[1083] § 101 lit. e) E-SIGN. Hier ähneln sich die Regelungen von UETA und E-SIGN, Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 15. Ferner soll gemäß § 101 lit. h) E-SIGN eine automatische Willenserklärung (*electronic agent*) wirksam sein, sofern sie der entsprechenden Person zuzurechnen ist.

[1084] § 101 lit. g) und § 11 UETA. § 16 UETA zu Wertpapieren wird in § 201 E-SIGN seinem Inhalt nach übernommen, jedoch auf übertragbare Aufzeichnungen beschränkt, die ein dinglich gesichertes Darlehn (*„a loan secured by real property"*) zum Gegenstand haben, § 201 E-SIGN, in wörtlicher Widergabe des § 16 UETA, dem lediglich ein weiterer Punkt hinzugefügt wurde, § 201 lit. a) (C) E-SIGN.

[1085] § 101 lit. d) Nr. 1 (B) E-SIGN, der im übrigen § 12 lit. a) Nr. 2 UETA entspricht.

[1086] Hinsichtlich der Aufbewahrung von Verträgen und Dokumenten können die Bundesregulierungsbehörde oder solche eines Bundesstaates auch Standards bestimmen, um die Einhaltung der in § 101 lit. d) E-SIGN (und in § 12 UETA) genannten Anforderungen an die Genauigkeit, Integrität und Zugängigkeit solcher Aufzeichnungen sicherzustellen. Siehe § 104 lit. b) Nr. 3 (A) S. 1 E-SIGN.

[1087] § 104 lit. b) Nr. 2 (A) und (C) (iii) E-SIGN. Anforderungen, die eine Verletzung der vorgenannten Grundsätze darstellen, sind erlaubt, wenn dies der Erreichung eines wichtigen öffentlichen Ziels (*important governmental objective*) dient und solange damit nicht der Einsatz einer bestimmten Software oder Hardware gefordert wird, § 104 lit. b) Nr. 3 (A) Satz 2 E-SIGN. Sofern ein überragendes öffentliches Interesse (*compelling governmental interest*) daran besteht, kann die Behörde gemäß § 104 lit. b)

viele bundesstaatliche Gesetze dies in das Ermessen der Verwaltung stellen, ist es bemerkenswert, dass im öffentlich-rechtlichen Bereich Institutionen nicht berechtigt sind, elektronische Dokumente und Signaturen abzulehnen.[1088]

2.5.3.3 Elektronische Signaturen in internationalen Transaktionen

In Bezug auf den internationalen (elektronischen) Geschäftsverkehr verpflichtet der E-SIGN den Wirtschaftsminister (Secretary of Commerce), die Akzeptanz und die Nutzung elektronischer Signaturen auf internationaler Ebene in Übereinstimmung mit § 101 dieses Gesetzes zu fördern. Er soll die notwendigen Maßnahmen treffen, um zum Zweck der Erleichterung des zwischenstaatlichen (*interstate*) und des Außenhandels die aus der elektronischen Signatur folgenden Hindernisse für den Handel weitestgehend auszuschließen oder zu reduzieren. Dabei soll er folgenden Prinzipien folgen[1089]:

> *„(B) Den Vertragsparteien zu erlauben, angemessene Authentifizierungstechnologien und Durchführungsmodelle* [implementation models] *für ihre Transaktionen zu bestimmen, sowie den Parteien zu versichern, dass diese Technologien und Durchführungsmodelle rechtlich anerkannt und durchgesetzt werden.*
>
> *(C) Den Vertragsparteien die Möglichkeit zu geben, in Gerichts- oder anderen Verfahren zu beweisen, dass ihre Authentifizierungsverfahren* [authentication approaches] *und ihr Rechtsgeschäft rechtsgültig sind.*
>
> *(D) Eine nicht diskriminierende Herangehensweise in Bezug auf elektronischer Signaturen und Authentifizierungsmethoden aus anderen Rechtsordnungen.“*[1090]

Und insbesondere:

> *„Die Beseitigung der auf der Papierform basierender Hindernisse für elektronische Rechtsgeschäfte durch Übernahme der relevanten Prinzipien des 1996*

Nr. 3 (B) auch verlangen, dass ein Dokument (*record*) in körperlicher oder papierner Form aufbewahrt wird, § 104 lit. c) Nr. 1 und lit. b) Nr. 3 (B) E-SIGN.

[1088] Miedbrodt, DuD 2000, S. 543

[1089] § 301 lit. a) Nr. 1: *„The Secretary of Commerce shall promote the acceptance and use, on an international basis, of electronic signatures in accordance with the principles specified in paragraph (2) and in a manner consistent with section 101 of this Act. The Secretary of Commerce shall take all actions necessary I a manner consistent with such principles to eliminate or reduce, to the maximum extent possible, the impediments to commerce in electronic signatures, for the purpose of facilitating the development of interstate and foreign commerce.”*

[1090] § 301 lit. a) Nr. 2 (B) bis (D): *„The principles specified in this paragraph are the following: ... (B) Permit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced. (C) Permit parties to a transaction to have the opportunity to prove in court or other proceedings that their authentication approaches and their transactions are valid.(D) Take a non-discriminatory approach to electronic signatures and authentication methods from other jurisdictions.”*

durch die... [UNCITRAL] *verabschiedeten Modellgesetzes für den elektronischen Geschäftsverkehr.“*[1091]

Dieses Modellgesetz der UNCITRAL hatte damit direkten Einfluss auf die gesetzgeberische Aktivität in den USA. Die unter (B) bis (D) dargestellten Prinzipien sind ein Ausfluss dessen. Im Vordergrund steht die Anerkennung der Privatautonomie, insbesondere die Möglichkeit eine bestimmte Authentifizierungstechnologie zu vereinbaren und diese sowie die Gültigkeit ihrer Verträge gerichtlich überprüfen zu lassen.[1092]

2.5.3.4 Umsetzung und Verhältnis zum bundesstaatlichen Recht

§ 102 bestimmt das Verhältnis des E-SIGN zum einzel- bzw. bundesstaatlichen Recht (*state law*).[1093] Danach dürfen die Bestimmungen des § 101 E-SIGN durch bundesstaatliche Gesetze, Rechtsverordnungen oder sonstige rechtliche Regeln nur geändert werden, sofern dadurch der UETA umgesetzt wird.[1094] Ansonsten ist eine Änderung durch *state law* ausgeschlossen, welches an alternative Prozesse weiter reichende rechtliche Folgen knüpft oder die Umsetzung einer bestimmten Technik für die Darstellung, Speicherung, Erstellung, Übertragung oder Authentifizierung von elektronischen Aufzeichnungen (oder Nachrichten) und Signaturen verlangt.[1095] Entgegenstehende lokale Regelungen sollen so verhindert werden.[1096] Die Wahl der gesetzlichen Regelungen ist dabei den Bundesstaaten belassen. Verboten ist ihnen aber der Erlass rechtlicher Vorschriften, die elektronischen Dokumenten und Signaturen die Rechtsgültigkeit absprechen allein weil sie in elektronischer Form vorliegen, sofern dies nicht im E-SIGN ausdrücklich

[1091] § 301 lit. a) Nr. 2 (A): *„... (A) Remove paper-based obstacles to electronic transactions by adopting relevant principles from the Model Law on Electronic Commerce adopted in 1996 by the United Nations Commission on International Trade Law.“* Zu den Modellgesetzen der UNCITRAL siehe nachfolgend unter 2.6.1 und 2.6.2.

[1092] Miedbrodt, DuD 2000, S. 545.

[1093] Ein angemessenes und anwendbares Bundesgesetz (oder Bundesrecht, *federal law*) kann entgegenstehendes bundesstaatliches Recht (*state law*) brechen, bzw. verdrängen (*to preempt*). Grundsätzlich geht Bundesrecht dem bundesstaatlichen Recht dann vor, wenn ersteres dies ausdrücklich bestimmt, wenn das bundesstaatliche Recht mit dem Bundesrecht nicht übereinstimmt und folglich eine klare Politik und Regelung dieser Materie auf Bundesebene verhindert, oder wenn das Bundesrecht bundesstaatliche Regelungen in einem bestimmten Bereich ausschließt, da es diesen selbst gänzlich regelt. Ausführlich: Nimmer, „Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws“, 2000, www.bmck.com/ueta-esign-2.doc, S. 4. Für einen Vorrang des Bundesrechts in dieser Materie wurde nach früherer Rechtsprechung ein tatsächlich grenzüberschreitender Verkehr verlangt. Nach heutiger Rechtsprechung genügt eine bloße Auswirkung auf den *interstate commerce*, welches bei einem grenzüberschreitenden Medium gegeben ist. Damit sind die einzelnen Bundesstaaten an die Regelungen des E-SIGN gebunden, Miedbrodt, DuD 2000, S. 544/545; Nimmer, a.a.O., S. 2.

[1094] § 102 lit. a) Nr. 1 E-SIGN. Siehe auch Collier/Shannon/Scott, „Electronic Signatures Legislation“. Das heißt, bundesstaatliche Gesetze gehen dem E-SIGN nur dort vor, wo sie den UETA umsetzen.

[1095] § 102 lit. a) Nr. 2 E-SIGN.

[1096] Nimmer, „Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws“, S. 2.

erlaubt ist.[1097] Der E-SIGN berührt nicht bundesstaatliche Gesetze über die Zuordnung (*attribution*) oder über Verpflichtungen der Parteien. (Signatur-)Gesetze, die an den Einsatz eines bestimmten Sicherheitsverfahrens (beweisrechtliche) Vermutungen knüpfen, bleiben folglich unberührt.[1098] Wie oben beschrieben entsprechen sich UETA und E-SIGN in ihrem Regelungsgehalt.[1099] Der E-SIGN greift dem UETA nicht vor. Bundesstaatliche Gesetze gehen dem E-SIGN nur dort vor, wo sie den UETA umsetzen.[1100] Die Bundesstaaten waren vor die Wahl gestellt, die Ermöglichungsregeln des E-SIGN zu nutzen oder diese auszuschließen und durch den UETA vollständig zu ersetzen.[1101] Die Regelungen des § 101 E-SIGN dürfen dabei aber durch kein bundesstaatliches Gesetz verdrängt werden, das nicht die hier festgelegte Technikneutralität wahrt.[1102] E-SIGN ist folglich ein *overlay law*, indem es im Übrigen keine Gesetze ändert, jedoch bestimmt, dass allen Rechtsgeschäften im zwischenstaatlichen oder Außenhandel, in denen eine Signatur, ein Vertrag oder eine Aufzeichnung eine Rolle spielt, nicht deshalb die Rechtswirksamkeit oder die Durchsetzbarkeit abgesprochen werden darf, weil sie in elektronischer Form vorliegen.[1103] Das heißt, der E-SIGN berührt andere Bundes- oder bundesstaatlichen Gesetze zu elektronischen Rechtsgeschäften nicht.[1104] Viele Bundesstaaten haben seit Erlass des E-SIGN Gesetze erlassen, die sich am E-SIGN orientieren, um die Wirksamkeit elektronischer Signaturen zu regeln. Insgesamt wird der Effekt des

[1097] Nimmer, „Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws", S. 4 und 5. Einem Gesetz, dass für die Rechtsgültigkeit den Einsatz einer bestimmten Technologie voraussetzt, geht der E-SIGN vor. Regelungen, nach denen bei Vereinbarungen der Parteien über den Einsatz einer bestimmten Technologie diese Technologie Unterschrifts- und Schriftformerfordernisse erfüllt und darüber hinaus eine (gesetzliche) Vermutung (der Authentizität oder Integrität) begründet wird, steht § 102 E-SIGN nicht im Wege.

[1098] Nimmer, „Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws", S. 5, 6 und 10.

[1099] Collier/Shannon/Scott, „Electronic Signatures Legislation".

[1100] Miedbrodt, DuD 2000, S. 544; Muenchinger, CLSR 2000, S. 380. Im jeweiligen bundesstaatlichen (Umsetzungs-)Gesetz sollte daher festgestellt werden, das es den E-SIGN verdrängt. Da der UETA auf solche Fälle beschränkt ist, in denen der Einsatz elektronischer Mittel vereinbart wurde, bliebe der E-SIGN ansonsten auf diejenigen Fälle anwendbar, in denen eine solche Vereinbarung nicht gegeben ist. Nimmer, „Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws", S. 7.

[1101] Nimmer, „Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws", S. 8. Auch Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 9, der ausführt, dass dies zu einer Situation führe, in der der E-SIGN auf einige und der UETA auf andere Rechtsgeschäfte Anwendung fänden, abhängig davon, wie die Bundesstaaten die beiden Gesetze umgesetzt haben. Er weist darauf hin, dass viele Bundesstaaten bei der Umsetzung des UETA diesen teilweise abgeändert haben, so dass fraglich ist, ob diese Abänderungen ihrerseits den E-SIGN verdrängten. Möglicherweise müssten sämtliche Vorschriften beider Gesetze erfüllt werden, damit ein Rechtsgeschäft in allen jeweils entscheidenden Rechtsordnungen rechtskräftig sei.

[1102] Durch § 102 E-SIGN sind die Bundesstaaten daran gehindert eine Technologie dahingehend zu favorisieren, dass sie sie zur einzigen machen, welche die Formerfordernisse erfüllt, Nimmer, „Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws", S. 9. Betroffen hiervon sind Signaturgesetze, welche die technischen und organisatorischen Rahmenbedingungen näher spezifizieren, Miedbrodt, DuD 2000, S. 544; Muenchinger, CLSR 2000, S. 380.

[1103] Siehe oben, § 101 lit. a) E-SIGN; Mason, *Electronic Signatures in Law*, S. 231.

[1104] Mason, *Electronic Signatures in Law*, S. 231; Nimmer, „Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws", S. 6, wendet jedoch ein, der E-SIGN habe den Effekt, dass bundesstaatliche Statutes of Frauds nun entweder die schriftliche Form (*writing*) oder eine elektronische Aufzeichnung (*electronic record*) verlangen müssten.

E-SIGN trotz seines weiten sachlichen Regelungsbereichs auf das substantielle Recht aber als sehr begrenzt beurteilt.[1105]

2.5.4 Uniform Computer Information Transactions Act

Der Uniform Computer Transactions Act (UCITA)[1106] vom September 2000 stellt eine spezifische handelsrechtliche Reaktion des US-amerikanischen Bundesgesetzgesetzgebers auf die neuen Handlungs- und Geschäftsformen des Internets dar.

2.5.4.1 Zielsetzung und Begriffsbestimmungen

Der UCITA ist ein reines Handelsgesetz.[1107] Ansatzpunkt für seine Regelungen sind die Vorschriften des UCC, insbesondere des Art. 2 UCC, der den Warenkauf behandelt – genauer den Kauf von gegenständlichen Waren.[1108] Diese passten nicht zu den neuen Geschäftsmöglichkeiten und bereits etablierten Geschäftsgepflogenheiten des E-Commerce.[1109] Gegenstand des UCITA sind folglich der Kauf von Computerinformationen, einschließlich Software etc. sowie Verträge über den Vertrieb von Information(en) über das Internet.[1110] Dabei unterscheidet er zwei Komponenten solcher Geschäfte: den (herkömmlichen) gegenständlichen (*tangible*) Teil und einen gegenstandslosen (*intangible*). Sein Ziel ist unter anderem, für Computerinformationsgeschäfte (*computer information transactions*) ein klares und einheitliches Recht und dabei moderne und innovative Regeln für den E-Commerce zu schaffen.[1111] Er behandelt daher

[1105] Mason, *Electronic Signatures in Law*, S. 231; Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 9. Auswirkung dieses weiten Regelungsbereichs sei eine unnötige Behinderung der Fähigkeiten der Bundesstaaten, ihre Bürger vor Betrügereien zu schützen.

[1106] Uniform Computer Information Transactions Act, offiziell als UCITA abgekürzt, Text aus: www.law.upenn.edu/bll/ulc/ucita/ucitaFinal00.htm.

[1107] Brennan/Barber, „Why Software Professionals Should Support The Uniform Computer Information Transactions Act“. Zu seiner Entstehungsgeschichte siehe z.B. Fendell/Kennedy, „UCITA Is Coming!!! Part Two: Practical Analysis for Licensors' Counsel“, TCL 2000 Nr. 8, S. 3-18.

[1108] Reine Informationen oder den Verkauf von Software umfasst er nicht (Überlassungsverträge wurden als Lizenzierung behandelt), ebenso wenig Unterstützungs- und Unterhaltungsverträge für Websites oder Internetzugangsverträge.

[1109] Brennan/Barber, „Why Software Professionals Should Support The Uniform Computer Information Transactions Act“; Nimmer, „UCITA: A Commercial Contract Code”, TCL 2000 Nr. 5, S. 3–19, S. 3 und 4.

[1110] Ursprünglich sollte daher der UCITA als neuer Art. 2B in den UCC eingefügt werden; Dreben/Werbach, TCL 2000, S. 12; Fendell/Kennedy, „UCITA is Coming!!! Part Two: Practical Analysis for Licensors' Council“, TCL 2000, S. 3-18, S. 3; Muenchinger, CLSR 2000, S. 382.

[1111] Siehe Brennan/Barber, „Why Software Professionals Should Support The Uniform Computer Information Transactions Act“; Nimmer, TCL 2000, S. 3 und 4. Der Anwendungsbereich des UCITA beschränkt sich auf Rechtsgeschäfte über den Vertrieb von Computerinformationen im weitesten Sinne. Auf den Kauf von anderen Dienstleistungen und Waren bleiben UETA und E-SIGN anwendbar; Muenchinger, CLSR 2000, S. 382. Der E-SIGN ist gemäß § 103 lit. a) Nr. 3 ausdrücklich auch auf solche Rechtsgeschäfte anwendbar, die unter die §§ 1-107 und 1-206 sowie unter Art. 2 und 2A UCC fallen. Gleiches gilt für den UETA, § 3 lit. b) Nr. 2.

zum Teil auch den Bereich der Erfüllung von Formvorschriften durch elektronische Kommunikationsformen. Die Regelungen zu elektronischen Verträgen und Signaturen betreffen unter anderem auch allgemeine und vereinheitlichende Regeln des Online-Vertragsschlusses, Regeln für elektronische Signaturen und zur Zurechnung (*attribution*) elektronischer Signaturen.[1112] *Electronic message* wird dabei definiert[1113] als

> *„eine Aufzeichnung oder Anzeige..., die zum Zweck der Kommunikation mit einer anderen Person oder einem elektronischen Vertreter* [electronic agent] *durch elektronische Mittel* [electronic means] *gespeichert, generiert oder übermittelt wird“.*[1114]

Information besteht laut gem. UCITA aus Daten, Text, Bildern, Tönen, „*mask works*“ oder Computerprogrammen[1115] und umfasst damit die entsprechende Definition im UETA. Eine Kopie ist

> *„das Medium auf dem Information zeitweise oder dauerhaft fixiert ist und von dem aus sie direkt oder mittels einer Maschine oder Einrichtung* [device] *wahrgenommen, reproduziert, genutzt oder übermittelt werden kann.“*[1116]

Computerinformation ist entsprechend definiert als Information in elektronischer Form, die von einem Computer oder durch dessen Nutzung erlangt wird oder die in einer durch einen Computer zu verarbeitenden Form besteht.[1117] Beide Definitionen gibt es nicht im UETA oder dem E-SIGN. Der UCITA beinhaltet auch Zurechnungsregeln und definiert dafür den Begriff Zurechnungs- oder Zuordnungsverfahren (*attribution procedure*) als

---

[1112] Brennan/Barber, „Why Software Professionals Should Support The Uniform Computer Information Transactions Act“.

[1113] Der UCITA definiert eine Vielzahl von Begriffen und übernimmt einige aus dem UCC; Fendell/Kennedy, TCL 2000, S. 9. Die Definitionen der Begriffe elektronisch und Aufzeichnung (*record*) stimmen überein mit denen des UETA und des E-SIGN. Elektronische Aufzeichnung ist nicht definiert. *Electronic* und *record* sind identisch mit den entsprechenden Begriffsbestimmung in UETA und E-SIGN.

[1114] § 102 lit. a) Nr. 28 UCITA: *„’Electronic message’ means a record or display that is stored, generated, or transmitted by electronic means for the purpose of communication to another person or electronic agent.“* Entscheidend ist hier, entsprechend den Definitionen in UETA und E-SIGN, das Merkmal *„durch elektronische Mittel”* (*„by electronic means”*).

[1115] § 102 lit. a) UCITA: „… *einschließlich deren Sammlungen und Zusammenstellungen“*, § 102 lit. a) Nr. 35 UCITA: *„’Information’ means data, text, images, sounds, mask works, or computer programs, including collections and compilations of them.“*

[1116] § 102 lit. a) Nr. 20 UCITA: *„’Copy’ means the medium on which information is fixed on a temporary or permanent basis and from which it can be perceived, reproduced, used, or communicated, either directly or with the aid of a machine or device.“*

[1117] § 102 lit. a) Nr. 10 Satz 1 UCITA: *„’Computer Information’ means information in electronic form which is obtained from or through the use of a computer or which is in a form capable of being processed by a computer.”*

„ein Verfahren zur Feststellung [to verify]*, dass eine elektronische Authentifikation, Anzeige, Mitteilung, Aufzeichnung oder Handlung diejenige einer bestimmten Person ist, oder um Veränderungen oder Fehler in den Informationen zu entdecken. Dieser Begriff umfasst Verfahren, die den Einsatz von Algorithmen oder anderen Codes, Identifikationswörtern oder Identifikationsnummern, Verschlüsselung oder telefonischer Rückbestätigung oder sonstiger Bestätigungen verlangen.“*[1118]

Diese Definition entspricht der des Sicherheitsverfahrens des UETA. Die Beweislast liegt auch hier bei derjenigen Person, die auf einen Vertrag vertraut und ihn durchsetzen will. Die Zurechnung kann dabei unter anderem durch den Nachweis der Effektivität eines solchen *attribution*-Verfahrens erfolgen. Auch der UCITA bietet keine gesetzliche Vermutung. Er schränkt nicht die möglichen Verfahren ein und berührt auch kein bundesstaatliches Signaturgesetz. Anders als UETA und E-SIGN definiert der UCITA aber auch den Begriff Authentifizierung oder Beglaubigung (*authentication*). Darunter ist zu verstehen, das jemand

„etwas [eigenhändig] *unterschreibt* [to sign]*; oder, mit dem Willen eine Aufzeichnung zu signieren, in anderer Art und Weise ein elektronisches Symbol, ein Geräusch* [sound]*, eine Mitteilung oder ein Verfahren durchführt oder anwendet, das sich auf diese Aufzeichnung bezieht, ihr beigefügt wurde oder sonst mit ihr logisch verknüpft oder verbunden ist.“*[1119]

2.5.4.2 Authentication und Zurechnung

Grundsätzlich stellt auch der UCITA die elektronische Form als gleichberechtigt neben die schriftliche Form.[1120] Er folgt dabei den Grundsätzen von E-SIGN und UETA[1121] und bestimmt:

[1118] § 102 lit. a) Nr. 5 UCITA: *„’Attribution procedure’ means a procedure to verify that an electronic authentication, display, message, record, or performance is that of a particular person or to detect changes or errors in information. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgement.”*

[1119] § 102 lit. a) Nr. 5: *„’Authentication’ means: (A) to sign; or (B) with the intent to sign a record, otherwise to execute or adopt an electronic symbol, sound, message, or process referring to, attached to, included in, or logically associated or linked with, that record.“* In Nr. 5 (b) wird die Handlung oder das Verfahren beschrieben, das der elektronischen Signatur in § 106 Nr. 5 E-SIGN und § 2 Nr. 8 UETA entspricht.

[1120] § 107 lit. a) UCITA: *„Einer Aufzeichnung oder Authentifizierung darf die rechtliche Wirksamkeit oder Durchsetzbarkeit nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt.“ („(a) A record or authentication may not be denied legal effect or enforceability solely because it is in electronic form.”)*.

[1121] Dort § 101 lit. a) Nr. 1 E-SIGN und §§ 5 lit. a) und 5 lit. a) und b) UETA.

> *„Dieses Gesetz verlangt nicht, das eine Aufzeichnung oder Authentifizierung durch elektronische Mittel oder in elektronischer Form generiert, gespeichert, gesendet, empfangen oder sonst verarbeitet wird. …*
>
> *In jedem Rechtsgeschäft* [transaction] *kann eine Person Anforderungen hinsichtlich der Art der Authentifizierung* [authentication] *oder Aufzeichnung stellen.“*[1122]

Wie auch UETA und E-SIGN berührt der UCITA ansonsten Bestimmungen zur *attribution* oder Authentifizierung nicht. Vielmehr bezieht sich die Gleichheit zwischen elektronischen und traditionellen Aufzeichnungen nur auf ihre Form.[1123] Gemäß § 213 lit. a) UCITA ist eine elektronische Authentifizierung, Nachricht oder Handlung grundsätzlich dann einer Person zuzurechnen, wenn feststeht, dass es ihre Handlung ist.[1124] Er legt dabei die Beweislast demjenigen auf, der auf diese Authentifizierung etc. vertraut hat.[1125] Entscheidend ist auch hier, dass die Parteien die Form der Authentifizierung bestimmen können, etwa den Einsatz der digitalen Signatur.[1126] Für die Authentifizierung kann zum Beispiel der Einsatz eines autentifizierenden Handlungs- oder Verfahrensablaufs nachgewiesen werden.[1127] Sofern dabei ein vereinbartes oder gesetzlich bestimmtes und wirtschaftlich vernünftiges und angemessenes *attribution*-Verfahren eingesetzt wurde, gilt die Authentifizierung als bewiesen.[1128] Die Zurechnung ist damit noch nicht festgestellt, der Einsatz eines solchen Verfahrens hat jedoch auch hier ein gewisses Gewicht.[1129] Die Effizienz und die wirtschaftliche Vernünftigkeit eines Zurechnungsverfahrens solle das Gericht bestimmen indem es folgende Regeln anwendet:

> *„1) Ein durch Gesetz bestimmtes Zurechnungsverfahren ist für Rechtsgeschäfte im Anwendungsbereich des jeweiligen Gesetzes oder der rechtlichen Regel*[-ung] *wirksam.*
>
> *2) Sofern nicht durch Absatz 1) bestimmt, ist die wirtschaftliche Vernünftigkeit und Wirksamkeit im Lichte des mit dem Verfahren Bezweckten und der wirt-*

[1122] § 107 lit. b) und c) UCITA: *„(b) This Act does not require that a record or authentication be generated, stored, sent, received, or otherwise processed by electronic means or in electronic form. (c) In any transaction, a person may establish requirements regarding the type of authentication or record acceptable to it.”* und lit. d): *„Eine Person, die einen elektronischen Vertreter einsetzt... ist durch die Handlungen des elektronischen Vertreters gebunden...“ („A person that uses an electronic agent… is bound by the operations of the electronic agent…”)* Folglich müssen gesetzliche Schriftform- oder Unterschriftserfordernisse dahingehend interpretiert werden, dass sie auch vorgenannte Aufzeichnungen und Authentifizierungen erlauben; Kommentar Nr. 1 zu § 107 UCITA, www.law.upenn.edu/bll/ulc/ucita/ucitaFinal00.htm.

[1123] Kommentar Nr. 2 zu § 107 UCITA.

[1124] § 213 bestimmt die Zurechnung entsprechend §§ 9 lit. a) Nr. 1 und 2, lit. b) und § 10 UETA.

[1125] § 213 lit. d) UCITA.

[1126] Kommentar Nr. 4 zu § 107 UCITA.

[1127] § 108 lit. a) UCITA: *„Authentication may be proven in any manner, including a showing that a party made use of information or access that could only have been available only if engaged in conduct or operations that authenticated the record or term.“*

[1128] § 108 lit. b) UCITA.

[1129] Kommentar Nr. 3 zu § 108 UCITA.

schaftlichen Umstände zum Zeitpunkt der Parteivereinbarung über das Verfahren oder des Einsatzes des Verfahrens zu ermitteln.

3) Für ein Zurechnungsverfahren kann jede den Umständen entsprechende wirtschaftlich vernünftige Sicherheitsvorrichtung oder Sicherheitsmethode eingesetzt werden.“[1130]

Unter anderem aufgrund der sich fortentwickelnden Technologie solle deren Entwicklung nicht begrenzt werden durch eine Regelung, die (nur) *eine* bestimmte Technologie als angemessen beschreibt. Vielmehr vertraut der US-amerikanische Gesetzgeber darauf, dass die Parteien im Einzelfall eine den wirtschaftlichen und sonstigen Umständen angemessene Zurechnungsmethode anwenden werden[1131], die nicht zwangsläufig auf dem neuesten und höchsten Stand der Technik, die vernünftigste oder gar eine unfehlbare Methode sein müsse. Vielmehr soll abgewogen werden u.a. zwischen den Kosten des Verfahrens im Verhältnis zum Wert der Transaktion, dem ausdrücklichen Willen und der freiwilligen Risikotragung der Parteien.[1132]

2.5.4.3 Änderungen in UCC und Statutes of Frauds

Wie bereits UETA und E-SIGN passt auch der UCITA die *common law*-Konzepte der Manifestierung einer Einwilligung an den elektronischen Kontext an. Danach muss eine Vertragspartei die Möglichkeit haben, die Vertragsklauseln zur Kenntnis zu nehmen, um ihr bewusst zu machen, dass ihr Verhalten als eine Form der Einwilligung verstanden werden kann.[1133] Im März 2000 wurde von der NCCUSL die Änderung einiger Regelungen des UCC beschlossen. Folglich wurde auch im UCC der Begriff *writing* durch *record* in seiner hier ausgeführten Definition und *signature* durch *authentication*

[1130] § 212 UCITA: *„The efficacy, including the commercial reasonableness of an attribution procedure is determined by the court, in making this determination, the following rules apply: (1) An attribution procedure established by law is effective for transactions within the coverage of the statute or rule. (2) Except as otherwise provided in paragraph (1), commercial reasonableness and effectiveness is determined in light of the purposes of the procedure and the commercial circumstances at the time the parties agreed to or adopted the procedure. (3) An attribution procedure may use any security device or method that is commercially reasonable under the circumstances.”*

[1131] Digitale Signaturen sind ausdrücklich nicht ausgenommen; Kommentar Nr. 1 und 3 zu § 212 UCITA.

[1132] Ferner seien einzubeziehen die Auswahl und Alternativen an Verfahren, die übrige von den Parteien eingesetzte Technologie, die Art des Rechtsgeschäfts und deren Umfang und Häufigkeit, die Schwierigkeit der Anwendung eines Verfahrens oder Bildung und Hintergrund der Parteien; Kommentar Nr. 4 zu § 212 UCITA.

[1133] Ausführlich Muenchinger, CLSR 2000, S. 382; Brennan/Barber, „Why Software Professionals Should Support The Uniform Computer Information Transactions Act“ (And What Will Happen If They Don’t)”, www.2bguide.com/docs/proucita4.doc. Siehe § 112 UCITA, insbesondere lit. a) Nr. 1: *„(a) A person manifests assent to a record or term if the person, acting with knowledge of, or after having an opportunity to review the record or term or a copy of it: (1) authenticates the record or term with intent to adopt it;…”*

in seiner hier genannten und auch in die Federal Rules of Evidence übernommenen Definition ersetzt.[1134]

2.5.5 Zusammenfassung und Kritik

Der Bundesgesetzgeber in den USA sah sich vor eine vergleichbare Aufgabe wie die EU-Kommission gestellt. Bereits existierende und teils sehr verschiedene bundesstaatliche Signaturgesetze sollten harmonisiert, unterstützt und ergänzt werden. Hierfür wählte der Bundesgesetzgeber jedoch einen anderen, zur RLeS und dem deutschen SigG konträren Lösungsansatz und mit dem Erlass eines Modellgesetzes und eines Interimsgesetzes, an deren Regelungen sich die bundesstaatlichen Gesetzgeber orientieren sollten, ein anderes Mittel der Harmonisierung. Der Ansatz des Bundesgesetzgebers in den USA ist ein rein marktorientierter, minimalistischer Ansatz der Regelung elektronischer Signaturen und Verträge. Grundsätzlich sollen die Parteien selbst das für Ihren Zweck geeignete Signaturverfahren wählen und vereinbaren. So soll sich die Technik mit der größten oder jeweils angemessenen Sicherheit durchsetzen.[1135]
Die elektronische Signatur wird sehr weit und nur über ihre Funktion definiert, ohne eine bestimmte Technologie zu verlangen. Aufgrund der Technologieneutralität werden auch nur Authentifizierungsverfahren und Zuordnungsverfahren (*attribution procedures*) funktionell beschrieben, ebenso Sicherheitsverfahren, die der Authentifizierung und Zuordnung zu einer Person dienen. Zertifikate werden nicht genannt. Akkreditierungs- oder Genehmigungsverfahren, Kontroll- oder Aufsichtsstrukturen sind nur vage umrissen. Elektronische Signaturen und Aufzeichnungen werden für grundsätzlich rechtswirksam erklärt, ebenso entsprechende Parteivereinbarungen. Die technische Offenheit, Flexibilität und Wettbewerbsneutralität kann als Vorteil des US-amerikanischen Ansatzes gelten[1136], insbesondere vor dem Hintergrund der bereits bestehenden Rechtslage, die elektronische Formen des *writing* und der *signature* grundsätzlich leichter akzeptiert. Diese tatsächliche Technikneutralität folgt auch schon aus dem Zwang, verschiedenste einzelstaatliche Signaturgesetze in ihrem Bestand zu bewahren und einzubeziehen. Allerdings werden deshalb Sicherheitsprobleme im Zusammenhang mit elektronischen Signaturen und Aufzeichnungen mangels genauerer technisch-organisatorischer Vorgaben nicht behandelt.
Da sich die Gleichstellung elektronischer Signaturen und Aufzeichnungen mit herkömmlichen Formen bereits zuvor aus der Anwendung der allgemeinen Definition der

[1134] Nimmer, TCL 2000, S. 7; Muenchinger, CLSR 2000, S. 381 und 382. Die Wertgrenze für Warenkäufe, bei deren Überschreitung gem. UCC 2-201 der Vertrag als Wirksamkeitsvoraussetzung durch eine von den Parteien authentifizierte Aufzeichnung bewiesen werden muss, wurde von 500 auf 5.000 US-$ angehoben. Nach wie vor wird zum Beweis nicht das Original, sondern nur eine Aufzeichnung wie oben beschrieben, verlangt. Die Authentifizierung darf dabei auch mittels Kryptographie erfolgen, auch wenn das Gesetz die akzeptablen Kriterien hierfür spezifiziert. Siehe Muenchinger, CLSR 2000, S. 381; auch Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 577, 578.

[1135] Geis, MMR 2000, S. 673, der ausführt, durch die US-amerikanischen Neuregelungen würde *„die Philosophie des freien Markts für das Internet interpretiert"*; Miedbrodt, DuD 2000, S. 545.

[1136] Zutreffend Geis, MMR 2000, S. 673.

signature ergab, wird die Bedeutung von UETA und E-SIGN für die Erfüllung des Statute of Frauds als insgesamt gering bewertet.[1137] Die Beweiskraft elektronischer Signaturen und Dokumente ist weiter abhängig von der Darlegung ihrer Authentizität und Integrität, etwa über den Nachweis des Einsatzes eines Sicherheitsverfahrens. Über diese kann eine Zuordnung (*attribution*) vorgenommen werden. Der Beweis der Authentifizierung soll gegeben sein, wenn ein vereinbartes oder gesetzlich bestimmtes und wirtschaftlich vernünftiges und angemessenes Zuordnungsverfahren eingesetzt wurde. Vermutungsregeln oder eine Risikoverteilung wurden nicht festgelegt. Es stand zu vermuten, dass der unerfahrene Privatnutzer preisgünstige Verfahren verwendet, deren Qualität der Intention des Gesetzgebers gerade widersprechen kann.[1138] Tatsächlich zeigt die nachfolgend dargestellte Rechtsprechung, dass von den Beteiligten zum Beispiel auch für rechtserhebliche und zum Teil formbedürftige Erklärungen vor allem Kommunikationsformen verwendet werden, die allenfalls einfache elektronische Signaturen darstellen. In der Folge müssten die Gerichte die Voraussetzungen für die Wirksamkeit einer elektronischen Signatur klarstellen, wobei die Beweislast bei demjenigen liegt, der auf die elektronische Signatur etc. vertraut hat. Die Urteile zeigen aber auch, dass auch in den USA elektronische Erklärungen, die den Anforderungen, die § 126b BGB an die Textform stellt, genügen, gesetzliche *writing*- und *signature*-Erfordernisse erfüllen können.[1139] Schon nach dem Gesetz sollen elektronische Aufzeichnungen Erfordernisse der schriftlichen Informationsübermittlung erfüllen können, sofern sie Anforderungen an ihre Beschaffenheit entsprechen, die auch an die deutsche Textform gestellt werden.[1140]

2.5.6 Formen der elektronischen Signatur

Mittlerweile gibt es auch in den USA Rechtsprechung zur Frage, welche Formen elektronischer Signaturen die gesetzlichen Formerfordernisse zum Beispiel der Statutes of Frauds erfüllen können. Im arbeitsrechtlichen Fall *Campbell v. General Dynamics Government Systems Corporation*[1141] wurde zunächst ausdrücklich festgehalten, dass eine E-Mail ein angemessenes Mittel sei, um bestimmte rechtserhebliche Informationen zu übermitteln und Verträge abzuschließen. Hier sei nochmals darauf hingewiesen, dass bei E-Mail eher als bei traditionellem Schriftverkehr die Gefahr besteht, unter die Hearsay Rule zu fallen und dann schon kein zulässiger Beweis zu sein, da sie häufig gerade

[1137] Zutreffend Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 577.

[1138] Kochinke/Geiger, K&R 2000, S. 600.

[1139] Dazu unten unter 3.3.1 und 3.3.2.

[1140] Die Aufbewahrung elektronischer Aufzeichnungen, um entsprechende Erfordernisse zu erfüllen, verlangt den Parteien eine gewisse Flexibilität hinsichtlich der Art der Speicherung ab, wenn sie diese in neue Medien überführen wollen. Gleiches gilt für Bestimmungen zu Originaldokumenten. Miedbrodt, DuD 2000, S. 544; Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 16.

[1141] *Campbell v. General Dynamics Government Systems Corporation*, 321 F.Supp.2d 142 (D.Mass. 2004), affirmed 407 F.3d 546 (1st Cir. 2005).

von einem Ereignis „berichten".[1142] Zudem besteht bei weitergeleiteten oder Antwort-Mails, denen die vorangegangenen Nachrichten angehängt oder beigefügt wurde, die Gefahr des sogenannten *hearsay-within-hearsay*: Veränderungen an dieser weitergeleiteten E-Mail durch den Versender sind für den Empfänger nicht feststellbar, wodurch bei solchen E-Mail-Ketten nicht nur die letzte, als Beweis vorgelegte sondern alle so eingeschlossenen E-Mails authentifiziert (*authenticated*) und zugelassen werden müssen. Allerdings muss das Gericht nur in der Lage sein in legitimer Weise darauf zu schließen, dass das betreffende Dokument authentisch ist. Weiter gehende Fragen der Vertrauenswürdigkeit betreffen dann eher dessen Beweiskraft als die Zulässigkeit.[1143] Hinzu kommt, dass E-Mails vielfach unter Ausnahmen von der Hearsay Rule fallen, etwa als Geschäftsunterlagen nach der *business record exeption*[1144], oder sie gar aufgrund von Briefkopf, Namensangaben, Geschäftskennzeichen, E-Mail-Adresse oder ähnlichem *self-authenticating* sein können.[1145]

In *Florida Department of Agriculture and Consumer Services v. Haire*[1146] wurde einem Richter erlaubt einen Beschluss (*warrant*) mittels elektronischer Signatur zu signieren. Es sei gäbe kein entsprechendes Verbot, solange es der Richter ist, der den Beschluss autorisiert und er dabei die volle Kontrolle über die Benutzung der elektronischen Signatur habe. Im New Yorker Fall *On Line Power Technologies, Inc., v. Square D. Company* wurde ausdrücklich entschieden, dass E-Mails wirksame elektronische Signaturen nach dem Statute of Frauds beinhalteten.[1147] In einem weiteren Fall dort, *Rosenfeld v. Zerneck*, genügte der Austausch zwar nicht für den Vertragsschluss, aber es wurde festgestellt, dass der Name am Ende einer E-Mail eine elektronische Signatur im Sinne des Statute of Frauds darstelle.[1148] Auch in *Bazak International Corp. v. Tarrant Apparel Group*[1149] urteilte das Gericht, dass eine E-Mail *writing* im Sinne des Statute of Frauds darstelle und dass der (getippte) Name des Versenders an dessen Ende und im Briefkopf der Gesellschaft als Unterschrift gelte. Unter Hinweis auf bestehendes *case law* begründete das Gericht:

[1142] Art. VIII, Rule 801 lit. c) Federal Rules of Evidence; Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 371.

[1143] O'Donnell/Lincoln, The Legal Intelligencer, August 13, 2007.

[1144] Art. VIII, Rule 803 Abs. 6 Federal Rules of Evidence; weitere Ausnahmen auch in Rule 804, ausführlicher Borges, Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 371-373; O'Donnell/Lincoln, The Legal Intelligencer, August 13, 2007.

[1145] Gem. Art. IX, Rule 902 Abs. 11 Federal Rules of Evidence, O'Donnell/Lincoln, The Legal Intelligencer, August 13, 2007.

[1146] *Florida Department of Agriculture and Consumer Services v. Haire*, 836 So.2d 1040 (Fla.App. 4 dist. 2003), corrected opinion *Haire v. Florida Department of Agriculture and Consumer Services*, Nos SC03-446 & Sc03-552, 12. Februar 2004.

[1147] Gem. N.Y. State Technology Law § 104 (2003) und 15 U.S.C. § 7001 (2003), siehe *On Line Power Technologies, Inc., v. Square D. Company*, 2004 WL 1171405 (S.D.N.Y.), wobei nicht klar ist, ob die Namensnennung am Ende der E-Mail oder in der E-Mail-Adresse oder beidem zugrunde gelegt wurde.

[1148] *Rosenfeld v. Zerneck*, 776 N.Y.S.2d 458 (Sup. 2004) (New York).

[1149] *Bazak International Corp. v. Tarrant Apparel Group*, 378 F.Supp.2d 377 (S.D.N.Y. 2005) (New York). Allerdings entschied das Gericht auch, dass E-Mails nicht das *writing*-Erfordernis des § 2-201 Abs. 2 UCC erfüllen könnten, da diese Vorschrift E-Mail nicht ausdrücklich als anerkannte Schriftform benenne.

> *„Obwohl E-Mails während ihrer Übertragung unkörperliche* [intangible] *Mitteilungen sind, ist diese Tatsache alleine nicht schädlich für ihre Beurteilung als Schriftform* [writings] *gemäß dem UCC. Postbriefe ausgenommen, sind die regelmäßig von den Gerichten als Erfüllung des ‚Schriftformerfordernisses' des UCC anerkannten Formen der Kommunikation wie Fax, Telex und Telegramm alles nicht verkörperte Formen der Kommunikation während Abschnitten ihrer Übermittlung. So wie mit diesen anerkannten Methoden versendete Mitteilungen als verkörpert gelten können und damit der Definition im UCC genügen, gilt dies für E-Mails ebenso."*[1150]

Auch im *federal case Lamle v. Mattle, Inc.* wurde der in der E-Mail enthaltene Name des Absenders als Erfüllung des *signature*-Erfordernisses in Bezug auf das California Statute of Frauds gewertet mit der auf das kalifornische *common law* gestützten Begründung:

> *„Wir können keinen bedeutsamen Unterschied erkennen zwischen einer getippten Unterschrift auf einem Telegramm und einer E-Mail."*[1151]

Die Frage nach dem Zeitpunkt der *authentication* und der Handlung, mit der der Unterzeichnende einer E-Mail diese Authentifizierung ausdrückt, wurde ebenfalls behandelt. Im digitalen Kontext wird dies nicht der Moment sein, in dem die jeweilige Person ihren Namen eintippt, einen Signaturtext einfügt oder dieser automatisch durch das E-Mail-Programm eingesetzt wird.[1152] In *International Casings Group, Inc. v. Premium Standard Farms, Inc.*[1153] stellte das Gericht fest, dass bei E-Mails, die den Namen des Versenders im Header oder am Ende der E-Mail aufweisen, das Drücken des „Senden"-Buttons den Akt der Authentifizierung und damit eine rechtswirksame Signatur gemäß des Missouri and North Carolina Electronic Transactions Act darstelle. Dieses Urteil war jedoch gestützt auf hinreichende ergänzende Beweise für den Willen der Parteien, diese E-Mails als authentisch anzusehen. Allerdings gab es auch nach Erlass der oben dargestellten Neuregelungen Urteile, die dem Austausch von E-Mails die Erfüllung der Formerfordernisse der Statues of Frauds absprachen.[1154] Entgegen der oben dargestell-

---

[1150] *Bazak International Corp. v. Tarrant Apparel Group*, 378 F.Supp.2d 377 (S.D.N.Y. 2005) (New York): *„Although emails are intangible messages during their transmission, this fact alone does not prove fatal to their qualifying as writings under the UCC. Aside from posted mails, the forms of communication regularly recognized by the courts as fulfilling UCC 'writing' requirement, such a sfax, telex, and telegram, are all intangible forms of communication during portions of their transmission. Just as messages sent using these accepted methods can be rendered tangible, thereby falling within the UCC definition, so too can emails."*

[1151] *Lamle v. Mattle, Inc.*, 394 F.3d 1355 (Fed. Cir. 2005): *„We can see no meaningful difference between a typewritten signature on a telegram and an email."*

[1152] Mason, *Electronic Signatures in Law*, S. 297.

[1153] *International Casings Group, Inc. v. Premium Standard Farms, Inc.*, 358 F.Supp.2d 863 (W.D.Mo. 2005), 2005 WL 486784.

[1154] Siehe z.B. *federal cases Hugh Symons Group, plc. v. Motorola, Inc.*, 292 F.3d 466 (5th Cir. 2002) (Statute of Frauds in Texas) und *General Trading International, Inc. v. Wal-Mart Stores, Inc.*, 320 F.3d 831 (8th Cir. 2003); *Central Illinois Light Company v. Consolidates Coal Company*, 235 F.Supp.2d 916 (C.D.Ill. 2002) (Illinois), wonach der Austausch von E-Mails lediglich beweist, dass die Parteien ver-

ten englischen Entscheidung *SM Integrated Transware Ltd. v. Schenker Singapore (Pte) Ltd.*[1155] wurde auch die automatische Anfügung der E-Mail-Adresse nicht ohne weiteres als *signature* bewertet. In *Poly USA, Inc. v. Trex Company, Inc.*[1156] wird festgestellt, dass dies, entsprechend den grundlegenden Prinzipien, allenfalls dort der Fall sein könne, wo eine entsprechende Absicht des Versenders feststehe. Dieser Wille wiederum muss durch weitere Beweise festgestellt werden können.

Es zeigt sich, dass die oben genannten Sicherheitsverfahren von UETA und E-SIGN und vor allem die digitale Signatur wie auch in der englischen neueren Rechtsprechung zur *electronic signature* in diesen bisherigen Urteilen keine Rolle spielen. Vielmehr wird die Frage behandelt, ob und unter welchen Bedingungen einfache elektronische Signaturen die entsprechenden Formerfordernisse erfüllen können. Hierbei wird im Einzelfall entschieden, ob die Form der elektronischen Signatur und die Umstände ihrer Erstellung beziehungsweise der Abgabe der entsprechenden signierten Erklärung den einzelnen Signaturerfordernissen genügen. Dabei kommen die Gerichte insbesondere bei Formerfordernissen, die gerade auch eine Beweisfunktion haben sollen, vielfach zu dem Ergebnis, dass die einfache elektronische Signatur, jedenfalls unter Berücksichtigung der vorgenannten ergänzenden Beweise oder Indizien, ausreichend ist. Auch hier sind folglich viele Parallelen zur deutschen Textform des § 126b BGB zu erkennen.[1157]

handelten; *Singer v. Adamson*, 2003 WL 2364985 (Mass. Land Ct.) (Massachusetts); *Sel-Lab Marketing, Inc. v. Dial Corp.*, 48 UCC Rep.Serv.2d 482, 2002 WL 1974056 (S.D.N.Y.) (New York), in dem nur eine der E-Mails unterschrieben war; *Hansen v. Transworld Wireless TV-Spokane, Inc.*, 111 Wash. App. 361, 44 P.3d 929, 47. U.C.CC. Rep.Serv.2d 460 (Div. 3 2002), *review denied*, 148 Wash.2d 1004, 60 P.3d 1211 (2003) (Wash. App. Div. 3 2002) (Washington), in dem E-Mails allein als interne Dokumente beurteilt wurden.

[1155] *SM Integrated Transware Ltd. v. Schenker Singapore (Pte) Ltd.* [2005] 2 SLR 651, [2005] SGHC 58, 92; siehe oben 2.4.5.

[1156] *Poly USA, Inc. v. Trex Company, Inc.*, W.D. Va. No. 5:05-CV-0031 (1. März 2006).

[1157] Dazu ausführlich unten unter 3.3.1 und 3.3.2.

2.6 Internationale nichtsstaatliche Regelungsinitiativen

Nachfolgend wird auf die Modellgesetze der United Nations Commission on International Trade Law (UNCITRAL) zum elektronischen Geschäftsverkehr und zu elektronischen Signaturen eingegangen.[1158] Die UNCITRAL ist das zentrale, mit dem internationalen Handelsrecht befasste Organ der Vereinigten Nationen. Sie soll Hindernisse für den internationalen Handel ausräumen oder vermindern, die durch Widersprüchlichkeiten der nationalen Gesetzgebungen entstehen. Dies soll durch die Aufstellung allgemeiner Prinzipien geschehen, die in den einzelnen Staaten übernommen werden.[1159]

2.6.1 UNCITRAL-Modellgesetz zum Elektronischen Geschäftsverkehr

Das Model Law on Electronic Commerce (MLeC) stammt bereits aus dem Jahr 1996, mit Ergänzungen aus dem Jahre 1998.[1160] Das MLeC sollte Hindernisse in Form von Schriftform- und Unterschriftserfordernisse abbauen helfen. Es konzentriert sich zunächst auf die Überarbeitung bestehender Vorschriften im Hinblick auf die Gleichstellung elektronischer Dokumente und Signaturen mit Unterschrift und schriftlicher Form.[1161] Es geht von den Begriffen elektronische Signatur und Datennachricht (*data message*) als elektronisches Gegenstück zum papiernen Dokument[1162] sowie dem Aussteller (*originator*) einer Datennachricht aus.[1163] Der Begriff der Urkunde (*writing*) wird durch den der *data message* ersetzt.[1164] Das MLeC bestimmt, dass Informationen die

---

[1158] Eine ausführliche Darstellung dieser und weiterer Regelungsinitiativen auf internationaler Ebene bietet Bierekoven, *Der Vertragsabschluss via Internet im internationalen Wirtschaftsverkehr*, Köln 2001, S. 337-404. Anzumerken ist, um die Bedeutung der UNCITRAL in diesem Zusammenhang hervorzuheben, folgendes: Im Jahr 2005 hatte die europäische Kommission den Rat der Europäischen Union gebeten, ein Mandat für die Verhandlungen im Rahmen der UNCITRAL über das UN-Übereinkommen zur Vereinfachung elektronischer Vertragsabschlüsse zu erteilen; Kurzinformation ITRB 2005, S. 173. Dieses Übereinkommen ist anschließend als UN-Konvention über die Verwendung elektronischer Kommunikation in internationalen Verträgen verabschiedet worden, siehe nachfolgend unter 2.6.3. Zu Aktivitäten der WTO siehe Leier, „Elektronischer Handel in der Welthandelsorganisation (WTO)“, MMR 2002, S. 781-787. Die Europäische Kommission erkannte bereits 1998 einen Bedarf an einer multilateralen, rechtlich nicht bindenden Internationalen Charta zum E-Commerce zwecks globalen Koordination der Beseitigung von Hindernissen der Online-Wirtschaft durch WTO und OECD. Die USA kritisierten dagegen den Aufbau einer weiteren Aufsichtsbehörde, da es bereits genügend Organe für die Koordinierung der Entwicklung des globalen Marktes gebe. Siehe bei York/Tunkel, S. 459.

[1159] York/Tunkel, S. 463. Das MLeC hat keine bindende Wirkung für die Staaten, soll jedoch Berücksichtigung bei der Überarbeitung nationaler Vorschriften finden; York/Tunkel, S. 95, 82. Die Modellgesetze sollen, im Gegensatz zu Abkommen, eine größere Flexibilität bei der Umsetzung ermöglichen. Die EU Initiativen sind hingegen durch konzertiertes Handeln geprägt. Siehe Blum, K&R 2000, S. 64.

[1160] „51/161 UNCITRAL Model Law on Electronic Commerce” vom 16. Dezember 1996, Text aus: www.uncitral.org/english/texts/electcom/ecommerceindex.htm. Die Abkürzung „MLeC“ wird hier in Anlehnung an die RLeC und RLeS eingeführt, ist jedoch außerhalb dieser Arbeit nicht gebräuchlich.

[1161] Chissick, S. 85.

[1162] Einschließlich E-Mail oder Telefax u.a., Art. 2 lit. a) MLeC: *„For the purposes of this Law: (a) ‘Data message’ means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;…”*; York/Tunkel, S. 82.

[1163] Art. 2 lit. c) MLeC.

[1164] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 78

rechtliche Wirksamkeit, Gültigkeit oder Durchsetzbarkeit nicht allein deshalb verweigert werden darf, weil sie in Form einer Datennachricht vorliegen.[1165] Es bestimmt hierfür das Konzept der schriftlichen Form (*writing*) neu, die auf ihre wesentliche rechtliche Eigenschaft, die Dauerhaftigkeit (oder Beständigkeit, *permanence*), beschränkt wird. Danach erfüllt eine Datennachricht das Erfordernis der Informationsübermittlung in schriftlicher Form, wenn die in ihr enthaltene Information für die spätere Referenz oder Einsichtnahme (*reference*) zugänglich (*accessible*) bleibt.[1166] Dies soll gelten unabhängig davon, ob das jeweilige Schriftformerfordernis zwingenden Charakter hat oder lediglich an die Nichtbeachtung rechtliche Folgen knüpft.[1167] Damit stellt das MLeC niedrige Anforderungen, die mit den entsprechenden englischen und US-amerikanischen Regelungen und auch mit der Textform des § 126b BGB vergleichbar ist.[1168] Gesetzliche Unterschriftserfordernisse können durch Datennachrichten erfüllt werden, wenn eine Methode der Identifizierung des Unterzeichners und zur Anzeige dessen Billigung der in der Datennachricht enthaltenen Informationen eingesetzt wird und diese Methode, im Lichte aller Umstände, einschließlich etwaiger Vereinbarungen, dem Zweck der Datennachricht entsprechend sicher (oder vertrauenswürdig, *„reliable as appropriate for the purpose“*) ist.[1169] Dabei geht das Modellgesetz davon aus, dass sich die rechtliche Gleichsetzung mit der handschriftlichen Unterschrift an den Zwecken der betreffenden Norm zu orientieren hat[1170], wie dies auch nach dem englischen und US-amerikanischen Recht der Fall ist.[1171] Dieser Ansatz entspricht, auch in seiner Orientierung auf die Parteiautonomie und Marktorientierung, am ehesten dem des US-amerikanischen Bundesgesetzgebers.

Wird eine Datennachricht zum Vertragsabschluss eingesetzt, soll dem Vertrag die Rechtswirksamkeit oder -gültigkeit nicht allein aus diesem Grund verweigert werden dürfen.[1172] Datennachrichten sollen auch Erfordernisse hinsichtlich der Aufbewahrung (*retention*) von Dokumenten und Aufzeichnungen erfüllen, sofern die darin enthaltene Information zum Zwecke der späteren Referenz zugänglich bleibt, die Information in

---

[1165] Art. 5 MLeC: *„Information shall not be denied legal effect, validity or enforce- ability solely on the grounds that it is in the form of a data message.”*

[1166] Art. 6 Abs. 1 MLeC: *„Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.”*

[1167] Art. 6 Abs. 2 MLeC.

[1168] Dazu siehe unten 3.3.1 und 3.3.2.

[1169] Art. 7Abs. 1 MLeC: *„Where the law requires a signature of a person, that requirement is met in relation to a data message if: (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.”* Siehe dazu auch unten unter 3.3.3.

[1170] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 73.

[1171] Siehe oben 2.4.4 und 2.5.5.

[1172] Art. 11 Abs. 1 S. 2 MLeC: *„Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.”* Gleiches gilt für jede andere Erklärung von Absender und Empfänger, Art. 12 Abs. 1 MLeC: *„As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.”*

dem Format aufbewahrt wird, in dem es auch generiert wurde, beziehungsweise in einem Format, in dem die Information akkurat wiedergegeben wird, und Herkunft und Empfänger sowie Datum und Zeit von Übermittlung und Empfang identifizierbar sind.[1173] Hierfür sollen Dienste Dritter in Anspruch genommen werden können[1174], grundsätzlich also auch Zertifikate und PKI eingesetzt werden können. Beweisregeln beziehungsweise Beweiszulassungsregelungen (*rules of evidence*) sollen nicht zur Nichtzulassung von Datennachrichten als Beweismittel führen nur aus dem Grund, dass sie in dieser Form (als Datennachricht) vorliegen, oder, wo sie den besten zu erbringende Beweis des Beweisführers darstellen, aus dem Grund, dass sie nicht im Original *(not in its original form*) vorliegen.[1175] Dabei soll unter anderem die Vertrauenswürdigkeit der Art und Weise der Generierung, Speicherung oder Übermittlung der Datennachricht berücksichtigt werden.[1176] Folglich ist das MLeC auf die freie Beweiswürdigung im Einzelfall ausgerichtet und entspricht in ihrer Feststellung der generellen Beweiszulassung den englischen, deutschen und US-amerikanischen Neuregelungen.

Gleiches wie für die Unterschriftserfordernisse gilt auch für solche Erfordernisse, die den Beweis durch das Original verlangen. Bedingung ist, dass eine vertrauenswürdige Zusicherung der Integrität der Information zum Zeitpunkt ihrer ersten Generierung besteht.[1177] Kriterium für die Feststellung der Integrität ist unter anderem, ob die Information vollständig ist. Der Standard der verlangten Vertrauenswürdigkeit soll im Lichte des Zweckes, für den die Information generiert wurde, festgestellt werden.[1178] Daneben finden sich Bestimmungen zur *attribution* von Datennachrichten. Danach soll diese vom Absender stammen, wenn dieser selbst, ein rechtmäßiger Vertreter oder ein „E-Agent" sie abgesendet hat.[1179] Ebenso, wenn ein vereinbartes Verfahren zur Bestimmung des Ausstellers ordnungsgemäß angewandt wird.[1180] Beides ist jedoch voll zu beweisen. Diese *attribution* soll nicht gelten, wenn der Empfänger nicht die nötige Sorgfalt ein-

---

[1173] Art. 10 Abs. 1 MLeC: *„Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied: (a) the information contained therein is accessible so as to be usable for subsequent reference; and (b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and (c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received."*

[1174] Art. 10 Abs. 2 MLeC.

[1175] Art. 9 Abs. 1 MLeC: *„In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence: (a) on the sole ground that it is a data message; or, (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form."*

[1176] Art. 9 Abs. 2 MLeC.

[1177] Art. 8 Abs. 1 MLeC.

[1178] Art. 8 Abs. 3 MLeC: *„For the purposes of subparagraph (a) of paragraph (1): (a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered,… (b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated..."*

[1179] Art. 13 MLeC.

[1180] Art. 13 Abs. 3 MLeC: *„As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if: (a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; …"*

gehalten hat oder Kenntnis von der mangelnden Authentizität der Datennachricht hatte.[1181] Auch hier wird deutlich, dass das MLeC nur grundsätzliche Anforderungen stellt. Spezielle Technologien werden nicht genannt und entsprechend auch keine weitergehenden technisch-organisatorischen Spezifikationen oder Rechtsfolgeregelungen.[1182] Allerdings schafft das MLeC eine widerlegbare Vermutung für die Zuverlässigkeit. Es lässt jedoch auch ausdrücklich Raum für nationale Ausnahmen und regelt die Beweisqualität nicht, so dass nur von einem eingeschränkten Einfluss auf die nationalen Beweisregelungen auszugehen ist.[1183] Dennoch hat das MLeC für zahlreiche Regelungsentwürfe Pate gestanden und auch die RLeS beeinflusst.[1184] Die genannten Anforderungen setzen dennoch einen niedrigen Sicherheitsstandard und tragen zur Sicherstellung der Integrität und Authentizität der Datennachrichten nichts bei, wiewohl die in der RLeS und im deutschen Recht umfassend gesetzlich eingefassten Signier- und Verschlüsselungstechnologien nicht ausgeschlossen sind.

