ISBN 978-3-8329-5035-4

Menke • Die elektronische Signatur im deutschen und brasilianischen Recht

22

Der Elektronische Rechtsverkehr 22

Fabiano Menke

Die elektronische Signatur im deutschen und brasilianischen Recht

Eine rechtsvergleichende Studie

Nomos

Der Elektronische Rechtsverkehr

Herausgegeben von
Prof. Dr. Alexander Roßnagel
in Zusammenarbeit mit
dem TeleTrusT Deutschland e.V.

Band 22

Fabiano Menke

Die elektronische Signatur im deutschen und brasilianischen Recht

Eine rechtsvergleichende Studie

Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Kassel, Univ., Diss., 2008
Institut für Wirtschaftsrecht
Tag der Disputation: 16. Dezember 2008

ISBN 978-3-8329-5035-4

1. Auflage 2009

Vorwort des Herausgebers

Elektronische Signaturen haben für den Rechts- und Geschäftsverkehr in elektronischen Netzen eine steigende Bedeutung. Elektronische Daten können jederzeit spurenlos verändert werden. Sie bieten daher keine verlässliche Grundlage für rechtliche Verpflichtungen und Berechtigungen. Im Streitfall taugen sie nicht als Beweismittel, weil mit ihrer Hilfe nicht nachgewiesen kann, ob sie sich noch in ihrem Originalzustand befinden. Nur mit Hilfe elektronischer Signaturen kann die Integrität und Authentizität elektronischer Willenserklärungen technisch sichergestellt und geprüft werden. Elektronische Signaturen sind daher die Basistechnologie des elektronischen Rechtsverkehrs. Sie finden in allen Staaten, auch in Brasilien und Deutschland, zunehmende Verbreitung.

Deutschland war der erste souveräne Staat, der für seine gesamte Rechtsordnung eine gesetzliche Regulierung elektronischer Signaturen verabschiedet hat. Durch das Signaturgesetz und die Signaturverordnung hat er 1997 eine umfassende Regelung des Angebots von Signaturverfahren getroffen und Sicherheitsanforderungen für die Technik und die organisatorische Sicherungsinfrastruktur elektronischer Signaturen festgelegt. Diese Regelungen wurden 2001 in einem neuen Signaturgesetz und einer neuen Signaturverordnung überarbeitet. Eine spezifische Beweisregelung, die auf die durch das Signaturgesetz gewährleistete Sicherheit Bezug nahm, wurde 2001 in § 292a ZPO erlassen und 2005 in Form des § 371a ZPO überarbeitet.

Brasilien hat seit 2001 Regelungen zur elektronischen Signatur in dem Präsidialerlass Medida Provisória Nr. 2.200, die zurzeit in ihrer dritten Ausgabe Nr. 2.200-2 in Kraft ist. Konkretisiert werden diese Regelungen durch zahlreiche Festlegungen eines Regulierungsausschusses. Aufgrund dieses Regelungskomplexes ist seit 2001 die Sicherungsinfrastruktur Brasiliens „Infra-Estrutura de Chaves Públicas Brasileira – ICP Brasil“ mit den Angeboten der brasilianischen Zertifizierungsdiensteanbieter aufgebaut worden. Die brasilianischen Signaturregelungen sind in ihren Grundprinzipien stark von der Gesetzgebung in Deutschland beeinflusst worden. Eine besondere Beweisregelung für elektronische Signaturen kennt das brasilianische Recht in Art. 10 § 1 Medida Provisória Nr. 2.200, die für akkreditierte Signaturen eine Echtheitsvermutung (mit unklaren Einschränkungen) vorsieht. Brasilien befindet sich in einer Übergangsphase, in der eine Überarbeitung des Regelwerks ansteht. Ein Entwurf für eine neue Regelung des Signaturrechts liegt im Parlament vor. Eine Analyse, die Vor- und Nachteile der deutschen Lösung für Brasilien aufarbeitet, könnte in dieser Situation sehr unterstützend wirken.

Für einen Rechtsvergleich zwischen Brasilien und Deutschland sind vor allem zwei Aspekte interessant, nämlich erstens die Sicherheitsanforderungen an die Funktionen der Sicherungsinfrastruktur und zweitens die auf dieser Sicherheit aufbauenden Regelungen des Beweisrechts.

Elektronische Signaturen können nicht voraussetzungslos genutzt werden. Während eine eigenhändige Unterschrift von jedem jederzeit hergestellt und geprüft werden kann, benötigen elektronische Signaturen eine umfangreiche Infrastruktur, die das Handwerkszeug zur Erzeugung und Prüfung von elektronischen Signaturen zur Verfügung stellen sowie die Sicherheit der gesamten Signaturverfahren gewährleisten muss. Die Knoten dieser Infrastruktur sind Zertifizierungsdiensteanbieter, die die Teilnehmer am elektronischen Rechtsverkehr identifizieren, die erforderlichen kryptographischen Schlüssel generieren, die öffentlichen Schlüssel zertifizieren, die Schlüsselpaare personalisieren und an die Teilnehmer ausgeben sowie ein permanentes Angebot von Verzeichnis-, Sperr- und Zeitstempeldiensten anbieten. Diese Leistungen der Sicherungsinfrastruktur sind notwendig, um Integrität und Authentizität elektronischer Signaturen gewährleisten und in Beweisverfahren prüfen zu können. Selbst bei gleichen Funktionen und gleicher Sicherheit kann sich das Maß der Vertrauenswürdigkeit in ihre Gewährleistung von Anbieter zu Anbieter unterscheiden, je nach dem, ob die Funktionserfüllung und ihre Sicherheit nur behauptet und gegenüber einer Behörde angezeigt wird, oder ob die Behörde diese vor Betriebsaufnahme – etwa in Form einer Akkreditierung – geprüft hat.

Der zweite Aspekt betrifft die Beweisregelungen, die für elektronische Signaturen im nationalen Beweisrecht vorgesehen sind. Wenn die Mathematik, die Technik und vor allem die organisatorische Infrastruktur sicher und vertrauenswürdig sind, könnte ein signiertes elektronisches Dokument auch mit besonderen Beweiswirkungen versehen werden. Je nach dem, wie vertrauenswürdig die Sicherungsinfrastruktur und die auf ihrer Grundlage erzeugten elektronischen Signaturen sind, können die Signaturen eventuell Grundlage eines Anscheinsbeweises oder gar einer Beweisvermutung sein.

Für beide Fragen hat Deutschland in seiner Rechtsordnung spezifische Antworten gegeben. Diese werden samt der signaturrechtlichen und beweisrechtlichen Dogmatik von Herrn Menke analysiert und bewertet. Ihnen werden eine Analyse und Bewertung der gleichen Aspekte im brasilianischen Recht gegenüber gestellt. Aus dem Vergleich werden wertvolle Schlussfolgerungen für das brasilianische Recht gezogen, die zu dessen Fortentwicklung beitragen können.

Mit dem vorliegenden Buch füllt Herr Menke eine Lücke der Rechtsvergleichung, die eine große praktische Relevanz hat. Indem er grundlegende Fragen nach der rechtstechnischen und dogmatischen Bearbeitung vergleichbarer Probleme in Brasilien und Deutschland systematisch analysiert, liefert er einen wichtigen Beitrag für mögliche Optionen rechtswissenschaftlicher Lösungen. Indem er aus dem Vergleich rechtlich angeleitete Vorschläge zur Fortentwicklung des Signaturrechts entwickelt, bietet er der Rechtspolitik wertvolle praxisrelevante Hinweise. Es ist der Arbeit zu wünschen, dass sie von den Politikern und Praktikern zur Kenntnis genommen wird und die Fortentwicklung des Signaturrechts in beiden Staaten beeinflusst.

Kassel, im Juli 2009 *Alexander Roßnagel*

Vorwort des Autors

Elektronische Signaturen sind die Basistechnologie für einen sicheren elektronischen Rechtsverkehr. Sie leisten einen wichtigen Beitrag für die Lösung des Problems der Authentizität und Integrität elektronischer Kommunikation und elektronischer Daten. Damit elektronische Signaturen erzeugt und geprüft werden können ist eine Sicherungsinfrastruktur aus Dienstleistern, Standards und Regeln erforderlich. Mit der Verabschiedung des ersten Signaturgesetzes aus dem Jahre 1997 – das erste Gesetz zur elektronischen Signatur für den gesamten Rechtsraum eines Landes – hat Deutschland eine Vorreiterrolle bei der Regulierung in diesem Bereich eingenommen. Das zweite und noch geltende Signaturgesetz wurde im Jahr 2001 angesichts des Erlasses der europäischen Richtlinie 1999/93 ins Leben gerufen. Deutschland hat darüber hinaus eine Reihe von Gesetzen verabschiedet, die die Anwendung und Rechtsfolgen elektronischer Signaturen regeln. Brasilien hat diese internationale Entwicklung nicht außer Acht gelassen. 2001 erließ die brasilianische Regierung die Medida Provisória Nr. 2.200, die sowohl Regelungen für eine Infrastruktur für elektronische Signaturen als auch eine Vorschrift zum Beweiswert elektronisch signierter und nicht signierter Dokumente vorsieht.

Die Vorreiterrolle Deutschlands hat die Realisierung der vorliegenden Arbeit motiviert. Sie ist als Rechtvergleichung angelegt. Verglichen werden die rechtlichen Bestimmungen des deutschen und des brasilianischen Signaturrechts zur Technik und Organisation sowie die beweisrechtlichen Vorschriften beider Länder bezüglich elektronisch signierter Daten. Ziel der Arbeit ist es, eine Verbesserung der brasilianischen Signaturregulierung und des angeknüpften Beweisrechts durch Rezeptionsvorschläge zu empfehlen. Die Arbeit wurde im Wintersemester 2008/2009 von der Universität Kassel als Dissertation angenommen.

An dieser Stelle möchte ich mich bei den Personen bedanken, die zum Gelingen der Arbeit beigetragen haben.

Für die intensive Betreuung der Dissertation sowie für die ständige Diskussionsbereitschaft danke ich meinem Doktorvater Prof. Dr. Alexander Roßnagel. Ich danke ihm außerdem für die schnelle Begutachtung der Arbeit und für die Annahme der Arbeit in die Schriftenreihe „Der Elektronische Rechtsverkehr“. Herrn Prof. Dr. Hans-Georg Flickinger danke ich für die Erstellung des Zweitgutachtens. Bei meinen Kollegen der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) bedanke ich mich für die wertvollen Diskussionsbeiträge und freundliche Unterstützung während meiner Zeit in Kassel. Erwähnen möchte ich auch die Namen von Andreas Hübner und Alexander Lyschik für die schwierige Arbeit des Korrekturlesens.

Meiner Frau Vanessa und meinem Sohn Thomas danke ich besonders für die unendliche und liebvolle familiäre Unterstützung. Für die akademische Motivation und Unterstützung seit der Studiumzeit bedanke ich mich bei Prof. Dr. Cláudia Lima Marques und Prof. Dr. Véra Maria Jacob de Fradera.

Der Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES und dem DAAD – Deutscher Akademischer Austauschdienst – danke ich für die Förderung meiner Promotion.

Ein herzlicher Dank gilt außerdem meinen Eltern, die mich kontinuierlich unterstützt haben und meinen Freunden Rafael Koerig Gessinger, Gustavo Vieira da Costa Cerqueira und Paulo César Rutzen.

Porto Alegre, im Juni 2009 Fabiano Menke

Inhaltsverzeichnis

Abkürzungsverzeichnis

a. A.	anderer Ansicht
Abs.	Absatz
AC	Autoridade Certificadora
AcP	Archiv für die civilistische Praxis
AO	Abgabenordnung
Ap. Civ.	Apelação Cível
APuZ	Aus Politik und Zeitgeschichte
AR	Autoridade de Registro
Art.	Artikel
BB	Betriebsberater
Bd.	Band
BeurkG	Beurkundungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BMFB	Bundesministerium
BNetzA	Bundesnetzagentur
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
bzw.	beziehungsweise
CC	Código Civil
CDC	Código de Defesa do Consumidor
CF	Constituição Federal
CPC	Código de Processo Civil
CR	Computer und Recht
CRL	Certificate Revocation List
DPC	Declaração de Práticas de Certificação
d.h.	das heißt
DuD	Datenschutz und Datensicherheit
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
Einl.	Einleitung
et al.	et alii
f.	folgend(e)
ff.	fortfolgende

FIPS	Federal Information Processing Standard
GG	Grundgesetz
HGB	Handelsgesetzbuch
Hrsg.	Herausgeber
ICP	Infraestrutura de Chaves Públicas
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ICST	Institute of Computer Sciences and Technology
i.E.	im Erscheinen
IETF	Internet Engineering Task Force
ITI	Instituto Nacional de Tecnologia da Informação
ITU	International Telecommunication Union
JA	Juristische Arbeitsblätter
MMR	Multimedia und Recht
MP	Medida Provisória
NJW	Neue Juristische Wochenschrift
NJW-RR	Neue Juristische Wochenschrift Rechtsprechungs-Report
Nr.	Nummer
OCSP	Online Certificate Status Protocol
OLG	Oberlandsgericht
OWiG	Gesetz über Ordnungswidrigkeiten.
PassG	Passgesetz
PC	Política de Certificado
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PIN	Persönliche Identifikationsnummer
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
Provet	Projektgruppe verfassungsverträgliche Technikgestaltung
PTB	Physikalisch-Technisch Bundesanstalt
RDC	Revista de Direito do Consumidor
REsp	Recurso Especial
RF	Revista Forense
RFC	Request for Comments
RLeS	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates v. 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen
Rn.	Randnummer(n)
RP	Revista de Processo
RS	Rio Grande do Sul
RT	Revista dos Tribunais
RTDC	Revista Trimestral de Direito Civil
s.	siehe
S.	Seite

SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SigV	Signaturverordnung
SP	São Paulo
SPED	Sistema Público de Escrituração Digital
SSL	Security Sockets Layer
SSST	Secretaria de Segurança e Saúde no Trabalho
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
SUSEPE	Superintendência de Seguros Privados
TARS	Tribunal de Alçada do Estado do Rio Grande do Sul
TJPR	Tribunal de Justiça do Estado do Paraná
TJRS	Tribunal de Justiça do Estado do Rio Grande do Sul
TJSP	Tribunal de Justiça do Estado de São Paulo
TPM	Trusted Platform Module
UmweltHG	Umwelthaftungsgesetz
UStG	Umsatzsteuergesetz
v.	verkündet
vgl.	vergleiche
VwVfG	Verwaltungsverfahrensgesetz
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
z.B.	Zum Beispiel
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik
ZZP	Zeitschrift für Zivilprozess

1. Teil: Einführung

1. Forschungsanlass

Mit Beginn der zweiten Hälfte der 90er Jahre im vorigen Jahrhundert wurde die Entwicklung der elektronischen Datenverarbeitung immer intensiver. Neu dabei war jedoch die Verarbeitung der Daten in Netzwerken. Diese haben sich mit den nationalen Netzen schließlich zu einem weltweit verknüpften Netz, dem Internet, verbunden. Mit Hilfe dieses Mediums werden Geschäfte abgewickelt, Mitteilungen ausgetauscht, Auskünfte eingeholt sowie unzählbare andere Dienstleistungen erbracht. Die Vorteile, welche mit der Anwendung des neuen Mediums entstehen, sind zahlreich, besonders was Kosteneinsparung und Schnelligkeit anbetrifft. Jedoch weist das Internet auch Probleme auf, so fehlt zum Beispiel die Klarheit über die Identität des Kommunikationspartners, da das Internet eine anonyme Kommunikation ermöglicht. Ebenso fehlt die Gewissheit darüber, dass die übermittelten Nachrichten unversehrt geblieben sind. Diese Probleme der Integrität und der Authentizität elektronisch erzeugter Daten sind dem Medium inhärent. Sie wurden mit dem massenhaften Anstand elektronischer Dokumente sowie durch das Internet virulent.

Um die Gewissheit in Hinsicht auf die Unversehrtheit der Nachricht und die Identität der Kommunikationspartner zu erhöhen, damit es möglich ist, Geschäfte und Mitteilungen mit größt möglicher Sicherheit zu tätigen, wurde als technische Lösung die digitale Signatur[1] entwickelt. Seit Mitte der 90er Jahre sind die Staaten dazu übergegangen, das Angebot und die Verwendung elektronischer Signaturen zu regeln. Auf diese Weise wurden bestimmte Methoden gesetzlich anerkannt, um einen hohen Grad von Sicherheit zu erreichen und damit für die abgegebenen Willenserklärungen, welche über die Computernetze weitergeleitet werden, Urheberschaft und Integrität (Echtheit) sicherzustellen.

Aus diesen Gründen hat der nordamerikanische Staat Utah im Jahre 1995 das erste Gesetz über die digitale Signatur erlassen, den sogenannten *Utah Digital Signature Act.* Deutschland war das erste Land Europas, welches durch ein Bundesgesetz die digitale Signatur regelte. Dieses „*Informations- und Kommunikationsdienste-Gesetz*“ vom 1. August 1997 enthielt Regelungen für Kommunikationsdienstleistungen und führte in Artikel 3 dieses Artikel-Gesetzes, dem Signaturgesetz die elektronische Signatur in das deutsche Rechtssystem ein.

Im Jahre 1999 erließ die Europäische Gemeinschaft die Richtlinie 1999/93, in welcher speziell die strukturellen Bedingungen der elektronischen Signatur europa-

1 Die digitale Signatur wird auf der Grundlage asymmetrischer Signaturverfahren erstellt und stellt damit nur eine Methode zur Erstellung elektronischer Signaturen dar. Die digitale Signatur ist somit ein Unterbegriff des Oberbegriffs elektronische Signatur.

weit geregelt werden. Deutschland sah sich dadurch gezwungen, ein neues Signaturgesetz auszuarbeiten, um sich den neuen europäischen Regelungen anzupassen. Dies geschah im Jahre 2001 durch das neue deutsche Signaturgesetz. 2005 wurde es bereits das erste Mal novelliert.

Außerdem hat Deutschland in der Folge eine Reihe von Gesetzen erlassen, welche die Anwendung elektronischer Signaturen und deren Rechtsfolgen regeln. Beispiele hierfür sind das Formanpassungsgesetz von 2001, das Dritte Verwaltungsverfahrensänderungsgesetz von 2002 sowie das Justizkommunikationsgesetz von 2005.

Durch diese Gesetzgebungsinitiativen erscheint Deutschland auf dem internationalen Schauplatz als Vorreiter in der Regelung elektronischer Signaturen. Brasilien hat ebenso die elektronische Signatur und ihre juristischen Auswirkungen durch die Medida Provisória Nr. 2.200 vom 28. Juni 2001 – welche bis heute in ihrer dritten Ausgabe unter Nr. 2.200-2 vom 24. August 2001 in Kraft ist – geregelt. Die Medida Provisória Nr. 2.200 und ihre Novellierungen haben die sogenannte ¨Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil“ (Brasilianische Infrastruktur Öffentlicher Schlüssel oder PKI) ins Leben gerufen. Ziel dieser „Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil“ ist es, der Gesamtheit von Interessenten, die den Wunsch haben, virtuelle Kommunikationen und Geschäfte mit ausreichender Sicherheit zu tätigen, verlässliche elektronische Signaturen zur Verfügung zu stellen.

Die Grundprinzipien, welche von dem regulativen Normenkomplex der ICP-Brasil angenommen wurden, sind bereits durch die deutsche Gesetzgebung beeinflusst worden. Dies gilt z.B. für die Notwendigkeit, ein Amt des öffentlichen Rechts an die Spitze der Hierarchie der dienstleistenden Unternehmen zu setzen. Im brasilianischen Fall handelt es sich dabei um das „Instituto Nacional de Tecnologia da Informação“, dessen Kernaufgabe darin besteht, andere dienstleistende Unternehmen im Bereich elektronischer Signaturen zuzulassen, diese zu überwachen sowie dafür zu sorgen, dass die rechtlichen Vorgaben, die sich auf die Tätigkeit beziehen, angewendet werden – dies alles mit dem Ziel, die Sicherheit des Systems und den Schutz des Verbrauchers zu gewährleisten.

Brasilien steht in einer Übergangsphase bei der Regulierung elektronischer Signaturen, obwohl die ICP-Brasil völlig operativ ist. Im Parlament wird der Gesetzentwurf Nr. 7.316/2002 diskutiert, welcher die Medida Provisória Nr. 2.200-2 ersetzen soll, jedoch ohne ihre Grundsätze zu widerrufen. Da sich Brasilien in seinem Regulierungsansatz an Deutschland orientiert und daher deutsche Lösungsansätze übertragbar sind, erscheint es gewinnbringend, eine vergleichende Untersuchung durchzuführen, die das Hauptziel hat, für die brasilianische Diskussion die Kenntnisse über die Verbindung zwischen diesen neuen Technologien und dem Recht zu erweitern und insbesondere Anregungen für die Fortentwicklung des Signaturrechts in Brasilien darzulegen. Das erste Modell (deutsches Modell) ist schon gut ausgebaut und praktisch konsolidiert. Das zweite Modell (brasilianisches Modell) wird noch ausgearbeitet und es fehlen, wie diese Arbeit zeigen wird, noch einige spezifische Regelungen, beziehungsweise könnten manche dieser Regelungen verbessert werden.

2. Untersuchungsgegenstand und seine Abgrenzung

Gegenstand dieser Arbeit ist es, einen Vergleich zwischen den rechtlichen Bestimmungen des deutschen und des brasilianischen Signaturrechts zur Technik und Organisation sowie zwischen den beweisrechtlichen Vorschriften beider Länder herzustellen.

Nicht im Mittelpunkt der vorliegenden Arbeit sind jedoch diejenigen Fragen, welche sich auf die Anwendungen der elektronischen Signatur wie zum Beispiel elektronische Vertragsschließung beziehen. Daher können Fragen nach den anwendbaren Regeln, der Abgabe einer elektronischen Willenserklärung, Angebot und Annahme sowie Zeitpunkt und Ort des Abschlusses eines Vertrags allenfalls am Rande behandelt werden. Eventuelle Bezugnahmen auf diese Konzepte können jedoch als illustrative Bemerkungen genutzt werden.

Die Forschungsarbeit beschränkt sich auf die Betrachtung der Regelungen zur elektronischen Signatur sowie auf die damit verbundenen Organisationen und weiterhin auf die Auswirkungen ihrer Verwendung betreffend die Beweisführung mit elektronisch signierten Dokumenten.

3. Methode und Gang der Untersuchung

Die vorliegende Untersuchung ist als Rechtsvergleich angelegt. Der methodologische Prozess der Untersuchung durchläuft grundsätzlich die drei klassischen Schritte von *Constantinesco*[2], nämlich: Darstellen, Verstehen und Vergleichen. Die Darstellung[3] dient der Kenntnis der gegenüberzustellenden Rechtsinstitute, welche den späteren Vergleich ermöglichen wird. Dabei sind die zu vergleichenden Elemente einzeln und gesondert anhand der Originalquellen beider Länder zu untersuchen. Es werden vor allem Materialien, Texte, Urteile, Literatur sowie Gesetze verwendet. Die Darstellung erfolgt generell ohne kritische Wertung.[4] Des Weiteren wird die Darstellung überdies sukzessiv durchgeführt. Dies bedeutet, dass die zu vergleichenden Elemente unterteilt und hintereinander spezifisch der Staaten getrennt dargestellt werden. Die andere Möglichkeit wäre, die Elemente simultan darzustellen, indem für jede Thematik die Lösungen der verschiedenen Rechte einander unmittelbar behandelt würden.[5] Die sukzessive Darstellung bietet jedoch eine bessere Möglichkeit, sich ein vollständiges Bild der analysierten Begriffe zu machen. Aus diesem Grund wurde sie in dieser Arbeit präferiert.

2 *Constantinesco* 1972, 137.

3 *Zweigert*/*Kötz* 1996, 42, sprechen von der Notwendigkeit Länderberichte fertigzustellen, in denen für jede Rechtsordnung oder auch für jeden Rechtskreis gesondert und mit allen bedeutsamen Nuancen der Gestaltung referiert wird.

4 *Zweigert*/*Kötz* 1996, 42.

5 *Constantinesco* 1972, 330.

Das Verstehen des zu vergleichenden Elements verlangt vom Durchführenden des Rechtsvergleiches im ursprünglichen Sinn vom *Constantinesco* die determinierenden Elemente der Rechtsordnung, ebenso zu kennen als auch die außerrechtlichen Elemente, welche das politische, wirtschaftliche und soziale Milieu prägen. Vermieden werden soll, dass der Rechtsvergleicher das untersuchte Rechtsinstitut in all seinen technischen Einzelheiten kennt, ohne dass er die Rolle versteht, welche es in der betreffenden Rechtsordnung spielt.[6] Ebenso ist der Einfluss anderer benachbarter oder ergänzender Rechtsinstitute der gleichen Rechtsordnung auf das zu vergleichende Element zu untersuchen.[7]

Der Vergleich erfolgt mittels der Gegenüberstellung der zu vergleichenden Elemente. Schwerpunkt dieser dritten Phase ist die Erstreckung der analytischen Untersuchung der Darstellung auf die kritische Würdigung der zum Vergleich hervorgehobenen Elemente. Der Vergleich verfolgt überdies das Ziel, Rezeptionsvorschläge – besonders für das brasilianische Recht – zu unterbreiten. Dabei ist der Begriff Rezeption in Anlehnung der „partiellen Rezeption" zu verstehen, das heißt, nur einzelne rechtliche Elemente oder Rechtsinstitute werden übernommen.[8]

Die beiden ersten Schritte – Darstellen und Verstehen – werden dabei dennoch nicht aufeinander folgend, sondern zum Teil grundsätzlich simultan ausgeführt. Die Phasen sind in der Praxis nicht hermetisch voneinander getrennt. Besonders der zweite Schritt „das Verständnis" des zu vergleichenden Elements wird an manchen Stellen verkürzt dargestellt werden. Zum einem, weist die Problematik der Untersuchung zwar viele Unterschiede in den beiden Ländern auf, zum anderen, sind jedoch die Phänomene der Unsicherheit im elektronischen Geschäftsverkehr sowie die dadurch bedingten technisch-organisatorischen Antworten des Rechts, sowohl in Deutschland und Brasilien, als auch weltweit ziemlich ähnlich, sodass eine detailliertere Ausweitung des Schrittes weniger zielführend für die Untersuchung wäre. Die Regelungen – wie diese Arbeit zeigen wird – unterscheiden sich teilweise lediglich geringfügig in einem Punkt, welcher jedoch bereits für rechtssichere oder rechtsunsichere Lösungen ausschlaggebend sein kann. Schließlich können diese Feinheiten einen entscheidenden Einfluss auf die gesamte Sicherheit des elektronischen Geschäftsverkehrs haben und sind deshalb herauszuarbeiten. Diese „kleinen" Unterschiede zwischen den Signaturregelungen beider Länder verlangen in der Regel aber keine umfangreiche Erklärung. Es ist für das Erfassen der Gesamtproblematik nicht notwendig, weshalb in Deutschland so und in Brasilien anders geregelt wird. Diese Unterschiede werden in einer sehr spezifischen technischen-dogmatischen Ebene festgelegt, welche relativ weit von einer Beziehung zu sozialen

6 *Constantinesco* 1972, 232.

7 *Constantinesco* 1972, 242.

8 Wie von *Constantinesco* 1972, 413 definiert. Von der *partiellen Rezeption* unterscheidet dieser Autor die *globale Übernahme*, wenn etwa ein ganzes Gesetzbuch übernommen wird, und die *eklektische Rezeption*, für den Fall, dass der rezipierende Staat Anleihen aus den Rechtsordnungen mehrerer Staaten entnimmt.

oder politischen Faktoren liegt, sodass die nähere Betrachtung fehl ginge. Eine andere Situation wäre als Beispiel gegeben, wenn diese Untersuchung den Vergleich des Rechtsinstituts „Scheidung der Ehe“ in einem islamistischen Land und in Deutschland zum Gegenstand hätte. In diesem Fall wäre sicherlich eine Fülle von ausführlichen u.a. historischen und soziologischen Überlegungen unabdingbar. In gewissem Sinne handelt es sich bei dieser Arbeit jedoch um einen Mikrovergleich, wie durch den Begriff von *Rheinstein* dargelegt wird.[9] Nach diesem Autor besteht der Mikrovergleich in der Untersuchung eng umgrenzter, konkreter Details eines Rechtssystems, welche jedoch das Ganze nicht außer Acht lassen darf. Die konkreten Aspekte der Analyse dürfen infolgedessen nicht als isolierte Gegebenheiten betrachtet werden, sondern müssen als Teil des Ganzen, nämlich des jeweiligen Rechtssystems behandelt werden.[10] Das Pendant zum Mikrovergleich ist der Makrovergleich, welcher sich mit den Rechtskreisen und Rechtssystemen im Ganzen beschäftig.[11]

Darüber hinaus ist der vorliegende Vergleich synchron oder horizontal, das heißt es werden zeitlich nah beieinander liegende, aber räumlich voneinander entfernte Rechtsordnungen verglichen. Das Gegenstück zum synchronischen Vergleich ist der diachronische oder horizontale Vergleich, welcher zeitlich voneinander entfernte Rechtsordnungen gegenüberstellt.[12]

3.1 Funktionalität

Ein rechtsvergleichendes Vorhaben bedarf einer gewissen Parallelität und Vergleichbarkeit der Vergleichsgegenstände, um wissenschaftlich verwertbare Erkenntnisse gewinnen zu können.[13] Die erforderliche Kongruenz liegt nahe, wenn das beforschte Rechtsinstitut in beiden Rechtsordnungen zu finden ist sowie dieselbe Funktion erfüllt.[14] Diese Vergleichbarkeit oder Funktionalität wird als methodologisches Grundprinzip des gesamten Rechtsvergleichs betrachtet,[15] denn unvergleichbares kann man nicht sinnvoll vergleichen.[16]

9 *Rheinstein* 1987, 32.

10 *Rheinstein* 1987, 32.

11 Für den Makrovergleich wird das Beispiel der Arbeit von *René David* und sein *Les grands systèms de droit contemporains* genannt, welcher die Gesamtheit aller Rechtssysteme zum Gegenstand hat, *Rheinstein* 1987, 33.

12 *Constantinesco* 1972, 51 f., Beispiel für einen diachronischen Rechtsvergleich wäre die Gegenüberstellung eines gegenwärtigen Rechtsinstitutes des deutschen Zivilrechts mit der Ausgestaltung, die es im römischen Recht gehabt hat.

13 *Constantinesco* 1972, 77.

14 *Constantinesco* 1972, 78; *Schwintowski*, JA 1991, 244; *Zweigert*/*Kötz* 1996, 11.

15 *Zweigert*/*Kötz* 1996, 11.

16 Als Beispiel für einen absurden Vergleich, wo keine Vergleichbarkeit gegeben sei, nennt *Constantinesco* 1972, 78 den Vergleich zwischen dem Erbrecht des überlebenden Ehegatten

Wie aus den bereits vorangestellten Überlegungen ersichtlich wird, besteht sowohl in Deutschland als auch in Brasilien die Herausforderung darin, das hohe Sicherheitsbedürfnis im elektronischen Geschäftsverkehr zu befriedigen. Beide Länder haben für diesen Zweck einen Rechtsrahmen geschaffen, zum einen durch die Etablierung einer Sicherungsinfrastruktur aus Dienstleistern, Dienstleistungen, Standards sowie verschiedenen Regeln. Zum anderen durch die Einführung von Vorschriften über die Beweiskraft elektronisch signierter Erklärungen, welche wiederum mit den Sicherheitsanforderungen der Sicherungsinfrastruktur verknüpft sind.

3.2 Kritische Wertung

Notwendiger Teil einer rechtsvergleichenden Untersuchung ist die kritische Wertung der zu vergleichenden Elemente.[17] Diese wird zusammen mit dem Vergleich durchgeführt. Im Ergebnis wird systematisch dargelegt, dass stellenweise eine Lösung sachgerechter als eine andere ist.[18] In dieser Arbeit werden Rezeptionsvorschläge für das brasilianische Recht gemacht. Sie beinhalten Regelungen welche dort nicht existieren und dem deutschen Recht entlehnt wurden. Obwohl ebenso punktuelle Vorschläge für das deutsche Recht gemacht werden, besteht das Hauptziel dieser Untersuchung darin, einen Beitrag zur Verbesserung der brasilianischen Signaturregulierung und des Beweisrechts mittels elektronisch signierter Dokumente zu leisten.