2.6.2 UNCITRAL-Modellgesetz zu Elektronischen Signaturen

Neben dem MLeC hat die UNCITRAL das Modelgesetz zur Elektronischen Signatur (MLeS)[1185] verabschiedet. Sein Anwendungsbereich ist wie der des MLeC auf den Einsatz elektronischer Signaturen in einem handelsrechtlichen Kontext beschränkt. Das MLeS beabsichtigt, zusätzliche Rechtssicherheit hinsichtlich des Einsatzes elektronischer Signaturen zu schaffen. Aufbauend auf dem im MLeC enthaltenen flexiblen Prinzip schafft es die Vermutung, dass elektronische Signaturen, wenn sie bestimmte Kriterien der technischen Vertrauenswürdigkeit einhalten, als Äquivalent zur eigenhändigen Unterschrift behandelt werden sollen. Das MLeS folgt dem technologieneutralen Ansatz. Daneben stellt das MLeS grundsätzliche Verhaltensregeln auf, die helfen sollen, die möglichen Verantwortlichkeiten der verschiedenen Parteien festzustellen.[1186] Das MLeS definiert die elektronische Signatur vergleichbar den oben genannten Definitionen der europäischen, englischen und deutschen Neuregelungen als

> *„Daten in elektronischer Form, die einer Datennachricht* [data message] *angefügt oder logisch mit ihr verknüpft werden und dafür genutzt werden, den Aus-*

[1181] Art. 13 Abs. 4 MLeC, zu den Vermutungsregelungen in MLeC und MLeS siehe auch unter 3.2.2.3.

[1182] Ferner stellt das MLeC in Art. 14 Regelungen zur Empfangsbestätigung auf. Parteivereinbarungen, auch solche, die Bestimmungen des MLeC ändern, werden ausdrücklich als wirksam beschrieben, Art. 4 MLeC.

[1183] Blum, K&R 2000, S. 66.

[1184] Müglich, MMR 2000, S. 8

[1185] UNCITRAL Model Law on Electronic Signatures vom 13 Juli 2001, Text aus: www.uncitral.org/english/texts/electcom/ecommerceindex.htm. Zur Abkürzung „MLeS" gilt das oben zum MLeC gesagte (siehe Fn. 1160).

[1186] Blum, K&R 2000, S. 64; Kurzzusammenfassung der UNCITRAL, www.uncitral.org/en-index.htm.

steller dieser Datennachricht zu identifizieren und dessen Billigung der in der Datennachricht enthaltenen Informationen festzustellen.“[1187]

Das MLeS stellt der elektronischen Signatur wiederum das Element des Zertifikats zur Seite und definiert dieses als Datennachricht oder Aufzeichnung, die die Verbindung zwischen dem Aussteller und den Signaturerstellungsdaten herstellt.[1188] Das MLeS setzt damit Minimalanforderungen an die Signatur, die als funktionelles Äquivalent zur Unterschrift dient.[1189] Unterschriftserfordernisse sollen durch solche elektronischen Signaturen erfüllt werden, die gemäß dem Zweck, für den die Datennachricht generiert oder übermittelt wurde, unter Berücksichtigung aller relevanten Umstande einschließlich Parteivereinbarungen, hinreichend sicher sind (*„as reliable as appropriate for the purpose“*).[1190] Das ist der Fall, wenn sie ausschließlich dem Aussteller zugeordnet ist, dieser die Signaturerstellungsdaten unter seiner alleinigen Kontrolle hatte und jede nachfolgende Veränderung der elektronischen Signatur erkennbar ist. Ferner in Fällen, in denen der Zweck des gesetzlichen (*legal*) Unterschriftserfordernisses darin liegt, Sicherheit hinsichtlich der Integrität der Information sicherzustellen, sofern zusätzlich jede nachträgliche Veränderung dieser Information erkennbar ist.[1191] Damit beinhaltet sie ebenfalls die in den meisten Definitionen zur elektronischen Signatur enthaltenen Elemente. Technisch-organisatorische Anforderungen werden nicht genannt. Vielmehr sollen die Parteien frei sein zu bestimmen, welche elektronische Signatur die Voraussetzungen erfüllt.[1192] Die Möglichkeit, die Vertrauenswürdigkeit (*reliability*) einer elektronischen Signatur in einem Verfahren darzulegen, soll nicht eingeschränkt werden.[1193] Außer im Wege der Parteivereinbarung soll keine bestimmte Methode der Her-

[1187] Art 2 lit. a) MLeS: *„'Electronic signature' means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message.”*

[1188] Art. 2 lit. b) MLeS: *„'Certificate' means a data message or other record confirming the link between a signatory and signature creation data.”* Zertifizierungsdiensteanbieter sollen neben der Zertifikatausstellung weitere Dienste in Verbindung mit elektronischen Signaturen anbieten, Art. 2 lit. e) MLeS: *„'Certification service provider' means a person that issues certificates and may provide other services related to electronic signatures.”*

[1189] Blum, K&R 2000, S. 64.

[1190] Art. 6 Abs. 1 MLeS: *„Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.”* Dies soll gleichermaßen für konstitutive Unterschriftserfordernisse gelten, wie auch für solche, die (lediglich) eine bestimmte Rechtsfolge für ihre Nichteinhaltung vorsehen, Art. 6 Abs. 2 MLeS.

[1191] Art. 6 Abs. 3 lit. a) bis d) MLeS: *„An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if: (a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person; (b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person; (c)any alteration to the electronic signature, made after the time of signing, is detectable; and (d) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.”*

[1192] Art. 7 Abs. 1 und 2 MLeS.

[1193] Art. 6 Abs. 4 lit. a) MLeS.

stellung von elektronischen Signaturen ausgeschlossen oder in ihrer rechtlichen Wirksamkeit beschränkt werden – solange sie den Anforderungen des MLeS oder anderer jeweils anwendbarer Bestimmungen genügt.[1194] Die Festlegung, welche elektronische Signatur diese Anforderungen erfüllt, soll privaten oder öffentlichen, durch den einzelnen Staat ernannten Stellen vorbehalten bleiben.[1195] Der Ansatz der UNCITRAL ist dabei ein marktwirtschaftlich orientierter. Eine Lizenzierungs- oder Genehmigungspflicht wird nicht bestimmt und die Parteiautonomie gilt nur dort nicht, wo die Uniform Rules oder nationales Recht sie ausdrücklich ausschließen. Die UNCITRAL schafft damit einen mittleren Sicherheitsstand, während die EU ein bekanntes Verfahren mit sehr hoher Sicherheit privilegiert. Die vorgeschlagenen Regelungen zur technisch-organisatorischen Infrastruktur können auf jedwedes Signaturverfahren angewandt werden. Es wird deutlich, dass auch das MLeS dem amerikanischen Regelungsansatz sehr ähnlich ist, bei dem die Bundesgesetze die bundesstaatlichen Signaturgesetze, auch die technologiespezifischeren, nicht ändern sondern ergänzen. Das MLeS stellt damit einen Minimalkonsens dar. Dadurch kann eine weitere Harmonisierung der die Sicherheitsinfrastruktur betreffenden zweckmäßigen und notwendigen rechtlichen Ausgestaltungen von nationalen Signaturregelungen nicht befördert werden. Vielmehr birgt die den nationalen Gesetzgebern bei der Ausgestaltung belassene Freiheit gerade die Gefährdung der Rechtsvereinheitlichung.[1196] Mit Ausnahme der in der MLeC festgeschriebenen und auch in die englischen und US-amerikanischen Neuregelungen aufgenommenen allgemeinen Beweiszulässigkeit elektronischer Dokumente, bietet dieser Regelungsvorschlag kein Mehr an Rechtssicherheit und Vorhersehbarkeit. Dies gilt umso mehr als MLeC und MLeS zwar eine begrenzte Haftung vorsehen, auf das Regelungselement der Kontrolle jedoch verzichten und lediglich die Möglichkeit der staatlich oder privat organisierten Prüfstellen für Signaturprodukte beinhalten.

Das MLeS zählt Faktoren auf, die bei der Beurteilung der Vertrauenswürdigkeit der vorgenannten Systeme, Verfahren und Personen zu berücksichtigen seien.[1197] Daneben bestimmt das MLeS die Pflichten und Verantwortlichkeiten der involvierten Parteien. So soll der Aussteller und Unterzeichner vernünftige Vorkehrungen treffen (*exercise reasonable care*), um die unautorisierte Nutzung von Signaturerstellungsdaten zu verhindern.[1198] Wenn ein Zertifikat eingesetzt wird, so sollen die Angaben des Nutzers, sofern sie von Bedeutung sind, richtig und vollständig sein.[1199] Auch der Dritte, der auf

[1194] Art. 3 MLeS. Abweichende Parteivereinbarungen sollen möglich sein, solange diese nach anwendbarem Recht nicht unwirksam würde, Art. 5 MLeS.

[1195] Art. 7 Abs. 1 bis 3.

[1196] So zutreffend Blum, K&R 2000, S. 69

[1197] Art. 10 MLeS. Diese Kriterien stellen keine haftungsbewährten Anforderungen dar, sondern sollen erst bei der gerichtlichen Beurteilung im Einzelfall herangezogen werden. Sie dienen also nur der Klärung und Verdeutlichung.

[1198] Art. 8 MLeS.

[1199] Er soll die vom Zertifizierungsdiensteanbieter angebotenen Sperr- oder Widerrufsdienste unverzüglich nutzen oder andere von ihm vernünftigerweise zu erwartende Maßnahmen ergreifen sofern er Kenntnis erlangt von einer möglichen Einflussnahme auf die Signaturerstellungsdaten etc., Art. 8 Abs. 1 und 2 MLeS: *„(1) Where signature creation data can be used to create a signature that has legal effect, each signatory shall: (a) exercise reasonable care to avoid unauthorized use of its signature creation data; (b) without undue delay, utilize means made available by the certification service pro-*

das Zertifikat oder die elektronische Signatur vertraut, soll vernünftige Maßnahmen ergreifen, um die Vertrauenswürdigkeit der elektronischen Signatur, beziehungsweise die Gültigkeit und Begrenzung des Zertifikats zu überprüfen.[1200] Die EU agiert hier zurückhaltender und regelt lediglich die Haftung der Zertifizierungsstelle. Neu ist, dass damit ein Kriterium für die Bösgläubigkeit formuliert wurde.[1201] Diese ausdrückliche Nennung der Pflichten insbesondere des Dritten ist zu begrüßen und wäre auch in die oben vorgestellten Regelungswerke ohne weiteres einfügbar gewesen. Sie entspricht auch der im *common law* grundsätzlich für den Empfänger angenommenen Pflicht zur Nachprüfung der Authentizität einer Signatur im Falle, dass an dieser Zweifel bestehen.[1202] Für die Pflichten und die Haftung des Zertifizierungsdiensteanbieters bestimmt das MLeS unter anderem, dass dieser vernünftige Vorkehrungen dafür treffen soll, dass alle seine wesentlichen und für das Zertifikat während seiner gesamten Gültigkeitsdauer relevanten oder in das Zertifikat aufgenommenen Angaben richtig und vollständig sind.[1203] Diese Regelung ist konsequent insofern, als dass die in einem Zertifikat notwendigerweise aufzunehmenden Informationen, über das in der Definition genannte hinaus, nicht näher bestimmt werden. Insgesamt aber ist diese Regelung durch den jeweils auslegungsbedürftigen Begriff der vernünftigen Vorkehrungen nicht belastbar. Daneben soll der Zertifizierungsdiensteanbieter einen Verzeichnisdienst vorhalten, mittels dessen Dritte (*relying parties*) ihrer Obliegenheit nachkommen und unter anderem feststellen können, ob der Signierende zum Zeitpunkt der Zertifikatsausstellung die Kontrolle über die Signaturerstellungsdaten innehatte, ob diese gültig waren, welche Methode zur Identitätsfeststellung des Unterzeichners verwandt wurde, ob Wertbegrenzungen oder Haftungsbeschränkungen für bestehen und ob die Signaturerstellungsdaten gültig und unverändert sind.[1204] Ferner soll er einen Sperr- und Widerrufsdienst vorhal-

vider pursuant to article 9, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if: (i) the signatory knows that the signature creation data have been compromised; or (ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised; (c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate. (2) A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph (1)."

[1200] Art. 11 MLeS: *„A relying party shall bear the legal consequences of its failure to: (a) take reasonable steps to verify the reliability of an electronic signature; or (b) where an electronic signature is supported by a certificate, take reasonable steps to: (i) verify the validity, suspension or revocation of the certificate; and (ii) observe any limitation with respect to the certificate."* Zu den Vermutungsregelungen in MLeC und MLeS siehe auch unter 3.2.2.3.

[1201] Blum, K&R 2000, S. 68.

[1202] Siehe dazu auch 3.2.2.3.

[1203] Art. 9 Abs. 1 lit. a) und b) MLeS: *„(1) Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall: (a) act in accordance with representations made by it with respect to its policies and practices; (b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or which are included in the certificate;…"*

[1204] Art. 9 Abs. 1 lit. d) MLeS: *„… (d) provide reasonably accessible means which enable a relying party to ascertain, where relevant, from the certificate or otherwise: (i) the method used to identify the signatory; (ii) any limitation on the purpose or value for which the signature creation data or the cer-*

ten,[1205] vertrauenswürdige Systeme, Verfahren und Personal bei der Ausübung seiner Tätigkeiten einsetzen und für ein Versagen hinsichtlich dieser Anforderungen gegebenenfalls haften.[1206] Mit Ausnahme der Pflicht, die Methode der Identitätsfeststellung erkennbar zu machen, gehen auch diese Haftungstatbestände nicht über das in der RLeS geforderte hinaus. Sobald jedoch ein nationaler Gesetzgeber das Identitätsfeststellungsverfahren ausgestaltet ist eine solche Haftungsregel obsolet. Auch bezüglich der Haftungsregelungen zeigt das MLeS also nur einen Minimalkonsens, auch wenn dieser über das in den Bundesgesetzen und vielen bundesstaatlichen Signaturgesetzen in den USA enthaltene hinaus geht, diesen also als Vorbild und Richtschnur dienen konnte – was zum Teil auch der Fall war. Dennoch können diese Haftungsregelungen weiter konkretisiert werden.

Bei der Bestimmung der Rechtswirksamkeit eines Zertifikats oder einer elektronischen Signatur soll deren Ausstellungs- oder Herkunftsort ebenso unbeachtlich sein wie der der Niederlassung des Vertragspartners.[1207] Ausländische Zertifikate und Signaturen sollen die gleiche rechtliche Wirksamkeit haben wie inländische, sofern sie eine vergleichbare Vertrauenswürdigkeit *(a substantially equivalent of reliability*) bieten.[1208] Maßgeblich sind also die Anforderungen im Anerkennungsstaat. Die Anforderungen an das Signaturverfahren richten sich aber nach dem Recht des Herkunftsstaates.[1209] Auch dies sind lediglich in einer gerichtlichen Einzelfallprüfung einzubeziehenden Aspekte.

Es wird erneut deutlich, was den US-amerikanischen und auch den Regelungsansatz von MLeC und MLeS auszeichnet: Die tatsächliche Sicherheit des jeweiligen Verfahrens wird erst in einer nachfolgenden Prüfung, etwa im gerichtlichen Verfahren, und nur im Einzelfall festgestellt. Bis zu dieser Feststellung bleiben die Parteien auf die jeweiligen verschiedenen Signaturregelungen ihrer Herkunftsstaaten verwiesen oder aber sie können die Rechtswirkung der von ihnen verwendeten Signaturen miteinander vereinbaren. Dieses Regelungskonzept dient nicht der Rechtssicherheit im Sinne einer objek-

tificate may be used; (iii) that the signature creation data are valid and have not been compromised; (iv) any limitation on the scope or extent of liability stipulated by the certification service provider; (v) whether means exist for the signatory to give notice pursuant to article 8 (1) (b); (vi) whether a timely revocation service is offered."

[1205] Art. 9 Abs. 1 lit. e) MLeS.

[1206] Art. 9 Abs. 1 lit. f) MLeS: *„... utilize trustworthy systems, procedures and human resources in performing its services"*, Abs. 2: *„A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph (1)."*

[1207] Art. 12 Abs. 1 MLeS: *„In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had to: (a) the geographic location where the certificate is issued or the electronic signature created or used; or (b) the geographic location of the place of business of the issuer or signatory."* Entscheidend ist nicht der Heimatstaat des Ausstellers, sondern die Zuverlässigkeit des Ausstellungs- und Signaturverfahrens. Siehe auch Blum, K&R 2000, S. 70.

[1208] Art. 12 Abs. 2 MLeS: *„A certificate issued outside* [the enacting State] *shall have the same legal effect in [the enacting State] as a certificate issued in* [the enacting State] *if it offers a substantially equivalent level of reliability."* Und Art. 12 Abs. 3 MLeS: *„An electronic signature created or used outside* [the enacting State] *shall have the same legal effect in* [the enacting State] *as an electronic signature created or used in* [the enacting State] *if it offers a substantially Equivalent level of reliability."*; Art. 12 Abs. 4 MLeS.

[1209] Blum, K&R 2000, S. 70. Grundsätzlich sollen Parteivereinbarungen über die Nutzung bestimmter Arten von elektronischen Signaturen ausreichen für die grenzüberschreitende Anerkennung dieser Signaturen, Art. 12 Abs. 5 MLeS.

tiven Vorhersehbarkeit der rechtlichen Beurteilung. Tatsächlich wird ein Minimalkonsens und nicht mehr als der Status Quo festgeschrieben und lediglich teilweise eine legislative Klärung bewirkt. Zustimmung fanden die Modellgesetze daher bei denjenigen, die auf internationaler Ebene jegliche dirigistischen Maßnahmen als systemfremd und daher nicht durchsetzbar ansahen. International konsensfähig sei danach allein die Marktorientierung, so dass mit den UNCITRAL-Modellgesetzen eine interessengerechte Balance gefunden worden sei, die sich an der streng marktwirtschaftlichen Funktionsweise des Internet orientiere.[1210] In Anbetracht der Fülle und Zersplitterung bestehender Regelungswerke sollte der in dem MLeS zum Ausdruck kommende Konsens in nationalen Systemen eingeführt werden.[1211] Von Interesse waren die Modellgesetze insbesondere für solche Staaten, die die Anforderungen an Signaturverfahren bis dato noch nicht geregelt hatten, was insbesondere auf einige US-amerikanische Einzelstaaten zutraf.[1212]

2.6.3 UN-Konvention über die Verwendung elektronischer Kommunikation in internationalen Verträgen

Im Jahr 2005 wurde UN-Konvention über die Verwendung elektronischer Kommunikation in internationalen Verträgen[1213] verabschiedet und bislang von mehreren Staaten unterzeichnet, darunter jedoch nicht die hier dargestellten Länder Deutschland, England und USA.[1214] Ausgehend vom Ziel der Harmonisierung und Vereinheitlichung des Rechts im internationalen Handel ist sie gedacht als Instrument für den Umgang mit elektronischen Vertragsabschlüssen und für die Beseitigung bestehender Hindernisse für den elektronischen Handel in bestehenden *uniform law conventions* und Handelsabkommen.[1215] Anwendungsbereich sind Verträge zwischen Parteien mit Geschäftssitzen in verschiedenen Staaten, ausgenommen jedoch unter anderem Verträge über den persönlichen, familiären oder Haushaltsgebrauch.[1216] Hier von Bedeutung sind vor allem Art. 8 und 9, die die Voraussetzungen für die Anerkennung von Verträgen in elektroni-

[1210] Diese Balance sei ferner gefährdet durch die viel weniger liberale EU-Richtlinie, die einen Schutz des gemeinsamen Marktes auf hohem Sicherheitsniveau und -standard vertrete. Dies ginge zu Lasten der internationalen Rechtsvereinheitlichung. So Blum, K&R 2000, S. 70, 71.

[1211] Wenigeren, dafür größer angelegten Regelungswerken solle mehr Vertrauen entgegen gebracht werden und dann für eine Region oder ein bestimmtes Rechtssystem zugeschnitten werden. So Baker et al., ILPF 2000.

[1212] Siehe Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 114, 115.

[1213] United Nations Convention in the Use of Electronic Communications in International Contracts, verabschieded von der 53. Versammlung der UN am 23. November 2005, Text aus www.uncitral.org/uncitral_texts/electronic commerce/2005Convention_text.html. Hier abgekürzt als UN-Konvention.

[1214] Die Konvention war zu unterzeichnen bis zum 16.1.2008. Unterzeichnerstaaten sind Zentralafrikanische Republik, China, Iran, Libanon, Madagaskar, Montenegro, Panama, Paraguay, Philippinen, Russische Föderation, Saudi Arabien, Senegal, Sierra Leone, Singapur und Sri Lanka, Stand 3.12.2007 laut www.uncitral.org/uncitral_texts/electronic commerce/2005Convention_status.html.

[1215] Zusammenfassung bei Mason, *Electronic Signatures in Law*, S. 133 ff.

[1216] Art. 1 und 2 UN-Konvention.

scher Form sowie die Anerkennung verschiedener Formerfordernisse und Methoden der Identifizierung der Parteien und der Zustimmung der Parteien behandeln. Den Begriff elektronische Signatur definiert die UN-Konvention nicht. Art. 9 Abs. 3 regelt aber, in Anlehnung an die oben dargestellten Regelungen von MLeC und MLeS[1217] die Vorschriften bezüglich Unterschriften:

> *„Wo das Recht die Unterzeichnung einer Kommunikation oder eines Vertrages verlangt, oder für das Fehlen der Unterschrift Konsequenzen androht, kann diese Voraussetzung in Bezug auf elektronische Kommunikation erfüllt werden indem:*
> *(a) eine Methode zur Identifizierung der Partei und zur Anzeige dessen Billigung der in der elektronischen Kommunikation enthaltenen Informationen eingesetzt wird, und*
> *(b) die eingesetzte Methode entweder:*
> *(i) im Lichte aller Umstände einschließlich etwaig relevanter Vereinbarungen dem Zweck, für den die elektronischen Kommunikation generiert oder kommuniziert wurde, entsprechend sicher* [oder vertrauenswürdig, reliable as appropriate for the purpose] *ist, oder*
> *(ii) tatsächlich, bewiesen entweder über die Methode selbst oder mittels weiteren Beweisen, die oben in Ziffer (a) beschriebenen Funktionen erfüllt hat.“*[1218]

Auch hier ist Kern die Beurteilung der eingesetzten Identifizierungsmethode als *„reliable as appropriate for the purpose“*. Durch die Ergänzungen im Vergleich zu den Vorschriften der MLeC und MLeS liegt in Art. 9 Abs. 3 die Betonung noch mehr auf der Vertrauenswürdigkeit der Methode des Signierens eines Dokuments, dem Zweck für den die Kommunikation geschaffen oder kommuniziert wird und insbesondere darauf, ob diese Signiermethode die genannten Funktionen erfüllt hat. Dieser neue Ansatz erlaubt (weiterhin) die Verwendung jeder Art der elektronischen Signatur. Insgesamt ist dieser Ansatz aber realistischer und pragmatischer.[1219]
Art. 9 Abs. 3 belegt erneut die Bedeutung ergänzender Beweise, um die Erfüllung der in lit. a) genannten Funktionen zu erfüllen. Auch aus den Explanatory Notes geht hervor, dass es für die Prüfung (*validation*) der einzelnen Signatur darauf ankommt, über genügend technische Beweise zu verfügen.[1220] Zu den rechtlichen, technischen und wirt-

[1217] Art. 6 Abs. 1 MLeS und insbesondere Art. 7Abs. 1 MLeC.

[1218] Art. 9 Abs. 3 UN-Konvention: *„Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if: (a) a method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and (b) the method used is either: (i) as reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or (ii) proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.“*

[1219] So auch Mason, *Electronic Signatures in Law*, S. 135.

[1220] Mason, *Electronic Signatures in Law*, S. 136.

schaftlichen Faktoren, die bei der Beurteilung der in Art. 9 Abs. 3 behandelten Signiermethode zu berücksichtigen seien, gehören danach die Fortschrittlichkeit der von den Parteien verwendeten Ausrüstung, die Natur ihrer Handelsbeziehungen, Art und Größe der Transaktion, die Funktion der entsprechenden Formvorschrift in der jeweiligen Rechtsordnung, die Fähigkeiten des Kommunikationssystems, die Erfüllung von Handelsbräuchen und -gewohnheiten, die Bedeutung und den Wert der in der elektronischen Kommunikation enthaltenen Informationen, die Verfügbarkeit alternativer Identifikationsmethoden und die Kosten deren Einsatzes, der Grad der Akzeptanz oder Ablehnung der verwendeten Identifikationsmethode sowie alle anderen relevanten Faktoren.[1221] Diese Kriterien sollen die richtige Interpretation des Prinzips der funktionellen Übereinstimmung (*functional equivalence*) in Bezug auf elektronische Signaturen sicherstellen.[1222] Dieser sogenannte Glaubwürdigkeitstest (*reliability test*), der auch in Art. 7 Abs. 1 lit. b) MLeC auftaucht, soll die Gerichte daran erinnern, auch andere Faktoren als ausschließlich die Technologie bei ihrer Bewertung zu berücksichtigen.[1223] Grundsätzlich können diese Kriterien aber auch durch andere, einfachere Technologien als die qualifizierte elektronische Signatur erfüllt werden.[1224] Vergleichbar mit der Textform des § 126b BGB ist das Erfordernis des Art. 9 Abs. 2 der UN-Konvention in Bezug auf Schriftlichkeits (*writing*)-Erfordernisse, wonach eine elektronische Kommunikation diese dann erfülle, wenn die in ihr enthaltene Information für die nachträgliche Referenz zugänglich ist.

2.6.4 OECD Guidelines for Cryptography Policy

Auch die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (Organisation for Economic Co-Operation and Development, OECD) vertritt den rein marktorientierten Ansatz. Wie bei den UNCITRAL-Modellgesetzen sind ihre Vorschläge nicht bindend. Bereits im Jahre 1997 hatte der Rat der OECD die Guidelines for Cryptography Policy (Guidelines)[1225] gebilligt, deren Prinzipien ebenfalls den nationalen Rechtsordnungen als Richtschnur dienen sollten. Die Guidelines definieren den Begriff Authentifizierung[1226] – eine Definition der elektronischen Signatur findet sich hingegen nicht. Allerdings wird der Begriff Verschlüsselung bestimmt[1227]. Die Guidelines spre-

[1221] § 162 der Explanatory Notes. Sie sind auch spezifischer als die in Art. 9 Abs. 1 RLeC genannten Aspekte, siehe Kilian, „The UN-Convention on the Use of E-Communications in international Contracts“, CRi 2007, S. 101-106, S. 103.

[1222] § 163 der Explanatory Notes.

[1223] § 162 der Explanatory Notes. Siehe auch unten unter 3.2.2.3 und 3.3.3.

[1224] Kilian, CRi 2007, S. 105.

[1225] http://www.oecd.org//dsti/sti/it/secur/prod/crypto1.htm.

[1226] Eine Funktion, um die Gültigkeit einer behaupteten Identität eines Nutzers, Hilfsmittels oder einer anderen Einheit in einem Informations- oder Kommunikationssystem festzustellen, Art. 3 Guidelines: *„…'Authentication' means a function for establishing the validity of a claimed identity of a user, device or another entity in an information or communications system."*

[1227] Als ein Verfahren, die Prinzipien, Mittel und Methoden der Umwandlung von Daten umfasst, um deren Informationsinhalt zu verbergen, deren Authentizität zu bewirken, unbemerkte Veränderungen, deren Nichtanerkennung und oder deren unautorisierten Gebrauch zu verhindern, Art. 3: *„'Cryp-*

chen nicht von Zertifikaten, sondern von Kryptographieschlüsseln[1228] und Schlüssel-Management-Systemen (*key management systems*), die als Systeme für die Erschaffung, Speicherung, Verteilung, Aufhebung, Löschung, Archivierung, Zertifizierung oder Anwendung von Kryptographieschlüsseln definiert werden.[1229] Der Begriff *non-repudiation* wird definiert als etwas mittels Verschlüsselungsmethoden Erlangtes (Eigentum, *property*), dass es einer (natürlichen oder juristischen) Person verwehrt, die Vornahme einer bestimmten Handlung zu leugnen.[1230] Dennoch stellen die Guidelines auf das Element der Verschlüsselung ab, was zu ihrer sonstigen Ausrichtung nicht passt. Die Guidelines verlangen, dass Verschlüsselungsmethoden vertrauenswürdig (*trustworthy*) sein sollen. Hilfreich sei die Evaluierung von Verschlüsselungsmethoden anhand von am Markt akzeptierten Kriterien.[1231] Die Nutzer sollen jede ihnen angemessen erscheinende Verschlüsselungsmethode wählen können. Dabei sollen Personen, die Daten besitzen, kontrollieren, nutzen oder auf sie Zugriff haben, für deren Vertraulichkeit und Integrität verantwortlich und deshalb vepflichtet sein, dafür angemessene Verschlüsselungsmethoden einzusetzen.[1232] Verschlüsselungsmethoden sollten im Wege einer strengen Marktorientierung entwickelt werden und dadurch Schritt halten mit der sich verändernden Technologie, den Bedürfnissen der Nutzer und den Gefahren.[1233] Daneben forderten die Guidelines die Ausgestaltung der Verantwortlichkeiten der Verschlüsselungsdiensteanbieter. Ferner sollte die Verantwortlichkeit der Nutzer für den Fall des Missbrauchs festgeschrieben werden.[1234]

Die Guidelines enthalten keinerlei nähere Anforderungen an technisch-organisatorische Infrastrukturen. Die wenigen konkreten Aspekte, die sich aus den Definitionen und den Prinzipien für die Ausgestaltung einer legislativen Regelung ergeben, sind gleichermaßen in allen oben vorgestellten Regelungswerken enthalten. Vielmehr stellen die Guidelines mit ihrer konsequenten und fast ausschließlichen Marktorientierung einen Gegenpol zum europäischen und zum deutschen Regelungsansatz dar. Es bestehen zahlreiche Überschneidungen mit den Lösungen des US-amerikanischen Bundesgesetzgebers. Dabei wird deutlich, dass die Prinzipien der Parteiautonomie, Selbstverantwortung und Marktfreiheit in den US-Regelungen umfassender und überzeugender ausgestaltet sind,

---

tography' means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use."

[1228] Art. 3 Guidelines.

[1229] Art. 3 Guidelines: *„'Key management system' means a system for generation, storage, distribution, revocation, deletion, archiving, certification or application of cryptographic keys."*

[1230] Art. 3 Guidelines: *„'Non-repudiation' means a property achieved through cryptographic methods, which prevents an individual or entity from denying having performed a particular action related to data."* Siehe dazu auch unten unter3.2.2.2.

[1231] Art. 8 Guidelines, Prinzip Nr. 1.

[1232] Art. 8 Guidelines, Prinzip Nr. 2. Zum Schutz bestimmter öffentlicher Interesse, wie dem Schutz des E-Commerce, soll es dem Staat erlaubt sein, eine Politik einzuführen, die von Verschlüsselungsmethoden die Gewährleistung eines bestimmten Sicherheitsniveaus verlangt.

[1233] Diese Marktorientierung soll sich auch auf die Entwicklung internationaler technischer Standards, Kriterien und Protokolle im Zusammenhang mit Verschlüsselungsmethoden erstrecken; Art. 8 Guidelines, Prinzip Nr. 3.

[1234] Art. 8 Guidelines, Prinzip Nr. 7.

auch und insbesondere hinsichtlich der Technikneutralität. Im Hinblick auf eine Annäherung und weitere Harmonisierung der europäischen und der US-amerikanischen Lösungen sind die hier genannten Prinzipien nicht hilfreich. Eine danach ausgerichtete gesetzgeberische Initiative wäre leicht durchsetzbar, weil sie eine Zurücknahme des staatlichen Einflusses bedeutet, ohne dadurch jedoch tatsächlich die Vertrauenswürdigkeit und Rechtssicherheit zu fördern. Sie stellt nicht mehr als den kleinsten gemeinsamen Nenner dar.

3 Diskussion

Einleitend kann folgende Aussage von *Mason* aus dem Jahr 2006 zur Signaturgesetzgebung und Anpassung der Formvorschriften zitiert werden:

> *„Es ist zu früh, um vorherzusagen wie sich elektronische Signaturen in einem formalen Kontext entwickeln werden, allerdings war der Drang der Gesetzgeber auf der ganzen Welt, die Komplexität digitaler Signaturen als funktionelles Äquivalent zur eigenhändigen Unterschrift zu etablieren, ein bisschen voreilig.“*[1235]

3.1 Kritische Würdigung der Gesetzesinitiativen und Schlussfolgerungen

Das in den US-amerikanischen und englischen Gesetzen erkennbare Grundverständnis der Legislative und die fortbestehenden Rechtsregeln sind Ausdruck der dortigen, auf dem *common law* basierenden Rechtssysteme. Die europäischen Richtlinien sind auf dem kontinentaleuropäischen, auf Kodifikation fußenden Rechtsverständnis aufgebaut und darüber hinaus Resultat eines Kompromisses der Mitgliedstaaten der EU. Laut Europäischer Kommission und deutschem Gesetzgeber bedarf es der größeren staatlichen Intervention, um alle Möglichkeiten des digitalen Marktes auszuschöpfen.[1236] Im Gegensatz wird in den USA ein weitgehend unreguliertes Regime bevorzugt, das der Philosophie des freien Markts ohne regulative gesetzliche Definitionen und Bestimmungen entspricht, in dem die Marktteilnehmer über die Qualität der eingesetzten Verfahren entscheiden.[1237] Diese Lösungsansätze stehen sich hier gegenüber.[1238] Mit einem Fokus auf das Regulierungsmodell der EU soll nachfolgend kurz auf die dargestellten Regelungsansätze kritisch eingegangen werden.

3.1.1 Divergierende nationale Regelungen

Ein wesentliches Ziel der Richtlinien der EU und der Gesetze des Bundesgesetzgebers der USA war die Harmonisierung bestehender und zukünftiger nationaler beziehungs-

---

[1235] *„It is too early to predict how electronic signatures in a formal context will develop, but the rush by legislators across the world to provide for the complexity of digital signatures as a functional equivalent of manuscript signature was somewhat premature”*, Mason, „Electronic Signatures in Practice”, J. High Tech L. 2006/2, S. 148-164, S. 164.

[1236] York/Tunkel, S. 459. Ein leichtes Aufsichtsmoment soll mit sozialer Verantwortung und Verbraucherschutz kombiniert werden. Die OECD favorisiert sogar die Entwicklung der Standardisierung durch die Wirtschaft. Siehe hierzu Baker, „E-Commerce: New Wine in Old Bottles”, ICCLR 2000, S. 293-296, S. 293.

[1237] Geis, MMR 2000, S. 667; Miedbrodt, DuD 2000, S. 545; York/Tunkel, S. 459; siehe auch nachfolgend unter 3.1.3.

[1238] Geis, MMR 2000, S. 673, der einen Wettbewerb der Lösungsansätze von EU und den USA (des Bundesgesetzgebers) erkannte, und Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 76, der einen Wettbewerb der Konzepte quer durch die traditionell unterschiedlichen Rechtsfamilien feststellt.

weise bundesstaatlicher Regelungen zu elektronischen Verträgen und Signaturen. Hinsichtlich der USA ist bereits festgestellt worden, dass dieses Ziel insbesondere in der Signaturgesetzgebung nur ansatzweise erreicht wurde, da viele Bundesstaaten den UETA nur mit einer Vielzahl von Änderungen und Auslassungen übernommen haben. Grund hierfür sind die besonderen Kompetenzregelungen wie sie oben dargelegt wurden.[1239] Die Richtlinien der EU fußen auf einer größeren Kompetenz zur Gesetzgebung auch in den Mitgliedstaaten und haben damit eine größere Durchsetzungschance. Wie alle Richtlinien der EU sind aber auch die RLeC und die RLeS Resultat eines Kompromisses der Mitgliedstaaten der EU. Dies hat vereinzelte Brüche in den Richtlinien zur Folge, auf die oben bereits eingegangen wurde.[1240] Eine tatsächliche Harmonisierung im Sinne einer gleichartigen Regelung konnten auch die RLeC und die RLeS nicht erreichen, was zum Teil auf den verschiedenen Rechtssystemen und damit unterschiedlichen Definitionen, Arten und Funktionen der Formerfordernisse beruht. Dies wird besonders im Vergleich der deutschen und englischen Neuregelungen zu Formvorschriften und der Signaturregelungen deutlich. Wie beschrieben war und konnte es allerdings nicht Ziel von RLeC und RLeS sein, nationale Vorschriften zu Formvoraussetzungen zu vereinheitlichen.[1241] Hinsichtlich der nationalen Formvorschriften hatten die Mitgliedstaaten folglich einen Freiraum bei deren Ausgestaltung und bei der Bestimmung der vom elektronischen Vertragsschluss ausgeschlossenen Rechtsgeschäfte. Welche Rechtsgeschäfte letztlich wann in den Anwendungsbereich der RLeS beziehungsweise der nationalen Gesetzen zu ihrer Umsetzung einbezogen würden, war und ist daher nicht abzusehen und divergiert von Staat zu Staat.[1242] Ein Beispiel sind die recht vorsichtige und restriktive Erlaubnis, die Schriftform des § 126 BGB durch die elektronische Form zu ersetzen, oder der sehr eingeschränkte Anwendungsbereich der Textform nach § 126b BGB, sowie die inhaltlich recht unbestimmte Ermächtigung des Secretary of State, Formerfordernisse anzupassen.

Ein weiterer Grund für divergierende Regelungen ist der den Mitgliedstaaten belassene Spielraum bei der Ausgestaltung der Signaturgesetze und -regelungen. So bedurften die Regeln der RLeS zur elektronischen Signatur weitgehend der Konkretisierung durch die Mitgliedstaaten. Zahlreiche unbestimmte Rechtsbegriffe und die erstrebte Technologieneutralität ließen erheblichen Raum für unterschiedliche Interpretationen und divergierende Anforderungen an Signaturverfahren.[1243] Den Mitgliedstaaten war auch die Möglichkeit belassen, eigene Anforderungen an elektronische Verträge und Signaturen aufrecht zu erhalten oder festzulegen. Diese Freiräume wurden zum Teil kritisiert[1244], ebenso die Einführung einer bloß freiwilligen Akkreditierung. Diese kann den Umstand, dass auf die Feststellung der Erfüllung der gesetzlichen Anforderungen durch ein bestimmtes Signaturverfahren verzichtet wurde, zwar mildern, wirkt aber vornehmlich auf

[1239] Siehe oben 2.5.3.4.

[1240] Siehe oben 2.2 und 2.2.3.

[1241] Siehe oben2.2.1.1 und 2.2.2.1.

[1242] Zutreffend Rennie, CLTR 1999, 240, 241, siehe auch oben unter 2.2.2.10 und 2.2.3.

[1243] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 102-104, 109.

[1244] Z.B. Kye, CLSR 2001, S. 27.

nationaler Ebene.[1245] Die Ausformungen solcher Verfahren divergieren zwischen England und Deutschland erheblich. Zum Beispiel mit der freiwilligen Akkreditierung der Zertifizierungsdiensteanbieter und der qualifizierten elektronischen Signatur nach dem deutschen SigG bestehen Unterschiede zu den englischen Neuregelungen in den ES Reg., die nur den Mindeststandard der RLeS übernehmen. Zwar sind PKI, TTP, Zertifikate und technisch-organisatorische Anforderungen in der RLeS tragende Elemente. Bei der Wurzelzertifizierung, den einzelnen an die Zertifizierungsdiensteanbieter gestellten Anforderungen und deren Kontrolle werden aber große Unterschiede zwischen den EU-Richtlinien, den deutschen und den englischen Umsetzungsregelungen deutlich. Hinsichtlich des Mechanismus zur Einhaltung der Anforderungen und Bedingungen bieten allein die RLeS und insbesondere ihre deutsche Umsetzung ein umfangreiches Geflecht an Organen und Strukturen. In England ist dies nach wie vor freiwilligen, von der Industrie geführten Organen überlassen.[1246] Die Möglichkeit der Mitgliedsstaaten zur Implementierung freiwilliger Akkreditierungssysteme und damit eigener Standards kann für den Markterfolg der auf diesen einzelstaatlichen Standards beruhenden Verfahren große Wirkung haben. Einzelstaatliche Vorschriften können also de facto einen größeren Einfluss haben, als es ihre freiwillige Natur nahe legt.[1247] Unterschiede bestehen auch bei der Umsetzung der Haftungsregelungen der RLeS in England und Deutschland, sowie hinsichtlich der technischen Komponenten und der Produkte für elektronische Signaturen. In Deutschland sind diese in ein wesentlich umfassenderes und rigideres Prüf- und Kontrollsystem eingebunden. In England sind sie teilweise nicht einmal erwähnt und sollen auch nicht geprüft werden. Deutlich wird der unterschiedliche Ansatz der Gesetzgeber auch durch die Aussetzung der entsprechenden Teile des EC-Act.
Diese Freiräume, Regelungslücken und Divergenzen sind grundsätzlich einer Harmonisierung nicht förderlich und führten auch tatsächlich zu einer uneinheitlichen Regelungslandschaft nicht nur zwischen England und Deutschland, sondern in der gesamten EU.[1248] Dass beispielsweise die Frage des Beweiswerts weder in der RLeC noch in der RLeS überhaupt adressiert wird, kann auch – wie *Deutsch* richtig feststellt – nicht dahin verstanden werden, dass keinerlei Regelungsbedarf gesehen und davon ausgegangen

[1245] So auch Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 133: „*Für den internationalen Geschäftsverkehr führt* [die freiwillige Akkreditierung] *kaum weiter.*"

[1246] Daraus wurde teilweise gefolgert, solche Gesetzgeber, auch in den USA, scheuten vor dem Aufwand der Implementierung staatlicher Überwachungs- oder Prüforganen zurück bis klar ist, wie sich der Markt und der Bedarf entwickeln; so Baker et al., ILPF 2000.

[1247] Z.B. die Möglichkeit für die Behörden, für Transaktionen mit ihnen elektronische Signaturen akkreditierter Zertifikatsanbieter zu verlangen; siehe Baker et al., ILPF 2000.

[1248] Zumal die Gestaltungsmöglichkeiten von den Mitgliedstaaten mitunter tatsächlich so genutzt werden, dass das Harmonisierungsziel faktisch kaum erreicht wird. Dazu siehe Rieß, „Selbstregulierungsinstrumente zur vertrauenswürdigen Kommunikation", DuD 2002, S. 532-535, S. 533. Ausführlich Dumortier et al., DuD 2004, S. 141-146, über eine Studie über die Umsetzung der RLeS in den EU-Mitgliedstaaten im Jahr 2004, insbesondere eingehend auf die sehr verschieden ausgestalteten Regelungen zu Überwachungssystemen (s. 142), freiwillige Akkreditierung (S. 142), Überprüfung der Signaturerstellungsprodukte etc. (S. 142), Art. 5 RLeS (S. 142), über die Übernahme der in den Anhängen der RLeS aufgeführten Anforderungen (S. 142, 143). Insgesamt hätten mehrere Staaten eigene technische Standards entwickelt und damit unterschiedliche Anforderungen aufgestellt, oder aber die anderweitige Entwicklung solcher Standards abgewartet, was zu einem Ausbleiben entsprechender Anbieter auf dem Markt geführt habe, S. 143.

wurde, die unterschiedlichen Beweisrechte stünden der Ausbreitung des elektronischen Geschäftsverkehrs nicht entgegen.[1249] Aufgrund der eingangs dargestellten Unterschiede zwischen den Rechtsordnungen, insbesondere in ihren gesetzlichen und rechtlichen Erfordernissen der Form und des Beweisrechts, wurde die relative Freiheit der Mitgliedsstaaten bei der Umsetzung jedoch – und wohl zu recht – als notwendig verteidigt.[1250] Das Beispiel England zeigt zwar, wie ein regulativer, umfassender und beschreibender Ansatz auf Grundlage des EU-Ansatzes – wenn auch in nur beschränktem Maße – in einer seiner Rechtstradition dem marktoffenen Ansatz zugeneigten Rechtsordnung Akzeptanz und Anwendung finden kann. Dies hat auch Gültigkeit für die US-amerikanische Rechtsordnung, auf die dies grundsätzlich übertragen werden kann. Ein Weg wäre folglich, darauf hinzuwirken, dass der Regelungsgehalt dieses europäischen Ansatzes wie er in der RLeC und RLeS zum Ausdruck kommt, konsequent und einheitlich auch in England und den USA sowie anderen *common law*-Staaten umgesetzt und zur Anwendung gebracht wird.[1251] Gegenstand einer solchen Harmonisierung wäre allerdings zunächst und vor allem die Signaturgesetzgebung. Aufgrund der teilweise so verschiedenen Funktionen, Ausformungen, Merkmale und Interpretationen der Formvorschriften zwischen dem deutschen Recht und dem Recht in den *common law*-Staaten England und USA sind einer weiteren Harmonisierung der Formvorschriften Grenzen gesetzt.

3.1.2 Maßgeblichkeit nationalen Rechts hinsichtlich der Formerfüllung

Dennoch könnten einzelne Rechtsgedanken und Regeln rechtsordnungsübergreifend Anwendung finden. So könnten, quasi als alternativer Weg, *rules* und *doctrines* des *common law*, wie sie gerade auch in den Urteilen zu elektronischen Signaturen in England und den USA zum Tragen kommen[1252], gegebenenfalls die Rechtsprechung in vergleichbaren Fällen in Deutschland befruchten. Englische und US-amerikanische Gerichte sehen sich bei der Beurteilung etwa der Beweisfähigkeit und Beweiskraft elektronischer Kommunikation wie E-Mails technisch vor die gleichen Voraussetzungen gestellt. Ihre Beurteilung fällt aber offenbar anders, jedenfalls teilweise differenzierter aus als dies in der Rechtsprechung in Deutschland derzeit der Fall ist.
Die RLeS und so auch das SigG und der EC Act wollen die fortgeschrittene elektronische Signatur mit einer weiter gehenden Rechtsfolge versehen. Sie soll, wenn von einer sicheren Signaturerstellungseinheit erstellt, gegenüber handschriftlichen Unterschriften als rechtlich gleichwertig angesehen werden, sofern sie die Anforderungen für handschriftliche Unterschriften erfüllt.[1253] Die Anforderungen an die handschriftliche Unterschrift finden sich im nationalen Recht der Formvorschriften. Ob die dort festgehaltenen

[1249] Deutsch, „Die Beweiskraft elektronischer Dokumente“, JurPC Web-Dok. 188/2000, Abs. 1-72, Abs. 27.

[1250] So Hoeren, *Grundzüge des Internetrechts*, S. 196.

[1251] Dazu auch nachfolgend unter 3.1.4.

[1252] Siehe 1.3.2.6, 1.3.3.6 sowie 2.4.5 und 2.5.5.

[1253] Erwägungsgrund 20 RLeS, Art. 5 Abs. 1 lit. a) RLeS.

Anforderungen erfüllt werden, also die (fortgeschrittene) elektronische Signatur die jeweiligen Funktionen der handschriftlichen Unterschrift erfüllt, ist nach diesem nationalen Recht zu beurteilen. Dabei unterscheiden einige Rechtsordnungen hinsichtlich dieser Anforderungen je nach dem Zeck der handschriftlichen Unterschrift. Der deutsche Gesetzgeber hat diese Möglichkeit in Bezug auf § 126 BGB allein der digitalen Signatur in Form der fortgeschrittenen elektronischen oder der qualifizierten elektronischen Signatur nach dem SigG zugebilligt und entsprechend die Gesetze so ausgestaltet, dass diese Funktionserfüllung durch einen entsprechenden technisch-organisatorischen und rechtlichen Unterbau und Kontrollmechanismen sichergestellt ist. Um nach englischem Recht die Voraussetzungen der handschriftlichen Unterschrift zu erfüllen, wird die fortgeschrittene elektronische Signatur – wie übrigens jede andere elektronische Signatur – folglich die Funktionen der Unterschrift gemäß dem jeweiligen einzelnen *signature*-Erfordernis erfüllen müssen.[1254] Gerichte in England und den USA beurteilen die Gültigkeit beider Formen, der einfachen elektronischen und der fortgeschrittenen elektronischen beziehungsweise der digitalen Signatur auf die gleiche Weise und nach den gleichen Maßstäben. Dabei wird die Feststellung der Law Commission zu berücksichtigen sein, dass jede elektronische Signatur – gleich wie sicher oder unsicher – das Erfordernis erfülle, dass eine Signatur den Willen des Signierenden wiedergeben solle, das Dokument oder die Mitteilung zu authentifizieren.[1255] Nach englischem Recht kann daher eine fortgeschrittene elektronische Signatur nicht per se eine größere Gültigkeit haben als jede andere Signatur. Gleiches muss grundsätzlich für die Beurteilung von einfachen elektronischen und von mit der europäischen fortgeschrittenen elektronischen Signatur vergleichbaren digitalen Signaturen nach US-Recht gelten.

Deshalb soll auf die der vorgenannten Rechtsprechung in England und den USA zugrunde liegenden *rules* und *principles* eingegangen werden. Die Urteile zu dort als rechtswirksam akzeptierten Formen der elektronischen Signatur betreffen dabei vor allem solche Arten der elektronischen Kommunikation, die vielfach mit der die Textform nach § 126b BGB erfüllenden elektronischen Erklärungen vergleichbar ist. Eine Anwendung dieser aus dem *common law* entlehnten Regeln und Grundsätzen auf elektronische Signaturen in Deutschland wäre eine auf Rechtsvergleichung und rechtswissenschaftlicher Betrachtung fußende Befruchtung und gegebenenfalls Harmonisierung, kein von der EU initiierter, legislativer Prozess.[1256] Bei einer Übertragung bestimmter Rechtsgrundsätze vom *common law* auf das deutsche Recht ist hier jedoch stets zu berücksichtigen, dass diese Rechtsregeln verschiedene in den unterschiedlichen Rechtsordnungen auftretende Probleme lösen sollen, eine Übertragung aber zumindest einen gleich gearteten Zweck einer solchen Regel voraussetzt. So stellen das englische und das US-amerikanische Recht Zulassungsbeschränkungen auf, weshalb zum Beispiel nach US-amerikanischem Recht elektronische mit schriftlichen Dokumenten gleichgestellt werden, um als *original* zu gelten und so die Zulassungsschranken zu überwin-

[1254] Mason, *Electronic Signatures in Law*, S. 151.

[1255] Law Commission „Electronic Commerce: Formal Requirements in Commercial Transactions Advice from the Law Commission", Dezember 2001, 3.28.

[1256] Siehe dazu unten unter 3.3.

den.[1257] Da es im deutschen Recht solche Beschränkungen nicht gibt, kann nicht ohne weiteres auf eine solche Gleichsetzung von elektronischen und schriftlichen Urkunden zum Beispiel nach der ZPO geschlossen werden.[1258]

3.1.3 Gesetzgebung als Regelungsinstrument

Ein wesentlicher Unterschied der der hier verglichenen Lösungsansätze ist die Zurückhaltung in den *common law*- oder *case law*-Rechtsordnungen, bestimmte rechtliche Regeln überhaupt in Gesetzesform zu fassen und diese detailliert auszugestalten. Dies beruht auf der grundsätzlichen Zurückhaltung vor der Aufstellung allgemein abstrakter materieller Rechtsgrundsätze, die nicht aus der Anwendung praktischer Rechtsfälle folgen. Die Legislative soll einzelne Rechtsprobleme regeln, ohne das *common law* grundsätzlich zu ändern. Gesetze müssen auch immer erst durch die Gerichte ausgelegt und angewendet werden, um tatsächlich in das Rechtssystem eingegliedert zu sein, wobei man sich dann in späteren Gerichtsverfahren wiederum auf diese Entscheidungen berufen kann.[1259] Auch zeigt die dargestellte Rechtsprechung aus England und den USA, dass das *common law* auf Grundlage der bestehenden Regeln und Rechtsgrundsätze tatsächlich die neuen Formen der *signature* aufnehmen und sich entsprechend adaptieren kann. Dennoch haben sich auch in den hier vorgestellten *common law*-Staaten Gesetze zur bestimmenden Kraft zur Verfolgung politischer Ziele entwickelt.[1260] Spätestens bei einer Anpassung bestehender gesetzlicher Formerfordernisse ist ein legislatives Vorgehen unabdingbar, wie sich zum Beispiel in England an der Ermächtigung des Secretary of State zur Änderung gesetzlicher Formerfordernisse durch *statutory instruments*, also legislative Regelungen, zeigt.[1261]
Grundsätzlich können strenge Kontrollen und stark ausgeweitete bürokratische Strukturen kontraproduktiv wirken, gerade im E-Commerce. Gleiches kann für gesetzliche Vorschriften gelten, die nicht durch Parteivereinbarung ausgeschlossen oder abgeändert werden können. Deshalb, so eine Ansicht, werde eine spezifische Signaturgesetzgebung, die sich nicht nur darauf beschränke, elektronische Signaturen als generell rechtswirksam zu erklären, letztlich eher schaden als nützen. Gesetzgebung solle, für das *common law* typisch, erst dann einsetzen, wenn identifizierbare Probleme bezüglich eines bereits bestehenden Sachverhalts auftauchten, nicht bevor dieser sich überhaupt herausgebildet habe. Es könne nicht vorhergesehen werden, ob ein heute verabschiedetes Signaturgesetz in der Zukunft die damit verfolgten Ziele auch tatsächlich errei-

[1257] Siehe oben 1.3.2.5, 1.3.3.5.

[1258] Deutsch, JurPC Web-Dok. 188/2000, Abs. 33; siehe auch Vergleich der Textform mit *writing* und *signature* im englischen und US-amerikanischen Recht in 3.3.1.

[1259] Miedbrodt in Bizer et al., S. 279, 280.

[1260] Smedinghoff/Hill Bro, JMJCIL 1999, S. 37: *„We live in an age of statutes…“*.

[1261] Siehe oben 2.4.2.4.

che.[1262] Diese Argumente stellen jedoch keinen hinreichenden Grund dar, grundsätzlich auf legislatives Handeln zu verzichten. Sie sind im Bezug auf die Frage der Formerfüllung durch elektronische Kommunikation zum Teil auch zeitlich überholt. Es steht allerdings nicht fest, dass beispielsweise der Ansatz, lediglich die Rechtsgültigkeit elektronischer Signaturen gesetzlich festzustellen, grundsätzlich sicherer und Erfolg versprechender ist, um den E-Commerce zu fördern und unbeabsichtigte Folgen zu verhindern.[1263] Dagegen steht der Nutzen einer Rechtssicherheit und vor allem Vorhersehbarkeit schaffenden Gesetzgebung. Entsprechend ihrer Ausgestaltung kann sie gerade als „*Pfad durch noch unentdeckte Territorien*" dienen, auch in *common law*-Rechtsordnungen.[1264] Einen gangbaren Weg zeigt dabei das Primat der Technologieneutralität im Sinne einer Nichtdiskriminierung einzelner, insbesondere zukünftiger Technologien.

Das *common* oder *case law* erlaubt es den Gerichten, das Recht auch neuen, unvorhergesehenen Entwicklungen und Umständen anzupassen. Es erscheint daher in seiner Anlage flexibler als das starr wirkende kodifizierte *statute law*. Das wirft die Frage auf, ob das vorgenannte Ziel der *predictability* durch das *common law* leichter erreicht werden kann. Problematisch können dabei jedoch die Langsamkeit und Heterogenität eines auf Gerichtsentscheidungen fußenden Systems sein.[1265] Bis zu einer bestimmten rechtlichen Frage überhaupt eine Entscheidung fällt, wird eine gewisse Zeit vergehen. Eine (mögliche) Rechtsunsicherheit besteht bis dahin fort. Ferner besteht die Gefahr voneinander abweichender Gerichtsentscheidungen und unterschiedlicher Beurteilungen von Rechtsordnung zu Rechtsordnung. Dies zeigt sich zum Beispiel in der Akzeptanz der E-Mail-Adresse als elektronische Signatur, die von einigen Gerichten in England und den USA zugelassen, von anderen aber auch ausdrücklich abgelehnt wurde.[1266] Die Lösung, von den Akteuren im E-Commerce zu verlangen, rechtlich unsichere oder durch das bestehende Recht ungeregelte Aspekte im Wege der Vertragsvereinbarung zu umgehen bis ein einschlägiger Präzedenzfall entschieden ist, kann tatsächlich seinerseits dazu führen, den Aufwand und die Kosten zu erhöhen.[1267] Die Gesetzgebung bietet dagegen den Vorteil, dass sie Rechtsicherheit und Vorhersehbarkeit innerhalb kürzerer Zeit bieten kann. Darüber hinaus kann damit Recht geschaffen werden im Sinne einer systematischen Herangehensweise an ein bestehendes Problem. Den Parteien kann so effektiv aufgezeigt werden, wie sie beim Einsatz neuer Technologien Risiken minimieren und Rechtstreitigkeiten verhindern können.[1268] Dies gilt auch in Bezug auf Modelle, die auf

[1262] Gesetze zur Regulierung von Geschäftspraktiken zu entwerfen, die noch gar nicht bestehen, würden diese nicht ermöglichen, sondern vielmehr verhindern; siehe Darstellung bei Smedinghoff/Hill Bro, JMJCIL 1999, S. 38.

[1263] Siehe obe 1.4.2.5 und nachfolgend unter 3.1.5

[1264] Smedinghoff/Hill Bro, JMJCIL 1999, S. 37, 38, die diese Aussage vor allem auf „*default rules*" bezogen haben, was jedoch auch für eine weiter gehende Gesetzgebung gelten kann. Sie legen ferner ausführlich dar, inwiefern Gesetzgebung Kosten reduzieren und ökonomisches Wachstum fördern kann.

[1265] Ausführlich hierzu Smedinghoff/Hill Bro, JMJCIL 1999, S. 32-34 m.w.N.

[1266] Oben unter 2.4.5 und 2.5.5.

[1267] Dies gilt generell für Rechtsfragen im Zusammenhang mit neuen Technologien. Ausführlich hierzu Smedinghoff/Hill Bro, JMJCIL 1999, S. 32-34 m.w.N.

[1268] Smedinghoff/Hill Bro, JMJCIL 1999, S. 32-34.

Selbstregulierung setzen. Die US-amerikanischen Neuregelungen, die UNCITRAL-Modellgesetze, insbesondere aber auch die OECD-Guidelines sprechen den Marktkräften ein großes Potential bei der Entwicklung sicherer und geeigneter Signaturverfahren zu.[1269] Wo es um den Schutz von Individualinteressen und die Durchsetzung von Allgemeininteressen geht, dürfen diese jedoch nicht allein den Marktinteressen zu überlassen bleiben, sondern durch allgemeingültige Regeln gesichert werden.[1270] Diese sollten nach der hier vertretenen *code law*-Tradition – für die hier betroffenen Rechtbereiche – durch legislative Initiativen erstellt werden. Auch eine Vereinheitlichung oder weitestgehende Harmonisierung, auf die wegen dann möglicher Beeinträchtigungen für den grenzüberschreitenden E-Commerce nicht verzichtet werden kann[1271], kann nur im Wege der legislativen Regelung erfolgen. Ob dabei problemadäquate Regelungen in eigene Gesetze gefasst oder in bestehende integriert werden, ist dann eine Frage der Rechtssystematik und der Rechtskultur.[1272]

3.1.4 EU-Richtlinien als Modell

Vielfach wurde der EU-Ansatz als mögliche Grundlage für eine solche – auch internationale – Harmonisierung begrüßt, da unterschiedliche Rechtsordnungen vereint und ein gangbarer harmonisierender Kompromiss gefunden worden seien.[1273] Ziel könne danach, wie oben angedeutet[1274], auch die Ausweitung der EU-Regelungsprinzipien auf andere Rechtsordnungen wie die USA sein. Die elektronischen Signaturen europäischer oder deutscher Qualität könnten die Norm werden, wo eine hochgradige Beweissicherheit verlangt wird und die Kosten dieser Verfahren im Verhältnis zu dem Wert stehen, den das Dokument oder das Rechtsgeschäft repräsentieren.[1275] Anforderungen an die Sicherheitsinfrastruktur unter Beibehaltung der gerade in den USA betonten Parteiautonomie festzulegen ist, wie die RLeS zeigt, kein Widerspruch. Die europäische Lösung stellt insofern tatsächlich einen gangbaren Kompromiss dar. Sie vermag, wenn auch

[1269] Siehe z.B. Tinnefeld, "Das Erbe Montesquieus, Europäisierung und Informationsgesellschaft", MMR 2006, S. 23-27, S. 26.

[1270] Christiansen, MMR 2000, S. 123; Roßnagel, MMR 2002, S. 67, 68.

[1271] Zutreffend Baker, ICCLR 2000, S. 293. Teilweise wird angemerkt, dass eine Harmonisierung auf internationaler Ebene auf dem Weg der Gesetzgebung kaum möglich sei, da langwierig und insbesondere „*mit kulturellen Identitäten behaftet*"; so Rieß, DuD 2002, S. 534. Ein weiterer hervorzuhebender Aspekt ist der Einfluss des US-amerikanischen Rechts, das vielfach in nationale Rechtsordnungen übernommen werde oder schlicht als „ius commune der Neuzeit" wirke; so Lutterbeck, CR 2000, S. 58, der darauf hinweist, dass 70 % aller internationalen Verträge nach New Yorker Kaufrecht gestaltet sind und die kontinentalen Rechtsordnungen der US-amerikanischen Rechtsordnung zum Beispiel die verschuldensunabhängige Produkthaftung und einen ausgeprägten Verbraucherschutz verdanken.

[1272] Zutreffend Roßnagel, MMR 2002, S. 68, 69.

[1273] So zutreffend Baker, ICCLR 2000, S. 296, der einen rechtsordnungsübergreifenden Ansatz verlangt.; auch Hoeren, *Grundzüge des Internetrechts*, S. 195, und Hoernle, JILT 2000; Roßnagel, K&R 2000, S. 323.

[1274] Siehe 3.1.1 und 3.1.2.

[1275] Geis, MMR 2000, S. 673/674: In allen anderen Fällen würden sich Lösungen unterhalb der europäischen „Hochsicherheitstechnologie" durchsetzen. Hier wiederum lägen die Vorteile der US-amerikanischen Lösung.

unter Verzicht auf eine wirkliche Harmonisierung[1276], den deutschen regulativen und technologiespezifischen Ansatz und die Eigenarten des englischen Rechtssystems mit seinen vielen Parallelen zum US-amerikanischen Rechtsverständnis zu umfassen, da sie als zum vermittelnden Ansatz tendierendes Regelungskonzept die Extreme des minimalistischen technologieneutralen und des technologiespezifischen Ansatzes vermeidet.[1277] Gleichzeitig verwirklicht sie einen Großteil dessen, was eingangs als für die rechtliche und gesetzliche Einrahmung der digitalen Signatur-Technologie als notwendig oder zweckmäßig erkannt wurde.[1278] Über die RLeS haben Deutschland als *civil law*-Rechtsordnung sowie England als *common law*-Rechtsordnung diese Elemente übernommen. Ein Brückenschlag zwischen diesen Rechtsordnungen ist somit auf diesem recht hohen Niveau der Signaturregulierung möglich, was durch mehrere bundesstaatliche Regelungsansätze in den USA noch unterstrichen wird. Die EU-Lösungen als Modell zu sehen, hieße vornehmlich auf die rechtliche Ausgestaltung der Sicherheitsinfrastrukturen gemäß RLeS abzustellen. Ausgangspunkt können die darin enthaltenen Definitionen von elektronischer Signatur, Zertifikat etc. sein, wobei unterschiedliche Sicherheitsniveaus vorgesehen werden könnten. Zumindest für die sicherste Form sollten dabei Anknüpfungspunkte für solche Rechtsfolgeregelungen enthalten sein, die den Akteuren eine gesetzlich festgeschriebene Sicherheit gewährleisten. Dies verlangt zumindest für diese Form der Zertifikate und elektronischen Signaturen die Einhaltung bestimmter Kriterien. Eine Vorabprüfung der Zertifizierungsdiensteanbieter, der Verfahren und Komponenten sollte folglich zumindest angeboten werden. Sofern gesetzlich festgestellt werden soll, dass eine bestimmte Form der elektronischen Signatur auch konstitutive oder sonstige sehr strenge Formerfordernisse und deren Funktionen erfüllt, so muss die Sicherheitsinfrastruktur entsprechend zwingend ausgestaltet sein. All dies ist in der RLeS enthalten.[1279] Eine solche Feststellung der Erfüllung der Funktionen der eigenhändigen Unterschrift durch eine bestimmte Form der elektronischen Signatur, etwa der fortgeschrittenen elektronischen Signatur, widerspräche auch nicht den dargestellten Grundsätzen der Beurteilung elektronischer Signaturen nach englischem oder US-amerikanischem Recht.[1280]

3.1.5 Die Generalklausel der allgemeinen Rechtsgültigkeit

Alle vorgestellten Gesetzesinitiativen sprechen elektronischen Dokumenten und Signaturen eine grundsätzliche Rechtswirkung und Beweiseignung zu, beziehungsweise regeln deren Beweiszulassung und nehmen (nur) bestimmte Dokumente und Vertragsty-

[1276] Siehe oben 3.1.1 und 3.1.2.

[1277] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 73, 109.

[1278] Sie oben unter 1.4.2.

[1279] Dabei wurde es jedoch als hinderlich angesehen, dass die technischen Sicherheitsstandards so hoch gesetzt würden. Nicht jeder Anbieter sei in der Lage oder gewillt, ihnen zu entsprechen. Auf internationaler Ebene könne dies als diskriminierende Erschwerung des Zugangs und als Wettbewerbs verzerrend abgelehnt werden. So Hoeren, ECLIP, Teil 1, Kap.1, S. 9.

[1280] Siehe unter 1.3.2 und 1.3.3.

pen davon aus.[1281] Die bloße rechtliche Anerkennung aller Formen von elektronischen Signaturen bietet aber für diese nicht per se die Rechtssicherheit, die zum Beispiel eine herkömmliche eigenhändige Unterschrift bei papiergebundenen Vertragsbeziehungen bieten soll.[1282] Die technische Offenheit, Flexibilität und Wettbewerbsneutralität des US-amerikanischen Ansatzes kann daher zwar als ein Vorteil bewertet werden.[1283] Allerdings werden dabei die Probleme der Authentizität und Integrität elektronischer Kommunikation und die Sicherheitsprobleme im Zusammenhang mit elektronischen Signaturen und Aufzeichnungen nicht gelöst, etwa das Problem der Identifikation des Unterzeichners.[1284] Anforderungen an Signaturverfahren können dabei allenfalls durch Klauseln der „hinreichenden Zuverlässigkeit" etc. umschrieben werden.[1285] Wird auf jegliche Anforderungen an das Signaturverfahren verzichtet, besteht keine Gewähr dafür, dass die elektronische Signatur die erhofften Schlüsse auf die Unverfälschtheit und den Urheber zulässt.[1286] Gerichte müssen dann die Voraussetzungen für die Wirksamkeit einer elektronischen Signatur feststellen.[1287] Die Beweiszulassung und die Beweiskraft elektronischer Aufzeichnungen hängen dabei von der Möglichkeit und Fähigkeit des Beweisführers ab, die Authentizität und Integrität des elektronischen Dokuments darzulegen, also von den – falls vorhanden – jeweils angewendeten Sicherheitsverfahren.[1288] Daraus ließe sich schlussfolgern, dass die bloße gesetzliche Feststellung wie in den US-amerikanischen Bundesgesetzen, nach der einfache elektronische Signaturen grundsätzlich Rechtsgültigkeit erlangen können sollen, angesichts ihres geringen Beweiswerts an den Bedürfnissen der Nutzer vorbei geht. Wie *Borges* wohl zutreffend ausführt, wäre das Konzept, die Erfüllung von Formvorschriften in jedem Falle von einer Würdigung aller Umstände abhängig zu machen, aus Sicht des deutschen Rechts

[1281] Teilweise wird argumentiert, spezifische Gesetzgebung zur Autorisierung des Einsatzes elektronischer Signaturen wäre überflüssig, wenn diese generell rechtswirksam wären; so etwa Smedinghoff/Hill Bro, JMJCIL 1999, S. 14 und 20. Bei Implementierung von Standards und technischen Anforderungen würde der staatenübergreifende Geschäftsverkehr aufgrund eines Mangels an Einheitlichkeit der verschiedenen gesetzlichen Regelungen vor nicht unerhebliche praktische Schwierigkeiten gestellt; ders., S. 20.

[1282] So zutreffend Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 15; siehe auch zum Zweck des Schriftformerfordernisses oben unter 1.2.

[1283] Geis, MMR 2000, S. 673.

[1284] Zutreffend Menna, VJLT 2001; Kochinke/Geiger, K&R 2000, S. 600; Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 19.

[1285] So zutreffend Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 114, der das Beispiel des UNCITRAL-Modellgesetzes zu Elektronischen Signaturen anführt (dazu oben 2.6.1, 2.6.2).

[1286] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 133.

[1287] Kochinke/Geiger, K&R 2000, S. 600.

[1288] Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions", S. 24, 25. Da Parteivereinbarungen, die Regelungen für elektronische Rechtsgeschäfte schaffen oder bestehende gesetzliche Regelungen abändern, grundsätzlich von den Gerichten aufrechterhalten würden, stellten sie die beste Möglichkeit, dar die Wirksamkeit und gewünschte Sicherheit der eingesetzten Verfahren sicherzustellen; ders., S. 30, 31; und Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 411, der die Regeln im US-amerikanischen Beweisrecht für angemessen hält, um die bestehenden Möglichkeiten des Nachweises der Urheberschaft einer elektronischen Aufzeichnung zur Beweisführung zu nutzen. Dazu auch unten 3.2.2 und 3.2.2.4 zu § 371a ZPO.

„schwer erträglich“.[1289] Wie aber die oben aufgeführten Urteile aus England und den USA zu (einfachen) elektronischen Signaturen zeigen[1290], scheinen zum einen die Nutzer elektronischer Kommunikation und die Akteure im E-Commerce ausgerechnet das Bedürfnis zu möglichst einfach gehaltener, unkomplizierter und schneller Kommunikation zu haben. Dieses Bedürfnis wird offenbar vielfach gestillt durch die Benutzung von Kommunikationsformen wie Fax und heute insbesondere E-Mail sowie durch den Vertragsschluss über Websites mittels Anklicken von „I accept“-Buttons. Dies wird durch die dargestellte Rechtsprechung deutscher Gerichte bestätigt.[1291] Vor allem aber scheint das englische und US-amerikanische Recht diesen Nutzern mit der vielfachen Akzeptanz dieser einfachsten Signaturen gerade auch für Beweiszwecke entgegenzukommen. Hier kann die generelle Anerkennung der Rechtswirksamkeit elektronischer Signaturen, soweit sie nicht ohnehin nur die Funktion einer gesetzlichen Klarstellung hat, also gerade angebracht sein. Dies schließt aber die Einführung von spezifischen gesetzlichen Signaturregelungen nicht aus, die lediglich den technisch-organisatorischen Unterbau und Kontrolle in Bezug auf eine Technologie, hier die digitale Signaturtechnik, sicherstellen sollen.

3.1.6 Die Bedeutung technisch-organisatorischer Anforderungen

Entscheidend ist nach wie vor, den Signierenden zweifelsfrei zu authentifizieren. Die in den Formerfordernissen zum Ausdruck kommenden Funktionen der Schriftlichkeit und der Unterschrift können zu diesem Zweck hinsichtlich elektronischer Dokumente und Signaturen durch eine regulative Struktur mit Rechtsfolgeregelungen ergänzt beziehungsweise sichergestellt werden. Hier sind, wie eingangs festgestellt, Anforderungen an die Identifikationsarchitektur, mithin gesetzliche technisch-organisatorische Anforderungen an die Infrastruktur und Verfahren bedeutsam.[1292] So können als sicher erachtete Formen der elektronischen Signatur gesetzlich garantiert und gegebenenfalls mit weiter gehenden Rechtsfolgen versehen werden. Sofern man an den Einsatz dieser Technologie sicherheitsrelevante Anforderungen an die Technik, Produkte, Verfahren und Personen stellt, diese kontrolliert und durch ein Haftungsregime ergänzt, bietet sie, wie oben bereits geschildert und in Deutschland – kritikwürdig – mit § 371a BGB umgesetzt[1293], die Möglichkeit im Wege von Vermutungsregeln die Rechtssicherheit derjenigen, die sie anwenden, noch zu erhöhen. Zudem kann, anders als im Wege der nachfolgenden gerichtlichen Überprüfung, dies insbesondere die Vorhersehbarkeit der rechtlichen Bewertung einer elektronischen Handlung stützen. Im Übrigen kann es für die meisten Transaktionen und Anwendungen im Internet sowie in vielen Rechtsordnungen allgemein den Akteuren überlassen bleiben zu entscheiden, welche Form der elektroni-

[1289] Zumal mit der Folge der Nichtigkeit bei Nichterfüllung, siehe Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 115.

[1290] Oben 2.4.5 und 2.5.5.

[1291] Siehe 1.3.1.4 sowie 3.3.6 und 3.3.7.

[1292] Oben 1.4.2.1 und 1.4.2.2.

[1293] Siehe 2.3.5.2 und 3.2.2.4.

schen Signatur sie einsetzen. Sofern jedoch eine von ihnen gewählte Signatur-Technologie bestimmte, vorher rechtlich festgesetzte Anforderungen erfüllt, kommt beziehungsweise käme ihnen dieser rechtliche Unterbau zugute. Einen solchen Unterbau bietet der Lösungsansatz der Signaturrichtlinie. Soll danach eine bestimmte Technologie wie die der digitalen Signatur gesetzlich reguliert werden, sind solche weiter gehenden technisch-organisatorischen Anforderungen notwendig, wie das Beispiel Deutschland zeigt. In den USA wäre auch auf Bundesebene eine umfassendere Regulierung – und damit auch eine Harmonisierung bereits bestehender einzelstaatlicher Signaturgesetze – als Reaktion auf die derzeit aktuelle Technologie der digitalen Signatur möglich. Wie das Beispiel England zeigt, hätte dies etwa auf Grundlage des Regelungsinhalts der RLeS geschehen können, eventuell unter deutlicher Hervorhebung des „opt-in"-Ansatzes und der Flankierung der in UETA, ES-Act und UCITA gefundenen Regelungen zur Parteiautonomie. Es wird deutlich, dass die Unterschiede der Regelungskonzepte zunächst auf der Ebene der Regulierung der Signaturtechnik und -verfahren liegen, weniger bei der rechtlichen und gesetzlichen Gleichstellung von handschriftlicher und elektronischer Unterschrift. Diese ließe sich auf der Grundlage eines technologiespezifischen Ansatzes ebenso durchführen wie auf Grundlage eines technologieneutralen.[1294]

3.1.7 Die Bedeutung der Technikneutralität

Alle verglichenen Gesetzeswerke sind technikneutral oder beabsichtigen dies zumindest. Dabei sind einige Signaturregelungen sehr ausführlich gehalten und favorisieren de facto eine bestimmte Technologie, wie etwa einige einzelstaatliche Signaturgesetze in den USA, das deutsche Signaturgesetz oder auch die RLeS. Das relativ hohe Niveau der Authentifizierung durch Zertifizierungsdiensteanbieter wird seit je her bemängelt wegen seiner operativen Zwänge und Kosten, die durchaus zu einer Behinderung des E-Commerce gerade auch zwischen verschiedenen Rechtsordnungen führen können.[1295] Tatsächlich technikneutral sind die Regelungen des US-Bundesgesetzgerbers. Die oben dargestellten Regelungen von UETA und E-SIGN, oder auch des MLeC und des MLeS, werfen die Frage auf, ob dieser Ansatz tatsächlich Rechtssicherheit und Vertrauen fördert und ob der dort propagierte Vorteil gegenüber einer stark regulierenden, technologiespezifischen Gesetzgebung tatsächlich besteht beziehungsweise wie weit dieser reicht – ob also Technikneutralität in ihren Ausformungen in den hier vorgestellten Neuregelungen wirklich von solch bedeutendem Wert ist.[1296] Die eingangs als Ziel ausgegebene Nichtdiskriminierung einzelner Technologien[1297] ist durch die teilweise

[1294] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 74.

[1295] Siehe Darstellung bei Smedinghoff/Hill Bro, JMJCIL 1999, S. 28.

[1296] Wie Smedinghoff/Hill Bro zutreffend bemerkt haben, habe die Technikneutralität in vielen Kreisen *„den Stellenwert eines Mantras bekommen, an dem Gesetzgebung zur elektronischen Signatur bemessen wird."* JMJCIL 1999, S. 35.

[1297] Siehe oben 1.4.2.6.

starke Präferenz einer bestimmten, hier zumeist der digitalen Signatur-Technologie, offensichtlich nicht erreicht worden.

Zunächst kann das Argument der Kosten und des Aufwands eines bestimmten Signaturverfahrens angeführt werden. Risiko, Umfang oder Bedeutung der jeweiligen Erklärung oder des Rechtsgeschäfts können dabei als Grund gerade für eine solch aufwändige und gesetzlich ausgestaltete und staatlich überprüfte Sicherheitsinfrastruktur für die digitale Signatur gelten. Diese kann eine der Bedeutung des Rechtsgeschäfts angemessene und vorhersehbare Rechtssicherheit praktisch und rechtlich, also gesetzlich fixieren. Andererseits wird mit diesem Argument auch das marktorientierte, freie Modell der grundsätzlichen rechtlichen Anerkennung aller Formen elektronischer Signaturen begründet. Beide dargestellten Ansätze, der tatsächlich technologieneutrale und der de facto auf die digitale Signatur fixierte, unterscheiden sich in einer Hinsicht nicht: Je größer die tatsächliche Sicherheit der eingesetzten Signaturverfahren sein soll und je mehr Wert von den Akteuren darauf gelegt wird, dass die eingesetzte elektronische Signatur tatsächlich rechtswirksam und beweiskräftig ist, desto mehr Aufwand sollte grundsätzlich bei ihrer Herstellung und Sicherheit betrieben werden (müssen). Dabei wird davon ausgegangen, dass – gleich in welcher Rechtsordnung und gleich unter welche Signaturgesetzgebung eine bestimmte Transaktion fällt – Rechtsgeschäfte ab einer bestimmten Bedeutung oder Wertgrenze den Einsatz der derzeit effektivsten und sichersten Technologie fordern werden. Dann macht es zunächst keinen Unterschied, ob diese sicherste Technologie durch Gesetz als einzig rechtsgültige und rechtwirksame elektronische Signatur vorgeschrieben wird, oder ob beispielsweise über die Regelungen zur *attribution* ein Gericht notwendig nur dieser selben Technologie zum Zeitpunkt der Entscheidung Integrität und Authentizität zuerkennen wird. Unabhängig davon, ob für ein bestimmtes Rechtsgeschäft unter einer bestimmten Rechtsordnung eine hohe Sicherheit und damit ein Verfahren mit bestimmten Eigenschaften gefordert werden soll oder der Einsatz eines solchen Verfahrens dem Belieben der Parteien überlassen bleibt, ist es für die Rechtssicherheit dieser Akteure und zur Sicherstellung einer erhöhten Vertrauenswürdigkeit dieses Verfahrens von Vorteil, eine Sicherheitsinfrastruktur vorzuhalten und zu kontrollieren.[1298] In Deutschland ergab sich dieser Bedarf schon aus den Funktionen der Formerfordernisse und, insbesondere in Bezug auf die Schriftform des § 126 BGB, deren Anforderungen an Schriftlichkeit und Unterschrift. Wie oben beschrieben wird eine solche Signaturregelung derzeit notwendig auf die Technik der digitalen Signatur und der PKI aufbauen. In England und den USA meinte man aufgrund der bestehenden Rechtslage und Anerkennung verschiedenster Formen des *writing* und der *signature*, ohne spezifische Signaturregulierung die notwendige Akzeptanz und auch Rechtssicherheit gewährleisten zu können. Dass eine spezifische Signaturregelung im obigen Sinn jedoch auch dort sinnvoll ist, zeigen viele bundesstaatliche Signaturgesetze in den USA und der Wert, der ihnen als Sicherheitsverfahren etc. zukommen kann – auch wenn es an spezifischer Rechtsprechung hierzu noch mangelt.

Die technologieoffenen Regelungsansätze bietet andererseits erst die Möglichkeit, dass auch für einfache elektronische Signaturformen angenommen wird, sie könnten be-

[1298] Siehe oben 1.4.2.1 und 1.4.2.2.

stimmte, zum Teil wesentliche Funktionen der Formerfordernisse der Schriftlichkeit und vor allem der Signatur erfüllen. Nach dem deutschen Ansatz des SigG und der Substituierung der Schriftform durch die elektronische Form, also eine mit digitaler Signatur versehene elektronische Erklärung oder Vereinbarung, wird dies für einfache elektronische Signaturen ausgeschlossen. Diese Möglichkeit scheint also allein nach dem *common law* auf Grundlage der oben genannten Referenzfälle zu bestehen. Andererseits hat der deutsche Gesetzgeber mit der Textform des § 126b BGB eine Möglichkeit rechtserheblicher elektronischer Erklärungen geschaffen, die – bei aller Beschränktheit der Textform in Anforderungen und Anwendungsbereich – einer gewissen Formenstrenge genügen können sollen. Einer besonderen Sicherheitsinfrastruktur bedarf es dabei nicht, um zumindest eine Dokumentationsfunktion zu erfüllen. Vielmehr bedient sich die Textform der bereits bestehenden Gegebenheiten und technischen Möglichkeiten, wie sie von den Akteuren im E-Commerce heutzutage genutzt werden. Um elektronischen Kommunikationen, die der Textform entsprechen oder gleichen, auch formwirksame Rechtskraft zukommen zu lassen, wäre daher ein solcher wirklich technikneutraler Ansatz förderlich. Denn dann wäre – wie im englischen und US-amerikanischen Recht vielfach betont wird[1299] – vor allem das jeweilige Formerfordernis und die durch dieses zu erfüllenden Funktionen maßgeblich.

[1299] Siehe oben 1.3.2.1, 2.4.4 und 2.4.5 sowie 1.3.3.1, 2.5.5 und 2.5.6.

3.2 Schwächen der digitalen Signatur

Wie an den oben dargestellten gesetzlichen Regelungen zu elektronischen Verträgen und Signaturen zu sehen ist, spielt die Technologie der digitalen Signatur eine herausragende Rolle in vielen Gesetzeswerken, etwa in der RLeS und dem SigG, auch den EC Reg., mit der fortgeschrittenen elektronischen Signatur. Die digitale Signatur – diese schließt in der nachfolgenden Betrachtung die fortgeschrittene elektronische Signatur nach RLeS, SigG und ES Reg. ein – soll dabei als Basistechnologie für die Rechtssicherheit im elektronischen Geschäftsverkehr dienen.[1300] Wie *Ulmer* für Deutschland hinsichtlich der Funktionsgleichheit mit der Schriftform zusammenfasst, erreiche die digitale Signatur die Abschlussfunktion durch die Bildung des Hash-Wertes, die Perpetuierungsfunktion durch die Herstellung eines zu archivierenden Datenträgers, sowie die Echtheitsfunktion durch die Verknüpfung von Dokumenteninhalt und Signatur. Die Verifikationsfunktion einer Unterschrift, die sichere Zuordnung zu einer einzelnen Person, werde durch die Vorschriften des SigG und die Beweisfunktion durch § 371a ZPO gewährleistet. Auch die Warnfunktion der Schriftform werde erreicht.[1301] Tatsächlich aber stehen (auch) ihr erhebliche Bedenken hinsichtlich ihrer Sicherheit und der Möglichkeit, die Funktionen herkömmlicher Formvorschriften zu übernehmen, entgegen. Dies wird durch die oben dargestellten Ausprägungen in der relevanten Gesetzgebung teilweise noch verstärkt. Nicht zuletzt hat sie sich bis heute am Markt nicht durchgesetzt.

3.2.1 Sicherheitsdefizite der digitalen Signatur

Gemäß der auf einer bestimmten Technologie basierenden, die digitale Signatur regulierende Gesetzgebung soll die Signatur vor allem zwei Funktionen erfüllen: die Person, welche die Signatur nutzt, authentifizieren und beweisen, dass sie die signierte Nachricht und deren Inhalt als eigene angenommen hat.[1302] Dies sind die Funktionen, die in allen hier dargestellten Rechtsordnungen zuförderst herkömmliche, eigenhändige Unterschriften auf verkörperten, papiernen Urkunden zu erfüllen in der Lage sein sollten und auf die wiederum besondere Beweisregeln zugeschnitten waren.[1303] Das deutsche Recht traut diese Funktionsgleichheit derzeit nur der digitalen Singatur-Technik, also der fortgeschrittenen elektronischen Signatur des SigG, zu. Für das *common law* wurde dagegen festgestellt, dass diese Ziele grundsätzlich auch durch jede andere Form der elektronischen Signatur erreicht werden können.[1304] Andererseits wird sogar angemerkt,

---

[1300] So wiederholt Roßnagel, „Die Sicherheitsvermutung des Signaturgesetzes“, NJW 1998, S. 3312-3320, S. 3313; ders., „Digitale Signatur im europäischen Rechtsverkehr“, K&R 2000, S. 313-323, S. 313/314; ders., NJW 2001, S. 1817-1826 S. 1817; zustimmend Hähnchen, NJW 2001, S. 2832;

[1301] Bevor eine Unterschrift gesetzt werde, halte der Erklärende regelmäßig inne aufgrund der Belehrungen vor Vertragsschluss und durch die Bedienung der Computeranlage, die besondere Handgriffe erfordere, die als Warnfunktion genügten; Ulmer, CR 2002, S. S. 211-212.

[1302] Mason, *Electronic Signatures in Law*, S. 5.

[1303] Siehe 1.2, 1.3.1.3, 1.3.2.5, 1.3.3.5.

[1304] Siehe oben 1.3.2.6 und 2.4.5 sowie 1.3.3.6 und 2.5.5.

dass eine eigenhändige Unterschrift diese Funktionen unter Umständen nicht erfüllen könne. Eine Technik, die alle Funktionen insbesondere der handschriftlichen Unterschrift im digitalen Umfeld nachbilden könne, existiere gar nicht. Jedenfalls sei die digitale Signatur dazu nicht in der Lage.[1305] *Schapper*, *Rivolta* und *Veiga Malta* drücken es so aus: Während im traditionellen Handel die forensische Qualität einer eigenhändigen Unterschrift substantielle Sicherheit bei der Authentifikation sicherstelle, existiere im digitalen Umfeld, wo das Signaturerstellungsverfahren selbst sicher sein müsse, keine wirkliche Entsprechung.[1306] Zuzustimmen ist jedenfalls der Aussage, dass es insgesamt schwierig ist, ein System zu konstruieren, dass nicht Gefahr läuft, seine Sicherheit zu kompromittieren.[1307]

3.2.1.1 Verbindung zwischen Verwender und Signaturschlüsselinhaber

Die Aussage einer digitalen Signatur ist, dass der private Schlüssel, mit dem die jeweilige Signatur erstellt wurde, mit dem zu dessen Verifizierung verwendeten öffentlichen Schlüssel verbunden ist, und dass die signierte Nachricht nach der Signierung nicht verändert wurde.[1308] Dabei wird den bedeutsamen technischen und rechtlichen Hindernissen, die dieser Behauptung entgegenstehen, wenig Beachtung geschenkt. Der Verifizierungsprozess ist undurchsichtig. Es besteht zum Beispiel die Möglichkeit, dass die digitale Signatur von einem elektronischen Dokument entfernt wird, ohne Spuren zu hinterlassen.[1309] Die digitale Signatur kann zwar den Absender identifizieren, aber nicht garantieren, dass es tatsächlich der Absender war, der das Dokument mit der digitalen Signatur versehen hat.[1310] Sie ist (ein mathematischer) Beweis dafür, dass der geheime Schlüssel, zum Zeitpunkt der Berechnung der Signatur in dem für die Signatur verwendeten Computer vorhanden war. Folglich besteht eine Verbindung zwischen dem geheimen Schlüssel und der Signierung des Dokuments. Dabei muss bedacht werden, dass der Schlüssel lediglich ein mathematischer Wert ist, der dem System zur Signierung zur Verfügung gestanden hat, jedoch nicht das Individuum identifiziert. Daher folgt aus dessen Verwendung nicht, dass der Signaturschlüsselinhaber den Computer veranlasst hat, diese mathematische Kalkulation vorzunehmen. Es besteht nicht notwendig eine Verbindung zwischen der Signierung des Dokuments durch den Computer und der Handlung des Signaturschlüsselinhabers. Die digitale Signatur bestätigt also nicht, dass es tatsächlich der Schlüsselinhaber war, der den privaten Schlüssel zur Signierung des

[1305] Mason, *Electronic Signatures in Law*, S. 5, 331.

[1306] Schapper/Rivolta/Veiga Malta, „Risk and Law in Authentication“, DEJ 2006, Vol. 3, S. 10-16, S. 11.

[1307] Mason, *Electronic Signatures in Law*, S. 331 m.w.N.

[1308] Mason, *Electronic Signatures in Law*, S. 5.

[1309] Mason, *Electronic Signatures in Law*, S. 277, 232.

[1310] Siehe auch Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 515, 516, der anzweifelt, ob sich nach den allgemeinen, von der Rechtsprechung und der Literatur entwickelten Grundsätzen über den Anscheinsbeweis aus der Verwendung eines geheimen Signaturschlüssels ein Anscheinsbeweis für die Urheberschaft des Schlüsselinhabers ergibt. Mason, *Electronic Signatures in Law*, S. 5; ders., J. High Tech L. 2006/2, S. 164.

Dokuments oder der Nachricht eingesetzt hat.[1311] Schon daraus wird geschlossen, dass die digitale Signatur vor derselben Schwierigkeit stehe wie eine einfache elektronische Signatur, etwa durch das Anklicken eines „Ich akzeptiere"-Button: eine Verbindung herzustellen zwischen der Handlung des Signierens und der Person, die diese Handlung ausgeführt hat.[1312] Es bestehen aber noch weitere Probleme beim Einsatz der digitalen Signatur, die Zweifel aufkommen lassen hinsichtlich der ihr insbesondere in den EU-Richtlinien und der deutschen Gesetzgebung zugesprochenen hervorgehobenen Position. Nicht zuletzt wird das entsprechende Zertifikat auf der Grundlage der vom Zertifikatinhaber angegebenen Informationen erstellt.[1313] Ohne weitere Überprüfung dieser Angaben lässt dies keine Rückschlüsse auf die tatsächliche Identität des Zertifikat- oder Schlüsselinhabers zu.[1314]

3.2.1.2 Das Passwortproblem

Bei heute gängigen digitalen Signaturen wird die Annahme, der Versender einer digital signierten Nachricht sei tatsächlich die behauptete Person, vor allem auf ein Sicherheitsmerkmal gestützt: den Passwort-Schutz.[1315] Es stellt zum Beispiel im deutschen Modell der fortgeschrittenen elektronischen Signatur eines der beiden Elemente des „Besitz und Wissen" dar, das der Sicherheit des Systems dienen soll.[1316] Das Passwort oder die PIN soll es dem Versender ermöglichen, Zugang zu dem Computer oder der Signaturerstellungseinheit zu erlangen beziehungsweise diese zu entsichern und zu veranlassen, das Dokument mit der digitalen Signatur zu versehen. Das Vertrauen in den Passwort-Schutz fußt dabei allein auf der Integrität des Passworts und dem vorhandenen Schutz des Passworts und des privaten Schlüssels.[1317] Die grundsätzlichen Schwächen eines Passwort-Schutzes sind bekannt: Es besteht die Gefahr, dass die Nutzer ihre Passwörter Dritten mitteilen oder sie sonst willentlich oder unwillentlich preisgeben. Nutzer tendieren vor allem dazu, Passwörter mit vorhersehbaren Charakteristiken zu wählen, um sich diese merken zu können. Diese fallen in den Bereich der sogenannten „*higher probability*"-Passwörter, eines sehr kleinen Bereichs möglicher Passwörter. Die Passwörter sind so anfälliger für einen Angriff, der mittels Anwendung wahrscheinlicher Passwörter das jeweilige zu erraten versucht.[1318] Problematisch ist auch eine mög-

[1311] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 515, 516; Mason, *Electronic Signatures in Law*, S. 5, 187.

[1312] Mason, *Electronic Signatures in Law*, S. 299; ders., J. High Tech L. 2006/2, S. 164.

[1313] Neuser, „Faule Kunden bei ‚Tante-Emma.com' – Eine europäische Vertrauenshaftung für elektronische Signaturen", MMR 1999, S. 67-74, S. 69, der auch vom Zertifikat als dem Ausreisevisum in die elektronische Welt spricht.

[1314] Dazu eingangs unter 1.4.2.1, 1.4.2.3.

[1315] Siehe dazu auch eingangs unter 1.4.2.1 und 1.4.2.2 sowie unten 3.2.1.2 und 3.3.7.2.

[1316] Noack/Kremer in Dauner-Lieb et al., *Anwaltkommentar BGB*, § 126a, Rn. 22.

[1317] Armgardt, Matthias / Adrian Spalka, "Der Anscheinsbeweis gemäß § 371a Abs. 1 S. 2 ZPO vor dem Hintergrund der bestehenden Sicherheitslücken bei digitalen Signaturen", K&R 2007, S. 26-32, S. 27, Mason, *Electronic Signatures in Law*, S. 331.

[1318] Mason, *Electronic Signatures in Law*, S. 331 m.w.N.; Roßnagel, Alexander / Andreas Pfitzmann, „Der Beweiswert der E-Mail", NJW 2003, S. 1209-1214, S. 1211.

liche Speicherung des Passwortes auf der entsprechenden Signaturerstellungseinheit. Nur wenn dies unterbleibt oder unmöglich gemacht, beziehungsweise das System so eingerichtet wird, dass sich die Signaturkarte nach wenigen fehlerhaften Eingaben der PIN selbst dauerhaft sperrt, kann die Wahrscheinlichkeit von Angriffen durch Erraten der PIN minimiert werden.[1319]

3.2.1.3 Das Signaturkarten-Problem

Die Signaturkarte ist das zweite Element des „Wissen und Haben". Sie dient als Signaturerstellungskomponente, auf der sich der geheime private Schlüssel befindet. Auf der Signaturkarte befinden sich ein Speicher für den geheimen Schlüssel und ein kleiner Rechner, der mit diesem Schlüssel für eine Datenmenge lokal die digitale Signatur berechnet. Der so generierte öffentliche Schlüssel des Schlüsselpaars der digitalen Signatur wird letztlich ausgegeben beziehungsweise veröffentlicht.[1320] Es soll ausgeschlossen werden, dass der Signaturinhaber selbst der Signaturkarte den geheimen Signaturschlüssel entnimmt und aufgrund des so kompromittierten, weil nicht mehr geheimen Schlüssels die Verantwortung für damit signierte Dokumente von sich weist. Folglich wird bei der Entwicklung von Signaturkarten größter Wert darauf gelegt, dass der dort gespeicherte geheime Schlüssel weder durch mechanische, thermische, elektrische, elektromagnetische oder software-basierte Angriffe rekonstruiert werden kann.[1321] Dennoch hat auch dieses Element Schwachstellen: Die größte ist wohl, dass sie keinen direkten Kommunikationsweg zum Nutzer bietet, sondern vollständig abhängig ist von dritten Geräten, um die Transaktionen abzuwickeln. Die hierfür eingesetzten Komponenten sind das Kartenlesegerät, der Computer und vor allem die darauf laufende Software, die den Nutzer bei der Erzeugung der Signatur führt und die das Ergebnis der Verifikation einer digitalen Signatur für das signierte Dokument zeigt. Diese dritten Geräte, zum Beispiel der Computer, an den die Signaturkarte angeschlossen wird, sind aber potentiell nicht vertrauenswürdig.[1322] Wenn diese Geräte kompromittiert sind, hat dies Auswirkungen auf die Signaturkarte und kann die Verlässlichkeit der mit ihr generierten digitalen Signatur zunichte machen.[1323]

[1319] Armgardt/ Spalka, K&R 2007, S. 27.

[1320] Armgardt/ Spalka, K&R 2007, S. 27; Mason, *Electronic Signatures in Law*, S. 332.

[1321] So Armgardt/ Spalka, K&R 2007, S. 27, die über den Erfolg dieser technischem Bemühungen in der Entwicklung von Signaturkarten jedoch nichts sagen, allerdings daraus schließen, dass weder Signaturverfahren noch die Signaturkarte angreifbar seien in dem Sinne, dass eine gültige digitale Signatur nur mit der Beteiligung einer entsicherten Signaturkarte erzeugt werden kann.

[1322] Siehe nachfolgend unter 3.2.1.3 und 3.2.1.5.

[1323] Armgardt/ Spalka, K&R 2007, S. 30; Mason, *Electronic Signatures in Law*, S. 332; Bohm, „Watch what you sign!", DEJ 2006, S. 43-47, S. 45.

3.2.1.4 Das Darstellungsproblem

Bei den heute gängigen Signaturverfahren muss der zu signierende Text zuvor gekennzeichnet werden. Das Problem der mehrdeutigen Präsentationen von Daten betrifft daher auch die digitale Signatur-Technologie. Eine objektivierte Darstellung von Daten wie auf Papier existiert nicht. Vielmehr hängt diese immer von der jeweils eingesetzten Hardware, Software und deren Konfiguration ab. Die Daten auf dem Bildschirm des Signaturausstellers können anders dargestellt werden als auf dem Bildschirm des Empfängers oder Prüfers.[1324] Grund ist, dass viele Dateitypen es erlauben, in einer Datei aktive Inhalte, das heißt Parameter oder Kommandos zu speichern, die das ausführende Programm in der Darstellung des Inhaltes beeinflussen. Es ist technisch leicht zu bewerkstelligen, Dateien zu erstellen, die in Abhängigkeit von der aktuellen Ausführungsumgebung ihre Darstellung ändern und also keine eindeutige intendierte Semantik haben.[1325] Dies ermöglicht vielfältige Fehler und Täuschungen. Für einen Nutzer ist zumeist nicht erkennbar, ob eine Datei solche aktiven Inhalte hat und ihre Semantik daher gegebenenfalls mehrdeutig ist. Insbesondere in fremder Systemumgebung kann der Signierende in der Regel weder die Darstellung des zu signierenden Textes noch die Korrektheit der verwendeten Programme kontrollieren. Ein Dritter kann eine Datei mit mehrdeutiger Semantik erstellen und seine Ausführungsumgebung auf dem Computer so einrichten, dass die Datei die für ihn günstige Semantik zeigt. Liegt eine Datei dieses Typs vor, wird man meist nicht bestimmen können, welche Semantik für den Signierenden wahrnehmbar war.[1326] Die Verifikation einer solchen Signatur wird dabei lediglich beweisen, dass eine unverfälschte Datei mit mehreren Semantiken vorliegt.[1327] Wie *Armgardt* und *Spalka* richtig anmerken, ist der Satz *„What you see is what you sign“* nicht allgemeingültig.

3.2.1.5 Das Manipulationsproblem

Ein damit zusammenhängendes beziehungsweise für die vorgenannten Aspekte ursächliches Problem ist dass des unbefugten Zugangs zum jeweiligen Computer beziehungsweise der Signaturerstellungseinheit. Diese Probleme können auftreten, wenn eine fremde Person sich durch schädliche Software wie Trojanische Pferde Zugang zum Computer verschafft und diesen zum Beispiel veranlasst ein Dokument auf dem Bildschirm anzuzeigen, während tatsächlich ein anderes signiert wird. Dabei kann es sein, dass der Besitzer des Computers beziehungsweise der Signaturschlüsselinhaber sich dieser Tatsache nicht bewusst ist. Der Signierende kann auch nicht sicher sein, dass nicht ein weiterer Signaturvorgang im Hintergrund abläuft, von dem er keine Kenntnis

[1324] Gesellschaft für Informatik (GI), „DuD Forum – Stellungnahme zum Gesetzentwurf ‚Formvorschriften des Privatrechts'“, DuD 2001, S. 38-40, S. 39; Armgardt/ Spalka, K&R 2007, S. 28.

[1325] Ausführliche Darstellung m.w.N. bei Armgardt/ Spalka, K&R 2007, S. 28.

[1326] GI, DuD 2001, S. 39.

[1327] Armgardt/ Spalka, K&R 2007, S. 28.

erlangt.[1328] Es ist für einen Dritten möglich, ein entsprechendes Programm zu entwerfen, das den Computer infiltriert und es dieser Person ermöglicht, den Computer aus der Ferne und ohne Berechtigung zu steuern und den privaten Schlüssel ohne Zustimmung des Signaturschlüsselinhabers zur Signierung von Dokumenten zu nutzen.[1329] Dabei kann das Schadprogramm nach dem Entsperren der Signaturkarte Hash-Werte beliebiger Dokumente mit Kommandos zum Signieren senden, oder den Inhalt des Secure Viewers[1330] verändern beziehungsweise dessen Inhalt noch vor dem Signieren austauschen, oder aber ganz die Regie in der Signaturanwendung übernehmen. Schließlich kann so auch die Verifikationskomponente der Signaturanwendung manipuliert werden mit der Folge, dass dem Benutzer auch im Fall ungültiger Signaturen eine Bestätigung der Echtheit angezeigt wird.[1331] In diesen Fällen kann der Computer nicht mehr als sichere Signaturerstellungseinheit angesehen werden. Die Fähigkeit, solche Dritteingriffe und Schadprogramme mittels einer Firewall oder einen Virenscanner zu verhindern, ist – insbesondere beim E-Mail-Verkehr – sehr begrenzt.[1332] Dem Grundsatz nach ist es zwar möglich, eine elektronische Signatur zu schaffen, die vertrauenswürdig ist und eine Verbindung herstellt zwischen Individuum und Dokument. Dazu müsste aber etwa ein Computer eingesetzt werden, der zu keinem Zeitpunkt Verbindung nach außen, insbesondere dem Internet, hatte und auch keine Komponenten beinhaltet, die jemals in einem mit der Außenwelt verbundenen Computer eingebaut waren, und indem über diesen Computer vollständige und alleinige Kontrolle durch den Signierenden, den Signaturschlüsselinhaber, ausgeübt wird. Erst dann ist es möglich, eine Verbindung zwischen der Person und der elektronischen Signatur herzustellen.[1333] Auf das Manipulationsproblem wird nachfolgend noch an mehreren Stellen eingegangen.

3.2.2 Vermutung hinsichtlich der Identität des Nutzers

3.2.2.1 Grundlagen gesetzlicher Vermutungsregeln

Die rechtlichen und praktischen Vorteile einer Vermutung der Sicherheit eines bestimmten Signaturverfahrens oder der Authentizität und Integrität eines damit signierten elektronischen Dokuments erscheinen grundsätzlich begrüßenswert. Solche rechtlichen

[1328] Mason, *Electronic Signatures in Law*, S. 188, 331 m.w.N.

[1329] Mason, *Electronic Signatures in Law*, S. 188; mit ausführlichen technischen Erläuterungen: Armgardt/ Spalka, K&R 2007, S. 29; Bohm, DEJ 2006, S. 45, 46.

[1330] Secure Viewer ist eine Bezeichnung für die für die Signaturerstellung verwendete Software oder Hardware, die es dem Signierenden ermöglicht, das zu signierende Dokument anzusehen und dann den Signaturvorgang auszulösen.

[1331] Armgardt/ Spalka, K&R 2007, S. 29.

[1332] Eine Firewall kann die Semantik der Datenlast in einem aus dem Netzwerk geladenen Datenpaket (etwa per E-Mail) nicht erkennen und folglich auch nicht entscheiden, ob es sich um den Teil eines Schadprogramms handelt. Die Weiterverbreitung über die Nutzung der Adressbücher der befallenen Computer wird daher mit Vorliebe genutzt. Der Virenscanner kann immer nur bereits bekannte Schadprogramme herausfiltern. Siehe bei Armgardt/ Spalka, K&R 2007, S. 29.

[1333] So Mason, *Electronic Signatures in Law*, S. 188, und Armgardt/ Spalka, K&R 2007, S. 32, bezogen auf den Gegenbeweis gem. § 371a Abs. 1 ZPO, siehe nachfolgend 3.2.2.4.

(beziehungsweise gesetzlichen) Vermutungen vereinfachen die Beweisführung, schaffen Rechtssicherheit und können – und sollen – den Einsatz einer bestimmten Technik fördern. Grundlage einer solchen Vermutung ist bei der digitalen Signatur die Annahme, sie böte der auf sie vertrauenden Partei ein größeres Maß an Sicherheit. Dies findet seinen Ausdruck in der Vermutung, eine digitale Signatur beweise, dass die Person, deren digitale Signatur verwendet wurde, diejenige ist, die den Signiervorgang tatsächlich verantwortet. Die technischen Probleme, die einer solchen Annahme entgegenstehen können, sind oben dargestellt worden.[1334] In der Folge kann sich der Signaturaussteller in der Situation wieder finden, dass er sich vor eine bedeutende Verantwortlichkeit für unautorisierte Rechtsgeschäfte gestellt sieht, nur weil er unwissentlich die Sicherheit einer Signaturerstellungseinheit nicht ausreichend geschützt hat. Gesetzliche Signaturregelungen, nach denen eine elektronische beziehungsweise digitale Signatur in der Lage sein soll, die Identität der Person zu authentifizieren, deren privater Schlüssel eingesetzt wurde, schaffen zudem eine Vermutung bezüglich des Nutzers einer elektronischen Signatur, die für die handschriftliche Signatur nicht existiert, siehe das Beispiel des § 371a Abs. 1 ZPO in Deutschland.[1335]
Die Frage, ob für elektronische Signaturen und Dokumente überhaupt gesetzliche Beweisregeln in Form der Beweisvermutung, der Beweislastumkehr oder des Anscheinsbeweises aufgestellt werden sollen, wird in den verschiedenen Ländern unterschiedlich beantwortet.[1336] In England wird allein geregelt, dass elektronische Dokumente nicht überhaupt vom Beweis ausgeschlossen sind und die Frage der Beweiskraft beziehungsweise der ordnungsgemäßen Verwendung der elektronischen Signatur überlässt man ausdrücklich dem Gericht.[1337] In den hier verglichenen legislativen Initiativen finden sich gesetzliche Vermutungsregeln oder Anscheinsbeweise nur in Art. 13 MLeC und Art. 8 MLeS sowie im bereits dargestellten § 371a Abs. 1 ZPO. Es zeigt sich, dass auch diese die herausgehobenen Stellung, die der digitalen Signatur vielfach – insbesondere in den EU-Richtlinien und deren deutschen Umsetzung – zugemessen wird, nicht stützen können.

3.2.2.2 *Non-repudiation*

In England ist die digitale Signatur, insbesondere deren Sicherheits-Infrastruktur, nicht gesetzlich ausgestaltet wie zum Beispiel in Deutschland. Gesetzliche Beweiskraftregelungen für elektronische Dokumente sind nicht vorhanden. Nur die grundsätzliche Zulassung als Beweis in Gerichtsverfahren ist neu geregelt worden. Ähnlich verhält es sich mit dem Bundesrecht zu elektronischen Dokumenten und Signaturen in den USA. Der Einsatz der digitalen Signatur ist in diesen Rechtsordnungen dennoch von den Gesetzen

[1334] 3.2.1.

[1335] Mason, *Electronic Signatures in Law*; siehe oben 2.3.5.1 und nachfolgend 3.2.2.4.

[1336] Siehe bei Stadler, „Der Zivilprozess und neue Formen der Informationstechnik, ZZP 2002, S. 413-444, S. 434.

[1337] Siehe oben 2.4.2.3.

und Rechtsvorschriften zum elektronischen Rechtsverkehr umfasst.[1338] Welche Voraussetzungen dort an die Wirksamkeit, Verlässlichkeit und Beweiskraft digitaler Signaturen gestellt werden, hängt vor allem von der Beurteilung der Gerichte ab. Dass digitalen Signaturen eine erhöhte Sicherheit und Zuverlässigkeit als der einfachen elektronischen Signatur zugesprochen werden kann, findet aber zum Beispiel einen Niederschlag darin, dass diese als Sicherheitsverfahren etwa bei der *attribution* gelten.[1339]
Ob die der digitalen Signatur zugesprochene besondere Sicherheit zu einer Vermutung hinsichtlich der Identität des Verwenders oder zu einer geänderten Beweislast führen kann oder sollte, wird dabei auch unter dem Stichwort *non-repudiation* diskutiert. *Repudiation* bedeutet dabei soviel wie die Urheberschaft oder Wirksamkeit von etwas zu bestreiten. Wenn beispielsweise ein System technisch nachweisen kann, dass eine Erklärung oder ein Dokument abgesendet oder empfangen wurde, soll es dem Empfänger beziehungsweise dem Versender obliegen nachzuweisen, dass es ihm nicht zugegangen ist beziehungsweise nicht von ihm versendet wurde.[1340] Grundlage ist im technischen Sinne ein hoher und bezifferbarer Grad an Wahrscheinlichkeit, dass etwa das technische Protokoll nachweisen kann, dass ein Dokument oder eine Nachricht von einem bestimmten Computer gesendet oder empfangen wurde. Ziel ist es, die Nutzer dergestalt an bestimmte Handlungen zu binden, dass, wenn sie diese Handlungen bestreiten, entweder ihre Böswilligkeit belegt ist oder aber beispielsweise feststeht, dass sie die Sicherung ihres privaten Schlüssels fahrlässig vernachlässigt haben.[1341] Als (technische) Antwort hierauf kann der betreffenden Person entweder das Recht zur Nichtanerkennung (*repudiation*) der digitalen Signatur genommen, oder aber die Beweislast vom Empfänger auf den angeblichen Urheber verschoben werden.[1342] Wie oben beschrieben mag die Technik der digitalen Signatur mit hoher Wahrscheinlichkeit nachweisen, dass ein elektronisches Dokument mit einer digitalen Signatur versehen wurde. Aber sie kann nicht zeigen, wer dies getan hat. Aufgrund der vorliegenden Technik mag es dabei vernünftig sein, anzunehmen der Signaturschlüsselinhaber beziehungsweise die im Zertifikat genannte Person habe die Signatur angebracht. Diese Vermutung hängt aber von der jeweils angewendeten Sicherheit insbesondere des Systems und der Komponenten, auf dem der private Schlüssel gespeichert ist, und von der Sorgfalt des Nutzers ab.[1343]
Die Sicherheit der eingesetzten Technik begründende Umstände müssen wiederum bewiesen werden. Damit steht auch dieses Konstrukt vor den gleichen oben[1344] beschriebenen Problemen.

[1338] Siehe Darstellungen oben unter 2.4.2.1, 2.4.3.1, 2.5.2.2, 2.5.3.1 und 2.5.4.1.

[1339] Siehe oben unter 2.5.2.4, 2.5.3.2, 2.5.4.2.

[1340] Die OECD hatte *non-repudiation* in den Guidelines for Cryptography Policy definiert als etwas mittels Verschlüsselungsmethoden Erlangtes (Eigentum, *property*), dass es einer (natürlichen oder juristischen) Person verwehrt, die Vornahme einer bestimmten Handlung zu leugnen, siehe oben 2.6.4.

[1341] Mason, *Electronic Signatures in Law*, S. 471. Die Nichtanerkennung (*repudiation*) einer handschriftlichen Unterschrift kann aus vielerlei Gründen erfolgen: Fälschung, Betrug, unbewusste Handlung etc.

[1342] Mason, *Electronic Signatures in Law*, S. 472.

[1343] Mason, *Electronic Signatures in Law*, S. 473.

[1344] 3.2.1.

Es wird deutlich, dass dieser Komplex in England und – zumindest auf Bundesebene – in den USA daher eher als Frage nach der allgemeinen Risikozuweisung und Beweislastverteilung hinsichtlich der Urheberschaft und damit der Sicherheit und Verlässlichkeit der eingesetzten Technik diskutiert wird. Dies findet seine Begründung in der Tatsache, dass für die Technik keine gesetzlichen Standards und (Vorab-)Prüfungen für die Verfahren und Komponenten und für die Zertifizierungsanbieter keine Prüfungen hinsichtlich ihrer Sicherheit und Zuverlässigkeit normiert sind, auf die sich gesetzliche Vermutungsregelungen oder andere Beweiskraftregeln stützen könnten. Grund hierfür ist wiederum die gewollte Technikneutralität dieser Regelungsansätze. Die Diskussion zeigt, dass sich Beweiskraft und Beweislast aus der eingesetzten Technik ergeben kann, sie sich aber nicht bereits a priori aus der Technik der digitalen Signatur ergeben müssen, so hoch deren Sicherheit auch eingeschätzt wird und so sehr ihr Einsatz propagiert wird. Zum anderen zeigt sich, dass diese Überlegung zur *non-repudiation* und ihrer Grundlagen, übertragen auf die rechtliche Beurteilung, grundsätzlich gleichermaßen auf alle Formen der Signatur, auch auf die digitale und die elektronische Signatur in ihrer einfachsten Form, angewendet wird. Eine Privilegierung der digitalen (oder fortgeschrittenen elektronischen) Signatur kann sich dort also allein aus einer vom Gericht festgestellten tatsächlichen höheren Sicherheit und Verlässlichkeit ergeben, wird aber nicht wie in Deutschland per Gesetz festgestellt.

3.2.2.3 Art. 13 MLeC und Art. 8 MLeS

Es ist anzunehmen, dass die in den Modellgesetzen der UNCITRAL aufgeführten Prinzipien von den englischen und US-amerikanischen Gerichten bei ihrer Beurteilung der elektronischen und digitalen Signatur berücksichtigt werden.[1345] Diese enthalten in Art. 13 MLeC und Art. 8 MLeS Regelungen zur Verantwortlichkeit von Aussteller und Empfänger beim Einsatz der elektronischen Signatur sowie zu den sich daraus ergebenden Vermutungen hinsichtlich der Authentizität und Integrität der signierten elektronischen Dokumente oder Kommunikation. Nach Art. 13 Abs. 3 MLeC soll der Empfänger von der Urheberschaft des Ausstellers ausgehen und gemäß dieser Annahme handeln dürfen, wenn der Adressat ein entsprechendes, zwischen den Parteien vereinbartes Verfahren eingesetzt hat, oder wenn er Zugang zu einer vom Aussteller zur Identifizierung verwendeten Methode hatte. Dies meint zum Beispiel die Prüfung des Zertifikats bei einer digitalen Signatur. Das soll nicht gelten, wenn der Empfänger hierbei nicht die nötige Sorgfalt eingehalten hat oder Kenntnis von der mangelnden Authentizität der Datennachricht hatte, Art. 13 Abs. 4 MLeC. Wenn die Datennachricht danach als diejenige des Ausstellers angesehen werden kann oder der Empfänger berechtigt ist von dieser Annahme auszugehen, dann soll der Empfänger ferner von der Integrität der Datennachricht ausgehen dürfen, Art. 13 Abs. 5 MLeC. Damit schafft das MLeC eine Vermutung dahingehend, dass eine Erklärung unter bestimmten Umständen als vom Aussteller

[1345] Mason, *Electronic Signatures in Law*, S. 483.

stammend angesehen werden kann.[1346] Die Beweispflicht kann dabei zwischen den Parteien wechseln. Wenn der Signaturschlüsselinhaber einen Prüfschlüssel veröffentlicht, wird bei dessen Benutzung davon auszugehen sein, dass der Signaturschlüsselinhaber diesen benutzt hat. Dabei wird vermutet, dass der Signaturschlüsselinhaber dafür Sorge trägt, dass nur er oder ein von ihm autorisierter Dritter den Schlüssel benutzt. Führt der Empfänger – als *verifying party* – die in Art. 13 Abs. 3 MLeC genannten Verfahren durch, wird er daran gehalten, dass er eine direkte Verbindung zwischen dem Zertifikat und Absender akzeptiert hat. Der Absender muss dann beweisen, dass er die mit der elektronischen beziehungsweise digitalen Signatur versehene Nachricht nicht versandt hat, was jedoch zu bezweifeln ist, wenn der Empfänger die erforderliche Sorgfalt angewandt hatte.[1347] Art. 8 MLeS beinhaltet ebenfalls Anforderungen an das Verhalten des Nutzers einer elektronischen und insbesondere einer digitalen Signatur. Von ihm wird verlangt, die erforderliche Sorgfalt beim Schutz der Signaturerstellungskomponenten und der Verhinderung deren unbefugten Nutzung walten zu lassen. Der Empfänger als auf die Signatur vertrauende Partei (*relying party*) wiederum soll gemäß Art. 8 MLeS die rechtlichen Konsequenzen für seine Unterlassung tragen, vernünftige (*reasonable*) Maßnahmen zur Verifizierung der Vertrauenswürdigkeit der elektronischen Signatur zu ergreifen. Allerdings ist die *relying party* nicht dazu verpflichtet, weil die Wirksamkeit der Signatur wiederum nicht vom Verhalten des Empfängers abhängen soll.
Die genannten Vermutungen und rechtliche Schlussfolgerungen können danach im *common law* aus dem Einsatz der elektronischen Signatur nur unter Berücksichtigung der jeweiligen (begleitenden) Umstände angeführt werden.[1348] Eine dabei zu berücksichtigende Voraussetzung ist, dass der Signierende bei der digitalen Signatur vollständige Kontrolle über die dafür eingesetzten Komponenten hat. Dies wird sowohl bei der Frage der *non-repudiation*[1349] als auch in Art. 13 MLeC und Art. 8 MLeS vorausgesetzt. Dies folgt aus der Tatsache, dass die im *common law* zur Beurteilung der elektronischen Signatur angewendeten Grundsätze die gleichen sind wie bei der anderer Signaturen. Die dort bestehenden Vermutungen hinsichtlich der Authentizität und Integrität beruhen ebenfalls auf der Annahme, dass der eigenhändig Unterzeichnende vollständige Kontrolle über die Unterschrift hat.[1350] Ferner wird Bezug genommen auf Fälle, in denen der Gebrauch eines Gummistempels dann als rechtswirksame *signature* anerkannt wurde, wenn der Signierende dieses Werkzeug sicher unter Kontrolle, das heißt sicher verwahrt hatte. Vor allem auch diese Tatsache der Sicherheit dessen Nutzung machte den Stempel überhaupt zu einer akzeptierten Form der Authentifizierung eines Dokuments[1351], siehe die Entscheidung in den oben erwähnten englischen Fällen *Goodman v. J. Eban Limited*[1352] und *British Estate Investment Society Ltd. v. Jackson (H M Inspec-*

[1346] Mason, *Electronic Signatures in Law*, S. 477.
[1347] Mason, *Electronic Signatures in Law*, S. 477, 478.
[1348] Mason, *Electronic Signatures in Law*, S. 481.
[1349] Oben 3.2.2.2.
[1350] Mason, *Electronic Signatures in Law*, S. 481, 482.
[1351] Mason, *Electronic Signatures in Law*, S. 483, 484.
[1352] Richter Evershed in *Goodman v. J. Eban Limited* [1954] 1 Q.B. S. 550, siehe oben 1.3.2.4.

tor of Taxes)[1353] sowie dem US-amerikanischen Fall *Robb v. The Pennsylvania Company for Insurance on Lives and Granting Annuities*[1354]. Wie es *McCullagh/Caell* ausdrücken:

> *„In einem auf Papier gegründeten Umfeld besteht ein absolut zuverlässiges System, da der oder die Unterzeichnende totale Kontrolle über den Signiermechanismus hat und der oder die Unterzeichnende sich nicht auf externe Informationen des Vertrauens verlassen muss, um seine oder ihre Unterschrift anzubringen. ... Nach common law ist die auf die Unterschrift vertrauende Partei beweisbelastet für den Nachweis, dass tatsächlich der behauptete Unterzeichner die Signatur angebracht hat. Dieser common law-Standpunkt hat sich in einem auf Papier gegründeten Umfeld entwickelt, in dem der Zeugenbeweis ein zuverlässiges Mittel zur Vermeidung von* [non-repudiation] *war. Aufgrund dieses zuverlässigen Mechanismus war es angemessen, die Beweislast der vertrauenden Partei aufzuerlegen ...“*[1355]

Eine entsprechende *rule of law* wurde in den vorbenannten Urteilen nicht aufgestellt, jedoch kann aus ihnen mit *Mason* zunächst gefolgert werden, dass dort, wo eine Technologie als Substitut für den physischen Akt des Aufbringens einer handschriftlichen Unterschrift genutzt wird, neue Überlegungen hinsichtlich der auf die Signatur angewandten Vermutungen angestellt werden müssen.[1356] Das Erfordernis der alleinigen Kontrolle über die Signaturerstellungskomponenten taucht auch in der Definition der fortgeschrittenen elektronischen Signatur in der RLeS, im SigG und in den ES Reg. auf.[1357] In den USA wurde in *Florida Department of Agriculture and Consumer Services v. Haire* das Urteil über eine elektronische Signatur explizit auch auf den Umstand gestützt, dass der signierende Richter die volle Kontrolle über deren Benutzung hatte.[1358] Dies vorausgesetzt, erscheint es angemessen, die Beweislast hinsichtlich des Einsatzes der elektronischen beziehungsweise digitalen Signatur bei dessen Verwender zu belassen, wie es auch in *Bank London Ltd. v. Bank of Tokyo Ltd.*, einem oben geschilderten Fall zu *tested telexes*, vom Gericht deshalb bestimmt wurde, weil der Versender die volle Kontrolle über die Umstände der Versendung hatte.[1359] Da die digitale Signa-

[1353] Richter Danckwerts in *British Estate Investment Society Ltd. v. Jackson (H M Inspector of Taxes)* (1954-1958) 37 Tax Cas, S. 79, S. 86; [1954] TR 397; 35 ATC 413; 50 R & IT 33, siehe oben 1.3.2.4.