3.3 Ablauf der vorliegenden Arbeit

Die vorliegende Arbeit gliedert sich in drei Teile. Der erste Teil entspricht dieser Einführung. Im zweiten Teil werden das deutsche und das brasilianische Signaturrecht dargestellt und anschließend verglichen. Schwerpunkt dieser Darstellungen sind die technisch-organisatorischen Vorschriften beider Rechtsordnungen. Die Darstellungen dienen – wie bereits ausgeführt – dem Verständnis des Themas als Voraussetzung des späteren Vergleichs. Die wichtigsten Unterschiede in beiden Modellen werden ermittelt und bewertet und es wird der Frage nachgegangen, ob eine Rezeption vorteilhafter Elemente in die jeweils andere Rechtsordnung in Betracht zuziehen ist.

im schweizerischen Recht und dem Erbrecht des unehelichen Kindes im holländischen Recht. Die Vergleichbarkeit sei nicht gegeben, weil es sich bei dem ersten zu vergleichenden Element um das Erbrecht des überlebenden Ehegatten handele, welches sich von dem zweiten Element, dem Erbrecht des unehelichen Kindes wesentlich unterscheide.

17 *Zweigert*/*Kötz* 1996, 46.

18 Kritisch zu der Bewertung der Lösung als “besser” oder “schlechter”, *Zweigert*/*Kötz* 1996, 46. Die Autoren stimmen jedoch zu, dass oft die Überlegenheit einer Lösung evident sei.

Im dritten Teil werden das deutsche und das brasilianische Beweisrecht dargestellt, mit dem Schwerpunkt der Beweisbarkeit mittels elektronischer Dokumente. Daran anschließend folgt erneut ein vergleichender Teil. Dieser ist etwas kürzer und hat zum Ziel, eine beweisrechtliche Vorschrift für die brasilianische Rechtsordnung vorzuschlagen. Die Arbeit schließt mit der Zusammenfassung der wichtigsten Ergebnisse.

4. Grundlagen und Voraussetzungen der elektronischen Signatur

Ist die Rede von elektronischen Signaturen, sind zwei wissenschaftliche Grundkomponenten zu betrachten, welche in einer Symbiose notwendige Vorraussetzungen für ihre Nutzbarkeit schaffen. Gemeint sind die Bereiche der Rechtswissenschaft und der Informationstechnik, welche sich wechselseitig Forderungen abbedingen. Diese zu vereinbaren ist nicht immer leicht.[19] Vor dem Hintergrund der wachsenden Bedeutung elektronischer Signaturen für den elektronischen Geschäftsverkehr werden die Wechselbeziehungen von Recht und Technik zunehmend in einer breiten Öffentlichkeit diskutiert. Aus diesem Grund ist ein technisches Verständnis eine wichtige Ausgangsbasis, um elektronische Signaturen und deren Systematik besser verstehen zu können. Im Folgenden soll deshalb zunächst auf die technische Seite der elektronischen Signatur eingegangen werden.

4.1 Symmetrische Verschlüsselung

Die Kryptographie ist so alt, wie eines der ältesten Gewerbe der Welt, die Spionage. Bereits die Griechen und Römer sollen kryptographische Verschlüsselungen für die sichere Übermittlung von Botschaften genutzt haben. Ihre Anwendung ist heute einer der bedeutendsten Grundbausteine der elektronischen Signatur. Dabei waren die anfänglich genutzten symmetrischen Verschlüsselungen, welche zum Beispiel auf dem einfachen Verschieben von Buchstaben basierten, relativ leicht zu entschlüsseln. Berühmtheit, was kryptographisches Know-how betrifft, im Zusammenhang mit ihrer „Unknackbarkeit“ erlangte die im zweiten Weltkrieg eingesetzte Enigma, eine Verschlüsselungsmaschine welche mit Hilfe von Walzen eine polyalphabetische Substitution nutzte, um militärische Nachrichten zu verschlüsseln. Bei den einfachen Verfahren reichte es häufig schon aus, verschiedene Möglichkeiten auszuprobieren, um auf des Rätsels Lösung zu kommen. Ein hoher Aufwand an Material und Personal war hingegen notwendig, um spätere Codierungen zu entschlüsseln. Seit 1940 war es den alliierten Streitkräften schließlich gelungen die Verschlüsselung der Enigma zu decodieren.[20]

19 *Bösing* 2005,19.

20 S. z.B. *Bauer* 2000, 3 ff.

Symmetrische Signaturen sind jedoch selbst mit einem komplizierterem Schlüssel unsicher, sogar wenn diese auch mit den leistungsfähigsten Rechnern nicht mehr zu entschlüsseln wären. Grundlegend verlangen symmetrische Verschlüsselungsverfahren nämlich, dass beide Seiten den Schlüssel kennen, was eine Geheimhaltung von vornherein schwieriger gestaltet und deren Einhaltung für den jeweils anderen nicht kontrollierbar ist. Gemeinhin könnte man postulieren, wenn zwei es wissen, weiß es einer zuviel, und damit gelte die Verschlüsselung als unsicher. Des Weiteren als nachteilig stellt sich die Notwendigkeit des sicheren Schlüsselaustausches dar sowie die Verwendung unterschiedlicher Schlüssel für verschiedene Geschäftsbeziehungen. Schlussendlich liegt ein hier letztgenannter bedeutender Nachteil darin, dass die gegenüber dem Partner gemachten Erklärungen nicht nachweisbar sind. Eine praktikable Lösung bietet die asymmetrische Verschlüsselung.

4.2 Asymmetrische Verschlüsselung

Diffie zusammen mit *Hellman* gebührt die Annerkennung für die Erkenntnis, zu welcher diese bereits 1976 gelangten, dass nicht beide Parteien der verschlüsselten Kommunikation über einen gleichen Schlüssel verfügen müssen.[21] Dabei liegen die Vorteile gegenüber der symmetrischen Verschlüsselung klar auf der Hand. Zum ersten ist kein Schlüsselaustausch mehr notwendig, zum zweiten kann ein Schlüssel für mehrere Geschäftsbeziehungen genutzt werden, dessen Vertraulichkeit kontrollierbar bleibt. Dies macht auch Erklärungen gegenüber dem Partner nachweisbar. Die Idee basiert auf die Verwendung von zwei verschiedenen Schlüsseln, die zusammen gehören: Einem privaten sowie einem öffentlichen Schlüssel, dem das Verfahren auch seinen Namen (Public-Key-Kryptographie) verdankt.[22] Dabei ist der private Schlüssel nur dem Signierer bekannt und nutzbar, um elektronische Signaturen zu erstellen. Im Gegensatz zu ihm, dient der allgemein beispielsweise im Bundesanzeiger bekannt, gemachte, öffentliche Schlüssel, welcher von jedem Empfänger signierter elektronischer Dokumente genutzt werden kann, der Prüfung der Echtheit einer Signatur. Das am weitesten verbreitete Verfahren ist das RSA, welches nach seinen Entwicklern Rivest, Shamir und Adleman benannt wurde und sich auf Faktorisierungsalgorithmen stützt.[23]

Asymmetrische Verfahren nutzen mathematische Schlüsselcodierungen, welche durch ihre Komplexität und Länge zwar eine höhere Sicherheit bieten, dafür jedoch in gleichem Maße mehr Zeit zum Ver- und Entschlüsseln benötigen. Dies ist eine relative Sicherheit, die darauf beruht, dass ein mathematisches Problem Angriffen durch das Erproben möglicher Schlüssel standhält. Die Sicherheit basiert auf dem Abstand zwischen den Möglichkeiten des Erprobens und der Größe des zu erpro-

21 *Singh* 2002, 305.

22 *Diffie*/*Hellmann* 1976, 644 ff.

23 *Fox*, DuD 1997, 69.

benden Zahlenraumes. Je größer die Rechenleistung eines Computers ist, desto eher bestünde die Möglichkeit einer Entschlüsselung, wobei heutige Schlüssel mit den derzeitig vorhandenen Rechnerkapazitäten nicht in praktisch relevanter Zeit decodiert werden können. Da sich die Rechnerleistung auf Grund des Fortschritts jedoch stetig verbessert, ist es eine Zeitfrage, bis der angewandte Schlüssel decodiert werden kann. Aus diesem Grunde sind Schlüssel vom Umfang her so gestaltet, dass sich der Versuch einer Entschlüsselung aus Zeitgründen für einen möglichen Angreifer nicht lohnt. Des Weiteren impliziert jedoch der Mehraufwand an Zeit, die Verwendung von Signaturen in mehreren Schritten zu vollziehen. Als erster Schritt werden Hashverfahren angewandt, wie im Folgenden erläutert wird.

4.3 Hashverfahren

Aufgrund des höheren Zeitbedarfes für den gesamten Prozess stellen Hashverfahren eine technische Abkürzung dar. Sie dienen dazu, Daten von beliebiger Länge auf Daten mit festem Umfang zu reduzieren (aus langen Texten werden kurze Texte). Im Anschluss werden diese gebildeten Hashwerte unter den Anforderungen erstens der Eindeutigkeit (eine bestimmte Datei hat immer den gleichen Hashwert), zweitens der Unumkehrbarkeit (ein Hashwert gibt keinen Aufschluss über die bestimmte Datei) und drittens der Kollisionsresistenz (jeder Hashwert ist nur einer bestimmten Datei zugeordnet) verschlüsselt. Im nächsten Schritt wird nun dieser Hashwert mit dem Signaturschlüssel signiert und danach die Daten zum Beispiel an einen Geschäftspartner versand. Dieser wird nun die empfangene elektronische Datei mittels des Hashverfahrens erneut hashen und den Signaturprüfschlüssel auf die Signatur anzuwenden. Wenn als Resultat der entschlüsselte Hashwert mit dem zum Überprüfungszweck selbst geschaffenen Hashwert übereinstimmt, kann der Empfänger von der Unversehrtheit (Integrität) des zugesandten elektronischen Dokuments ausgehen. Der oben angesprochene private Schlüssel dient dabei der Verschlüsselung des Hashwerts des elektronischen Dokuments des Senders und der öffentliche Schlüssel dem Empfänger zur Überprüfung der Signatur dieses Dokuments. Heutzutage wird das Prüfergebnis in den zwei Zuständen grün für „good“ oder rot für „not good“ dargestellt.

4.4 Chipkarten

Bei der herkömmlichen Unterschrift werden außer einem Schreibgerät keine Hilfsmittel verwendet. Wenn das Schreibgerät verloren gehen sollte, kann es durch ein beliebiges anderes substituiert werden. Die Unterschrift kann nach ihrer Natur nur persönlich verwendet werden, was sie einzigartig macht. Eine Manipulation ist an dieser Stelle nicht möglich. Die Fähigkeit, eine Unterschrift zu leisten, ist gemeinhin immer gegeben – im Gegensatz zur Verwendung elektronischer Signaturen, welche auf zahlreiche technische Komponenten (Hardware) und ihrem Zusammenspiel mit

ihrer Umgebung gestützt sind und damit eine größere Angriffsfläche bietet.[24] Umso strikter sind die Anforderungen an die verwendete Hardware, Software sowie ihre Nutzer zu formulieren. Als Träger des geheimen Schlüssels und der Kryptofunktionen bieten sich Chipkarten ähnlich der bekannten Kreditkarten an, wobei auch andere Speichermedien denkbar wären. Die Anforderungen, welche die Chipkarte erfüllen muss, bestehen in der Einmaligkeit des geheimen Schlüssels, welcher weiterhin geheim gehalten werden soll. Er darf daher den geschützten Träger (Chipkarte) nie verlassen.

Hardware und Software müssen in der Form gestaltet sein, dass die eben genannten Anforderungen erfüllt sind. Das heißt, ein Kartenlesegerät muss geeignet sein, die korrekten Daten auslesen zu können, ohne sie zu kopieren oder zu manipulieren. Ansonsten könnten Nutzer die Authentizität ernsthaft anzweifeln. Des Weiteren sind bei der Übergabe der Hardware an seinen Nutzer hohe Anforderungen an die Identifizierung von Personen zu stellen, damit nicht Dritte in unredlicher Absicht die Nutzung der Komponenten ermöglicht wird. So ist es beispielsweise sinnvoll, wie von Banken praktiziert, die Karten-PIN und die Chipkarte dem rechtmäßigen Empfänger getrennt zuzusenden. Dies allein ist letztlich jedoch nicht der Garant, um die Authentizität der signierten elektronischen Dokumente zu gewährleisten oder zu prüfen. Dafür ist weiterhin ein „vertrauenswürdiger Dritter“ notwendig, welcher die geforderten Merkmale bestätigen kann.[25] Wird die elektronische Signatur richtig angewandt, beinhaltet sie einen hohen Nutzwert mit der gleichen Sicherheit und Unterschriftenfunktion wie herkömmliche Unterschriften.

4.5 Zertifikate und Zertifizierungsdienstanbieter

Um dem erwähnten Schlüsselpaar des asymmetrischen Verfahrens vertrauen zu können, muss eine sichere und zuverlässige Zuordnung beider Schlüssel zu einer bestimmten Person gewährleistet sein. Denn in der Regel kennt der Empfänger einer elektronisch signierten Erklärung den Signaturschlüssel-Inhaber nicht und hat keine weitere Möglichkeit, dessen Identität zu verifizieren.[26] Diese Zuordnung kann nur durch eine zuverlässige Instanz erfolgen, die so genannte „vertrauenswürdige Dritte“.[27] Diese bestätigt gegenüber dem Rechtsverkehr, dass ein öffentlicher Schlüssel zu einer bestimmten Person gehört. Diese Bestätigung erfolgt durch das Ausstellen eines elektronischen Dokuments namens Zertifikat, das von einem so genannten Zertifizierungsdienstanbieter elektronisch signiert wird. Das elektronische Zertifikat enthält u.a. zwei sehr wichtige Informationen: den jeweiligen öffentlichen Schlüssel

24 *Pordesch* 2002, 38.

25 *Roßnagel* 1995, 135.

26 *Baum* 1999, 6.

27 *Roßnagel*, RMD, SigG Einl., Rn. 19.

sowie den Namen[28] der Person, der er zugeordnet ist.[29] Entscheidend in diesem Zusammenhang ist, dass der Zertifizierungsdienstanbieter den Teilnehmer korrekt identifiziert, etwa durch einen persönlichen Kontakt bei Vorlage eines Personalausweises oder eines Reisepasses. Nur mit einer richtigen Identifizierung kann verhindert werden, dass jemand unter falschem Namen praktisch missbräuchlich im elektronischen Rechtsverkehr handelt.[30]Die bedeutenden Leistungen eines Zertifizierungsdienstanbieters erschöpfen sich aber nicht mit der Identifikation des Teilnehmers und mit der Ausstellung des Zertifikats. Zertifikate müssen von diesen gesperrt werden, wenn der Signaturschlüssel-Inhaber wegen eines bestimmten Grundes (z. B. Verlust der Chipkarte) danach verlangt. Darüber hinaus gehört zur alltäglichen Aufgaben eines Zertifizierungsdienstanbieters u. a. die Führung eines Sperr- und Verzeichnisdienstes, um Empfänger elektronisch signierter Dokumente die Überprüfung der Gültigkeit des Zertifikats zu ermöglichen.

28 Der Name muss unverwechselbar sein, das heißt es darf nicht passieren, dass eine elektronische Signatur auf mehrere Personen mit dem gleichen Namen zuordbar ist. Dann wäre eine eindeutige rechtliche Zuordnung problematisch. Die Aufgabe der Namensgebung gehört somit zum Leistungsspektrum eines Zertifizierungsdiensteanbieters. S. hierzu *Roßnagel*, RMD, SigG Einl., Rn. 24.

29 BR-Drs. 966/96, 27.

30 *Roßnagel*, RMD, SigG Einl., Rn. 24.

2. Teil: Vergleich der Signaturregelungen

1. Die elektronischen Signaturen in Deutschland: Entstehungsgeschichte und Rechtsrahmen

1.1 Das erste deutsche Signaturgesetz von 1997

In der Auseinandersetzung zur Förderung des elektronischen Rechtsverkehrs wurden in Deutschland drei verschiedene Ansätze vertreten.[31] Dem ersten Ansatz entsprechend – von manchen Ministerien vertreten – wäre die Festsetzung von besonderen Vorschriften für digitale Signaturen unnötig. Die schon existierende Rechtsordnung hindere kaum die Nutzung von digitalen Signaturen. Sie könne innerhalb des formfreien Rechtsverkehrs problemlos verwendet werden. Man solle zunächst Erfahrung mit der Nutzung von Signaturen sammeln und vielleicht später ihren Beweiswert regeln. Für den Aufbau von signaturgeeigneten Sicherungsinfrastrukturen[32], sollte vor allem überprüft werden, ob sie nicht dem Markt überlassen werden sollten.[33]

Nach dem zweiten Ansatz – von der Bundesnotarkammer vertreten – sollte eine Äquivalenz zwischen eigenhändiger Unterschrift und digitaler Signatur geschaffen werden. Vorschlag des Entwurfs der Bundesnotarkammer war es auch, die Beweiswirkungen des digital signierten Dokumentes dem unterschriebenen Dokument gleichzustellen.

Der dritte Ansatz ist vor allem von der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) vorgeschlagen worden.[34] Nach diesem sollte dringend zunächst eine Sicherungsinfrastruktur mit den Rahmenbedingungen für digitale Signaturen etabliert werden. Besonders mit dem Ziel, Fehlentwicklungen zu vermeiden und die Sicherheit im elektronischen Rechtsverkehr zu erhöhen. Erst danach sollten die Form- und Beweisvorschriften mit der Zeit angepasst werden. Besonders bemerkenswert im Gesetzesentwurf von provet war der Vorschlag, die verschiedenen Funktionen der Sicherungsinfrastruktur auf unterschiedliche Instanzen zu verteilen und nicht nur auf eine Zertifizierungsstelle zu konzentrieren. Im Gesetzentwurf waren folgende Funktionen als isoliertes Angebot vorgesehen: Registrierung (§ 9),

31 *Roßnagel*, RMD, SigG Einl., Rn. 48.

32 Für die Bezeichnung Sicherungsinfrastruktur siehe *Hammer*, DuD 1998, 91.

33 *Roßnagel*, RMD, SigG Einl., Rn. 49.

34 Bereits ein erster Entwurf eines Sicherungsinfrastruktur-Gesetzes im Rahmen der Simulationsstudie Rechtspflege im Jahr 1992. Im Jahr 1996 hat provet im Auftrag des Bundesministeriums für Bildung und Forschung einen eigenen Gesetzesentwurf erstellt; zum Gesetzesentwurf siehe http://www.provet.org/bib/mmge/er-g.htm.

Schlüsselerzeugung (§ 10), Zertifizierung (§ 11), Personalisierung und Ausgabe (§ 12), Verzeichnis (§13), Zeitbestätigung (§ 14).

Der Gesetzgeber hat sich für den dritten Ansatz entschieden. Die Verabschiedung des Signaturgesetzes stützte sich auf die Erkenntnis, dass am Anfang der Entwicklung lediglich das Handwerkszeug für die Verwendung von digitalen Signaturen geschaffen werden sollte, das heißt die Etablierung einer vertrauenswürdigen Sicherungsinfrastruktur, ohne im Vorfeld Beweisregelungen festzusetzen.[35] Die Beweisfunktion von digital signierten Daten sollte über die faktische Sicherheit der im Gesetz vorgesehenen Signaturverfahren erreicht werden. Es sollte dann davon ausgegangen werden, dass diese Sicherheit von den Gerichten im Rahmen der freien Beweiswürdigung honoriert würde.[36]

Das erste deutsche Signaturgesetz (SigG 1997) trat am 1.8.1997 in Kraft und wurde dadurch weltweit das erste Gesetz über Rahmenbedingungen für digitale Signaturen, welches von einem Bundesparlament verabschiedet worden ist. Das Signaturgesetz wurde als Teil (Artikel 3) des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG) beschlossen. Zweck dieses Gesetzes (§ 1 Abs. 1 SigG 1997) war es, Rahmenbedingungen für digitale Signaturen zu schaffen. Durch die Möglichkeit zur Feststellung von Fälschungen ihrer selbst oder Verfälschungen signierten Daten, sollten digitale Signaturen als sicher gelten können. Das Angebot und die Anwendung von anderen Signaturverfahren, außerhalb des Rahmens des Gesetzes waren nicht ausgeschlossen. Diese hatten aber nicht die Vermutung, sicher zu sein.

Auf den Sicherheitszweck des § 1 Abs. 1 SigG 1997 wurde in fünfzehn weiteren Vorschriften näher eingegangen. Ferner ist eine Rechtsverordnung (SigV 1997) mit anderen konkretisierenden Einzelheiten von der Bundesregierung erlassen worden. Darauf folgend werden die wichtigsten Merkmale dieses Gesetz dargestellt.

1.1.1 Begrifflichkeiten

Das SigG 1997 definierte in § 2 Abs. 1 die digitale Signatur als ein Siegel zu digitalen Daten, welches mit einem privaten Schlüssel erzeugt wird und „mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde (…) versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt“. Kritik bekommen hat diese Legaldefinition in Bezug auf die Verwendung des Ausdruckes „Siegel“ sowie für „Signaturschlüssel“, als Bezeichnung des öffentlichen Prüfschlüssels.[37] Das Wort Siegel wäre für den Gesetzestext ungeeignet, denn im alltäglichen Sprachgebrauch wird es als Abdruck eines Stempels in einem formbaren Stoff ver-

35 S. BR-Drs. 966/96, 28.

36 S. BR-Drs. 966/96, 26.

37 *Roßnagel*, DuD 1997, 77.

standen, was mit digitalen Signaturen nichts zu tun hätte.[38] Und den öffentlichen Schlüssel als „Signaturschlüssel" zu bezeichnen wäre technisch inkorrekt, weil dieser der Prüfung der Signatur diente und deswegen „Signaturprüfschlüssel" genannt werden solle.[39]

Darüber hinaus definierte § 2 Abs. 3 SiG 1997 ein Zertifikat als eine digitale Bescheinigung, versehen mit einer digitalen Signatur, die Angaben über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person (Signaturschlüssel-Zertifikat) oder einer gesonderten digitalen Bescheinigung, die unter eindeutiger Bezugnahme auf ein Signaturschlüssel-Zertifikat weitere Angaben (Attributszertifikat) enthält. Der Zeitstempel verdiente auch eine gesetzliche Anerkennung und wurde in § 2 Abs. 4 als eine „mit einer digitalen Signatur versehene digitale Bescheinigung einer Zertifizierungsstelle, dass bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben", definiert.

1.1.2 Zertifizierungsstellen

Im Rahmen des SigG 1997 konnten den Betrieb einer Zertifizierungsstelle natürliche oder juristische Personen übernehmen. Ihre Hauptaufgabe laut § 2 Abs. 2 SigG 1997 bestand in der Zuordnung von öffentlichen Signaturschlüsseln zu natürlichen Personen. Der Betrieb einer Zertifizierungsstelle gemäß § 4 Abs. 1 bedurfte einer Genehmigung, erteilt von der Regulierungsbehörde für Telekommunikation und Post (RegTP).[40] Zur Erteilung dieser Lizenz waren grundsätzlich drei Voraussetzungen vorgesehen (§ 4 Abs. 3). Der Kandidat sollte zunächst Zuverlässigkeit besitzen, welche vorlag, wenn die für den Betrieb maßgeblichen Rechtsvorschriften eingehalten würden. Zudem sollten die Mitarbeiter der Zertifizierungsstelle über die dafür erforderlichen Kenntnisse, Erfahrungen und Fertigkeiten verfügen, was im Sinne des Gesetzes den Begriff von Fachkunde erfüllte. Ferner sollte der Antragsteller alle Maßnahmen zur Erfüllung der gesetzlichen und in der Signaturverordnung vorgesehenen Bestimmungen in einem Sicherheitskonzept darstellen sowie dieses von einer anerkannten Stelle prüfen lassen.

Die Zertifizierungsstelle hatte im Rahmen des SigG 1997 eine Reihe von Pflichtdienstleistungen zu erbringen. Nach § 5 Abs. 1 SigG 1997 hatte sie Personen, die ein Zertifikat beantragten, zuverlässig zu identifizieren und diese einem öffentlichen Signaturschlüssel zuzuordnen sowie das durch ein Signaturschlüssel-Zertifikat zu bestätigen. Die von ihr erzeugten Schlüssel und Identifikationsdaten waren nach § 6 SigV 1997 dem Teilnehmer persönlich zu übergeben. Auf Verlangen sollte die Zertifizierungsstelle Angaben über die Vertretungsmacht für eine dritte Person in das

38 *Roßnagel*, DuD 1997, 78.

39 *Roßnagel*, DuD 1997, 78.

40 Im Juli 2005 wurde die RegTP in Bundesnetzagentur umbenannt. Siehe hierzu nachfolgende in diesem Teil Gliederungspunkt 1.3.4.

Signatur-Schlüsselzertifikat oder in ein Attributszertifikat eintragen unter der Voraussetzung, dass die Einwilligung des Dritten zur Aufnahme dieser Angaben nachgewiesen wurde (§ 5 Abs 2. SigG 1997). Signaturschlüssel- sowie Attributszertifikate sollten gemäß § 5 Abs. 1 SigG 1997 und § 8 Abs. 1 SigV 1997 über öffentlich erreichbare Telekommunikationsverbindungen für die Dauer von mindestens 10 Jahren nachprüfbar zu halten sein. Eine weitere Pflichtdienstleistung der Zertifizierungsstellen (§ 6 SigG 1997) war die Unterrichtung des Antragstellers. Diese musste die erforderlichen Sicherungsmaßnahmen, die von ihm vorzunehmen waren, enthalten. Dazu gehörten beispielsweise neben dem persönlichen Gewahrsam des privaten Schlüssels, die Geheimhaltung der PIN zur Identifikation gegenüber dem Schlüsseldatenträger. Des Weiteren war über die Einsetzung von geeigneten technischen Komponenten zu unterrichten, welche für die Erzeugung sowie Prüfung von digitalen Signaturen als auch für die Darstellung von zu signierenden Daten notwendig waren.[41] Ferner war die Zertifizierungsstelle verpflichtet, laut §§ 8 SigG 1997 und 9 SigV 1997 einen jederzeit von Teilnehmer erreichbaren Sperrdienst bereitzustellen, um Zertifikatssperrungen im Zertifikat-Verzeichnis kenntlich zu machen. Auf Verlangen des Teilnehmers waren digitale Daten mit einem Zeitstempel zu versehen (§ 9 SigG 1997).

1.1.3 Regulierungsbehörde: Wurzelinstanz und Kontrolle

Gemäß § 4 Abs. 1 SigG 1997 war die Regulierungsbehörde für Telekommunikation und Post (RegTP) für die Lizenzierung von Zertifizierungsstellen zuständig. Außerdem stand die RegTP als Wurzelinstanz an höchster Position der Zertifizierungsstruktur. Diese Zertifizierungsstruktur war mit der RegTP als Wurzelinstanz bundeseinheitlich und zweistufig. Ihr oblag die Ausstellung von Zertifikaten, die wiederum von den Zertifizierungsstellen zum Signieren von Endnutzerzertifikaten eingesetzt wurden (§ 3 SigG 1997). Für die Vergabe von Zertifikaten sollte die RegTP nach § 4 Abs. 5 Satz 2 SigG 1997 alle Vorschriften erfüllen, die für die Zertifizierungsstellen galten. Insbesondere sollte die RegTP gemäß § 14 Abs. 4 SigG 1997 geeignete und bestätigte Komponente verwenden, Dokumentationspflichten gemäß § 10 SigG 1997 beachten und gemäß § 5 Abs. 5 SigG 1997 und §§ 5, 10, 11 und 12 SigV 1997 organisatorischen sowie technische Sicherungsmaßnahmen vornehmen. Ferner sollte sie gemäß § 4 Abs. 5 Satz 3 SigG 1997 die von ihr ausgestellten Zertifikate in einem Verzeichnis abrufbar und nachprüfbar halten.

Der Regulierungsbehörde oblag zudem nach § 3 SigG 1997 die Überwachung der Einhaltung der Anforderungen aus dem SigG 1997 sowie aus der SigV 1997. Zu diesem Zweck konnte die RegTP laut § 13 Abs. 1 Satz 2 SigG 1997 die Benutzung ungeeigneter technischer Komponenten sowie eventuell den Betrieb einer Zertifizie-

41 Die Konkretisierung der Unterrichtungspflicht ist im § 4 Abs. 1 der SigV 1997 festgelegt worden.

rungsstelle vorübergehend ganz oder teilweise untersagen. Vorgesehen war auch das Betreten der Geschäftsräume der Zertifizierungsstelle während der üblichen Betriebszeiten, um Einsicht in Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstigen Unterlagen zu nehmen (§ 13 Abs. 2 SigG 1997). Überdies konnte die Regulierungsbehörde, gemäß § 15 Abs. 3 SigV 1997 in angemessenen Zeitabständen sowie bei Anhaltspunkten für eine Verletzung von Vorschriften des Gesetzes oder der Verordnung, Kontrollen durchführen. In § 13 Abs. 5 SigG 1997 war eine weitere Aufgabe der RegTP im Rahmen der Kontrolle festgelegt, wonach die Behörde den elektronischen Rechtsverkehr zu beobachteten hatte, in der Absicht dessen Sicherheit zu gewährleisten. Hierzu war ihr die Möglichkeit gegeben, eine Sperrung von Zertifikaten anzuordnen, immer wenn Tatsachen rechtfertigten, dass Zertifikate gefälscht oder nicht hinreichend fälschungssicher waren.

Eine bedeutende Pflicht der Regulierungsbehörde, besonders im Bezug auf die notwendige Kontinuität der Überprüfbarkeit digitaler Signaturen, war sicherzustellen, dass wenn eine Zertifizierungsstelle ihre Tätigkeiten einstellte, eine andere sie übernahm oder dass die Verträge mit den Signaturschlüssel-Inhaber abgewickelt würden (§ 13 Abs. 4 Satz 1 SigG 1997). Dies galt auch wenn die Zertifizierungsstelle einen Antrag auf Eröffnung eines Konkurs- oder Vergleichsverfahrens stellte und die Tätigkeiten nicht fortgesetzt wurden (§ 13 Abs. 2 SigG 1997).

1.1.4 Sicherheitsvermutung

Obgleich im Rahmen des SigG 1997 keine Beweisregel zugunsten digitaler Signaturen festgesetzt wurde, ist die Existenz einer Sicherheitsvermutung mit Beweiswirkungen vertreten worden.[42] Diese Vermutung war aus dem § 1 Abs. 1 SigG 1997 hergeleitet, in dem es heißt: „Zweck des Gesetzes ist es, Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten … können". Mit dieser Formulierung wollte der Gesetzgeber nicht nur einen Programmsatz etablieren, sondern auch „eine neue Vermutungsregel, die am ehesten als vorgezogener Anscheinsbeweis bezeichnet werden kann"[43]. Diese Sicherheitsvermutung bezog sich auf die Technik der digitalen Signatur und auf ihr Prüfverfahren. Als sicher konnte die digitale Signatur gelten, denn zu erwarten war, dass sie nur vom Signaturschlüssel-Inhaber erzeugt worden sein konnte und dass die signierten Daten nicht unbemerkbar verändert werden konnten. Das Prüfverfahren seinerseits konnte Fälschungen digitaler Signaturen oder Verfälschungen signierter Daten feststellen.[44] Die Sicherheitsvermutung erfasste nicht die Tatsache, dass der Signaturschlüssel-

42 *Roßnagel*, NJW 1998, 3312. Die Begründung zum deutschen Signaturgesetz aus dem Jahr 2001 anerkennt, dass im Rahmen des SigG 1997 eine Sicherheitsvermutung galt. Hierzu, BT-Drs. 14/4662, 28.

43 *Roßnagel*, NJW 1998, 3316.

44 *Roßnagel*, NJW 1998, 3316.

Inhaber die elektronischen Daten signieren wollte (Autorisierung).[45] Was die Rechtswirkungen der Sicherheitsvermutung betrifft, sollte sie eine Beweiserleichterung begründen.[46] Diese führte nicht zu einer Umkehrung der Beweislast, sondern zu einem vorläufigen Beweis der Sicherheit des Signaturverfahrens und der Unverfälschtheit der Signatur, bis die Vermutungsbasis vom Gegenbeweis erschüttert wurde.[47] Für die Erschütterung der Vermutungsbasis lag die Beweislast bei demjenigen, der sie angriff. Hierzu war der Beweis des Gegenteils nicht erforderlich, es reichte nur der Gegenbeweis in die Richtung, dass ein wichtiger Bestandteil der Vermutungsbasis nicht vorlag.[48]

1.1.5 Datenschutz

Angesichts des großen Wertes, der auf den Datenschutz im deutschen Recht gelegt wird, ließ das SigG 1997 diese Materie nicht außer Acht. § 12 Abs. 1 bestimmte, dass die Zertifizierungsstelle personenbezogene Daten nur beim Betroffenen selbst und nur insoweit erheben durfte, als dies für Zwecke eines Zertifikates erforderlich war. Somit unterlagen sie einer strengen Zweckbindung.[49] Nach § 12 Abs. 2 SiG 1997 waren die Zertifizierungsstellen verpflichtet, Pseudonymendaten an die Sicherheits- und Geheimdienstbehörden zu übermitteln, soweit dies für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich war.