[1354] *Robb v. The Pennsylvania Company for Insurance on Lives and Granting Annuities*, 40W.N.C. 129, 3 Pa.Super. 254, 1897 WL 3989 (Pa.Super. 1897), bestätigt durch 186 Pa. 456, 40 A969 (Pennsylvania), siehe oben 1.3.3.4.

[1355] McCullagh/Caelli, „Non-Repudiation in the Digital Environment”, First Monday, Vol. 5, No. 8, August 2000, http://.firstmondayorg/issues/issue5_8/mccullagh/ index.html.

[1356] Mason, *Electronic Signatures in Law*, S. 485.

[1357] Siehe oben 2.2.2.2, 2.3.3.1 und 2.4.3.1

[1358] *Florida Department of Agriculture and Consumer Services v. Haire*, 836 So.2d 1040 (Fla.App. 4 dist. 2003), corrected opinion *Haire v. Florida Department of Agriculture and Consumer Services*, Nos SC03-446 & Sc03-552, 12. Februar 2004.

[1359] *Bank London Ltd. v. Bank of Tokyo Ltd.* [1995] CLC 496; [1996] 1 C.T.L.R. T-17; Mason, *Electronic Signatures in Law*, S. 486, 491.

tur jedoch auch das Internet nutzt beziehungsweise nutzen kann, fällt genau diese Kontrolle über die Umstände der Anwendung der Signatur und die Übermittlung schwerer. Wie in Art. 13 MLeC und Art. 8 MLeS dargestellt, kann hier grundsätzlich eine Vermutung hinsichtlich der Authentizität und Integrität nur zugunsten des Empfängers bestehen. Will der Signierende diese Vermutung erschüttern, muss er demnach nachweisen, dass die digitale Signatur nicht von ihm stammt, etwa weil die vorausgesetzte Kontrolle (siehe oben dargestellte Sicherheitsprobleme etc.) nicht bestand. Um den auf die digitale Signatur Vertrauenden nicht dem Risiko auszusetzen, dass sich der Signierende auf den Umstand der mangelnden Kontrolle wegen der Unsicherheit zum Beispiel des Internets beruft, soll das oben dargestellte Verhältnis der Pflichten der Parteien bei der Verwendung von digitalen Signaturen Anwendung finden. Der Ausweg wäre hier dann letztlich wohl eine Rückforderung entstandener Schäden über Ansprüche wegen Vertragsbruch oder *negligence*.[1360] Vorerst bleibt es bei dem Dilemma: bei Anwendung von Vermutungen wie denen in MLeC und MLeS kann es dem vermeintlichen Signaturaussteller aufgrund der Manipulationsmöglichkeiten unter Umständen schwer fallen, erfolgreich zu beweisen, dass die Signatur nicht von ihm stammt; andererseits sieht sich nach den Regeln des *common law* der Empfänger als beweisbelastete *relying party* vor die Schwierigkeit gestellt, hinreichende Beweise für die Identität des vermeintlichen Signaturausstellers zu erbringen.[1361]

3.2.2.4 § 371a Abs. 1 ZPO – Anscheinsbeweis mit digitaler Signatur

In Deutschland sind rechtliche Folgen der elektronischen Signatur nur für die Form der qualifizierten und damit auch der akkreditierten elektronischen Form geregelt. Anknüpfungspunkt ist hier die Überprüfung der qualifizierten elektronischen Signatur. Die für diese digitale Signatur eingeführte Beweiserleichterung über § 371a Abs. 1 S. 2 ZPO beziehungsweise dessen Vorgängervorschrift § 292a ZPO[1362] wird stark kritisiert. Zum einen wird bemängelt, dass danach der Anschein der Echtheit nicht auf einem nach der Lebenserfahrung typischen Geschehensablauf, sondern auf einer gesetzlichen Vorgabe beruhe[1363] und es den hier fingierten Erfahrungssatz zur Sicherheit der Signatur tatsächlich nicht gebe.[1364] Es sei auch systematisch nur schwer nachvollziehbar, dass einem Augenscheinsobjekt, das grundsätzlich der freien richterlichen Beweiswürdigung unterliege, unter der Voraussetzung des Vorliegens eines bislang gesetzlich nicht geregelten Anscheinsbeweises dieselbe, das Gericht bindende Beweiskraft übertragen werde wie

[1360] So im Ergebnis auch Mason, *Electronic Signatures in Law*, S. 491.

[1361] McCullagh/Caelli, „Non-Repudiation in the Digital Environment", die schlussfolgern, dass es ohne die Einführung vertrauenswürdiger Signaturmechanismen gleich ist, welche der Positionen angewandt wird, da keine von beiden eine adequaten Lösung biete.

[1362] Darstellung oben 2.3.5.1.

[1363] Czeguhn, Ignacio, „Beweiswert und Beweiskraft digitaler Dokumente im Zivilprozess", JuS 2004, S. 124-126, S. 126; Huber in Musielak, § 371a, Rn. 7.

[1364] Czeguhn, JuS 2004, S. 126; Stadler, ZZP 2002, S. 434. Zu den Voraussetzungen des richterrechtlichen Anscheinsbeweises siehe unten unter 3.3.10.1.

einer Urkunde.[1365] Da bei einer handschriftlichen Unterschrift erst der Beweis ihrer Echtheit zur Anwendbarkeit der Vermutung des § 440 Abs. 1 ZPO führt, würden dem Empfänger qualifiziert signierter Erklärungen größere Beweisvorteile eingeräumt als dem Empfänger handschriftlich unterschriebener Schriftstücke.[1366] Vor allem aber setzt § 371a Abs. 1 S. 2 ZPO wegen der Verknüpfung mit dem Ergebnis der Überprüfung der Zuordnung des Signaturprüfschlüssels nach dem SigG voraus, dass der Beweisführer alle Voraussetzungen einer qualifizierten elektronischen Signatur § 2 Nr. 2 und 3 SigG nachweisen kann.[1367] Zu diesen sechs Voraussetzungen gehört unter anderem auch hier die alleinige und totale Kontrolle über die zur Erstellung der Signatur verwendeten Mittel. Hierzu bedarf es einer erfolgreichen technischen Prüfung der Signatur mit einer nach § 17 Abs. 2 SigG und § 15 Abs. 2 SigV geprüften Prüfsoftware. Gerät eine der Voraussetzungen für die qualifizierte elektronische Signatur in Zweifel, muss der Beweisführer deren Vorliegen beweisen, also zum Beispiel die technische und organisatorische Sicherheit beim Zertifizierungsdiensteanbieter nachweisen.[1368] Gelingt ihm dies, bedarf er der Beweiserleichterung des § 371a Abs. 1 S. 2 ZPO jedoch de facto nicht mehr.[1369] Gelingt ihm der Nachweis dagegen nicht, hilft auch diese Beweiserleichterung nicht weiter, weil es an der Grundlage für ihre Anwendbarkeit fehlt. Das ist wahrscheinlich, da es an einer behördlichen Vorabprüfung der Zertifizierungsdiensteanbieter bei der qualifizierten elektronischen Signatur fehlt. Dort müssen die Anbieter ihren Betrieb nur anzeigen.[1370] Ob die Anbieter die Betriebsvoraussetzungen erfüllen, kann nicht sicher angenommen werden und muss bis zum Nachweis in einem Gerichtsverfahren offen bleiben. Für sie gibt es keinen belastbaren Anschein, dass sie alle Voraussetzungen von SigG und SigV erfüllen.[1371] Hinzu kommt, dass dem Erklärungsempfänger kein Auskunftsanspruch gegen den Zertifizierungsdiensteanbieter des Signaturausstellers zusteht[1372] und er so allenfalls über die Regeln einer „sekundären Behauptungslast“ dem Gegner, so dieser Zugang zu diesen Daten hat, insoweit substantiierten Vortrag abverlangen müsste.[1373] Der Umstand, dass der Anscheinsbeweis des § 371a ZPO Merkmale zum Gegenstand hat, die allesamt in der Sphäre des Erklärenden liegen, wird denn auch als Rechtfertigung der Vorschrift gesehen.[1374] Ergibt die technische Prüfung

[1365] Klein, JurPC web-Dok. 198/2007, Abs. 61.

[1366] Blaurock/Adam, „Elektronische Signatur und europäisches Privatrecht“, ZEuP 2001, S. 93-115, S. 110, 111.

[1367] Dies sind immerhin sechs, siehe Darstellung bei GI, DuD 2001, S. 39; Roßnagel, Alexander, „Das neue Recht elektronischer Signaturen - Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO“, NJW 2001, S. 1817-1826, S. 1826. ; Stadler, ZZP 2002, S. 433.

[1368] Einsele in MüKo, § 126, Rn. 34; Huber in Musielak, § 371a, Rn. 8; Noack/Kremer, , *Anwaltkommentar BGB*, § 126a, Rn. 75; Roßnagel/Fischer-Dieskau, NJW 2006, S. 806-808, S. 807.

[1369] GI, DuD 2001, S. 39; Huber in Musielak, § 371a, Rn. 8; GI, DuD 2001, S. 39; Roßnagel NJW 2001, S. 1826; Stadler, ZZP 2002, S. 434.

[1370] Siehe oben 2.3.3.3.

[1371] GI, DuD 2001, S. 39.

[1372] Huber in Musielak, § 371a, Rn. 8: Roßnagel NJW 2001, S. 1826.

[1373] Stadler, ZZP 2002, S. 433.

[1374] Heusch, *Die elektronische Signatur – Änderungen des Bürgerlichen Rechts aufgrund der Signatur-Richtlinie (1999/93/EG) durch das Gesetz zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001*, Berlin 2004, S. 202.

der Signatur, dass diese vom Aussteller stammt, hat wiederum dieser große Schwierigkeiten einer Inanspruchnahme zu entgehen. So zum Beispiel bei missbräuchlicher Verwendung seiner Signaturkarte, wenn er nicht rechtzeitig die Signaturkarte hat sperren lassen.[1375]

Diese Problematik verstärkt sich noch, wenn Signaturen und Zertifikate aus der EU oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum in Spiel kommen. Diese sind nach § 23 Abs. 1 SigG qualifizierten elektronischen Signaturen gleichgestellt, wenn sie Art. 5 Abs. 1 RLeS[1376] erfüllen.[1377] Dabei ist nicht ausgeschlossen – sondern wahrscheinlich –, dass für viele ausländische Zertifizierungsdiensteanbieter keine Anzeigepflicht und kein mit dem deutschen vergleichbares Überwachungsverfahren bestehen. Ein Beispiel ist gerade England.[1378] An ausländische Signaturen werden durch diese Anerkennung geringere Anforderungen gestellt werden.[1379]

In noch weiterem Maße kann dies für Signaturen gelten, die auf Zertifikaten aus Drittstaaten außerhalb der EU, etwa den USA, beruhen. Diese werden ebenfalls qualifizierten elektronischen Signaturen gleichgestellt, wenn ein in der EU niedergelassener Zertifizierungsdiensteanbieter für diese Zertifikate einsteht.[1380] Hier wird zutreffend eingewandt, dass dies jedoch nur einen zusätzlichen Haftungsschuldner schafft, nicht aber einen Anschein für ausreichende Sicherheit begründet.[1381] Dieses Problem ist auch nicht einem Umsetzungszwang hinsichtlich der RLeS geschuldet. Denn die RLeS fordert nicht, ausländische Signaturverfahren mit Beweisvermutungen zu versehen.

Die Voraussetzungen einer qualifizierten elektronischen Signatur wird der Erklärungsempfänger bei der „akkreditierten" Signatur, also der qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung, nachweisen können. Dann nämlich hilft ihm die technisch-organisatorische Sicherheitsvermutung des § 15 Abs. 4 S. 4 SigG, da dann sicher davon ausgegangen werden kann, diese akkreditierte Signatur mit dem Signaturschlüssel des im zu Grunde liegenden qualifizierten Zertifikat angegebenen Signaturschlüssel-Inhabers erzeugt wurde, die signierten Daten nicht mehr verändert wurden und der Signaturschlüssel-Inhaber die Signatur erzeugt oder autorisiert hat.[1382] Schlüssig wäre es daher gewesen, hätte man die Beweisvermutung an diese höchste Stufe der Signaturverfahren nach dem SigG gebunden. Dies wird teilweise auch befürwortet als Signal der gewünschten Förderung akkreditierter Signaturverfahren.[1383] Das hätte frei-

[1375] Hähnchen, NJW 2001, S. 2833.

[1376] Art. 5 Abs. 1 RLeS: *„Die Mitgliedstaaten tragen dafür Sorge, dass fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und die von einer sicheren Signaturerstellungseinheit erstellt werden,... 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,..."*

[1377] Siehe oben unter 2.2.2.9, 2.3.3.6 und 2.4.3.

[1378] Siehe oben unter 2.4.2.2, 2.4.3.2.

[1379] GI, DuD 2001, S. 39.

[1380] Siehe oben unter 2.2.2.9 und 2.3.3.6.

[1381] GI, DuD 2001, S. 39.

[1382] Huber in Musielak, § 371a, Rn. 4, 9; Noack/Kremer in Dauner-Lieb et al., *Anwaltkommentar BGB*, § 126a, Rn. 26.

[1383] GI, DuD 2001, S. 40.

lich auf die Zertifizierungsdiensteanbieter einen nicht unerheblichen Druck ausgeübt, eine Akkreditierung anzustreben, was auf eine faktische Pflicht zur Vorabprüfung und Genehmigung (Akkreditierung) hinauszulaufen drohte. Das wiederum widerspräche dem Grundsatz des freien Marktzuganges innerhalb der EU.
Problematisch ist auch die Festlegung der Anforderungen an den Gegenbeweis, also der Tatsachen, die „ernstliche Zweifel" an der rechtlich zurechenbaren Abgabe der Willenserklärung begründen. Hier läuft es darauf hinaus, festzustellen, wie leicht eine Manipulation etwa durch Trojaner möglich ist, ob ein wirksamer Schutz gegen solche Schadprogramme besteht, man solche Trojaner rechtzeitig bemerken und deren Manipulation noch nachträglich feststellen kann. Wie oben festgestellt sind solche Angriffe möglich[1384], ein Schutz vor ihnen aber kaum möglich, solange die betreffenden Komponenten an das Internet angeschlossen sind. Solche Angriffe sind auch nicht notwendig feststellbar.[1385] Daher hat der Signaturinhaber keine realistische Möglichkeit, den Gegenbeweis zu führen, es sei denn die für die Signatur verwendeten Komponenten sind und waren zu keinem Zeitpunkt mit dem Internet weder direkt noch indirekt verbunden[1386], was das gesamte System aus Hardware und Software für die praktische Nutzung unbrauchbar machte.
Es bleibt festzuhalten, dass die Vorschrift des § 371a BGB die von ihr bezweckte Erleichterung bei der Beweisführung und damit den Zweck der Förderung der qualifizierten elektronischen Signatur nicht erreicht. Stattdessen wirft sie mehr Probleme auf, als sie an Lösungen bieten kann. Es ist nachvollziehbar, wenn deshalb gefordert wird, dass – wenn überhaupt – ein Anscheinsbeweis besser durch die Gerichte auf Grundlage der dafür bestehenden Maßgaben entwickelt werden sollte.[1387]

3.2.3 Mangelnde Akzeptanz

Das größte Manko der digitalen Signatur ist jedoch ihre mangelnde Verbreitung und Akzeptanz. Dies gilt für alle hier dargestellten Rechtsordnungen. Die bei der Einführung der oben dargestellten gesetzlichen Neuregelungen zur Jahrtausendwende vielfach geäußerten Hoffnungen auf eine baldige großflächige Verbreitung im elektronischen Rechtsverkehr sind nicht erfüllt worden. Schon damals wurde die Möglichkeit der Förderung durch die Verwendung im Behörden- und Gerichtsverkehr als die größte Stimulans für den Markt angesehen. Mittlerweile sind diesbezüglich zahlreiche Vorschriften ergangen, die den Austausch rechtserheblicher Erklärungen mit den Behörden, Gerichten und anderen öffentlichen Stellen ermöglichen und zum Teil sogar fördern oder als ausschließlichen Kommunikationsweg fordern – und dafür die Verwendung der digitalen Signatur voraussetzen. Dennoch ist erstaunlich, dass diese Technologie zum Beispiel weder für den Austausch vertraulicher Daten etwa im Anwalt-Mandanten-

[1384] 3.2.1.
[1385] Armgardt/ Spalka, K&R 2007, S. 31; Mason, *Electronic Signatures in Law*, S. 188.
[1386] Dazu auch oben 3.2.1.5.
[1387] GI, DuD 2001, S. 40.

Verhältnis, noch für Transaktionen von erheblichem Wert, etwa dem Autokauf im Internet, eine größere Verbreitung gefunden hat. Vielmehr werden die enormen Vorteile der elektronischen Kommunikation per Internet und der einfachen Handhabung, Speicherung und Bearbeitung elektronischer Dokumente offenbar gern angenommen. Sicherheitsvorkehrungen gehen aber in den meisten Fällen über den Schutz des Computers mittels Virenprogrammen und Firewalls nicht hinaus. Die noch vor nicht allzu langer Zeit geäußerte Zuversicht, mit den letzten gesetzlichen Neuerungen im Jahr 2005 und der Gründung des Signaturbündnisses, der beabsichtigten Einführung der sogenannten JobCard, digitalem Personalausweis, Gesundheitskarte etc., würden die Startschwierigkeiten der elektronischen Signatur und der elektronischen Form vergessen sein und deren Nutzung so selbstverständlich sein wie die Nutzung der Schriftform, ja dass sogar die elektronische Kommunikation wie selbstverständlich einhergehen würde mit elektronischer Signatur[1388], ist enttäuscht worden. Nach wie vor stehen einer breiten Anwendung der PKI-Technologie die mangelhafte Unterstützung durch bestehende Software und zu geringe Interoperabilität der bestehenden Verfahren, zu hohe Kosten, mangelndes Verständnis und zu große Betonung des Technologischen anstelle eines Abstellens auf die Bedürfnisse der Nutzer und das Fehlen einer – wie es *Meinel/Gollan* 2002 ausdrückten – „Killer-Applikation" entgegen.[1389] *Hoeren* spricht daher von der qualifizierten elektronischen Signatur als einer „Totgeburt".[1390] Die Schwächen der digitalen Signatur führen vielmehr zudem dazu, dass Signaturgesetze vielfach als unzureichend bewertet werden, zumal auch andere Technologien für sich beanspruchen können, eine sichere Authentifizierung herzustellen[1391] – ganz abgesehen davon, dass zunehmend Informations-, Impressums- und Aufklärungspflichten, insbesondere gegenüber Verbrauchern, die Warnfunktion der Schriftform übernehmen.[1392]

[1388] Noack/Kremer in Dauner-Lieb et al., *Anwaltkommentar BGB*, § 126a, Rn. 7-9.

[1389] Schapper/Rivolta/Veiga Malta, DEJ 2006, S. 12, 13; Bohm, DEJ 2006, S. 46; Meinel/Gollan, "Der elektronische Personalausweis? Elektronische Signaturen und staatliche Verantwortung", JurPC Web-Dok. 223/2002, Abs. 1-15, Abs. 15.

[1390] Hoeren, „Das Pferd frisst keinen Gurkensalat – Überlegungen zur Internet Governance", NJW 2008, S. 2615-2619, S. 2616.

[1391] Schapper/Rivolta/Veiga Malta, DEJ 2006, S. 12, 13.

[1392] So zutreffend Hoeren, NJW 2008, S. 2616.

3.3 Aufwertung elektronischer Erklärungen in Textform

Aus der oben dargestellten mangelnden Akzeptanz der digitalen Signatur in Form der qualifizierten elektronischen Signatur hat *Hoeren* kürzlich gefolgert:

> *„An die Stelle der Schriftform trat die Textform im Sinne des § 126b BGB."*[1393]

Erklärungen, die den Voraussetzungen der Textform des § 126b BGB entsprechen, weisen viele der Merkmale auf, die nach englischem und US-amerikanischen Recht unter Formerfordernisse des *writing* und des *signed writing* subsumiert werden können. Dabei sind die Funktionen, die dort den jeweiligen Formerfordernissen zugemessen werden und die also auch durch diese Form der Erklärung erfüllt werden können, weiter gehende als die bloße Informations- und Dokumentationsfunktion die der deutsche Gesetzgeber der Textform zumisst.[1394] Zudem können elektronische Erklärungen, die der Textform entsprechen, als einfache elektronische Signatur nach allen hier vorgestellten Gesetzen, Richtlinien und Modellgesetzen fungieren. Elektronische Signaturen dieser Art – ohne die Merkmale der digitalen Signatur – wiederum sind in England und USA hinsichtlich verschiedener Unterschriftserfordernisse als ausreichend anerkannt und die entsprechenden elektronischen Mitteilungen als echt beurteilt worden.[1395] Anhand dieser Entscheidungen aus den letzten Jahren wird dabei auch die differenzierte Behandlung solcher Erklärungen durch englische und US-amerikanische Gerichte deutlich. Es ist zu fragen, in welchen Fällen unter welchen Voraussetzungen diese Akzeptanz zustande kommt und ob hieraus – in Anbetracht der mangelnden Akzeptanz der digitalen Signatur und dem offensichtlichen vielfachen Gebrauch einfacher elektronischer Kommunikationsformen wie E-Mail und Internetverträgen – Argumente für eine Aufwertung von der Textform entsprechenden elektronischen Erklärungen abgeleitet werden können. Eine maßgebliche Frage ist dabei, ob diesen elektronischen Dokumenten nicht doch weitere Funktionen als eine bloße Informations- und Dokumentationsfunktion zukommen kann, etwa eine Identitätsfunktion. Letztlich geht es vor allem um die Frage, ob ihnen eine höhere Beweiskraft zugebilligt werden kann, als dies derzeit nach dem Willen des Gesetzgebers und den Beurteilungen deutscher Gerichte der Fall ist.

3.3.1 Vergleich der Textform mit *writing* und *signed writing*

Die Textform des § 126b BGB ist eine Form der Erklärung, die – unabhängig von der Art und Weise ihrer Erstellung – in Schriftzeichen lesbar und dauerhaft wiederzugeben sein soll. Eine Verkörperung ist nicht notwendig, sie kann also auch als elektronische Datei oder elektronisches Dokument, beispielsweise als E-Mail, bestehen. Sie soll der Information und vor allem der Dokumentation dienen. Damit erfüllten Erklärungen in

[1393] Hoeren, NJW 2008, S. 2616.

[1394] Siehe oben 2.3.4.2 im Vergleich zu dem Formfunktionen wie dargestellt in 1.3.2.1 ff., 1.3.3.1 ff.

[1395] Siehe oben 2.4.5 und 2.5.6.

der Textform des § 126b BGB zunächst die Voraussetzungen des Dokuments beziehungsweise der Urkunde (*document*) im englischen Civil Evidence Act 1995 und den Civil Procedure Rules 1998 als alles, in dem Informationen einer Beschreibung aufgezeichnet werden können, ungeachtet der dafür eingesetzten Mittel, sowie des Finance Act 1993, der Computeraufzeichnungen ausdrücklich einschließt. Auch das sonst im *common law* gebräuchliche Verständnis des Dokuments als geschriebene, schriftliche Sache, ungeachtet des Materials, auf welches die Schriftzeichen aufgebracht sind, kann unter die Definition des § 126b BGB der Textform subsumiert werden, solange es dauerhaft die enthaltene Schrift wiedergeben kann. Dass ein Dokument nach englischem Recht grundsätzlich als Beweis taugen muss, steht dem nicht entgegen. Zwar wird der Textform weder ein besonderer Beweiswert noch eine große Warnfunktion zugemessen. Andererseits sprach der deutsche Gesetzgeber der Textform nicht jeglichen Beweiswert ab. Vielmehr sind elektronische Dokumente in Textform als Augenscheinsobjekt der freien Beweiswürdigung zugänglich, also als Beweis tauglich.[1396] Auch eine Vielzahl von *writing*-Erfordernissen im englischen Recht würden Erklärungen, die der Textform entsprechen, erfüllen können. So verlangt der Copyright, Designs and Patents Act 1988 lediglich eine Form von Zeichen oder Code, gleich ob handschriftlich oder auf andere Weise erstellt und unabhängig von Methode und dem Medium ihrer Aufzeichnung. Auch die Voraussetzungen des *writing* im Interpretation Act 1978, die sämtliche Verfahren, Worte in sichtbarer Form zu präsentieren oder zu vervielfältigen umfassen, wären durch Erklärungen in Textform erfüllt, gerade auch als elektronisches Dokument oder elektronische Datei. Die hierfür nach englischem Recht geforderte Dokumentationsfunktion der im *writing* enthaltenen Information soll der Textform nach dem Willen des deutschen Gesetzgebers gerade zukommen.[1397] Im Übrigen begegneten elektronische Dokumente in Textform der gleichen fortbestehenden Unsicherheit hinsichtlich der Formerfüllung bestimmter *writing*-Erfordernisse soweit diese konstituierende Funktion haben. Diese Formerfordernisse der Schriftlichkeit sind in ihrer Funktion und Bedeutung jedoch ohnehin näher an der Schriftform des § 126 Abs. 1 BGB, wenn nicht mit dieser identisch, insbesondere da sie zumeist zudem die *signature* oder andere Förmlichkeiten verlangen (dazu nachfolgend). Auch die Voraussetzung der Reduzierung auf eine verkörperte Form eines *written document* gemäß dem US-amerikanischen UCC sollten Erklärungen in Textform, auch als elektronische Dokumente oder Dateien, erfüllen können. Denn als *writing* sind in den USA danach Telexe, Telegramme, Telefaxe, Magnetbänder, magnetische Aufzeichnungen, Internetverträge und damit Webseiten, sofern sie ausgedruckt und gespeichert werden können, und andere elektronische Vereinbarungen, mithin Erklärungen, anerkannt. *Writing* gemäß den Federal Rules of Evidence umfasst ausdrücklich Buchstaben, Wörter oder Zahlen unabhängig von der Art ihrer Entstehung wie Handschrift, Maschinenschreiben, Drucken, Fotokopieren, Fotografie, magnetischen Impuls, mechanische oder elektronische Aufzeichnung oder andere Formen der Zusammenstellung von Daten. Spätestens der UETA hat de lege festgestellt, dass gesetzliche *writing*-Erfordernisse in den USA auch durch elektronische Auf-

[1396] Siehe oben 1.3.2.5, 1.3.2.6 und 2.3.5.

[1397] Siehe Darstellung oben unter 2.3.4.2.

zeichnungen erfüllt werden können. Es zeigt sich, dass *writing*-Erfordernisse im englischen und US-amerikanischen Recht in ihren Voraussetzungen dem Erfordernis der dauerhaften Wiedergabemöglichkeit in Schriftzeichen gleichen beziehungsweise dieses umfassen. Ebenso ist die von den Gesetzgebern beabsichtigte Funktion der Dokumentation ähnlich, wiewohl in England und den USA vielfach die Beweisfunktion schriftlich festgehaltener Erklärungen und Vereinbarungen hervorgehoben wird. Auch die schriftliche Form (*writing*), wie sie das MLeC in Art. 6 versteht, ist mit der Textform vergleichbar, indem sie auf ihre Dauerhaftigkeit (*permanence*) beschränkt wird und keine Unterschrift verlangt. Die Datennachricht erfüllt danach das Erfordernis der Informationsübermittlung in schriftlicher Form, wenn die in ihr enthaltene Information für die spätere Referenz zugänglich bleibt. Diese Anforderungen entsprechen den in § 126b BGB enthaltenen.[1398]

Eine eigenhändige Unterzeichnung der Erklärung in Textform ist laut § 126b BGB nicht notwendig. Bei der in diesem Sinne unterschriftslosen Erklärung soll jedenfalls aber die Person des Erklärenden angegeben und der Abschluss der Erklärung erkennbar gemacht sein. Der Namen des Erklärenden soll die Herkunft der Erklärung erkennen lassen. Hierfür genügt zum Beispiel bei papiernen Dokumenten die Verwendung einer Nachbildung der Namensunterschrift auf einem Faksimilestempel oder sonstige mechanische Vervielfältigungen der Unterschrift und bei elektronischen Erklärungen etwa die Anbringung einer eingescannten Namensunterschrift.[1399] Bereits diese Benennung des Erklärenden kann unter Umständen den Voraussetzungen entsprechen, die das englische und US-amerikanische Recht an eine Unterschrift (*signature*) stellen. Nach englischem Recht können Faksimiles einer Unterschrift, unabhängig vom Wiedergabeprozess, als *signature* genügen, folglich Reproduktionen, Abschriften, Abdrucke, Ab- und Nachbildungen der Unterschrift, einschließlich der Wiedergabe der Unterschrift in einem elektronischen Format. Maßgeblich ist zunächst, wie auch nach US-amerikanischem Recht, ob diese *signature*, im Falle der Erklärung in Textform die Namensnennung, mit dem Willen aufgebracht wird, die jeweilige Erklärung etc. zu signieren und zu authentifizieren – was freilich zu beweisen ist. Zumindest letzteres muss aber für den Aussteller der Textform angenommen werden. Im *common law* ist diese Intention auch im Falle massenhaft erstellter Erklärungen angenommen worden, also auch für einen der laut deutschem Gesetzgeber originären Anwendungsbereiche der Textform.[1400] Eine handschriftliche Unterzeichnung ist nicht notwendig erforderlich. Ob die jeweilige Art der Unterschrift ein *signature*-Erfordernis erfüllen kann, hängt im *common law* – wie oben beschrieben[1401] – ferner vom jeweiligen Schriftformerfordernis und den damit verbundenen Funktionen, die die *signature* jeweils erfüllen soll, ab. Insbesondere auch für die Zwecke des Statutes of Frauds wurde dies in England für die bloße Namensnennung am Ende einer E-Mail, die damit auch die Voraussetzungen der Textform nach § 126b BGB

[1398] So auch Heydn in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 236.

[1399] Noack/Kremer, *Anwaltkommentar BGB*, § 126b, Rn. 20.

[1400] Vergleiche die Darstellung der Rechtsprechung unter 1.3.2.4, 1.3.2.6, 1.3.3.4, 1.3.3.6 sowie 2.4.5 und 2.5.6 mit der Zielsetzung des deutschen Gesetzgebers zur Textform unter 2.3.4.2 und unten 3.3.10.5.

[1401] Siehe 2.4.5 und 2.5.6.

erfüllte, angenommen.[1402] Gleiches wurde zuvor für die eingescannte handschriftliche Unterschrift angenommen.[1403] Auch laut UCC kann jedes Symbol, sofern es durch eine Partei mit der vorhandenen Absicht, ein Schriftstück zu authentifizieren, aufgebracht wird, eine Unterschrift darstellen. UETA bestimmt, dass eine elektronische Signatur auch gesetzliche Unterschriftserfordernisse erfüllen kann, ohne dabei über die oben genannten Merkmale hinausgehende Anforderungen an die elektronische Signatur zu stellen. E-Mails, die eine bloße Namensnennung des Verfassers im Text oder im Header enthielten, wurden daher auch hier als elektronische Signatur anerkannt[1404], auch für die Zwecke der Statute of Frauds.[1405]

Erklärungen und elektronische Dokumente, die in Deutschland die Voraussetzungen der Textform erfüllen, können also, den entsprechenden Willen des Ausstellers vorausgesetzt und belegt, zumeist die Voraussetzungen, die gesetzliche Formerfordernisse in England und den USA an das *writing*, insbesondere aber an die Unterschrift (*signature*) stellen, erfüllen. Vor allem wurden solche, der Textform entsprechenden elektronischen Dokumente in England und den USA tatsächlich als *writing* und sogar als *signature* von den Gerichten anerkannt. Das ist bemerkenswert, stellt man die nach dem Willen des deutschen Gesetzgebers der Textform zugesprochenen begrenzten Funktionen der Information und Dokumentation denjenigen Funktionen gegenüber, die Erfordernisse des *writing* und der *signature* im englischen und US-amerikanischen Recht erfüllen sollen. Dies gilt insbesondere, wo angenommen wird, dass eine Namensnennung in einer E-Mail – beziehungsweise einer Erklärung in Textform – oder gar die bloße E-Mail-Adresse die jeweiligen Funktionen der Formvorschriften erfüllen können sollen. Denn letztere umfassen insbesondere die Authentifikations- und Beweisfunktion, siehe das gegen betrügerische Ansprüche gerichtete und der Beweisbarkeit von Versprechen dienende *signature*-Erfordernis des Statute of Frauds[1406], was nach deutschem Recht gesetzlich allenfalls für eigenhändig unterzeichnete papierne Dokumente angenommen wird. Nach Signierung eines Vertrages, soll der Unterzeichner gehindert sein, später dessen Existenz oder Inhalt zu bestreiten.[1407] Dass einfache elektronische Dokumente

---

[1402] *Hall v. Cognos Limited*, Industrial Tribunal Case No. 1803325/97; *J. Perreira Fernandes SA v. Mehta* [2006] 1 WLR 1543; [2006] 2 All ER 891; [2006] 1 All ER (Comm) 885; [2006] All ER (D) 264; [2006] IP & T 546; The Times, 16. Mai 2006; [2006] EWHC 813 Ch.); *SM Integrated Transware Ltd. v. Schenker Singapore (Pte) Ltd.* [2005] 2 SLR 651, [2005] SGHC 58, 92.

[1403] *Re a debtor (No. 2021 of 1995), Ex p, Inland Revenue Commissioners v. The debtor; Re a debtor (No. 2022 of 1995), Ex, Inland Revenue Commissioners v. The debtor* [1996] 2 All E.R. 1208, S. 345, 351, zur Faxübertragung.

[1404] *Florida Department of Agriculture and Consumer Services v. Haire*, 836 So.2d 1040 (Fla.App. 4 dist. 2003), corrected opinion *Haire v. Florida Department of Agriculture and Consumer Services*, Nos SC03-446 & Sc03-552, 12. Februar 2004, *On Line Power Technologies, Inc., v. Square D. Company*, 2004 WL 1171405 (S.D.N.Y.); *Rosenfeld v. Zerneck*, 776 N.Y.S.2d 458 (Sup. 2004) (New York); *Bazak International Corp. v. Tarrant Apparel Group*, 378 F.Supp.2d 377 (S.D.N.Y. 2005) (New York); *International Casings Group, Inc. v. Premium Standard Farms, Inc.*, 358 F.Supp.2d 863 (W.D.Mo. 2005), 2005 WL 486784; *Poly USA, Inc. v. Trex Company, Inc.*, W.D. Va. No. 5:05-CV-0031 (1. März 2006).

[1405] *Lamle v. Mattle, Inc.*, 394 F.3d 1355 (Fed. Cir. 2005).

[1406] Siehe oben unter 1.3.2.1 ff., 1.3.3.1 ff.

[1407] *Smit International Singapore Pte Ltd v. Kurnia Dewi Shipping SA (The Kurnia Dewi)* [1997] 1 Lloyd's Rep 552; *L'Estrange v. Graucob* [1934] 2 K.B. 394; siehe auch oben unter 1.3.2.3.

und Kommunikationen unter Umständen dort diese Funktionen erfüllen sollen, kann nicht allein in ihrer (technischen) Natur begründet liegen. Denn diese führte in Deutschland gerade dazu, dass der Textform die Fähigkeit, weitere als die oben genannte Informations- und Dokumentationsfunktionen zu erfüllen, abgesprochen wird. Insbesondere die der Schriftform des § 126 BGB zugesprochene Warn-, Identitäts- und Beweisfunktion soll sie nicht erfüllen können. Das sollen elektronische Dokumente wie eine E-Mail hier nur unter Verwendung einer digitalen Signatur leisten können. Die Beurteilung englischer und US-amerikanischer Gerichte steht damit auch im Gegensatz zur Beurteilung deutscher Gerichte zur Beweiskraft von E-Mails und elektronischen Dokumenten, mithin auch der Textform (siehe auch nachfolgende Darstellungen).
Dabei muss berücksichtigt werden, dass die Signatur im *common law* als verkörperter und vertrauenswürdiger Beweis der Zustimmung und des Rechtsbindungswillens des Ausstellers sowie zur Feststellung dessen Identität und der Echtheit und Unverfälschtheit des Dokuments dienen kann – aber nicht muss. Diese Feststellungen sind nicht notwendiger Ausfluss der Einhaltung einer bestimmten Form, das heißt sie folgen nicht zwingend aus dem Vorliegen einer *signature*, wie dies für eigenhändig unterzeichnete Urkunden nach deutschem Recht angenommen wird. Im *common law* sind verschiedenste Formen der Signatur anerkannt. Die Gerichte stellen auf die Intention der Parteien ab und beziehen weitere Beweise und Indizien in ihre Beurteilung mit ein. Die Funktion, die eine Signatur ausübt, ist bedeutsamer als ihre Form. Problematisch scheinen allerdings auch in England und den USA weiterhin Erfordernisse zu sein, nach denen beispielsweise ein Vertrag *in writing* abgeschlossen, nicht bloß bewiesen werden muss, wie der Immobilienkaufvertrag, bei dem dieses Formerfordernis also konstitutiv wirkt. Auch ist zu berücksichtigen, dass konstitutive Formerfordernisse, die zwingend die handschriftliche Unterschrift verlangen, auch in England und den USA wohl nur durch elektronische Signaturen erfüllt werden können, die schwierig zu fälschen sind und die Echtheit des betreffenden Dokuments ebenso wie eine eigenhändige Unterschrift garantieren.
Auch der deutsche Gesetzgeber erkannte ein Verkehrsbedürfnis nach Erleichterung der strengen Schriftform hin zu einer Form der Erklärung, bei der die eigenhändige Unterschrift entbehrlich beziehungsweise unangemessen und Verkehrs erschwerend ist.[1408] Auch erkannte er, dass die Frage, welche Formerfordernisse und Formzwecke notwendig seien, sich an dem betreffenden Rechtsvorgang und nicht an der Art und Weise der Anfertigung der Erklärung orientieren müsse.[1409] Wie oben dargestellt ist der Kreis der Rechtsgeschäfte und rechtserheblichen Erklärungen, in denen elektronische Dokumente als *writing* und einfache elektronische Signaturen als *signature* akzeptiert werden, im englischen und US-amerikanischen Recht weitaus größer als der sehr begrenzte Anwendungsbereich der Textform des § 126b BGB und als es die Rechtsprechung zur Beweiskraft elektronischer Dokumente in Deutschland im Ergebnis zuließe. Die in Deutschland zur Begründung angeführte Natur dieser Dokumente, Erklärungen und

[1408] BT-Drucks. 14/4987, S. 18, 19; Einsele in MüKo, § 126b, Rn. 1; Geis, MMR 2000, S. 671.
[1409] BT-Drucks. 14/4987, S. 18, 19; Einsele in MüKo, § 126b, Rn. 1.

Vereinbarungen als bloß digitale, unverkörperte und leicht manipulierbare Dateien ist jedoch hier wie dort gleich.

3.3.2 E-Mail als Textform und elektronische Signatur

Sofern elektronische Dokumente und Dateien Form und Funktion der Textform erfüllen sollen, so müssen sie den Namen des Erklärenden enthalten, damit der Empfänger deren Herkunft erkennen kann.[1410] Dabei muss die Erklärung und damit auch die Benennung des Erklärenden in Schriftzeichen lesbar zu machen und zur dauerhaften Wiedergabe geeignet sein.[1411] Dies kann durch die Abbildung einer eingescannten Unterschrift oder die bloße Namensnennung in der elektronischen Erklärung erfolgen. An welcher Stelle in der Erklärung die Bennennung des Erklärenden erfolgt, ist gleichgültig. Sie kann also zum Beispiel im Kopf der Erklärung, bei E-Mails im Header, oder im Inhalt der Erklärung auftauchen, solange ihr Empfänger die Person, die die Erklärung in eigener Verantwortung abgibt, mit hinreichender Deutlichkeit erkennen kann. Auch die Verwendung von Vor- oder Spitznamen oder Pseudonymen ist unter dieser Voraussetzung möglich. Sofern dabei der Abschluss der Erklärung kenntlich gemacht wird, kann, wenn nicht eine andere Nachbildung der Unterschrift des Erklärenden hierfür verwendet wird, die übliche Benennung des Erklärenden am Ende des Textes erfolgen. Der Einsatz einer qualifizierten elektronischen Signatur des Erklärenden oder Ausstellers ist nicht erforderlich. Diese Benennung des Erklärenden beziehungsweise dessen Namensnennung in der elektronischen Erklärung, beispielsweise der E-Mail, erfüllt die Voraussetzungen der elektronischen Signatur wie sie in allen hier vorgestellten Vorschriften, Richtlinien und Modellgesetzen definiert wird.[1412] Alle diese Definitionen der elektronischen Signatur – in ihrer einfachsten Form – sind sehr ähnlich. Sie enthalten folgende Elemente:

(a) Daten (RLeS, SigG, EC Act, MLeS) oder (unter anderem) Verfahren (UETA, E-SIGN) in elektronischer Form.

(b) Diese Daten müssen anderen elektronischen Daten beigefügt oder mit diesen logisch verbunden werden.

(c) Die Funktion der elektronischen Signatur ist es, als Methode der Authentifizierung (RLeS, SigG) beziehungsweise zur Feststellung der Authentizität und/oder Integrität (EC Act, MLeS) zu dienen, beziehungsweise das Dokument oder die Aufzeichnung zu signieren (UETA, E-SIGN).[1413]

[1410] Siehe ausführlich oben 2.3.4.2.

[1411] Zur Abgrenzungsproblem zwischen E-Mails mit dynamischen HTML-Inhalten und Websites siehe oben unter 2.3.4.2.

[1412] Noack/Kremer, *Anwaltkommentar BGB*, § 126b, Rn. 20.

[1413] Art. 2 Nr. 1 RLeS, § 2 Abs. 1 SigG, : *„Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“*; § 7 Abs. 2 EC Act: *„Im Sinne dieses Paragraphen ist eine elektronische Signatur alles in elektronischer Form, das (a) in eine elektronische Mitteilung oder in elektronische Daten aufgenommen oder anders logisch mit ihnen verknüpft ist; und (b) vorgibt, so aufgenommen oder verknüpft zu sein, um der Feststellung*

Die Benennung des Erklärenden in der elektronischen Variante der Textform stellt solche elektronischen Daten dar, die anderen elektronischen Daten – der Erklärung – beigefügt werden. Sie dient insbesondere auch zur Authentifizierung des Erklärungsinhalts durch den Erklärenden beziehungsweise Aussteller.[1414] Aus diesen Definitionen der elektronischen Signaturen geht nicht ausdrücklich hervor, dass dabei die Daten authentifiziert werden sollen, denen diese elektronische Signatur beigefügt wird. Allerdings mag unterstellt werden, dass die Daten von der das Dokument oder die Mitteilung signierenden Person mit der Absicht hinzugefügt werden, dessen Text rechtsverbindlich zu bestätigen.[1415]

Fraglich ist, ob hierfür bereits die Namensangabe in der E-Mail-Adresse ausreicht, wie dies 2006 in im englischen Fall *J. Perreira Fernandes SA v. Mehta*[1416] in Bezug auf das Statute of Frauds akzeptiert wurde und auch im US-amerikanischen Fall *Poly USA, Inc. v. Trex Company, Inc.*[1417], ebenfalls in 2006, unter gewissen Voraussetzungen angenommen wurde. Dies setzte zunächst voraus, dass sich aus der E-Mail-Adresse der Name des Erklärenden, wenn auch als Vor-, Spitz oder Nachnahme, ergibt und damit für den Erklärungsempfänger kenntlich wird. Das Merkmal der Beifügung zu oder der Verknüpfung mit den übrigen, die Erklärung darstellenden Daten wird im Verhältnis der E-Mail-Adresse zum Inhalt und den übrigen Bestandteilen der E-Mail gegeben sein, auch wenn die E-Mail-Adresse vom Textkörper der E-Mail getrennt ist. Denn sofern eine E-Mail-Adresse nicht so in das elektronische Dokument E-Mail aufgenommen oder mit diesem verknüpft wäre, würde ihr Inhalt weder versendet noch seinen Empfänger erreichen. Unter diesen Voraussetzungen könnte eine E-Mail-Adresse eine elektronische Signatur gemäß den hier vorgestellten Regelungen darstellen.[1418] Um dabei die Voraus-

---

der Authentizität der Mitteilung oder Daten, der Integrität der Mitteilung oder Daten, oder beidem zu dienen."; Art. 2 lit. a) MLeS: *„Daten in elektronischer Form, die einer Datennachricht angefügt oder logisch mit ihr verknüpft werden, und dafür genutzt werden, den Aussteller dieser Datennachricht zu identifizieren und dessen Billigung der in der Datennachricht enthaltenen Informationen festzustellen."*; § 2 Nr. 8 UETA [und § 106 Abs. 5 E-SIGN]: *„Eine ‚elektronische Signatur' ist* [Der Begriff ‚elektronische Signatur' bezeichnet] *jeder elektronische Ton, jedes elektronische Symbol oder jedes elektronische Verfahren, der oder das [einem elektronischen Vertrag oder] einer elektronischen Aufzeichnung beigefügt oder mit [diesem] dieser logisch verknüpft ist und von einer Person mit dem Willen, diese Aufzeichnung zu signieren, ausgeführt oder gebilligt wurde."* Auch der Begriff *authentication* aus § 102 lit. A) Nr. 5 UCITA umfasst den Vorgang des Signierens, des Anbringens oder logischen Verknüpfens oder Verbindens eines elektronisches Symbols, eines Geräuschs mit, oder des Anwendens eines Verfahrens auf eine Mitteilung.

[1414] So auch *Mehta v. J. Perreira Fernandes SA* [2006] 1 WLR 1543, [2006] EWHC 813 (Ch), Abs. 28, 30, wonach die Namenseinfügung in den Textkörper der E-Mail eine hinreichende Signatur gemäß Statute of Frauds darstellen kann.

[1415] Mason, *Electronic Signatures in Law*, S. 277, der die elektronische Signatur auch beschreibt als alles in elektronischer Form, das dazu genutzt werden kann, die Absicht des Signierenden aufzuzeigen, seine Signatur solle rechtlich bindend sein. Auch Cordes, S. 183.

[1416] *J. Perreira Fernandes SA v. Mehta* [2006] 1 WLR 1543; [2006] 2 All ER 891; [2006] 1 All ER (Comm) 885; [2006] All ER (D) 264; [2006] IP & T 546; The Times, 16. Mai 2006; [2006] EWHC 813 Ch.), später aufgehoben durch *Mehta v. J. Perreira Fernandes SA* [2006] 1 WLR 1543, [2006] EWHC 813 (Ch).

[1417] *Poly USA, Inc. v. Trex Company, Inc.*, W.D. Va. No. 5:05-CV-0031 (1. März 2006).

[1418] So auch Mason, *Electronic Signatures in Law*, S. 317, 318. A.A. *Mehta v. J. Perreira Fernandes SA* [2006] 1 WLR 1543, [2006] EWHC 813 (Ch), Abs. 29, wo das Gericht diese Trennung bei einer wie

setzungen der Textform zu erfüllen, müsste zudem der Abschluss des E-Mail-Textes kenntlich gemacht werden, etwa durch einen darauf hinweisenden Zusatz. Solche elektronischen Erklärungen galten in den oben dargestellten Urteilen englischer und US-Amerikanischer Gerichte[1419] als *signed writing* zum Beispiel gemäß den Statutes of Frauds. Fraglich ist jedoch, ob dies auch im Falle der automatischen Einfügung der E-Mail-Adresse durch das E-Mail-Programm oder den Service Provider gelten kann. Genau dieser Umstand hat im englischen Fall *Mehta v. J. Perreira Fernandes SA* zu dem Urteil geführt, dass keine *signature* vorliege:

> *„Worauf hier vertraut wird ist eine E-Mail-Adresse. Dies ist für E-Mails die Entsprechung zur Fax- oder Telexnummer. ... Kann vernünftiger Weise angenommen werden, dass der automatisch generierte Name und Faxnummer des Absenders auf einem gefaxten Dokument ... eine Signatur ... darstellt? Wenn dem so ist, so hängt die Antwort allein davon ab, ob der Absender wusste, dass die Nummer oder Adresse auf der Empfänger-Kopie erscheinen würde.“*[1420]

Ohne dahingehende Beweise könne aber nicht grundsätzlich davon ausgegangen werden, dass Absender oder Empfänger der E-Mail oder deren Service Provider die E-Mail-Adresse als *signature* wollten und einsetzen, womit es fraglich sei, ob die automatische E-Mail-Adresseinfügung eine Unterschrift gemäß Statute of Frauds darstellen könne.[1421] Ob deren Voraussetzungen erfüllt sind, sei danach zu beurteilen, ob das Verhalten des angeblich Unterzeichnenden für einen verständigen Dritten (*a reasonable person*) auf einen solchen Willen schließen lasse.[1422] Hier wird wieder erneut die Bedeutung des *intents to authenticate* und von dafür sprechenden Beweisen oder Indizien deutlich. Im konkreten Fall urteilte das Gericht deshalb:

> *„Meines Erachtens ist die Einfügung einer E-Mail-Adresse unter diesen Umständen ein eindeutiges Beispiel für eine zufällige* [incidental] *Einfügung des Namens. ... Ohne entgegenstehende Beweise ist es aus meiner Sicht nicht möglich zu urteilen, dass die automatische Einfügung einer E-Mail-Adresse... als Unterschrift gewollt ... ist.* [So zu entscheiden] *... würde, denke ich, den Zweck der Vorschrift wie ich ihn verstehe unterminieren oder potenziell unterminieren und stünde den grundlegenden Prinzipien der* [Referenzfälle] *entgegen ... und*

üblich automatisch eingefügten Absender-E-Mail-Adresse als Hinweis darauf ansah, dass die Adress-Einfügung rein zufällig und kein willentlicher Akt sei.

[1419] 2.4.5 und 2.5.6.

[1420] *„What is relied upon is an e-mail address. It is the e mail equivalent of a fax or telex number. ... Can it sensibly be suggested that the automatically generated name and fax number of the sender of a fax on a faxed document ... would constitute a signature ...? If* [this] *is right then the answer depends solely upon whether the sender knew that the number or address would appear on the recipient's copy.”*, *Mehta v. J. Perreira Fernandes SA* [2006] 1 WLR 1543, [2006] EWHC 813 (Ch), Abs. 23.

[1421] *Mehta v. J. Perreira Fernandes SA* [2006] 1 WLR 1543, [2006] EWHC 813 (Ch), Abs. 25, 28.

[1422] *Mehta v. J. Perreira Fernandes SA* [2006] 1 WLR 1543, [2006] EWHC 813 (Ch), Abs. 30.

hätte weit reichende und völlig unbeabsichtigte rechtliche und wirtschaftliche Folgen.“[1423]

Diese Argumentation ist schlüssig. Es ist zweifelhaft, ob grundsätzlich davon ausgegangen werden kann, dass der Absender – auch wenn er um die automatische Einfügung seiner E-Mail-Adresse durch, bei oder nach dem Absendevorgang oder -befehl weiß – einen solchen Willen, die Erklärung zu authentifizieren, hat. Es ist jedoch nicht ausgeschlossen und mag durch ergänzende Beweise oder Indizien belegt werden.
Für die hier interessierende Erfüllung der Voraussetzung aus § 126b BGB, dass die Person des Erklärenden genannt werden muss, ist die Frage eines solchen Automatismus ohne Belang. Die Textform verlangt einen solchen Willen zur Authentifizierung nicht, wiewohl die Namensnennung zumindest im Textkörper einer E-Mail unter bestimmten Umständen Ausdruck genau dieses Willens sein kann. Ist dies der Fall und wird dies vom Gericht auch so erkannt, so ist zu fragen, ob dieser Umstand Auswirkung auf die Bewertung der Echtheit und Urheberschaft der E-Mail haben kann oder haben muss.

3.3.3 *Reliability test* gemäß MLeS, MLeC und UN-Konvention bei Textform und E-Mail

Art. 6 Abs. 1 MLeS, Art. 7 Abs. 1 lit. b) MLeC und Art. 9 Abs. 3 der UN-Konvention enthalten mit dem sogenannten *reliability test* Anforderung an Identifizierungsmethoden (*as reliable as appropriate for the purpose*), die bei der Feststellung der Authentizität elektronischer Kommunikationen zu berücksichtigen seien.[1424] Sie treten neben die bereits dargestellten Pflichten und Verantwortlichkeiten von Absender und Empfänger solcher Nachrichten.[1425] Daneben listet § 162 der Explanatory Notes zum MLeC weitere bei der rechtlichen Beurteilung einer bestimmten Identifizierungsmethode zu berücksichtigende Faktoren auf. Ob eine Methode in ausreichender Weise den Unterzeichner identifiziert, soll danach unter anderem vom Zweck der elektronischen Kommunikation, der von den Parteien verwendeten Ausrüstung, der Art und Größe der Transaktion, der Bedeutung und dem Wert der in der elektronischen Kommunikation enthaltenen Informationen, der Verfügbarkeit alternativer Identifikationsmethoden und deren Kosten, dem Grad der Akzeptanz der verwendeten Identifikationsmethode sowie der Funktion der entsprechenden Formvorschrift abhängen. Unter letzterem Aspekt lässt sich die Frage der angemessenen Zuverlässigkeit gemessen an dem Formerfordernis nach deutschem Recht nunmehr eindeutig beurteilen. Wird per Gesetz die Schriftform und mithin

[1423] *„In my judgement the inclusion of an e-mail address in such circumstances is a clear example of the includion of a name which is incidental. … Absent evidence to the contrary, in my view it is not possible to hold that the automatic insertion of an e-mail address is … “… intended for a signature …”.* [To hold thus] *... would I think undermine or potentially undermine what I understand to be the Act's purpose, would be contrary to the underlying principle to be derived from* [the authorities] *... and would have widespread and wholly unintended legal and commerical effects.”*, *Mehta v. J. Perreira Fernandes SA* [2006] 1 WLR 1543, [2006] EWHC 813 (Ch), Abs. 29.

[1424] Siehe oben unter 2.6.1 und 2.6.3.

[1425] Oben 2.6.1 und 2.6.2.

die Einhaltung der Voraussetzungen des § 126 BGB verlangt, so ist dies nur mit der elektronischen Form gemäß § 126a BGB und folglich nur mit der qualifizierten elektronischen Signatur zu erfüllen. Gleiches gilt dort, wo öffentlich rechtliche Vorschriften die Schriftform verlangen, wobei bei prozessualen Formerfordernissen Aufweichungen bestehen.[1426] Welche Formen der elektronischen Kommunikation bei gewillkürten Schriftformerfordernissen ausreichen sollen, lässt sich ebenfalls dem Gesetz, § 127 BGB, entnehmen.

Übertragen werden könnten die Grundsätze des *reliable as appropriate for the purpose* vielleicht auf die Diskussion um die Beweiskraft von E-Mail und Textform und die Feststellung der Authentizität einer solchen Kommunikation. In der Rechtsprechung deutscher Gerichte, in der die Beweiskraft elektronischer Kommunikationen wie E-Mail und elektronischer Verträge etwa bei Internetversteigerungen behandelt wurde, spielten die oben genannten Aspekte aus § 162 Explanatory Notes offenbar keine Rolle.[1427] Sie könnten dennoch als Argument für die Förderung der rechtlichen Akzeptanz der Textform dienen. Dabei könnte die bloße Namensnennung oder die eingescannte Unterschrift als Bilddatei in einer E-Mail, also die einfache elektronische Signatur, bei bestimmten, zum Beispiel ihrem Wert nach begrenzten Rechtsgeschäften als angemessene Authentifizierungsmethode genügen. Denn in den allermeisten Fällen, etwa beim Erwerb von Waren und Dienstleistungen über das Internet, werden die Parteien den Austausch von E-Mails oder die Verwendung von *Click-Wrap*-Verträgen als eine den Umständen und dem Wert der Transaktionen angemessene Form der Kommunikation ansehen. Andernfalls hätten sie sich nicht für diese Form entschieden. Damit taucht der Aspekt der Differenzierung je nach Art und Umfang des betreffenden, durch elektronische Kommunikation oder die Textform zu erfüllende Rechtsgeschäfts auf. Ist es sinnvoll, die Anforderungen an die Authentifizierungsmethode und also in die für die Darlegung der Echtheit und Integrität einer Erklärung jeweils entsprechend herabzusetzen oder zu erhöhen? Die in eine ähnliche Richtung wie der *reliability test* zielende Frage, nämlich ob die Verwendung von E-Mails in den jeweiligen Umständen angemessen und vernünftig (*appropriate and reasonable*) ist, wurde zum Beispiel im US-Fall *Bazak International Co. v. Mast Industries, Inc. 73*[1428] diskutiert:

> *„… ob E-Mail eine angemessene und vernünftiger Weise zu erwartende Form der Kommunikation darstellt, ist vor Gericht eine Tatsachenfrage* [question of fact]. *Hier verlangt die Lösung der Frage eine tatsächliche Untersuchung der Handelsgebräuche und Geschäftsgepflogenheiten. … Spätere E-Mail-Korrespondenz … liefert jedoch einen Beweis, auf dessen Grundlage eine ver-*

[1426] Zum prozessualen Schriftformerfordernis bei bestimmenden Schriftsätzen siehe unten 3.3.12.

[1427] Siehe Darstellung unten unter 1.3.2.6.

[1428] *Bazak International Co. v. Mast Industries, Inc. 73* N.Y.2d 111, 7 UCC Rep. Serv. 2d 1380 (1989), bzw. 535 N.E. 2d 633 (N.Y. 1989): *„… whether email is an appropriate and reasonably expected form of communication between the two particular parties before the court is a question of fact. Here, the issue's resolution requires a factual inquiry into trade usage and course of dealing. … Yet later email correspondence … provides evidence in light of which a reasonable jury could find that the parties did accept email as an appropriate form of communication."* Siehe auch oben 1.3.3.2.

nünftige Jury darauf schließen könnte, dass die Parteien dies als angemessene Kommunikationsform akzeptierten."

Diese Überlegung ließe sich gleichermaßen auf eine elektronische Kommunikation übertragen, die die Formerfordernisse der Textform nach § 126b BGB erfüllt. Unter gewissen Umständen kann beispielsweise der Austausch von E-Mails nebst Namensangabe oder eingescannter Unterschrift eine durchaus angemessene Art der Kommunikation auch für rechtserhebliche Erklärungen sein, was sogar die Identifizierung des Kommunikationspartners einschließt. Sofern eine E-Mail zum Vertragsschluss verwendet wird und die Namensangabe darin als Akt der Authentifizierung dieser Nachricht gewollt ist, so ist nicht einzusehen, warum, zumal wenn diese Kommunikationsform zwischen den Parteien bewusst und einvernehmlich geschieht, dies subjektiv für diese Parteien nicht eine den Zwecken entsprechend angemessene oder zuverlässige Identifizierungsmethode sein soll. Denn unter diesen Voraussetzungen soll die E-Mail nach englischem und US-Amerikanischem Recht sogar *signature*-Erfordernisse erfüllen können. Die Entscheidung der Parteien für diese Kommunikationsform und das damit dieser entgegengebrachte Vertrauen umfasst auch die Frage der Identität des Vertragspartners. Sofern ein gesetzliches, zwingendes Formerfordernis nicht eine andere Erklärungsform verlangt und somit diese Kommunikationsform ausschließt, ist, unter Einbeziehung der Aspekte aus § 162 Explanatory Notes, nicht ersichtlich, warum dies nicht auch nach objektiven Maßstäben – und nach deutschem Recht – eine dem Zweck angemessen zuverlässige Form sein soll, die Echtheit der Nachricht festzustellen. Gerade dieser Ausschluss der elektronischen Kommunikationsform wird aber nach deutschem Recht bei gesetzlichen Formerfordernissen zumeist der Fall sein. Bei zwingenden gesetzlichen Formerfordernissen kann die Formerfüllung, zumindest nach dem deutschen Rechtsverständnis, nicht von der Wahl und den Motiven der Parteien und der von ihnen angewendeten Technologie abhängig sein. Anders ist dies bei der freien Formwahl der Parteien. Hier ist jedoch mit § 127 BGB eine entsprechende Regelung gefunden, die einen *reliability test* überflüssig macht, zumal auch eine E-Mail die gewillkürte Schriftform erfüllen können soll.[1429]

Der *reliability test* wird als unrealistisch kritisiert in dem Fall, dass über die Identität der Parteien beziehungsweise des Signierenden und über die Echtheit des Dokuments zwischen den Parteien kein Zweifel und kein Streit herrschen. Sofern ein Dokument in gutem Glauben signiert worden sei und die Vertragsparteien den Vertrag als authentisch und wirksam anerkennen, bestünde kein Grund für das Gericht, die Frage der Echtheit weiter zu behandeln. Dann nämlich sei die Methode der Generierung des Dokuments irrelevant.[1430] Diese Feststellung ist so richtig wie überflüssig. Auch nach deutschem Recht ist eine unbestrittene E-Mail beziehungsweise eine E-Mail, deren Inhalt und Identität des Versenders unbestritten ist, als Beweismittel des Augenscheins im Rahmen der freien Beweiswürdigung unproblematisch. Dennoch soll die Bedeutung des *reliability test* insofern beschränkt sein, als dass er gemäß § 164 der Explanatory Notes von einer

[1429] Dazu unten 3.3.12.