1.2 Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (RLeS)

1.2.1 Die Signaturrichtlinie

Die Verabschiedung des SigG 1997 trug dazu bei, die Beschleunigung des Prozesses zur Schaffung eines normativen Rechtsrahmens für den elektronischen Rechtsverkehr innerhalb des europäischen Raums voranzutreiben. Die Europäische Kommission schlug zunächst am 13.5.1998 ein Regelungsmodell vor, das weitgehend im Gegensatz zu dem Ansatz des SigG 1997 stand.[50] Zulassungsverfahren für Zertifizierungsstellen und technische Komponenten waren nicht vorgesehen. Ob die Sicherheitsanforderungen eingehalten wurden, war Sache der Zertifizierungsstellen, denn der Markt sollte die erforderliche Sicherheit spontan hervorbringen. Zwei An-

45 *Roßnagel*, NJW 1998, 3316.
46 *Rapp* 2002, 34.
47 *Roßnagel*, NJW 1998, 3316 ff.
48 *Roßnagel*, NJW 1998, 3317.
49 *Roßnagel*, DuD 1997,77.
50 *Roßnagel*, MMR 1999, 261.

hänge sahen Anforderungen an den Inhalt von Zertifikaten und an Zertifizierungsstellen vor. Würden die Anforderungen an die Zertifizierungsstellen erfüllt, dann sollten den daraus resultierenden Signaturen der gleiche Beweiswert wie handschriftlichen Unterschriften zuerkannt werden. Nach dem Entwurf waren die Zertifizierungsstellen lediglich mit einer vom Verschulden unabhängigen Haftung bedroht.

Der ursprüngliche Entwurf wurde vom Europäischen Rat am 27.11.1998 zunächst abgelehnt, dann aber nach einigen Ergänzungen am 22.4.1999 als Entwurf einer Richtlinie für gemeinsame Rahmenbedingungen für elektronische Signaturen (RLeS) in den Gesetzgebungsprozess eingebracht und am 02.12.1999 verabschiedet. Sie trat am 19.1.2000 in Kraft. Die Ergänzungen haben die Richtlinie dem Konzept des SigG 1997 angenähert.[51] Auf der einen Seite sind zwei weitere Anhänge aufgenommen worden: Anhang III mit Anforderungen an sichere Signaturerstellungseinheiten und Anhang IV mit Empfehlungen zu einer sicheren Überprüfung der Signatur. Auf der anderen Seite sind Kontrollverfahren vorgesehen worden. Zum einen zur Kontrolle der Konformität von sicheren Signaturerstellungseinheiten, die von geeigneten privaten oder öffentlichen Stellen durchgeführt werden sollten. Zum anderen sollten die Mitgliedsstaaten ein Aufsichtssystem zur Überwachung der Zertifizierungsdiensteanbieter einrichten, die qualifizierte Zertifikate ausstellen (Art. 3 Abs. 3 RLeS).

1.2.2 Die wichtigsten Grundsätze und Bestimmungen der Signaturrichtlinie

Durch die Richtlinie wurde anerkannt (Erwägungsgrund 4), „dass die elektronische Kommunikation und der elektronische Geschäftsverkehr ‚elektronische Signaturen' und entsprechende Authentifizierungsdienste für Daten erfordern". Ziel war es, divergierende Regeln, die „ein ernsthaftes Hindernis für die elektronische Kommunikation und den elektronischen Geschäftsverkehr darstellen", zu vermeiden. Zu diesem Zweck sind einige Grundsätze und Bestimmungen formuliert, welche im Folgenden dargestellt werden.

1.2.2.1 Marktfreiheit

Die Richtlinie legt an mehreren Stellen klar fest, dass die Anbieter von Zertifizierungsdiensten, „diese ungehindert ohne vorherige Genehmigung bereitstellen können" (Erwägungsgrund 10). Art. 3 der Richtlinie wird mit der Überschrift „Marktzugang" benannt und verbietet gleich im ersten Absatz, dass die Mitgliedsstaaten eine Bereitstellung von Zertifizierungsdiensten von einer vorherigen Genehmigung abhängig machen. Dennoch wird der allgemeine Grundsatz der Marktfreiheit von mehreren Vorschriften relativiert, wenn nicht eingeschränkt. Zum einen sieht Art. 3

51 *Roßnagel*, MMR 1999, 261.

Abs. 2 RLeS die Möglichkeit vor, dass die Mitgliedsstaaten freiwillige Akkreditierungssysteme für Zertifizierungsdiensteanbieter einführen, um das Niveau ihrer Dienste zu erhöhen. Voraussetzung dafür ist die Festlegung von objektiven, transparenten, verhältnismäßigen und nicht diskriminierenden Anforderungen. Zum anderen fordert die Richtlinie von den Mitgliedsstaaten, ein System zur Überwachung der in ihrem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter zu etablieren, welche öffentlich qualifizierte Zertifikate ausstellen (Art. 3 Abs. 3). Ferner wird der Marktzugang eingeschränkt, indem geeignete öffentliche oder private Stellen die Übereinstimmung sicherer Signaturerstellungseinheiten mit den Anforderungen des Anhangs III feststellen müssen (Art. 3 Abs. 4).

Obwohl im Rahmen der Richtlinie der Marktzugang für Anbieter von qualifizierten Zertifikaten und für Anbieter, die sich einem Akkreditierungsverfahren unterwerfen, teilweise eingeschränkt wird, gilt somit der allgemeine Grundsatz der Marktfreiheit: Prinzipiell bedarf der Betrieb eines Zertifizierungsdienstes keiner Genehmigung.

1.2.2.2 Technologieoffenheit

Die Signaturrichtlinie erkennt den so genannten Grundsatz der Technik- oder Technologieoffenheit an. Nach Erwägungsgrund 8 erfordert die rasche technologische Entwicklung und der globale Charakter des Internets ein Konzept, das verschiedene Technologien und Dienstleistungen für die elektronische Authentifizierung ermöglicht. Konkretisiert wird diese Leitlinie durch die Anwendung von Begriffsbildungen, welche „elektronische Signatur“ statt „digitale Signatur“ oder „Signaturerstellungs- und -prüfdaten“ statt direkt „private-„ oder „öffentliche Schlüssel“ zu erwähnen.[52] Diese sollen abstrakt und an keine spezifische Technik angeknüpft sein, wie beispielsweise bei der Definition der elektronischen Signatur des Art. 2 Nr. 1[53], welche prinzipiell durch eine eingescannte Unterschrift erfüllt werden kann.[54] Darauf aufbauend wird aber eine Technologieoffenheit von der Richtlinie nicht verfolgt, denn die Anforderungen an „fortgeschrittene“ und „qualifizierte elektronische Signaturen“ beziehen sich faktisch auf die bekannte Technik asymmetrischer Kryptographie.[55] Das Gleiche gilt für die in der Richtlinie enthaltene Formulierung „Zertifikat“, die bei anderen Authentifizierungsverfahren wie beispielsweise der Biometrie keine Rolle spielen, da diese die Ausstellung von Zertifikaten nicht voraussetzt.[56] In

52 *Roßnagel* 2002, 137.

53 Nach Art. 2 Nr. 1 „elektronische Signatur“ sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.

54 *Rapp* 2002, 39.

55 *Roßnagel* 2002, 137.

56 *Gravesen*/*Dumortier*/*Van Eecke*, MMR 1999, 578.

der Tat ist der Ansatz der Technologieoffenheit nicht ganz zutreffend in seiner Beziehung zu den möglichen einsetzbaren Verfahren zur virtuellen Unterzeichnung und Authentifizierung. Rasche Entwicklungen in diesem Bereich, die den Unterschriftsersatzstatus verdienen, sind in absehbarer Zeit nicht zu erwarten, wie die Richtlinie davon ausgegangen ist. Die Kryptographie hat eine lange und komplexe Geschichte, schon ab ihrer frühesten Einsätze in Ägypten um 1900 v.Chr.[57] Die asymmetrischen Verfahren wurden schon in den 1970-er entwickelt. Seitdem wurde viel unternommen, um die akademische Gemeinschaft mit ihren verschieden interdisziplinären Gebieten und die Entscheidungsträger davon zu überzeugen, dass diese Technologie eine bedeutende Rolle spielen kann.

1.2.2.3 Unterteilung der Signaturverfahren in Klassen und ihre Rechtswirkung

Ein Merkmal der Signaturrichtlinie ist die Unterteilung der Signaturverfahren in verschiedenen Klassen. Zunächst sind alle elektronischen Signaturen als „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen", definiert. Zur Erfüllung des formalen Kriteriums der elektronischen Signatur können grundsätzlich alle Arten von Signaturen zwischen einer eingescannten Unterschrift und einer digitalen Signatur im Rahmen einer PKI-Sicherheitsinfrastruktur ausreichen.[58] Der Begriff ist somit sehr weit und ohne zusätzliche Anforderungen festgelegt.

Die zweite Stufe der elektronischen Signaturen, die „fortgeschrittene elektronische Signatur"[59], umfasst die erste Klasse und verlangt dazu noch vier weitere Anforderungen. Sie muss ausschließlich dem Unterzeichner zugeordnet sein, die Identifizierung des Unterzeichners ermöglichen, die alleinige Kontrolle der Erstellungsmitteln durch den Unterzeichner gestatten und die Feststellung einer nachträglichen Veränderung der Daten ermöglichen. Hierzu sind die Voraussetzungen zwar an die digitale Signatur angenähert, aber die im Internet frei verfügbaren Implementierungen von Pretty Good Privacy (PGP) wären schon ausreichend, um die Voraussetzungen zu erfüllen.[60]

57 *Singh* 2002, 14 ff.

58 *Tettenborn* 2000, 238.

59 Nach *Gravesen*/*Dumortier*/*Van Eecke*, MMR 1999, 585, sei die Legaldefinition der fortgeschrittenen Signatur des Art. 2 Nr. 2 RLeS der Literatur zur asymmetrischen Kryptographie und der darauf aufbauenden Vorarbeit der UNCITRAL-Arbeitsgruppen entnommen.

60 Das Modell „Pretty Good Privacy" (PGP) ist ein Verschlüsselungs- und Signierprogramm, das auf einem „Web of Trust" basiert. Es wird auf die Identität eines Teilnehmers dadurch vertraut, dass andere Teilnehmer seine Identität bestätigen. Das Modell ist grundsätzlich für geschlossene Netze geeignet, und nicht für offene, über die beweisrelevante Geschäfte abgewickelt werden, *Roßnagel*, RMD, SigG § 14, Rn. 79.

Dazu könnte man auch von einer dritten Klasse sprechen, die alle Anforderungen der „elektronischen" sowohl der „fortgeschrittenen" Signatur enthält und noch zwei weitere: Sie muss auf einem qualifizierten Zertifikat[61] beruhen und von einer sicheren Signaturerstellungseinheit[62] erstellt werden. Obwohl die Richtlinie eine qualifizierte elektronische Signatur nicht definiert, setzt sie diese dritte Klasse im Art. 5 Abs. 1 Nr. 1 voraus, weil diese Klasse die Rechtsfolge bewirken kann, die eigenhändige Unterschrift zu ersetzen. Die Existenz einer dritten Klasse von Signaturen wird auch in der Literatur anerkannt[63] und aus dem Art. 5 Abs. 1 hergeleitet. Nach dieser Vorschrift sollen die Mitgliedsstaaten Sorge dafür tragen, dass die fortgeschrittene Signatur, die auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erstellt wird, die rechtlichen Anforderungen an eine handschriftliche Unterschrift erfüllt. Im Endeffekt, wird eine Äquivalenz zwischen der fortgeschrittenen elektronischen Signatur mit diesen zwei weiteren Anforderungen und einer handschriftlichen Unterschrift etabliert.

Es ist aber zu erwähnen, dass die Richtlinie eventuelle Diskriminierungen gegen die rechtliche Wirksamkeit einfacher oder fortgeschrittener Signaturen verhindern will.[64] Hierbei sollen nach Erwägungsgrund 16 die freiwilligen privatrechtlichen Vereinbarungen zwischen den Parteien und ihrer Geschäftsfreiheit respektiert werden (beispielsweise geschlossene Nutzernetze), soweit dies im Rahmen des innerstaatlichen Rechts möglich ist.[65] Des Weiteren sollen die Mitgliedsstaaten Sorge tragen, dass der einfachen elektronischen Signatur ihre Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen wird, weil sie in elektronischer Form vorliegt oder die Voraussetzungen einer fortgeschrittenen Signatur „mit besonderer Qualität" nicht erfüllt werden (Art. 6 Abs. 2 RLeS).[66]

61 Die Anforderungen des qualifizierten Zertifikats sind in Anhang I der Richtlinie geregelt. Nach Art. 2 Nr. 10 RLeS werden qualifizierte Zertifikate von Zertifizierungsdiensteanbieter ausgestellt, die die Anforderungen des Anhangs II der Richtlinie erfüllen.

62 Die Anforderungen an die Signaturerstellungseinheit sind in Anhang III der Richtlinie.

63 *Geis* spricht von der fortgeschrittenen elektronischen Signatur mit besonderer Qualität, MMR 2000, 669. *Gravesen*/*Dumortier*/*Van Eecke*, MMR 1999, 579, verwenden die Bezeichnung „qualifizierte Signatur" zur sprachlichen Vereinfachung.

64 *Gravesen*/*Dumortier*/*Van Eecke*, MMR 1999, 581, halten es für überflüssig, eine generelle Vorschrift hinsichtlich der Zulässigkeit als Beweismittel von elektronischen Daten vorzusehen, da in keinem der Mitgliedsstaaten ein spezifisches Verbot dagegen existiert. Die beweisrechtliche Zielsetzung der Vorschrift bleibe deswegen faktisch davon abhängig, ob die freie Beweiswürdigung in der fraglichen Jurisdiktion gewährleistet ist.

65 Kritisch zu der in der Richtlinie enthaltenen Abgrenzung im Anwendungsbereich geschlossener und offener Nutzernetze, weil geschlossene Systeme so eine Größe erreichen können, dass sie einer breiten Öffentlichkeit zugänglich sind und eine Aufnahme nicht von besonderen persönlichen oder wirtschaftlichen Voraussetzungen abhängig ist, *Gassen* 2003, 184.

66 Art. 9 der E-Commerce Richtlinie (2000/31/EG) versteift das Nichtdiskriminierungsprinzip, indem er anordnet, dass die Mitgliedsstaaten sicherzustellen haben, dass ihre für den Ver-

1.2.2.4 Haftung

Angesichts der Tatsache, dass im Rahmen der Richtlinie die Zertifizierungsdienste prinzipiell ohne Vorabprüfung angeboten werden können und einem anlassbezogenen Überwachungssystem unterworfen sind, steigt die Bedeutung einer Haftungsregelung erheblich.[67] Dabei soll diese die Rolle einer „Drohung" spielen und den Zertifizierungsdiensteanbieter zur Einhaltung der Anforderungen der Richtlinie bewegen.

Art. 6 enthält eine Haftungsregelung für die Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, nach welcher sie für die Schäden gegenüber Dritten, die vernünftigerweise auf das Zertifikat vertrauen, haften. Die Zertifizierungsdiensteanbieter haften dafür, dass a) alle Informationen und vorgeschriebenen Angaben eines qualifizierten Zertifikats korrekt und vollständig sind, b) der im Zertifikat angegebene Unterzeichner zum Zeitpunkt der Ausstellung des Zertifikats im Besitz der Signaturerstellungsdaten (privater Schlüssel) war, die den im Zertifikat angegebenen beziehungsweise identifizierten Signaturprüfdaten (öffentlicher Schlüssel) entsprechen, c) falls der Zertifizierungsdienstanbieter sowohl Signaturerstellungsdaten als auch Signaturprüfdaten erzeugt, beide Komponenten in komplementärer Weise eingesetzt werden können, d) der Widerruf eines Zertifikats rechtzeitig eingetragen wird.

Ein Merkmal dieser Haftung ist die Verschuldung mit Beweislastumkehr. Im Streitfall muss der Anbieter immer nachweisen, dass er nicht fahrlässig gehandelt hat (Art. 6 Abs. 1 RLeS). Der Zertifizierungsdiensteanbieter kann allerdings Beschränkungen für die Verwendung des Zertifikats angeben - vorausgesetzt, dass diese Beschränkungen für Dritte erkennbar sind. Für Schäden, die über diese Beschränkungen hinausgehen, haftet der Zertifizierungsdiensteanbieter nicht (Art. 6 Abs. 3 RLeS). Ferner muss der Zertifizierungsdiensteanbieter nach Anhang II h) über ausreichende Finanzmittel verfügen, insbesondere um das Haftungsrisiko für Schäden zu tragen, wie beispielsweise durch den Abschluss einer Versicherung.

1.2.2.5 Anerkennung von internationalen Zertifikaten

Ein anspruchsvolles Ziel der Signaturrichtlinie ist es, einen Beitrag zur Entwicklung des internationalen Geschäftsverkehrs, nicht nur im europäischen Raum, sondern auch weltweit zu leisten. Hierbei erfasst der Richtliniengeber vor allem Vereinba-

tragsabschluss 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.

67 *Roßnagel* 2002, 138.

rungen mit Drittländern über multilaterale Regeln, die die gegenseitige Anerkennung der Zertifizierungsdienste betreffen (Erwägungsgrund 23, RLeS).

Die Zertifikate von einem Zertifizierungsdiensteanbieter eines Drittlandes, die öffentlich als qualifizierte Zertifikate ausgestellt werden, sollen den Zertifikaten einem in der Gemeinschaft niedergelassen Zertifizierungsdiensteanbieter rechtlich gleichgestellt werden, wenn sie eine von drei Voraussetzungen erfüllen (Art. 7 Abs. 1). Entweder erfüllt der Zertifizierungsdiensteanbieter die Anforderungen der Richtlinie und hat sich einer freiwilligen Akkreditierung eines Mitgliedsstaats unterworfen oder ein in der Europäischen Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen der Richtlinie erfüllt, steht für die Zertifikate des Anbieters aus dem Drittland ein. Die dritte Möglichkeit wäre, dass das Zertifikat oder der Zertifizierungsdiensteanbieter aus dem Drittland im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Europäischen Gemeinschaft und dem Drittland oder der internationalen Organisation anerkannt ist.

1.2.3 Signaturrichtlinie und Anpassungsbedarf des Signaturgesetz 1997

Die Signaturrichtlinie sieht im Art. 13 vor, dass die Mitgliedsstaaten die erforderlichen Rechts- und Verwaltungsvorschriften erlassen müssen, um ihren Bestimmungen nachzukommen. Mit der Verabschiedung und dem Inkrafttreten der Signaturrichtlinie stellte sich dann zuerst die Frage, ob ein Anpassungsbedarf des Signaturgesetzes 1997 bestand und wenn ja, in welchen Umfang, und wie eine Anpassung stattfinden sollte.[68]

Inhaltlich gab es mehrere Punkte im deutschen Signaturrecht, die entweder angepasst, ergänzt oder neu miteinbezogen werden mussten. Zunächst mussten die Definitionen und die Gesetzessprache des Signaturgesetzes 1997 erheblich geändert werden, um diese an die technikoffenen Formulierungen und Konzepte der Signaturrichtlinie anzupassen. Gestrichen werden sollte ebenso die im Signaturgesetz 1997 enthaltene Lizenzierungspflicht für die Inbetriebnahme einer Zertifizierungsstelle, da eine solche Anforderung im Widerspruch zum Marktfreiheitsgrundsatz der Signaturrichtlinie stand. Angesichts des Art. 6 der Richtlinie sollte in das deutsche Signaturrecht eine neue Haftungsregelung einbezogen werden. Des Weiteren sollten die Rechtsfolgen der fortgeschrittenen elektronischen Signatur mit besonderer Qualität geregelt werden, um diese gemäß Art. 5 Abs. 1 der Signaturrichtlinie der rechtlichen Wirksamkeit der handschriftlichen Unterschrift gleichzustellen. Ferner sollten auch die Vorschriften zur Anerkennung ausländischer Zertifikate gemäß den Richtliniebestimmungen angepasst werden.

Die Bundesregierung entschloss sich dem Parlament ein neues Signaturgesetz vorzulegen, um die technischen und organisatorischen Anforderungen der Signaturrichtlinie umzusetzen. Die Bestimmung zur Gleichstellung der elektronischen Signa-

68 *Roßnagel*, RMD, SigG Einl., Rn. 146.

tur mit der eigenhändigen Unterschrift ist durch eine Änderung des BGB herbeigeführt worden. Außerdem ist die ZPO mit einer von der Richtlinie nicht geforderten Beweiserleichterung versehen worden. Im Folgenden wird das aus dem zweiten Signaturgesetz entstandenem Signaturrecht untersucht.

1.3 Das zweite Signaturgesetz

Am 22.5.2001 trat in Deutschland das zweite Signaturgesetz (im Folgenden: SigG) in Kraft. Erforderlich war die Verabschiedung eines neuen Signaturgesetzes nicht nur um die Signaturrichtlinie ins deutsche Recht umzusetzen, sondern auch zum Zweck der Aufnahme der Ergebnisse der Evaluierung des Signaturgesetzes 1997 ins neue Gesetz.[69] Die Evaluierung war eine Aufforderung des Deutschen Bundestags an die Bundesregierung anlässlich der Verabschiedung des Signaturgesetzes 1997. Der Regierungsbericht schlug punktuelle technische Verbesserungen vor, einige basierend auf Auseinandersetzungen der Rechtswissenschaft, wie Regelungen zur Auslagerung von Funktionen der Zertifizierungsstelle auf Drittdienstleister und zur Anerkennung von Prüf- und Bestätigungsstellen.[70] Ferner wurden die Anregungen der Berufskammern hinsichtlich der Ausstellung und Sperrung von Zertifikaten sowie bezüglich der Verwendung von Pseudonymen mit Angaben über berufsrechtliche Zulassungen aufgenommen.[71] Das Signaturgesetz wurde durch die Rechtsverordnung von 16.11.2001 näher konkretisiert.

Im Folgenden sind die technischen und rechtlichen Rahmenbedingungen, die aus dem Signaturgesetz und der Signaturverordnung resultieren, darzustellen.

1.3.1 Das technologische Konzept

Geprägt von den Grundsätzen der Signaturrichtlinie verfolgt das Signaturgesetz einen technikoffenen Ansatz. Um das zu erreichen, verwendet es die abstrakten Begriffsdefinitionen der Signaturrichtlinie wie „elektronische Signatur“, „Signaturschlüssel“ und „Signaturprüfschlüssel“ anstelle von Formulierungen wie „digitale Signatur“, „privater Schlüssel“ und „öffentlicher Schlüssel“. Kernstück des Signaturgesetzes sind jedoch die qualifizierten und akkreditierten Signaturverfahren, die auf der Technik der asymmetrischen Kryptographie basieren.

69 BT-Drs. 14/4662, 14.

70 *Roßnagel*, NJW 2001, 1818.

71 BT-Drs. 14/4662, 17.

1.3.2 Zertifizierungsstruktur und Gültigkeitsmodell

Eine Zertifizierungsstruktur hat ihre Bedeutung darin, dass der Empfänger eines elektronisch signierten Dokuments dessen Urheberschaft durch den öffentlichen Schlüssel des Signierers bestätigen lassen kann. Für diesen Zweck soll der Empfänger sowohl die Authentizität des Zertifikats seines Kommunikationspartners überprüfen, als auch die Authentizität der gesamten Zertifikatskette (Zertifizierungsdiensteanbieter und wiederum das Zertifikat der Instanz, die das Zertifikat des Zertifizierungsdiensteanbieters ausgestellt hat).

Im Rahmen der qualifizierten Signaturverfahren im Signaturgesetz ist grundsätzlich die Konfiguration von zwei Zertifizierungsstrukturen möglich. In der ersten Variante ist die Bundesnetzagentur als oberste Instanz positioniert, welche nach § 16 Abs. 1 SigG die Zertifikate der akkreditierten Zertifizierungsdiensteanbieter ausstellt und so mit ihrem selbst signierten Wurzelzertifikat als Vertrauensanker für die Bestätigung der Authentizität der von ihr ausgestellten Zertifikate fungiert. Der Bundesnetzagentur kommt ein hohes Vertrauen aufgrund ihrer öffentlich-rechtlichen Stellung und ihrer Funktion als Aufsichtsbehörde zu.[72] In diesem Zusammenhang besteht die akkreditierte Zertifizierungsinfrastruktur hauptsächlich aus drei Ebenen. In der obersten Position befindet sich die Aufsichts- und Regulierungsbehörde, die Bundesnetzagentur. In der zweiten Ebene liegen die akkreditierten Zertifizierungsdiensteanbieter und in der dritten die Endnutzer.

Der akkreditierten Zertifizierungsstruktur der Bundesnetzagentur entspricht als Gültigkeitsmodell das Kettenmodell.[73] Dies ergibt sich aus § 16 Abs. 1 SigG. Danach stellt die zuständige Behörde den akkreditierten Zertifizierungsdiensteanbietern die für ihre Tätigkeit benötigten qualifizierten Zertifikate aus.[74] Das Kettenmodell verhindert, dass mit dem Widerruf oder Ablauf der Zertifikate in der ersten oder in der zweiten Ebene alle in der Hierarchie untergeordneten Zertifikate ungültig werden.[75] Zur Gültigkeit der Signatur genügt es, dass das entsprechende Zertifikat zum Zeitpunkt des Signierens gültig war, unabhängig davon, ob die übergeordneten Zertifikaten noch gültig waren. Die Zertifikate müssen lediglich zum Zeitpunkt ihrer Anwendung gültig sein: Das Teilnehmerzertifikat bei der Signierung des Dokuments, das Zertifikat der Zertifizierungsstelle bei der Ausstellung des Teilnehmerzertifikats und das Zertifikat der Wurzelinstanz bei der Zertifizierung des Trustcenters.[76] Diese Eigenschaft ist von besonderer Bedeutung für elektronisch signierte

72 *Fischer-Dieskau* 2006, 91.

73 *Lo Iacono*/*Dietze*, DuD 2005, 16.

74 Die Bundesnetzagentur stellt den Zertifizierungsdiensteanbieter mehrere Zertifikate aus, wenn für jede seine Tätigkeiten ein eigenes Zertifikat verwendet wird. Somit bestehen Zertifikate für die Zertifikaterstellung, für das Signieren beim Sperrdienst und soweit angeboten für Zeitstempelzertifikate.

75 *Büger*/*Esslinger*/*Koy*, DuD 2004, 138.

76 *Lo Iacono*/*Dietze*, DuD 2005, 15.

Dokumente, welche dauerhaft überprüfbar sein müssen. Würde die Gültigkeit der Signatur von dem Gültigkeitszeitraum der höherrangigen Zertifikate abhängen, wäre das Signieren von Dokumenten, die langfristig aufbewahrt werden müssen, praktisch sinnlos, denn ihre Gültigkeit würde stets verloren gehen, wenn die übergeordneten Zertifikate gesperrt würden oder abgelaufen wären.

Die andere Variante einer Zertifizierungsstruktur im Rahmen des Signaturgesetzes ist die der angezeigten Zertifizierungsdiensteanbieter, nach welcher den Anbietern völlig frei steht, ihre Zertifizierungsstrukturen zu konfigurieren. Vorgesehen für diese ist keine vorgegebene gemeinsame Zertifizierungsstruktur mit anderen Anbietern.[77] Sie können möglicherweise lediglich ein Selbstzertifikat haben[78], mit dem Nachteil, dass dieses Zertifikat in keiner Vertrauenshierarchie eingebettet ist. Die Verlässlichkeit des Zertifikats bezieht sich rein auf das Vertrauen und auf den Ruf des Zertifizierungsdiensteanbieters. Ob das Zertifikat tatsächlich von den darin namentlichen genannten Ausstellern stammt, lässt sich nicht ohne weiteres überprüfen. Vielmehr wird es davon abhängen, ob der Signaturempfänger das Selbstzertifikat schon kennt oder ob ein Dritter, dem er vertraut, es bestätigt.[79] Dabei können gegenseitige Anerkennungen von Selbstzertifikaten zwischen angemeldeten Zertifizierungsdiensteanbietern helfen, um die Vertrauenswürdigkeit ihrer Zertifikate zu verstärken. Hierbei handelt es sich um die so genannte Cross-Zertifizierung oder um eine Bridge-CA oder eine Kombination beider Systeme. Bei der Cross-Zertifizierung werden Wurzelzertifikate mehrerer Zertifizierungsstellen verkettet.

Bei der Zertifizierungsstruktur der Anbieter qualifizierter Zertifikate ohne Akkreditierung kann sowohl das oben erwähnte Kettenmodel als auch das so genannte modifizierte Schalenmodell verwendet werden. Das modifizierte Schalenmodell ist eine Variante des Schalenmodells, das auf dem internationalen Standard X.509 und auf dem RFC 3280 basiert.[80] Anders als beim Kettenmodell erfordert das Schalenmodell zur Gültigkeit der Signatur, dass zum Zeitpunkt ihrer Verifikation das Teilnehmerzertifikat sowie alle zugrunde liegenden Zertifikate gültig waren.[81] Das modifizierte Schalenmodell seinerseits verlangt die Gültigkeit aller übergeordneten Zertifikate zum Zeitpunkt der Erzeugung der elektronischen Signatur und nicht zum Zeitpunkt der Verifikation.[82] Im Vergleich zum Kettenmodell sind somit das Schalenmodell und das modifizierte Schalenmodel restriktiver. Der Unterschied zwi-

77 *Roßnagel*, MMR 2002, 217.

78 Gegen die Möglichkeit der Selbstzertifizierung, *Rapp* 2002, 56. Der Grund dafür ist, dass die Zertifizierung des Signaturschlüssels die Identifikation des Signaturschlüsselinhabers voraussetzt und diese darf nur durch die Personenverschiedenheit zwischen der feststellenden und der zu identifizierenden Person erfolgen; a. A. *Bizer*, DuD 2002, 107; siehe hierzu unten in diesem Teil Gliederungspunkt 1.3.3.3.1.

79 *Roßnagel*, MMR 2002, 217.

80 *Büger*/*Esslinger*/*Koy*, DuD 2004, 138.

81 *Lo Iacono*/*Dietze*, DuD 2005, 15.

82 *Dietze*/*Gießmann*/*Lo Iacono*, DuD 2005, 207.

schen dem Kettenmodell und dem modifizierten Schalenmodell ist, dass beim modifizierten Schalenmodel das Endnutzerzertifikat (und nicht die schon mit diesem Zertifikat signierten Dokumente) seine Gültigkeit verliert, wenn ein übergeordnetes Zertifikat abläuft oder gesperrt wird. Beim Kettenmodel bleiben die untergeordneten Zertifikate in diesem Fall gültig. Die Verwendung des modifizierten Schalenmodels verursacht angesichts dieser Tatsache im Vergleich zum Kettenmodell erhöhte Kosten, wenn ein Wurzelzertifikat oder ein Zertifizierungsdiensteanbieterzertifikat gesperrt werden muss. Denn allen Nutzern müssen neue Zertifikate ausgestellt werden, was vermutlich auf die Kosten des Signaturschlüssel-Inhabers gehen soll.[83] Das Schalenmodel zeichnet sich somit dadurch aus, nutzerunfreundlich zu sein und steht nicht im Einklang zu den Vorschriften des Signaturgesetzes für qualifizierte Zertifikate.[84]

1.3.3 Die Signaturverfahren

Den Bestimmungen der Signaturrichtlinie folgend, unterteilt das Signaturgesetz die verschiedenen Signaturverfahren in Stufen. Anders als die Richtlinie, die nur zwei elektronische Signaturen definiert, aber drei kennt, definiert das Signaturgesetz vier verschiedene Signaturstufen.