[1430] Mason, *Electronic Signatures in Law*, S. 136.

Partei nicht angerufen werden darf, um die eigene Signatur zu leugnen, wenn die tatsächliche Identität und Intention, zu signieren, bewiesen werden konnte. Die Voraussetzung, dass eine Signatur *„as reliable as appropriate"* sein solle, dürfe laut UNCITRAL nicht zu einem Verfahren (*court trier in fact*) führen, in dem, weil die elektronische Signatur nicht (ihrem Zweck) entsprechend sicher gewesen sein mag, der gesamte Vertrag als ungültig erklärt werde, obwohl die Echtheit der Signatur nicht in Frage steht. Ein solches Ergebnis sei unglücklich, da es der Partei eines Vertrages, für den eine Unterschrift gefordert ist, erlaube, seinen Verpflichtungen durch die Behauptung zu entkommen, ihre oder die Signatur der anderen Partei sei unwirksam – nicht, weil eine Signatur nicht vorläge oder das entsprechende Dokument verändert worden sei, sondern allein deshalb, weil das Signaturverfahren nicht entsprechend sicher sei.[1431] Für nicht einer bestimmten Form bedürfende Verträge beziehungsweise für die freie Formwahl ist dem aus Sicht des deutschen Rechts zuzustimmen. Gleiches wird für das englische und das US-amerikanische Recht gelten. Die hinter dem *reliability test* stehende Überlegung ist folglich die, dass keine der Parteien sich allein durch Berufung auf einen technologischen Umstand, der sich im Einzelfall überhaupt nicht ausgewirkt haben muss, aus der vertraglichen Verpflichtung stehlen können soll. Genau diesen Effekt aber hätte eine generelle Verneinung der Beweiskraft von E-Mail und (elektronischer) Textform. Die Einstellung deutscher Gerichte zur Beweiskraft elektronischer Dokumente und Kommunikation führt zum gleichen Ergebnis wie die Anwendung des *reliability test*, der angewendet wird, obwohl die Parteien sich bewusst für diese Kommunikationsform und damit für diese (einfache) Authentifizierungsmethode entschieden haben. Die Beschränkung des Anwendungsbereiches des *reliability test*, wie sie vorstehend beschrieben und von der UNCITRAL gefordert wird, soll jedoch gerade ein einseitiges aufbürden des Risikos auf eine Partei verhindern. Die Folgen der deutschen Rechtsprechung zur Beweiskraft elektronischer Dokumente und Kommunikation sind insoweit also nicht konform mit dem Modellgesetzen der UNCITRAL – setzt man voraus, dass die dort behandelten Formen der Kommunikation eine elektronische Signatur beinhalten, was nach obiger Feststellung[1432] bei der Namensnennung in einer E-Mail etc. der Fall ist. *Mason* kritisiert den *reliability test* auch grundsätzlich dahingehend, dass die Frage, ob eine Identifizierungsmethode dem Zweck des jeweiligen Rechtsgeschäfts entsprechend vertrauenswürdig und angemessen ist, einigermaßen irrelevant sei, weil die Menschen dazu neigten, jede ihnen zur Verfügung stehende Form der Kommunikation zu nutzen, ohne sich über die rechtlichen Auswirkungen der jeweiligen Methode Gedanken zu machen. Dies sei immer so gewesen und es erscheine unüblich, dass nun Gesetzgeber solche zusätzlichen Anforderungen oder Voraussetzungen aufstellen sollten – insbesondere hinsichtlich des *common law*, wo solche Voraussetzungen zuvor an neue Technologien wie zum Beispiel an die Nutzung von Telegrammen nicht gestellt wurden.[1433] Hier deu-

[1431] § 163 Explanatory Notes zur UN-Konvention.

[1432] Siehe 3.3.1 und 3.3.2.

[1433] Mason, *Electronic Signatures in Law*, S. 243. siehe Darstellung oben unter 1.3.2.4 und 1.3.3.4.

tet sich an, dass letztlich die Frage der generellen Risikoverteilung und der Einbeziehung ergänzender Beweise und Indizien entscheidend ist.[1434]

3.3.4 Das Kriterium der Zuverlässigkeit der elektronischen Signatur

Anknüpfend an das zuvor erwähnte Merkmal der *reliability* (Zuverlässigkeit) der elektronischen Signatur soll nochmals kurz erwähnt werden, welche Bedeutung englische und US-amerikanische Gerichte diesem Kriterium für die Rechts- und Formwirksamkeit der Signatur beimessen. Danach hängt die Gültigkeit der Signatur von der Funktion ab, die sie erfüllt, nicht notwendig von der Form, in der sie erscheint. Hinzu kommt, dass auch wenn die Art einer Signatur, zum Beispiel das Anklicken eines „Ich akzeptiere"-Buttons zur Bestellung von Waren, als weniger sicher als die handschriftliche Unterzeichnung gilt, daraus nach englischem und US-amerikanischen Recht nicht notwendig folgt, dass die Zuverlässigkeit oder Vertrauenswürdigkeit (*reliability*) der Signatur ihre Rechtsgültigkeit beeinträchtigt.[1435] Sollte diese Frage jedoch streitig sein und vor Gericht geklärt werden müssen, so kommt es hier insbesondere auf die Menge und die Qualität der den Parteien vorliegenden Beweise an. Sehr wahrscheinlich wird die Zuverlässigkeit der Signatur auch hier davon abhängen, dass hinreichender Beweis dafür erbracht wird, ob beispielsweise der entsprechende Button gedrückt wurde oder nicht. Selbst wenn dies feststeht folgt daraus aber nicht, dass der angebliche Unterzeichner dies getan hat. Auch diese Verbindung zwischen der Handlung des Signierens und der Identität der Person muss bewiesen werden.[1436]

3.3.5 Beweisführung mit elektronischen Dokumenten und Signaturen

Elektronische Signaturen, elektronische Dokumente, E-Mails oder die vorgenannten Kopien und Ausdrucke etc. sind nach allen hier verglichenen Rechtsordnungen als Beweismittel zugelassen, allerdings nur der freien Beweiswürdigung zugänglich. Elektronische Dokumente haben keine Urkundsqualität im Sinne des Zivilprozessrechts und ohne qualifizierte elektronische Signatur finden die auf Urkunden anwendbaren Beweisregeln keine Anwendung auf sie, § 286 Abs. 2 ZPO. Sie sind Augenscheinsbeweis in dessen Beurteilung das Gericht fei ist.[1437] Es liegt im Ermessen des Gerichts über dessen Beweiswert zu befinden.[1438] Letzteres kann als besonderer Vorteil gewertet werden, da dabei im Einzelfall durch das Gericht zum Beispiel festzustellen ist, welche Vorkehrungen gegen Manipulationen getroffen worden sind und ob unter Berücksichtigung dieser Umstände vernünftige Zweifel an der Person des Ausstellers oder dem Inhalt der

[1434] Dazu ausführlich unter 3.3.8, 3.3.9, 3.3.11.

[1435] Mason, *Electronic Signatures in Law*, S. 299, 316.

[1436] Mason, *Electronic Signatures in Law*, S. 299.

[1437] Siehe oben 1.3.1.4, 2.3.5.1.

[1438] Niemann, CLSR 2001, S. 28. Siehe auch oben unter 1.3.2.5, 1.3.2.6, 1.3.3.4, 1.3.3.6, 2.3.52.4.5, 2.5.6.

Erklärung bestehen, weshalb die freie Beweiswürdigung auch als *„das effektivste und flexibelste Mittel zur Wahrheitsfindung“* und einer Beweiskraftregel überlegen gepriesen wird.[1439] Wollte man es dagegen nicht beim Grundsatz freier Beweiswürdigung belassen, etwa weil man die Sicherheit eines bestimmten Signaturverfahrens honorieren und dieses fördern möchte, wären eigene Beweisregeln für diese zu schaffen. In Deutschland ist dies für einen besonderen Fall mit § 371a Abs. 1 ZPO erfolgt, jedoch mit zweifelhaftem Erfolg.[1440] Es ist also zunächst zu fragen, wie die Beweisführung bei elektronischen Dokumenten und elektronischer Kommunikation möglich ist.

3.3.5.1 Art und Qualität der Beweise

Während es möglich ist, dass eine elektronische (digitale) Signatur die selben Funktionen wie eine handschriftliche Unterschrift erfüllt, existiert das entsprechende signierte Dokument nicht als physisches Objekt wie der Inhalt eines Dokumentes in papierner Form. Auch wenn sie jenseits der physischen Welt zu existieren scheint, ist sie doch abhängig von der Existenz einer gegenständlichen Aufzeichnung. Diese kann mittels Speicherung auf einer Festplatte, im Arbeitsspeicher oder als Darstellung auf einem Bildschirm geschehen. Es ist nicht notwendig beabsichtigt, dass eine elektronische Signatur eine verkörperte Form hat. Dies lässt zunächst den Schluss zu, dass dem Beweis der Absicht, das Dokument zu signieren, eine bedeutende Rolle zukommt, wenn bestritten wird, dass ein Dokument oder eine Mitteilung signiert wurde.[1441] Anders als eine handschriftliche Unterschrift verändert eine elektronische Signatur nicht notwendig den Dokumententräger. Die mit dem Träger verbundene Information sind auch Metadaten, also Daten über Struktur und Inhalt ihrer Quelle. In Bezug auf papierne Dokumente sind dies zum Beispiel Informationen wie dessen Titel, das Datum, Informationen über Erklärenden und Empfänger oder implizite Metadaten wie die verwendeten Schrifttypen, besondere Markierungen und Bezeichnungen, zum Beispiel als vertraulich. Bezüglich digitaler Daten müssen diese impliziten Metadaten erst erkennbar gemacht werden, um bei der Interpretation des Zweckes des Dokuments zu helfen. Diese Daten können der Software entnommen werden. Digitale Aufzeichnungen enthalten daher normalerweise zwei wesentliche Arten von Information: den Inhalt des Dokuments und dessen interne Struktur sowie die Metadaten, die die Aufzeichnung und jede ihrer Bestandteile beschreiben.[1442] Unterschieden werden kann auch in Daten, die eine Person am Computer erstellt, beispielsweise den Inhalt eines eine Textdokuments, und solchen, die der Computer automatisch generiert, wie die beschriebenen Metadaten, bei E-Mail und Internetkommunikation auch Log-in-Daten der Internet Service Provider oder sonstige Verbindungsdaten. Bezüglich ersteren kann beispielsweise in den USA die Frage der Anwendbarkeit der Hearsay Rule aufkommen. Bei vom Computer generierten Daten ist die Fra-

[1439] Deutsch, JurPC Web-Dok. 1888/2000, Abs. 51.

[1440] Siehe Ausführungen oben 3.2.2.4.

[1441] Mason, *Electronic Signatures in Law*, S. 275.

[1442] Siehe auch oben zum Darstellungsproblem unter 3.2.1.4.

ge der Authentizität von besonderer Bedeutung.[1443] Änderungen der Metadaten eines digital gespeicherten Originaldokuments werden zum Beispiel hervorgerufen, wenn dieses geöffnet, gelöscht oder sein Inhalt verändert oder neu geschrieben wird. Diese Metadaten werden dann zu einem entscheidenden Mittel der Nachforschung.[1444]

3.3.5.2 Technische Beweise bei E-Mails

Die Bedeutung der Metadaten als Beweismittel wird dort deutlich, wo es darum geht, die Eigenschaft der E-Mail-Adresse als Signatur der E-Mail zu bewerten. Als Argument für diese Beurteilung kann angeführt werden, dass die E-Mail ein einheitliches Dokument ist und die E-Mail-Adresse als Signatur gerade nicht vom übrigen Text des Dokuments getrennt ist. Die in der Absender-, Adress- und Betreffzeile enthaltene Signatur kann nicht vom übrigen Dokumentenkörper getrennt werden. Diese Informationen sind auch weder bei der Darstellung der E-Mail auf dem Bildschirm noch beim Ausdruck der E-Mail von ihrem Text oder Inhalt getrennt.[1445] Hiergegen wird zwar eingewandt, dass die bei der Anzeige von E-Mails erkennbaren Absenderdaten völlig willkürlich sein können und daher keine Beweiskraft haben.[1446] Allerdings können zur Prüfung die Daten aus dem sogenannten „Envelope" der E-Mail herangezogen werden. Der üblicherweise verborgene Quellcode (*source code*) stellt einen integralen Bestandteil der E-Mail dar, ebenso alle sonst mit der E-Mail verbundenen Daten wie die Client-Software, die Kommunikationskette über die Server oder andere technische Informationen. Diese Metadaten können als technischer Beleg zumindest als Indiz von gewissem Wert bei der Beweisführung sein und eine Verbindung schaffen zur Person des Erklärenden beziehungsweise Ausstellers.[1447] So können beispielsweise auf dem Empfängerserver aufgrund der Kommunikations-Metadaten bestimmte Überprüfungen vorgenommen werden, wie der Vergleich des vom Senderserver übermittelten Namens und der vom Empfängerserver registrierten IP-Adresse, die Überprüfung der Existenz der E-Mail-Adresse des Absenders auf dem Senderserver, oder die Abfrage von Datensätzen für die Identifikation des berechtigten Senderservers für eine bestimmte E-Mail-Adresse.[1448] Für stark strukturierte Dateien wie das Postfach von Microsoft Outlook wird angenommen, dass ihnen, da sie kaum manipulierbar seien, eine recht hohe Beweiskraft zukomme, währenddessen andere E-Mail-Programme, bei denen reine Textdateien verwendet würden, auf einfachste Weise manipuliert werden könnten.[1449]

[1443] Flamm/Solomon, „Admissibility of Digital Exhibits in Litigation", DOAR Litigation Consulting, 2004.

[1444] Mason, *Electronic Signatures in Law*, S. 276; Bohm, DEJ 2006, S. 45.

[1445] Mason, *Electronic Signatures in Law*, S. 314, 315.

[1446] Siehe die bereits dargestellte deutsche Rechtsprechung; Schmidt/Pruß/Kast, „Technische und juristische Aspekte zur Authentizität elektronischer Kommunikation", CR 2008, S. 267-272, S. 269, mit ausführlicher Darstellung zur Erhebung technischer Beweise bei E-Mails

[1447] Mason, *Electronic Signatures in Law*, S. 314, 315; Schmidt/Pruß/Kast, CR 2008, S. 269.

[1448] Schmidt/Pruß/Kast, CR 2008, S. 268.

[1449] Schmidt/Pruß/Kast, CR 2008, S. 269 m.w.N.

Diese technischen Aspekte sind in den benannten Urteilen deutscher Gerichte zur Beweiskraft elektronischer Dokumente und Signaturen nicht berücksichtigt worden, wiewohl auch deutlich wird, dass solche Daten nicht als Beweis angeboten wurden. Dennoch bleibt bemerkenswert, wie sehr im Vergleich die englischen und US-amerikanischen Gerichte auch auf Indizien, also auf die Gesamtheit der Umstände und die vorliegenden, auch technischen Beweise für den Willen der Parteien, das jeweilige elektronische Dokument zu authentifizieren, abstellen.[1450] Dies gilt gerade auch für die Kommunikation über das Internet, deren Ausformungen nicht per se jegliche Beweiskraft abgesprochen wird allein mit dem Hinweis auf die Unsicherheit dieser Kommunikationsmethode. Ein Grund hierfür wird sein, dass Indizien und ergänzende Beweise vielfach für die Prüfung der Beweiszulassung und die *authentication* herangezogen werden müssen, soweit das elektronische Dokument nicht *self-authenticated* ist.[1451] Dennoch wird auch hier anerkannt, dass E-Mails – zumal vielfach informell und ohne weit reichende Reflexion verfasst – das Recht dabei vor Herausforderungen stellen, die bei herkömmlichen Briefen mit formellem Briefkopf, Gliederung und Unterschriftsfeld nicht bestanden.[1452] Interessant ist, dass sich die Gerichte dabei auf frühere Urteile berufen können, die ebenfalls die Reaktion des Rechts auf neue Technologien zum Gegenstand hatten. In den dargestellten Fällen etwa zu Telegrammen, Telex und Fax fehlen Hinweise auf die mangelnde Sicherheit und Verlässlichkeit der Kommunikationsform. Dies mag in der tatsächlich höheren Verlässlichkeit dieser Kommunikationsmittel aufgrund einer gewissen Geschlossenheit ihrer Systeme begründet liegen. Im US-Fall *People v. Hagan* wurde die Urheberschaft eines Fax über folgende Indizien hinsichtlich der Authentifizierung zur Überzeugung des Gerichts nachgewiesen: Der übliche Ablauf der Versendung von Faxmitteilungen wurde mittels Zeugenbeweis dargestellt; es stand fest, dass das Absendergerät ohne Fehlermeldung funktioniert hatte, der Empfänger hatte das Fax erhalten und zudem ein Fax diesen Inhalts vom Versender erwartet und letzterer hatte nicht geltend gemacht, dass die Übermittlung fehlerhaft gewesen sei.[1453] In Deutschland wurde die Aussagekraft eines Fax-Sendeprotokolls diskutiert. Diesem sollte laut OLG München die Kraft eines Anscheinsbeweises zukommen, da es wegen der sehr hohen Übertragungssicherheit als typischer Geschehensablauf anzusehen sei, dass Daten eines Telefax, dessen Absendung feststeht und dessen Übertragung im Sendeprotokoll mit dem "OK"-Vermerk bestätigt ist, beim Empfänger auch angekommen sind. Auch hier war die Absendung durch Zeugen bewiesen.[1454] Die hinreichende Sicherheit bei der Übertragung wurde von BGH und Bundesarbeitsgericht jedoch bezweifelt, ein

[1450] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 380, zum *circumstantial evidence*.

[1451] Siehe dazu oben 1.3.2.5 und vor allem 1.3.3.5.

[1452] O'Donnell/Lincoln, „Authenticating E-Mail Discovery as Evidence", The Legal Intelligencer, August 13, 2007, www.law.com/jsp/legaltechnology/PubArticleFriendly LT.jsp?id=1186736525985.

[1453] *People v. Hagan*, 583 N.E.2d, 494 (Ill. 1991) (Illinois), bei Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 406, 407.

[1454] OLG München, Beschl. v. 08.10.98, 15 W 2631/98, JurPC Web-Dok. 153/1999, Abs. 1-16, Abs. 10, 12; a.A. BGH, Urt. v. 07.12.1994, VIII ZR 153/93 , NJW 1995, 665, und Bundesarbeitsgericht (BAG), Urt. v. 14.08.2002, 5 AZR 169/01. Lexetius.com/2002,1919 [2002/11/166]; siehe auch unten 3.3.10.3.

Anscheinsbeweis deswegen abgelehnt.[1455] *Borges* nennt einen Fall in den USA, in dem jemand unter dem Namen und dem E-Mail-Konto eines Mitarbeiters eine E-Mail verschickte und dennoch als Urheberin ermittelt wurde. Entscheidend war, dass der angebliche Versender, unter dessen Namen die E-Mail verschickt worden war, zum fraglichen Zeitpunkt nachgewiesenermaßen keinen Zugang zu seinem Konto hatte und mittels Log-Dateien der Server nachgewiesen werden konnte, dass die wahre Urheberin die E-Mail von ihrem heimischen Computer versandt hatte.[1456] Neben weiteren spielten also auch Beweise in Form der Metadaten eine Rolle. Erneut wird der Wille englischer und US-amerikanischer Gerichte deutlich, ergänzende Beweise und Indizien heranzuziehen beziehungsweise zuzulassen, um die Echtheit eines Dokuments oder die Urheberschaft einer Erklärung festzustellen. Dies wird unterstützt durch die Vorgaben von UETA und UCITA hinsichtlich der zu berücksichtigenden Aspekte und Umstände bei der Feststellung der *authentication* einer Erklärung.[1457] Grundsätzlich wäre die Berücksichtigung solcher Aspekte auch durch deutsche Gerichte im Rahmen der freien Beweiswürdigung möglich, sofern sie überhaupt dargelegt und entsprechende technische Beweise vorgelegt werden. Gegebenenfalls ist es hier auch vermehrt an den Gerichten, die Parteien in flexibler Handhabung der Verfahrensgrundsätze auf die Möglichkeit entsprechender Beweisvorträge hinzuweisen.

3.3.5.3 Kosten-Nutzen-Relation

Der volle Beweis der Urheberschaft elektronischer Dokumente ist unter Umständen sehr aufwändig, vielfach nicht mit wirtschaftlich sinnvollem Aufwand möglich, zumal wenn die Urheberschaft substantiiert bestritten wird. Eine solche Beweisführung mit Metadaten etc. setzte bei E-Mail-Dokumenten zunächst voraus, dass entsprechende Protokollinformationen der Mail-Server erhoben wurden, diese aussagekräftig, bekannt, noch vorhanden und verfügbar sind. Nicht alle Server erheben aber die für eine solche Beweisführung notwendigen Informationen. Zudem besteht, zumindest in Deutschland, kein Herausgabeanspruch solcher Informationen gegen den Mail-Server-Betreiber.[1458] Eine Beweisführung bezüglich elektronischer Dateien, insbesondere der vom Computer automatisch generierten Daten, wird auch die Darlegung des einwandfreien Funktionierens des Geräts einschließen müssen.[1459] Das Darstellungsproblem hat ebenfalls Auswirkungen auf den Aufwand der Beweisführung – insbesondere bei verschlüsselten Da-

[1455] Die Datenübertragung könne an Defekten am Empfangsgerät, z.B. einem Papierstau, oder an Leitungsstörungen oder -verzerrungen, die zum Abbruch der Verbindung führten, gescheitert sein, ohne daß die Unterbrechung und mißglückte Datenübermittlung im Sendebericht ausgewiesen werde, BGH, NJW 1995, S. 666, 667. Ebenso BAG, Urt. v. 14.08.2002, 5 AZR 169/01.

[1456] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 406 m.w.N. Siehe auch grundsätzlich zu elektronischen Beweismitteln Willer/Hoppen, „Computerforensik – Technische Möglichkeiten und Grenzen“, CR 2007, S. 610-616.

[1457] Siehe oben unter 2.5.2.4 und 2.5.4.2.

[1458] Roßnagel/ Pfitzmann, NJW 2003, S. 1209-1214, S. 1210.

[1459] Flamm/Solomon, „Admissibility of Digital Exhibits in Litigation”, DOAR Litigation Consulting, 2004.

teien. Die Frage der korrekten Darstellung einer Datei und die Frage nach dem Zeitpunkt und Ort ihrer Generierung kann nur vom Sachverständigen zuverlässig beantwortet werden. Denn auch wenn der Beweis anhand der Spuren der Bearbeitung und Übermittlung einer Datei an der Datei selbst oder deren Hard- oder Softwareumgebung technisch möglich ist, darf ein Gericht – wie *Ulmer* richtig anmerkt – dies nicht, da es Schlüsse auf Tatsachen aus den dargestellten oder in Augenschein genommenen Phänomenen zöge, die auf der Grundlage technischer Lehren beruhen. Kein Gericht besitzt hier eigene Sachkunde oder könnte diese den Erfordernissen des § 286 ZPO entsprechend darlegen. Es bedarf also immer eines Sachverständigen. *Ulmer* dazu:

> *„Prozesse unter Verwendung elektronischer Dokumente werden lange dauern und teuer werden."*[1460]

Nicht in allen Fällen, in denen das Vorliegen einer Unterschrift oder die Identität des Versenders streitig ist, werden sich ein solch hoher Aufwand und die damit verbundenen Kostenrisiken bei der Beweisführung vor Gericht lohnen. Dieser Aufwand ist erkennbar größer als beim Urkundsbeweis, für den die Vorlage des entsprechenden Dokuments (im Original oder als Kopie) genügt. Für einen überzeugenden Beweisantritt mit elektronischen Dokumenten ist es zunächst notwendig sicherzustellen, dass die Daten jederzeit und auf längere Zeit lesbar gemacht werden können und dass elektronisch gespeicherte Dokumente während des gesamten Bearbeitungsvorgangs nicht verwechselt oder verfälscht werden können. Dies kann über ein Dokumentenverwaltungssystem erfolgen[1461], was jedoch zumindest bei Privaten kaum Anwendung finden wird. Dieser Kosten-Nutzen-Aspekt gilt seinem Grundsatz nach gleichermaßen in allen vorgestellten Rechtsordnungen und wird vielfach ein Hemmnis für die erfolgreiche Beweisführung und Rechtsdurchsetzung darstellen.

3.3.6. Unsicherheit elektronischer Dokumente

Im oben genannten Fall *On Line Power Technologies, Inc., v. Square D. Company*[1462] wurde neben der Anerkennung der elektronischen Signaturen unter dem Statute of Frauds festgehalten, dass der Austausch von E-Mails ausreichenden Beweis für die Absicht der Parteien bot, eine Vereinbarung abzuschließen. Da das *writing* und *signing* nach dem Statute of Frauds gerade auch den Zweck der Schaffung eines hinreichenden Beweises hat, ist dies eine bemerkenswerte Äußerung im Vergleich zu den Entscheidungen deutscher Gerichte in ähnlichen Fällen. Diese Beurteilung scheint dem allge-

[1460] Ulmer, CR 2002, S. 212, der zutreffend darauf hinweist, dass dies noch problematischer wird bzgl. Zugang oder Verfügbarkeit der Datei im Sinne des § 312e Abs. 1 S. 1 Nr. 4 und S. 2 BGB bei einer der Parteien, insbesondere, wenn computergenerierte und -übermittelte Dokumente in Rede stehen, die tatsächlich von keinem Menschen wahrgenommen würden.

[1461] Vehslage, Thorsten, „Beweiswert elektronischer Dokumente", K&R 2002, S. 531-533, S. 532, 533.

[1462] *On Line Power Technologies, Inc., v. Square D. Company*, 2004 WL 1171405 (S.D.N.Y.), siehe oben 2.5.6.

meinen Einwand der mangelnden Sicherheit und Verlässlichkeit elektronischer Kommunikation entgegenzustehen.

3.3.6.1 Manipulierbarkeit elektronischer Dokumente

Als Argument gegen die Beweiskraft elektronischer Dokumente, die nicht mit einer digitalen Signatur versehen sind, wird deren leichte Fälschbarkeit angeführt. Genannt werden deren nicht vorhandene stoffliche Fixierung sowie insbesondere die Manipulationsmöglichkeiten zum Beispiel mittels Trojanischer Pferde oder nachträglichem Editieren und Verändern des Dokuments. Das AG Bonn führte entsprechend in einem Fall, in dem E-Mail-Ausdrucke als Beweis für das Bestehen einer Vereinbarung vorgelegt wurden, aus:

> *„Auch die vom Kläger vorgelegten E-Mails vermögen eine solche Behauptung nicht zu beweisen. ... vermag auch die Vorlage von E-Mail-Ausdrucken allein noch keinen hinreichenden Ausdruck für einen Beweis zu erbringen. Es ist allgemein bekannt, dass E-Mail-Dateien manipulierbar sind. Selbst wenn die entsprechenden E-Mails grundsätzlich vom Beklagten abgesandt worden sein sollten, wäre es möglich, dass einzelne Worte oder einzelne Sätze dieser E-Mails von Dritten abgeändert worden sind. Soweit kann diesen ... vorgelegten E-Mail-Ausdrucken keinerlei Beweiswert beigemessen werden.“*[1463]

Auch hier hätte es also weiterer Beweise zur Untermauerung des Klägervortrags sowie deren Beachtung durch das Gericht bedurft. Gegen das Argument der fehlenden oder ungenügenden Beweiskraft elektronischer Kommunikation aufgrund deren leichten Fälschbarkeit sind aber auch grundsätzliche Bedenken angebracht. Dies belegt schon der Vergleich mit herkömmlichen Formen der Schriftlichkeit und den dafür verwendeten Materialien. In der englischen Literatur wird die Prämisse – zumindest für das *common law* – angezweifelt, in elektronischer Form gespeicherte Informationen seien weniger sicher als Informationen, die auf papiernen Dokumenten aufbewahrt werden. Diese Prämisse übersehe, dass Papier, wie auch magnetische und optische Medien, bis zur Unbrauchbarkeit verfallen und zerstört oder gestohlen werden können. Dagegen erlaube die elektronische Speicherung (sogar) die Aufbewahrung unzähliger Kopien dieser Informationen.[1464] Unter ausdrücklichem Hinweis auf die deutsche Rechtsprechung hierzu[1465] kritisiert auch *Mason* dieses Argument als fehlgehend. Jedes papierne Dokument könne gefälscht werden. Die Tatsache der Fälschung von Beweisen sei nicht neu. Würde das Argument der leichten Fälschbarkeit durch die Gerichte akzeptiert, wie dies in den dargestellten deutschen Fällen der Fall ist, so müsse logisch jedes urkundliche Be-

[1463] AG Bonn, Urt. v. 25.10.2001, 3 C 193/01, NJW-RR 2002, S. 1363; so auch Ernst, Stefan, „Beweisprobleme bei E-Mail und anderen Online-Willenserklärungen“, MDR 2003, S. 1091-1094, S. 1092.

[1464] Griffiths/Harrison in Campbell, *E-Commerce and the Law of Digital Signatures*, S. 653.

[1465] Hier benannt AG Bonn, NJW-RR 2002, S. 1363, siehe oben.

weisstück ausgeschlossen werden, da es manipulierbar sei. Tatsächlich aber müsse die Frage, ob ein Beweisstück tatsächlich gefälscht sei, vor Gericht geklärt werden und der auf diesen Beweis vertrauenden Partei im Zweifel die Möglichkeit gegeben werden, ergänzende Beweise vorzulegen, um die Echtheit des Dokuments zu belegen.[1466] Dem ist zuzustimmen. *Mason* folgert daraus, dass wegen der grundsätzlichen Fälschbarkeit auch papierner Dokumente die Juristen regelmäßig die vorliegenden Urkundenbeweise (*documentary evidence*) *„durchsieben"* müssten, um die Echtheit der Dokumente zu überprüfen.[1467]

Diese Überlegungen lassen sich auf die deutsche Diskussion um die Beweiskraft elektronischer Dokumente übertragen. Allerdings legt die Rechtsprechung in Deutschland den Schluss nahe, dass es gerade dazu vielfach mit dem Hinweis auf die mangelnde Beweiskraft elektronischer Kommunikation nicht kommen wird. Vielmehr sind elektronische Dokumente als Beweis nur dann unproblematisch, wenn sie unbestritten sind. Diese Überlegungen zeigen aber auch, dass man es sich mit der schlichten Gleichsetzung elektronischer Dokumente mit leichter Fälschbarkeit und Unsicherheit und der damit verbundenen Diskriminierung gegenüber papiernen Dokumenten zu einfach macht. Um den tatsächlichen, die Echtheit eines elektronischen (oder papiernen) Dokuments ausmachenden Tatsachen gerecht zu werden, muss dem Grundsatz nach eine unvoreingenommene Einzelfallprüfung erfolgen. Ob bei dieser Prüfung von der beweisbelasteten Partei der entsprechende Beweis erbracht werden kann, oder ob dabei Beweiskraftregeln eingreifen, ist eine andere Frage. Neben der ferner in jedem Einzelfall entscheidenden Frage, ob neben den elektronischen Beweisen wie E-Mails etc. auch andere Beweise überhaupt vorliegen, bleibt zu fragen, ob diese von der deutschen Rechtsprechung aufgestellte Hürde auch anderweitig überwunden werden kann.

3.3.6.2 Die Bedeutung des *writing material* nach englischem und US-amerikanischem Recht

Hier lassen sich zum Vergleich Fälle aus den *case law* in England und den USA anführen, in denen es um die Rechtswirksamkeit von Unterschriften ging, die in einer Art vorgenommen wurden, die eine leichte Fälschung erlaubten. In den englischen Fällen *Geary v. Physic*[1468] und in *Lucas v. James*[1469] wurden Unterschriften beziehungsweise Ergänzungen auf Vertragsdokumenten mit einem Bleistift anstatt mit Tinte aufgebracht. Die Frage war, ob dieses Schreibmaterial, das im Gegensatz zur Tinte vom entsprechenden Dokument wieder entfernt werden kann, eine wirksame Unterschrift herbeifüh-

[1466] Mason, *Electronic Signatures in Law*, S. 110; auch Schapper/Rivolta/Veiga Malta, DEJ 2006, S. 11, die anführen, dass eine Unterschrift traditionell nicht den Gedanken der Sicherheit fördern sollte (*„However, from a traditional legal perspective, a signature has never meant to convey notions of security; ..."*), sondern die Idee der Zustimmung, auch wenn eine mit Tinte handgeschriebene Unterschrift einen größeren Beweiswert habe. So auch O'Donnell/Lincoln, The Legal Intelligencer, August 13, 2007 mit Verweis auf einen entsprechenden Ausspruch des Pennsylvania Superior Court.

[1467] Mason, *Electronic Signatures in Law*, S. 110.

[1468] *Geary v. Physic* (1826) 5 B & C 234; 108 ER 87.

[1469] *Lucas v. James* (1849) 7 Hare 410; 68 ER 170.

ren kann und als Beweis taugt beziehungsweise zugelassen werden kann. Dies wurde bejaht:

> *„Es gibt keine* [*authority*, Präzedenzfälle]*, die dort, wo das Recht die schriftliche Form eines Vertrages verlangt, das Schreiben mit Tinte fordern.“*[1470]

Daraus wird gefolgert, die Art des Schreibmaterials sei irrelevant, solange es nicht vom Dokument entfernt würde und die Unterschrift beziehungsweise der Vertragstext mit Rechtsbindungswillen aufgebracht wurde.[1471] Auch in den USA wurde der Gebrauch von Bleistiften in einer Vielzahl von Fällen akzeptiert.[1472] In *Kleine v. Kleine* bestand eine Partei einer Vereinbarung über eine Grundstücksübertragung darauf, das entsprechende *deed* mit Bleistift zu unterschreiben, weil sie davon ausging, eine solche Unterschrift wäre unwirksam. Das Gericht kommentierte dies als

> *„… falsche, von vielen Laien vertretene Ansicht, dass ein* [deed] *mit Füllfederhalter und Tinte unterschrieben werden muss.“*[1473]

Hingegen wurde in *United States v. Thompson*[1474] die Unterschrift mit einem Bleistift auf einem Urteil als unwirksam erklärt, da diese so leicht auszuradieren sei und damit die Urkunde angreifbar mache. Hinter dieser auch in Bezug auf elektronische Dokumente und Signaturen verwendete Begründung steht folgende Logik: Für die Unterschrift wurde ein Material verwendet, das ausradierbar beziehungsweise löschbar ist. Folglich ist die Unterschrift nicht wirksam, da sie gelöscht werden kann. Diese Ansicht wird als auf einer fehlerhaften Prämisse basierende falsche Schlussfolgerung kritisiert. Denn die bloße Möglichkeit der Löschung verhindere nicht, dass das Dokument unterschrieben worden ist.[1475] Diese Argumentation ist schlüssig. Was bleibt ist die Frage, wie dann die Unterzeichnung oder die dadurch zum Ausdruck gebrachte Authentizität und damit Echtheit bewiesen werden können. So ist auch hier wieder die Bedeutung der weiteren Umstände und ergänzender Beweise zu unterstreichen. Im genannten Fall lag dem Gericht die mittels Bleistift aufgebrachte handschriftliche Unterschrift vor, so dass der Beweis darüber als gegeben angenommen wurde. Wäre die Unterschrift ausradiert und das Vorliegen einer wirksamen Unterschrift dann angezweifelt (*tested*) worden, so

---

[1470] Lord Abbott in *Geary v. Physic* (1826) 5 B & C 234; 108 ER 87, S. 237: *„There is no authority for saying that where the law requires a contract to be in writing that writing must be in ink.“*

[1471] Mason, *Electronic Signatures in Law*, S. 108.

[1472] *Brown v. The Butchers & Drovers' Bank*, 6 Hill 443, 41Am.Dec. 755 (New York, Abzeichnung (*endorsement*) einer *bill of exchange*); *Clossen v. Stearns*, 4 Vt. 11, 1831 WL 2104 (Vt.), 23 Am.Dec. 245 (Vermont, Abzeichnung einer *promissory note*); *Great Western Printing Co., v. Belcher*, 127 Mo.App. 133, 104 S.W. 894 (Missouri, Ergänzung auf einer Originalrechnung); *Merritt v. Clason, 12 Johns*. 102, 7 Am.Dec. 286, 1 N.Y.S.C. 1814-15 92 *affirmed as The Executors of Clason v. Bailey*, 14 Johns. 484 (New York, *memorandum* eines Vertrages in einem Notizbuch); Appeal of Knox, 131 P. 220, 18 A. 1021, 6 L.R.A. 353, 17 Am.St.Rep. 798 (Pennsylvania, Testamentsurkunde).

[1473] *Kleine v. Kleine* 219 S.W. 610, 281 Mo. 317: *„… erroneous view, entertained by many laymen, that a deed must be signed with pen and ink.“*

[1474] *United States v. Thompson* 2 Cranch C.C. 409, 28 F.Cas. 89, 2 D.C. 409, No. 16484.

[1475] Mason, *Electronic Signatures in Law*, S. 110.

wäre es für die Echtheit des Dokuments auf von den weiteren vorliegend Beweisen und ihrer Überzeugungskraft angekommen.[1476]

3.3.7 Unsicherheit elektronischer Kommunikation

Neben den oben genannten Aspekten der mangelnden Verkörperung und der Möglichkeit der Manipulation von elektronischen Dokumenten wird vor allem deren Versendung auf elektronischem Weg als Argument für deren mangelnde Beweiskraft angeführt. Dies trifft insbesondere die Versendung solcher elektronischen Dokumente und E-Mails über das Internet. Diese Versendung erfolgt zumeist über Simple Mail Transfer Protocol (SMTP) und vielfach sogar ohne Passwortschutz. Dies sowie deren Weg über das Internet über Routerrechner und die bereits erwähnten Manipulationsmöglichkeiten durch Trojaner führe dazu, dass diese elektronische Kommunikation unsicher und damit ohne Beweiswert sei. Diese Bedenken werden allgemein dem elektronischen Vertragsschluss über das Internet, auch über Plattformen wie Internetauktionen, entgegengebracht. Bisher noch nicht von der Rechtsprechung behandelt ist der Umstand, dass auch E-Mails mittlerweile häufig aktiven, das heißt einen auch nach Zugang der E-Mail veränderbaren HTML-Inhalt haben wie Websites.[1477]

3.3.7.1 Manipulation und Maskeradeangriffe Dritter

Als Dritteingriffe in die elektronische Kommunikation kommen das Abfangen, Verändern und Manipulieren von Erklärungen, insbesondere E-Mails durch einen Dritten in Betracht. Hierzu müsste sich der Dritte Zugang zu den relevanten Router-Servern verschaffen und die ihn interessierenden Nachrichten herausfiltern.[1478] Hier wird zutreffen angemerkt, dass diese Gefahr der unberechtigten Fälschung, des Abfangens, Kopierens und Manipulierens auch bei der Kommunikation auf anderem Weg besteht und nicht typisch ist für die elektronische Kommunikation.[1479] Eine andere Möglichkeit sind sogenannte Maskerade-Angriffe, bei denen in die Konfiguration des E-Mail-Programms auf dem Ausgangsrechner durch den Dritten die „falsche“ Absenderadresse eingefügt und das Wegeprotokoll der SMTP-Server manipuliert werden müssen.[1480] Wie geschildert haben deutsche Gerichte unter dem nicht weiter ausgeführten Hinweis auch auf diese Gefahren E-Mail-Dateien und Ausdrucken von E-Mail-Dateien jegliche Beweiskraft abgesprochen.[1481]

[1476] So auch Mason, *Electronic Signatures in Law*, S. 110.

[1477] Stadler, JurPC Web-Dok. 136/2006, Abs. 10.

[1478] Mankowski, NJW 2002, S. 2823.

[1479] Mason, *Electronic Signatures in Law*, S. 332, siehe auch oben 3.3.6.1.

[1480] Mankowski, NJW 2002, S. 2823. Spam-Mails stellten kein Problem dar, da entweder die angegebene E-Mail-Adresse überhaupt nicht existiere, oder der Inhaber der angegebenen tatsächlich existierenden E-Mail-Adresse könne nachweisen, dass die E-Mail nicht von ihm stamme. Bei sog. Spoof-Mails ohne Absenderangabe komme es ebenfalls nicht zu einer Fehlzuordnung.

[1481] Z.B. AG Bonn, NJW-RR 2002, S. 1363.

3.3.7.2 Nochmals: Das Passwortproblem

Auf das grundsätzliche Problem bei der Auswahl von Passwörtern durch den Nutzer und die damit einhergehende erhöhte Wahrscheinlichkeit, diese erraten zu können, sowie auf die Gefahr der Weitergabe von Passwörtern etc. wurde oben bereits eingegangen.[1482] Diese Aspekte spielen auch bei der Beurteilung des Passwortschutzes für den Zugang zu E-Mail-Konten oder Internetplattformen wie Internetauktionen eine Rolle. Dabei ist zu unterscheiden zwischen Passwörtern für den Zugang zum Mail-Konto, die keinerlei Schutz gegen Maskeradeangriffe bieten, weil der Angreifer für Manipulationen gar nicht auf den Zugriff auf das echte E-Mail-Konto angewiesen ist, und solchen, die den unmittelbaren Zugang zu Plattformen wie Internetauktionen ermöglichen.[1483] Dennoch, so *Mankowskis* optimistische Beurteilung, vereinten Passworte ein akzeptables Kostenniveau, leichte Begreifbarkeit, einfaches Handling und einen hinreichenden Sicherheitsgrad bei geringen Implementierungs- und Pflegekosten. Andere Lösungen, die größeren Schutz vermittelten, seien komplizierter, weniger gut für Laien handhabbar und im Zweifel teurer.[1484] Doch täuschen auch diese Aspekte nicht über grundlegende Probleme des Passwortschutzes hinweg. Schließlich ist ein Passwortsystem nur so gut wie die vorangegangene Identifizierung des Nutzers[1485] und kann, wird es online ohne weitere Identitätsprüfung vergeben, tatsächlich kein Legitimationsmittel darstellen.[1486] Deutsche Gerichte haben entschieden, dass auch ein mittels Passwortschutz geschütztes E-Mail-Konto oder der Passwortschutz einer Internetplattform nicht als taugliche Beweise beziehungsweise ausreichendes Indiz für die Identität des Versenders der E-Mail gelten können. Sofern ihm das Passwort bekannt ist, könne jedermann unter Verwendung der E-Mail-Adresse zum Beispiel an der Internetauktion im Namen des Inhabers des E-Mail-Kontos teilnehmen. Aus dem Begriff des Passwortes ergebe sich zwar,

> *„dass es durch den Verwender nicht weitergegeben werden soll, welche Sicherheitskriterien einzuhalten sind, ist jedoch nicht festgelegt.“*[1487]

In diesem Fall waren dem Gericht irgendwelche Sicherheitshinweise nicht bekannt. Tatsächlich wurden und werden auch immer wieder Schwachstellen des Schutzes von Passwörtern bei Systembetreibern bekannt.[1488] Zutreffend hat das LG Erfurt zudem darauf hingewiesen, dass es bei vielen E-Mail-Diensteanbietern in der Benutzermaske eine Voreinstellung gebe, in der der Verwender das Passwort, auch wenn es nicht lesbar ist,

---

[1482] Siehe 3.2.1.2.

[1483] Ernst, MDR 2003, S. 1093.

[1484] Mankowski, Anmerkung zu LG Aachen, Urt. v. 15.12.2006 – 5 S 184/06 – „Handeln in fremden Namen bei Online-Auktion“, CR 2007, S. 606-607, S. 607.

[1485] Roßnagel/Pfitzmann, NJW 2003, S. 1211; siehe auch eingangs unter 1.4.2.1, 1.4.2.3.

[1486] Wiebe, „Anmerkung zu AG Erfurt, Urt. v. 14.09.2001 – 28 C 2354/01 – Nachweis der Authentizität bei Internetauktionen“, MMR 2002, S. 128-129, S. 129.

[1487] AG Erfurt, JurPC Web-Dok. 71/2002.

[1488] Roßnagel/Pfitzmann, NJW 2003, S. 1211.

automatisch vermerken könne.[1489] Laut AG Erfurt sei die Legitimationsprüfung im Internet per Passwort auch nicht zu vergleichen mit der Verwendung einer EC-Karte, da dort der Vorgang nicht nur durch das bloße Wissen der Geheimzahl (des Passworts) sondern nur im Zusammenspiel von Geheimzahl und EC-Karte (Besitz und Wissen) ausgelöst werden kann und darüber hinaus die Kommunikation direkt mit dem Endgerät stattfinde, nicht über eine offenes und damit unsicheres Kommunikationsmedium wie das Internet.[1490] Zur Gefahr des Hackens und Phishings führt das Gericht weiter aus:

> *„Aus verschiedenen Publikationen ist dem Gericht zudem bekannt, dass es häufig für Dritte leicht ist, selbst gewählte Passwörter herauszubekommen. ... Bei dem Passwort handelt es sich um ein ständig verwendetes Legitimationsmerkmal, das durchaus von Dritten beziehungsweise Hackern abgelesen werden kann.“*[1491]

Dies betreffe auch existierende Standards, etwa für TAN-Nummern, die ebenfalls durch Dritte ausspioniert werden könnten.[1492] Weitere Ausführungen etwa zur Wahrscheinlichkeit solcher Angriffe fehlen jedoch. Mit der sich in der Folge stellenden Frage der Wahrscheinlichkeit eines solchen Angriffs beschäftigt sich die unten folgende Diskussion um einen Anscheinsbeweis bei E-Mails.[1493]

3.3.8 Allgemeine Risikozuweisung

Wie festgestellt genügt derzeit im Gerichtsverfahren die bloße Erwähnung der Möglichkeit einer Manipulation elektronischer Kommunikation, um die Beweiskraft elektronischer Dokumente und Kommunikation zunichte zu machen. Ein substantiiertes Bestreiten des Versendens, des Erhalts oder der Unverfälschtheit einer E-Mail oder einer über eine Website kommunizierten Erklärung ist nicht erforderlich. In Ermangelung anderer, ergänzender Beweise ist derjenige, der die seinen Anspruch stützenden Tatsachen allein auf solche elektronischen Dokumente und Dateien stützen kann, dem Belieben der anderen Partei ausgeliefert. Diese kann, wenn sie sich am Vertrag nicht länger halten lassen will, behaupten, die fraglichen Erklärungen stammten nicht von ihr oder sie habe diese nie erhalten. Wie *Mankowski* es ausdrückt, dürfte sich dann niemand mehr sicher sein *„wirklich ein Geschäft abgeschlossen zu haben.“*[1494] Gleiches gilt für die Verwen-

[1489] AG Erfurt, JurPC Web-Dok. 71/2002.

[1490] AG Erfurt, JurPC Web-Dok. 71/2002; zum Vergleich mit EC-Karten siehe auch nachfolgend unter 3.3.10.3.

[1491] AG Erfurt, JurPC Web-Dok. 71/2002.

[1492] AG Erfurt, JurPC Web-Dok. 71/2002. Für eine Darstellung des Problems bei Online-Banking mit PIN und TAN sowie den dort angenommenen Anscheinsbeweisen siehe Borges, Georg, „Rechtsfragen des Phishing - Ein Überblick“, NJW 2005, S. 3313-3317, und Kind/Werner, „Rechte und Pflichten im Umgang mit PIN und TAN“, CR 2006, S. 353-360.

[1493] 3.3.10, 3.3.10.6.

[1494] Mankowski, „Wie problematisch ist die Identität des Erklärenden bei E-Mails wirklich?”, NJW 2002, S. 2822-2828, S. 2822.

dung elektronischer Erklärungen zur Einhaltung der Textform, bei denen danach der Empfänger ebenfalls leicht Erhalt oder Inhalt der Erklärung beziehungsweise der Erklärende deren Abgabe und Echtheit bestreiten kann. Dann nützte dem Erklärenden die Einhaltung der Form nichts. Tatsächlich haben deutsche Gerichte daraus geschlossen, dass Integrität und Authentizität bei dieser Kommunikationsform generell nicht feststehen. Vor diesem Hintergrund sei

> *„hinzunehmen, dass ein Klageanspruch aus elektronischem Vertragsschluss wohl fast nie zu beweisen ist.“*[1495]

Dieses Risiko habe der BGH mit seiner Grundsatzentscheidung zum Vertragsschluss im Rahmen einer Internetauktion nicht ausschließen wollen.[1496] Hierzu ist anzumerken, dass der BGH den Aspekt der mangelnden Beweiskraft elektronischer Dokumente im benannten Urteil nicht diskutiert hat. Die durch die Verneinung der Beweiskraft elektronischer Kommunikation folgende Risikoverteilung wurde nicht adressiert.[1497] Es lässt sich darüber streiten, ob mit *Mankowski* durch diese Risikoverteilung tatsächlich droht, dass der Rechtsverkehr zum Erliegen gebracht werde.[1498] Dem ist offensichtlich nicht so. Vielmehr ist die Nutzung des Kommunikationsmediums Internet zum Vertrieb und Erwerb von Waren und Dienstleistungen weit verbreitet. Daraus aber zu schließen, die Nutzer würden dabei bewusst den Umstand, ihre Ansprüche mangels Beweisbarkeit nicht durchsetzen zu können, in Kauf nehmen und ihre Geschäfte in Kenntnis dieses Risikos durchführen, kann für die große Mehrheit der vor allem privaten Nutzer wohl nicht angenommen werden. Wahrscheinlich ist sich ein Großteil der Nutzer dieses juristischen Risikos nicht wirklich bewusst. Es ist auch fraglich, ob es den Rechtsverkehr im Internet tatsächlich in seiner Existenz gefährden würde, wüssten alle Beteiligten um dieses Risiko.

Es bleibt aber die Frage, ob die Tatsache, dass letztlich jedes Sicherheits-, hier beispielsweise jedes Passwortsystem überlistet werden kann, dazu führen soll, das gesamte Risiko des elektronischen Geschäftsverkehrs allein dem Adressaten elektronischer Kommunikation aufzuerlegen.[1499] Genau dies hat das OLG Hamm in einer Entscheidung Ende 2006 jedoch erneut bestätigt und angeführt, entsprechende Risiken müsse der Internet-Nutzer, also hier der Verkäufer, einkalkulieren.[1500] Auch das OLG Naumburg hatte zuvor festgestellt, dass der Verkäufer bei der Nutzung einer Internetauktion in Kenntnis der Missbrauchsmöglichkeiten das Risiko eingehe, dass Fälle von Kaufreue

[1495] LG Bonn, CR 2004, S. 218, 219.

[1496] So das LG Bonn, CR 2004, S. 218 unter Verweis auf BGH, Urt. v. 07.11.2001, VIII ZR 13/01, NJW 2002, S. 363.

[1497] Vor allem waren im dort behandelten Fall der Austausch und der Inhalt der gegenständlichen E-Mails nicht bestritten, sondern lagen wirksame Willenserklärungen vor. Vielmehr hatte die Partei, die offenbar an den Vertrag nicht mehr gebunden sein wollte, versucht, ihre Willenserklärung anzufechten. BGH, NJW 2002, S. 364.

[1498] Mankowski, NJW 2002, S. 2824.

[1499] So Ernst, MDR 2003, S. 1093.

[1500] OLG Hamm, Urt. v. 16.11.2006, 28 U 84/06, NJW 2007, S. 611.

auf Seiten des Käufers ohne Folgen bleiben.[1501] Diese Ausführungen vermögen nicht zu überzeugen. Wie *Wiebe* zutreffend ausführt, ginge eine Haftung der Marktplatzbetreiber für die Identität der Teilnehmer bei Internetauktionen und ähnlichen Foren zu weit.[1502] Es mag auch sein, dass ein Großteil der gewerblichen Anbieter von Waren und Dienstleistungen im Internet gelegentliche Verluste durch nach Vertragsschluss unwillig gewordenen Kunden in ihre Kostenrechnungen einbeziehen und so auf alle Kunden verteilen. Diese Tatsache bietet jedoch keine zufrieden stellende Antwort auf die rechtstheoretische Frage, ob das Risiko des Eintritts der mit der elektronischen Kommunikation verbundenen Gefahren einer der Parteien und wenn ja, welcher der Parteien, aufgebürdet werden soll. Hier hilft auch nicht der Hinweis, die Parteien, beispielsweise der Verkäufer, müssten sich darüber im Klaren sein, dass eine solche anonyme Kaufanbahnung nicht die Rechtssicherheit bieten könne, wie das beim Vertragsschluss *„auf herkömmliche Art"* möglich sei.[1503] Nun ist der Handel über das Internet nicht der einzige „anonyme" Weg der Kaufanbahnung und freilich sagt das Gericht nicht, was es unter einer herkömmlichen Art versteht. Diesem Argument kann auch entgegengehalten werden, dass durch das Anlegen des E-Mail-Kontos eine Risikoquelle eröffnet wird, für die der Nutzer eine gewisse Haftung übernimmt, weshalb ihm – so zutreffend *Winter* – im Streitfall mehr abzuverlangen ist als bloß ein pauschaler Hinweis auf die Sicherheitsrisiken des Internets.[1504] Der Käufer sei tatsächlich kein ganz unbeteiligter Dritter, sondern habe aus dem System Nutzen ziehen wollen, weshalb das Missbrauchsrisiko nicht allein dem Verkäufer einseitig zuzuweisen sei.[1505] *Roßnagel* sieht dies dennoch ähnlich wie das OLG Hamm im vorgenannten Urteil und spricht denjenigen Internet-Nutzern, die es versäumen, ihre rechtserheblichen Willenserklärungen mit der digitalen Signatur, hier der qualifizierten oder akkreditierten elektronischen Signatur zu versehen, sogar die Schutzwürdigkeit ab. Für bedeutsame Rechtsgeschäfte oder den Kauf besonders wertvoller Waren etc. stünde eine sichere Alternative bereit, die es in diesen Fällen zu nutzen gelte.[1506] Dem ist entgegen zu halten, dass dies letztlich auf eine Verpflichtung der Vertragsparteien hinausliefe, die qualifizierte oder zumindest die fortgeschrittene elektronische Signatur einzusetzen, die in der gesetzlichen Wertung keine Entsprechung findet. Außer in den gesetzlich geregelten Fällen, in denen etwa die Schriftform des § 126 BGB vorgeschrieben ist und wo diese also nur durch die elektronische Form des § 126a BGB ersetzt werden kann, findet sich eine solche Verpflichtung nicht. Dies zu akzeptieren würfe auch die Schwierigkeit auf, auslegungsfähige und auslegungsbedürftige Begriffe wie „bedeutsam" oder „wertvoll" in Bezug auf die jeweiligen Rechtsgeschäfte,

[1501] OLG Naumburg, Urt. v. 02.02.2004, 9 U 145/03.

[1502] Wiebe, Anmerkung zu AG Erfurt, MMR 2002, S. 129

[1503] LG Magdeburg, Urt. v. 21.10.2003, 6 O 1721/03, K&R 2005, S. 191; bestätigt durch OLG Naumburg, Urt. v. 02.02.2004, 9 U 145/03.

[1504] Winter, „Anmerkungen zum Urteil des AG Erfurt vom 14.09.2001 – 28 C 2354/01", JurPC Web-Dok. 109/2002, Abs. 17.

[1505] Zutreffend ebenfalls Winter, „Anmerkung zu LG Konstanz, Urt v. 19.4.2002 – 2 O 141/01 A – Darlegungs- und Beweislast bei Onlineauktion", MMR 2002, S. 836-837, S. 836.

[1506] Roßnagel, Alexander, „Anmerkung zu OLG Köln vom 06.09.2002", K&R-Kommentar, K&R 2003, S. 84-86, S. 86.

etwa im Sinne einer Wertgrenze, zu bestimmen, um die Grenze zu definieren, an dem der jeweiligen Partei der Schutz des Rechts – mit diesem, lax gesagt, „Selber-schuld"-Argument – verwehrt werden soll. Für die Beurteilung durch das Gericht liefe dies wiederum auf eine Art *reliability test* im Sinne des *„as reliable as appropriate for the purpose"*[1507] hinaus. Vor allem aber geht diese Sicht an der Lebenswirklichkeit insoweit vorbei, als dass sich die Technologie der digitalen Signatur eben nicht in dem Maße und erst recht nicht in den Personenkreisen durchgesetzt hat, die einen Großteil des eben bisweilen auch hochpreisigen (Autokauf etc.)[1508] elektronischen Geschäftsverkehrs bestreiten. Auch für Fälle der heute so üblich gewordenen Internetauktion die Verwendung der digitalen Signatur-Technologie zu verlangen, bedeutete für den elektronischen Geschäftsverkehr letztlich eine wohl größere Gefahr als das Fortbestehen des hier diskutierten Nachteils bei der Beweisführung des Empfängers.
Eine Alternative wäre, die Beweislast und damit vorgenanntes Risiko dem vermeintlichen Versender der elektronischen Kommunikation aufzubürden. Auch hierzu hat die deutsche Rechtsprechung eine klare Ansicht, siehe zum Beispiel LG Bonn zu Internetplattformen:

> *„Die Mitgliedschaft in einem Internetauktionshaus mit Mitgliedsnamen und Passwort führt nicht zur Überbürdung der Missbrauchsgefahr auf dieses Mitglied."*[1509]

Eine Beweislastumkehr aus Billigkeitsgesichtspunkten wird unter Hinweis auf die dem Vertragsschluss zugrunde liegenden Gefahrenbereiche, nach denen dies nicht geboten sei, abgelehnt.[1510] Dieser Gefahr des unbefugten Eingriffs eines Dritten in die Online-Kommunikation hätten sich beide Parteien gleichermaßen ausgesetzt.[1511] In diesem komplexen System könne allenfalls derjenige einen gewissen Einfluss ausüben, der eine Website im Internet platziert habe. Ihm könnten bestimmte Sorgfaltspflichten zum Beispiel bei der Dokumentationspflicht auferlegt werden und dieser sei es auch, der als „Initiator" des Verkaufs die Vorteile des Internet für seine Zwecke nutzen möchte. Es läge daher sogar näher, ihm das mit der Nutzung des Internet verbundene Risiko aufzuerlegen.[1512] Auch das OLG Hamm und das OLG Naumburg lehnen eine Umkehr der Beweislast gerade deshalb ab, weil der Internet-Verkäufer in Kenntnis der Missbrauchsmöglichkeiten dieses Risiko eingehe und es einkalkuliere.[1513] Diesbezüglich gilt das oben dazu Gesagte.

[1507] Siehe oben 3.3.3.

[1508] So stritten bspw. die Parteien in oben benannter Internetkauf-Entscheidung des BGH, NJW 2002, S. 363 um einen Autokauf im Wert von 26.350,00 EURO.

[1509] LG Bonn, CR 2004, S. 218; bestätigt durch OLG Köln, JurPC Web-Dok. 364/2002; so auch LG Bonn, MMR 2002, S. 255, und LG Magdeburg, K&R 2005, S. 191.

[1510] LG Bonn, MMR 2002, S. 256; OLG Köln, JurPC Web-Dok. 364/2002.

[1511] LG Bonn, MMR 2002, S. 256; OLG Köln, JurPC Web-Dok. 364/2002; LG Bonn, CR 2004, S. 218; LG Köln, Urt. v. 27.10.2005, 8 O 15/05, BeckRS 2006 07259.

[1512] LG Bonn, MMR 2002, S. 256; OLG Köln, JurPC Web-Dok. 364/2002; LG Bonn, CR 2004, S. 218.

[1513] OLG Hamm, NJW 2007, S. 611; OLG Naumburg, Urt. v. 02.02.2004, 9 U 145/03.