1.3.3.1 Die einfache elektronische Signatur

Auf der niedrigsten Stufe befindet sich die einfache elektronische Signatur im Sinn von § 2 Abs. 1 SigG. Hierbei wird die Definition der Signaturrichtlinie für die „elektronische Signatur“ im Ganzen übernommen: „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“. Die Tatbestandsmerkmale dieser Definition können beispielsweise schon einfache E-Mails mit den Namensangaben des Absenders erfüllen. Die einfachen Signaturen sind mit keinen spezifischen Rechtsfolgen verbunden.[85]

1.3.3.2 Die fortgeschrittene elektronische Signatur

Die fortgeschrittene elektronische Signatur wird im § 2 Abs. 2 des SigG definiert. Ebenso wie die einfache elektronische Signatur, wurde der Begriff von der Signaturrichtlinie völlig übernommen. Zu der Definition der elektronischen Signatur werden

83 *Fischer-Dieskau* 2006, 102.

84 *Dietze*/*Gießmann*/*Lo Iacono*, DuD 2005, 208.

85 *Roßnagel*, MMR 2002, 215.

vier weitere Anforderungen hinzugefügt. Die fortgeschrittene elektronische Signatur muss ausschließlich dem Unterzeichner zugeordnet sein, die Identifizierung des Unterzeichners ermöglichen, die alleinige Kontrolle der Erstellungsmittel durch den Unterzeichner gestatten und die Feststellung einer nachträglichen Veränderung der Daten ermöglichen.[86]

1.3.3.3 Die qualifizierte elektronische Signatur

Im Rahmen des Signaturgesetzes sind die qualifizierten Signaturen die dritte Stufe von den vier vorgesehenen Signaturverfahren. Was die Signaturrichtlinie nicht explizit anerkennt[87], wird im deutschen Signaturgesetz klar definiert: die qualifizierte Signatur. Diese stützt sich auf die vier Anforderungen der einfachen und der fortgeschrittenen Signatur und noch zwei weiteren, nämlich die des Art. 5 Abs. 1 Nr. 1 RLeS: die Signatur muss auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt werden (§ 2 Abs. 3 SigG). Die Regelungen des Signaturgesetzes fokussieren die qualifizierten Verfahren. Für diese ist lediglich eine Anzeige der Zertifizierungsdiensteanbieter vor der Inbetriebnahme bei der Bundesnetzagentur erforderlich.

1.3.3.3.1 Das gültige qualifizierte Zertifikat

Die erste besondere Voraussetzung der qualifizierten Signatur ist, dass sie auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht. Ein qualifiziertes Zertifikat muss nach § 7 Abs. 1 Satz 1 SigG bestimmte Angaben enthalten:

- den Namen des Signaturschlüssel-Inhabers oder ein unverwechselbares Pseudonym,
- den zum Signaturschlüssel-Inhaber zugeordneten Signaturprüfschlüssel (öffentlicher Schlüssel),
- die Bezeichnung der Algorithmen zur Benutzung des Signaturprüfschlüssels,
- die laufende Nummer des Zertifikats,
- Gültigkeitszeitraum des Zertifikats,
- den Namen des Zertifizierungsdienstanbieters, der das Zertifikat ausgestellt hat, sowie des Staates, in dem er niedergelassen ist,

86 S. näher *Roßnagel*, MMR 2003, 164.

87 Denn die Richtlinie spricht von „fortgeschrittenen elektronischen Signaturen“ die auf einem qualifizierten Zertifikat beruhen und zusätzlich von einer sicheren Signaturerstellungseinheit erstellt werden, ohne die Bezeichnung „qualifizierte elektronische Signatur“ zu verwenden.

- Angaben, dass es sich um ein qualifiziertes Zertifikat handelt. Des Weiteren kann das Zertifikat Angaben darüber enthalten, auf die sich die Nutzung des Signaturschlüssels bestimmter Anwendungen nach Art oder Umfang beschränkt. Nach Bedarf kann das Zertifikat auch Attribute des Signatur-Schlüsselinhabers enthalten.

Das Signaturgesetz sieht nicht die Möglichkeit vor, dass Zertifikate unter dem Namen einer juristischen Person ausgestellt werden dürfen. Gemäß § 2 Abs. 9 SigG dürfen nur natürliche Personen als Signaturschlüssel-Inhaber auftreten.[88]

Das qualifizierte Zertifikat muss ferner nach § 7 Abs. 1 Satz 1 SigG eine qualifizierte elektronische Signatur tragen. Der Gesetzgeber hat in diesem Zusammenhang nur an die Anforderungen des qualifizierten Zertifikates des Signaturschlüssel-Inhabers, jedoch nicht an die des Zertifizierungsdienstanbieters gedacht.[89] Denn Urheber dieser Signatur darf nach § 2 Nr. 7 SigG nur ein Zertifizierungsdiensteanbieter sein. Es ist somit klar, dass die qualifizierte Signatur mit Zertifikat des Signaturschlüssel-Inhabers vom Zertifizierungsdiensteanbieter stammt.[90] Für akkreditierte Zertifizierungsdiensteanbieter hingegen stellt nach § 16 Abs. 1 SigG die Bundesnetzagentur die entsprechenden Zertifikate aus. Die qualifizierte Signatur des Zertifikats des angezeigten Zertifizierungsdiensteanbieters kann jedoch entweder von ihm selbst (Selbstzertifizierung) oder von einem anderen Zertifizierungsdiensteanbieter (Cross-Zertifizierung) stammen.[91] Angesichts dieser Regelungslücke des Signaturgesetzes schlägt die Literatur die Anwendung des Anhangs I h) RLeS vor.[92] Danach muss in einem qualifizierten Zertifikat lediglich „die fortgeschrittene elektronische Signatur des ausstellenden Zertifizierungsdiensteanbieters“ angegeben sein. Der Weg für eine Selbstzertifizierung ist somit offen. Wie *Bizer* zu Recht darauf hinweist, stehen im Vordergrund des Konzepts der Richtlinie eher die Anforderungen den Nachweis der Integrität der Angaben des qualifizierten Zertifikats zu erfüllen, als den Nachweis der Authentizität zu gewährleisten.

1.3.3.3.2 Die sichere Signaturerstellungseinheit

Die Sicherheit von Signaturerstellungseinheiten setzt die Gewährleistung von zwei Bedingungen voraus: Erstens ihre Einmaligkeit und zweitens die Geheimhaltung des privaten Schlüssels.[93] Dazu darf dieser nicht aus dem öffentlichen Schlüssel oder

88 S. hierzu kritisch *Skrobotz*, DuD 2004, 410; *Fischer-Dieskau*/*Roßnagel*, MMR 2004, 134.

89 *Bizer*, DuD 2002, 107.

90 Zu dieser Problematik, siehe bereits in diesem Teil Gliederungspunkt 1.3.2.

91 Siehe bereits in diesem Teil Gliederungspunkt 1.3.2.

92 *Bizer*, DuD 2002, 107; a. A. in Bezug auf die Existenz einer Regelungslücke im Signaturgesetz *Bösing* 2005 94 ff.

93 *Wohlmacher*/*Fox*, DuD 1997, 260 ff.

signierten Daten abgeleitet werden. Falls der private Schlüssel ausgeforscht und kopiert wird, sind seine vorausgesetzte Einmaligkeit und somit auch die Zuordnung der damit erstellten Signatur zum Teilnehmer nicht mehr gegeben. Erforderlich ist daher die alleinige Kontrolle des Signaturschlüssels durch den Teilnehmer. Grundsätzlich darf nur er ihn verwenden.[94] Des Weiteren müssen bei der Signaturerzeugung Komponenten benutzt werden, die eine Speicherung des privaten Schlüssels außerhalb des Speicherorts ausschließen. Zur Umsetzung dieser Anforderungen können beispielsweise geeignete Chipkarten, PCMCIA-Karten[95] oder Sicherheitstoken mit eingebauten Prozessoren zur Schlüsselerzeugung genutzt werden. Diese Komponenten, nach dem Stand der Technik, können nicht ausgelesen werden. Bei der Erzeugung des Schlüssels außerhalb der Chipkarte oder des Sicherheitstoken müssen die Komponenten ein Ausforschen des privaten Schlüssels, während der Erzeugung und Übertragung auf das Speichermittel, ausschließen. Nach § 15 Abs. 1 SigV müssen sichere Signaturerstellungseinheiten gewährleisten, dass der Signaturschlüssel erst dann angewendet werden kann, wenn die Identifikation des Signierers entweder durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale gegeben ist. Diese Vorschrift bezieht sich zunächst durch den Ausdruck „Besitz“ auf Produkte wie Chipkarten oder Sicherheitstoken[96], die eine gewisse Tragbarkeit aufweisen. Jedoch es ist nicht auszuschließen, dass sich andere Konzepte an den Begriff anpassen, wie beispielsweise das so genannte Trusted Platform Module, eine durch die Trusted Computing Group spezifizierte Lösung, die ähnliche Funktionen wie eine Smartcard bietet.[97] Der Ausdruck „Wissen“ ist als PIN oder Passwort zu verstehen und die biometrischen Merkmale sind Verhaltens- oder Körpercharakteristika, wie beispielsweise Gesicht, Finger oder Iris.[98] Die Bedeutung der Verwendung von biometrischen Verfahren in diesem Zusammenhang liegt darin, dass diese Technologie eine wichtige Rolle bei der Frage der Autorisierung in der elektronischen Kommunikation spielen kann. Insbesondere weil in der elektronischen Welt der Missbrauch der PIN zur Signaturkarte möglich ist, ohne dass der Signaturempfänger es erkennt. Ferner ist es auch möglich, dass der Signierende

94 *Roßnagel*, MMR 2008, 23.

95 PCMCIA steht für „Personal Computer Memory Card International Association“. Die Bezeichnung wird auch für die Karten verwendet, die aus den Spezifikationen dieses Vereins stammen. Die Karten sind u.a. Speichererweiterungenkarten für PCs. Siehe hierzu www.pcmcia.org.

96 Die amtliche Begründung zu § 15 Abs. 1 SigV verweist auf eine Karte als Beispiel für die Erfüllung des Begriffs „Besitz“; *Bröhl*/*Tettenborn* 2001, 168.

97 Das TPM ist eine fest an das Mainboard von Personal Computern und Notebooks gelötete Smartcard. Unter anderen Funktionen dient das TPM der Erzeugung von asymmetrischen und symmetrischen Schlüsseln mit Hilfe eines hardwarebasierten Zufallszahlengenerators, der Signaturerstellung, der Hashwertberechnung und der asymmetrischen Verschlüsselung. S. hierzu *Stumpf*/*Sacher*/*Roßnagel*/*Eckert*, DuD 2007, 357.

98 Amtliche Begründung zu § 15 Abs. 1 SigV; *Bröhl*/*Tettenborn* 2001, 168.

seine Signaturkarte und seine PIN an Dritte weitergibt und dadurch Signaturen ohne seine Willen, aber in seinem Namen erstellet werden können.[99]

Im Rahmen des SigG dürfen Signaturschlüssel auf der sicheren Signaturerstellungseinheit sowohl vom Nutzer selbst (§ 17 Abs. 1 Satz 2) als auch durch den Zertifizierungsdiensteanbieter erzeugt werden (§ 17 Abs. 3 Nr. 1).

1.3.3.4 Die qualifizierte elektronische Signatur mit Anbieterakkreditierung

Obwohl nicht explizit definiert, schafft das SigG eine weitere Stufe von Signaturverfahren, die so genannte „qualifizierte elektronische Signatur mit Anbieterakkreditierung".[100] Das ergibt sich aus der systematischen Analyse von mehreren Vorschriften des SigG. § 15 SigG regelt die freiwillige Akkreditierung von Zertifizierungsdiensteanbietern. Der deutsche Gesetzgeber hat sich für die Etablierung eines freiwilligen Anbieterakkreditierungssystems gemäß Art. 3 Abs. 2 RLeS entschieden. Diese Vorschrift ermöglicht laut Erwägungsgrund 11 RLeS, dass die Mitgliedsstaaten ein solches System einführen, um eine Steigerung des Niveaus der erbrachten Dienste zu ermöglichen. Da es in Deutschland das Akkreditierungssystem im Rahmen des Signaturgesetzes 1997 in Form einer Genehmigung gab, der man sich freiwillig unterzog, wurde mit dem Signaturgesetz die mit der Bundesnetzagentur in der Spitze bestehende und schon operierende PKI-Infrastruktur fortgesetzt.

Gegenüber den qualifizierten Verfahren unterscheidet sich die Anbieterakkreditierung in verschiedenen Aspekten. Zertifizierungsdiensteanbieter akkreditierter Signaturen werden beispielsweise vorab von Prüf- und Bestätigungsstellen sowie von der Bundesnetzagentur[101] dahingehend geprüft, ob sie die Anforderungen des SigG erfüllen.[102] Dagegen werden Zertifizierungsdiensteanbieter qualifizierter Verfahren vorab nicht kontrolliert, sie müssen vielmehr gemäß § 4 Abs. 3 SigG spätestens mit der Betriebsaufnahme der Bundesnetzagentur diese lediglich anzeigen. Daraus folgt, dass Anbieter qualifizierter Signaturen über eine behauptete, aber nicht über eine nachgewiesene organisatorische Sicherheit verfügen.[103]

Darüber hinaus bieten akkreditierte Signaturen die Möglichkeit des Nachweises ihrer umfassenden technischen Sicherheit. Gleiches gilt bezüglich all ihrer Hardwarekomponenten, da diese ebenso vorab überprüft werden. Diese müssen gemäß § 11 Abs. 3 SigV die Vorgaben des Abschnitts I der Anlage 1 SigV erfüllen sowie

99 S. *Tielemann*/*Fischer-Dieskau*/*Pordesch*/*Brandner*/*Barzin*, in: Roßnagel/Schmüker 2005, Kap. 9.1; *Roßnagel*, MMR 2008, 22 ff.

100 Wie *Roßnagel* zu Recht hinweist, wird die Bezeichnung „akkreditierte Signatur" in der Praxis verwendet, obwohl nicht die Signatur, sondern das Verfahren des Anbieters akkreditiert ist, MMR 2002, 215.

101 Siehe hierzu unten in diesem Teil Gliederungspunkt 1.3.4.2.

102 *Roßnagel*, MMR 2002, 216.

103 *Roßnagel*, MMR 2002, 216.

nach § 15 Abs. 7 SigG dem Stand von Wissenschaft und Technik entsprechen. Für die qualifizierten Signaturen werden laut § 17 Abs. 4 SigG lediglich die sichere Signaturerstellungseinheit sowie die Komponenten zur Schlüsselerzeugung bei Zertifizierungsdiensteanbietern vorab geprüft. Eine Vorabprüfung der Signaturprüf- und Signaturanwendungskomponenten oder der technischen Komponenten für Verzeichnis-, Sperr- und Zeitstempeldienste findet nicht statt.

Ein weiterer Unterschied besteht darin, dass nach § 16 Abs. 1 SigG nur die Zertifikate akkreditierter Anbieter von der Bundesnetzagentur ausgestellt werden. Dies garantiert zum einen die Vertrauenswürdigkeit der gesamten Zertifikatskette, denn Signaturempfänger können sich auf die Stabilität einer behördlichen Entität verlassen, welche die Identität der Zertifizierungsdienstanbieter bestätig. Zum anderen trägt die einheitliche Referenz der zuständigen Behörde dazu bei, die notwendige Interoperabilität zwischen den Leistungen verschiedener Zertifizierungsdiensteanbietern zu schaffen, da sich Zertifikate aller akkreditierten Entitäten in der gleichen Zertifikatstruktur befinden.[104]Zertifizierungsdiensteanbieter qualifizierter Verfahren erhalten hingegen kein Zertifikat der Bundesnetzagentur und müssen sich folglich entweder selbst zertifizieren oder von einem anderen Zertifizierungsdiensteanbieter durch eine so genannte „Brückenlösung“ zertifiziert werden.[105] Diese Lösung bringt jedoch Unsicherheiten mit sich, wenn der im Zertifikat namentlich angegebene Zertifizierungsdiensteanbieter dem Signaturempfänger nicht in vertrauter Weise bekannt ist.

Ferner zeichnen sich akkreditierte Zertifikate im Vergleich zu einfachen qualifizierten Zertifikaten dadurch aus, dass sie langfristig prüfbar bleiben. Laut § 4 Abs. 2 SigV müssen akkreditierte Zertifikate mindestens weitere 30 Jahre ab dem Schluss des Jahres, in dem ihre Gültigkeit endet, prüfbar oder abrufbar gehalten werden. Qualifizierte Zertifikate haben gemäß der Bestimmung des § 4 Abs. 1 SigV dagegen lediglich eine garantierte Überprüfbarkeit für die Dauer ihrer Gültigkeit plus fünf Jahre ab Jahresende. Dieser Unterschied hat eine ausschlaggebende Bedeutung für Teilnehmer, die ihre elektronischen Dokumente aufbewahren müssen oder wollen. Wichtig in diesem Zusammenhang ist überdies, dass nur bei akkreditierten Zertifizierungsdiensteanbietern, die ihre Tätigkeiten einstellen, die Bundesnetzagentur sicherstellen muss, dass die Tätigkeit durch einen anderen Zertifizierungsdiensteanbieter übernommen wird oder, falls dieser temporär nicht zur Verfügung steht, sie selbst diese Tätigkeit übernimmt.[106] Anbieter qualifizierter Zertifikate müssen gemäß § 13 Abs. 1 Satz 2 SigG selbst dafür sorgen, dass die bestehende Dokumentation und die noch gültigen Zertifikate von einem anderen Zertifizierungsdiensteanbieter übernommen werden.[107]

104 BT-Drs. 14/4662, 29.

105 *Bizer*, DuD 2002, 107; *Roßnagel*, MMR 2002, 217; *Hammer*/*Petersen* 2001, 192 ff.

106 Hierzu siehe unten in diesem Teil Gliederungspunk 1.3.4.2.

107 *Roßnagel*, MMR 2002, 219.

1.3.4 Die Bundesnetzagentur und ihre Aufgaben

Laut § 3 SigG obliegen der Bundesnetzagentur[108] die Aufgaben der zuständigen Behörde nach dem Signaturgesetz sowie nach der Rechtsverordnung.[109] Würde man alle einzelnen Aufgaben der Bundesnetzagentur auflisten, käme man zu einem Ergebnis von dreißig Tätigkeiten. Von diesen dreißig werden hier fünf zentrale Tätigkeiten dargestellt: erstens die Aufsicht über die Einhaltung der Bestimmungen des Gesetzes und der Rechtsverordnung, zweitens die Akkreditierung der Zertifizierungsdiensteanbieter, drittens das Betreiben der obersten nationalen Zertifizierungswurzelinstanz, viertens die Anerkennung von Prüf- und Bestätigungsstellen und fünftens das Erstellen und Veröffentlichen von Katalogen und Listen. Im Folgenden werden diese Aufgaben einer näheren Betrachtung unterzogen.

1.3.4.1 Aufsichtsaufgaben

Die Bundesnetzagentur muss gemäß § 19 Abs. 1 Satz 1 SigG grundsätzlich darauf achten, dass die Regelungen des Signaturgesetzes und der Rechtsverordnung von den Zertifizierungsdiensteanbietern eingehalten werden. Die Aufsichtskompetenz der Bundesnetzagentur fängt im Moment der Aufnahme des Betriebs durch die Zertifizierungsdiensteanbieter (§ 19 Abs. 1 Satz 2 SigG) an. Damit die Einhaltung der Regelungen gewährleistet wird, obliegt es zunächst der Bundesnetzagentur, Maßnahmen zu treffen (§ 19 Abs. 2 SigG). Das Signaturgesetz definiert dabei nicht, was unter „Maßnahmen“ zu verstehen ist. Es ist aber davon auszugehen, dass es sich nicht um durchgreifende Reaktionen handelt, sondern vielmehr um Hinweise und Verwarnungen an den Zertifizierungsdiensteanbieter. Drastischere Aufsichtsmaßnahmen können erst dann durchgeführt werden, wenn die „Maßnahmen“ nach § 19 Abs. 2 keinen Erfolg versprechen (§ 19 Abs. 3 SigG). In diesem Fall handelt es sich dann um die vorübergehende, teilweise oder vollständige Untersagung des Betriebes des Zertifizierungsdiensteanbieters (§ 19 Abs. 3 SigG). Dieses Verfahren bedingt jedoch bestimmte gesetzliche Voraussetzungen. Es dürfen erst dann Maßnahmen getroffen werden, wenn es die Tatsachen rechtfertigen und beispielsweise der Zertifizierungsdiensteanbieter nicht die für den Betrieb eines Zertifizierungsdienstes erforderliche Zuverlässigkeit und Fachkunde besitzt oder wenn er nicht über die erforderliche Deckungsvorsorge verfügt (§ 19 Abs. 3 SigG).[110] Die Verwendung von

108 Die Bundesnetzagentur hieß ursprünglich Regulierungsbehörde für Telekommunikation und Post (RegTP). Ihre Umbenennung erfolgte aufgrund des Gesetzes über die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn, vom 7.7.2005.

109 Siehe hierzu *Roßnagel*, MMR 1998, 468 ff.

110 Auf diese Weise darf im Rahmen des Signaturgesetzes keine systematische Kontrolle durch die Bundesnetzagentur erfolgen, um nicht gegen Art. 3 Abs. 1 RLeS zu verstoßen; BT-Drs.

ungeeigneten Produkten für qualifizierte elektronische Signaturen durch Zertifizierungsdiensteanbieter oder das Nichteinhalten anderer Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach dem Signaturgesetz und der Rechtsverordnung erfüllt nach § 19 Abs. 3 SigG ferner einen Grund für die Untersagung. Nach § 19 Abs. 4 SigG kann die Bundesnetzagentur die Sperrung von qualifizierten Zertifikaten anordnen, wenn Tatsachen vorliegen, welche die Annahme rechtfertigen, dass qualifizierte Zertifikate gefälscht oder nicht hinreichen fälschungssicher sind. Das gleiche gilt für den Fall, dass sichere Signaturerstellungseinheiten Sicherheitsmängel aufweisen, die unbemerkte Fälschungen qualifizierter Signaturen oder unbemerkte Verfälschungen signierter Daten zulassen.

Zur Erfüllung ihrer Aufsichtsaufgaben kann die Bundesnetzagentur die Mitwirkung von Zertifizierungsdiensteanbietern und Dritten, welche die Aufgaben von diesen übernehmen, in Anspruch nehmen. Hierbei handelt es sich gemäß § 20 Abs. 1 SigG um die Möglichkeit des Betretens der Geschäfts- und Betriebsräume dieser Dienstleister durch die zuständige Behörde und die in ihrem Auftrag handelnden Personen. Dies kann während der üblichen Betriebszeiten stattfinden. Auf Verlangen kann die Bundesnetzagentur Einsicht in die in Betracht kommenden Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstigen Unterlagen nehmen.

Ferner verhängt die Bundesnetzagentur Bußgelder für die elf Ordnungswidrigkeiten, die im § 21 Abs. 1 SigG vorgesehen werden. Dafür ist sie gemäß § 36 Abs. 1 Nr. 1 OWiG zuständig. Die Bundesnetzagentur erhebt darüber hinaus gemäß § 22 Abs. 1 SigG Kosten für die freiwillige Akkreditierung von Zertifizierungsdiensteanbietern, für die Ausstellung von qualifizierten Zertifikaten laut § 16 Abs. 1 SigG und von Bescheinigungen nach § 16 Abs. 3 SigG, für die Anerkennung von Prüf- und Bestätigungsstellen nach §18 SigG sowie für Maßnahmen nach § 19 Abs. 1 bis 4 SigG, die im Rahmen der Aufsicht durchgeführt werden müssen. Abgaben für die ständige Führung des von § 19 Abs. 6 SigG geforderten Verzeichnis- und Sperrdienstes werden von der zuständigen Behörde gemäß § 22 Abs. 2 SigG von den angezeigten Zertifizierungsdiensteanbietern erhoben. Das gleiche gilt für akkreditierte Zertifizierungsdiensteanbieter, die für die ständige Erfüllung des Verzeichnis- und Sperrdienstes nach § 16 Abs. 2 SigG. eine Abgabe an die zuständige Behörde entrichten müssen.

Des Weiteren gehört es im Rahmen der Aufsicht zur Aufgabe der Bundesnetzagentur die Papierprüfung der Herstellererklärungen in Bezug auf die Produkte für qualifizierte elektronische Signaturen durchzuführen.[111] Gemäß § 17 Abs. 4 Satz 3 SigG müssen die Hersteller von diesen Produkten jedoch spätestens bis zum Zeitpunkt des Inverkehrbringens des Produkts eine Ausfertigung ihrer Erklärungen in schriftlicher Form bei der Bundesnetzagentur hinterlegen. Entsprechen die Herstellererklärungen den Anforderungen des Signaturgesetzes und der Signaturverord-

14/4662, 31. Die zuständige Behörde kann nur dann eingreifen, wenn Anhaltspunkte für Fehler vorliegen. Hierzu, *Fischer-Dieskau*/*Steidle*, MMR 2006, 72.

111 Zu sicheren Produkten siehe in diesem Teil Gliederungspunkt 1.3.5.7.

nung, werden sie im Amtsblatt der zuständigen Behörde veröffentlicht (§ 17 Abs. 4 Satz 4 SigG). Es handelt sich dabei aber lediglich um eine formelle Papierprüfung und nicht um eine umfassende Prüfung, bei welcher zusätzlich die Signaturanwendungskomponenten die signaturrechtlichen Anforderungen erfüllen müssen.[112]

1.3.4.2 Akkreditierungsaufgaben

Eine weitere erhebliche Aufgabe der Bundesnetzagentur bezieht sich auf die Akkreditierung von Zertifizierungsdiensteanbietern. Gemäß Art. 3 Abs. 2 RLeS setzt das Signaturgesetz das Konzept der freiwilligen Akkreditierung um. Im Rahmen des Signaturgesetzes 1997 war eine Genehmigung der zuständigen Behörde mit Vorabprüfung der Maßnahmen zur Erfüllung der Sicherheitsanforderungen erforderlich. Aber auch nach § 1 Abs. 2 SigG 1997 stand es einer Zertifizierungsstelle frei, eine Genehmigung zu beantragen. Allerdings war die Sicherheitsvermutung des § 1 Abs. 1 SigG 1997 an die Genehmigung geknüpft.[113]

Um sich von der Bundesnetzagentur akkreditieren zu lassen, muss der Zertifizierungsdiensteanbieter einen Antrag stellen (§ 15 Abs. 1 Satz 1 SigG). Bei dem Akkreditierungsverfahren kann sich die zuständige Behörde privater Stellen bedienen. Aber der Bundesnetzagentur bleibt in jedem Falle die letzte Entscheidung über die Akkreditierung des jeweiligen Kandidaten vorbehalten.[114] Sind die Voraussetzungen des Signaturgesetzes und der Rechtsverordnung nicht erfüllt, ist die Akkreditierung nach § 15 Abs. 4 SigG zu versagen. Zu erteilen ist sie, wenn der Zertifizierungsdiensteanbieter vorab nachweist, dass die Anforderungen des Signaturgesetzes und der Rechtsverordnung erfüllt sind. Wird der Zertifizierungsdiensteanbieter akkreditiert, erhält er ein Gütezeichen, das die nachgewiesene technische und organisatorische Sicherheit zum Ausdruck bringt.[115]

Falls die Pflichten des Gesetzes oder der Rechtsverordnung von Zertifizierungsdiensteanbietern nicht erfüllt werden, hat die Bundesnetzagentur die Akkreditierung zu widerrufen oder, soweit die Gründe bereits zum Zeitpunkt der Akkreditierung vorlagen, zurückzunehmen, soweit eventuelle fehlerbehebende Maßnahmen keinen Erfolg versprechen. Werden die Tätigkeiten des Zertifizierungsdiensteanbieters als Folge eines Antrags auf Eröffnung eines Insolvenzverfahrens eingestellt, ist die Bundesnetzagentur in einer ihrer wesentlichsten Aufgabe gefordert. Sie hat Maßnahmen zur Übernahme der Tätigkeiten durch einen anderen akkreditierten Zertifizierungsdiensteanbieter zu ergreifen (§ 15 Abs. 6 SigG). Dadurch soll sichergestellt werden, dass die Verträge mit den Signaturschlüssel-Inhabern abgewickelt werden.

112 *Fischer-Dieskau*/*Steidle*, MMR 2006, 73; *Roßnagel*, MMR 2007, 490.

113 Siehe hierzu *Roßnagel*, NJW 1998, 3312.

114 BT-Drs. 14/4662, 27.

115 Möglich ist somit, dass das Gütezeichen im Geschäftsverkehr als Vertrauensfaktor dient. Siehe hierzu *Jandt* 2008, 279.

Sollte im Extremfall kein anderer Zertifizierungsdiensteanbieter die Dokumentation des Anbieters übernehmen, welcher seinen Betrieb einstellt, so hat die Bundesnetzagentur dies zu tun. Hierbei handelt es sich hauptsächlich um die Dokumentation in Bezug auf die ausgestellten qualifizierten Zertifikate, damit diese im Lauf der Zeit überprüfbar bleiben. In der Praxis der Bundesnetzagentur musste diese schon einmal die Dokumentation eines Zertifizierungsdiensteanbieters übernehmen. In diesem Fall wurde die Akkreditierung der Medizon AG (Anbieter im Gesundheitswesen) im Jahr 2003 widerrufen. Es haben sich auch schon mehrere Fälle ereignet, wo ein Zertifizierungsdiensteanbieter die Tätigkeiten eines anderen übernommen hat. Die Tätigkeiten von mehreren Steuerberater- und Rechtsanwaltskammern sind vom Unternehmen Datev eG übernommen worden.[116]

Im Sommer 2008 sind bei der Bundesnetzagentur sieben Zertifizierungsdiensteanbieter, die sowohl qualifizierte Zertifikate als auch qualifizierte Zeitstempel ausstellen, akkreditiert. Zwei andere Anbieter akkreditierten sich ausschließlich für die Ausstellung von qualifizierten Zertifikaten und einer ausschließlich für die Ausstellung von qualifizierten Zeitstempeln.

1.3.4.3 Wurzelinstanzaufgaben

Die Bundesnetzagentur ist auch die oberste nationale Zertifizierungsinstanz in der Hierarchie der akkreditierten Zertifizierungsdiensteanbieter. Sie wird als Wurzelinstanz der deutschen Public Key Infrastruktur benannt, denn sie befindet sich an der Spitze einer umgekehrten baumartigen Infrastruktur, in der die Zertifizierungsdiensteanbieter die „Zweige“ bilden. Hierbei stellt die Bundesnetzagentur den Zertifizierungsdiensteanbietern die für ihre Tätigkeiten benötigten qualifizierte Zertifikate aus (§ 16 Abs. 1 Satz 1 SigG). Zur Erfüllung dieser Aufgabe muss die zuständige Behörde allen für Zertifizierungsdiensteanbieter geltenden Vorschriften für die Vergabe und Sperrung von qualifizierten Zertifikaten folgen (§ 16 Abs. 1 Satz 2 SigG). Hierfür ist ein geeignetes Trustcenter erforderlich, in dem die alltäglichen Operationen der Wurzelinstanz durchgeführt werden.[117]

116 S. www.bundesnetzagentur.de → elektronische Signatur → Zertifizierungsdiensteanbieter → Akkreditierte Zertifizierungsdiensteanbieter, die ihre Tätigkeit eingestellt haben.

117 Die Kosten für die Hochbau- und Infrastrukturgestaltung der deutschen Wurzelinstanz (vier Büroräume mit Vereinzelungsschleuse, gepanzerten Türen und Fenstern, Einbruch-, Wasser- und Brandmeldeanlage und eigener Stromversorgung) betrug circa 348.000 €. Die IT-Infrastruktur (Internet-Server, Schlüsselgenerator u.a.) lang um die 358.000 €. S. hierzu www.bundesnetzagentur.de → elektronische Signatur → FAQ → Frage 6.

1.3.4.4 Anerkennung von Prüf- und Bestätigungsstellen

Die Bundesnetzagentur erkennt nach § 18 Abs. 1 SigG natürliche oder juristische Personen an, die entweder als Bestätigungsstelle oder Prüf- und Bestätigungsstelle im Rahmen des Signaturgesetzes wirken. Die Prüf- und Bestätigungsstellen unterstützen die zuständige Behörde dabei, die Einhaltung der Vorschriften des Signaturgesetzes und der Signaturverordnung zu überprüfen und zu bestätigen, insbesondere was die Erfüllung der Akkreditierungsvoraussetzungen gemäß § 15 SigG und die Anforderungen an Produkte für qualifizierte elektronische Signaturen angeht.

Im Signaturgesetz 1997 waren die Voraussetzungen und das Verfahren der Anerkennung nicht vorgesehen. Die Entscheidung über die Anerkennung lag somit im freien Ermessen der zuständigen Behörde.[118] Die Bestätigungsstellen waren und sind aber immer noch Private, die eigenständig mit hoheitlichen Aufgaben und Befugnissen beliehen worden sind. Sie haben die Anträge auf Produktbestätigungen gegenüber den Antragstellern beschieden.[119] Die Prüf- und Bestätigungsstellen für das Akkreditierungsverfahren waren auch als Beliehen[120] anzusehen, weil sie eine völlig selbständige durch das Gesetz übertragende öffentliche Aufgabe erfüllten.[121] Die Ausübung der Aufgaben von Prüf- und Bestätigungsstellen in dieser Form wiesen somit Eingriffe in das Grundrecht auf Freiheit der Berufsausübung von Herstellern, Einführern oder Vertreibern von technischen Komponenten sowie von Zertifizierungsdiensteanbietern auf. Das gleiche galt für die Notwendigkeit einer Anerkennung durch die Bundesnetzagentur für Prüf- und Bestätigungsstellen. Hier ist ebenso ein Eingriff in das Grundrecht auf Freiheit der Berufsausübung gegeben, denn eine mögliche Verweigerung dieser Anerkennung wirkt sich als Eingriff in die Berufsfreiheit aus".[122]Dieses Grundrecht ist im Art. 12 Abs. 1 GG vorgesehen und nach dieser Vorschrift ist ein Gesetz erforderlich, um es zu regeln.[123] Gemäß dem Bundesverfassungsgericht ist in solchen Fällen notwendig, dass der Bürger die Möglichkeit hat, aus dem Gesetz erkennen zu können, „welche Schranken seiner Freiheit im einzelnen gezogen sind".[124] In der Literatur wurde nach diesen Argumenten eine Erweiterung der Vorschriften gefordert, mit dem Ziel die Anerkennung und ihr Verfahren gesetzlich zu regeln und einen Rechtsanspruch auf Anerkennung vorzusehen, wenn die gesetzlich festzulegenden Voraussetzungen erfüllt sind.[125]

118 *Roßnagel*, MMR 1999, 347.

119 *Roßnagel*, MMR 1999, 344.

120 Beliehene Unternehmen sind natürliche oder juristische Personen des Privatrechts, die hoheitliche Funktionen im eigenen Namen und meist auch im eigenen Interesse, aber im Auftrag des Staates ausüben, ohne Teil der Staatsorganisation zu sein. *Creifelds* 2002, 193.

121 *Roßnagel*, MMR 1999, 344.

122 BVerfGE 86, 28, 37.

123 *Roßnagel*, MMR 1999, 347.

124 BVerfGE 80, 257, 267.

125 *Roßnagel*, MMR 1999, 347.

Angesichts der erwähnten wissenschaftlichen Auseinandersetzung über die Anerkennung von Prüf- und Bestätigungsstellen, regeln Signaturgesetz und Signaturverordnung die Materie ausführlicher. Auf der einen Seite bestimmt § 18 Abs. 1 SigG, dass die Interessenten auf die Anerkennung die für die entsprechende Tätigkeit erforderliche Zuverlässigkeit, Unabhängigkeit und Fachkunde nachweisen müssen[126], und nach § 18 Abs. 2 SigG ihre Aufgaben unparteiisch, weisungsfrei und gewissenhaft zu erfüllen haben. Auf der anderen Seite konkretisiert die Rechtsverordnung detaillierter das Verfahren und die Voraussetzungen der Anerkennung. § 16 Abs. 1 SigV bestimmt alle Anforderungen des Antrags einer Prüf- und Bestätigungsstelle.[127] Erforderlich ist auch der Nachweis, dass der Kandidat über ausreichende Erfahrungen in der Anwendung der Prüfkriterien verfügt (§ 16 Abs. 2 SigV). Die Vorgaben für die Prüfung von Produkten für qualifizierte elektronische Signaturen werden in einer Anlage der Signaturverordnung festgelegt. Hierbei werden Anforderungen an Prüftiefen, Schwachstellenbewertung, Stärke der Mechanismen und Algorithmen festgesetzt.

Somit wird mit dem Signaturgesetz eine klare gesetzliche Grundlage für die Anerkennung von Prüf- und Bestätigungsstellen und für die Ausübung ihrer Tätigkeiten geschaffen.

1.3.4.5 Erstellen und Veröffentlichen von Katalogen und Listen

Angesichts ihrer Funktionen und dem Gebot der Transparenz ist die Bundesnetzagentur auch verpflichtet, mehrere Listen und Kataloge zu erstellen und zu veröffentlichen. Diese können als Informationsaufgaben bezeichnet werden.

Nach § 16 Abs. 2 SigG hat die Bundesnetzagentur die Namen, Anschriften und Kommunikationsverbindungen der akkreditierten Zertifizierungsdiensteanbieter sowie den Widerruf oder die Rücknahme einer Akkreditierung und gegebenenfalls die Beendung und die Untersagung des Betriebes eines akkreditierten Zertifizierungsdiensteanbieters jederzeit über öffentlich zugängliche Kommunikationsverbindungen nachprüfbar und abrufbar zu halten. Dazu gehört auch die behördliche Pflicht, die von der Bundesnetzagentur ausgestellten und gesperrten qualifizierten Zertifikate in einem Verzeichnis zu führen. Im Verzeichnis der Bundesnetzagentur sind auch die qualifizierten Zertifikate für Signaturprüfschlüssel oberster ausländischer Zertifizierungsdiensteanbieter, die nach § 23 Abs. 2 SigG als gleichwertig anerkannt sind, aufzunehmen (§ 18 Abs. 4 SigV).

126 Was unter Zuverlässigkeit, Unabhängigkeit und Fachkunde zu verstehen ist, wird auf § 16 Abs. 3 SigV näher gegangen.

127 Hierbei werden u.a. Anforderungen, der aktuelle Handelsregisterauszug, Belege zum Nachweis der finanziellen Unabhängigkeit und Belege zum Nachweis der erforderlichen technischen, administrativen und juristischen Fachkunde verlangt.

Gemäß § 19 Abs. 6 SigG muss die Bundesnetzagentur auch die Namen der bei ihr angezeigten Zertifizierungsdiensteanbieter sowie der Zertifizierungsdiensteanbieter, die ihre Tätigkeit eingestellt haben oder deren Betrieb untersagt wurde, veröffentlichen.

In Bezug auf die Produkte für qualifizierte elektronische Signaturen hat die Bundesnetzagentur die Herstellererklärungen dieser Produkte, die den Anforderungen des Gesetzes und der Signaturverordnung entsprechen, in ihrem Amtsblatt zu veröffentlichen (§ 17 Abs. 4 SigG). Angesichts eventueller Festlegungen von Normen durch den Ausschuss für elektronische Signaturen, der die europäische Kommission unterstützt (§ 15 Abs.6 SigV), veröffentlicht die Bundesnetzagentur im Bundesanzeiger die aktuell gültigen Anforderungen an die Produkte für qualifizierte elektronische Signaturen. Ebenfalls im Bundesanzeiger wird laut Anlage 1 Abschnitt I Nr. 2 zur SigV eine Übersicht der sicherheitsgeeigneten Algorithmen und zugehörigen Parameter sowie der Zeitpunkt, bis zu dem die Eignung jeweils gilt, von der Bundesnetzagentur veröffentlicht.[128] Das Bundesamt für Sicherheit in der Informationstechnik bestimmt, unter Berücksichtigung internationaler Standards, diese Sicherheitseignung. Dabei sind Experten aus Wirtschaft und Wissenschaft zu beteiligen.

Nach § 16 Abs. 5 SigV hat die Bundesnetzagentur die Einzelheiten zu den Anforderungen an den Antrag auf die Anerkennung als Prüf- und Bestätigungsstellen im Bundesanzeiger zu veröffentlichen.

Des Weiteren stellt die zuständige Behörde auf ihrer Internetseite viele andere Informationen in Bezug auf ihre Tätigkeiten, wie beispielsweise ihren Signaturprüfschlüssel, Daten über ihre öffentlich erreichbare Kommunikationsverbindungen, Publikationen und Präsentationen von Spezialisten mit technischen und juristischen Fragen über das Thema elektronische Signaturen zur Verfügung.[129]

1.3.5 Zertifizierungsdiensteanbieter

Gemäß § 2 Abs. 8 SigG sind Zertifizierungsdiensteanbieter natürliche oder juristische Personen, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen. Diese Vorschrift ist zusammen mit § 2 Abs. 7 SigG zu interpretieren, der das „qualifizierte Zertifikat“ definiert. Hierbei weist die Definition auf die Anforderungen an die Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen hin. Im Folgenden wird auf die Anforderungen an die deutschen Zertifizierungsdiensteanbieter eingegangen.

128 Diese Information ist von großer Bedeutung für das Verfahren der erneuten Signatur, das im § 17 SigV geregelt wird. Hierzu auch,im diesen Teil Gliederungspunkt 1.3.5.5.2.

129 S. hierzu www.bundesnetzagentur.de → elektronische Signatur → Veröffentlichungen.

1.3.5.1 Zuverlässigkeit und Fachkunde

Gemäß § 4 Abs. 2 SigG ist eine Grundvoraussetzung für den Betrieb eines Zertifizierungsdienstes Zuverlässigkeit und Fachkunde des Dienstanbieters. Das Gesetz definiert Zuverlässigkeit als Gewährleistung für die Einhaltung der für den Betrieb eines Zertifizierungsdienstes maßgeblichen Rechtsvorschriften. Die Anforderung an die Zuverlässigkeit ist keine Neuigkeit des Signaturgesetzes im deutschen Recht. Vielmehr wurde der Begriff dem allgemeinen Gewerberecht entnommen.[130] Was den Umfang der Rechtsvorschriften, die geachtet werden müssen, angeht, sind nicht nur die Bestimmungen des Signaturrechts zu erfüllen, sondern auch die weiteren Anforderungen, wie beispielsweise steuer- und sozialversicherungsrechtliche Regelungen.[131] Das Überprüfen der Zuverlässigkeit obliegt zunächst der Bundesnetzagentur, wobei sie eine Prognoseentscheidung trifft.[132] Anknüpfungspunkte für eine Prognose sind Tatsachen, die unter einem Rückgriff auf ein festgestelltes Fehlverhalten in der Vergangenheit oder für ein künftig zu erwartendes Fehlverhalten des Zertifizierungsdiensteanbieters in der Zukunft rechtfertigen.[133] Es wird auch vertreten, dass die fehlende Zuverlässigkeit auch aus mangelnder wirtschaftlicher Leistungsfähigkeit, Steuerrückständen oder anderem steuerlichen Fehlverhalten resultieren kann.[134]

Die Fachkunde ist dann gegeben, wenn die im Betrieb eines Zertifizierungsdienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen (§ 4 Abs. 2 Satz 3 SigG). Weitere Stützpunkte für die Erfüllung des Begriffs „Fachkunde“ können aus der in § 16 Abs. 3 Nr. 1 SigV enthaltener Definition herausgezogen werden.[135] Nach dieser Vorschrift besitzt derjenige Fachkunde, der auf Grund seiner Ausbildung, beruflichen Bildung und praktischen Erfahrung zur ordnungsgemäßen Erfüllung der ihm obliegenden Aufgaben geeignet ist. Vom Gesetz gefordert ist infolgedessen, dass der Zertifizierungs-

130 *Demmel*, in: Manssen, Bd. 2, § 4, SigG Rn.7. Die Anforderung der Zuverlässigkeit kommt in mehreren Vorschriften der Gewerbeordnung vor, wie beispielsweise im § 33a Abs. 2 Nr. 1, nach welchem einer der Versagungsgründe der Erlaubnis zu Schaustellungen von Personen in Geschäftsräumen das Vorliegen von Tatsachen ist, die die Annahme rechtfertigen, dass der Antragsteller die für den Gewerbebetrieb erforderliche Zuverlässigkeit nicht besitzt.

131 *Demmel*, in: Manssen, Bd. 2, § 4, SigG Rn.8.

132 *Demmel*, in: Manssen, Bd. 2, § 4, SigG Rn.9.

133 *Demmel*, in: Manssen, Bd. 2, § 4, SigG Rn.10. Die Unzuverlässigkeit liegt vor, wenn ein Schadenseintritt durch das Fehlverhalten des Zertifizierungsdiensteanbieters im Hinblick auf das bisherige Verhalten nach dem gewöhlichen Lauf der Dinge in der Zukunft wahrscheinlich sein wird (BVerwG, GewArch. 1996, 250).

134 *Demmel*, in: Manssen, Bd. 2, § 4, SigG Rn.12.

135 § 16 Abs. 3 Nr. 1 SigV definiert den Begriff „Fachkunde“ im Rahmen der Festlegung der Mindestkriterien für Kandidaten auf die Anerkennung als Bestätigungsstelle oder Prüf- und Bestätigungsstelle.

diensteanbieter befähigte Mitarbeiter einstellt, die theoretische und praktische Kenntnisse um die alltäglichen Aufgaben eines Zertifizierungsdienstes haben.

1.3.5.2 Deckungsvorsorge

Zertifizierungsdiensteanbieter müssen nach § 12 SigG über eine geeignete Deckungsvorsorge verfügen, um den gesetzlichen Verpflichtungen zum Ersatz von Schäden nachzukommen. Auf die Bedeutung einer solchen Vorschrift im Zusammenhang mit einer spezifischen Verantwortungsregelung wurde schon früher in Deutschland hingewiesen.[136] Eine solche Deckung soll immer dann einen Ersatz garantieren, wenn der Zertifizierungsdiensteanbieter die Anforderungen des Signaturgesetzes und der Signaturverordnung verletzt oder wenn seine Produkte für qualifizierte elektronische Signaturen oder sonstige Sicherungseinrichtungen versagen und Schäden daraus entstehen. § 12 Satz 2 SigG legt die Mindestsumme von 250.000 Euro für die Deckungsvorsorge für jeden durch ein haftungsauslösendes Ereignis verursachten Schaden fest.

Wie die Deckungsvorsorge auszugestalten ist, bestimmt die Signaturverordnung. Nach § 9 SigV ist sie entweder durch eine Haftpflichtversicherung oder durch eine Freistellungs- oder Gewährleistungsverpflichtung eines Kreditinstituts zu erbringen.

Entscheidet sich der Zertifizierungsdiensteanbieter für den Abschluss eines Versicherungsvertrages, sind einige Anforderungen zu befolgen: Erstens muss die Versicherung manche Vorschriften des Gesetzes über den Versicherungsvertrag berücksichtigen (§ 9 Abs. 2 Nr. 1 SigV). Zweitens legt die Signaturverordnung bezüglich der Mindestversicherungssumme fest, dass sie 2,5 Millionen Euro für den einzelnen Versicherungsfall betragen muss (§ 9 Abs. 2 Nr. 1 Satz 1 SigV). Ein Versicherungsfall nach der Verordnung ist jedes auf den Einzelfall bezogenes haftungsauslösende Ereignis im Sinne des § 12 Satz 1 SigG, unabhängig von der Anzahl der dadurch ausgelösten Schadensfälle. Die Regelung schafft somit eine Unterscheidung zwischen „Versicherungsfall“ und „Schadensfall“ (dem einzelnen Schaden), wobei der Begriff Versicherungsfall breiter ist und mehrere Schadensfälle umfasst. Die Bestimmungen des Signaturgesetzes und der Signaturverordnung sind dann so zu verstehen, dass das Signaturgesetz die Mindestdeckungssumme von 250.000 Euro für den einzelnen eingetretenen Schaden festlegt und die Signaturverordnung wiederum eine Gesamtdeckungssumme in Höhe von 2,5 Millionen vorsieht. Dies bedeutet, dass die Gesamtmindestsumme das Zehnfache des einzelnen Schadensfalls umfassen muss.[137] Das klassische Beispiel hierfür ist das des falsch ausgestellten Zertifikats, auf dessen Daten mehrere Personen vertrauen und dadurch Schäden erleiden. Die so genannten Serienschäden sind somit von der Norm erfasst.[138] Da kaum Erfah-

136 *Roßnagel*, DuD 1997,79.

137 Amtliche Begründung zu § 9 SigV.

138 *Bröhl*/*Tettenborn* 2001, 153.

rungen in Bezug auf Schadenereignisse im Rahmen von Zertifizierungsdiensten bestehen, ist die Höhe der Mindestdeckungssummen auf eine Prognose des hinreichenden Gesamtschutzes für alle Geschädigten gestützt.[139] Es ist auch laut § 9 Abs. 2 Nr. 1 Satz 3 SigV verwehrt, eine Vereinbarung zu treffen, nach welcher ein Fehler, der sich in mehreren Zertifikaten, Zeitstempeln oder in der Zertifikatsgültigkeitsauskunft auswirkt, als ein Versicherungsfall gilt. Jedoch ist es möglich, die Versicherungsleistungen für alle in einem Jahr verursachten Schäden vertraglich zu limitieren. Die Jahreshöchstleistung muss aber mindestens 10 Millionen Euro betragen (§ 9 Abs. 2 Nr. 1 Satz 4 SigV).

Es steht den Zertifizierungsdiensteanbietern auch die Möglichkeit frei, die Deckungsvorsorge in Form einer Freistellungs- oder Gewährleistungsverpflichtung eines Kreditinstituts beizubringen. Anwendbar ist hierbei die klassische Bankbürgschaft, die wahrscheinlich in den Fällen eines kurzfristigen Markteinstiegs eine rasche Beschaffung der erforderlichen Deckungsvorsorge ermöglichen kann.[140]

1.3.5.3 Sicherheitskonzept

Die Maßnahmen zur Erfüllung der Sicherheitsanforderungen des Signaturgesetzes und der Signaturverordnung sind in einem Sicherheitskonzept zu dokumentieren und der Bundesnetzagentur aufzuzeigen. Das Sicherheitskonzept muss bereits praktisch umgesetzt sein, das heißt, es muss Organisations- und Sicherheitsroutinen beschreiben, die schon implementiert sind und nicht erst geplante einzusetzende Maßnahmen (§ 4 Abs. 2 Satz 4 SigG). Werden bestimmten Aufgaben des Zertifizierungsdienstanbieters an Dritte übertragen, dann muss dies nach § 4 Abs. 5 SigG ins Sicherheitskonzept einbezogen werden. Die Anforderungen an den Inhalt des Sicherheitskonzeptes sind in der Rechtsverordnung vorgesehen. Nach § 2 Abs. 1 muss das Sicherheitskonzept alle erforderlichen technischen, baulichen und organisatorischen Sicherheitsmaßnahmen und deren Eignung beschreiben. Kern des Sicherheitskonzepts sind die Vorkehrungen und Maßnahmen zur Sicherstellung und Aufrechterhaltung des Betriebes, insbesondere bei Notfällen (Abs. 4) sowie bei Abschätzung und Bewertung verbleibender Sicherheitsrisiken (Abs. 6). Was das eingesetzte Personal betrifft, muss der Zertifizierungsdiensteanbieter das Verfahren zur Beurteilung und Sicherstellung seiner Zuverlässigkeit beschreiben (Abs. 5). Des Weiteren muss das Sicherheitskonzept eine Übersicht über die eingesetzten Produkte für qualifizierte elektronische Signaturen (Abs. 2) und über die Aufbau- und Ablauforganisation sowie die Zertifizierungstätigkeit (Abs. 3) enthalten.

139 Amtliche Begründung zu § 9 SigV.

140 *Bröhl*/*Tettenborn* 2001, 151.

1.3.5.4 Identifikation und Übergabe der Signaturerstellungseinheit

Eine der wichtigsten Regelungen zur Gewährleistung von Rechtssicherheit in einer Public Key Infrastruktur ist die bezüglich der Identifikation der Teilnehmer. Gelingt einem Betrüger ein qualifiziertes Zertifikat mit gefälschten Identifikationsdokumenten zu erstellen, dann ist es höchstwahrscheinlich, dass dieses Zertifikat Schäden im Geschäftsverkehr verursachen wird. Darum werden nach § 5 Abs. 1 SigG die Zertifizierungsdiensteanbieter verpflichtet, Personen, die ein qualifiziertes Zertifikat beantragen, zuverlässig zu identifizieren. Das Identitätsprüfverfahren wird durch § 3 SigV näher konkretisiert. Hierbei hat der Zertifizierungsdiensteanbieter die Identität des Antragstellers anhand des Personalausweises oder eines Reisepasses zu prüfen. Auszunehmen ist bei erneutem Antrag auf ein Zertifikat der Fall, wenn der Teilnehmer schon über ein qualifiziertes Zertifikat verfügt. Dann ist auf eine erneute Identifizierung zu verzichten.

Bis zum Inkrafttreten des ersten Gesetzes zur Änderung des Signaturgesetzes[141] war die Identifizierung grundsätzlich nur durch einen persönlichen Kontakt möglich. Mit der Novellierung wird aber zugelassen, insbesondere zu Gunsten von Kreditinstituten, dass die von ihnen zu einem früheren Zeitpunkt erhobenen personenbezogene Daten des Antragstellers für die Identitätsprüfung benutzt werden, sofern diese Daten eine zuverlässige Identifikation gewährleisten (§ 5 Abs. 1 Satz 2 SigG).[142] Eine zuverlässige Identifikation ist gegeben, wenn die Daten gemäß § 3 Abs. 1 SigV anhand eines gültigen Ausweises erhoben wurden und noch aktuell sind.[143] Beabsichtigt ist hier die Nutzung der schon seit langem operativen bewährten Verfahrensprozesse wie bei der Registrierung und Ausgabe von EC-, Bankkunden- oder Versichertenkarten, diesmal für die Ausgabe von Signaturkarten mit qualifizierten Zertifikate.[144] Mit der Abschaffung der Notwendigkeit eines persönlichen Kontaktes bei der Identifizierung hat der deutsche Gesetzgeber das Sicherheitsniveau der qualifizierten Verfahren klar reduziert, mit dem Ziel das Verfahren zu vereinfachen und damit einen Beitrag zu der Verbreitung der qualifizierten elektronischen Signaturen zu leisten.

Der vom Zertifizierungsdiensteanbieter bereitgestellte Signaturschlüssel muss zusammen mit den Identifikationsdaten dem Signaturschlüssel-Inhaber auf der sicheren Signaturerstellungseinheit persönlich übergeben werden. Die Übergabe ist gemäß § 5 Abs. 2 SigV schriftlich oder mit einem qualifiziert elektronisch signierten Dokument zu bestätigen, es sei denn, dass eine andere Übergabe vereinbart wird.

141 BGBl. I 2005, 2.

142 Der Satz 2 wurde im § 5 SigG durch das erste Gesetz zur Änderung des Signaturgesetzes hinzugefügt.

143 *Roßnagel*, NJW 2005, 386.

144 BT-Drs. 15/3417, 6.

Mit der bereits erwähnten Novellierung entfällt die Notwendigkeit einer eigenhändigen oder signierten Vereinbarung für die Bestätigung der Übergabe.[145]

1.3.5.5 Unterrichtungspflicht

Der Nutzer ist ein sehr wichtiges Glied der Sicherheitskette der Signaturverfahren. Wenn Signaturschlüssel-Inhaber beispielsweise unsichere technische Komponenten verwenden und dadurch ihre geheimen Schlüssel oder Identifikationsdaten in falsche Hände gelangen lassen, kann die Verlässlichkeit der elektronischen Signaturen verloren gehen.[146] Daher gewinnt die Unterrichtungspflicht an Bedeutung, denn durch sie wird der Versuch unternommen, die hohe Gesamtsicherheit für digitale Signaturverfahren zu garantieren.

Die Unterrichtungspflicht des § 6 SigG setzt die Bestimmung des Anhangs II Buchstabe k) RLeS um. Zentrales Ziel der europäischen Vorschrift ist es, den Signaturschlüssel-Inhaber durch den Zertifizierungsdiensteanbieter über die genauen Bedingungen zur Anwendung des Zertifikats zu informieren. Eine Unterrichtungspflicht war schon im § 6 SigG 1997 vorgesehen.[147] Die im § 6 SigG vorgesehene Unterrichtungspflicht enthält grundsätzlich drei verschiedene Aspekte. Der Zertifizierungsdiensteanbieter muss den Antragsteller über die Maßnahmen zur sicheren Anwendung von qualifizierten elektronischen Signaturen, über die Notwendigkeit einer erneuten Signatur und über die rechtlichen Wirkungen einer Anwendung von Signaturen unterrichten. Regelungsadressat ist somit nicht der Signaturschlüssel-Inhaber, sondern der Zertifizierungsdiensteanbieter, der verpflichtet ist, den Antragssteller über diese drei Themen zu unterrichten.[148] Der Antragssteller wird nicht verpflichtet, die ihm erklärten Maßnahmen zu treffen. Die Sicherungsmaßnahmen sind vielmehr Obliegenheiten, also Verhaltensanforderungen an den Signaturschlüssel-Inhaber, deren Nichteinhaltung Nachteile nach sich ziehen.

Im Folgenden sind die verschiedenen Themen der Unterrichtung sowie ihre Form und Ausgestaltung näher zu betrachten.

145 *Roßnagel*, NJW 2005, 386.

146 *Roßnagel*, RMD, § 6 SigG Rn. 1.

147 § 6 SigG 1997: „Die Zertifizierungsstelle hat die Antragsteller nach § 5 Abs. 1 über die Maßnahmen zu unterrichten, die erforderlich sind, um zu sicheren digitalen Signaturen und deren zuverlässiger Prüfung beizutragen. Sie hat die Antragsteller darüber zu unterrichten, welche technischen Komponenten die Anforderungen nach § 14 Abs. 1 und 2 erfüllen, sowie über die Zuordnung der mit einem privaten Signaturschlüssel erzeugten digitalen Signaturen. Sie hat die Antragssteller darauf hinzuweisen, dass Daten mit digitaler Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird."

148 *Roßnagel*, RMD, § 6 SigG Rn. 3.

1.3.5.5.1 Maßnahmen zur Sicherheit

Der Antragssteller ist nach § 6 Abs. 1 Satz 1 SigG über die geeigneten Maßnahmen, die einen Beitrag zu der Sicherheit von qualifizierten elektronischen Signaturen und ihrer zuverlässigen Prüfung leisten, zu unterrichten. Hierbei handelt es sich um die notwendige Anwendung von sicheren Produkten zur Erzeugung, Darstellung und Prüfung von Signaturen. Da die Verwendung von qualifizierten Anwendungskomponenten keine Wirksamkeitsvoraussetzung für die mittels der Komponente erzeugten Signaturen ist, vergrößert sich die Bedeutung der Unterrichtungspflicht bezüglich des Einsatzes von sicheren Komponenten.[149] Denn obschon die entsprechenden Erzeugungs- und Prüfprogramme in der Regel einfach und benutzerfreundlich sind, sind Bedienfehler immer möglich.[150]

1.3.5.5.2 Erneuerung der Signaturen

Zum anderen müssen Zertifizierungsdiensteanbieter den Antragssteller gemäß § 6 Abs. 1 Satz 2 SigG unterrichten, dass nach Bedarf seine bereits signierten Dokumente erneut zu signieren sind. Eine erneute Signatur wird insbesondere erforderlich für Dokumente, die langfristig beweiskräftig zu archivieren sind. Wie lange ein Dokument aufzubewahren ist, hängt von den spezifischen Zielen und Anforderungen im betreffenden Fall ab. Im deutschen Zivilrecht gilt eine Verjährungsfrist von 30 Jahren. Dies macht die Aufbewahrung von Unterlagen, die einen Anspruch begründen können mindestens für diesen Zeitraum erforderlich. In der Verwaltung sind unterschiedliche Aufbewahrungsanforderungen und -zwecke zu beachten, eine Aufbewahrung von mehr als 30 Jahren wird nur in Ausnahmefällen notwendig.[151]

Grund für die Erneuerung ist, dass im Gegensatz zu handschriftlich unterschriebenen Papierdokumenten, elektronisch signierte Dokumente mit der Zeit an Beweiswert verlieren.[152] Entscheidend dafür ist, dass die verwendeten kryptografischen Verfahren aufgrund wissenschaftlicher Erkenntnisse in der Mathematik oder technischer Forstschritte bei der Leistungsfähigkeit von Rechnern an Sicherheitswert verlieren.[153]

Die Neusignierung funktioniert als reines Sicherungsmittel für bereits existierende Signaturen.[154] Somit dient sie nicht der Abgabe einer Willens- oder Wissenserklärung oder der Bestätigung des ursprünglichen Inhalts des elektronischen Doku-

149 *Fischer-Dieskau*/*Steidle*, MMR 2006, 68.

150 *Skrobotz*, in: Manssen, Bd. 2, § 6 SigG Rn. 2.

151 *Fischer-Dieskau* 2006, 40; *Roßnagel*/*Fischer-Dieskau*/*Jandt*/*Knopp* 2007, 89; *Fischer-Dieskau*/*Roßnagel*/*Pordesch*, in: Roßnagel/Schmücker 2006, 26.

152 *Brandner*/*Pordesch*/*Roßnagel*/*Schachermayer*, DuD 2002, 97.

153 Amtliche Begründung zu § 17 SigV. Näher hierzu auch *Fischer-Dieskau* 2006, 163.

154 *Roßnagel*/*Fischer-Dieskau*/*Pordesch*/*Brandner*, CR 2003, 303.

mentes. Dies hat zur Folge, dass es unerheblich ist, wer die erneute Signatur anbringt. In Frage käme ein Archivar oder sogar ein dritter Dienstleister.[155]

§ 17 Satz 2 SigV regelt das Verfahren zur erneuten Signatur. Gemäß der Vorschrift sind die Daten vor Ablauf der Eignung von Algorithmen und zugehöriger Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Hierbei muss nicht jedes Dokument neu elektronisch signiert werden, sondern es besteht die Möglichkeit, viele Dokumente zugleich mit einer Signatur erneut zu signieren.[156]

Darüber hinaus sieht Satz 3 vor, dass die erneute Signatur mit geeigneten neuen Algorithmen oder zugehörigen Parametern zu erfolgen hat[157], frühere Signaturen einschließt und einen qualifizierten Zeitstempel trägt. Das Verfahren der erneuten Signatur basiert auf dem Prinzip der Verschachtelung, wonach die bestehenden Signaturen durch die neue geschützt werden. Die Prüfung erfolgt zunächst bei der neuen Signatur und dann bei den alten, im Kern platzierten Signaturen.[158] Der Zeitstempel dient zum einen dem Nachweis, dass die Neusignierung tatsächlich vor Ablauf der Sicherheitseignung der verwendeten Algorithmen und zugehörigen Parametern durchgeführt worden ist. Zum anderen verhindert er, dass neue qualifizierte Signaturen zu einem späteren Zeitpunkt durch eine Rückdatierung der Systemzeit des Rechners angebracht werden.[159]

Als Vorteil bringt das Verfahren der Neusignierung zudem die Erhöhung des Beweiswerts im Vergleich zum ursprünglich signierten Dokument.[160] Ohne eine solche Sicherheitsmaßnahme ist es möglich, Signaturen des Dokuments spurlos zu entfernen. Da die erneute Signatur die „alten" Signaturen des Dokuments umschließt, wird die Integrität des „Signaturpakets" abgesichert und ein nachträgliches Löschen einzelner Signaturen erkennbar.

Ein praktisches Beispiel der Anwendung dieses Verfahrens ist im Jahr 2007 erfolgt. Die Bundesnetzagentur hat Umstellungsarbeiten im Rahmen ihrer Wurzelaktivitäten zur Verwendung größerer Schlüssellängen und neuer Hash-Algorithmen durchgeführt. Dadurch ist die Bundesnetzagentur seitdem in der Lage, Zertifikate der akkreditierten Zertifizierungsdiensteanbieter mit einer Schlüssellänge von 2048 Bit RSA zur Verfügung zu stellen. Dabei hat die Bundesnetzagentur, entsprechend den Bestimmungen des § 17 SigV, die von ihr mit „alten" Algorithmen und Parametern ausgestellten Zertifikate, neu signiert.[161]

155 *Fischer-Dieskau* 2006, 179.

156 *Brandner*/*Pordesch*/*Roßnagel*/*Schachermayer*, DuD 2002, 98; *Fischer-Dieskau*/*Roßnagel*/*Pordesch*, in: Roßnagel/Schmücker 2006, 28.

157 Laut § 17 SigG sowie Anlage 1 Abschnitt I Nr. 2 zur SigV wird eine Übersicht der sicherheitsgeeigneten Algorithmen und zugehörigen Parameter sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt von der Bundesnetzagentur im Bundesanzeiger veröffentlicht.

158 *Fischer-Dieskau* 2006, 180.

159 Amtliche Begründung zu § 17 SigV; *Fischer-Dieskau* 2006, 180.

160 *Roßnagel*/*Fischer-Dieskau*/*Jandt*/*Knopp* 2007, 64.