Logisch fortgesetzt müssen diese Ansichten auch für über das Internet versandte Erklärungen in Textform gelten. Zu bedenken ist hierbei aber ergänzend, dass es nicht nur zuförderst um das Risiko geht, dass sich die mit der Nutzung des Internet verbundenen Gefahren des unbefugten Dritteingriffs etc. verwirklichen. Vielmehr wird hier dem Empfänger das Risiko aufgebürdet, dass sein Vertragspartner, der nun vertragsunwillig geworden ist, unter Vorschützung einer bloßen Möglichkeit der Verwirklichung dieser Gefahren sich eine Rückzugsmöglichkeit von seinen vertraglichen Verpflichtungen verschafft, ohne hierfür einen der gesetzlich legitimierten Gründe wie beispielsweise einen Anfechtungsgrund wegen Irrtums darlegen und eben auch beweisen zu müssen. Hierin ist auch ein Gegensatz zu gesetzgeberischen Wertungen wie etwa des Anfechtungsrechts zu erblicken.[1514] Dabei geht es also weniger um die Frage, ob dieses Risiko von den Parteien und damit systemimmanent etwa wirtschaftlich aufgefangen wird, sondern darum, ob diese Risikoverteilung wünschenswert ist und wenn nicht, ob und wie dieses unerwünschte Ergebnis abgewendet werden kann.
Im englischen und US-amerikanischen Recht stellt sich aufgrund der dargestellten Sicht und Beurteilung der Gerichte dieses Problem nicht, jedenfalls nicht in dieser Ausprägung. Auch dort wurde in Verfahren – insbesondere in Strafverfahren – vielfach auf den Umstand, dass Computerdaten verändert worden sein könnten hingewiesen. Die Gerichte haben aber auf nicht näher gestützte Behauptungen des Dritteingriffs mit einiger Skepsis reagiert. Ohne spezifische Beweise für eine Änderung oder Manipulation berührt danach die bloße Möglichkeit der Manipulation die Echtheit einer Computerdatei nicht.[1515] Aus *United States v. Bonallo*:

> *"Die Tatsache, dass es möglich ist, in einem Computer enthaltene Daten zu verändern, ist völlig unzureichend, um Unzuverlässigkeit zu begründen."*[1516]

Ohne besondere Beweise der Manipulation gingen Vermutungen der Veränderung von Computer-Daten zu Lasten deren Beweiswerts (*weight*), nicht zu Lasten deren Zulassung (*admissibility*) als Beweis.[1517] Hier erbringen grundsätzlich Indizien den Beweis für Urheberschaft und Echtheit einer Computerdatei.[1518] Dieser Beweis auch für einen möglichen Dritteingriff muss also von der Partei, die sich darauf stützt, vorgebracht werden. Dies ist dem Grundsatz nach auch gemäß deutschem Zivilprozessrecht von ihr zu verlangen, wie unten[1519] noch weiter ausgeführt wird.

[1514] So auch Winter, JurPC Web-Dok. 109/2002, Abs. 18, und MMR 2002, S. 836.

[1515] Kerr, „Computer Records and the Federal Rules of Evidence", U.S. Department of Justice, United States Attorneys's USA Bulletin, März 2001, Vol. 49, No. 2, www.usdoj.gov/criminal /cybercrime/usamarch2002_ 4.htm

[1516] United States v. Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988): *„The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness."*

[1517] Kerr, „Computer Records and the Federal Rules of Evidence", unter Hinweis auf *United States v. Bonallo*, *United States v. Glasser*, 773 F.2d 1553, 1559 (11th Cir. 1985) und *United States v. Allen*, 106 F.3d 695, 700 (6th Cir. 1997).

[1518] Kerr, „Computer Records and the Federal Rules of Evidence".

[1519] Siehe 3.3.11.

3.3.9 *Reply letter doctrine*

Wie bereits oben wiederholt erwähnt[1520] ermöglicht es das US-amerikanische Beweisrecht, zur Authentifizierung einer Urkunde neben dem direkten Beweis auch Indizien vorzubringen. Den ergänzenden Beweisen und dem Abstellen auf die weiteren Umstände, den *circumstantial evidence*, kann also eine große Bedeutung zukommen.[1521] Zu beachten ist, dass es hierbei zunächst (nur) um die *authentication*, also den Nachweis der Authentizität geht, damit das betreffende elektronische Dokument nach US-amerikanischem Recht als Beweis zugelassen wird. Ist diese Hürde genommen, ist der volle Beweis der Echtheit nicht notwendig ebenfalls erbracht, insbesondere wenn die Urheberschaft bestritten ist.[1522] Eine der sich bei den Indizienbeweisen bei der *authentication* herausgebildeten Fallgruppen ist die *reply letter doctrine*. Entwickelt wurde sie für Briefe, die eine Reaktion auf einen vorangegangenen Brief darstellen. Wenn sich aus dem Brief ergibt, dass sein Verfasser Kenntnisse hat, die unter normalen Umständen nur die Person haben kann, die den oder die vorangegangenen Brief(e) verfasst hat, dann kann nach der Lebenserfahrung davon ausgegangen werden, dass der Brief vom angeblichen Unterzeichner stammt. Voraussetzung ist also, dass der fragliche Brief ein Antwortbrief (*reply letter*) ist, mit dem auf den vorhergehenden Brief reagiert und inhaltlich Bezug genommen wird. Weitere Elemente sind das Erscheinungsbild des Briefes, nach dem dieser Brief vom angeblichen Verfasser geschrieben wurde, sowie die Verlässlichkeit der postalischen Übersendung. Letztere lässt nach der Lebenserfahrung die Annahme zu, dass der mit Briefpost versandte Brief nur vom Empfänger oder einer von ihm ermächtigten Person geöffnet wird. Damit kann die im Antwortbrief zum Ausdruck kommende Kenntnis auf eine bestimmte Quelle zurückgeführt werden.[1523]
Interessant ist, dass der Anwendungsbereich der *reply letter doctrine* mit der Zeit auf andere Kommunikationsformen und -wege wie die Übermittlung per Bote, Telegramme, *mailgram*, Telex, Telefax und selbst auf Telefonate ausgedehnt wurde. Aus diesem Grund ist es möglich, diese Grundsätze auch für die elektronische Kommunikation zu übernehmen. Hinsichtlich des ersten Anknüpfungspunkts der *reply letter doctrine*, dem Inhalt der Mitteilung, bestehen keine Unterschiede zwischen E-Mail und den vorgenannten Kommunikationsformen wie dem Brief.[1524] Wie oben beschrieben kann eine Unterschrift, auch die elektronische Signatur, diesen Zweck erfüllen.[1525] Weitere Voraussetzung ist jedoch der Nachweis der ordnungsgemäßen Absendung des ersten Kommunikationsakts, wofür allerdings nicht der Vollbeweis erforderlich ist. Es ist fraglich, ob dieser Nachweis beispielsweise bei E-Mails ebenfalls geführt werden kann, etwa durch die Absenderkennung. Das war in der US-amerikanischen Literatur offenbar um-

[1520] Siehe 1.3.3.5, 2.5.2.4, 2.5.4.2, 2.5.5.

[1521] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 381.

[1522] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 403.

[1523] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 381, 382.

[1524] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 382, 383, 407, 408 m.w.N.

[1525] Smedinghoff, „The legal Requirements for Creating Secure and Enforceable Electronic Transactions“, S. 18.

stritten.[1526] Die bislang ergangenen und oben dargestellten Urteile zur Formwirksamkeit der E-Mail[1527] lassen jedoch darauf schließen, dass die Namensnennung in der E-Mail als *signature* anerkannt werden kann und damit als Akt der *authentication* gilt.[1528] Bezüglich der Frage der *authentication* stellte ein Bundesgericht in *International Casings Group, Inc. v. Premium Standard Farms, Inc.* im Jahr 2005 fest, dass bei E-Mails mit Absenderkennung das Drücken des „Senden"-Buttons den Akt der Authentifizierung und damit eine rechtswirksame Signatur darstelle.[1529] Auch wenn diesem Urteil, wie auch im oben dargestellten Fall *People v. Hagan*[1530], zahlreiche weitere *circumstantial evidences* wie Zeugenbeweise zugrunde lagen, ist diese Feststellung doch ein starker Hinweis darauf, dass die *reply letter doctrine* auch bei E-Mails tatsächlich Anwendung finden und entscheidende Indizien für die Authentizität und die Urheberschaft eines elektronischen Dokuments bieten kann.

Am Beispiel der USA zeigt sich, dass der Nachweis des Urhebers eines elektronischen Dokuments aufgrund der tatsächlichen Verhältnisse der elektronischen Kommunikation schwierig sein kann, den Parteien aber über das Beweisrecht dennoch Mittel an die Hand gegeben werden, um die Urheberschaft zu beweisen. Für England findet die *reply letter doctrine* als Beweisregel keine Erwähnung. Doch auch dort zeigen viele Fälle, dass ergänzende Beweise und Indizien wie die *signature* in einer E-Mail eine große Rolle spielen können, wenn die Identität des Unterzeichners fraglich ist.[1531] So wurde in *J. Perreira Fernandes SA v. Mehta*[1532] entschieden, dass Beweise in Form weiterer E-Mail-Kommunikation von derselben Adresse ausreichten, um die Authentizität der in Frage stehenden E-Mail zu belegen. In Deutschland ist, wie ebenfalls mehrfach betont, die Berücksichtigung dieser ergänzenden Beweise und Indizien im Rahmen der freien Beweiswürdigung möglich – unabhängig von einer eventuellen Bestrebung, die *reply letter doctrine* für das deutsche Recht zu adaptieren. Umso erstaunlicher ist es, dass deutsche Gerichte in den vorliegenden Urteilen zur Beweiskraft elektronischer Dokumente und Kommunikation diese Aspekte nicht oder kaum einbezogen haben. Dies ist

---

[1526] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 382, 383, 408 m.w.N.

[1527] Siehe 2.5.6.

[1528] *Doherty v. Registry of Motor Vehicles*, No. 97/CV0050 (Suffolk, SS Massachusetts District Court, May 28, 1997); *Cloud Corporation v. Hasbro, Inc.*, 314 F.3d 289 (7th Cir. 2002) (*federal case*); *Lamle v. Mattle, Inc.*, 394 F.3d 1355 (Fed. Cir. 2005); *Shattuk v. Klotzbach*, 14 Mass. L. Rptr. 360; 2001 WL 1839720 (Mass. Super.); *Florida Department of Agriculture and Consumer Services v. Haire*, 836 So.2d 1040 (Fla.App. 4 dist. 2003), corrected opinion *Haire v. Florida Department of Agriculture and Consumer Services*, Nos SC03-446 & Sc03-552, 12. Februar 2004; *United States of America v. Siddiqui*, 235 F.3d 1318 (11th Cir. 200) (*federal*); *On Line Power Technologies, Inc., v. Square D. Company*, 2004 WL 1171405 (S.D.N.Y.); *Rosenfeld v. Zerneck*, 776 N.Y.S.2d 458 (Sup. 2004) (New York); *Bazak International Corp. v. Tarrant Apparel Group*, 378 F.Supp.2d 377 (S.D.N.Y. 2005) (New York).

[1529] *International Casings Group, Inc. v. Premium Standard Farms, Inc.*, 358 F.Supp.2d 863 (W.D.Mo. 2005), 2005 WL 486784.

[1530] *People v. Hagan*, 583 N.E.2d, 494 (Ill. 1991) (Illinois), bei Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 406, 407.

[1531] Z.B. *SM Integrated Transware Ltd. v. Schenker Singapore (Pte) Ltd.* [2005] 2 SLR 651, [2005] SGHC 58, 92; siehe auch Mason, *Electronic Signatures in Law*, S. 186.

[1532] *J. Perreira Fernandes SA v. Mehta* [2006] 1 WLR 1543; [2006] 2 All ER 891; [2006] 1 All ER (Comm) 885; [2006] All ER (D) 264; [2006] IP & T 546; The Times, 16. Mai 2006; [2006] EWHC 813 Ch.)

zu bemängeln, gäbe es hierzu doch – wie dargestellt – ausreichend Anknüpfungspunkte. Immerhin haben deutsche Gerichte solche Aspekte bezüglich der Frage des Zugangs einer Erklärung, hier eines Bescheides einer Behörde, berücksichtigt, siehe beispielsweise ein Urteil des Oberverwaltungsgerichts (OVG) Münster aus 1994 zur bereits erwähnten Faxübertragung:

> *„Dennoch ist die Annahme des* [vorinstanzlichen Gerichts]*, dass vom Zugang des Bescheides ... auszugehen sei, im Ergebnis zutreffend. Die vom* [Verwaltungsgericht] *im Anschluss an seine Ausführungen zur fehlenden Substantiierung gemachten weiteren Darlegungen zu den konkreten Tatsachen, aus denen sich schließen lässt, dass die Klägerin den Bescheid erhalten habe, reichen aus, beim Senat die Überzeugung zu bilden, dass die Klägerin den Bescheid erhalten hat. Dazu hat das* [vorinstanzliche Gericht] *im Einzelnen ausgeführt, dass die Klägerin sich ... in einer Weise verhalten hat, die unerklärlich wäre, wenn sie den Bescheid nicht erhalten hätte. So nimmt* [unter anderem] *die Aussetzung der Vollziehung der Gewerbesteuerfestsetzung ... ausdrücklich auf den Bescheid ... Bezug. ... Noch eindeutiger spricht für den Zugang des Bescheides, dass ... Vollstreckungsversuche stattgefunden haben und gegen den Geschäftsführer der Klägerin das Verfahren auf Abgabe der eidesstattlichen Versicherung eingeleitet worden ist, ohne dass dieser sich jemals darauf berufen hätte, es fehle an der Festsetzung der Vorauszahlungen ... Schließlich kommt hinzu, dass der Prozessbevollmächtigte der Klägerin ... den Erlass von Messbescheiden für die Vorauszahlungen beantragt hat, ohne gegenüber dem vollstreckenden Beklagten geltend zu machen, dass bisher Vorausleistungen nicht festgesetzt worden seien. All dies lässt nur den Schluss zu, dass der Bescheid vom 15. 6. 1988 der Klägerin wirksam bekannt gegeben worden ist.“*[1533]

Schon dieses einzelne Beispiel zeigt, dass die bei der *reply letter doctrine* zu berücksichtigenden Umstände auch von deutschen Gerichten für die Feststellung von Zugang und Inhalt einer Erklärung maßgeblich sein können. Und dies bei der Kommunikationsform Telefax, die sowohl eine der Erscheinungsformen der Erklärung in Textform darstellen kann, als auch vielfach als Vergleich zur E-Mail bemüht wird. Auch eine Übernahme der *reply letter doctrine* in deutsches Recht wäre grundsätzlich denkenswert, da sie allein nach technischen Umständen einer Erklärung und der Lebenswahrscheinlichkeit fragt. Hierbei wäre allerdings zu berücksichtigen, dass eine Anwendbarkeit der *doctrine* auf E-Mails auch im US-amerikanischen Recht noch nicht durch ein Gericht festgestellt wurde. Außerdem dient sie als Beweiszulassungsregel zunächst der *authentication* und liefert keinen Vollbeweis der Urheberschaft und Echtheit der Erklärung.

[1533] OVG Münster, Urt. v. 07.03.1994, 22 A 1063/91, NVwZ 1995, S. 1228, 1229; ebenso das OLG München, JurPC Web-Dok. 153/1999, Abs. 14: *„Von all dem abgesehen, sieht der Senat im Schreiben der Beklagten an die Klägerin – per Fax an diese übersandt –, in dem sie sich auf die fristlose Kündigung ausdrücklich bezieht, durchaus ein weiteres Indiz für den Zugang der Kündigung, zumal die Klage erst nach diesem Schreiben am 25.04.1998 der Beklagten zugestellt worden ist.“*

3.3.10 Anscheinsbeweis bei E-Mail und Textform

Eine weitere Möglichkeit der Erleichterung für die beweisbelastete Partei böte ein Anscheinsbeweis auch bei solchen elektronischen Dokumenten, für die nicht die Verwendung einer digitalen Signatur und damit gegebenenfalls eine Vorabprüfung deren Sicherheit streitet. Nach der dargestellten Rechtsprechung deutscher Gerichte soll nicht einmal die Verwendung eines Passwortschutzes zu einer Beweiserleichterung hinsichtlich der Feststellung der Identität des Vertragspartners führen.[1534] Kern des vor allem von *Mankowski* propagierten Anscheinsbeweises ist nun die Aussage, dass typischerweise unter einer bestimmten E-Mail-Adresse der Inhaber dieser Adresse oder zumindest eine von ihm ermächtigte Person agiere.[1535] Dieser Anschein wird von der ganz herrschenden Meinung in der Literatur und Rechtsprechung abgelehnt.[1536] Es ist jedoch zu fragen, ob diese Diskussion unter Einbeziehung der Aussagen englischer und US-amerikanischer Gerichte zur Beweiskraft elektronischer Dokumente und zur Formwirksamkeit einfacher elektronischer Signaturen nicht nochmals belebt werden könnte und sollte. Der Vorteil eines solchen Anscheinsbeweises für die Identität des Erklärenden[1537] läge in der Verhinderung der offensichtlichen Nachteile der aktuellen Rechtslage. Er käme auch den elektronisch versandten Erklärungen in Textform zugute.

[1534] Siehe 1.3.2.6 und unten 3.3.10.6.

[1535] Mankowski, NJW 2002, S. 2824; so auch Winter, JurPC Web-Dok. 109/2002; in Beschränkung auf passwortgeschützte E-Mail-Systeme auch Ernst, MDR 2003, S. 1093; ähnlich Vehslage, K&R 2002, S. 531, der behauptet, es könne mit guten Gründen davon ausgegangen werden, dass bei Einhaltung der Grundsätze eines ordnungsgemäßen Dokumentenmanagements der Beweis des ersten Anscheins zu Grunde zu legen sei; ebenso Geis, Ivo „Elektronische Kommunikation und Dokumentation – eine rechtliche Betrachtung“, www.informatik.uni-jena.de/dbis/lehre/ss2006/geis/TutoriumUniJenaNeu.pdf.

[1536] Z.B. LG Bonn, MMR 2002, S. 255; OLG Köln, Urt. v. 06.09.2002, 19 U 16/02, JurPC Web-Dok. 364/2002, Abs. 1-15; LG Bonn, CR 2004, S. 218; LG Köln, BeckRS 2006 07259; OLG Hamm, NJW 2007, S. 611; im Ergebnis auch AG Erfurt, JurPC Web-Dok. 71/2002; AG Karlsruhe-Durlach, Urt. v. 02.08.2001, 1 C 355/01, MMR 2002, S. 64; LG Konstanz, Urt. v. 19.04.2002, 2 O 141/01, JurPC Web-Dok. 291/2002; LG Magdeburg, Urt. v. 21.10.2003, 6 O 1721/03, K&R 2005, S. 191; OLG Naumburg, Urt. v. 02.02.2004, 9 U 145/03; OLG Köln, Urt. v. 13.01.2006, 19 U 120/05, JurPC Web-Dok. 48/2006, Abs. 1-21; Geis, www.informatik.uni-jena.de/dbis/lehre/ss2006/geis/TutoriumUniJenaNeu.pdf; Hoffmann, DSWR 2006, S. 61, 62; Noack/Kremer, „Online-Auktionen: eBay als neue Herausforderung für den Rechtsanwalt?“, AZW Reihe Nummer 2004_12_02 (Dec 27, 2004), S. 16, 17; Roßnagel/Pfitzmann, NJW 2003, S. 1209-1214; Roßnagel, K&R 2003, S. 84-86; Wiebe, Andreas, „Anmerkung zu LG Bonn, Urt. v. 07.08.2001 – 2 O 450/99 – Identität eines Teilnehmers an einer Internetauktion“, MMR 2002, S. 257-258.

[1537] Losgelöst von der Frage eines möglichen Anscheinsbeweises über den Zugang einer elektronischen Kommunikation, den Mankowski z.B. für Eingangs- und Lesebestätigungen als gegeben ansieht, ders., „Zum Nachweis des Zugangs bei elektronischen Erklärungen, NJW 2004, S. 1901-1907, S. 1903, ähnlich auch Herwig, „Zugang und Zustellung in elektronischen Medien“, MMR 2001, S. 145-149, S. 146f.; siehe dazu auch Kau, *Vertrauensschutzmechanismen im Internet, insbesondere im E-Commerce*, Karlsruhe 2006, S. 143 ff., der auf technische Lösungen wie fortgeschrittene technische Rückkoppelungsmechanismen u.a. verweist, insgesamt aber von einer diesbezüglichen Zurückhaltung der Rechtsprechung ausgeht; vergleichbar bereits 2001 Waltl in Loewenheim/Koch, S. 184, der bei Empfangsbestätigungen eine – aus heutiger Sicht freilich zu weit gehende – dem Rückschein eines Einschreibebriefs vergleichbare Beweismöglichkeit sieht.

3.3.10.1 Grundlagen des Anscheinsbeweises

Ein Anscheinsbeweis setzt einen typischen Geschehensablauf voraus, bei dem nach der Lebenserfahrung aus einem feststehenden, also unstreitigen oder bewiesenen Erfolg auf eine bestimmte Ursache zu schließen ist.[1538] Hier wäre also von dem Vorliegen einer unter einer bestimmten Adresse verschickten E-Mail auf die Identität des angegebenen Absenders und des tatsächlich Erklärenden zu schließen. Typizität verlangt nicht, dass die entsprechende Verkettung zwingend notwendig ist, sondern nur, dass sie so häufig vorkommt, dass ihre Wahrscheinlichkeit sehr groß ist. Gefordert ist ein für das praktische Leben brauchbarer Grad an Gewissheit, welcher den Zweifeln Schweigen gebietet, auch ohne sie vollständig auszuschließen. Durch Regelmäßigkeit, Üblichkeit und Häufigkeit muss sich auf den ersten Blick ein Muster ergeben. Die bloße, abstrakte Möglichkeit eines anderen als des typischen Verlaufs erschüttert dabei den Anscheinsbeweis nicht. Es muss nicht jedes Restrisiko ausgeschlossen sein. Erst die ernsthafte, nicht nur theoretische Möglichkeit eines anderen Ablaufs steht der für einen Anscheinsbeweis nötigen Regelbildung entgegen.[1539] Maßgeblich für die Annahme eines Anscheinsbeweises ist daher das Vorliegen des typischen Geschehensablaufs.

3.3.10.2 Umkehrschluss aus § 371a ZPO

Gegen einen solchen Anscheinsbeweis wird angeführt, dass die gesetzliche Wertung des § 371a ZPO dagegen spreche. Ausschließlich die qualifizierte elektronische Signatur rechtfertige die Annahme eines Anscheinsbeweises.[1540] Nähme man für andere elektronische Erklärungen ebenfalls einen Anscheinsbeweis an, unterliefe dies die Privilegierung der elektronischen (digitalen) Signatur.[1541] Hier ist zu beachten, dass diese Diskussion schon um den durch § 371a ZPO ersetzten § 291a ZPO geführt wurde. Die dort vorgebrachten Argumente gelten aber gleichermaßen für die Regelung des § 371a ZPO. Dazu wird ausgeführt, der Gesetzgeber habe mit der Einführung des § 371a ZPO die oben dargestellte, einen Anscheinsbeweis bei nicht mit qualifizierter elektronischer Signatur versehenen Dokumenten und Kommunikationen ablehnende Rechtsprechung, ausdrücklich bestätigt.[1542] Die vorstehend angeführte Schlussfolgerung setzt jedoch zunächst voraus, dass es die Absicht des Gesetzgebers war, nur und ausschließlich der qualifizierten elektronischen Signatur anscheinsbegründende Kraft beizumessen und dies für andere elektronische Erklärungen auszuschließen. Eine solche Absicht lässt sich aber in den Materialien des Gesetzgebungsverfahrens etc. nicht finden.[1543] Es ist nicht

[1538] BGH, NJW 1996, S. 1828; LG Bonn, MMR 2002, S. 256.

[1539] Mankowski, NJW 2002, S. 2824; ders. "Für einen Anscheinsbeweis hinsichtlich der Identität des Erklärenden bei E-Mails", CR 2003, S. 44-50, S. 45; jeweils m.w.N.

[1540] LG Köln, BeckRS 2006 07259; Roßnagel/Pfitzmann, NJW 2003, S. 1213; eine entsprechende Anwendung von § 371a Abs. 1 auf private elektronische Dokumente ohne qualifizierte elektronische Signatur ablehnend: Klein, JurPC web-Dok. 198/2007, Abs. 57.

[1541] Roßnagel/Pfitzmann, NJW 2003, S. 1213.

[1542] Hoffmann, DSWR 2006, S. 62.

[1543] So zutreffend Mankowski, CR 2003, S. 47.

ersichtlich, dass § 291a ZPO – und dies gilt gleichermaßen für § 371a ZPO – eine abschließende Regelung ist. Die Tatsache, dass der Gesetzgeber für die qualifizierte elektronische Signatur eine Beweiserleichterung geschaffen hat, schließt nicht aus, dass für andere Arten der elektronischen Erklärung ein richterrechtlich entwickelter Anschein begründet wird. Dies liegt auch im Rahmen der dem Gericht durch § 286 ZPO eingeräumten freien Beweiswürdigung.[1544] Hiergegen wird angeführt, dass der Gesetzgeber mit der Einführung des § 371a ZPO die Möglichkeit, für einfache elektronische Erklärungen oder Dokumente eine Einstufung über der als Augenscheinsbeweisobjekt gemäß § 371 Abs. 1 S. 2 ZPO nicht vorgenommen habe.[1545] Jedoch spricht auch dieser Umstand nicht zwingend gegen die Annahme eines Anscheinsbeweises.

3.3.10.3 Vergleich mit anerkannten Anscheinsbeweisen

Ein weiteres Argument für die Ablehnung ist, dass die Kommunikation über das Internet, auch bei Verwendung von Passwörtern, größeren Missbrauchsmöglichkeiten und Missbrauchsrisiken ausgesetzt sei, als dies beispielsweise beim Btx-Verfahren oder bei EC-Karte mit PIN-Nummer der Fall sei, für die eine solche Beweiserleichterung in bestimmten Fällen anerkannt ist.[1546] *Mankowski* führt dagegen an, dass die Rechtsprechung zum Beispiel auch bei Telefonabrechnungen einen Anscheinsbeweis greifen ließe, obwohl die betreffenden Einrichtungen anerkanntermaßen nicht vollständig manipulationsresistent seien.[1547] Gegen den Inhaber eines Telefonanschlusses spricht dabei ein Anscheinsbeweis für die zutreffende Erfassung der Gebühren, obwohl ebenfalls die Möglichkeit besteht, das sich ein Dritter in ein das Telefonsystem aufschaltet. Diese Möglichkeit soll jedoch nicht genügen, um den Anscheinsbeweis zu beseitigen.[1548] Sofern die Passwortvergabe – auch online – nach vorheriger Identitätsprüfung des E-Mail-Kontoinhabers erfolge, könne jedoch laut *Mankowski* auch einem Passwortschutz eine hinreichende Verlässlichkeit zugeschrieben werden. Wertungsmäßig sei daher ein Vergleich zum Passwort-System bei Btx und der dort anerkannten Beweisbegünstigung des Erklärungsempfängers nahe liegend, was für den von ihm propagierten Anscheinsbeweis spreche.[1549] In den Btx-Fällen, auf die hier Bezug genommen wird, hatte die Rechtsprechung eine Beweislastumkehr zugunsten des Anbieters angenommen, da aufgrund der passwortgeschützten Teilnehmeradresse und damit der festen Nutzerkennung festgestellt werden konnte, dass der jeweilige häusliche Btx-Anschluss tatsächlich genutzt worden war.[1550] Unklar war nur, ob dies durch den Betroffenen selbst oder durch

[1544] Mankowski, CR 2003, S. 47.

[1545] Hoffmann, DSWR 2006, S. 62; Klein, JurPC Web-Dok. 198/2007, Abs. 57.

[1546] Wiebe, Andreas, Anm. zu LG Bonn, MMR 2002, S. 255, S. 257, 258.

[1547] Mankowski, NJW 2002, S. 2825 m.w.N.; Winter, JurPC Web-Dok. 109/2002.

[1548] Winter, JurPC Web-Dok. 109/2002; LG Bonn, CR 2004, S. 218 unter Verweis auf Mankowski, NJW 2002, S. 2282.

[1549] Mankowski, NJW 2002, S. 2826.

[1550] Siehe dazu bspw. Borsum/Hoffmeister, „Rechtsgeschäftliches Handeln unberechtigter Personen mittels Bildschirmtext“, NJW 1985, S. 1205-1207.

andere erfolgte. Eine Übertragung auf Fälle des E-Mail-Verkehrs wird von der Rechtsprechung jedoch abgelehnt, da hier gerade nicht feststehe, ob die Abgabe der fraglichen Erklärung aus dem (gegenständlichen) Einflussbereich des Beklagten stamme.[1551] Dass eine dahingehende Unsicherheit besteht, ist richtig. Soweit dies jedoch damit begründet wird, dass nicht feststehe, ob einer der Computer des Beklagten für die Versendung der fraglichen E-Mail genutzt wurde[1552], mutet diese Argumentation fragwürdig an. Schließlich sind E-Mail-Konten gerade nicht wie ein Festnetztelefon- oder Btx-Anschluss an einen gegenständlichen Zugang gebunden, sondern können von jedem Ort mit Internetzugang versendet werden, solange man über das entsprechende Passwort des E-Mail-Kontos verfügt.[1553] Insofern ist dem Gericht zuzugeben, dass eine Parallele hinsichtlich eines Abstellens auf die gegenständlichen Risikosphären der Betreffenden nicht besteht. *Mankowski* wendet hier ein, wie in den Btx-Fällen sei eine E-Mail-Adresse jedoch genau einem Inhaber zugeordnet. Dieser Umstand sei entscheidend, nicht die Verknüpfung mit einem bestimmten Endgerät. Das Argument, Btx verwende im Gegensatz zum offenen Kommunikationsmedium Internet eine anschlussbezogene Kennung, was die Annahme der Benutzung durch den Namensträger erlaube, sei falsch, weil auch E-Mails auf dem Prinzip der einmaligen und exklusiven Zuordnung beruhten.[1554] Hierbei verkennt er jedoch, dass gerade diese Zuordnung im entscheidenden Moment der Abgabe der erheblichen Erklärung über das bestimmte E-Mail-Konto möglich sein müsste, nicht bloß im Moment der Einrichtung dieses E-Mail-Kontos. Selbst für den Zeitpunkt der Erstanmeldung des Nutzers beim Betreiber kann eine solche Zuordnung nicht sicher angenommen werden. Wie zutreffend eingewendet wird, erfolgt diese Zuordnung etwa bei einem E-Mail-Betreiber wie zum Beispiel „GMX“ häufig ausschließlich online, sodass die Identität des Teilnehmers tatsächlich niemals als eindeutig festgestellt werden kann.[1555]

Ebenfalls über das Telekommunikationsnetz übertragen werden Fax-Mitteilungen, weshalb vielfach Vergleiche zu E-Mails angestrengt werden und sie hier kurz erwähnt werden sollen. Teilweise wurde für diese Kommunikationsform eine hohe Übertragungssicherheit angenommen, weshalb der "OK"-Vermerk auf einem Fax-Sendeprotokoll einen Beweis des ersten Anscheins für den Zugang des Fax darstelle.[1556] Dies wird von BGH und BAG jedoch abgelehnt. Durch den Sendebericht werde nur die Herstellung der Verbindung zwischen dem Sende- und dem Empfangsgerät angezeigt, für die geglückte

---

[1551] LG Bonn, MMR 2002, S. 256; OLG Köln, JurPC Web-Dok. 364/2002.

[1552] LG Bonn, MMR 2002, S. 256: *„Anders als bei der Nutzung von Btx-Anschlüssen lässt sich hier ... kein Anschein zu Lasten des Beklagten aus der (gegenständlichen) Nutzung eines bestimmten Anschlusses einer Verbindung ableiten, weil bereits nicht feststeht, dass einer seiner beiden* [E-Mail-] *Anschlüsse zur Abgabe des Gebots genutzt wurde“*, bestätigt durch OLG Köln, JurPC Web-Dok. 364/2002.

[1553] So auch LG Bonn, CR 2004, S. 218.

[1554] Mankowski, NJW 2002, S. 2826 mit Verweis auf LG Berlin, Urt. v. 16.05.2002, 16 O 4/02, CR 2002, S. 606.

[1555] LG Bonn, MMR 2002, S. 257; OLG Köln, JurPC Web-Dok. 364/2002.

[1556] OLG München, JurPC Web-Dok. 153/1999, Abs. 10, in Bezug auf § 130 Abs. 1 S. 1 BGB. Dabei habe der Empfänger zudem die Möglichkeit, in ihm zumutbarer Weise einen abweichenden Geschehensablauf als ernsthaft möglich darzulegen und zu beweisen, indem er die eigenen Empfangsaufzeichnungen vorlegt, aus denen sich Übertragungsfehler ersehen ließen; Abs. 12.

Übermittlung der Daten und das Ausbleiben von Störungen besitze das Sendeprotokoll hingegen keinerlei Aussagewert, da die Datenübertragung an Defekten am Empfangsgerät oder an Leitungsstörungen scheitern könne, ohne dass die Unterbrechung oder missglückte Datenübermittlung im Sendebericht ausgewiesen werde. Der Sendebericht könne daher allenfalls ein Indiz für den Zugang sein, da auch die Vermutung einer hohen Verbindungs- und Übertragungssicherheit noch keine verlässliche Grundlage für einen Anscheinsbeweis abgebe.[1557]

Der Kontoinhaber wiederum haftet für eine Geldautomatenabhebung unter Verwendung von EC-Karte und PIN oder einen Online-Überweisungsauftrag unter Verwendung von PIN und TAN.[1558] Hier ist anzumerken, dass das Beweisthema des Anscheinsbeweises bei der EC-Karte die Frage ist, ob aus der Abhebung seitens eines Dritten mit EC-Karte und PIN auf die (fahrlässige) gemeinsame Aufbewahrung von EC-Karte und PIN durch den Karteninhaber zu schließen ist. Dabei geht es um eventuelle Obliegenheitsverletzungen des Karteninhabers, nicht um eine unmittelbare Zurechnung der Abhebung zum Karteninhaber selber.[1559] *Mankowski* geht noch weiter und nimmt an, ganz vorherrschend bliebe in diesen Fällen ein Anscheinsbeweis dafür übrig, dass eine Abhebung unter Verwendung der PIN durch den EC-Karten-Inhaber erfolgt oder dieser jedenfalls den Missbrauch ermöglicht hat. Übertragen auf das Online-Banking, insbesondere unter Verwendung von PIN und TAN, stelle dieser Vergleich vielmehr ein Argument für als gegen den Anscheinsbeweis zumindest bei passwortgeschützten E-Mails dar. Dass im Internet theoretisch größere Angriffsmöglichkeiten zum Ausspähen von Passwörtern bestehen, ändere nichts an der immer noch sehr geringen Wahrscheinlichkeit eines solchen Angriffs.[1560] Unabhängig von der Frage der Wahrscheinlichkeit eines Angriffs muss ein solcher Anscheinsbeweis beim Online-Banking mit *Kind/Werner* jedoch deshalb abgelehnt werden, weil es zumeist an der notwendigen Pflichtverletzung tatsächlich fehlt.[1561] Dies dann, wenn der Bankkunde ihm zur Verfügung stehende Schutzmaßnahmen ergriffen hat, wie ein aktuelles, noch nicht rechtskräftiges Urteil des AG Wiesloch vom 4.7.2008 zu bestätigen scheint, nach dem das Bankinstitut haftet, wenn Kundendaten unerlaubt abgefangen werden (Phishing), obwohl dieser ein gängiges Virenschutzprogramm benutzt.[1562] Tatsächlich sagt das eingangs angeführte Argument, die Kommunikation über das Internet sei größeren Missbrauchsrisiken und -möglichkeiten ausgesetzt als beim Btx-Verfahren oder der Verwendung von EC-Karte und PIN oder von PIN und TAN, zunächst nichts über die Wahrscheinlichkeit solchen Missbrauchs aus. Diese müsste eine reale und nicht bloß theoretische Möglichkeit darstellen, um dem Anscheinsbeweis die Grundlage zu entziehen. Der wesentliche Unterschied liegt hier

[1557] BGH, NJW 1995, S. 665 – 667; ebenso BAG, Urt. v. 14.08.2002, 5 AZR 169/01.

[1558] Zum Anscheinsbeweis beim Online-Banking – diesen ablehnend – Kind/Werner, CR 2006, S. 359 f.

[1559] Zutreffend Mankowski, CR 2003, S. 46.

[1560] Mankowski, CR 2003, S. 46, 47.

[1561] Kind/Werner, CR 2006, S. 359 f.

[1562] AG Wiesloch, Urt. v. 4.7.2008 – 4 C 57/08 –, bei www.spiegel.de und www.faz.net, entgegen einem vorhergegangenen Urteil des LG Köln vom 5.12.2007 – 9 S 195/07 –, JurPC Web-Dok. 12/2008, Abs. 1-59, wonach der Kunde bestimmte Sorgfaltspflichten zu beachten und insbesondere eine jeweils aktuelle Virenschutzsoftware, Firewall und regelmäßige Updates des Betreibssystems zu nutzen habe.

jedoch darin – und damit ist der Gegenansicht zuzustimmen –, dass bei den EC-Karten-Fällen und beim Online-Banking die Kenntnis der PIN allein nicht genügt, sondern es dazu auch den Besitz der EC-Karte beziehungsweise der TAN bedarf.
Diese Vergleiche sprechen also nicht für die Annahme eines Anscheinsbeweises, schließen diesen jedoch auch nicht per se aus. Entscheidend ist die Frage der Wahrscheinlichkeit und der Lebenserfahrung, so vorhanden.[1563] Entsprechende Anscheinsbeweise für Btx- oder Fax-Übertragungen, aber auch bei Transaktionen mittels EC-Karte und PIN und/oder TAN existieren im englischen und US-amerikanischen Recht offenbar nicht. Grundsätzlich ist hier die auf einen Umstand vertrauende Partei für diesen beweispflichtig, also etwa dafür, dass die fragliche Transaktion vom Kontoinhaber ermächtigt wurde. Ob der Kontoinhaber oder ein Dritter die Transaktion durch Angabe der korrekten PIN ausgeführt hat, ist also vom Gericht positiv festzustellen.[1564] Dort ergangene Urteile unterstreichen vielmehr wiederum die Bedeutung der ergänzenden Beweise und der Beweispflicht. Im US-amerikanischen Fall *Judd v. Citibank*[1565] waren folglich Fragen der Qualität der vorliegenden Beweise, der Beweispflicht und der Glaubhaftigkeit entscheidend. Zugrunde lag ein Fall, in dem eine Bankkundin zwei Geldabhebungen entdeckte, die zu einem Zeitpunkt vorgenommen worden waren, als sie sich an ihrem Arbeitsplatz befand. Auf Grundlage der vorliegenden Beweise gab das Gericht ihrer Klage auf Rückerstattung der Geldbeträge statt, da es überzeugt war, dass die Klägerin die Abhebungen nicht hatte vornehmen können. In einem englischen strafrechtlichen Fall wurde eine Verurteilung aufgrund angeblicher Transaktionen mittels Geldautomaten aufgehoben, weil die Bank die Herausgabe von Informationen über das Computersystem, Aufzeichnungen und Geschäftsabläufe im Verfahren verweigert hatte.[1566] Für das deutsche Recht sind diese Vergleiche hier unergiebig.

3.3.10.4 Übereinstimmung mit gesetzlichen Wertungen

Eine Beweiserleichterung in Form des Anscheinsbeweises abzulehnen bedeute laut *Mankowski* einen Widerspruch zu bestehenden gesetzlichen Wertungen. Für einen solchen Anscheinsbeweis spreche der Vergleich mit der gesetzlich festgeschriebenen Beweislast bei schriftlichen Erklärungen, die ihrerseits ebenfalls manipulierbar seien. Insbesondere bei einem Erstkontakt habe eine handschriftliche Unterschrift des Unbekannten keinen wirklichen Authentizitätswert. Der Einwand, die Unterschrift sei gefälscht, und der entsprechende Nachweis gehörten aber zum Gegenvortrag des scheinbar Erklärenden.[1567] Dem ist zuzustimmen.[1568] Vor allem aber behauptet *Mankowski* – unter Verweis auf die Strafbewehrung möglicher Dritteingriffe in die E-Mail-

[1563] Dazu nachfolgend 3.3.10.6.
[1564] Mason, *Electronic Signatures in Law*, S. 301.
[1565] *Judd v. Citibank*, N.Y.City Civ.Ct., 435 N.Y.S.2d 210 (New York).
[1566] Siehe Darstellung bei Mason, *Electronic Signatures in Law*, S. 301.
[1567] Mankowski, NJW 2002, S. 2824, 2825.
[1568] Siehe dazu auch 3.3.4, 3.3.6.2.

Kommunikation[1569] –, dass die Rechtsordnung sich selbst „desavouierte", wenn sie diesen strafrechtlichen Schutz nicht ernst nehmen und seinen gewollten Abschreckungseffekt in Abrede stellen würde. Die Grundannahme müsse daher, wolle die Rechtsordnung ihre eigenen Anreizsetzungen ernst nehmen, von rechtstreuem Verhalten ausgehen. Er fragt, ob die bloße Möglichkeit eines strafbaren Eingriffs Dritter wirklich entlasten und nicht erwünschte Schutzbehauptungen tragen können solle.[1570] Sich pauschal auf die Sicherheitsrisiken des Internet zu berufen, stünde im Widerspruch dazu, dass sich der Nutzer sich diesen Risiken zum Trotz des Internets bedient.[1571] Auch dies ist ein Argument für eine Revision der derzeit bestehenden Risikozuweisung. Ferner führt *Mankowski* an, das Vertrauen des Empfängers in die Absenderabgabe sei noch schützenswerter, wenn sich der E-Mail-Kontakt im Rahmen einer organisierten Internet-Plattform ereigne. Dabei treffe den Betreiber die Nebenpflicht gegenüber den Teilnehmern, die Systemsicherheit zu wahren und das System gegen unbefugte Eingriffe von dritter Seite abzusichern. Die Plattform-Teilnehmer selbst hätten nur geringe Schutzmöglichkeiten und stünden insoweit nicht in der Verantwortung, da typisches Angriffsobjekt Dritter das Rechnersystem des Plattformbetreibers sein werde. Die Plattform-Teilnehmer dürften erwarten, dass der Betreiber nach dem Stand der Technik Vorkehrungen zur Sicherheit treffe.[1572] Diese Ansicht scheint gestärkt durch ein Urteil des OLG Brandenburg vom 16.11.2005, wonach ein Betreiber eines elektronischen kommerziellen Marktplatzes als Störer für Dritte haftet, die sich ohne Befugnis unter dem Namen eines anderen Marktteilnehmers anmelden, und entsprechende Vorsorge gegen Rechtsverletzungen treffen muss.[1573] Dieses Vertrauen, das über die Pflichtenstruktur des BGB normativ abgesichert sei, solle man auch im Verhältnis zum scheinbaren Absender honorieren.[1574] *Mankowski* argumentiert hier mit dem schützenswerten Vertrauen des Nutzers in die Schutzvorkehrungen des Betreibers und damit in die Absenderangaben. Eine Haftung des Plattformbetreibers oder E-Mail-Service Providers für die Identität der bei ihm Angemeldeten besteht dennoch zu Recht derzeit nicht.[1575] Und selbst wenn der Nutzer um konkrete Schutzmechanismen des Betreibers weiß und – was bei der allgemeinen Kenntnis möglicher Dritteingriffe fraglich ist – auf diese vertraut, bedeutet dies nicht per se, dass dieses Vertrauen tatsächlich schützenswert ist. Je mehr Angriffe und Manipulationen bekannt werden, was derzeit der Fall ist, desto weniger kann und darf der Nutzer darauf vertrauen, dass sein Betreiber solche Eingriffe in sein E-Mail- oder Plattformkonto ausschließen werde. Dass – zumindest für den dort zugrunde liegenden Fall der Internetauktionsplattform – gerade keine hinreichenden Schutzmaßnahmen und insbesondere keine vertrauenswürdige Identitätsprüfung vorla-

[1569] In Betracht kämen die Straftatbestände der §§ 267 Abs. 1, 269 Abs. 1 und 303a StGB; Mankowski, NJW 2002, S. 2823; ders., CR 2003, S. S. 45.

[1570] Mankowski, NJW 2002, S. 2826.

[1571] Mankowski, CR 2003, S. 46.

[1572] Mankowski, NJW 2002, S. 2824.

[1573] OLG Brandenburg, Urt. v. 16.11.2005, 4 U 5/05, MMR 2006, S. 107-110.

[1574] Mankowski, NJW 2002, S. 2824 unter Hinweis darauf, dass ein Abbedingen dieser Pflichten des Betreibers gegen § 307 Abs. 2 Nr. 2 BGB verstöße.

[1575] Wiebe, Anmerkung zu AG Erfurt, MMR 2002, S. 129

gen, es sich also um ein grundsätzlich unsicheres System handelt, bestätigt das vorgenannte Urteil des OLG Brandenburg gerade.[1576]

3.3.10.5 Kein Wertungswiderspruch zur Einführung des § 126b BGB

Als normatives Argument führt *Mankowski* die Absicht des Gesetzgebers an, den elektronischen Geschäftsverkehr fördern und für diesen einen funktionellen rechtlichen Rahmen schaffen zu wollen. Auf dieser Zielsetzung beruhe die Einführung der Textform. Diese solle gerade dazu dienen, E-Mails und entsprechende elektronische Erklärungen zu fördern.[1577] Die Begründung des Gesetzgebers lautet:

> *„Entscheidender Beurteilungsmaßstab für die Entscheidung, welche Formtatbestände im Einzelnen für die Textform geöffnet werden sollen, ist die zu gewährende Sicherheit im Rechtsverkehr. Die Textform ist nur für solche Formtatbestände vorgesehen, bei denen eine ausreichende Sicherheit auch gegeben ist, wenn ... die Erklärung ... nur mittels telekommunikativer Einrichtung übermittelt wird. Dies gilt vor allem für die Formtatbestände, bei denen keiner der Beteiligten und auch kein Dritter ein ernsthaftes Interesse an einer Fälschung haben kann.“*[1578]

Dass in der überwältigend großen Anzahl der Fälle der hier in Frage stehenden elektronischen Kommunikation, wie sie für rechtserhebliche Erklärungen zum Beispiel zum Erwerb von Waren und Dienstleistungen über das Internet eingesetzt wird, ein solches ernsthaftes Interesse an Fälschung gerade nicht besteht, ist oben bereits angedeutet worden und wird nachfolgend nochmals erörtert.[1579] Das belegt auch die vom Gesetzgeber eingeräumte Möglichkeit, rechtserhebliche Erklärungen wie Widerrufsbelehrungen in genau diesem Anwendungsbereich zuzulassen.[1580] Sofern man einer „telekommunikativen Einrichtung“ wie dem Internet und dem E-Mail-Verkehr überhaupt jede Verlässlichkeit im Sinne von Schutz vor Dritteingriffen und Manipulationen abspräche, bedürfte es des Merkmals der *„ausreichenden Sicherheit“* nicht. Diese Gesetzesbegründung machte dann keinen Sinn. Genau darum, ob der E-Mail-Verkehr eine ausreichende Sicherheit bietet, dreht sich aber die Frage nach der Annahme eines Anscheinsbeweises. Es soll gerade vor dem Hintergrund der seit der Einführung der elektronischen und der Textform seit 2001 gemachten Erfahrungen festgestellt werden, ob die damals insbesondere vom Gesetzgeber genannten Annahmen und Begründungen hinsichtlich der Anwendungsbereiche der Formtatbestände auch heute noch überzeugend sind oder einer

[1576] So auch Spindler, „Anmerkung zu OLG Brandenburg, Urt. v. 16.11.2005 – 4 U 5/05 – Störerhaftung von eBay bei Identitätsdiebstahl“, MMR 2006, S. 110-111, S. 111.

[1577] Siehe oben 2.3.4.2; Mankowski, NJW 2002, S. 2826.

[1578] Amtliche Begründung, BT-Drs. 14/4987, S. 18.

[1579] Siehe 3.3.10 und 3.3.10.6.

[1580] Siehe oben 2.3.4.2.

Anpassung bedürfen. Falsch ist deshalb die von der oben zitierten Gesetzesbegründung abgeleitete Behauptung *Roßnagels* und *Pfitzmanns*, E-Mail sei

> *„nur dann akzeptabel, wenn es für die Erklärung kein Fälschungsrisiko gibt. Gibt es aber ein Fälschungsrisiko, ist E-Mail für die Willenserklärung – zumindest als Rechtsform und als Beweismittel – ungeeignet."*[1581]

Schon die oben zitierte Gesetzesbegründung verlangt (nur) ausreichende Sicherheit, nicht den absoluten Ausschluss jedes Fälschungsrisikos. E-Mails als für rechtserhebliche Willenserklärungen ungeeignet zu bewerten ist widersinnig[1582] und widerspräche allem oben dargestellten legislativen Bemühungen in Europa und den USA.[1583] Die vom Gesetzgeber gewollte Förderung des elektronischen Rechts- und Geschäftsverkehrs meint nicht ausschließlich die mittels digitaler Signatur-Technologie abgesicherte Kommunikation. Erst recht schließt diese Förderung die einfache elektronische Signatur zum Beispiel in Form beziehungsweise im Rahmen einer E-Mail nicht aus.[1584] Zwar hat der Gesetzgeber in seiner Begründung für die Einführung der Textform angeführt:

> *„Da elektronische Nachrichten auf ihren Transport durch offene Netze für den Adressaten unerkennbar gefälscht oder verändert werden können, bedarf es … eines sicheren Rahmens zur elektronischen Authentifizierung des Kommunikationspartners und Überprüfung der Integrität der übermittelten Daten."*[1585]

Daraus ist jedoch nur zu entnehmen, dass es einen entsprechenden Bedarf an sicherer Kommunikation gibt, dem entsprochen werden muss. Das ist mit der Einführung der fortgeschrittenen beziehungsweise der qualifizierten elektronischen Signatur geschehen. Es stellt aber keine Grundvoraussetzung der Nutzung elektronischer Nachrichten dar. Erst recht sagt dies nichts darüber aus, welche rechtliche Qualität und Beweiskraft der unbestritten in ihrer Sicherheit und Formwirksamkeit unter der elektronischen Form angesiedelten Textform, zum Beispiel in Form von E-Mails, zugesprochen werden kann. Die Überlegungen zum Anscheinsbeweis sind also durchaus mit dem Ziel der Förderung des elektronischen Rechts- und Geschäftsverkehrs konform. Was nun durch die Einführung der Textform an Förderung für die elektronische Erklärung erreicht würde, wäre laut *Mankowski* über den Weg der Beweislastverteilung wieder genommen, wenn man bereits die bloße Möglichkeit eines Dritteingriffs ausreichen ließe, um einen Vollbeweis von Identität und Authentizität durch den Empfänger zu fordern. Das ei-

[1581] So Roßnagel/Pfitzmann, NJW 2003, S. 1212.

[1582] Es ist auch fraglich, was mit E-Mail als Rechtsform gemein ist. Sollte dies tatsächlich die E-Mail als rechtserhebliche Willenserklärung – die im Übrigen als solche anerkannt ist – umfassen, liefe diese Forderung darauf hinaus, dass jede nicht mit einer digitalen Signatur versehene elektronische Kommunikation nicht nur nicht beweiskräftig sondern sogar nicht rechtsgültig sein solle.

[1583] Der Gesetzgeber hat vielmehr ein besonderes Fälschungsrisiko bei der Textform nicht gesehen; Mankowski, CR 2003, S. 45.

[1584] So aber Roßnagel/Pfitzmann, NJW 2003, S. 1212.

[1585] Amtliche Begründung, BT-Drs. 14/4987, S. 10; ebenso amtliche Begründung zum sigG, BR-Drs. 966/96, S. 28, und zum 3. VwVfÄG, BT-Drs. 14/9000, S. 26.

gentliche Grundanliegen sei so durch die Beweislastverteilung konterkariert, was gerade nicht funktionsgerecht sei.[1586] Des Weiteren bestünde ein Widerspruch zwischen Strenge beim Identitätsnachweis und sachgerechtem Bejahen des Rechtsbindungswillens bei elektronischen Erklärungen ohne übertriebene Hintertüren und Ausstiegsmöglichkeiten für den Erklärenden.[1587] Dem ist nach dem bisher Festgestellten zuzustimmen.

3.3.10.6 Typizität des Geschehensablaufs

Mankowski führt als Hauptargument und Grundlage für den Anscheinsbeweis für die Identität des Versenders die geringe Wahrscheinlichkeit eines Dritteingriffs an. Er fragt, wie wahrscheinlich es sei, dass eine einzelne Erklärung von Dritten abgefangen, verändert oder sonst manipuliert werde. Die riesige Zahl täglich in aller Welt verschickter E-Mails schütze die einzelne E-Mail.[1588] Die Lebenserfahrung zeige vielmehr, dass die Erwartung, eine E-Mail stamme tatsächlich vom angegebenen Absender, kaum einmal enttäuscht werde.[1589] Bei passwortgeschützen E-Mail-Konten bestünden mit der E-Mail-Adresse und dem Passwort sogar zwei vertrauensbegründende Momente, was die Wahrscheinlichkeit eines dadurch „doppelten Diebstahls“ der elektronischen Identität nochmals sinken lasse.[1590] Die Verwendung höherer Sicherheitsstandards für eine hinreichend verlässliche Basis zu verlangen, wäre eine normative Überhöhung. Gefordert sei hier eine tatsächliche Basis.[1591] Für solche Manipulationen und für sogenannte Maskerade-Angriffe sei zudem eine gewisse technische Kompetenz nötig.[1592] Insgesamt seien die Möglichkeiten Dritter, eine E-Mail Abzufangen und zu verändern sehr gering. Es bestünden vor allem nur sehr geringe Anreize für Dritteingriffe, da nur sehr selten eigene Vorteile für den Täter zu erwarten seien. Dem Missbraucher beziehungsweise Angreifer könne es im Grunde nur darum gehen, dem Empfänger oder dem angegebenen Absender zu schaden. Tatsächlich hatte zumindest das LG Konstanz ausgeführt, dass kaum ein Dritter Interesse daran habe, ein fremdes Passwort und damit Zugang zu einer Verkaufsplattform zu erlangen.[1593] Laut *Mankowski* verminderten diese geringen Anreize die Wahrscheinlichkeit von Dritteingriffen entscheidend.[1594] Zudem sei der

[1586] Mankowski, NJW 2002, S. 2826.

[1587] Mankowski, NJW 2002, S. 2826 unter Verweis auf BGH, Urt. v. 07.11.2001, VIII ZR 13/01, NJW 2002, S. 363.

[1588] Mankowski, NJW 2002, S. 2823; ders., CR 2003, S. 44-50, S. 45; zustimmend Winter, MMR 2002, S. 836, und Ernst, MDR 2003, S. 1093, allerdings nur für den Fall der passwortgeschützten Plattform und unter der Voraussetzung, dass das Passwortsystem eine gewisse Hindernisschwelle setze.

[1589] Mankowski, NJW 2002, S. 2824. so auch Mason, *Electronic Signatures in Law*, S. 332.

[1590] Mankowski, CR 2007, S. 607.

[1591] Mankowski, CR 2003, S. 45.

[1592] Mankowski, NJW 2002, S. 2823. Spam-Mails stellten kein Problem dar, da entweder die angegebene E-Mail-Adresse überhaupt nicht existiere, oder der Inhaber der angegebenen tatsächlich existierenden E-Mail-Adresse könne nachweisen, dass die E-Mail nicht von ihm stamme. Bei sog. Spoof-Mails ohne Absenderangabe komme es ebenfalls nicht zu einer Fehlzuordnung.

[1593] LG Konstanz, Urt. v. 19.04.2002, 2 O 141/01, JurPC Web-Dok. 291/2002; MMR 2002, S. 835.

[1594] Mankowski, CR 2003, S. 45; ders., NJW 2002, S. 2823; so auch Mason, *Electronic Signatures in Law*, S. 332.

Abschreckungseffekt einer möglichen Strafverfolgung als Gegenanreiz einzukalkulieren.[1595] Hier nochmals erwähnt wird das Argument, der Gesetzgeber selbst sehe keine relevanten Fälschungsrisiken, weshalb er die Textform eingeführt habe.[1596] In welchem Maße die genannten Aspekte die Wahrscheinlichkeit eines Dritteingriffs tatsächlich beeinflussen, mag Ansichtssache und dauerhaft streitig bleiben. Letztlich maßgeblich ist, ob die vorausgesetzte Typizität in der Realität wirklich besteht.

Diese für den Anscheinsbeweis nötige Typizität eines bestimmten Geschehensablaufs und der absolute Ausnahmecharakter anderer, wenngleich denklogisch möglicher Geschehensabläufe lägen vor, jedenfalls dann, wenn nicht gerade ein Missbrauch des E-Mail-Kontos offensichtlich sei.[1597] Insoweit bestünde ein vom Adressinhaber zurechenbar gesetzter Rechtsschein.[1598] Diese Argumentation ersetzt jedoch nicht den empirischen Nachweis der Typizität. Zumindest grundsätzlich ist *Mankowski* nach dem oben Festgestellten[1599] jedoch zuzugeben, dass, wenn ein Kommunikationsmedium schwierig zu manipulieren sei, man dem scheinbar Erklärenden substantiierten Gegenvortrag dafür abverlangen müsse, dass die Erklärung entgegen dem Anschein nicht von ihm stamme.[1600] Hierzu beruft er sich auf das bereits erwähnte Urteil des ArbG Frankfurt a.M.[1601] und ein Urteil des AG Ettlingen[1602], die E-Mails tatsächlich Beweiskraft zugemessen haben. Hier ist zwar einzuwenden, dass diese Urteile nichts zu dem hier behaupteten typischen Geschehensablauf aussagen. Dennoch wird deutlich, was unter einem typischen Geschehensablauf bei der Versendung von E-Mails zu verstehen ist: Der Versender nutzt nach Anmeldung eines E-Mail-Kontos dieses zur Erzeugung einer E-Mail, der vor oder bei Versendung typischerweise eine durch das E-Mail-Programm automatisch generierte Angabe der E-Mail-Absender-Adresse beigefügt wird. Vielfach wird noch ein Name oder ein ebenfalls automatisch generierter Briefkopf oder ähnliches in den Text der E-Mail eingefügt beziehungsweise diesem angehängt. Die so versendete E-Mail erreicht daraufhin das E-Mail-Konto des vom Versender angegebenen Adressaten. Zumindest dann, wenn eine (technische) Überprüfung der E-Mail-Envelopes[1603] eine Übereinstimmung der Informationen über die Absender-IP-Adresse mit dem Mailserver des behaupteten Absenders festgestellt wird, so kann mit *Schmidt/Pruß/Kast* von einem typischen Geschehensablauf ausgegangen werden, der auf einen bestimmten Ablauf

[1595] Siehe oben 3.3.10.4; Mankowski, NJW 2002, S. 2823; ders., CR 2003, S. S. 45; Winter, JurPC Web-Dok. 109/2002, Abs. 14; a.A. Klein, JurPC web-Dok. 198/2007, Abs. 59. Z.B. ist die Fälschung von Erklärungen in Textform nach § 269 StGB, u.U. auch nach § 268 StGB, strafbar, siehe bei Boente/Riehm, „Das BGB im Zeitalter digitaler Kommunikation – Neue Formvorschriften“, JURA 2001, S. 793-798, S. 795.

[1596] Mankowski, CR 2003, S. 45.

[1597] Mankowski, NJW 2002, S. 2824; Winter, JurPC Web-Dok. 109/2002.

[1598] Mankowski, NJW 2002, S. 2824, unter Berufung auf OLG Oldenburg, Urt. v. 11.01.1993, 13 U 133/92, NJW 1993, S. 1400, und LG Berlin, Urt. v. 16.05.2002, 16 O 4/02, NJW 2002, S. 2569.

[1599] Siehe 3.3.8.

[1600] Mankowski, NJW 2002, S. 2824, unter Berufung auf LG Aachen, Urt. v. 31.10.1996, 8 O 244/96, CR 1997, S. 153.

[1601] ArbG Frankfurt, JurPC Web-Dok. 125/2002, Abs. 1-10.

[1602] AG Ettlingen, Urt. v. 11.05.2001, 2 C 259/00, JurPC Web-Dok. 65/2002.