161 S. www.bundesnetzagentur.de → elektronische Signatur.

1.3.5.5.3 Rechtswirkung

Schließlich muss der Zertifizierungsdiensteanbieter den Antragsteller darüber unterrichten, dass in der Regel eine qualifizierte elektronische Signatur im Rechtsverkehr die gleiche Wirkung hat, wie eine handschriftliche Unterschrift (§ 6 Abs. 2 SigG). Die Vorschrift liegt in Verbindung mit §§ 126 Abs. 3 und 126a Abs. 1 BGB, die grundsätzlich die elektronische Form und die Gleichstellung zwischen der qualifizierten elektronischen Signatur und der eigenhändigen Unterschrift begründet. Die Gleichstellung wird im öffentlichen Recht bestätigt, indem § 3 a Abs. 2 VwVfG bestimmt, dass eine durch Rechtsvorschrift angeordnete Schriftform durch die elektronische Form ersetzt werden kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt wird. § 87a Abs. 3 und 4 AO regeln zudem die Möglichkeit, die Schriftform durch die elektronische Form für Anträge, Erklärungen oder Mitteilungen an die Finanzbehörden sowie für Verwaltungsakte oder sonstige Maßnahmen zu ersetzen. Auch § 36a Abs. 2 SGBI ermöglicht eine durch Rechtsvorschrift angeordnete Schriftform durch die elektronische Form zu ersetzen. Ferner bestimmt § 371a Abs. 1 Satz 2 ZPO den Anschein der Echtheit für die privaten elektronischen Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind.[162]

Alle diese Regelungen können für fachlich versierte Personen selbstverständlich sein, aber für die Mehrheit der Anwender ist dagegen die rechtliche Wirkung von qualifizierten Signaturen schwer nachzuvollziehen. Dabei können sich viele Laien noch denken, dass die Rechtsverbindlichkeit einer Willenserklärung nur durch die eigenhändige Unterschrift zustande kommt. Besonders in den Fällen, in denen diese nicht nur die Wirkung der Formwahrung hat, sondern auch bereits ein Teil der Erklärungshandlung ist.[163] Dabei ist ebenso zu beachten, dass sich die deutsche Rechtsordnung und somit die deutsche Rechtskultur immer noch weit überwiegend auf das Medium Papier stützt. [164] Daneben ist die Tradition und Wertschätzung der eigenhändigen Unterschrift und ihrer Rechtsverbindlichkeit als prägendes Merkmal der modernen Gesellschaft über Jahrhunderte etabliert worden. Da jedoch die deutsche Rechtsordnung grundsätzlich für die Gleichstellung einer elektronischen Signatur mit der eigenhändigen Unterschrift sorgt, zeigt sich die immense Bedeutung der Unterrichtungspflicht über die Rechtswirkung. Des Weiteren verfolgt diese Unterrichtungspflicht, die mit der Schriftform bezweckte Warnfunktion[165] auf den elektronischen Rechtsverkehr zu übertragen.[166]

162 S. hierzu 3. Teil 1.6.4.

163 *Skrobotz*, in: Manssen, Bd. 2, § 6 SigG Rn. 44.

164 *Roßnagel* 1995, 268.

165 Über die Erfüllung der Funktionen der eigenhändigen Unterschrift durch die elektronische Signatur, siehe 3. Teil 1.6.4.1.1.

166 BT-Drs. 14/4662, 22.

Auch über die Risiken des Missbrauchs der Signaturkarte ist der Antragsteller zu unterrichten.[167] Hierbei handelt es sich beispielsweise um die Möglichkeit, dass die Signaturkarte dem Signaturschlüssel-Inhaber abhanden kommt und ein Dritter Signaturen in seinem Namen erstellt. Eine andere Missbrauchsmöglichkeit besteht darin, dass der Signaturschlüssel-Inhaber einem Dritten für eine bestimmte Handlung seine Signaturkarte zur Verfügung stellt und er die vereinbarten Grenzen des Geschäfts überschreitet.[168] Zwar kann es dem Signaturschlüssel-Inhaber gelingen, den Anschein der Echtheit des § 371a ZPO zu erschüttern, seine Haftung kann jedoch aufgrund des Missbrauchs der Signaturkarte immer noch zustande kommen.[169]

Aus diesen Gründen entsteht die besondere Bedeutung dieser Vorschrift darin, dass sie bezweckt, nicht nur über die technischen Aspekte, sondern auch über die rechtlichen Folgen der qualifizierten elektronischen Signaturen aufzuklären.

1.3.5.5.4 Form der Unterrichtung

Nach § 6 Abs. 3 SigG ist die Unterrichtung[170] dem Antragsteller in Textform zu übermitteln. Die Einführung der Textform durch das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr erzielte eine Erleichterung des Rechtsverkehrs durch den Verzicht auf die eigenhändige Unterschrift für Formtatbestände, bei denen keiner der Beteiligten und kein Dritter ein ernsthaftes Interesse an einer Fälschung der Erklärung haben kann.[171] Die Textform wiederum wurde durch das erste Gesetz zur Änderung des Signaturgesetzes (Art. 1 Abs. 4 Buchstabe a) als Form der Unterrichtung in das Signaturgesetz eingeführt. Dabei wurde die Notwendigkeit der Aushändigung einer schriftlichen Belehrung abgeschafft. Die Änderung wurde vom Gesetzgeber damit gerechtfertigt, dass weder in der Signaturrichtlinie noch in den Signaturgesetzen der anderen europäischen Mitgliedstaaten eine solche Anforderung vorgesehen ist.[172] Um die vorgesehene Textform zu erfüllen, reicht eine einfache E-Mail.[173]

167 *Skrobotz*, in: Manssen, Bd. 2, § 6 SigG Rn. 53.

168 *Skrobotz*, in: Manssen, Bd. 2, § 6 SigG Rn. 50.

169 *Schemmann*, ZZP 118 (2005), 174.

170 Gemäß § 126b BGB wird die Textform „durch Gesetz vorgeschrieben, so muss die Erklärung in einer Urkunde oder auf andere zur dauerhaften Wiedergabe in Schriftzeichen geeignete Weise abgegeben, die Person des Erklärenden genannt und der Abschluss der Erklärung durch Nachbildung der Namensunterschrift oder anders erkennbar gemacht werden".

171 BT-Drs. 14/4987,18.

172 BT-Drs. 15/3417, 8.

173 *Borges* 2003, 606.

Wie bei der Identifikation des zukünftigen Signaturschlüssel-Inhabers wird auch bei der Unterrichtung auf eine persönliche Mitwirkung verzichtet, was angesichts der Bedeutung der Unterrichtungspflicht zu bedauern ist.

1.3.5.5.5 Ausgestaltung der Unterrichtung

Konkretisiert wird die Unterrichtungspflicht noch durch § 6 SigV, der die Mindestanforderungen an die Unterrichtung festlegt. Zusätzlich zu den bereits schon erwähnten Maßnahmen zur Sicherheit, zur erneuten Signatur und zu den Rechtswirkungen, hat der Zertifizierungsdiensteanbieter den Antragsteller über andere Themen zu unterrichten. Nr. 4 behandelt die Unterrichtung über die Möglichkeit von Beschränkungen in qualifizierten Zertifikaten nach § 7 Abs. 1 Nr. 7 SigG einzutragen. Nr. 6 macht erforderlich, dass der Antragsteller über die Existenz eines freiwilligen Akkreditierungssystems informiert wird. Darüber hinaus muss der Zertifizierungsdiensteanbieter den Antragssteller über die zur Verfügung stehenden Beschwerde- und Schlichtungsmöglichkeiten, sowie über die Einzelheiten der Inanspruchnahme solcher Verfahren (Nr. 7) und über das Verfahren der Sperrung von Zertifikaten (Nr. 8) unterrichten. Dies hat gemäß § 6 SigV nach der Antragsstellung und vor der Zertifikaterteilung in einer allgemein verständlichen Sprache zu erfolgen.[174]

1.3.5.6 Sperrung von qualifizierten Zertifikaten

Von Bedeutung für die gesamte Sicherheit einer Public Key Infrastruktur ist die Bereitstellung eines Widerrufssystems, damit dem Signaturschlüssel-Inhaber die Möglichkeit angeboten wird, wenn nötig und angesichts mancher Ereignisse, wie Verlust oder Diebstahl der Signaturerstellungseinheit, die Sperrung seines Zertifikats vor dem Ablauf des Gültigkeitszeitraums anzuordnen. Damit wird die Zuordnung eines öffentlichen Schlüssels zu einer Person beendet und ab dem Zeitpunkt der Bekanntmachung der Sperrung in einem Sperrverzeichnis, können nachträgliche digitale Signaturen dem Signaturschlüssel-Inhaber nicht mehr zugerechnet werden.[175] Die Sperrung bezieht sich nicht auf den privaten Schlüssel, sondern auf die Bestätigungsaussage des Zertifizierungsdiensteanbieters über die Gültigkeit des Zertifikats, wodurch der Schlüssel weiterhin genutzt werden kann.[176]

Die Sperrung von qualifizierten Zertifikaten wird in § 8 SigG geregelt. Konkretisiert wird diese Norm durch § 7 SigV.

174 *Roßnagel*, RMD, § 6 SigG Rn. 20.

175 *Roßnagel*, RMD, § 8 SigG Rn. 1.

176 *Fox*, DuD 2001, 485.

1.3.5.6.1 Verpflichtung zur Sperrung und Sperrungsgründe

Nach § 8 Abs. 1 SigG hat der Zertifizierungsdiensteanbieter ein qualifiziertes Zertifikat zu sperren, wenn ein Signaturschlüssel-Inhaber oder sein Vertreter dies verlangt. Daraus ergibt sich die Pflicht zu einer Dienstleistung. Die Durchführung der Sperrung liegt somit nicht im freien Ermessen des Zertifizierungsdiensteanbieters, vielmehr gewährleistet die Regelung dem Zertifikatsinhaber einen Anspruch auf die Sperrung nach der entsprechenden Beantragung.[177] Der Signaturschlüssel-Inhaber kann somit jederzeit und ohne weitere Begründungen die Sperrung seines Zertifikates verlangen. Ein betroffener Dritter kann auch Interesse an der Sperrung haben. Das gilt insbesondere, wenn ein Zertifikat nach § 5 Abs. 2 SigG Angaben über eine Vertretungsmacht für eine dritte Person, sowie berufsbezogen oder sonstige Angaben zur Person enthält. In diesem Fall kann gemäß § 8 Abs. 2 SigG auch die dritte Person oder die für die berufsbezogenen oder sonstigen Angaben zur Person zuständige Stelle die Sperrung des Zertifikates verlangen. Typisch hierfür ist das Beispiel einer Berufsorganisation wie einer Rechtsanwalts- oder Steuerberatungskammer sowie der Arbeitgeber, der angesichts neuer Umstände das Zertifikat außer Kraft setzen muss. [178]

Als Sperrungsgrund sieht das Gesetz ferner den Fall vor, dass ein Zertifikat auf Grund falscher Angaben zu § 7 ausgestellt wird. Angaben sind als falsch zu betrachten, wenn sie nicht der Wahrheit entsprechen oder wenn sie rechtswidrig sind, z.B. bei einem Verstoß gegen das Namensrecht.[179] Hierbei handelt es sich um Daten, die vom Antragsteller angegeben werden, wie zum Beispiel Angaben zum Namen, zu Pseudonymen, zu Attributen und über die Vertretungsmacht für eine dritte Person. Gemäß § 8 Abs. 1 Satz 1 SigG ist ein weiterer Sperrungsgrund die Einstellung der Tätigkeiten eines Zertifizierungsdiensteanbieters, falls diese nicht von einem anderen Zertifizierungsdiensteanbieter übernommen werden. Laut § 19 Abs. 4 SigG kann auch die Bundesnetzagentur eine Sperrung von qualifizierten Zertifikaten anordnen, wenn Tatsachen rechtfertigen, dass qualifizierte Zertifikate gefälscht[180] oder nicht hinreichend fälschungssicher sind oder wenn sichere Signaturerstellungseinheiten Sicherheitsmängel aufweisen, die unbemerkte Fälschungen qualifizierter elektronischer Signaturen oder unbemerkte Verfälschungen der mit ihnen signierten Daten zulassen.

177 *Roßnagel*, RMD, § 8 SigG Rn. 47.

178 In der Tat, diese Möglichkeit der Sperrung durch Dritte greift die im Rahmen der Evaluierung des SigG 1997 von den Berufskammern geäußerte Vorschläge auf. BT-Drs. 14/4662, 23.

179 *Roßnagel*, RMD, § 8 SigG Rn. 54.

180 Falsche Zertifikate sind beispielsweise solche, die falsche Angaben enthalten, qualifiziert zu sein, obwohl ihr Aussteller kein Zertifizierungsdiensteanbieter im Sinne des Gesetzes ist. *Skrobotz*, in: Manssen, Bd. 2, § 8 SigG Rn. 27.

Auch sind vertragliche Vereinbarungen von weiteren Sperrungsgründen möglich. Dies wurde in § 8 Abs. 1 SigG durch das erste Gesetz zur Änderung des SigG hinzugefügt.

1.3.5.6.2 Sperrverfahren

Auslöser für das Sperrverfahren ist entweder der Antrag des Zertifikatsinhabers, des betroffenen Dritten oder eine Anordnung der zuständigen Behörde. Um dies zu ermöglichen muss der Zertifizierungsdiensteanbieter einen Sperrdienst bereitstellen. § 7 Abs. 1 SigV fordert, dass der Zertifizierungsdiensteanbieter eine Telefonverbindung für diesen Zweck bekannt gibt. Zusätzliche Kommunikationsmöglichkeiten wie Fax, E-Mail oder Brief sind nicht ausgeschlossen, besonders für die Fälle, bei denen keine Eile besteht, wie beispielsweise bei einem erwünschten Ausstieg aus dem elektronischen Geschäftsverkehr durch den Zertifikatsinhaber.[181] Um aber effektiv zu sein, muss der Sperrdienst jederzeit erreichbar sein, Tag und Nacht und auch am Wochenende offen stehen.[182] Vor der Sperrung muss der Zertifizierungsdiensteanbieter sich von der Identität der zur Sperrung Berechtigten überzeugen (§ 7 Abs. 2 SigV). Geeignet ist hierfür ein speziell für diesen Zweck verabredetes Passwort, welches bei der Übergabe der Signaturerstellungseinheit erteilt werden kann.

Der Zertifizierungsdiensteanbieter ist dann verpflichtet, das Zertifikat laut § 8 Abs. 1 SigG „unverzüglich" zu sperren. Weder das Gesetz noch die Verordnung bestimmen konkret eine maximale Reaktionszeit für den Zertifizierungsdiensteanbieter. Nach dem Maßnahmenkatalog des deutschen BSI darf die Reaktionszeit bis zum Wirksamwerden des Sperreintrags zehn Minuten nicht überschreiten.[183] Die Maßnahmenkataloge des BSI, die im Rahmen des SiG 1997 zwingend beachtet werden mussten, haben aber für das Signaturgesetz lediglich einen empfehlenden Charakter.[184] Obwohl keine Norm eine bestimmte maximale Reaktionszeit für die Sperrung festlegt, ist das Wort „unverzüglich" als „schnellstmöglich" zu verstehen, so dass unverhältnismäßige Verzögerungen vermieden werden müssen.

Zur Sicherheit des elektronischen Geschäftsverkehrs muss die Sperrungsverfügung den Zeitpunkt enthalten, ab dem sie gilt, ohne dass die Möglichkeit besteht, dies rückwirkend festzulegen (§ 8 Abs. 1 Sätze 3 und 4 SigG). Sperrungen gelten somit nur für die Zukunft. Die Sperre erfolgt dann mit ihrer Eintragung im Zertifikatsverzeichnis mit Angabe von Datum und Sperrzeit mit dem Vermerk „gesperrt". Wichtig in diesem Zusammenhang ist, dass nach dem deutschen Signaturrecht Sperrlisten zur Eintragung der Zertifikatssperrungen nicht ausreichen. Das ergibt sich aus der Auslegung von § 5 Abs. 2 SigV i. V. m. § 5 Abs. 1 Satz 3 SigG. Nach

181 *Skrobotz*, in: Manssen, Bd. 2, § 8 SigG Rn. 46.

182 *Skrobotz*, in: Manssen, Bd. 2, § 8 SigG Rn. 44.

183 BSI-SigI-B4.

184 BSI-GeS, 6.

diesen Vorschriften darf ein Zertifikat von Zertifizierungsdiensteanbietern erst dann in ein Zertifikatsverzeichnis aufgenommen werden, wenn der Signaturschlüssel-Inhaber den Erhalt der sicheren Signaturerstellungseinheit gegenüber dem Zertifizierungsdiensteanbieter bestätigt hat. Da Sperrlisten nur gesperrte Zertifikate (negativ) aufführen, enthalten sie keine Aussage über die Gültigkeit oder sogar über die Existenz eines Zertifikats. Eine Evidenzprüfung ermöglichen sie darum grundsätzlich nicht.[185] Folglich werden die signaturrechtlichen Anforderungen zur Führung eines Zertifikatsverzeichnisses nur durch positive Listen, derzeit technisch einzig über eine OCSP-Abfrage[186] erhältlich, erfüllt.[187]

1.3.5.7 Sichere Produkte

In der Vertrauenskette einer Public Key Infrastruktur spielt die technische Sicherheit eine wesentliche Rolle. Zertifizierungsdiensteanbieter müssen gemäß § 5 Abs. 5 SigG zuverlässige Produkte für qualifizierte elektronische Signaturen einsetzen, welche mindestens die Anforderungen nach den §§ 4 bis 14 sowie § 17 oder § 23 des Signaturgesetzes erfüllen. Ausschlaggebend ist die bereits erwähnte Notwendigkeit des Einsatzes sicherer Signaturerstellungseinheiten[188] sowie ergänzend der Signaturanwendungskomponenten, welche für die Darstellung zu signierender Daten notwendig sind. Sie müssen die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht.

1.3.5.8 Haftung

Haftungsregelungen können verschiedene Aufgaben haben. Vor allem besitzen sie normalerweise eine Steuerungsfunktion. Sie werden im Zivilrecht, im Umweltrecht, im Verbraucherschutzrecht und in vielen anderen Sondergesetzen festgelegt. Eine grundlegende Zielsetzung von Haftungstatbeständen ist ihre Ausgleichs- und Kompensationsfunktion. Hierbei soll der Verletzer dem Geschädigten dessen Schaden ausgleichen. Dabei soll der Geschädigte so gestellt werden, wie er stünde, wenn das schädigende Ereignis nicht eingetreten wäre. Eine weitere Funktion der Haftungsregelungen ist die präventive Wirkung. Hierzu soll die Haftungsandrohung künftige

185 S. hierzu *Tielemann*/*Fischer-Dieskau*/*Pordesch*/*Brandner*/*Barzin*, in: Roßnagel/Schmücker 2006, 99.

186 S. hierzu in diesem Teil 2.2.9.1.4.1.

187 S. hierzu *Tielemann*/*Fischer-Dieskau*/*Pordesch*/*Brandner*/*Barzin*, in: Roßnagel/Schmücker 2006, 99.

188 S. Hierzu bereits in diesem Teil Gliederungspunk 1.3.3.3.2.

Eingriffe und Schäden vermeiden. Der erwartete Effekt ist, dass der potentielle Schadensverursacher sich sorgfältiger und schadensvermeidender verhält.

Haftungsregelungen können auch eine bedeutende Rolle in einer Sicherungsinfrastruktur wie einer PKI spielen. Ihre Einführung in das Signaturrecht mag dabei helfen, den Verbraucherschutz, das Vertrauen sowie die Akzeptanz von Signaturverfahren zu stärken.[189]

1.3.5.8.1 Haftung im Signaturgesetz

§ 11 SigG setzt die Haftungsregelung des Artikels 6 RLeS um, nach welchem die Mitgliedstaaten gewährleisten müssen, dass die Zertifizierungsdiensteanbieter, in Bezug auf Schäden gegenüber einer Stelle, einer juristischen oder natürlichen Person, die vernünftigerweise auf das Zertifikat vertraut, dafür haftet. Die Regelung berücksichtigt auch den Regierungsbericht zum Informations- und Kommunikationsdienst-Gesetz (IuKDG), der auf die Notwendigkeit einer spezifischen Haftungsregelung für die Zertifizierungsdiensteanbieter hingewiesen hat.[190] Anders als die Richtlinie, die lediglich eine Mindestregelung vorsieht[191], legt das Signaturgesetz eine umfassende Haftung fest. Nach § 11 Abs. 1 Satz 1 SigG, muss der Zertifizierungsdiensteanbieter die von Dritten erlittenen Schäden ersetzen, wenn er die Anforderungen des Signaturgesetzes oder der Signaturverordnung verletzt hat oder wenn seine Produkte für qualifizierte elektronische Signaturen oder sonstige technische Sicherungseinrichtungen versagen. Gemäß § 11 Abs. 4SigG haftet der Zertifizierungsdiensteanbieter auch für die Handlungen beauftragter Dritte oder beim Ausstellen ausländischer Zertifikate nach § 23 Abs. 1 Nr. 2 SigG.[192]

Was die dogmatische Einordnung der Vorschrift betrifft, handelt es sich um eine deliktische Haftungsnorm. Ersatzberechtigte sind ausschließlich Dritte, die keine vertragliche Beziehung zur Zertifizierungsstelle haben. Sie müssen aber nicht unbe-

189 *Thomale* 2003, 87.

190 BT-Drs. 14/1191, 33.

191 Gemäß der Mindestregelung des Art. 6 RLeS haftet der Zertifizierungsdiensteanbieter dafür, dass die Informationen eines qualifizierten Zertifikates zum Zeitpunkt seiner Ausstellung korrekt sind, und dass dieses alle vorgeschriebenen Angaben enthält (Buchstabe a)), der im qualifizierten Zertifikat angegebene Person zum Zeitpunkt der Ausstellung des Zertifikats im Besitz der Signaturerstellungsdaten (private Schlüssel) war (Buchstabe b)), und dass in Fällen bei denen der Zertifizierungsdiensteanbieter sowohl den privaten sowie den öffentlichen Schlüssel erzeugt, diese in komplementärer Weise genutzt werden können (Buchstabe c)).

192 Laut § 23 Abs. 1 Nr. 2 sind elektronische Signaturen aus Drittstaaten qualifizierten elektronischen Signaturen gleichgestellt, wenn das Zertifikat aus dem Drittland als qualifiziertes Zertifikat ausgestellt und für eine elektronische elektronische Signatur bestimmt ist und wenn ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter für das Zertifikat einsteht.

dingt Empfänger einer elektronischen Signatur sein.[193] Es reicht aus, wenn Dritte auf die elektronische Signatur oder auf das darauf basierende Zertifikat vertraut haben und einen Schaden erleiden, um einen Anspruch auf Schadenersatz aufgrund der Haftungsregelung geltend zu machen.

Der Signaturschlüssel-Inhaber seinerseits schließt mit dem Zertifizierungsdiensteanbieter einen Vertrag, aufgrund dessen der Letztere haftet. Die Haftung richtet sich nach § 280 Abs. 1 Satz 1 BGB, wonach der Gläubige den Ersatz des entstehenden Schadens verlangen kann, wenn der Schuldner eine Pflicht aus dem Schuldverhältnis verletzt. Die Haupt- und Nebenpflichten des Zertifizierungsdiensteanbieters sind durch seine Pflichtdienstleistungen im Signaturgesetz normiert. Wichtig dabei ist, dass der Zertifizierungsdiensteanbieter seine Haftung nicht durch allgemeine Geschäftsbedingungen ausschließen darf.[194] Das würde gegen § 305 b BGB verstoßen, der verhindern soll, dass Rechte, die sich aus zugesicherten Eigenschaften ergeben, durch formularmäßige Freizeichnungen beschränkt werden.[195] Ein solcher Haftungsausschluss würde ebenfalls § 307 Abs. 2 Nr. 2 BGB verletzen. Dieser charakterisiert eine unangemessene Benachteiligung, die wesentliche Rechte oder Pflichten, die sich aus der Natur des Vertrags ergeben, so einschränkt, dass die Erreichung des Vertragszwecks gefährdet ist.[196]

Bei dem Tatbestand des § 11 SigG handelt es sich um eine Verschuldenshaftung mit Beweislastumkehr.[197] Das ergibt sich aus § 11 Abs. 2, wonach die Ersatzpflicht nicht eintritt, wenn der Zertifizierungsdiensteanbieter nicht schuldhaft gehandelt hat. Es obliegt somit dem Zertifizierungsdiensteanbieter nachzuweisen, dass er die Anforderungen nach dem SigG und SigV eingehalten hat. Hierbei zeigt sich die besondere Bedeutung einer ordentlichen Führung der Dokumentation seitens des Zertifizierungsdiensteanbieters nach § 10 SigG.[198] Es ist für den Zertifizierungsdiensteanbieter also vorteilhaft, sein höchstmögliches Sorgfaltsniveau bei der Dokumentation immer beizubehalten, um Schadenersatzansprüche zu vermeiden.

Der Zertifizierungsdiensteanbieter haftet auch nicht, wenn der geschädigte Dritte die Fehlerhaftigkeit der Angabe des Zertifikats kannte oder kennen musste (§ 11 Abs. 1 Satz 2 SigG). Art und Umfang des Schadenersatzes werden nach den §§ 249 ff. BGB[199] bestimmt.[200] Das Mitverschulden des Dritten wird nicht ausgeschlossen.

193 *Thomale* 2003, 131.

194 *Thomale* 2003, 72.

195 *Thomale* 2003, 72.

196 *Thomale* 2003, 73.

197 BT-Drs. 14/4662, 25.

198 *Roßnagel* 2000,455.

199 Diese Vorschriften des BGB determinieren grundsätzlich, dass wer zum Schadenersatz verpflichtet ist, entweder den ursprünglichen Zustand herzustellen hat (§ 249 Abs. 1) oder statt der Herstellung den dazu erforderlichen Geldbetrag zu entschädigen hat (§ 250). Ferner bestimmt das BGB, dass der zu ersetzende Schaden auch den entgangenen Gewinn umfasst (§

§ 254 BGB findet Anwendung. Bestand bei der Entstehung des Schadens ein Mitverschulden des Geschädigten, so hängt nach § 254 Abs. 1 BGB die Verpflichtung zum Ersatz sowie der Umfang des zu leistenden Ersatzes insbesondere davon ab, inwieweit der Schaden vorwiegend von dem einen oder dem anderen Teil verursacht worden ist. Abs. 2 des § 254 BGB sieht die Möglichkeit des Verschuldens des Geschädigten auch vor, wenn er den Schaden hätte abwenden oder mindern können. Zudem wird die Möglichkeit des Eintretens eines Mitverschuldens in den Fällen angedeutet, in welchen der Dritte durch das Nachprüfen des Zertifikats die Schäden verringern oder vermeiden kann.[201] Das Überprüfen eines Zertifikats stellt aus rechtlicher Sicht meistens eine Obliegenheit dar.[202] Bei der Beurteilung des Mitverschuldens des Drittens, der auf ein Zertifikat vertraut, soll vom Gericht auch Wert darauf gelegt werden, ob dieser gleichzeitig Signaturschlüsselinhaber ist oder ob er sich lediglich als „einfacher" Teilnehmer des elektronischen Geschäftsverkehrs präsentiert. Besitzt der Dritte ein qualifiziertes Zertifikat, ist davon auszugehen, dass er vom Zertifizierungsdiensteanbieter gemäß § 6 SigV unterrichtet worden ist.[203] Inhalt der Unterrichtung sind auch die Sicherheitsmaßnahmen seitens des Signaturschlüsselinhabers in seiner Funktion als Empfänger elektronischer Signaturen. Dabei sind besonders die Maßnahmen bei der Prüfung einer qualifizierten Signatur wichtig, wobei nur geeignete technische Komponenten einzusetzen sind. Es ist somit ein Prüfprogramm anzuwenden, welches sicherstellt, dass der Signaturschlüsselinhaber alle relevanten Informationen bekommt, um die Signatur bewerten zu können.[204] Obwohl das Einsetzen geeigneter Prüfprogramme, genau wie das Überprüfen von Signaturen, eine Obliegenheit darstellt, besteht die Möglichkeit eines späteren Vorwurfs der Fahrlässigkeit gegenüber dem Signaturschlüsselinhaber, der auf die Angaben eines Zertifikates vertraute.[205]

252), und dass wegen eines Schadens, der nicht Vermögensschaden ist, Entschädigung in Geld nur in den durch das Gesetz bestimmten Fällen gefordert werden kann (§ 253).

200 BT-Drs. 14/4662, 25.

201 BT-Drs. 14/4662, 25.

202 Obliegenheiten begründen weder einen Erfüllungsanspruch noch bei ihrer Verletzung eine Schadensersatzforderung. Ihre Befolgung ist vielmehr ein Gebot des eigenen Interesses, da derjenige, dem sie obliegt bei ihrer Verletzung einen Rechtsverlust oder rechtlichen Nachteil erleidet (wie beim Mitverschulden). Das Verschulden ist also ein Verschulden gegen sich selbst. Sie ist verletzt, wenn die Partei in zurechenbarer Weise gegen ihr eigenes Interesse handelt.Tielemann/Fischer-Dieskau/Pordesch/Brandner/Barzin, in: Roßnagel/Schmüker 2005, 99. Das UNCITRAL Model Law für elektronische Signaturen bewertet das Verhalten des Dritten (die so genannte „relying party"), der auf ein Zertifikat vertraut, auch als eine Obliegenheit, indem es im Art. 11 bestimmt, dass der Dritte die rechtlichen Konsequenzen für das Scheitern der Prüfung eines Zertifikats ertragen muss.

203 Zu der Unterrichtung, siehe in diesem Teil Gliederungspunkt 1.3.5.5.

204 *Thomale* 2003, 190.

205 *Thomale* 2003, 191.

1.3.5.8.2 Die Rolle der Zertifikatsbeschränkung

Nach § 7 Abs. 1 Nr. 7 SigG kann ein qualifiziertes Zertifikat Angaben darüber enthalten, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen, nach Art oder Umfang beschränkt sein soll. Die Zielrichtungen der Beschränkungen sind verschieden. Zunächst eröffnet sie dem Teilnehmer, der kein oder lediglich ein eingeschränktes Vertrauen in die Sicherheit der Signaturverfahren hat, die Möglichkeit einer Risikobegrenzung.[206] Im Fall des Abhandenkommens von Chipkarte und PIN oder Missbrauch eines beauftragten Dritten sollen die Risiken von Schäden reduziert werden. Zudem kann es von Interesse für die Arbeitgeber sein, eine Limitierung auf die Nutzung des Zertifikats nur für den dienstlichen Bereich des Arbeitnehmers einzutragen.[207] Darüber hinaus kann sich jemand die Beschränkung auch als Übereilungsschutz zu Nutze machen.

In Bezug auf das Thema Haftung kann die Beschränkung der Nutzung des Zertifikats eine wichtige Rolle spielen. Eine der wichtigsten Ziele der Beschränkung, aus der Perspektive der Zertifizierungsdiensteanbieter, ist in diesem Zusammenhang die Möglichkeit der Haftungslimitierung. Wird ein qualifiziertes Zertifikat auf bestimmte Anwendungen nach Art oder Umfang beschränkt, so tritt die Ersatzpflicht laut § 11 Abs. 3 SigG nur im Rahmen dieser Beschränkungen ein. Das Interesse an der Eintragung ist somit für den Zertifizierungsdiensteanbieter als Mittel der Risikokalkulation von besonderer Bedeutung.[208] Obwohl nicht im Gesetz vorgesehen, muss die Beschränkung aber deutlich und erkennbar sein.[209] Vertraut ein Dritter auf die Unbeschränktheit eines Zertifikats, das aber eine undeutliche Limitierung enthält, dann tritt die Haftung des Zertifizierungsdiensteanbieters ein.[210]

1.3.5.9 Qualifizierte Zeitstempel

Das Signaturgesetz definiert qualifizierte Zeitstempel als elektronische Bescheinigungen eines Zertifizierungsdiensteanbieters, der die im Signaturgesetz und Signaturverordnung vorgesehenen Anforderungen erfüllt, darüber, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Zeitstempeln kommt eine erhebliche Funktion bei Situationen zu, in denen der genaue Zeitpunkt einer Willenserklärung nachgewiesen werden muss.[211] Denn sie verhindern ein Vor-

206 BR-Drs. 966/96.

207 *Fischer-Dieskau*/*Gitter*/*Hornung*, MMR 2003, 384.

208 *Fischer-Dieskau*/*Gitter*/*Hornung*, MMR 2003, 385.

209 *Blum*, DuD 2001, 75. Für eine Gesetzesänderung zur Erweiterung der Vorschrift mit der Annahme der Anforderung der „Erkennbarkeit", *Thomale* 2003, 221.

210 *Fischer-Dieskau*/*Gitter*/*Hornung*, MMR 2003, 385.

211 *Roßnagel*, RMD, § 2 SigG Rn. 77.

oder Rückdatieren von digitalen Dokumenten.[212] Zeitstempel belegen aber nicht, dass der Empfänger tatsächlich das elektronische signierte Dokument erhalten hat. Der Nachweis, ob und wann eine Nachricht empfangen wurde, ist eine Funktion, die weder elektronische Signaturen noch Zeitstempel erfüllen. Erforderlich ist ein qualifizierter Zeitstempel auch bei der Erneuerung einer Signatur, gemäß § 17 SigV.[213]

Angestoßen wird das Verfahren der Zeitstempelung durch das Übertragen der mit einem Zeitstempel zu versehenden Daten an den Zeitstempeldienst des Zertifizierungsdiensteanbieters. Aber zu Gunsten des Daten- und Geheimnisschutzes müssen nicht alle Dokumente übermittelt werden, sondern „die digitale Signatur der signierten Daten".[214] Der Zeitstempeldienst verfügt als Systembestandteil über eine nachweisbar von außen unbeeinflussbare geeichte Uhr.[215] Die digitale Bestätigung mit den Angaben der aktuellen Uhrzeit wird an die signierten Daten angehängt und an den Absender zurückgeschickt.[216]

1.3.5.10 Datenschutz

Der Datenschutz ist dem Gesetzgeber des Signaturgesetzes nicht außer Acht geblieben. Im Folgenden ist dieses Thema allgemein und in Bezug auf das deutsche Signaturrecht zu behandeln.

1.3.5.10.1 Bedeutung und Entwicklung

Im deutschen Recht gilt Datenschutz als Grundrechtsschutz und Funktionsbedingung eines demokratischen Gemeinwesens.[217] Grund hierfür ist, dass das Individuum sich nur frei entwickeln und entfalten kann, wenn es die Möglichkeit hat, zu wissen, was seine Kommunikationspartner von ihm wissen. Verlangt wird somit die Selbstbestimmung des Betroffenen bezüglich der Erhebung und Verwendung seiner personenbezogenen Daten.

Im Vergleich zu anderen Rechtsgebieten ist der Datenschutz verhältnisweise jung. In den letzten Jahrzehnten ist seine Bedeutung in Deutschland stetig gestiegen. Im Bundesland Hessen trat am 30.9.1970 das erste Datenschutzgesetz der Welt in Kraft. Im Laufe der 70er Jahre haben alle Bundesländer der Bundesrepublik Deutschland ein Datenschutzgesetz verkündet und im Jahr 1978 trat das deutsche

212 BR-Drs. 966/96,32.

213 Siehe hierzu bereits in diesem Teil 1.3.5.5.2.

214 *Roßnagel*, RMD, § 2 SigG a. F. Rn. 80.

215 Zuständig für die offizielle Zeit in Deutschland ist die Physikalisch-Technischen Bundesanstalt (PTB), eine Oberbehörde des Bundesministeriums für Wirtschaft und Technologie.

216 *Gassen* 2003, 61.

217 *Roßnagel* 2003, 2.

Bundesdatenschutzgesetz (BDSG) in Kraft. Vielleicht wurde der wichtigste Grundstein für die Entwicklung des Datenschutzrechtes aber mit dem so genannten Volkszählungsurteil des Bundesverfassungsgerichts gelegt.[218] Auslöser war eine im Mai 1983 durch das Volkszählungsgesetz geplante Volkszählung, die aufgrund dieses Urteils erst im Jahr 1987 durchgeführt worden ist. Das Volkszählungsurteil erkennt das in der Literatur schon früher dargelegte und diskutierte Recht auf informationelle Selbstbestimmung[219] als die verfassungsrechtliche Grundlage des Datenschutzrechts an.[220] Hergeleitet ist die informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit der Menschenwürde des Art. 1 Abs. 1 GG. Für die unfreiwillige Erhebung und Verarbeitung von Daten hat das Urteil die Pflicht aufgestellt, „dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt". Berücksichtigt werden muss auch der Grundsatz der Verhältnismäßigkeit. Aus der Forderung des Bundesverfassungsgerichts, die Erhebung und Verarbeitung von Daten „bereichsspezifisch" und „präzise" zu behandeln, ist eine Fülle von bereichsspezifischen Regelungen entstanden. In den 90er Jahren wurde das Datenschutzrecht zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr durch Erlass der Richtlinie 95/46/EG europäisiert.

1.3.5.10.2 Datenschutz im Signaturrecht

Von erheblicher Bedeutung für die Stärkung des Vertrauens des Nutzers von Signaturverfahren sind auch die Datenschutzregelungen in Bezug auf die Tätigkeiten der Zertifizierungsdiensteanbieter. In ihren täglichen Aktivitäten verarbeiten Zertifizierungsdiensteanbieter eine beachtliche Datenmenge, wie unter anderem Daten zu ausgestellten Zertifikaten, zur Identität der Signaturschlüssel-Inhaber, zu Pseudonymen und deren Klarnamen, zu Auskünften über gesperrte Zertifikate und zu Attributen.

§ 14 Abs. 1 SigG erlaubt die Erhebung von personenbezogenen Daten durch den Zertifizierungsdiensteanbieter nur unter der Bedingung, dass die Daten unmittelbar beim Betroffenen selbst erhoben werden und nur insoweit, als dies für Zwecke eines qualifizierten Zertifikates erforderlich ist. Bei Dritten ist eine Datenerhebung nur mit Einwilligung des Betroffenen zulässig. In dieser Bestimmung sind allgemeine Grundsätze des Datenschutzrechts zu finden.

218 BVerfGE 65, 1.

219 Das Recht auf informationelle Selbstbestimmung des Einzelnen wird als das Rechtsgut gesehen, das eigentlich zu schützen ist, denn die Daten selbst sind nicht zu schützen. Daraus ergibt sich, dass der Begriff „Datenschutz" in der Realität als irreführend betrachtet wird. Hierzu, *Roßnagel*, APuZ, 2006, 9.

220 *Roßnagel* 2003, 8.

Erstens findet sich hier das Gebot der Transparenz, indem die Datenerhebung und -verarbeitung dem Betroffenen bekannt sein muss. Wie im Volkszählungsurteil gefordert, muss es dem Betroffenen möglich sein, zu wissen, „wer was wann und bei welcher Gelegenheit über ihn weiß“.[221] Die Transparenz ermöglicht dem Betroffenen, die Rechtmäßigkeit der Datenverarbeitung zu überprüfen, um sich gegen eventuelle Missbräuche zu wehren.[222]

Der zweite, in dieser Vorschrift vorgesehene Datenschutzgrundsatz ist die Erforderlichkeit der Datenerhebung. Grund hierfür ist, dass personenbezogene Daten zu verarbeiten, ein Eingriff in die informationelle Selbstbestimmung darstellt und dadurch nur im erforderlichen Umfang erfolgen darf.[223] An den Worten des Bundesverfassungsgerichts werden die Leitlinien des Erforderlichkeitsprinzips ausgerichtet: „Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen.“[224] Das Signaturgesetz beschränkt die Datenerhebung auf die erforderlichen Zwecke eines qualifizierten Zertifikates. Darunter versteht die Regelung aber nicht nur die Daten für den Inhalt des Zertifikats im engeren Sinne, laut § 7 Abs. 1 SigG, sondern auch die Daten, die für die Ausübung der normalen Tätigkeiten eines Zertifizierungsdiensteanbieters nötig sind. Dies sind unter anderen Daten über die Identifizierung des Teilnehmers, Schlüssel- und Zertifikatserzeugung und Signaturkarteübergabe.

Ferner ist in der Vorschrift das Prinzip der Zweckbindung zu finden, da § 14 Abs. 1 Satz 1 SigG die Datenverarbeitung auf die Zwecke eines qualifizierten Zertifikats beschränkt. Gemeint ist hier eine Datenerhebung, die nur soweit geht, wie es nötig ist, die Erreichung des vom Gesetz erlaubten oder vom Betroffenen eingewilligten Zwecks, zu erzielen. Diese Einschränkung ergibt sich aus § 14 Abs. 1 Satz 2 SigG, der entweder ein Gesetz oder die Einwilligung des Betroffenen als einzige mögliche Legitimationsgrundlage für eine Zweckänderung vorsieht.

1.3.5.10.3 Pseudonyme und ihre Aufdeckung

Laut § 5 Abs. 3 SigG hat der Zertifizierungsdiensteanbieter auf Verlangen eines Antragstellers in einem qualifizierten Zertifikat anstelle seines Namens ein Pseudonym aufzuführen. Pseudonyme können eine bedeutende Rolle als Mittel des Selbstdatenschutzes spielen.[225] Im elektronischen Geschäftsverkehr können sie bei den Fällen nützlich sein, wo eine Identifizierung nicht unbedingt erforderlich ist, aber die Verantwortlichkeit garantiert werden soll. Denn Pseudonymität ist keine Ano-

221 BVerfGE 65, 1 (43).

222 *Roßnagel*, RMD, § 14 SigG Rn. 56.

223 BVerfGE 65, 1 (43, 46).

224 BVerfGE 65, 1 (46).

225 *Roßnagel*, RMD, § 14 SigG Rn. 66.

nymität und ein Pseudonym muss immer dem Signaturschlüssel-Inhaber zugeordnet sein (§ 7 Abs. 1 Nr. 1 SigG).[226] Ist ein Pseudonym mit Angaben über eine berufsrechtliche Zulassung vom Teilnehmer beantragt, dann ist nach § 5 Abs. 3 Satz 2 SigG eine Einwilligung von der entsprechenden Berufskammer erforderlich.[227]

Bei der Verwendung von Pseudonymen muss aber erstens für den berechtigen Interessenten ein allgemeiner Aufdeckungsanspruch gewährleistet sein und zweitens ist ein effektives und unbürokratisches Aufdeckungsverfahren notwendig, das den Vertragspartner ohne großen Aufwand über die Identität des pseudonym Handelnden informiert.[228] Ist kein Anspruch auf Pseudonymaufdeckung vorgesehen oder wird das Aufdeckungsverfahren exzessiv verkompliziert und nicht in einer zumutbaren Weise gestaltet, dann droht durch die Verwendung von Pseudonymen Rechtsunsicherheit und Misstrauen. Dies wäre gerade das Gegenteil, was eine PKI anstrebt und verspricht. Trotz dieses Aspekts muss aber auch die informationelle Selbstbestimmung des Signaturschlüssel-Inhabers gewährleistet werden, mittels einer Prozedur, durch die die Aufdeckungsgründe glaubhaft darzustellen sind. Der Signaturschlüssel-Inhaber ist vor der Aufdeckung anzuhören und danach von der Aufdeckung zu informieren, damit er weiß, wer die Zuordnungsinformation erhalten hat.[229]

Das Signaturgesetz sieht eine Unterrichtungspflicht über die Ermittlung der Daten der ersuchenden Behörde gegenüber dem Signaturschlüssel-Inhaber vor, wenn die gesetzlichen Aufgaben der Behörde dadurch nicht beeinträchtig werden oder wenn das Interesse des Signaturschlüssel-Inhabers an der Unterrichtung überwiegt (§ 14 Abs. 2 Satz 2). Es ist sicherlich keine leichte Aufgabe, diese beiden widersprüchlichen Werte – Effizienz des Verfahrens und Selbstbestimmung des Betroffenen – in ein Gleichgewicht zu bringen, aber nur so kann die Verwendung von Pseudonymen im elektronischen Geschäftsverkehr vertrauenserweckend sein.

Gemäß § 14 Abs. 2 Satz 1 SigG hat der Zertifizierungsdiensteanbieter die Daten über die Identität des Signaturschlüssel-Inhabers auf ihr Ersuchen hin an die zuständigen Stellen zu übermitteln, wenn diese Maßnahme für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachritendienstes oder

226 Anders als Pseudonyme enthalten „anonyme Daten mindestens eine Einzelangabe über eine Person, ohne dass diese Person allerdings bekannt ist“. *Roßnagel*/*Scholz*, MMR 2000, 723. Besonderes Merkmal der Anonymität ist, „dass für die Einzelangaben zu einer Person die Wahrscheinlichkeit, dass diese der Person zugeordnet werden können, so gering ist, dass sie nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet“. *Roßnagel*/*Scholz*, MMR 2000, 724.

227 Somit liegt es im Spielraum der Berufskammern auszuschließen, ob ihre Mitglieder ihre beruflichen Leistungen unter einem Pseudonym erbringen dürfen. Hierzu BT-Drs. 14/662, 21.

228 *Roßnagel* 2003, 1229.

229 *Roßnagel*, RMD, § 14 SigG Rn. 74.

des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich ist. Bei dem behördlichen Auskunftsersuchen hinsichtlich der Daten hat der Zertifizierungsdiensteanbieter keine materielle Prüfungskompetenz, was die Rechtmäßigkeit des Ersuchens betrifft. Diese obliegt der Behörde.[230] Möglich ist auch, dass im Rahmen von anhängigen Verfahren und nach Maßgaben der für die Behörden geltenden Bestimmungen, Gerichte eine Datenaufdeckung anordnen. Dabei ist aber die Ausgangssituation für private Zertifizierungsdiensteanbieter schwierig, denn für das zivil- und arbeitsgerichtliche Verfahren – mit der Ausnahme von §§ 422, 429 ZPO – darf das Gericht nicht um Mitteilung von Urkunden ersuchen.[231] Obwohl die Bundesregierung den Umweg über die Vernehmung des Sachbearbeiters des Zertifizierungsdiensteanbieters vorgeschlagen hat, bleibt diese Frage immer noch ungelöst.[232]

1.3.5.10.4 Ausdehnung der Datenschutzvorschriften

Die signaturrechtlichen Datenschutzregelungen gelten nach § 14 Abs. 3 SigG nicht nur für die Zertifizierungsdiensteanbieter im Sinne des Gesetzes – das heißt, Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen – sondern auch für Anbieter von einfachen und fortgeschrittenen Signaturverfahren. Die Regelung entspricht der Datenschutzanforderung des Art. 8 Abs. 2 in Verbindung mit Art. 2 Nr. 11 RLeS, die auch andere Zertifizierungsdiensteanbieter umfasst. Als einzige Bestimmungen des Signaturgesetzes, die auch „nicht signaturgesetzkonforme“ Zertifizierungsdiensteanbieter beachten müssen, heben die Vorschriften zum Datenschutz die besondere Bedeutung dieses Anliegens im deutschen und europäischen Recht hervor.

Ausgehend von diesen Grundgedanken zur Systematik der elektronischen Signatur und ihrer rechtlichen Handhabung in Deutschland soll im Folgenden die Struktur der Betrachtung auch für die brasilianischen Gegebenheiten beibehalten werden, um im dritten Teil der Arbeit einen Rechtsvergleich übersichtlich darstellen zu können.

2. Die elektronischen Signaturen in Brasilien: Entstehungsgeschichte und Rechtsrahmen

Um die Gegebenheiten in Brasilien richtig verstehen zu können, ist es wichtig einen Blick in die Vergangenheit zu werfen. Dieser hier anschließende Exkurs zur Geschichte des brasilianischen Signaturrechts zeigt in kurzen Zügen die bedeutendsten Entwicklungen.

230 *Roßnagel*, RMD, § 14 SigG Rn. 71.

231 BT-Drs. 14/4987, 18.

232 *Roßnagel*, RMD, § 14 SigG Rn. 73.

2.1 Die Rechtsverordnung Nr. 3.587 und die Medida Provisória Nr. 2.200-2

Brasilien hat die wichtigsten internationalen Gesetzgebungsinitiativen verfolgt und auf sie reagiert. Im September 2000 ist die Rechtsverordnung Nr. 3.587[233] vom Bundespräsidialamt verkündet worden. Diese Verordnung hat die so genannte ICP[234]-Gov, eine PKI für die brasilianische Bundesverwaltung, geschaffen. Ziel dieser Infrastruktur war die Verbreitung der kryptographischen Verfahren zur Verwendung im Rahmen elektronischer Signaturen ausschließlich innerhalb der Bundesverwaltung. Forciert wurde auch der Übergang der papiergebundenen Verfahren innerhalb der Verwaltung zur Verwendung elektronischer Dokumente. Die Anwendung der elektronischen Signaturen sollte einen Beitrag in Richtung der Gewährleistung der Integrität und Authentizität dieser Umwandlung leisten.

Die ICP-Gov ist in der Praxis nicht implementiert worden. Nach ihrer Gründung und angesichts der zunehmenden Bedeutung des Internets als Raum für Informationsaustausch und wirtschaftliche Betätigung sowohl in Brasilien als auch auf internationaler Ebene hat die Bundesregierung sich für die Erschaffung einer breiteren und flächendeckenderen Infrastruktur, nicht nur für die Verwendung innerhalb der gesamten Bundesverwaltung, sondern auch auf die privat-rechtlichen Unternehmen und auf den normalen Bürger entschieden. Am 28. Juni 2001 wurde die Medida Provisória (MP) Nr. 2.200 vom Bundespräsidenten erlassen, die die so genannte ICP-Brasil (für das ganze Land) geschaffen hat. Problematisch war dabei, dass vor dem Erlass der Medida Provisória verschiedene Gesetzesentwürfe über Rahmenbedingungen für die Einführung von digitalen Signaturen und allgemein über den elektronischen Geschäftsverkehr zur Diskussion im Parlament standen.[235] Besonders die plötzliche Verabschiedung der Normen stieß auf Kritik. Den Kritikern nach sei die seit langem dauernde Debatte über das Thema innerhalb des Parlaments von der Regierung einfach ignoriert worden.[236]

Die Medida Provisória könnte als „provisorische Maßnahme“ ins Deutsche übersetzt werden. Die Medida Provisória ist kein Gesetz im formellen Sinn, denn ursprünglich wird sie nicht vom Parlament verabschiedet. Diese Gesetzesart hat ähnliche Merkmale wie das italienische „decreto-legge“, das spanische „Real Decreto-ley“ und das portugiesische „Decreto“.[237] Gemäß Artikel 62 der brasilianischen Verfassung wird die Medida Provisória, welche die Kraft eines Gesetzes hat, allein

233 Verordnungstext unter www.planalto.gov.br → Legislação → Decretos → 2000.

234 Die Abkürzung ICP steht für Infra-Estrutura de Chaves Públicas. Das ist die Übersetzung für den bekannten Begriff:„Public-Key Infrastructure“ (PKI).

235 Wenigstens drei Gesetzentwürfe waren im Gesetzgebungsverfahren im Parlament als die MP 2.200 erlassen wurde. Die Gesetzentwürfe Nr. 1.483 von 1999, Nr. 1589 von 1999 (beide in der Abgeordnetenkammer) und Nr. 672 von 1999 (im föderativen Senat).

236 Zu Kritiken siehe *Marcacini*/*Costa* 2001.

237 Hierzu *Amaral Júnior* 2004, 55.

vom Bundespräsidenten beschlossen.[238] In der Praxis aber werden die so genannten Medidas Provisórias vom Bundespräsidenten und manchmal auch zusammen mit den entsprechenden Bundesministern unterschrieben.[239] Die grundsätzlichen Vorbedingungen für die Erlassung einer Medida Provisória sind die Wichtigkeit und die Dringlichkeit der Maßnahme. Dies sind Maßstäbe, die nicht ganz objektiv sind und die nicht selten zu heftigen Diskussionen führen.[240]

Ursprünglich ist die MP 2.200 zweimal neu erlassen worden. Heutzutage gilt sie in ihrer dritten Fassung, der so genannten MP 2.200-2. Dem ist so, weil bis September 2001 alle MPs nach 30 Tagen vom Parlament verabschiedet werden mussten, sonst traten sie außer Kraft. In der Praxis hat das brasilianische Parlament fast nie innerhalb des knappen Zeitraums von 30 Tagen eine MP in ein Gesetz umgewandelt. Manche MPs sind mehr als hundert Mal von der Regierung erneut verkündet worden, denn für die Anzahl der Erneuerungen gab es keine Grenze. Im September 2001 ist eine Verfassungsänderung in Kraft getreten, die so genannte Emenda Constitucional Nr. 32, durch die die Erneuerung der MPs erschwert worden ist. Der Art. 62 der Constituição Federal wurde so geändert, dass die MPs innerhalb von 60 Tagen unbedingt vom Parlament in ein Gesetz umgewandelt werden müssen, sonst verlieren sie endgültig ihre Gültigkeit. Diese Frist darf nur einmal um weitere 60 Tage verlängert werden (§ 3 des Artikels 62).[241] Nach 45 Tagen ohne Beschluss im Parlament gewinnt die MP eine Priorität in der Tagesordnung des Parlaments (§ 6 des Artikels 62). Auch wurde von derselben Verfassungsänderung bestimmt, dass die schon vor dieser Verfassungsänderung geltenden MPs unberührt bleiben, bis sie definitiv vom Parlament beschlossen werden. Das ist für MP 2.220-2 der Fall, die in ihrer dritten Fassung fristlos gilt.

Hinzuweisen bleibt noch darauf, dass die MP 2.200-2 wahrscheinlich durch ein Gesetz ersetzt werden wird. Die Abgeordnetenkammer erarbeitet seit 2002 den Gesetzentwurf Nr. 7316/2002, der schon viel umfangreicher als die MP 2.200-2 ist, aber gleichzeitig ihre wichtigsten Grundsätze bestehen lässt.

238 Auch Griechenland hat einen nationalen Regelungsrahmen für elektronische Signaturen durch einen Präsidialerlass eingeführt. Der Präsidialerlass 150/2001 setzte die europäische Signaturrichtlinie in die griechische Rechtsordnung um. Hierzu *Komnios* 2007, 255 ff.

239 *Amaral Júnior* 2004, 230.

240 Die Rechtsprechung des brasilianischen Supremo Tribunal Federal, das brasilianische Bundesverfassungsgericht, verfolgt einen Ansatz, wonach die richterliche Kontrolle der Kriterien von Wichtigkeit und Dringlichkeit der Medida Provisória nur ausnahmsweise ausgeübt werden darf und nur in den Fällen bei denen offensichtlich ist, dass die Kriterien nicht berücksichtigt worden sind. ADI – MC 1910-DF, AI-AgR 489-108-RS. Hierzu auch *Amaral Júnior* 2004, 55.

241 Das bedeutet, dass nach der Verfassungsänderung, die MP maximal einmal verlängert werden darf.

2.2 Die Medida Provisória Nr. 2.200-2 und die Merkmale der Infrastruktur für öffentliche Schlüssel

2.2.1 Allgemeines

Die MP 2.200-2 ist kein umfangreiches Gesetz. Sie enthält nur 20 Artikel, die knapp vier Seiten ausfüllen. Sie regelt die Hauptpfeiler der Sicherungsinfrastruktur, legt in § 1, Artikel 10 aber auch die Gleichstellung einer digitalen Signatur mit der eigenhändigen Unterschrift fest.

Die MP 2.200-2 regelt die Besetzung und Aufgaben des Regulierungsausschusses[242] (Comitê Gestor), die Hauptaufgaben der Aufsichtsbehörde (Instituto Nacional de Tecnologia da Informação), der Zertifizierungsdiensteanbieter (Autoridades Certificadoras – ACs) und der Identifikationsstellen (Autoridades de Registro – ARs).[243] Das Gesetz verwendet die Bezeichnungen „Autoridades Certificadoras" und „Autoridades de Registro", die von den im englischen Sprachraum üblichen „Certification Authority" (CA) und „Registration Authority" (RA) abstammen und übernommen wurden. Der Gesetzentwurf Nr. 7316/2002 (Art. 2, IX) verwendet die Formulierung „prestador de serviços de certificação", eine direkte Übersetzung des Begriffs „Zertifizierungsdiensteanbieter" der europäischen Signaturrichtlinie.

2.2.2 Das technologische Konzept

Die brasilianische Infrastruktur ist nicht technikneutral. Das bedeutet, dass die MP Nr. 2.200-2 offensichtlich und ausdrücklich das technologische Konzept der digitalen Signaturen mit Anwendung öffentlicher Schlüsselsysteme auf der Basis asymmetrischer Verschlüsselungsverfahren verfolgt hat. Nach Art. 6 zum Beispiel obliegt dem akkreditierten Zertifizierungsdiensteanbieter die „Ausstellung von digitalen Zertifikaten, die kryptographische Schlüssel den Signaturschlüssel-Inhabern zuordnen".[244] Obwohl bei der Verabschiedung der MP 2.200-2 die Grundsätze der Signaturrichtlinie 1999/93/EG in Brasilien bereits bekannt waren, wurde das Prinzip der Technikoffenheit[245] nicht übernommen. Stattdessen wurde die Literatur berücksich-

242 Im Art. 3.

243 Art. 5 bis 9.

244 Das digitale Zertifikat ordnet eigentlich einen öffentlichen Schlüssel einer Person zu und nicht die beiden kryptographischen Schlüssel.

245 Die Technologieoffenheit wird im Erwägungsgrund 8 der Signaturrichtlinie wie folgt begründet: „Die rasche technologische Entwicklung und der globale Charakter des Internets erfordern ein Konzept, das verschiedenen Technologien und Dienstleistungen im Bereich der elektronischen Authentifizierung offen steht". Im Text der Richtlinie wird das Konzept durch Begriffsbildungen wie etwa „elektronische Signaturen" statt „digitale Signaturen" und „Signaturprüfdaten" statt direkt „öffentliche kryptographische Schlüssel" ausgedrückt.

tigt, die darauf hinweist, dass sich das Prinzip „bei näherem Hinsehen [...] als ideologischer Überbau, unnötige Verkomplizierung der Regelungen und praktisch irrelevant“ erweist.[246] Es ist irrelevant, weil das Ziel jeder Sicherungsinfrastruktur für offene Netze auch die Verbreitung der Identifikationsmittel ist. Fraglich ist, ob die erwünschte Interoperabilität und Verbreitung in einem reinen technikoffenen System verwirklicht werden können. Eigentlich sind diese anzustrebenden Ziele erst dann erreicht, wenn eine Festlegung von Parametern und Standards durchgeführt wird. Dazu muss darauf hingewiesen werden, dass die Interoperabilität dann das genaue Gegenteil von Technologie-Neutralität[247] bedeuten kann.[248] Denn wenn alle Möglichkeiten für Identifikationsmechanismen offen bleiben, wird es schwer eine einheitliche Wahl von allen Beteiligten zu gewährleisten.

Auch innerhalb der Signaturrichtlinie der EG wird die im Prinzip gewollte Technologieoffenheit im Endeffekt nicht geschaffen. Die Definition von fortgeschrittenen elektronischen Signaturen zum Beispiel erfasst in der Praxis nur digitale Signaturverfahren. Auch die Anforderungen der vier Anhänge der Richtlinie richten sich an die asymmetrischen Verschlüsselungsverfahren.[249]

Trotz dieser Argumente hat sich der Gesetzgeber im Entwurf Nr. 7.316/2002 für die technologisch neutrale Variante entschieden. Die Begründung des Entwurfes spricht von einer Notwendigkeit zur „Anpassung der nationalen Vorschriften an die Begriffsbestimmungen der internationalen Gesetzgebungsinitiativen“.[250] Dadurch werden Begriffe wie „elektronische Signatur“ (assinatura eletrônica) und „fortgeschrittene elektronische Signatur“ (assinatura eletrônica avançada) in das brasilianische Signaturrecht eingeführt.

246 *Roßnagel* 2002a, 137. Auch kritisch zu dem technologieunabhängigen Ansatz *Fischer-Dieskau* 2006, 98, 191.

247 Über den Ausdruck „technology neutrality“ siehe *Baum* 1999, 4. Dieser Autor weist darauf hin, dass der Ausdruck „…is more a political buzzword than a clearly defined legal concept. In its most common usage, it refers to laws, regulation or other types of rules which purports to favour neither PKIs nor other technologies. The myth advanced by the technology-neutrality lobby is that such rules will ensure the unfettered development of diverse information security technologies and solutions, ensure mutual recognition of e-commerce transactions, and prevent non-tariff trade barriers to global competition for e-commerce services. But myth is not reality”.

248 *Schwemmer* 2001, 5.

249 *Roßnagel* 2002a, 137.

250 Übersetzung eines Satzes des Erwägungsgrundes Nr. 4. Gesetzbegründung unter http://www.planalto.gov.br/ccivil_03/Projetos/Quadros/quadro_PL/2002.htm.

2.2.3 Zertifizierungsstruktur

Merkmal der brasilianischen Zertifizierungsstruktur ist das Vorliegen eines umgekehrten baumartigen Zertifizierungsgraphen. Dadurch bildet sich eine hierarchische Kette, in der die Aufsichtsbehörde Instituto Nacional de Tecnologia da Informação die Funktion der Wurzel-Zertifizierungsinstanz übernimmt. Dazu gehört ihre Selbstzertifizierung, das heißt sie selber bestätigt ihre Schlüsselpaare ohne die Mitwirkung eines Dritten. Die zweite Ebene wird von den von der Aufsichtsbehörde zertifizierten Zertifizierungsdiensteanbietern gebildet. Diese erhalten ein Wurzelzertifikat der Aufsichtsbehörde, das die Vertrauenswürdigkeit der Zertifikatkette sichern soll. Zum einen wird der Zertifizierungspfad mit der Aufsichtsbehörde als oberste Instanz und Vertrauensanker festgelegt. Und andererseits können die Zertifikate aller akkreditierten Zertifizierungsdiensteanbieter ohne weiteres auch von den Prüfprogrammen anderer Anbieter überprüft werden, da sie sich in der gleichen Zertifikatsstruktur befinden.[251] Eine weitere Hierarchieebene ist möglich, da die Zertifizierungsdiensteanbieter der zweiten Ebene die Möglichkeit haben, wiederum andere Zertifizierungsdiensteanbieter zu zertifizieren. Und in der letzten Ebene steht schließlich der Endnutzer. Somit besteht eine vierstufige Infrastruktur, wobei jede Zertifizierungsinstanz mehrere Schlüsselpaare verwenden darf, um die Zertifikate von anderen Zertifizierungsdiensteanbietern oder Endnutzern zu signieren.

2.2.4 Die Regulierung: Der Regulierungsausschuss

Eigenschaft der MP 2.200-2 ist ihr geringer Umfang. Wegen der daraus resultierenden geringen Regelungsdichte wurde ein Regulierungsausschuss (Comitê Gestor) ins Leben gerufen (Art. 4), der bestimmte operative Regelungen treffen kann. Zur Besetzung des Ausschusses gehören Vertreter von Ministerien, Regierungsorganen und Repräsentanten von verschiedenen Organisationen der Zivilgesellschaft (insgesamt 12 Mitglieder), die vom Bundespräsidenten ernannt werden.[252]

Das Comitê Gestor entscheidet durch Beschlüsse (Resoluções), die vorher von einer technischen Kommission erarbeitet werden. Laut Art. 4 der MP 2.200-2 soll der Ausschuss die technischen Standards zum Betreiben der Wurzelinstanz und die Voraussetzungen, Kriterien und Verfahren zur Akkreditierung von Zertifizierungsdiensteanbietern, Identifizierungsstellen und sonstigen Diensteanbietern des Gebiets festlegen. Zudem obliegen dem Comitê Gestor andere Aufgaben, wie die Überprü-

251 *Roßnagel*, MMR 2002, 217.

252 Laut Art. 3 der MP 2.200-2 wird der Ausschuss so gegliedert: Je ein Repräsentant von folgenden Ministerien: Justiz, Finanzen, Entwicklung und Industrie, Wissenschaft und Technologie, Planung und Haushalt, Sicherheitskabinett im Präsidialamt der Republik und Casa Civil (Präsidialamt); fünf Repräsentanten von verschiedenen Organisationen der Zivilgesellschaft.

fung der Wurzelinstanz, die Kontrolle der Angemessenheit der geltenden Normen und Standards und, falls nötig, ihre Aktualisierung. Außerdem kommt dem Comitê Gestor die Koordinierung des Verfahrens zur Feststellung gleichwertiger Sicherheit bei der gegenseitigen Anerkennung von Signaturverfahren zwischen Brasilien und anderen Ländern zu. Nach Art. 4, § 1 darf der Ausschuss auch manche Regulierungsbefugnisse an die Aufsichtsbehörde delegieren. Das Comitê Gestor hat von September 2001 bis Juli 2008 schon 48 Resoluções beschlossen, welche von der Aufsichtsbehörde umgesetzt werden.