[1603] Siehe oben 3.3.5.2 und Schmidt/Pruß/Kast, CR 2008, S. 268, 269.

hinweist und es dem Gericht ermöglicht, die Tatsache der Absendereigenschaft im Wege des Anscheinsbeweises als bewiesen anzusehen.[1604] Fraglich ist, ob solch ein Anschein auch ohne diesen Nachweis aufgrund technischer Prüfung angenommen werden kann. Der Einwand, E-Mails würden in so vielen verschiedenen sozialen Kontexten und Prozessen und in so unterschiedlicher Weise technisch realisiert und geschützt, dass kein typischer Geschehensablauf festgestellt werden könne[1605], überzeugt allerdings nicht. Unabhängig von den vorgenannten Aspekten werden die Stationen einer E-Mail-Generierung und deren Versendung gleich sein. Welche sozialen Kontexte, etwa das Schreiben einer privaten informellen E-Mail vom heimischen PC oder die E-Mail, die am Arbeitsplatz zur formellen Kommunikation mit Vorgesetzten, Kunden, unbekannten Dritten etc., sollen diese wesentlichen Merkmale der E-Mail-Kommunikation inwiefern verändern? Der erwähnte Schutz von E-Mail-Konten[1606] betrifft den Zugang zu einem E-Mail-Konto, sagt aber ebenfalls nichts über die Wahrscheinlichkeit eines Vorgangs oder dessen Typizität oder Atypizität aus.
Die ganz überwiegende Rechtsprechung lehnt das Vorliegen eines für den Anschein vorausgesetzten typischen Geschehensablaufs ab[1607], auch wenn das AG Bremen zumindest eine Computersabotage als jeder Lebenserfahrung widersprechend beurteilt hat.[1608] Eine solche Typizität lasse sich aufgrund der mangelnden Sicherheit des Internets nicht feststellen. Hinsichtlich Passwortsystemen begründet die Rechtsprechung diese Ablehnung mit dem mangelnden Schutz vor Drittzugriffen, der diesen in ihrer tatsächlich genutzten Form zu Eigen sei:

> *„Allein aus der Tatsache, dass das Gebot von einer Person abgegeben wurde, die das Passwort des Beklagten kannte, folgt nach Auffassung des Gerichts kein Anschein zu Lasten des Beklagten. Im Hinblick auf den derzeitigen Sicherheitsstandard der im Internet verwendeten Passwörter als solche und auf die Art ihrer Verwendung kann nicht der Schluss gezogen werden, dass der Verwender eines Passworts nach der Lebenserfahrung auch derjenige ist, auf den dieses Passwort ursprünglich ausgestellt wurde oder zumindest jemand, dem er die Kenntnis dieses Passworts ermöglicht hat.“*[1609]

Es seien – im konkreten Fall, der jedoch als beispielhaft für die Mehrzahl der E-Mail-Fälle stehen kann – keine Maßstäbe für die Verschlüsselung eines Passwortes festgelegt, ebenso wenig darüber, wie sicher das Passwort beim Betreiber „verwaltet“ werde.

[1604] Schmidt/Pruß/Kast, CR 2008, S. 272.

[1605] So Roßnagel/Pfitzmann, NJW 2003, S. 1211.

[1606] Wie oben unter 3.3.7.2 behandelt.

[1607] Z.B. LG Bonn, MMR 2002, S. 255; OLG Köln, JurPC Web-Dok. 364/2002, Abs. 1-15; LG Bonn, CR 2004, S. 218; LG Köln, BeckRS 2006 07259; OLG Hamm, NJW 2007, S. 611; AG Erfurt, JurPC Web-Dok. 71/2002; AG Karlsruhe-Durlach, MMR 2002, S. 64; LG Magdeburg, K&R 2005, S. 191; OLG Naumburg, Urt. v. 02.02.2004, 9 U 145/03; OLG Köln, JurPC Web-Dok. 48/2006, Abs. 1-21.

[1608] AG Bremen, Urt. v. 20.10.2005, 16 C 168/05, NJW 2006, S. 518, S. 519.

[1609] LG Bonn, MMR 2002, S. 256, bestätigt durch OLG Köln, JurPC Web-Dok. 364/2002; so auch LG Magdeburg, K&R 2005, S. 191; OLG Naumburg, Urt. v. 02.02.2004, 9 U 145/03; LG Bonn, CR 2004, S. 218; LG Köln, BeckRS 2006 07259.

Es seien Beispiele bekannt, in denen auch als besonders sicher geltende Sicherheitssysteme von unbefugten Dritten überwunden wurden.[1610] Ein online verwendetes Passwort sei weitaus größeren Zugriffsmöglichkeiten Dritter ausgesetzt als in den Btx-Fällen.[1611] Auch die Tatsache, dass weltweit täglich Millionen von Rechtsgeschäften per Internetauktion klaglos abgewickelt werden, lasse den Schluss auf die Verlässlichkeit des Mediums Internet im Allgemeinen und der Kommunikationsplattform Internetauktion im Besonderen nicht zu. Hierfür spreche ebenso wenig, dass ein unbefugter Dritter eher selten ein wirtschaftliches Interesse an dem Eingriff in eine Internetauktion haben werde[1612] – womit dieser Umstand zumindest zugestanden wird. *Ernst* stimmt dagegen der Annahme eines Anscheinsbeweises zumindest für bestimmte passwortgeschützte Plattformen zu. Voraussetzung sei, dass das Passwortsystem selbst eine gewisse Hindernisschwelle setze, also nicht ohne größeren Aufwand zu umgehen sei. Dass letztlich jedes System überlistet werden könne, solle nicht dazu führen, das gesamte Risiko des elektronischen Geschäftsverkehrs allein dem Adressaten aufzuerlegen.[1613] Dem ist nach oben Festgestelltem[1614] zuzustimmen. Dieser Differenzierung wird von der Rechtsprechung jedoch nicht gefolgt. Die Mitgliedschaft in einem Internetauktionshaus mit Mitgliedsnamen und Passwort führe nicht zur Überbürdung der Missbrauchsgefahr auf dieses Mitglied.[1615] Für eine Zurechnung nach den Grundsätzen des Handelns unter fremden Namen kraft Rechtsscheins mangele es im Hinblick auf den derzeitigen Sicherheitsstand im Internet an einem schutzwürdigen Vertrauen des Empfängers. Für die passwortgeschützte Teilnahme an einer Internetauktion unter fremden Mitgliedsnamen bestünde keine Anscheinsvollmacht.[1616] Anfang 2006 hat auch das OLG Köln unter Hinweis auf die *„nach wie vor unvermindert gegebenen Missbrauchsmöglichkeiten“* verneint, dass die Einrichtung eines E-Mail-Kontos und eines Benutzerkennworts einen schützenswerten Vertrauenstatbestand für den Empfänger zu schaffen vermag. Es stünde nicht fest, wer unter der in der Kommunikation angegebenen Bezeichnung „C“ gehandelt habe.[1617] Es ist jedoch zweifelhaft, ob die Schutzwürdigkeit des Vertrauens mit solch pauschalen Vermutungen abgelehnt werden kann.[1618] Auch das AG Bremen hat in einem Fall, in dem es ebenfalls um eine mögliche Rechtsscheinshaftung aufgrund Duldungs- oder Anscheinsvollmacht ging, zugestanden, dass ohne ein Vertrauen des Ge-

[1610] LG Bonn, MMR 2002, S. 257, das ferner auf die im konkreten Fall vorliegende Aussage des Betreibers (GMX) verweist, nach der nach dem derzeitigen Stand der Technik ein Schutz der übertragenen Daten nicht gewährt werden könne; OLG Köln, JurPC Web-Dok. 364/2002, OLG Hamm, NJW 2007, S. 611.

[1611] LG Bonn, MMR 2002, S. 257; OLG Köln, JurPC Web-Dok. 364/2002.

[1612] LG Bonn, CR 2004, S. 218, das auf die Grundsatzentscheidung des BGH, Urt. v. 07.11.2001, VIII ZR 13/01, NJW 2002, S. 363, zum Vertragsschluss im Rahmen einer Internetauktion verweist, in dem dieser das Risiko, dass deshalb ein Klageanspruch aus elektronischem Vertragsschluss wohl fast nie zu beweisen sei, nicht habe ausschließen wollen. Siehe auch oben unter 3.3.10.2.

[1613] Ernst, MDR 2003, S. 1093.

[1614] Siehe 3.3.9.

[1615] LG Bonn, CR 2004, S. 218.

[1616] LG Bonn, CR 2004, S. 218; OLG Köln, JurPC Web-Dok. 364/2002.

[1617] OLG Köln, JurPC Web-Dok. 48/2006, Abs. 16.

[1618] Siehe auch 3.3.10.4.

schäftsverkehrs in die Identität der übrigen Benutzer ein Handel unter Benutzernamen, wie er beispielsweise bei eBay stattfinde, ausgeschlossen wäre.[1619] Es fährt dann aber fort:

> *„Die technische Unsicherheit ermöglicht lediglich eine gelegentliche Hervorrufung des Rechtsscheins, die dem legitimierten Benutzer nicht zuzurechnen ist.“*[1620]

Es fällt auf, dass mit Ausnahme der oben dargestellten oder zitierten Erläuterungen, keine weiter reichenden Erklärungen für das Bestehen der Gefahr von Dritteingriffen und Manipulationen gegeben werden. Diese Gefahren werden als *„gerichtsbekannt“*[1621] dargestellt, beziehungsweise es wird auf die in den ersten hierzu ergangenen Urteilen verwendete Formulierung *„im Hinblick auf den derzeitigen Sicherheitsstandard der im Internet“*[1622] zurückgegriffen. Allein das LG Konstanz hat mithilfe eines Sachverständigen festgestellt, dass es die Gefahr der Fälschung und Manipulation *„nicht nur als theoretisch, sondern durchaus als real“* einschätze.[1623] In der Tat scheint gerade dies die entscheidende Frage: Ob die mit der Kommunikation über das Internet unbestreitbar verbundenen Gefahren als bloße absolute Ausnahme angesehen werden können, die den Anschein, eine E-Mail stamme von angegebenen Absender, nicht beseitigen kann. Das von *Mankowski* angeführte Argument der großen Anzahl E-Mails, bei denen der Anschein der Identität des Versenders der Wahrheit entspreche, spricht tatsächlich dafür, dass dieser Lebenssachverhalt sehr regelmäßig, üblich und häufig ist.[1624] Insofern sind Rückschlüsse auf einen logisch nachvollziehbaren Zusammenhang durchaus möglich, zumindest wo zusätzlich ein Passwortschutz vorhanden ist.[1625] Ob daraus der notwendige Grad an Gewissheit erwächst, ist aber zumindest nicht sicher. Statistische Angaben fehlen weitgehend.[1626] Es ist jedoch zweifelhaft, ob von einer bloß abstrakten Möglichkeit eines anderen Geschehensverlaufs ausgegangen werden kann. Vielmehr scheint, wie es das LG Konstanz schon in 2002 seinem Urteil zugrunde legte[1627], die Möglich-

[1619] AG Bremen, NJW 2006, S. 519.

[1620] AG Bremen, NJW 2006, S. 519.

[1621] So OLG Naumburg, Urt. v. 02.02.2004, 9 U 145/03.

[1622] LG Bonn, MMR 2002, S. 256; OLG Köln, JurPC Web-Dok. 364/2002; LG Magdeburg, K&R 2005, S. 191; OLG Naumburg, Urt. v. 02.02.2004, 9 U 145/03; LG Bonn, CR 2004, S. 218; LG Köln, BeckRS 2006 07259.

[1623] LG Konstanz, JurPC Web-Dok. 291/2002.

[1624] A.A. Klein, JurPC web-Dok. 198/2007, Abs. 59; auch Roßnagel/Pfitzmann, NJW 2003, S. 1211, die behaupten, die große Zahl ließe Rückschlüsse auf kausale Zusammenhänge nicht zu. Auf dieser Stufe geht es jedoch zunächst um die Frage der Wahrscheinlichkeit. Dieses Argument müsste i.Ü. auch gegen jede Art (richterlicher) Anscheinsbeweise angeführt werden. Die hohe Wahrscheinlichkeit ist Grund für die für den Anschein notwendige Gewissheit. Deshalb kommt es auch nicht, wie von Roßnagel/Pfitzmann behauptet, auf einen logisch nachvollziehbaren Zusammenhang zwischen feststehendem Erfolg (E-Mail) und Ursache (Autorenschaft) *„aufgrund bestimmter Sicherheitsmaßnahmen“* an.

[1625] So auch Ernst, MDR 2003, S. 1092.

[1626] Laut Frankfurter Allgemeine Zeitung, www.faz.net, v. 04.07.2008 hat das Bundeskriminalamt jedoch im Jahr 2007 eine Zunahme von Diebstählen von Passwörtern (Phishing) um etwa 20 Prozent auf rund 4200 Fälle registriert; die Zahl der nicht registrierten Fälle mag weitaus höher liegen.

[1627] LG Konstanz, JurPC Web-Dok. 291/2002, und oben.

keit des Dritteingriffs und der Manipulation eine wenn auch unwahrscheinliche, so doch ernsthafte Möglichkeit zu sein.[1628] Auch das OLG Brandenburg hat (indirekt) die grundsätzliche Unsicherheit des Systems hinsichtlich eines Identitätsmissbrauchs auch bei passwortgeschützten Internetauktionsplattformen festgestellt.[1629] Zutreffend deutet aktuell *Wietzorek* in diesem Zusammenhang auf die „Qualität" der von Kriminellen gefälschten E-Mails hin, die mittlerweile so täuschend echt aussähen, dass auch ein verständiger Nutzer davon ausgehen müsse, diese E-Mail stamme von dem vermeintlichen Versender. Richtig ist auch, dass neuere Viren sich der auf dem befallenen Computer befindlichen Adressbüchern bedienen, um sich mittels des befallenen Computers selbst zu versenden.[1630] Der als Grundlage des Anscheinsbeweises anzunehmenden Typizität muss man in der von *Mankowski* geforderten pauschalen Form nach alledem also zumindest skeptisch gegenüber stehen. In jedem Fall muss die Einzelfallbetrachtung unter Einschluss der weiteren Umstände und technischer Beweise Grundlage sein, die dann gegebenenfalls zu einem Beweis des Anscheins führen kann.

3.3.10.7 Erschütterung des Anscheins - qualifiziertes Bestreiten

Dennoch: Eine mittels Anscheinsbeweis erreichte Überzeugung des Gerichts beruht auf einem als typisch angesehenen Geschehensablauf. Das hierfür notwendige Maß an Wahrscheinlichkeit des Geschehensablaufs wird häufig mit der Formel „wenn – fast immer" beschrieben.[1631] Der Beweis wird dabei also aufgrund einer geringeren Wahrscheinlichkeit erreicht als für die volle Überzeugung des Gerichts erforderlich. Deshalb kann die auf einem Anscheinsbeweis gründende Überzeugung des Gerichts relativ leicht erschüttert werden. Um den Anscheinsbeweis zu widerlegen, braucht der Beweisgegner nicht den vollen Beweis des Gegenteils führen. Der Anschein muss lediglich erschüttert werden durch Tatsachen, die die ernsthafte Möglichkeit eines anderen als des der allgemeinen Erfahrung entsprechenden Geschehensablaufs ergeben. Ernsthaft ist eine solche Möglichkeit, wenn der andere Geschehensablauf nicht erheblich unwahrscheinlicher ist als der typische. Die diese Möglichkeit ergebenden Tatsachen sind zur vollen Überzeugung des Gerichts zu beweisen.[1632]

[1628] So auch aktuellere Stimmen wie Borges, NJW 2005, S. 3313; Kind/Werner, CR 2006, S. 360, m.w.N. und Verweis auf die Homepage der Arbeitgruppe Identitätsschutz im Internet http://www.a-i3.org; Wietzorek, Michael, „Der Beweis des Zugangs von Anhängen in E-Mails", MMR 2007, S. 156-159, S. 157. Auch Storr, MMR 2002, S. 582, der in Bezug auf den elektronischen Verwaltungsakt einen gesicherten Erfahrungssatz dahingehend, dass eine gewöhnliche E-Mail den Empfänger überhaupt erreicht, verneint. Im Vergleich zum Anscheinsbeweis bei postalischen Zusendungen seien im Internet weder die transportierenden Unternehmen noch der Weg, den die elektronische Mitteilung nehmen wird, vorab feststellbar. Mangels Erfahrungssatz ließe auch ein Vermerk über Abgang einer elektronischen Mitteilung bei der Behörde keinen entsprechenden Anscheinsbeweis zu.

[1629] OLG Brandenburg, MMR 2006, S. 107-110.

[1630] Wietzorek, MMR 2007, S. 157 mit weiteren Darstellungen.

[1631] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 493, m.w.N.; Ernst, „Trojanische Pferde und die Telefonrechnung", CR 2006, S. 590-594, S. 594.

[1632] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 493, 494 m.w.N.

Dass eine solche reale Möglichkeit in der oben beschriebenen Gefahr des Dritteingriffs grundsätzlich existiert, steht fest. Hier hätte der Beweisgegner nur für den jeweiligen Einzelfall darzulegen, weshalb der als typisch angenommene Geschehensablauf im Sinne obigen Anscheins nicht vorliegen kann. Sofern im Einzelfall nur die Erschütterung des Anscheins verlangt ist, sollte dies für den Beweisgegner, hier den E-Mail-Adressinhaber, ohne wesentliche Schwierigkeiten möglich sein. Dann obliegt es wieder dem Beweisführer, den vollen Beweis dafür zu erbringen, dass eine elektronische Erklärung mit ihrem konkreten Inhalt vom Adressinhaber versendet wurde. Der Beweisgegner sollte sich aber – wie oben bereits mehrfach angemerkt – nicht allein allgemein und pauschal auf die mehr oder weniger wahrscheinlichen Gefahren der elektronischen Kommunikation über das Internet oder die Manipulierbarkeit elektronischer Dokumente berufen dürfen. Ein substantiiertes, schlüssiges Vorbringen – beziehungsweise ein qualifiziertes Bestreiten – bezogen auf den konkreten Fall sollte dem Beweisgegner dabei abverlangt werden dürfen.[1633] Ein Anscheinsbeweis schneidet eine solche substantiierte Verteidigung nicht ab, verlagert aber die Last sachgerechter Weise zu jener Partei, welche die besseren Informationen über den Geschehensablauf hat.[1634] Einen auch für die Gerichte bedenkenswerten Aspekt führt *Ernst* aus, wenn er sagt, dass zwar eine immense Gefahr der Infizierung des eigenen Computers mit Trojanern und Viren beim Internetbesuch bestehe, gleichzeitig aber die Kenntnis hierüber bei den Nutzern steige und Schutzprogramme wie Firewalls und Anti-Viren-Programme auch für Privatnutzer vielfach kostenfrei zu haben und einfach zu bedienen seien. Folglich könne sich derjenige, der dauernd online sei, nicht ohne weiteres darauf berufen, er verstehe davon nichts. Vielmehr seien ihm vorgenannte Sicherheitsvorkehrungen zuzumuten.[1635] Dies führt – unabhängig von der Annahme eines Anscheinsbeweises – für die Gerichte dazu, dass der Vortrag einer bloß theoretischen Möglichkeit einer Manipulation ohne Nennung konkreter Anknüpfungspunkte nicht ausreichen kann, um zur geforderten vollen Überzeugung des Gerichts von der Möglichkeit des atypischen Ablaufs zu gelangen.[1636]

3.3.11 §§ 439 ff. analog – Pflicht zum substantiierten Vortrag und Bestreiten

Ob eine in Urschrift vorgelegte und mangelfreie Privaturkunde im Prozess als echt anzuerkennen ist, entscheiden die Partien. Eine Vermutung wie bei öffentlichen Urkunden nach § 437 Abs. 1 ZPO gibt es hier nicht. Mit der Vorlage der Urkunde behauptet der Beweisführer ihre Echtheit. Dazu besteht eine Erklärungspflicht des Gegners, die sich bei unterschriebenen Urkunden auf die Echtheit der Unterschrift beziehen muss, siehe § 439 Abs. 1 und 2 ZPO.[1637] Gibt der Gegner – trotz Aufforderung – keine Erklärung ab, so gilt die Echtheit nach Abs. 3 als zugestanden. Ebenso ist es laut § 138 Abs. 3,

[1633] So auch Winter, MMR 2002, S. 837.

[1634] So zutreffend Mankowski, „Anmerkung zu LG Bonn, Urt. v. 19.12.2003 – 2 O 472/03 – Sofortkauf-Option bei eBay“, MMR 2004, S. 182-183, S. 182.

[1635] Ernst, CR 2006, S. 593.

[1636] So im Ergebnis auch Ernst, CR 2006, S. 594.

[1637] Huber in Musielak, § 439, Rn. 1.

wenn er sich mit Nichtwissen erklärt, obwohl behauptet wird, die Urkunde stamme von ihm. Das ausdrückliche oder stillschweigende oder bei einer fremden Urkunde mit Nichtwissen zulässige Bestreiten der Echtheit erfordert dann den vollen Beweis dazu.[1638] Elektronische Dokumente sind dagegen im Gerichtsverfahren keine Privaturkunden, sondern allein als Augenscheinsbeweis zu behandeln. Die für Urkunden bestehenden Erklärungspflichten über die Echtheit, hier die Urheberschaft, einer Urkunde sind auf sie ebenso wenig anwendbar wie die für Urkunden existierende Vermutung der Echtheit. Dennoch scheint das Vertrauen in elektronische Dokumente ähnlich schutzwürdig wie jenes in Urkunden. Es liegt also nahe, eine analoge Anwendung des § 439 Abs. 1 ZPO zu diskutieren. Dabei würde dem vermeintlichen Urheber des elektronischen Dokuments die Erklärungslast zufallen. Dieser müsste sich substantiiert zur Echtheit des elektronischen Dokuments erklären, also dazu, ob er dieses verfasst hat. Wie *Borges* zutreffen annimmt, ist dies dem vermeintlichen Urheber auch zumutbar, weil er diesen Umstand typischerweise erkennen kann,[1639] siehe auch vorstehende Überlegungen zur Erschütterung des Anscheinsbeweises.[1640]

In eine ähnliche Richtung zielt folgende Überlegung von *Noack* und *Kremer*, die angeführt wird, um deutlich zu machen, dass ein wie oben dargestellter Anscheinsbeweis überflüssig ist: Die wesentlichen Tatsachen, anhand derer sich ein Dritteingriff oder eine Manipulation darlegen und beweisen ließe, lägen im Wahrnehmungsbereich des vermeintlichen Urhebers, beispielsweise des E-Mail-Adressinhabers oder des Inhabers eines anderen Konten auf einer Internetplattform. Schon deshalb sei von diesem ein qualifizierter Vortrag beziehungsweise ein substantiiertes Bestreiten zu verlangen, wolle er unter Hinweis auf einen Missbrauch zum Beispiel von den aus der elektronischen Kommunikation sich ergebenden vertraglichen Pflichten befreit werden.[1641] Richtigerweise sollte der grundsätzlich besser informierten Partei die Substantiierungslast auferlegt werden. Denn schon unter § 138 ZPO mindert sich die Substantiierungslast für die bestreitende Partei, wenn sie keinen Einblick in die behaupteten Vorgänge hat. Auch können die Substantiierungsanforderungen an die behauptungs- und beweisbelastete Partei dann reduziert sein mit der Folge, dass einfaches Bestreiten durch den zwar besser informierten, aber nicht risikobelasteten Gegner dann nicht genügt.[1642] Den Maßstab der jeweiligen Substantiierung kann und muss das Gericht im Einzelfall bestimmen. Es gibt jedenfalls keinen sinnfälligen Grund für die Gerichte, sich mit einem pauschalen Hinweis auf mögliche Gefahren der Manipulation zufrieden zu geben. Dies machte überdies das Konstrukt der analogen Anwendung des § 439 Abs. 1 ZPO überflüssig. Ein substantiiertes Bestreiten kann gerade unter Zuhilfenahme und Einbeziehung ergänzender Beweise und Indizien geschehen, wird oftmals sogar auf diese angewiesen sein. Leider ist dieser Weg von den Gerichten bisher noch nicht beschritten worden. Es zeigt sich aber, dass es grundsätzlich auch nach deutschem Recht und den hier bestehenden

[1638] Huber in Musielak, § 439, Rn. 2.

[1639] Borges, *Verträge im elektronischen Geschäftsverkehr*, S. 482.

[1640] 3.3.10.7.

[1641] So Noack/Kremer, AZW Reihe Nummer 2004_12_02 (Dec 27, 2004).

[1642] Stadler in Musielak, § 138, Rn. 10.

gesetzlichen Vorschriften möglich und zweckmäßig ist, die von den englischen und US-amerikanischen Gerichten für maßgeblich erachteten Aspekte zukünftig in größerem Umfang zu berücksichtigen bei der Beurteilung der Rechtswirksamkeit und Urheberschaft einfacher elektronischer Signaturen und elektronischer Erklärungen in Textform. Das Verlangen nach Substantiierung hat jedoch seine Grenzen: es bleibt das grundsätzliche Problem des (substantiierten) Bestreitens des von der Gegenseite behaupteten Zugangs einer Erklärung, also des Nichtzugangs. Im Falle des mutmaßlichen Empfängers, der behauptet, eine Erklärung nicht erhalten zu haben, kann eine Substantiierung des Beweisantrags nicht erwartet werden.[1643]

3.3.12 Bestimmende Schriftsätze per Computer-Fax und E-Mail

Berücksichtigung sollen nicht zu letzt die Urteile deutscher Gerichte zur Zulässigkeit von per Telefax und vor allem mittels Computer-Fax an das Gericht übermittelten bestimmenden Schriftsätzen finden. Diese Rechtsprechung ist oben bereits erwähnt worden, soll jedoch hier nochmals dargestellt werden, da die Begründungen der Gerichte in zweierlei Hinsicht für diese Arbeit befruchtend sind: Zum einen werden die Funktion der verfahrensrechtlichen Formvorschriften durch die Rechtsprechung so gefasst, dass sie Parallelen zu den der Textform zugesprochenen Funktionen aufweisen. Zum anderen nutzen die Gerichte dabei vielfach Argumente, die von den englischen und US-amerikanischen Gerichten ebenfalls verwendet wurden und werden, um die Erfüllung von Schriftformerfordernissen wie der Statute of Frauds (*signature* und *writing*) durch vergleichbare elektronische Kommunikationen und E-Mails zu begründen. Nicht zuletzt ist auf die Ähnlichkeiten der Kommunikation per Computer-Fax und E-Mail und die dabei verschwimmenden (technischen) Grenzen einzugehen und zu überlegen, ob die Computer-Fax-Rechtsprechung die Diskussion um die durch die Textform zu erfüllenden Funktionen und ihre Beweiskraft befruchten kann.
Bestimmende Schriftsätze müssen gemäß den einschlägigen Verfahrensvorschriften grundsätzlich in Schriftform bei Gericht eingereicht werden. Laut § 130 Nr. 6 ZPO beispielsweise sollen die vorbereitenden Schriftsätze die Unterschrift der Person, die den Schriftsatz verantwortet, enthalten, bei Übermittlung per Telefax die Wiedergabe der Unterschrift in der Kopie (Telekopie). Den Zweck dieser Schriftformerfordernisses beschrieb der Gemeinsame Senat der obersten Gerichtshöfe des Bundes (GmS-OGB) im Jahr 2000 wie folgt:

> *„Die Schriftlichkeit soll gewährleisten, dass aus dem Schriftstück der Inhalt der Erklärung, die abgegeben werden soll, und die Person, von der sie ausgeht, hinreichend zuverlässig entnommen werden können. Außerdem muss feststehen, dass es sich bei dem Schriftstück nicht nur um einen Entwurf handelt, sondern*

[1643] So auch Storr, MMR 2002, S. 582 in Bezug auf den Zugang eines elektronischen Verwaltungsakts, dessen Zugang (und den Zeitpunkt des Zugangs) gemäß § 41 Abs. 2 Hs. 2 VwVfG im Zweifel die Behörde nachzuweisen hat. Ein Anscheinsbeweis könne daher nur dann zulässig sein, wenn nicht der Zugang, sondern der Zeitpunkt des Zugangs fraglich sei.

dass es mit Wissen und Willen des Berechtigten dem Gericht zugeleitet worden ist.“[1644]

Schon hier wird zunächst deutlich, dass die Anforderungen der prozessualen Schriftlichkeitserfordernisse unter denen des § 125 BGB liegen. Sie haben lediglich den Charakter einer Sollvorschrift.[1645] Auch das Bundesverfassungsgericht (BVerfG) führte 2002 zur einfachen Schriftform des § 410 Abs. 1 StPO, die keine Unterzeichnung durch einen Verteidiger oder Rechtsanwalt verlangt, und zur Notwendigkeit einer handschriftlichen Unterzeichnung des Schriftstücks aus, dass es nach der Zweckbestimmung dieses Schriftformerfordernisses genüge, wenn aus dem Schriftstück ansonsten in einer jeden Zweifel ausschließenden Weise ersichtlich sei, von wem die Erklärung herrührt und dass kein bloßer Entwurf vorliegt.[1646] Die Einreichung solcher bestimmenden Schriftsätze mittels (auch telefonisch aufgegebenem) Telegramm und Fernschreiben (Telex) sowie Telefax und sogar per Btx ist daher seit langem anerkannt. Im Falle des Telegramms sei, so der GmS-OGB, allein die auf Veranlassung des Absenders am Empfangsort erstellte, für den Adressaten bestimmte Telegrammurkunde maßgeblich, so dass es nicht darauf ankomme, ob diese auf einer „Unterschrift“ beruht, die am Absendeort aufgenommen und vom Erklärenden unterzeichnet worden ist.[1647] Zur Einreichung per Btx führte das Bundesverwaltungsgericht (BVerwG) bereits 1995 aus:

„Da ... Verfahrensvorschriften ... nicht Selbstzweck sein dürfen, schließt das Erfordernis der Schriftlichkeit die eigenhändige Unterschrift nicht um ihrer selbst Willen, sondern deshalb ein, weil in der Regel allein sie die Verlässlichkeit der Eingabe sicherstellt. Wo sich im Einzelfall dasselbe Ergebnis auf andere Weise feststellen lässt, sind Ausnahmen möglich und in der Rechtsprechung auch seit langem zugelassen. Selbst das vollständige Fehlen der Unterschrift schließt danach die Formgerechtigkeit der Klage nicht schlechthin aus, wenn sich aus anderen Anhaltspunkten eine der Unterschrift vergleichbare Gewähr für die Urheberschaft und den Willen, das Schreiben in den Verkehr zu bringen, ergeben und dem Bedürfnis nach Rechtssicherheit genügt ist. Entscheidend ist, ob sich aus dem bestimmenden Schriftsatz allein oder in Verbindung mit den ihn begleitenden Umständen die Urheberschaft und der Wille, das Schreiben in den Verkehr zu bringen, hinreichend sicher ergeben, ohne dass darüber Beweis erhoben werden müsste.“[1648]

[1644] GmS-OGB, Beschl. v. 05.04.2000, NJW 2000, S. 2340, 2341.

[1645] Stadler in Musielak, § 130, Rn. 1.

[1646] BVerfG, Beschl. v. 04.07.2002, 2 BvR 2168/00, NJW 2002, S. 3534, 3535.

[1647] GmS-OGB, NJW 2000, S. 2341.

[1648] BVerwG, Beschl. v. 19.12.1995, 5 B 79/94, NJW 1995, S. 2121, 2122 zu Klageerhebung mittels Btx-Mitteilung gem. § 8 Abs. 1 S. 1 VwGO; so auch Bundessozialgericht (BSG), Beschl. v. 15.10.1996, 14 BEg 9/96, NJW 1997, S. 1254, 1255. Das LAG Mecklenburg-Vorpommern (LAG MV), Beschl. v. 21.08.1997, 1 Ta 18/97, NZA-RR 1998, S. 32, 33, hat später in Bezug auf § 130 Nr. 6 ZPO dazu ausgeführt: *„Es ist zunächst davon auszugehen, dass ... vorbereitende Schriftsätze eine Unterschrift enthalten sollen. Obwohl im Gesetz eine bloße Sollvorschrift und kein zwingendes Formerfordernis formuliert ist, ist schon das RG davon ausgegangen, dass ...* [die Unterschrift] *handschriftlich zu erfolgen hat. Die*

Als solche Umstände sollen die Benennung von Verfahrensbeteiligten, Verfahrensgegenstand und Prozessziel in der Klageschrift sowie die Angabe der Codenummer des Teilnehmeranschlusses der Klägerin nebst Absenderanschrift gelten. Diese ließen eine Absendung durch einen Dritten oder die versehentliche Übersendung eines internen Vorgangs durch die Klägerin selbst als ausgeschlossen erscheinen.[1649] Diese Ausführungen gleichen denjenigen englischer und US-amerikanischer Gerichte zur *signature* bei Btx und ähnlichen „neuen" Technologien.[1650] Zuletzt war auch die Übermittlung per Computerfax, also des mittels PC-Modem unmittelbar an das Telefax-Empfangsgerät des Gerichts geleiteten Schriftsatzes, als formgerechte Einhaltung verfahrensrechtlicher Formvorschriften akzeptiert worden[1651], auch wenn das Bundessozialgericht (BSG) zunächst feststellte:

> *„Der eingescannten und mittels bloßen Tastendrucks eingefügten Unterschrift kann im Rechtsverkehr keine andere Bedeutung zukommen als der maschinenschriftlichen Angabe des Namens. Sie hat keinen Beweiswert für die Frage, ob der Unterzeichner auch Urheber des Schriftstücks ist und dieses bewusst in den Verkehr gebracht hat."*[1652]

Denn, wie das LAG Mecklenburg-Vorpommern (LAG MV) zutreffend ausführt:

> *„Es ist ... nicht ohne weiteres ersichtlich, ob es sich dabei um die telekopierte Wiedergabe einer auf der Vorlage handschriftlich vollzogenen Unterschrift handelt oder um eine mittels Scanner in den PC eingegebene und einem im PC ohne geschriebene Vorlage erstellten Telefax auf technischem Wege beigefügte Unterschrift. ... Sie wäre nicht eigenhändig,..."*[1653]

---

technische Entwicklung hat es allerdings sodann schon früh als notwendig erscheinen lassen, von diesem von der Rechtsprechung postulierten strengen Schriftformerfordernis Ausnahmen zu gestatten, um die rechtzeitige Übermittlung fristgebundener Erklärungen durch Zuhilfenahme neuer technischer Übertragungsmittel zu ermöglichen.".

[1649] BVerwG, NJW 1995, S. 2122; so auch LAG MV, NZA-RR 1998, S. 32, 34, dass hierzu ausführt: *„In der Tat ist bei Aufgabe eines Telegramms ... am wenigsten nachvollziehbar, dass das bei Gericht eingehende Telegramm auch tatsächlich von dem darin angegebenen Absender herrührt, während bei den heute üblich gewordenen technischen Übermittlungsformen, also etwa der Übersendung eines Telefaxes unmittelbar vom Telefaxgerät des Absenders an dasjenige des Gerichts wie auch bei einer Übersendung aus einem mit einem Telefaxmodem versehenen PC, die Identität des Absenders durch den Ausdruck einer Absenderkennung oder Telefaxnummer zusätzlich kenntlich gemacht wird."*.

[1650] Siehe unter 1.3.2.4 und 1.3.3.4, bspw. *Morton v. Copeland* (1855) 16 C B, S. 516; *Tourret v. Cripps* (1879) 48 L J Ch, S. 567; 27 WR; *Bridges (Town Clerk of Cheltenham) v. Dix* (1890-91) 7 TLR, S. 215; *Goodman v. J. Eban Limited* [1954] 1 Q.B. S. 550; *Hessenthaler v. Farzin*, 564 A.2d S. 990 (Pa.Super. 1989); *United States of America v. Siddiqui*, 235 F.3d 1318 (11th Cir. 200) (*federal*).

[1651] BSG, NJW 1997, S. 1254, 1255 zur Zulässigkeit des Computerfax in Bezug auf das Schriftformerfordernis des § 151 Abs. 1 SGG; a.A. BAG, Urt. v. 27.03.1996, 5 AZR 576/94, NJW 1996, S. 3164, in Bezug auf § 130 ZPO.

[1652] BSG, NJW 1997, S. 1255.

[1653] *„..., weil das Wesen der Handschriftlichkeit darin besteht, dass die Bewegung des Schreibens als solche durch die natürliche Person auf das Schriftstück übertragen werden muss."* LAG MV, NZA-RR 1998, S. 33.

Die Urheberschaft der Klägerin ließe sich dennoch dem Umstand entnehmen, dass sie den Schriftsatz mit ihrem Namen und ihrer Anschrift abgeschlossen habe, so im Falle des BSG, oder aber die Person des Erklärenden wie im Falle des GmS-OGB in der Regel dadurch eindeutig bestimmt sei, dass eine Unterschrift eingescannt sei, sowie durch die Hinzufügung des Hinweises „*dieser Brief wurde maschinell erstellt, wird nicht eigenhändig unterschrieben*“, mit dem deutlich gemacht würde, dass aus technischen Gründen auf eine eigenhändige Unterschrift verzichtet würde oder die Erklärung wegen der gewählten Übertragungsform nicht unterzeichnet werden könne.[1654] Dadurch kann also die Authentizität des Verfassers bei eingescannter Unterschrift in gleicher Weise festgestellt werden wie bei einem normalen Telefax[1655], insbesondere durch die Berücksichtigung anderer in der Erklärung enthaltener Informationen. Durch diesen Erklärungsabschluss erfüllt ein solcher Schriftsatz im Übrigen auch die Form des § 126b BGB. Der GmS-OGB weiter:

> *„Diese Umstände sprechen dagegen, dass die Mitteilung unbewusst oder versehentlich in den Verkehr gebracht wurde. Nach der Lebenserfahrung bedient sich ein Rechtsmittelführer der modernen Kommunikationsmöglichkeiten gerade zur Vermeidung sonst drohender Fristüberschreitungen.“*[1656]

Auch der Wille, einen solchen Schriftsatz dem Gericht zuzuleiten, könne also in aller Regel nicht ernsthaft bezweifelt werden.[1657] Der BGH hat dies neuerlich im Fall eines Computerfax bestätigt, dem ein persönlich unterzeichneter Ausdruck einer Berufungsbegründungsschrift, der anschließend gescannt und elektronisch übermittelt wurde, zugrunde lag:

> *„Dies stellt eine lediglich äußerliche (technische, nicht aber inhaltliche) Veränderung des von dem Prozessbevollmächtigten durch seine eigenhändige Unterschrift autorisierten bestimmenden Schriftsatzes dar und ändert deshalb nichts daran, dass der fristgerecht eingegangene Schriftsatz auf Veranlassung des Prozessbevollmächtigten dort als körperliche Urkunde erstellt worden ist.“*[1658]

Hier finden sich weitere deutliche Ähnlichkeiten zu den Urteilen und Begründungen englischer und US-amerikanischer Gerichte zur Akzeptanz einfachster Formen der

---

[1654] BSG, NJW 1997, S. 1255; GmS-OGB, NJW 2000, S. 2341.

[1655] So zusammenfassend Splittgerber, „Die elektronische Form von bestimmenden Schriftsätzen“, CR 2003, S. 23-28, S. 25, der zudem die Frage aufwirft, inwieweit der Empfänger den Unterschied zu einem normalen Telefax erkennen könne, und der darauf hinweist, dass die Gefahr der Fälschung oder Abänderung bei der Übertragung auf Grund der gleichen Übertragungsweise von Computer- und normalem Fax genau die gleiche sei. Zur rechtlichen Qualität gescannter Dokumente siehe z.B. Roßnagel, „Die Bedeutung gescannter Dokumente“, NJW 2006, S. 2145-2150, der zu der Beurteilung kommt, dass auch mit gescannten Dokumenten Beweis geführt werden könne, der Ausgang der Beweisaufnahme jedoch weniger sicher und das Ergebnis weniger gut vorhersehbar sei wie bei einem Urkundsbeweis, siehe S. 2149.

[1656] BSG, NJW 1997, S. 1255; auch BVerfG, NJW 2002, S. 3535.

[1657] GmS-OGB, NJW 2000, S. 2341.

[1658] BGH, Beschl. v. 14.01.2008, II ZR 85/07, NJW 2008, S. 1199-1201, S. 1200.

signature beispielsweise gemäß den Statutes of Frauds. So stellt etwa in *Re a debtor* die Telekopie eine Reproduktion der Unterschrift dar, weshalb diese Kopie ihrerseits als unterschrieben gilt. Selbst in Fällen, in denen die Signatur digitalisiert und danach dem Fax beigefügt wird, so dass das Fax die erste verkörperte Kopie dieses Dokuments darstellt, soll dieses Dokument als signiert gelten.[1659] Wie dort mehr auf den Willen des Erklärenden zu Signieren als auf die Form der Signatur abgestellt wird[1660], muss hier vor allem der Wille, das Schreiben in den Verkehr zu bringen, feststehen. Wie dort kann auf diesen Willen insbesondere auch aus den Umständen und also aus Indizien geschlossen werden, und diese Funktion nicht allein durch eine (eigenhändige) Unterzeichnung gesichert werden.[1661] Allein, in England und den USA findet sich diese Begründung nicht lediglich in Bezug auf den begrenzten Anwendungsbereich prozessualer Schriftformerfordernisse, sondern hinsichtlich nahezu aller, insbesondere solche der Statutes of Frauds, die sogar eine besondere Beweisfunktion haben. Hält man sich die oben dargestellte Entwicklung der *common law*-Rechtsprechung und die entsprechenden Begründungen dazu vor Augen, warum auch einfachste *signatures* akzeptiert wurden, so weisen auch die weiter gehenden Ausführungen der deutschen Gerichte beachtliche Parallelen dazu auf, siehe das LAG MV:

> *„Eingedenk der vom* [Reichsarbeitsgericht] *schon 1929 formulierten Erkenntnis, dass sich auch die Rechtsprechung den technischen Fortschritten anschließen und anpassen muss, würde es eine durch nichts zu begründende Ungleichbehandlung darstellen, die Erleichterungen der Übermittlung von Erklärungen im Telegrammverkehr nicht auch auf die im Zuge der Weiterentwicklung der Nachrichtentechnik ermöglichten sonstigen Übertragungsmittel in gleicher Weise anzuwenden.*“[1662]

Dies entspräche der langjährigen Entwicklung dieser Rechtsprechung, die dem technischen Fortschritt auf dem Gebiet der Telekommunikation Rechnung trüge.[1663] Das Argument der (wirtschaftlichen) Notwendigkeit der Anpassung des Rechts an den technischen Fortschritt und der Vereinfachung des Signiervorganges taucht bereits in frühen Urteilen in England und den USA zum *writing* und der *signature* auf.[1664] Gleiches gilt

[1659] *Re a debtor (No. 2021 of 1995), Ex p, Inland Revenue Commiccioners v. The debtor; Re a debtor (No. 2022 of 1995), Ex, Inland Revenue Commissioners v. The debtor* [1996] 2 All E.R. 1208, S. 341, 345, ausführlich dargestellt unter 1.3.2.4; aber auch *Madden v. Hegadorn*, 565 A.2d, S. 725 (N.J. Sper.L 1989), 236 N.J.Super. 280, affirmed 571 A.2d 296 (N.J. 1989), 239 N.J. Super 268, dargestellt unter 1.3.3.4.

[1660] Siehe oben 1.3.2.3, 1.3.2.6, 1.3.3.3, 1.3.3.6, 2.4.5 und 2.5.6.

[1661] Wie vorstehend.

[1662] LAG MV, NZA-RR 1998, S. 32, 34, ähnlich auch GmS-OGB, NJW 2000, S. 2341.

[1663] GmS-OGB, NJW 2000, S. 2341.

[1664] Z.B. in in den englischen Fällen *Goodman v. J. Eban Limited* [1954] 1 Q.B. S. 550, S. 557, *British Estate Investment Society Ltd. v. Jackson (H M Inspector of Taxes)* (1954-1958) 37 Tax Cas, S. 79, S. 86; [1954] TR 397; 35 ATC 413; 50 R & IT 33, *Godwin v. Francis* (1870) LR 5 CP 295; 22 LT Rep NS 338, *McBlain v. Cross* (1872) LT 804 (Telegramm), *Clipper Maritime Ltd. v. Shirlstar Container Transport Ltd., The Anemone*, [1987] 1 Lloyd's Rep., S. 546, 556 (Telex), *Re a debtor (No. 2021 of 1995), Ex p, Inland Revenue Commiccioners v. The debtor; Re a debtor (No. 2022 of 1995), Ex, Inland Revenue Commissioners v. The debtor* [1996] 2 All E.R. 1208, S. 345 (Fax), sowie in den USA bei-

für das Argument der Gleichbehandlung mit der Sendung per telefonisch aufgegebenem Telegramm, bei dem auch keine schriftliche Vorlage auf Papier entstünde[1665], sowie für folgende Ausführungen:

> *„Es erscheint auch nicht sinnvoll, zu fordern, dass von der technischen Möglichkeit Gebrauch zu machen ist, die Unterschrift des Absenders etwa mittels eines Scanners in den PC einzulesen, in die Datei, in der der zu übermittelnde Schriftsatz erstellt wird, zu übertragen und so dem bei Gericht eingehenden Schriftstück als scheinbare Unterschrift beizufügen, ... Da für das Gericht ohnehin nicht erkenntlich ist, ob die Beifügung der Unterschrift auf technischem Wege tatsächlich von dem im Schriftstück angegebenen Absender veranlasst ist, würde hierin lediglich eine Erschwernis der technischen Übermittlung liegen, die eine erhöhte Echtheitsgewähr letztlich doch nicht mit sich brächte."* [1666]

Darauf, dass die Unterschrift lediglich in einer anderen Schrifttype „geschrieben" und später ausgedruckt wird, könne es, so das Finanzgericht Hamburg, für die Frage, ob der Zweck der Schriftform gewahrt ist, nicht ankommen.[1667] Maßgeblich für die Beurteilung der Wirksamkeit des elektronisch übermittelten Schriftsatzes sei nicht eine etwa beim Absender vorhandene Kopiervorlage oder eine nur im Textverarbeitungs-PC befindliche Datei, sondern allein die auf seine Veranlassung am Empfangsort erstellte

---

spielsweise in *State of North Carolina v. Watts*, 289 N.C. 445, 222 S.E.2d, S. 389, 392, *Leesley Bros. v. A. Rebori Fruit Co.*, 162 Mo.App. 195, 144 S.W. 138, *La Mar Hosiery Mills, Inc., v. Credit and Commodity Corporation*, 28 Misc.2d 764, 216 N.Y.S.2d 496, 72 Am.Jur.2d, *Joseph Denunzio Fruit Co., v. Crane*, 79 F.Supp. 117 *reversed on other grounds upon rehearing* 89 F.Supp. 962 (Telegramm), *Madden v. Hegadorn*, 565 A.2d, S. 725 (N.J. Sper.L 1989), 236 N.J.Super. 280, affirmed 571 A.2d 296 (N.J. 1989), 239 N.J. Super 268, *Parma Tile Mosaic & Marble Co., Inc. v. Estate of Fred Short, d/b/a Sime Construction Co.*, 155 Misc.2d 950, 590 N.Y.S.2d 1019 (Supp. 1992), *motion for summary judgement affirmed*, 209 A.D.2d 495, 619 N.Y.S..2d S. 628 *reversed* 663 N.E.2d 633 (N.Y. 1996), 640 N.Y.S.2d 477 (Ct.App. 1996), 87 N.Y.2D 524, S. 635 (alle bzgl. Fax); sämtlich oben dargestellt unter 1.3.2.4, 1.3.2.6, 1.3.3.4, 1.3.3.6, 2.4.5 und 2.5.6.

[1665] LAG MV, NZA-RR 1998, S. 32, 34.

[1666] LAG MV, NZA-RR 1998, S. 32, 34; so auch Finanzgericht (FG) Hamburg, Zw.Urt. v. 21.11.2000, II 137/00, NJW 2000, S. 992: denkbar sei, dass die Unterschrift aus Anlass der Übermittlung des Schriftsatzes eingescannt wurde, oder dass die einmal eingescannte Unterschrift als Textbaustein gespeichert wurde, um bei Bedarf in ein Dokument kopiert zu werden, und: *„Über die Authentizität des Schriftstücks und die Person seines Verfassers und Absenders kann ein so hergestellter Schriftsatz keinen stärkeren Beweis erbringen als ein Schriftsatz ohne „Unterschrift", aber mit erkennbarem Verfassernamen."*; auch BVerfG, NJW 2002, S. 3535: *„Auf der Grundlage dieser Rechtsprechung wäre das Ausgangsgericht gehalten gewesen, ... zu fragen, ob der ... Einspruch ... von dem Bf. herrührte und dieser ihn mit Wissen und Wollen in den Verkehr gebracht hat. Dabei hätte das Gericht berücksichtigen müssen, dass als Absender der Name des Bf., der auch maschinenschriftlich unter dem Schreiben zu finden ist, genannt war und in dem Schreiben zusätzlich das Aktenzeichen und das Zustelldatum des Strafbefehls und damit Daten genannt waren, die in der Regel allein dem Betroffenen bekannt sind. ... Der Notwendigkeit einer solchen Prüfung ... steht die Entscheidung des* [GmS-OGB] *... nicht entgegen, ...* [dieser] *... ist nicht dahin zu verstehen, dass ausschließlich im Fall einer eingescannten Unterschrift das Schriftformerfordernis erfüllt sei."*

[1667] Denn schon bisher habe die Frage, ob die Unterschrift des Absenders auf dem eingehenden Schriftstück abgebildet war oder nicht, keine Bedeutung gehabt, denn auch Telegramm und Fernschreiben gäben das Bild des Namenszuges nicht wieder, FG Hamburg, NJW 2000, S. 992.

körperliche Urkunde.[1668] Dieses Merkmal erfüllt auch eine E-Mail sowie jedes Dokument in Textform.

Gerichte in Deutschland sowie in England und den USA stellen also vergleichbare Überlegungen an, wenden diese jedoch hier auf einen sehr begrenzten und dort auf einen wesentlich größeren Kreis von Sachverhalten an. Zwar wird dies im *common law* ermöglicht durch ein Weniger an Formenstrenge sowie durch ein Abstellen auf die Erfüllung der Funktion der jeweiligen Formvorschrift. Dabei kann deren Erfüllung, insbesondere das Vorliegen des *will to authenticate*, auch durch weitere Umstände als die jeweilige konkrete Form der *signature* belegt werden. Es liegt für englische und US-amerikanische Gerichte also näher, weniger auf die Form als auf die im Einzelfall erfüllte Funktion abzustellen, als für die nach dem kodifizierten und abstrakteren deutschen Recht entscheidenden Gerichte. Insgesamt stellt das *common law* für die Erfüllung von Formerfordernissen geringere Hürden, und zwar durchgehend und vergleichbar etwa für verwandte Arten und Ausformungen der *signature*. Eine elektronische Kommunikation wie eine E-Mail kann dort – unter gewissen Voraussetzungen – eine Signatur darstellen und den mit dieser verbundenen Beweiswert aufweisen. Das wird dann aber an der Fähigkeit der jeweiligen Art der Signatur beziehungsweise der (elektronischen) Kommunikation, die geforderte Funktion zu erfüllen, festgemacht und nicht ein technisch identischer Sachverhalt in vergleichbaren Fällen verschieden bewertet. In Deutschland hat dagegen schon der Gesetzgeber einer bestimmten Art der Erklärung, der Textform, bestimmte Eigenschaften abgesprochen, hier die Beweiskraft und weitere Funktionen der Schriftform. Zwar differenziert auch das deutsche Recht nach der konkreten Form und Strenge eines Schriftformerfordernisses, siehe die vorstehenden Ausführungen zum Prozessrecht. Zudem ist berücksichtigen, dass auch nach englischem und US-amerikanischem Recht etwa die Beweisfunktion nicht allein aus der *signature* herrührt, sondern sich in den gezeigten Fällen aus dieser und den sie begleitenden Umständen ergibt. Dass eine elektronische Kommunikation in der Gesamtschau dort auch Beweiskraft haben und die Identitätsfunktion erfüllen kann, liegt aber nicht allein in der geringeren Formenstrenge vieler Formerfordernisse begründet. Dem technisch identischen Sachverhalt wird in Deutschland schon durch Gesetzgeber, Rechtsprechung und Literatur diese Funktion abgesprochen, obwohl eine freie Beweiswürdigung auch deutschen Gerichten eine vergleichbare Beurteilung erlaubte.

Spätestens die vorstehenden Begründungen der deutschen Gerichte, nach denen insbesondere dem Computerfax die Erfüllung der prozessualen Schriftformerfordernisse zugesprochen wird, sind ein Widerspruch zur grundsätzlichen Verneinung jeglicher Beweiskraft von elektronischer Kommunikation wie E-Mails und von E-Mail-Ausdrucken. Die Formerfordernisse im deutschen Recht sind in ihren Funktionen und ihrem Gehalt verschieden, in diesem Vergleich einmal konstitutives Schriftformerfordernis, einmal bloße Sollvorschrift im Prozessrecht. Der technische Sachverhalt ist jedoch bei E-Mail und Computerfax vergleichbar. In beiden Fällen entsteht eine Erklärung lediglich als digitale Datei und wird elektronisch auf telekommunikativen Weg übermittelt. Eine in Bezug auf die Person des Erklärenden Sicherheit gewährende (technische) Komponente

[1668] GmS-OGB, NJW 2000, S. 2341; so auch FG Hamburg, NJW 2000, S. 992.

existiert in beiden Fällen nicht.[1669] Der Unterschied zur E-Mail besteht beim Computerfax allein darin, dass als Empfänger keine E-Mail- (oder IP-) Adresse, sondern ein Telefonanschluss vorliegt, was tatsächlich weniger Möglichkeiten bietet, den Text während der Übermittlung zu manipulieren.[1670] Wie *Splittgerber* richtig feststellt, können nach vorstehend dargestellter Rechtsprechung insbesondere des BVerfG die Funktionen Ernsthaftigkeit und Identitätssicherung durch den getippten Inhalt eines Computerfaxes sichergestellt werden. Die Trennlinie zur E-Mail ist verschwommen, da bezüglich des in beiden Fällen elektronisch am Bildschirm getippten Inhalts kein Unterschied besteht.[1671] Auch wenn die Computerfax-Rechtsprechung vor dem Hintergrund des Anspruchs auf rechtliches Gehör und effektiven Rechtsschutz ergangen ist und deshalb eine direkte Übertragung auf E-Mails nicht ohne weiteres möglich ist[1672], fragt es sich doch, warum von den Gerichten vergleichbare Überlegungen wie zum Computerfax nicht auch in den oben dargestellten Fällen bei der Frage der Urheberschaft einer E-Mail oder Internetkommunikation angestellt wurden. Hier hätten zumindest weitere Indizien, die auf die Identität des Erklärenden hinweisen können, einbezogen werden können. Insbesondere, da es dabei gerade nicht um die Erfüllung des konstitutiven Schriftformerfordernisses nach § 125 BGB geht.

Hier wird eine weitere Parallele der Computerfax-Rechtsprechung zum *common law* deutlich, indem insbesondere darauf abgestellt wird, dass der so übermittelte Schriftsatz Angaben enthält, über deren Kenntnis allein der jeweilige Verfahrenbeteiligte, also die angegebene Person, verfügen kann. Dies stellt eine der *reply letter doctrine* vergleichbare Überlegung dar und zeigt, dass deutsche Gerichte diesen Erwägungen gegenüber durchaus aufgeschlossen sind. Zuletzt soll nochmals deutlich herausgestellt werden, dass ein Computerfax in der Form und mit dem Inhalt, wie es der Computerfax-Rechtsprechung zugrunde lag, die Voraussetzungen der Textform erfüllt. Folglich liegen hier Urteile deutscher Gerichte vor, die der Textform – in dieser Gestalt – einen Beweiswert auch hinsichtlich der Identität des Erklärenden zubilligen, in dem sie sie als ausreichende Basis für Rückschlüsse auf die Person des Ausstellers erachten. Wendet man die in dieser Rechtsprechung wie auch in den bereits vielfach genannten englischen und US-amerikanischen Urteilen angewandten Grundsätze auf andere Gestalten der Textform wie der E-Mail an, so ist nicht ersichtlich, warum letzterer und damit der Textform insgesamt nicht auch ein gewisser, zumindest aber größerer Beweiswert in Bezug auf den Aussteller zugebilligt werden soll, als dies in Deutschland derzeit der

[1669] Das Erfordernis, hier eine digitale Signatur zu verwenden, ist aufgrund des reinen Ordnungscharakter z.B. der §§ 130 Abs. 1 Nr. 6, 130a ZPO und der vorstehenden Rechtsprechung zu bestimmenden Schriftsätzen ebenfalls nur eine Sollbestimmung, zutreffend Splittgerber, CR 2003, S. 26, der zudem klarstellt, dass deshalb eine Übermittlung per einfacher E-Mail nach dem Wortlaut ausreichend sei.

[1670] Stadler in Musielak, § 129 ZPO, Rn. 11.

[1671] Splittgerber, CR 2003, S. 27.

[1672] Schweinoch/Böhlke/Richter, „E-Mails als elektronische Geschäftsbriefe mit Nebenwirkungen", CR 2007, S. 167-171, S. 169. Auch hat der BGH, NJW 1995, S. 66, angenommen, dass Störungen der Fax-Übermittlung in der Sphäre der Gerichte nicht auf den Bürger abgewälzt werden dürften und der Eingang von Schriftsätzen bei Gericht durch technische Fehler des Empfangsgeräts nicht gehindert werde. Gleichzeitig hat er aber auch festgetsellt, dass es nicht fernliege, diese Grundsätze auch auf die Zugangsproblematik im Privatrechtsverkehr zu übertragen.

Fall ist. Tatsächlich steht derzeit nach deutscher Rechtsprechung allein das Abstellen auf die auch beim Computerfax auf Veranlassung des Absenders beim Empfänger erzeugte körperliche Urkunde der Übertragung dieser Rechtsprechung auf die E-Mail entgegen, weil ein per E-Mail übermittelter Schriftsatz als digitale Datei eine derartige Form nicht annimmt.[1673] Der BGH hat dennoch kürzlich einen nach Unterzeichnung gescannten, im pdf.-Format digitalisierten Schriftsatz, der anschließend per E-Mail versandt wurde, als Erfüllung der Schriftform des § 130 Nr. 6 ZPO anerkannt. Dass die Unterschrift nur in Kopie wiedergegeben ist, sei unschädlich, weil die Geschäftsstelle sich bereit erklärt hatte, den Schriftsatz als pdf-Datei per E-Mail-Versandt entgegenzunehmen und mit einem Eingangsvermerk zu versehen.[1674] Ein erhöhtes Risiko, dass eine über das Internet übermittelte Datei auf diesem Wege verfälscht werden könnte, rechtfertige eine Ungleichbehandlung von Telekopien und Bilddateien beim Unterschriftserfordernis nicht. Schon ein per Computerfax mit eingescannter Unterschrift erlaube kaum eine Überprüfung, ob der Schriftsatz tatsächlich von demjenigen autorisiert ist, von dem er autorisiert zu sein scheint.[1675] Wo aber die Möglichkeit bestünde, eine Berufungsbegründung elektronisch zu übermitteln, sei es sachlich nicht zu rechtfertigen, anders als bei einem Telefax die Wiedergabe der Unterschrift in der Kopie nicht genügen zu lassen. Das Gericht bezweifelt zudem die Unterscheidung zwischen „Computerfax“ und „Normalfax“. Es könne nicht darauf ankommen, durch welches Gerät das Telefax aufgezeichnet (durch einen an den Computer angeschlossenen Scanner oder durch eine herkömmliches Telefaxgerät) und versandt worden sei.[1676] Wie bereits oben festgestellt verschwimmen die Grenzen also zunehmend. Und da jederzeit nach Eingang einer E-Mail durch deren Ausdruck ein solches körperliches Schriftstück erstellt werden kann, müssen nach dem oben Festgetselltem bestimmende Schriftsätze letztlich auch per E-Mail wirksam sein[1677] – was zudem der vorstehenden Annahme zum Beweiswert der E-Mail nicht widerspricht. Wie *Schweinoch*, *Böhlke* und *Richter* zutreffend darlegen, kann die Computerfax-Rechtsprechung auch deshalb nicht nur isoliert für das Prozessrecht gelten, da dies dann zu einem Wertungswiderspruch zwischen der nicht disponiblen gesetzlichen Schriftform nach § 126 BGB im Prozessrecht, die mittels E-Mail erfüllt werden kann, und der privatrechtlich vereinbarten „doppelten“ Schriftform nach § 127 Abs. 1 BGB in Verbindung mit § 125 S. 2 BGB führte. Bei der gewillkürten Schriftform kann dieses Ergebnis nämlich nur über § 127 Abs. 2 BGB erreicht werden.[1678] Auch einen weiteren – hier erwähnenswerten – Aspekt führen sie an: Der Charakter von E-Mails als Geschäftsbrief aufgrund der auch für sie obligatorischen Pflicht-

[1673] Splittgerber, CR 2003, S. 26. Dieser Aspekt wurde zumindest auch für das australische *common law* gesehen, vgl. Christensen/Low, „Moving the Statute of Frauds to the Digital Age“, ALJ 77:416, 2003, S. 2.

[1674] BGH, Beschl. v. 15.07.2008, X ZB 8/08, NJW 2008, S. 2649-2651, S. 2650.

[1675] BGH, NJW 2008, S. 2650.

[1676] BGH, NJW 2008, S. 2650.

[1677] So auch Schweinoch/Böhlke/Richter, CR 2007, S. 169.

[1678] Schweinoch/Böhlke/Richter, CR 2007, S. 169, nach denen eine E-Mail stets die Schriftform des § 127 BGB erfülle.

angaben für den elektronischen Geschäftsverkehr[1679] verstärke ihren formalen Charakter und nähere sie dem klassischen Geschäftsbrief in Papierform weitgehend an, weshalb Geschäftspartner nunmehr an rechtsgeschäftliche Erklärungen oder Vertragsabschlüsse per E-Mail ebenso gebunden seien, wie an Erklärungen mittels solcher klassischer Briefe.[1680] Dieser Gedanke ist schlüssig – und die bisherige Rechtsprechung mit ihrer Annahme der nicht vorhandenen Beweiskraft von E-Mails steht im Widerspruch dazu.

3.3.13 Leitlinien der beweisrechtlichen Bewertung elektronischer Kommunikation

Die Überlegungen und Vergleiche aus Abschnitt 3.3 führen zu konkreten Forderungen an Gesetzgeber und Gerichte. Letztere sind gehalten, im Rahmen der freien Beweiswürdigung nach § 286 Abs. 2 ZPO bei elektronischen Dokumenten und Erklärungen, insbesondere bei E-Mails, die Anforderungen an deren Beweiskraft nicht zu hoch setzen. Der durch die derzeitige Rechtsprechung provozierte Effekt, bei dem der bloße Hinweis auf eine mögliche Manipulation jede Möglichkeit des Beweises durch E-Mail, Internetkommunikation und entsprechende Ausdrucke vernichtet, führt zu ungerechten Ergebnissen. Aus vergleichbaren Überlegungen heraus sind dem oben dargestellten *reliability test* Beschränkungen auferlegt worden. Entsprechende Begrenzungen der Möglichkeit, sich von einer elektronisch abgegebenen Erklärung ohne Rechtsgrund und mithilfe der bloßen Vermutung eines Dritteingriffs loszusagen, fehlen im deutschen Recht. Ein Schlüssel zu einer interessen- und risikogerechteren Lösung ist die Zubilligung einer erhöhten Beweiskraft elektronischer Kommunikation. Dies kann im Einzelfall durch die Einbeziehung ergänzender Indizien und Beweise neben der als elektronische Datei gespeicherten Erklärung, die sich aus den Umständen ihrer Erstellung, Abgabe und ihrem Empfang ergeben, sowie den diesen elektronischen Daten anhaftenden Metadaten erreicht werden. Dies ist auch nach deutschem Recht im Rahmen der freien Beweiswürdigung möglich. Die Urheberschaft, Abgabe und Zugang einer elektronischen Erklärung könnte so wahrscheinlich in einer größeren Anzahl an Fällen etabliert werden, als dies derzeit der Fall ist. Zu fordern ist daher zunächst eine größere Offenheit der Gerichte für die Berücksichtigung solcher ergänzenden, auch technischen Beweise. Zwar sind die Gerichte im Zivilprozess grundsätzlich abhängig von den von den Parteien angebotenen und beigebrachten Beweisen. Vielfach wird sich dies in der Vorlage des elektronischen Dokuments selbst oder eines Ausdrucks etwa der streitgegenständlichen E-Mail erschöpfen. Doch schon daraus lassen sich vielfach wichtige Hinweise für die Echtheit und insbesondere die Urheberschaft entnehmen. In einzelnen Fällen kann dabei auch ein Beweis des ersten Anscheins für die Urheberschaft einer elektronischen Kommunikation entstehen. Dies gilt am ehesten für solche Erklärungen, die mittels eines den Zugang durch ein Passwortsystem reglementierenden Kommunikationssystems erstellt und versandt werden. Jedenfalls ist dieser Umstand bei der Beweiswürdigung einzubeziehen

[1679] Gem. Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister (EHUG), in Kraft seit 1.1.2007, BGBl. I 2006, S. 2553 v. 15.11.2006.

[1680] Schweinoch/Böhlke/Richter, CR 2007, S. 169.

und zu würdigen. Aufgrund der technisch wenig aufwändigen und in der Realität vielfach vorkommenden Manipulation durch unberechtigte Dritte kann in der Regel jedoch ein grundsätzlicher Anscheinsbeweis für die Urheberschaft der in der Absenderzeile einer E-Mail genannten Person nicht angenommen werden. Hierfür fehlt es schlicht an der geforderten sehr hohen Wahrscheinlichkeit der Identität von angegebenem und tatsächlichem Verfasser und damit an der notwendigen Typizität. Ein solcher Anscheinsbeweis existiert auch nicht im englischen oder US-Amerikanischen Recht.
Dennoch kann die unkritische Gleichsetzung von E-Mail-Kommunikation mit unsicherer, nicht beweiskräftiger Kommunikation nicht fortgeführt werden. Vielmehr muss die Betrachtung des Einzelfalls und die Berücksichtigung dessen besonderer Umstände der Grundsatz sein. Auch wenn eine Übernahme der *reply letter doctrine* und anderer *common law*-Regeln nicht ohne Weiteres und nicht umfänglich möglich ist, gehören etwa die im Rahmen der *reply letter doctrine* zu berücksichtigenden Aspekte zu denjenigen, denen größere Bedeutung beigemessen werden kann und muss. Vor allem aber muss dabei im Rahmen der bestehenden Prozessregeln der ZPO die Substantiierung des eigenen Vortrags auch desjenigen verlangt werden, der sich auf eine Manipulation beruft. Dies gilt insbesondere dann, wenn dies wie zumeist die besser informierte Partei ist. Hierauf sollte das Gericht hinwirken. Sofern zum Beispiel die beweisbelastete Partei keine technischen Beweise wie Sachverständigengutachten zur Prüfung der sich aus dem Metadaten ergebenden Hinweise auf die Urheberschaft einer elektronischen Datei, etwa des Envelopes und der Versendeangaben einer E-Mail, anbietet, mag es angezeigt erscheinen, dass das Gericht die Partei auf entsprechende Möglichkeiten der technischen Beweisführung hinweist. Die Sachverhalte und Urteilsbegründungen der hier dargestellten Urteile zur Beweiskraft von elektronischen Erklärungen lassen vermuten, dass derzeit die Kenntnisse über die Möglichkeiten solcher Beweisführung bei den Parteien und den Gerichten zumindest lückenhaft sind und einen limitierenden Faktor darstellen. Ließe sich dieser damit überwinden, besteht der wesentliche limitierende Faktor der Kosten einer zumeist auf Sachverständige angewiesenen technische Beweisführung fort. Das damit verbundene Kostenrisiko wird auch in Zukunft die entscheidende Hemmschwelle für die Durchsetzung von im Übrigen berechtigten Ansprüchen sein, wenn diese allein mittels elektronischer Dateien beweisbar wären. Über eine solche größere Differenzierung und Fokussierung auf die Umstände des Einzelfalles können diese Forderungen jedoch nicht hinausgehen. Eine grundlegende Änderung des deutschen Beweisrechts in Gesetz und Rechtsprechung lässt sich daraus nicht herleiten. Sie ist – wie gezeigt – auch nicht notwendig. Dennoch ergäbe sich danach im Einzelfall vielfach ein Beweis für die Authentisierung einer elektronischen Erklärung und damit ein größerer Beweiswert solcher elektronischen Kommunikationsformen, als dies bislang von Gerichten und Gesetzgeber zugestanden wird. Dieses Ergebnis entspricht überdies auch dem Willen des Gesetzgebers, den E-Commerce zu fördern. Es ermöglicht zudem, den Anwendungsbereich der Textform nach § 126b BGB, deren Verwendung in Zukunft größtenteils in solchen elektronischen Erklärungen liegen wird, auszuweiten, etwa auf prozessuale Schriftformerfordernisse und weitere Aufklärungs- und Mitteilungspflichten im Zivilrecht, aber auch in anderen Rechtsgebieten.

Ergebnis

Die *writing*- und *signature*-Erfordernisse im englischen und US-amerikanischen Recht sind nur zum Teil mit denen mit der Schriftform des §126 BGB vergleichbar. Allerdings bestehen große Ähnlichkeiten zwischen den als Erfüllung der *signed-writing*-Erfordernissen von englischen und US-amerikanischen Gerichten anerkannten Formen der *signature* und solchen Kommunikationsformen, die im deutschen Recht die Voraussetzungen des §126b BGB für die Textform erfüllen. Dabei erfüllen diese Formen der Kommunikation, beziehungsweise des *signed writing* oder der Textform, in England und USA vielfach solche (gesetzlichen) Formerfordernisse, denen insbesondere eine Beweisfunktion zukommt, wie beispielsweise der Statute(s) of Frauds. Dagegen soll die Textform allein eine Dokumentationsfunktion erfüllen können. Eine Beweisfunktion wird ihr abgesprochen. Demanch verneint die deutsche Rechtsprechung für entsprechende, insbesondere elektronische, Kommunikationsformen wie die E-Mail jeglichen Beweiswert. Auch englische und US-amerikanische Gerichte erkennen offenbar die Probleme der Manipulierbarkeit solcher Kommunikation, kommen aber dennoch zu abweichenden Ergebnissen, nach denen solchen elektronischen Erklärungen nicht prinzipiell jeglicher Beweiswert und damit die Durchsetzbarkeit und Rechtskraft abgesprochen wird. Vielmehr werden von den englischen und US-amerikanischen Gerichten in weit größerem Maße ergänzende Beweise und Indizien bei der rechtlichen Beurteilung solcher (elektronischen) Kommunikationen berücksichtigt. Es besteht somit eine wesentlich größere Ähnlichkeit und Nähe zur Behandlung von herkömmlichen, etwa papiernen postalischen Kommunikationen und Dokumenten und zu traditionellen Formen der Signatur.

Grund hierfür sind die Unterschiede zum deutschen Recht in Gesetzgebung und Rechtsprechung. Vorschriften ähnlich der §125 ff. BGB oder der §416 ff. ZPO existieren in den *common law*-Rechtsordnungen England und den USA nicht. Es wird wesentlich mehr auf das einzelne Formerfordernis und die Funktionen, die dieses erfüllen soll, abgestellt. Die Ausprägung, in der eine Erklärung oder eine Form der Authentisierung diese Funktion erfüllt, ist zweitrangig. Somit sind diese Formen des *signed writing* und der *signature* vielfältiger und deren Konzept offener für neue Techniken. Zudem ist der Wille, eine Erklärung zu signieren, entscheidend, der wiederum nicht nur durch das signierte Dokument, sondern vor allem auch durch ergänzende Beweise und Indizien wie die Umstände des Signiervorgangs nachgewiesen werden kann. Hierzu haben sich Regeln wie die *non-repudiation* oder die *reply letter doctrine* herausgebildet, die gleichermaßen wie auf herkömmliche Erklärungen auch auf elektronische Erklärungen und Signaturen Anwendung finden. Wesentliche Aspekte dieser Regeln können aufgrund der gleichen technischen Grundlagen, die zu Bedenken hinsichtlich der Vertrauenswürdigkeit elektronischer Kommunikation führen, etwa aufgrund der Manipulationsgefahr, ebenso auf die richterliche Beurteilung solcher Kommunikation im Rahmen der freien Beweiswürdigung nach deutschem Recht angewendet werden. Hinzu kommen technische Beweise mittels Metadaten und ähnlichem, die größere Beachtung finden sollten.

Im englischen und US-amerikanischen Recht werden nach den vorgenannten Regeln einfache elektronische und digitale Signaturen gleich behandelt, das heißt nach densel-

ben Maßstäben bemessen. Eine Privilegierung der digitalen Signatur etwa in Form der fortgeschrittenen elektronischen Signatur der Signaturrichtlinie – die in Deutschland und England gleichermaßen und in einzelnen Bundesstaaten der USA vergleichbar geregelt sind – findet nicht statt. Ihre gegebenenfalls höher bewertete Sicherheit und Verlässlichkeit muss das jeweilige digitale Signaturverfahren beziehungsweise die darauf vertrauende Partei im Einzelfall nachweisen. Sie werden aber sehr wahrscheinlich eine hervorgehobene Bedeutung als Verfahren der *authentication* oder auch als Grundlage der *non-repudiation* erhalten. Grundsätzlich ist eine gesetzliche Regelung und Regulierung der Anwendung digitaler Signaturverfahren sinnvoll. Sie erlaubt, über das Gesetz auf Grundlage der Sicherstellung technisch-organisatorischer Anforderungen und deren (Vorab-)Prüfung Beweiskraft- und Vermutungsregeln für einzelne Signaturverfahren aufzustellen. Für konstitutive Schriftformerfordernisse, die für besonders bedeutsame Rechtsgeschäfte verlangt werden, sind digitale Signaturen als elektronisches Substitut der eigenhändigen Unterschrift erforderlich, da sie trotz aller Schwachpunkte die derzeit höchste Sicherheit bieten. Dies haben auch der englische und der Bundesgesetzgeber in den USA erkannt; die Gerichte dort werden wohl ähnlich entscheiden.
Die Signaturgesetzgebung hierzu ist jedoch uneinheitlich, auch im Rahmen der Umsetzung der E-Commerce- und Signaturrichtlinie in Europa. Hier wäre aufgrund der Technikbezogenheit einer solchen Regulierung Spielraum für weitere Harmonisierungsbestrebungen. Eine weitergehende Harmonisierung der Formvorschriften aber ist schon wegen der oben angesprochenen Unterschiede weder gewünscht, noch durchführbar. In England und den USA wird daher die Erfüllung eines Formerfordernisses durch elektronische und digitale Signaturen von den Voraussetzungen des einzelnen Formerfordernisses abhängen und im Einzelfall zu entscheiden sein. In Deutschland ist für konstitutive Schriftformerfordernisse gemäß §126 BGB die elektronische Form zu erfüllen. Die hierfür geschaffenen gesetzlichen Beweiskraft- und Anscheinsregeln sind jedoch kritikwürdig. Unterhalb der mit hohen technisch-organisatorischen Hürden versehenen digitalen Signaturverfahren, wie zum Beispiel nach dem deutschen Signaturgesetz, existieren in der Praxis die eingangs behandelten einfacheren (elektronischen) Kommunikationsformen, die in wesentlich größerem Maße als die digitale Signatur für viele Arten von Rechtsgeschäften genutzt werden, aber auf besondere Sicherheitsverfahren verzichten. Dies betrifft insbesondere Erklärungen per E-Mail oder andere Formen der Internetkommunikation, wie etwa beim Internetvertrag. Diese, vielfach die Voraussetzungen der Textform nach §126b BGB sowie der *signature* oder gar des *signed writing* nach englischem und US-amerikanischem Recht erfüllenden Erklärungen können und müssen nach den in dieser Arbeit gewonnenen Erkenntnissen durch die Gerichte in ihrer Beweis- und Rechtskraft gestärkt werden, etwa durch Anwendung einzelner Aspekte der vorgenannten, aus dem englischen und US-amerikanischen Recht entliehenen Grundsätze. Eine weitere Stärkung deren Beweiskraft kann durch konsequente Forderung des substantiierten Vortrags desjenigen gelingen, der sich auf eine Manipulation der digitalen Datei oder deren Übertragung beruft. Aus diesen Gründen kann und sollte das neue Formerfordernis der Textform auch auf einen erweiterten Kreis von Rechtsgeschäften und rechtserheblichen Erklärungen Anwendung finden.

Abkürzungsverzeichnis

ABA	American Bar Association
a.F.	alte Fassung
AG	Amtsgericht
AktG	Aktiengesetz
ALJ	Australian Law Journal
AZW	Arbeitspapiere zum Deutschen und Internationalen Zivil- und Wirtschaftsrecht
BAG	Bundesarbeitsgericht
BB	Der Betriebsberater
Beschl.	Beschluss
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BLR	Business Law Review
BSG	Bundessozialgericht
B2C	Business to Consumer (-*Commerce*)
B2B	Business to Business (-*Commerce*)
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
CISG	Wiener UN-Übereinkommen über Verträge über den internationalen Warenkauf
CR	Computer und Recht
CRi	Computer Law Review International
CTLR	Computer and Telecommunication Law Review
DB	Der Betrieb
ders.	derselbe
DEJ	Digital Evidence Journal
dies.	dieselbe, dieselben
DIG	Dienste der Informationsgesellschaft
DuD	Datenschutz und Datensicherheit
DStR	Deutsches Steuerrecht (*Zeitschrift*)
DSWR	Zeitschrift für Praxisorganisation, Betriebswirtschaft und Datenverarbeitung

DTI	Department Of Trade And Industry (*Großbritannien*)
EC Act	Electronic Communications Act 2000
ECLIP	Electronic Commerce Legal Issues Platform
ECLP	E-Commerce Law & Policy
E-Commerce	electronic commerce, elektronischer Geschäftsverkehr
EC-Order	Companies Act 1985 (Electronic Communications) Order 2000
EC Reg.	Electronic Commerce (EC Directive) Regulations
EDI	Electronic Data Interchange
EGG	Gesetze über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz)
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
E-Mail	electronic mail, elektronische Post
E-SIGN	Electronic Signature in Global and National Commerce Act
ES Reg.	Electronic Signatures Regulations 2002
etc.	Etcetera
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
FernAbsRL	EU-Fernabsatzrichtlinie über den Verbraucherschutz bei Vertragsschlüssen im Fernabsatz (Fernabsatzrichtlinie)
FG	Finanzgericht
Fn.	Fußnote
FormG	Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr
GI	Gesellschaft für Informatik
GmS-OGB	Gemeinsamer Senat der obersten Gerichtshöfe des Bundes
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
HGB	Handelsgesetzbuch
Hrsg.	Herausgeber
HS	Halbsatz
ICCLR	International Company and Commercial Law Review
ILPF	Internet Law and Policy Forum
ITRB	Der IT Rechts-Berater
IuKdG	Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste

J. High Tech L.	Journal of High Technology Law
JILT	The Journal of Information, Law and Technology
JKomG	Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz
JMJCIL	The John Marshall Journal of Computer and Information Law
JURA	Juristische Ausbildung
JurPC	Internetzeitschrift für Rechtsinformatik und Informationsrecht
Kap.	Kapitel
KG	Kammergericht
K&R	Kommunikation und Recht
lit.	litera, Buchstabe
LAG	Landesarbeitsgericht
LG	Landgericht
LJ	Lord Justice
Ltd.	Limited (*Gesellschaft mit beschränkter Haftung*)
MDR	Monatsschrift für Deutsches Recht
MLeC	UNCITRAL Model Law on Electronic Commerce (Modellgesetz zum Elektronischen Geschäftsverkehr)
MLeS	UNCITRAL Model Law on Electronic Signatures (Modellgesetz zu Elektronischen Signaturen)
MMR	MultiMedia und Recht
m.w.N.	mit weiteren Nachweisen
NCCUSL	National Conference of Commissioners on Uniform State Laws
n.F.	Neue Fassung
NJW	Neue Juristische Wochenschrift
NJW-CoR	Neue Juristische Wochenschrift Computerreport
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
OECD	Organisation for Economic Co-Operation and Development
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PKI	Public Key Infrastructure
Re	Regina (Königin, Vereinigtes Königreich)

RG	Reichsgericht
RLeC	Richtlinie über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr; Elektronischer Geschäftsverkehr-Richtlinie; E-Commerce-Richtlinie)
RLeS	Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (Signaturrichtlinie)
Rn.	Randnummer
RR	Rechtsprechungs-Report
S.	Seite
SGG	Sozialgerichtsgesetz
SLR	Stanford Law Review
SigG	Signaturgesetz
StGB	Strafgesetzbuch
TCL	The Computer Lawyer
TLR	Texas Law Review
TTP	Trusted Third Parties
u.a.	und andere
UETA	Uniform Electronic Transactions Act
UCC	Uniform Commercial Code
UCITA	Uniform Computer Information Transactions Act
ULR	Uniform Law Review
UNCITRAL	United Nations Commission on International Trade Law
USA	United States of America, Vereinigte Staaten Amerikas
u.U.	unter Umständen
VersR	Versicherungsrecht – Zeitschrift für Versicherungsrecht, Haftungs- und Schadensrecht
VJLT	Virginia Journal of Law and Technology
VwVfG	Verwaltungsverfahrensgesetz
VVG	Versicherungsvertragsgesetz
Web-Dok.	Web-Dokument
WTO	World Trade Organisation
www	(auch WWW oder W.W.W.) World Wide Web

ZEuP	Zeitschrift für Europäisches Privatrecht
ZMR	Zeitschrift für Miet- und Raumrecht
ZPO	Zivilprozessordnung
z.T.	zum Teil
ZZP	Zeitschrift für Zivilprozess

Literaturverzeichnis

Abel, Stefan	„Urkundenbeweis durch digitale Dokumente“, MMR 1998, S. 644-650
Armgardt, Matthias / Adrian Spalka	„Der Anscheinsbeweis gemäß § 371a Abs. 1 S. 2 ZPO vor dem Hintergrund der bestehenden Sicherheitslücken bei digitalen Signaturen“, K&R 2007, S. 26-32
Baker, Martin	„E-Commerce: New Wine in Old Bottles?“, ICCLR 2000, S. 293-296
Baker, Steward / Rosa Barceló / Eric Greenwald / Chris Kaner	„An Analysis of International Electronic and Digital Signature Implementation Initiatives”, ILPF Sept. 2000, www.ilpf.org/groups/analysis_IEDSII.htm
Beese, Dietrich / Jutta Merkt	„Europäische Union zwischen Konvergenz und Re-Regulierung – Die neuen Richtlinien entwürfe der Kommission“, MMR 2000, S. 532-537
Berger, Christian	„Beweisführung mit elektronischen Dokumenten“, NJW 2005, 1016-1020
Bertsch, Andreas / Sophie-D. Fleisch / Markus Michels	„Rechtliche Rahmenbedingungen des Einsatzes digitaler Signaturen“, DuD 2002, S. 69-75
Beucher, Klaus / Andrea Schmoll	„Kryptotechnologie und Exportbeschränkungen“, CR 1999, S. 529-534
von Bernstorff, Christoph Graf	*Einführung in das englische Recht*, 2. Auflage, C.H. Beck, München 2000
Bierenkoven, Christiane	*Der Vertragsabschluss via Internet im internationalen Wirtschaftsverkehr – Zustandekommen – Schriftform – Beweisrecht – Elektronische Signaturverfahren*, Carl Heymanns Verlag, Köln 2001
Blaurock, Uwe / Jürgen Adam	„Elektronische Signatur und europäisches Privatrecht“, ZEuP 2001, S. 93-115
Blobel, Bernd / Peter Pharow	„Wege zur elektronischen Patientenakte“, DuD 2006, S. 164-169
Blum, Felix	„Das UNCITRAL-Modellgesetz zu elektronischen Signaturen”, K & R 2000, S. 63-71
Boehme-Neßler, Volker	*CyberLaw – Lehrbuch zum Internetrecht*, C.H. Beck, München 2001
Boente, Walter / Thomas Riem	„Das BGB im Zeitalter digitaler Kommunikation – Neue Formvorschriften“, JURA 2001, S. 793-798
Bohm, Nicholas	„Watch What You Sign!”, DEJ 2006, Vol. 3, S. 43-47
Bonell, Michael Joachim	“The UNIDROIT Principles and Transnational Law”, 2000, www.unidroit.org/english/publications/review/articles/2000-2.htm

Bonke, Jörg / Nico Gellmann	„Die Widerrufsfrist bei eBay-Auktionen – Ein Beitrag zur Problematik der rechtzeitigen Belehrung des Verbrauchers in Textform“, NJW 2006, S. 3169-3173
Borges, Georg	*Verträge im elektronischen Geschäftsverkehr – Vertragsabschluß, Beweis, Form, Lokalisierung, anwendbares Recht*, C.H. Beck, München 2003
ders.	„Rechtsfragen des Phishing - Ein Überblick“, NJW 2005, S. 3313-3317
Borsum, Wolfgang / Uwe Hoffmeister	„Rechtsgeschäftliches Handeln unberechtigter Personen mittels Bildschirmtext“, NJW 1985, S. 1205-1207
Bösing, Sebastian	*Authentifizierung und Autorisierung im elektronischen Rechtsverkehr*, NOMOS, Baden-Baden 2005
Bovenschulte, Andreas / Martin Eifert	„Rechtsfragen der Anwendung technischer Produkte nach Signaturgesetz – Signaturerstellungseinheiten und -anwendungskomonenten“, DuD 2002, S. 76-78
Brandner, Ralf / Ulrich Pordesch / Alexander Roßnagel / Joachim Schachermayer	„Langzeitsicherung qualifizierter elektronischer Signaturen“, DuD 2002, S. 97-103
Brandner, Ralf / Ulrich Pordesch	„Konzept zur signaturgesetzkonformen Erneuerung qualifizierter Signaturen“, DuD 2003, S. 354-359
Brennan, Lorin / Glenn A. Barber	„Why Software Professionals Should Support The Uniform Computer Transactions Act (And What Will Happen If They Don’t)“, www.2bguide.com/docs/proucita4.doc
Brisch, Klaus M.	„Computer und Recht aktuell – Textform und elektronische Form“, CR 1999, S. 537-538
Brooks, Gary	„The Task Ahead (Part 2)”, ECLP 2001, S. 6-7
de Bruin, Ronald	*Consumer Trust in Electronic Commerce: Time for Best Practice*, Kluwer Law Int., Den Haag 2002
Büger, Matthias / Bernhard Esslinger / Henrik Koy	„Das deutsche Signaturbündnis – Ein pragmatischer Weg zum Aufbau einer interoperablen Sicherheitsinfrastruktur und Applikationslandschaft“, DuD 2004, S. 133-140
Buchmann, Felix	„Die Widerrufsbelehrung im Spannungsfeld zwischen Gesetzgebung und Rechtsprechung – Vorschlag für ein Muster für Fernabsatzgeschäfte mit Waren im Internet“, MMR 2007, S. 347-353
Büllesbach, Alfred / Anja Miedbrodt	„Überblick über die internationale Signaturregulierung“, CR 2000, S. 751-757
Campbell, Dennis (Hrsg.)	*E-Commerce and the Law of Digital Signatures*, Oceana Publications, 2005
ders.	*The Internet: Laws and Regulatory Regimes*, Volume 2, Yorkhill Law Publishing, 2007

Chissik, Michael	*Electronic Commerce – Law and Practice*, Sweet & Maxwell, London 1999
Chissick, Michael / Guy Veysey	„The Perils of On-Line Contracting", CTLR 2000, S. 121-122
Christensen, Sharon / William Duncan / Rouhshi Low	„The Statute of Frauds in the Digital Age – Maintaining Integrity of Signatures", Murdoch University Electronic Journal of Law, Vol. 10, No. 4, December 2003, www.Murdoch.edu.au/elaw/issues/v10n4/christensen104_text.html
Christensen, Sharon / Rouhshi Low	„Moving the Statute of Frauds to the Digital Age", Australian Law Journal 77:416, 2003
Christiansen, Per	„Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet", MMR 2000, S. 123-129
Collier / Shannon / Scott	„Electronic Signatures Legislation", Memo from NACS Counsel, www.nacsonline.com/NACS/Resource/Government-/electronic_sig_070500_ir.htm
Collin, P.H. / Sigrid Janssen / Anke Kornmüller / Rupert Livesey	*PONS Fachwörterbuch Recht: Englisch-Deutsch, Deutsch-Englisch*, Klett Verlag, Stuttgart/Düsseldorf/Leipzig 1998
Cordes, Alexandra	*Form und Zugang von Willenserklärungen im Internet im deutschen und US-amerikanischen Recht*, LIT, Münster 2001
Cornelius, Kai	„Vertragsabschluss durch autonome elektronische Agenten", MMR 2002, S. 353-358
Coyle, Michael	„Still Waiting for Critical Mass", ECLP 2001, S. 8-9
Creifelds, Carl / Hans Kaufmann	*Rechtswörterbuch*, Beck'sche Verlagsbuchhandlung, München 1992
Crichard, Mark	„UK Electronic Communication Act 2000 – Take-off Time for E-Business or a Missed Opportunity?", CLSR 2000, S. 397-399
Czeguhn, Ignacio	„Beweiswert und Beweiskraft digitaler Dokumente im Zivilprozess", JuS 2004, S. 124-126
Dauner-Lieb, Barbara / Thomas Heidel / Manfred Lepa, Gerhard Ring (Hrsg.)	*Das neue Schuldrecht in der anwaltlichen Praxis*, Deutscher Anwaltverlag, Bonn 2002
Dauner-Lieb, Barbara / Thomas Heidel / Gerhard Ring (Hrsg.)	*Anwaltkommentar BGB Band 1: Allgemeiner Teil mit EGBGB*, DeutscherAnwaltverlag, Bonn 2005
Deutsch, Thomas	„Die Beweiskraft elektronischer Dokumente", JurPC Web-Dok. 188/2000, Abs. 1-72
Deville, Rainer / Regina Kalthegener	„Wege zum Handelsverkehr mit elektronischer Unterschrift", NJW-CoR 1997, S. 168-172

Dietrich, Florian / Ruben Hofmann	„3... Gerichte, 2... Wochen, 1... Monat? – Konfusion um die Widerrufsfristen bei eBay", CR 2007, S. 318-322
Diedrich, Frank	„A Law of the Internet? Attempts to Regulate Electronic Commerce", JILT 2000, S. 1 - 23
Docter, Nicolette / Arie van Bellen	„Model code of Conduct for Electronic Commerce", The EDI Law Review 1999, S. 187-208
Downes, T. Antony	*Textbook on Contract*, 5. Aufl., Blackstone Press Limited, London 1997
Downing, Susannah / Justin Harrington	„The Postal Rule in Electronic Commerce: A Reconsideration", Talley's Communications Law, Vol. 5, No. 2, 2000, S. 43-47
Dreben, Ron N. / Johanna L. Werbach	„Senators Versus Governors: State and Federal Regulation of E-Commerce", TCL 2000, S. 3-15
Dreßel, Jens / Wolfram Viefhues	„Gesetzgeberischer Handlungsbedarf für den elektronischen Rechtsverkehr – werden die wahren Probleme gelöst?", K&R 2003, S. 434-????
Dumortier, Jos / Patrick van Eecke	„Electronic Signature – The European Draft Directive on a Common Framework for Electronic Signatures", CLSR 1999, S. 106-112
Dumortier, Jos / Stefan Kelm / Hans Nilsson / Georgia Skouma / Patrick van Eecke	„The legal and market aspects of electronic signatures", DuD 2004, S. 141-146
Edwards, Lilian / Charlotte Walden	*Law & The Internet – A Framework for Electronic Commerce*, Hart Publ., Oxford 2000
Ernst, Stefan	„Der Mausklick als Rechtsproblem – Willenserklärungen im Internet", NJW-CoR 1997, S. 165-167
ders.	„Beweisprobleme bei E-Mail und anderen Online-Willenserklärungen", MDR 2003, S. 1091-1094
ders.	„Trojanische Pferde und die Telefonrechnung – Einflussmöglichkeiten von Schadsfotware auf den Anscheinsbeweis für die Richtigkeit von Telefonrechnungen", CR 2006, S. 590-594
Fendell, Charles H. / Dennis McKennedy	„UCITA Is Coming!!! Part Two: Practical Analysis for Licensors Council", TCL 2000, S. 3-18
Fischer-Dieskau, Stefanie / Rotraud Gitter / Sandra Paul / Roland Steidle	„Elektronisch signierte Dokumente als Beweismittel im Zivilprozess", MMR 2002, S. 709-713
Fischer-Dieskau, Stefanie / Roland Steidle	„Die Herstellererklärung für Signaturanwendungskomponenten – Eine Erleichterung zur Verbreitung elektronischer Signaturen?", MMR 2006, S. 68-73
Flamm, Suzan / Samuel H. Solomon	„Admissibility of Digital Exhibits in Litigation", DOAR Litigation Consulting, 2004, http://macproppid.com/ document s/Admissibility.pdf

Fringuelli, Pietro Graf / Matthias Wallhäuser	„Formerfordernisse beim Vertragsschluss im Internet", CR 1999, S. 93-101
Geis, Ivo	„Die elektronische Signatur: Eine internationale Architektur der Identifizierung im E-Commerce", MMR 2000, S. 667-674
ders.	„Die neue Signaturverordnung: Das Sicherheitssystem für die elektronische Kommunikation", K&R 2002, S. 59-61
ders.	„Elektronische Kommunikation und Dokumentation – eine rechtliche Betrachtung", www.informatik.uni-jena.de/dbis/lehre/ss2006/geis/TutoriumUniJenaNeu.pdf
Gesellschaft für Informatik	„DuD Forum – Stellungnahme zum Gesetzentwurf ‚Formvorschriften des Privatrechts'", DuD 2001, S. 38-40
Giessmann, Ernst-Günter	„Standards für Elektronische Signaturen – ETSI und die europäische Standardisierung", DuD 2003, S. 749-752
Goergen, Ute (Hrsg.)	*An Introduction to English Contract Law – For German Readers with Exercises*, Nomos, Baden-Baden 1997
Gotthard, Michael / Carsten Beck	„Elektronische Form und Textform im Arbeitsrecht: Wege durch den Irrgarten", NZA 2002, S. 876-883
Gramlich, Ludwig	„Die Regulierungsbehörde für Telekommunikation und Post (RegTP) im Jahr 2004", CR 2005, S. 560-568
Gravesen, Gavan / Jos Dumortier / Patrick van Eecke	„Die Europäische Signaturrichtlinie – Regulative Funktion und Bedeutung der Rechtswirkung", MMR 1999, S. 577-585
Habersack, Mathias / Peter Hommelhoff / Uwe Hüffer / Karsten Schmidt (Hrsg.)	*Festschrift für Ulmer zum 70. Geburtstag am 2. Januar 2003*, Walter De Gruyter Recht, 2003
Hähnchen, Susanne	„Das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr", NJW 2001, S- 2831-2834
Hansen, Mathias	„Das elektronische Transaktionssiegel – Eine Alternative für qualifizierte elektronische Signaturen?", DuD 2004, S. 233-237
Hay, Peter	*U.S.-Amerikanisches Recht – Ein Studienbuch*, C.H. Beck, München 2000
Heller, Arne / Salmeh Sadeghi / Teresa Dretzki / Catharina L. Ruhe	„Die Online-Hauptversammlung – Überlegungen zur unmittelbaren Ausübung der Aktionärsrechte via Internet", CR 2002, S. 592-598
Herwig, Volker	„Zugang und Zustellung in elektronischen Medien", MMR 2001, S. 145-149

Heusch, Clemens-August	*Die elektronische Signatur – Änderungen des Bürgerlichen Rechts aufgrund der Signatur-Richtlinie (1999/93/EG) durch das Gesetz zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001*, Tenea Verlag für Medien, Berlin 2004
Hladjk, Jörg	„Gütesiegel als vertrauensbildende Maßnahme im E-Commerce – Motive, Modelle und Rechtsgrundlagen“, DuD 2002, S. 597-600
ders.	„Qualität und Effektivität von Gütesiegeln – Eine Übersicht über nationale und internationale Angebote“, DuD 2002, S. 672-678
Hoeren, Thomas	„Internet und Recht – Neue Paradigmen des Informationsrechts“, NJW 1998, S. 2849-2928
ders.	*Grundzüge des Internetrechts – E-Commerce / Domains / Urheberrecht*, 2. Aufl., C.H. Beck, München 2002
ders.	*Skript Internetrecht*, Stand März 2008, www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Maerz08.pdf
ders.	„Das Pferd frisst keinen Gurkensalat – Überlegungen zur Internet Governance“, NJW 2008, S. 2615-2619
Hörnle, Julia	„The European Union Takes Initiative in the Field of E-Commerce – Commentary“, JILT 2000, Vol. 3, http://elj.-warwick.ac.uk/jilt/00-3/hornle.html
Hoffmann, Helmut	„Die Entwicklung des Internetrechts bis Mitte 2004“, NJW 2004, S. 2569-2576
ders.	„Die Entwicklung des Internetrechts bis Mitte 2005“, NJW 2005, S. 2595-2600
ders.	„Die Entwicklung des Internetrechts bis Mitte 2006“, NJW 2006, S. 2602-2608
ders.	„Anmerkung zu OLG Hamburg, Urt. v. 24.8.2006 – 3 U 103/06 – Dauer der Widerrufsfrist bei eBay-Auktionen“, MMR 2006, S. 676-677
ders.	„Die Entwicklung des Internetrechts bis Mitte 2007“, NJW 2007, S. 2594-2599
ders.	„Die Entwicklung des Internetrechts bis Mitte 2008“, NJW 2008, S. 2624-2630
Hoffmann, Mathis	„Der Beweiswert elektronischer Dokumente“, DSWR 2006, S. 60-62
Jansen, Thomas	„Legal Aspects of Doing E-Commerce Business in Germany”, ICCLR Spe. 1999, S. 39-42
Jewell, Michael	*An Introduction to English Contract Law*, 1. Aufl., Nomos, Baden-Baden 1997

Johnson, David R. / David G. Post	„Law and Borders - The Rise of Law in Cyberspace", 48 Stanford Law Review 1367 (1996)
Jungermann, Sebastian	„Der Beweiswert elektronischer Signaturen", DuD 2003, S. 69-72
Kaiser, Andreas / Dennis Voigt	„Vertragsschluss und Abwicklung des Electronic Commerce im Internet – Chancen und Risiken", K&R 1999, S. 445-453
Kaner, Cem	„Why You Should Oppose UCITA", TCL 5/2000, S. 20-32
Kath, Peter / Anne Riechert	*Internet-Vertragsrecht*, Haufe, Freiburg Berlin 2002
Kau, Christian	*Vertrauensschutzmechanismen im Internet, insbesondere im E-Commerce*, Schriften des Zentrums für angewandte Rechtswissenschaft, Band 5, Universitätsverlag Karlsruhe, Karlsruhe 2006
Kaufmann, Noogie C.	„Das Online-Widerrufsrecht im Spiegel der Rechtsprechung – Eine Bestandsaufnahme zur Fortentwicklung des Online-Widerrufsrechts durch die Judikative", CR 2006, S. 764-770
Kennedy, Angus J.	*The Rough Guide to The Internet*, 6. Aufl., Rough Guides Ltd., London 2000
Kerr, Orin S.	„Computer Records and the Federal Rules of Evidence", U.S. Department of Justice, United States Attorneys's USA Bulletin, März 2001, Vol. 49, No. 2, www.usdoj.gov/criminal/cybercrime/usamarch2002_4.htm
Kilian, Wolfgang	„The UN-Convention on the Use of E-Communications in International Contracts – Applicability, scope and potential impact of the emerging pendant CISG", CRi 2007, S. 101-106
Kind, Michael / Dennis Werner	„Rechte und Pflichten im Umgang mit PIN und TAN", CR 2006, S. 353-360
Klees, Andreas	„Anmerkung zu BGH, Urt. v. 16.03.2006 - III ZR 152/05 – Haftung des Anschlussinhabers für R-Gespräche", CR 2006, S. 458-460
Klein, Susanne	„Die Beweiskraft elektronischer Verträge – Zur Entwicklung der zivilprozessrechtlichen Vorschriften über die Beweiskraft elektronischer Dokumente", JurPC Web-Dok. 198/2007, Abs. 1-71
Kochinke, Clemens / Matthias Geiger	„Trends im US-Computer- und Internetrecht", K & R 2000, S. 594-602
Kodek, Georg E.	„Der Zivilprozeß und neue Formen der Informationstechnik", ZZP 2002, S. 445-490
Köhler, Markus / Hans-Wolfgang Arndt	*Recht des Internet*, C.F. Müller Verlag, 5. Aufl., Heidelberg 2006

Kröger, Detlef / Marc André Gimmy	*Handbuch zum internetrecht – Electronic Commerce – Informations-, Kommunikations- und Mediendienste*, 2. Aufl., Springer, Berlin / Heidelberg 2002
Kye, Cecilia	„E-Commerce in the EU: Bringing Businesses and Consumers Aboard“, CLSR 2001, vol. 17, S. 25-27
Lapp, Thomas	„Elektronische Rechnung – Zulässigkeit, Vorsteuerabzug, Vertragsklauseln“, ITRB 2006, S. 44-47
Leier, Barbara	„Haftung der Zertifizierungsstellen nach dem SigG – Betrachtung der geltenden und Überlegungen zur zukünftigen Rechtslage“, MMR 2000, S. 13-17
Leier, Klaus-Peter	„Elektronischer Handel in der Welthandelsorganisation (WTO)“, MMR 2002, S. 781-787
Lejeune, Mathias	„Die Reform des Widerrufsbelehrungen für den Online Handel – Erste Anmerkungen zum zweistufigen Ansatz der Bundesregierung“, CR 2008, S. 226-231
Lloyd, Ian J.	*Information Technology Law*, 4. Aufl., Butterworths, London 2004
Loewenheim, Ulrich / Frank A. Koch (Hrsg.)	*Praxis des Online-Rechts*, C.H. Beck, München 2001
Lüdemann, Volker / Nils Adams	„Die elektronische Signatur in der Rechtspraxis”, K&R 2002, S. 8-12
Luigs, David A.	„The United States Electronic Signatures law (E-SIGN)“, K&R 2002, S. 533-537
Lutterbeck, Bernd	„Globalisierung des Rechts – am Beginn einer neuen Rechtskultur?“, CR 2000, S. 52-60
ders.	„Das Netz ist der Markt - Governance in der Onlineökonomie“, Sonderausgabe der Zeitung "Das Parlament" vom 25.9.1998
Maennel, Frithjof A.	„Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission“, MMR 1999, S. 187-192
Mankowski, Peter	„Textform und Formerfordernisse im Miet- und Wohnungseigentumsrecht“, ZMR 2002, S. 481-489
ders.	„Wie problematisch ist die Identität des Erklärenden bei E-Mails wirklich?“, NJW 2002, S. 2822-2828
ders.	„Für einen Anscheinsbeweis hinsichtlich der Identität des Erklärenden bei E-Mails – Zugleich Anmerkung zu OLG Köln, Urt. v. 6.9.2002 – 19 U 16/02“, CR 2003, S. 44-50
ders.	„Anmerkung zu LG Bonn, Urt. v. 19.12.2003 – 2 O 472/03 – Sofortkauf-Option bei eBay“, MMR 2004, S. 181-183

ders.	„Zum Nachweis des Zugangs bei elektronischen Erklärungen“, NJW 2004, S. 1901-1907
ders.	„Anmerkung zu LG Aachen, Urt. v. 15.12.2006 – 5 S 184/06 – Handeln in fremdem Namen bei Online-Autkion“, CR 2007, S. 606-607
Marsden, Christopher T.	„Co-Regulation in European Media and Internet Sectors”, MMR 2005, S. 3-7
Mason, Stephen	„Electronic Signatures Explained“, Internet Newsetter for Lawyers January/February 2002, by Delia Venables, www.venables.co.uk/n0201signatures.htm
ders.	„Lawyers and Electronic Signatures“, Internet Newsetter for Lawyers July/August 2005, by Delia Venables, www.venables.co.uk/n0507signatures.htm
ders.	„Electronic Signatures in Practice”, J. High Tech L. 2006 / 2, S. 148-164
ders.	*Electronic Signatures in Law*, 2. Aufl., Tottel Publishing, Haywards Heath, 2007
May, Clifford	„Computer-Based Evidence – The Identification and Recovery of Evidence in Electronic Format”, CLSR 2000, S. 162-165
Mayer, Franz	„Recht und Cyberspace“, NJW 1996, S. 1782-1791
Mayer, Ulrich	„Nichtige Gesellschafterbeschlüsse einer GmbH“, NZG 2007, S. 448-450
McCullagh, Adrian / William Caelli	„Non-Repudiation in the Digital Environment”, First Monday, Vol. 5, No. 8, August 2000, http://.firstmondayorg/issues/issue5_8/mccullagh/ index.html
McKendrick, Ewan	*Contract Law*, 4. Aufl., Palgrave, Basingstoke 2000
Meinel, Christoph / Lutz Gollan	„Der elektronische Personalausweis? – Elektronische Signaturen und staatliche Verantwortung – Was fehlt den heutigen digitalen Signaturen“, JurPC Web-Dok. 223/2002, Abs. 1-15
Menna, Marianne	„From Jamestown to the Silicon Valley, Pioneering A Lawless Frontier: The Electronic Signatures in Global and National Commerce Act”, VJLT 2001, www.vjolt.net/vol6/issue6/v6i2-a12-Menna.html
Miedbrodt, Anja	„Regelungsansätze und -strukturen in US-amerikanischer Signaturgesetzgebung“, DuD 1998, S. 389-394
dies.	„Das Signaturgesetz in den USA – Electronic Signatures in Global and National Commerce Act“, DuD 2000, S. 541-545

dies.	„Unterschiede im Regulierungsverständnis der deutschen und der amerikanischen Rechtskultur“, Bizer, Johann u.a. (Hrsg.), *Umbruch von Regelungssystemen in der Informationsgesellschaft, Freundesgabe für Alfred Büllesbach*, Stuttgart 2002, S. 273-282
Miedbrodt, Anja / Alfred Büllesbach	„Überblick über die internationale Signaturregulierung“, CR 2000, S. 751-757
Miedbrodt, Anja / Patrick Mayer	„E-Commerce – Digitale Signaturen in der Praxis“, MDR 2001, S. 432-436
Moritz, Hans-Werner	„Quo vadis elektronischer Geschäftsverkehr?“, CR 2000, S. 61-72
Müglich, Andreas	„Neue Formvorschriften für den E-Commerce – Zur Umsetzung der EU-Signatur-Richtlinie in deutsches Recht“, MMR 2000, S. 7-13
Muenchinger, Nancy	„E-Commerce – US – Proposed US Legal Solutions to Questions Concerning Electronic Commerce“, CLSR 2000, S. 378-385
Musielak, Hans-Joachim (Hrsg.)	*Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz*, 5. Auflage, München 2007
Nazerali, Julie / David Cowan	„E-Commerce and Cross-Border-Shopping – Can the EU Untangle the Web?“, BLR 2000, Vol. 21, S. 117-118
Neuser, Uwe	„Faule Kunden bei ‘Tante-Emma.com’ – Eine europäische Vertrauenshaftung für elektronische Signaturen”, MMR 1999, S. 67-74
Niemann, Jan-Malte	„Electronic Transactions Bill – Germany – Taking German Private Law to the Digital Era: The Government Bill for the Adjustment of Formal Requirements“, CLSR 2001, Vol. 17, S. 28-31
Nimmer, Raymond T.	„Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws”, http://www.bmck.com/ueta-esign-2.doc
ders.	„UCITA: A Commercial Contract Code”, TCL 2000, Vol. 17, S. 3-19
Noack, Ulrich	„Hauptversammlung und Neue Medien“, BB 1998, S. 2533
ders.	„Digitaler Rechtsverkehr: Elektronische Signatur, elektronische Form und Textform“, DStR 2001, S. 1893-1897
ders.	*Unternehmenspublizität – Bedeutung und Medien der Offenlegung von Unternehmensdaten*, Bundesanzeiger Verlag, Köln 2002

ders.	„Amtliche Unternehmenspublizität und digitale Medien“, in Habersack et. al., *Festschrift für Peter Ulmer zum 70. Geburtstag*, 2003, S. 1244-1262
Noack, Ulrich / Sascha Kremer	„Online-Auktionen: eBay als neue Herausforderung für den Rechtsanwalt?“, AZW Reihe Nummer 2004_12_02 (Dec 27, 2004)
Nöcker, Gregor	„Urkunden und EDI-Dokumente“, CR 2000, S. 176-182
Nowak, Ulrich	„Der elektronische Vertrag - Zustandekommen und Wirksamkeit unter Berücksichtigung des neuen „Formvorschriftenanpassungsgesetzes““, MDR 2001, S. 841-844
Oberndörfer, Julian	„Digitale Wertpapiere im Licht der neuen Formvorschriften des BGB“, CR 2002, S. 358-362
O’Donnell, Beatrice / Thomas A. Lincoln	„Authenticating E-Mail Discovery as Evidence“, The Legal Intelligencer, August 13, 2007, www.law.com/jsp/legaltechnology/PubArticleFriendlyLT.jsp?id=1186736525985
Palandt	*Bürgerliches Gesetzbuch*, 66. Aufl., C.H. Beck, München 2008
Perry, Raymond	„W-conveyancing: Promise and Reality “, Internet Newsetter for Lawyers September/October 2003, by Delia Venables, www.venables.co.uk/n0309econveyancing.htm
ders.	„Does e-conveyancing mean disaster for the High Street conveyancer? The End is Nigh – Or Possibly Not“, Internet Newsetter for Lawyers September/October 2004, by Delia Venables, www.venables.co.uk/n0409 econveyancing.htm
Peters, Falk	„E-Government – eine kleine Tour d´horizon“, CR 2003, S. 68-74
Pullen, Mike / Kelly Logan	„The European Union Proposed Legal Framework for E-Commerce”, ICCLR Spe. 1999, S. 21-28
Ramming, Klaus	„Ermöglichen die neuen §§ 126 Abs. 3, 126a BGB die Ausstellung elektronischer Konnossemente?“, VersR 2002, S. 539-541
Randolph, Jr., Patrick	„Has Congress Murdered the Statute of Frauds?“, http://dirt.umkc.edu/files/sof.htm
Rebmann, Kurt / Franz Jürgen Säcker / Roland Rixeder (Hrsg.)	*Münchner Kommentar zum BGB*, Band 1, Allgemeiner Teil, §§ 1-240, 5. Auflage, München 2006
Redeker, Helmut	„Schriftformerfordernisse im E-Commerce: In welcher Form können Schriftformerfordernisse den E-Commerce behindern?”, ITRB 2001, S. 46-48

Reimann, Mathias	*Einführung in das US-amerikanische Privatrecht*, 2. Aufl., C.H. Beck, München 2004
Rennie, Michele	„EU Electronic Commerce Directive: August 1999 – Amendments Still Avoid Consumer Internet Protection“, CTLR 1999, S. 239-242
Rieß, Joachim	„Selbstregulierungsinstrumente zur vertrauenswürdigen Kommunikation“, DuD 2002, S. 532-535
Roßnagel, Alexander	„Die Sicherheitsvermutung des Signaturgesetzes“, NJW 1998, S. 3312-3320
ders.	„Europäische Signatur-Richtlinie und Optionen ihrer Umsetzung“, MMR 1999, S. 261-266
ders.	„Digitale Signaturen im europäischen elektronischen Rechtsverkehr“, K & R 2000, S. 313-323
ders.	„Auf dem Weg zu neuen Signaturregelungen – Die Novellierungsentwürfe für SigG, BGB und ZPO“, MMR 2000, S. 451-461
ders.	„Das neue Recht elektronischer Signaturen - Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO“, NJW 2001, S. 1817-1826
ders.	„Weltweites Internet – globale Rechtsordnung?“, MMR 2002, S. 67-71
ders.	„Anmerkung zu OLG Köln, Urt. v. 06.09.2002“, K&R-Kommentar, K&R 2003, S. 84-86
ders.	„Die fortgeschrittene elektronische Signatur“, MMR 2003, S. 164-170
ders.	„Elektronische Signaturen mit der Bankkarte? – Das erste Gesetz zur Änderung des Signaturgesetzes“, NJW 2005, S. 385-388
Roßnagel, Alexander / Stefanie Fischer-Dieskau / Ulrich Pordesch / Rals Brandner	„Erneuerung elektronischer Signaturen – Grundfragen der Archivierung elektronischer Dokumente“, CR 2003, S. 301-306
Roßnagel, Alexander / Stefanie Fischer-Dieskau	„Automatisiert erzeugte elektronische Signaturen“, MMR 2004, S. 133-139
dies.	„Elektronische Dokumente als Beweismittel - Neufassung der Beweisregelungen durch das Justizkommunikationsgesetz“, NJW 2006, S. 806-808
Roßnagel, Alexander / Andreas Pfitzmann	„Der Beweiswert der E-Mail“, NJW 2003, S. 1209-1214
Roßnagel, Alexander / Daniel Wilke	„Die rechtliche Bedeutung gescannter Dokumente“, NJW 2006, S. 2145-2150

Rüßmann, Helmut	„Das Beweisrecht elektronischer Dokumente“, http://ruessmann.jura.uni-sb.de/rw20/people/ruessmann/Elbeweis/ELBEWEIS.htm, 1995
Savino, William F. / David S. Widenor	“Emerging Methods of e-Contracting – Will an Electronic “John Hancock” Satisfy the Statute of Frauds?”, Buffalo Law Journal, May 2005, http://www.damonmorey.com/bljmay2005.htm
Saxby, Stephen	„CLSR Briefing – News and Comment on Recent Developments from Around the World”, CLSR 16/2000, S. 55-57
Schapper, Paul / Mercedes Rivolta / Joao Veiga Malta	„Risk and Law in Authentication“, DEJ 2006, Vol. 3, S. 10-16
Scheffler, Hauke / Christian Dressel	„Vorschläge zur Änderung zivilrechtlicher Formvorschriften und ihre Bedeutung für den Wirtschaftszweig E-Commerce“, CR 2000, S. 378-384
Schindler, Werner	„Technik und Recht – Sichere digitale Kommunikation – Motivation, Anforderungen, mathematisch-technische Realisierung und rechtliche Aspekte“, K&R 2002, S. 481-490
Schirmbacher, Martin	„Von der Ausnahme zur Regel: Neue Widerrufsfristen im Online-Handel? – Zugleich Anmerkungen zu den Urteilen des KG v. 18.7.2006 – 5 W 156/06 und des OLG Hamburg v. 24.8.2006 – 3 U 103/06“, CR 2006, S. 673-677
Schmidl, Michael	„Die elektronische Signatur – Funktionsweise, rechtliche Implikationen, Auswirkungen der EG-Richtlinie“, CR 2002, S. 508-517
Schmidt, Markus / Michael Pruß / Christian Kast	„Technische und juristische Aspekte zur Authentizität elektronischer Kommunikation“, CR 2008, S. 267-272
Schneider, Jochen	*Handbuch des EDV-Rechts – IT-Vertragsrecht – Rechtsprechung – AGB – Vertragsgestaltung - Datenschutz – Rechtsschutz*, 3. Aufl., Verlag Dr. Otto Schmidt, Köln 2003
Scholz, Oliver	„Die Einführung elektronischer Handelsregister im Europarecht“, EuZW 2004, S. 172-176
Schöttle, Hendrik	„Zahlungsmittel im elektronischen Geschäftsverkehr“, K&R 2007, S. 183-187
Schumacher, Stephan	„Digitale Signaturen in Deutschland, Europa und den USA – Ein Problem, zwei Kontinente, drei Lösungen?“, CR 1998, S. 758-763
Schweinoch, Martin / Dietmar Böhlke / Christoph Richter	„E-Mails als elektronische Geschäftsbriefe mit Nebenwirkungen – Bedeutung und Tragweite der neuen Pflichtangaben für den elektronischen Geschäftsverkehr“, CR 2007, 167

Schwemmer, Jürgen	„Lösungen und Probleme – Ein langer Weg zur Interoperabilität“, www.bundesnetzagentur.de/media/archive/1350.pdf
Shears, Peter / Graham Stephenson	*James' Introduction to English Law*, Butterworths, London / Dublin / Edinburgh 1996
Selby, John	„Enhancing Trust in Online Auctions: eBay's Australian Experience With Code and Law“, Cri 2007, S. 172-176
Singleton, Susan	*eCommerce: A Practical Guide to the Law*, Gower, Aldershot 2001
Smedinghoff, Thomas J.	„The Legal Requirements for Creating Enforceable Electronic Transactions”, Sept. 2002, www.bmck.com/ecommerce/article-electronic-transactions2.doc
Smedinghoff, Thomas J. / Ruth Hill Bro	„Moving With Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce”, JMJCIL 1999, Vol. 17, S. 723ff.
Sookman, Barry	„Legal Framework for E-Commerce Transaction”, CTLR 2001, Vol. 7, S. 85-95
Spindler, Gerald	„Anmerkung zu OLG Brandenburg, Urt. v. 16.11.2005 – 4 U 5/05 – Störerhaftung von eBay bei Identitätsdiebstahl“, MMR 2006, S. 110-111
Splittgerber, Andreas	„Die elektronische Form von bestimmenden Schriftsätzen“, CR 2003, S. 23-28
Stadler, Astrid	„Der Zivilprozeß und neue Formen der Informationstechnik“, ZZP 2002, S. 413-444
Stadler, Thomas	„Widerrufsfrist bei eBay-Auktionen – Können Webseiten die Voraussetzungen der Textform nach § 126b BGB erfüllen?“, JurPC Web-Dok. 136/2006, Abs. 1-26
Steinbeck, Anja	„Die neuen Formvorschriften im BGB“, DStR 2003, S. 644-650
Storr, Stefan	„Elektronische Kommunikation in der öffentlichen Verwaltung – Die Einführung des elektronischen Verwaltungsakts“, MMR 2002, S. 579-584
Tetley, William	„Mixed Jurisdictions: Common Law vs. Civil Law (codified and uncodified) (Part I)“, ULR 3/1999, S. 591-619
Thomale, Hans-Christoph	„Die Haftungsregelung nach § 11 SigG“, MMR 2004, S. 80-86
Tinnefeld, Marie-Theres	„Das Erbe Montesquieus, Europäisierung und Informationsgesellschaft“, MMR 2006, S. 23-27
Ulmer, Detlef	„Online-Vertragsschluss – ein Verfahren wird populär?“, CR 2002, S. 208-213

Vehslage, Thorsten	„Das geplante Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr", DB 2000, S. 1801-1805
ders.	„Beweiswert elektronischer Dokumente", K&R 2002, S. 531-533
Viefhues, Wolfram	„Referentenentwurf des Justizkommunikationsgesetz (JKomG) – auf dem Wege zur elektronischen Gerichtsakte", CR 2003, S. 541-548
ders.	„Das Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz", NJW 2005, S. 1009-1016
Viefhues, Wolfram / Helmut Hoffmann	„ERVG: Gesetz zur Verhinderung des elektronischen Rechtsverkehrs? – Praktische Auswirkungen des Diskussionsentwurfs und Anpassungsbedarf an die Regelungen bei den Gerichten der europäischen Gemeinschaften", MMR 2003, S. 71-76
Viefhues, Wolfram / Karl-Heinz Volesky	„Elektronischer Rechtsverkehr – wird die Chance genutzt?", K&R 2003, S. 59-64
Walden, Ian /Julia Hörnle (Hrsg.)	*E-Commerce Law and Practice in Europe*, ECLIP, Woodhead Publ. Ltd., Cambridge 2001
Wiebe, Andreas	„Anmerkung zu AG Erfurt, Urt. v. 14.09.2001 – 28 C 2354/01 – Nachweis der Authentizität bei Internetauktionen", MMR 2002, S. 128-129
ders.	„Anmerkung zu LG Bonn, Urt. v. 07.08.2001 – 2 O 450/99 – Identität eines Teilnehmers an einer Internetauktion", MMR 2002, S. 257-258
Wietzorek, Michael	„Der Beweis des Zugangs von Anhängen in E-Mails", MMR 2007, S. 156-159
Will, Martin	„Wahlen und Abstimmungen via Internet und die Grundsätze der allgemeinen und gleichen Wahl", CR 2003, S. 126-133
Willer, Christoph / Peter Hoppen	„Computerforensik – Technische Möglichkeiten und Grenzen", CR 2007, S. 610-616
Winter, Ralf	„Anmerkungen zum Urteil des AG Erfurt vom 14.09.2001 – 28 C 2354/01". JurPC Web-Dok. 109/2002, www.jurpc.de/aufsatz/20020109.htm
ders.	„Anmerkung zu LG Konstanz, Urt. v. 19.04.2002 – 2 O 141/01 A – Darlegungs- und Beweislast bei Onlineauktion", MMR 2002, S. 836-837
Worthy, John / Grant Anderson	„E-Commerce UK – UK Moves Towards Electronic Commerce Bill", CLSR 1999, S. 397-400
Wuermeling, Ulrich	„E-Commerce – Germany: Implementation of the E-Commerce-Directiv in Germany, CLSR 2001, S. 168-169

York, Stephen / Daniel Tunkel	*E-Commerce – A Guide to the Law of Electronic Business*, 2nd. Edition, Butterworths, London 2000
Zetzsche, Dirk	„Die Aktionärsrechte-Richtlinie: Auf dem Weg zur virtuellen Hauptversammlung“, NZG 2007, S. 686-692
Zöller, Richard (Hrsg.)	*Zivilprozessordnung*, 27. Aufl., Verlag Dr. Otto Schmidt, Köln 2007