Die Resoluções enthalten die detaillierten Regelungen für das Betreiben der gesamten Infrastruktur. Die Strukturierung dieser Normen richtet sich nach den IETF Spezifikationen (den so genannten RFC).[253] Die Standards von verschiedenen Institutionen wurden berücksichtigt. Unter anderem wurden folgende Standards befolgt: Für die Formatierung der digitalen Zertifikate die Version Nr. 3 des RFC 3280; für die kryptographischen Spezifikationen der Dateien und Algorithmen der Standard ITU X.509, für die kryptografischen Hardware Standards die PKCS Dokumente[254] sowie die FIPS-Normen[255].

2.2.5 Die Aufsichtsbehörde

Eine umstrittene Frage bei der Gründung der ICP-Brasil in Bezug auf die Ausgestaltung der Sicherungsinfrastruktur war, ob die dazugehörigen Funktionen tatsächlich eine öffentliche Aufgabe oder vielmehr eine Privatangelegenheit darstellen. Diskutiert wurde, ob und inwieweit der Staat eine Rolle bei der Ausgestaltung der neuen Infrastrukturen spielen sollte.[256] So wie der deutsche Gesetzgeber entschied sich die

253 Die Internet Engineering Task Force (IETF) ist eine Arbeitsgruppe des Internet Achitecture Board (IAB). Ihr Auftrag ist die Entwicklung und Förderung von Internetstandards. Sie ist eine offene, Internationale Vereinigung von Netzwerktechnikern, Herstellern und Anwendern, die für Vorschläge zur Standardisierung des Internets zuständig ist. Die RFCs (Request for Comments) sind die Dokumente die aus den Diskussionen der IETF folgen. Es existiert keine förmliche Mitgliedschaft oder Mitgliedsvoraussetzung. Zur Internetseite der IETF siehe: http://www.ietf.org.

254 PKCS steht für Public Key Cryptography Standards, die wurden von den RSA Laboratorien ab 1991 entwickelt und manche werden, wie die PKCS 7, von den RFCs der Internet Engineering Task Force beschrieben.

255 FIPS steht für Federal Information Processing Standard. Das ist die Bezeichnung für technische Standards des Institute of Computer Sciences and Technology (ICST) aus den Vereinigten Staaten von Amerika.

256 Stimmen wie die von *Pedro Rezende*, *Augusto Marcacini* und *Marcos Costa* waren klar gegen die Einmischung des Staates in die Funktionen einer Public Key Infrastruktur. Der Staat dürfte höchstens seine eigene interne Infrastruktur betreiben. *Rezende*/*Marcacini*/*Costa*, 2003.

brasilianische Regierung für eine Infrastruktur, in der der Staat zwar private Unternehmen zulässt, sich aber die Aufsicht des Systems vorbehält. Die Leistungen einer solchen Sicherungsinfrastruktur sind Leistungen der öffentlichen Daseinsvorsorge und dadurch vergleichbar mit Verkehrs-, Telekommunikations- oder Energieinfrastrukturen.[257] Oft wird dieses Merkmal verkannt und oft wird vergessen, dass vollständig kompatible Infrastrukturen leichter durch staatliche Organisationen geschaffen werden können.[258] Der Markt allein trägt eben gerade keine Verantwortung für die allgemeine interoperable Verbreitung der Dienste und noch weniger für den Schutz der Interessen von Konkurrenten, Verbrauchern, Zulieferern, unbeteiligten Dritten oder künftigen Generationen.[259]

In der ICP-Brasil werden die Aufsichtsmaßnahmen gemäß Art. 5 der MP 2.200-2 von der Behörde Instituto Nacional de Tecnologia da Informação (ITI) mit Sitz in Brasilia durchgeführt. Das ITI betreibt die oberste Zertifizierungsstelle der nationalen Hierarchie und wird deshalb als Wurzelinstanz (AC Raiz) bezeichnet. Es akkreditiert die Zertifizierungsdiensteanbieter nach einer Prüfung vor der Betriebsaufnahme, bei der ermittelt wird, ob sie die Anforderungen der MP 2.200-2 und der Beschlüsse des Regulierungsausschusses erfüllen. Diese Vorabprüfung gemäß Art. 3.4 Resolução Nr. 44 wird nur von der Aufsichtsbehörde und ihrem Personal realisiert. Am Ende des Akkreditierungsverfahrens stellt das ITI anhand seines privaten Schlüssels die Zertifikate für die akkreditierten ACs aus, damit sie für die Endkunden ihrerseits Zertifikate ausstellen können. Laut Art. 2.1, a), Resolução Nr. 44 werden akkreditierte Anbieter auch nach der Akkreditierung jährlich von einer dritten Prüfstelle geprüft. Außerdem kann das ITI eine akkreditierte Zertifizierungsstelle jederzeit kontrollieren.

Unter der Aufsicht des ITI stehen akkreditierte Zertifizierungsdiensteanbieter, akkreditierte Identifikationsstellen und akkreditierte sonstige Diensteanbieter. Den nicht akkreditierten Zertifizierungsdiensteanbietern obliegt keine der in der MP 2.200-2 und in den weiteren Normen festgelegten Pflichten. Sie werden weder vorab überprüft noch nach ihrer Betriebsaufnahme kontrolliert.

257 *Roßnagel*, DuD, 1995, 262; hierzu auch *Hammer*, der eine Infrastruktur als ein *sozio-technisches System* definiert „das in einer Region oder einem organisatorischen Komplex für viele Nutzer (Anwenderkreis) einen *einheitlichen* Satz von *Leistungsmerkmalen* oder Dienstleistungen bereitstellt. Die Nutzer können weitgehen frei entscheiden, wann, wie und zu welchem Zweck sie die von der Infrastruktur bereitgestellten Nutzungsoptionen einsetzen.“, *Hammer* 1995, 42 f.

258 Wichtig ist hier die Warnung von *Adams*/*Lloyd* 1999, 27, in dem Sinn, dass eine allgemein verbreitete Infrastruktur die „piecemeal, point-to-point, ad hoc, non interoperable“ Lösungen vermeidet und eine einheitliche Sicherheit quer durch mehrere Anwendungen ermöglicht. Die Autoren weisen auch zu Recht darauf hin, dass ein echtes Chaos herrschen würde, wenn jeder seine eigenen Kommunikationsverbindungen allein führen und festsetzen könnte.

259 *Roßnagel*, MMR, 2002, 69.

Von Bedeutung ist nicht nur die Aufgabe der Ausstellung der nötigen Zertifikate der Zertifizierungsdiensteanbieter, sondern auch die Durchführung einer Palette anderer Maßnahmen, wie die Führung eines Zertifikatsverzeichnisses mit den für die Zertifizierungsdiensteanbieter ausgestellten Zertifikaten. Dieses Verzeichnis spielt eine große Rolle bei der Vertrauenswürdigkeit der Zertifikatkette. Es ermöglicht die Verifizierung der Zertifikate, indem es klarstellt, ob das jeweilige Zertifikat wirklich von dem entsprechenden Zertifizierungsdiensteanbieter stammt und ob es gültig ist.

Darüber hinaus hat die Aufsichtsbehörde gemäß Art. 6.1 Resolução Nr. 41 den Stand von Wissenschaft und Technik immer zu beachten und bei Bedarf die Algorithmen und zugehörigen Parameter in Bezug auf die Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen zu aktualisieren. Die Aktualisierungen der Parameter werden auf der Internetseite der Aufsichtsbehörde veröffentlicht.

2.2.6 Die akkreditierten Zertifizierungsdiensteanbieter

Weil das brasilianische Signaturrecht „sonstige" Zertifizierungsdiensteanbieter nicht definiert und regelt, werden in dieser Arbeit nur die akkreditierten Zertifizierungsdiensteanbieter betrachtet. Die „Autoridades Certificadoras" sind die Hauptdienstleister einer Public Key Infrastruktur. Die brasilianische Regulierung bindet die Akkreditierung von Betreibern an drei verschiedene Arten von Voraussetzungen: 1) formelle Anforderungen; 2) finanzielle Leistungsfähigkeit, 3) technische Fachkunde und Sicherheit.

2.2.6.1 Die formellen Anforderungen

Zwei formelle Anforderungen zur Akkreditierung als Zertifizierungsdiensteanbieter werden im Rahmen der ICP-Brasil vorgesehen. Zum einen muss der Kandidat gemäß Art. 2.1, a, Resolução Nr. 47 entweder die Form einer juristischen Person des privaten oder des öffentlichen Rechts aufweisen. Gestattet wird die Akkreditierung des Organs einer juristischen Person des öffentlichen Rechts. Ausgeschlossen wird somit, dass natürliche Personen akkreditierte Zertifizierungsdienste in Betrieb nehmen.[260] Zum anderen müssen sich nach Art. 2.1,1, d, sowohl Verwaltungssitz als auch Trustcenter des Kandidaten in Brasilien befinden.

260 Anders als im deutschen Signaturrecht, das im § 2 Nr. 8 SigG auch natürliche Personen für die Tätigkeiten als Zertifizierungsdiensteanbieter zulässt. Der Ansatz basiert auf Art. 2 Nr. 11 RLeS.

2.2.6.2 Die finanzielle Leistungsfähigkeit

Aufgrund der langfristigen Pflichten[261] der Zertifizierungsdiensteanbieter und auch wegen der Natur des Dienstes spielt die finanzielle Leistungsfähigkeit als Voraussetzung zur Akkreditierung eine wesentliche Rolle. Das Betreiben einer Zertifizierungsstelle darf keine zeitweilige Tätigkeit sein. In diesem Bereich herrscht das Vertrauen als wichtigster Wert und das wird nur durch Stabilität und Verlässlichkeit gebildet. Auch wenn die finanziellen Daten nicht allein solche erwünschten Ziele gewährleisten können, ist es nicht zu verkennen, dass sie zumindest teilweise etwas von dem Grad der Verlässlichkeit eines Unternehmens erkennen lassen.

Die finanzielle Leistungsfähigkeit des Kandidaten wird nach Art. 3, a) Resolução Nr. 47 durch die Auswertung seiner Bilanzen sowie durch das Gutachten eines Wirtschaftsprüfers bewertet. Dazu muss der Kandidat der Aufsichtsbehörde entsprechende Dokumente vorlegen, wie steuerliche Negativbescheinigungen gegenüber den verschiedenen Bundes-, Landes- und Gemeindebehörden sowie eine Negativbescheinigung des Insolvenzgerichts.

2.2.6.3 Die technische Fachkunde und Sicherheit

Um akkreditiert zu werden, muss der Kandidat die technische Zuverlässigkeit und Fachkunde in einer Vorabprüfung bei der Aufsichtsbehörde unter Beweis stellen. Im Grunde muss dargelegt werden, dass die für den Betrieb maßgeblichen Rechtsvorschriften eingehalten werden. Unter anderem werden der Aufsichtsbehörde vom Akkreditierungskandidaten drei Dokumente vorgelegt, die als Kern der Tätigkeiten betrachtet werden können. Diese Dokumente sind das Sicherheitskonzept, das Dokument „Declaração de Práticas de Certificação"[262] und das Dokument „Política de Certificado"[263].

2.2.6.3.1 Das Sicherheitskonzept

Das Sicherheitskonzept umfasst hauptsächlich vier Kategorien von Sicherheitsanforderungen: Zuverlässigkeit des eingesetzten Personals, die bauliche Sicherheit der Zertifizierungsstelle, die logische Sicherheit[264] und die Sicherheit der kryptografi-

261 Zum Beispiel die Pflicht zur unbefristeten Führung eines Zertifikatsverzeichnisses nach Ablauf der Zertifikate, zur Sicherung der Prüfbarkeit von Signaturen im Laufe der Zeit (Art. 6.3.1 Resolução Nr. 42). Hierzu siehe unten in diesem Teil Gliederungspunkt 2.2.9.1.3.

262 Eine Übersetzung des englischen „Certification Practice Statement".

263 Eine Übersetzung des englischen „Certificate Policy".

264 Die logische Sicherheit umfasst im Besonderen alle Maßnahmen die verhindern dass Computer, Hard- und Software unberechtig benutzt werden oder die unerlaubten Zugriff entdecken.

schen Mittel. Es enthält unter anderem Informationen über die Vorkehrungen und Maßnahmen zur Sicherstellung und Aufrechterhaltung des Betriebs bei Notfällen, das so genannte „Plano de Continuidade do Negócio“, das jährlich getestet werden soll. Die Richtlinien zu allen Sicherheitskonzepten innerhalb der ICP-Brasil wurden von der Resolução Nr. 39 festgesetzt und müssen von den akkreditierten Zertifizierungsdiensteanbietern sowie von der Wurzelinstanz berücksichtig werden. Die Präzisierung wird aber von den Zertifizierungsdiensteanbietern durchgeführt. Anders als die Dokumente „Política de Certificado“ und „Declaração de Práticas de Certificação“ ist das Sicherheitskonzept geheim zu halten und darf nicht veröffentlicht werden, da es vertrauliche Informationen über die Sicherheit der Tätigkeiten und Struktur der jeweiligen Zertifizierungsstelle enthält.

2.2.6.3.2 Declaração de Práticas de Certificação

Das Dokument „Declaração de Práticas de Certificação“ beschreibt in einer ganz detaillierten Weise die allgemeinen Tätigkeiten und Pflichten des Zertifizierungsdiensteanbieters und besonders die Verfahrensweise, wie die digitalen Zertifikate ausgestellt und verwaltet werden. Im Einzelnen werden die Anforderungen und Verfahren zur Identifikation des Antragstellers eines Zertifikats und zur Erstellung, Sperrung und Erneuerung von Zertifikaten beschrieben. Die minimalen Anforderungen für eine „Declaração de Práticas de Certificação“ sind in der Resolução Nr. 42 enthalten. Der Aufbau dieser Norm lehnt sich dabei an die Empfehlungen des RFC 2527 an.

2.2.6.3.3 Políticas de Certificados

Das Dokument „Políticas de Certificado“ spezifiziert Informationen über die Zertifikate, die von dem Zertifizierungsdiensteanbieter ausgestellt werden. Es informiert unter anderem über das Zertifikatprofil und die möglichen Kategorien von Zertifikatsinhabern. Da es in der ICP-Brasil verschiedene Zertifikatsstufen[265] innerhalb des Akkreditiertenverfahrens gibt, wird für jeden Zertifikatstyp eine separate „Política de Certificado“ von der AC erarbeitet und veröffentlicht.

Zum Begriff, s. unter: http://www4.in.tum.de/~popp/teaching/onlinebusiness/ausarbeitungen/ausarbeitung3.doc.

265 Hierzu siehe unten in diesem Teil Gliederungspunkt 2.2.9.1.2.1.

2.2.6.4 Übersicht über den brasilianischen Markt für akkreditierte Zertifizierungsdiensteanbieter

Im Rahmen der ICP-Brasil sind schon vierzehn akkreditierte Zertifizierungsdiensteanbieter in Betrieb. Von diesen gehören vier der öffentlich-rechtlichen Verwaltung, drei gemischtwirtschaftlichen Unternehmen und fünf der Privatwirtschaft an. Im September 2008 ließ sich die AC OAB akkreditieren. Die OAB (Ordem dos Advogados do Brasil) ist die nationale Anwaltskammer und Anwaltsvereinigung Brasiliens.

Bei den drei Privaten handelt es sich um die Firmen AC Sincor, die Versicherungsmaklergewerkschaft des Bundeslandes São Paulo, die AC Certisign, der erste Zertifizierungsdiensteanbieter in Brasilien und Hauptvertreter des nordamerikanischen Unternehmen Verisign, und die AC Serasa, ein Unternehmen für Wirtschafts- und Finanzinformationen. Serasa verfügt über Brasiliens größte Datenbank mit Daten über Personen, Unternehmen und Wirtschaftsgruppen und leistet aktive Unterstützung bei den meisten Kredit- und Geschäftsentscheidungen, die in Brasilien getroffen werden. Der Privatwirtschaft gehören auch die AC Fenacon – der nationale Verein der Steuerberater – sowie die AC Fenacor, der nationale Verein der Versicherungsmakler an.

Die Zertifizierungsdiensteanbieter der öffentlich-rechtlichen Verwaltung sind die AC Presidência da República, die AC Secretaria da Receita Federal – AC SRF, die AC Imesp und die AC Jus. Die AC Presidência da República erstellt eigentlich nur Zertifikate für die Beamten des Präsidialamtes, für die Bundesminister und ihre Mitarbeiter. Die Secretaria da Receita Federal ist die oberste brasilianische Steuerbehörde. Sie stellt digitale Zertifikate nur für bestimmte Zertifizierungsdiensteanbieter aus, die wiederum für die Endkunden[266] ihre Zertifikate ausstellen. Die Zertifikate für die Endkunden werden vor allem für elektronische steuerliche Anwendungen benutzt.[267] Ein weiterer öffentlich-rechtlicher Zertifizierungsdiensteanbieter ist die AC Jus, die zur judikativen Gewalt gehört. Sie besteht aus einer Versammlung von verschiedenen obersten Gerichtshöfen des Bundes und Gerichten der Länder. Die AC Imesp gehört der Regierung des Bundeslandes São Paulo. Die Hauptaufgabe von Imesp ist das Betreiben des offiziellen Gesetzblattes São Paulos.

Zu der Kategorie der gemischtwirtschaftlichen Unternehmen, die auch eine Zertifizierungsstelle betreiben, gehören die AC Serpro, AC Petrobrás, AC Prodemge und die AC Caixa Econômica Federal. Serpro (Serviço Federal de Processamento de

266 Als Endkunde werden hier natürliche sowie juristische Personen gemeint, denn nach brasilianischem Signaturrecht dürfen beide Signaturschlüsselinhaber sein.

267 Das „e-CAC“ (Centro Virtual de Atendimento ao Contribuinte – virtuelle Dienststelle für den Steuerzahler) ermöglicht den Zugang zu verschiedenen Dienstleistungen, wie die elektronische Steuererklärung, das formelle Verfahren zur Aufteilung steuerlichen Schulden, die elektronische Vollmacht zur Vertretung des Steuerzahlers sowie die Beschaffung von allen persönlichen steuerlichen Informationen des Steuerzahlers.

Dados) ist das größte IT-Unternehmen Brasiliens. Gebunden an das Bundesfinanzministerium ist Serpro landesweit Zulieferer der Informationstechnologiedienste vieler Organe und Behörden des Ministeriums. Dienste wie die elektronische Steuererklärung und alle Systeme der Sozialverwaltungsbehörden werden von Serpro entwickelt. Petrobras ist eine der größten Ölfirmen weltweit und betreibt eine virtuelle AC. Prodemge ist auch ein IT-Unternehmen, aber seine Tätigkeiten beschränken sich ausschließlich auf den Bereich des Bundeslandes Minas Gerais. Die Bank Caixa Econômica Federal ist die staatliche Bundessparkasse Brasiliens mit 33 Millionen Kunden und die größte öffentliche Bank des Landes und Lateinamerikas.

Obschon diese relativ große Anzahl von Zertifizierungsdiensteanbietern existiert, verfügen die meisten von ihnen über kein eigenes Trustcenter.[268] Vielmehr bedient sich die Mehrheit der akkreditierten ACs des Modells der so genannten virtuellen Zertifizierungsstellen. Dabei tritt das Unternehmen oder die öffentliche Stelle nach außen hin mit ihrem Namen als akkreditierter Zertifizierungsdiensteanbieter auf, aber die technische Infrastruktur und manchmal auch die ganz operationelle Unterstützung wird von einem anderen Zertifizierungsdiensteanbieter geliefert. Das ist so, weil das Betreiben eines Zertifizierungsdienstes eine so hohe Zuverlässigkeit und Fachkunde erfordert, die nicht ohne weiteres zu schaffen sind. Eine bedeutende finanzielle Investition ist deswegen von den Interessenten zu tätigen, nicht nur in Bezug auf die notwendigen hoch qualifizierten Mitarbeiter, sondern auch in Bezug auf den physischen Schutz der Gebäude[269], in denen die Zertifikate ausgestellt werden. Nicht alle, die als Zertifizierungsstelle am Markt auftreten wollen, sind bereit, dafür den entsprechenden Aufwand zu betreiben. Aus diesem Grund kann die vertragliche Zusammenarbeit zwischen dem akkreditierten Zertifizierungsdiensteanbieter (als Dienstleister) und dem Interessenten, der Zertifizierungsstelle werden möchte (als Dienstleistungsempfänger), auch nutzbringend sein. Zu erwägen wäre aber auch, dass eine zumutbare Entscheidung immer getroffen werden muss und bisweilen der einfache Erwerb von Zertifikaten im Markt noch viel nutzbringender sein kann als der Preis eines solchen Vertrags.

268 Von den zehn akkreditierten Zertifizierungsdiensteanbietern, die in Brasilien tätig sind, verfügen nur vier über ihr eigenes Trustcenter, nämlich die ACs: Serasa, Serpro, Certisign und Caixa Econômica Federal.

269 Zu beachten ist die Beschreibung von *Roßnagel* über die erforderlichen baulichen Sicherheitsmaßnahmen der Zertifizierungsstelle. Diese sollen verhindern, dass Unbefugte den Zugang zu Einrichtungen und Anlagen erhalten. Um das zu gewährleisten, sind Zäune, massive Wände, die bauliche Ausgestaltung, Einrichtungen der Zugangskontrolle, Sicherung von Trassen für Leitungen oder Abschirmungen gegen Abstrahlung erforderlich. Die Sicherheitsvorkehrungen sollen auch Bedrohungen durch Feuer oder Wasser reduzieren. In: *ders*., RMD, § 2 SigV 2001, Rn. 47.

2.2.7 Die Identifikationsstellen

Wie bereits erwähnt[270], spielen die Identifikations- oder Registrierungsstellen – in Brasilien Autoridades de Registro (AR) genannt – eine erhebliche Rolle in jeder PKI. Ihre Kernaufgabe ist die Identifizierung des Zertifikatsantragstellers durch eine zuverlässige Identitätsprüfung. Die Identifikation ist von so großer Bedeutung, dass der kleinste Fehler in dieser Tätigkeit erhebliche Schäden verursachen kann. Man kann sich vorstellen, was für Beschädigungen ein Betrüger herbeiführen könnte, der bei einer Identifikationsstelle ein akkreditiertes Zertifikat unter dem Namen eines anderen und durch die Vorlage gefälschter Dokumente erwirbt. In der ICP-Brasil könnte die Situation noch schlimmer werden, da in dieser Infrastruktur die Möglichkeit zur Einfügung einer Beschränkung ins Zertifikat auf bestimmte Anwendungen nicht vorgesehen ist. Weil der Antragsteller zur Erlangung eines Personalausweises immer einen persönlichen Kontakt mit der entsprechenden Behörde herbeiführen muss, soll eine Sicherungsinfrastruktur wie eine PKI auf so eine persönliche Mitwirkung nicht verzichten. Denn in der virtuellen Welt sind die digitale Signatur und das digitale Zertifikat viel mehr als ein Personalausweis. Die digitale Signatur gilt auch als Schriftformersatz und manchmal (wie z.B. in Deutschland) stützt sie auch einen Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung.

Art. 7 der MP 2200-2 bestimmt ganz klar, wie die Identitätsprüfung des Antragstellers durchzuführen ist: Die Beantragung von Signaturverfahren darf nur mit persönlichem Kontakt durchgeführt werden. Eine Ausnahme dieser Regel gibt es nur für den erneuten Antrag auf ein Zertifikat. Nur dann und gemäß Art. 3.2.2, b, Resolução Nr. 42, darf der Zertifikatsinhaber vor der Ablauffrist des noch gültigen Zertifikats ein neues Zertifikat durch ein elektronisch signiertes Formular beantragen (mittels einer akkreditierten Signatur). Diese Möglichkeit ist aber auf ein einziges Mal begrenzt. Nach dem Ablauf des zweiten Zertifikats muss dann wieder die persönliche Mitwirkung bei der Identifizierung und Übergabe stattfinden. Laut Art. 3.1.9.1, Resolução Nr. 42, haben die ARs die Identifizierung des Antragstellers anhand seines Personalausweises oder Reisepasses vorzunehmen. Für den Antrag auf ein Zertifikat der Stufe A4 oder S4[271] muss der Antragsteller ein weiteres Dokument mit Foto vorlegen. Dazu muss auch die gegenwärtige Anschrift des Antragstellers nachgewiesen werden.[272]

Die ARs müssen sich auch von der Aufsichtsbehörde akkreditieren lassen. Ihre Vorabprüfung wird aber nicht von ITI, sondern von einer dritten Prüfungsstelle

270 S. bereits in diesem Teil Gliederungspunkt 1.3.5.4.

271 Für die verschiedenen Zertifikatsstufen innerhalb der akkreditierten Verfahren, siehe unten Gliederungspunkt 2.2.9.1.2.1.

272 Diese Information steht nicht im brasilianischen Personalausweis.

durchgeführt.[273] Jeder Zertifizierungsdiensteanbieter muss entweder sich selbst auch als AR akkreditieren lassen oder einen Dritten, der die Identifikationsfunktionen an seiner Stelle übernehmen wird. Die Akkreditierung von mehreren an einen Zertifizierungsdiensteanbieter gebundenen Identifikationsstellen erleichtert die Verbreitung von Signaturverfahren. In einem Land mit kontinentalen Dimensionen wie Brasilien spielen diese Organisationen eine erhebliche Rolle bei der flächendeckenden Einführung der elektronischen Signaturen. Bis zum Jahr 2008 waren bereits 79 ARs mit über 670 Identifikationspunkten landesweit akkreditiert.[274]

Die Identifizierung des Antragstellers ist auch der richtige Moment zur Erfüllung einer Pflicht jedes Zertifizierungsdiensteanbieters und auch der Zertifizierungsstellen. Es handelt sich um die Pflicht zur Unterrichtung des Antragstellers. Im brasilianischen Signaturrecht gibt es keine besondere Vorschrift, die diese Pflicht im notwendigen Umfang vorsieht. Trotzdem ist sie immer ein bedeutender Baustein im Sicherheitsgebäude einer PKI. Obwohl nicht ausdrücklich im Signaturrecht festgelegt, kann diese Unterrichtungspflicht aus der allgemeinen Informationspflicht der Art. 6, III, Art. 14 und Art. 31 des brasilianischen Verbraucherschutzgesetzbuchs (Código de Defesa do Consumidor – CDC) hergeleitet werden. Art. 6, III, CDC bestimmt als grundlegendes Recht des Verbrauchers die angemessene und eindeutige Information über die verschiedenen Produkte und Dienstleistungen, mit einer genauen Spezifizierung angesichts ihrer Menge, Merkmale, Gestaltung, Qualität und Preis. Außerdem muss sich die Unterrichtung auch auf ihre Risiken erstrecken. Art. 14 CDC stellt eine Haftungsregel dar, die bestimmt, dass der Anbieter von Dienstleistungen ohne Rücksicht auf Unrecht und Verschulden dem Geschädigten den Schaden, der durch den Fehler des Dienstleisters verursacht wird, zu ersetzen ist. Bemerkenswert ist, dass der Dienstleister auch für Schäden wegen mangelnder Information über den Dienst und seine potentiellen Risiken haftet. Und Art. 31 CDC bestimmt, dass das Angebot und die Darstellung von Produkten und Dienstleistungen klare, korrekte, präzise und offensichtliche Informationen in der portugiesischen Sprache über die Merkmale, Eigenschaften, Menge, Gestaltung, Preis, Garantie, Haltbarkeitsdauer, Ursprung und über Risiken, die die Gesundheit und Sicherheit des Verbrauchers gefährden können, angeben müssen. Der Código de Defesa do Consumidor ist im Jahr 1990 in Kraft getreten, aber die allgemeine Informationspflicht gab es im brasilianischen Vertragsrecht auch schon vorher und wurde dort als Nebenpflicht betrachtet. Sie wurde ursprünglich von der Rechtsprechung entwickelt und aus dem allgemeinen Grundsatz von Treue und Glauben abgeleitet.[275] Diese

273 Die brasilianische Aufsichtsbehörde hat schon sieben Prüfungsstellen anerkannt. Die aktuelle Liste ist unter http://www.iti.gov.br/auditoria/Cadastro_de_Auditoria_Independente.pdf abrufbar.

274 Siehe hierzu http://www.iti.br/twiki/bin/view/Certificacao/Indicadores.

275 Siehe z.B. TJRGS, Ap. Cível 588042580, Rel. Des. Ruy Rosado de Aguiar Jr., v. 16.8.88.

Entwicklung wurde von den Studien von verschiedenen brasilianischen Juristen beeinflusst, die vertraut mit der deutschen zivilrechtlichen Literatur waren.[276]

2.2.8 Die sonstigen Diensteanbieter

Art. 5 MP 2.200-2 erwähnt die so genannten „prestadores de serviços habilitados", das heißt dritte Dienstleister, die Dienste anbieten, welche der Besteller aus finanziellen oder organisatorischen Gründen nicht in der Lage ist, selbst zu leisten. Ein weiterer Grund, Dienste von Dritten in Anspruch zu nehmen, kann der Mangel an Erfahrung, Fachkunde oder an geeigneter Ausrüstung darstellen. Dies entspricht dem Fall eines virtuellen Zertifizierungsdiensteanbieters. Diese wollen zwar am Markt als Zertifikatsaussteller auftreten, besitzen jedoch in der Regel kein eigenes Trustcenter sowie Personal mit der notwendigen Fachkunde im PKI-Bereich. Es bleibt dann die Möglichkeit, auf der Grundlage einer vertraglichen Absprache, mit Dritten technisch-organisatorische Dienstleistungen zu vereinbaren.

Gemäß Art. 2.1.3.1 Resolução Nr. 47 werden auch die „prestadores de serviços de suporte" akkreditiert. Ihre mögliche Dienstleistungen können: 1) die Bereitstellung der physischen Infrastruktur sowie der logischen Hardware- und Software-Komponenten, 2) die Bereitstellung von Mitarbeitern mit der notwendigen Fachkunde, und 3) die Bereitstellung der physischen Infrastruktur sowie der Hardware- und Software-Komponente sowie von Mitarbeitern mit der notwendigen Fachkunde sein. Der Besteller muss sich für eine dieser drei Varianten entscheiden und bei der Antragstellung für seine Akkreditierung erklären, welcher „prestador de serviços de suporte" mit ihm verbunden ist.

2.2.9 Die Signaturverfahren

Anders als das deutsche Signaturgesetz kennt das brasilianische Signaturrecht nur zwei Signaturverfahren: Die akkreditierte digitale Signatur und die sonstigen Signaturen. Damit wird Nachfragern die Möglichkeit geboten, sich anwendungs- und risikoadäquat zwischen zwei Kategorien von Signaturverfahren zu entscheiden. Das akkreditierte Verfahren wird ausführlich reguliert. Die sonstigen Signaturen dagegen werden zwar im Gesetz anerkannt, aber nicht weiter geregelt.

276 Unter anderen ist auf die Namen von *Francisco Cavalcanti Pontes de Miranda* und *Clóvis Veríssimo do Couto e Silva* zu verweisen.

2.2.9.1 Die akkreditierten Verfahren

Auf der höchsten Stufe stehen die akkreditierten Verfahren. Die konstitutiven Anforderungen dieser Verfahren werden im Gesetzestext nicht übersichtlich beschrieben wie zum Beispiel im deutschen Signaturgesetz, das klar und praktisch die Anforderungen des qualifizierten Zertifikats in einer einzigen Vorschrift festlegt. Die MP 2.200-2 regelt eigentlich nur die Anforderungen von akkreditierten Verfahren. Sie werden teilweise schon im Gesetzestext festgesetzt und viele andere Anforderungen sind in der Vorschrift Resolução Nr. 41 des Regulierungsausschusses namens „Requisitos mínimos para as políticas de certificados“[277] enthalten. Dadurch sind die Voraussetzungen der akkreditierten Verfahren in ihrer Gesamtheit nicht sehr übersichtlich und auch nicht ohne weiteres erkennbar.

2.2.9.1.1 Das akkreditierte digitale Zertifikat

Wie schon dargestellt ist die brasilianische Infrastruktur nicht technikneutral. Darum werden im Gesetz und in den Nebenregelungen keine abstrakten Begriffe wie „Zertifikate“ oder „elektronische Signaturen“ definiert, sondern direkt die allgemeinen Anforderungen des akkreditierten Verfahrens bestimmt.

2.2.9.1.1.1 Die Zertifikatstypen

Die Resolução Nr. 41 des Regulierungsausschusses bestimmt die Mindestanforderungen eines akkreditierten Zertifikats. Erstens beschreibt die Regel die verschiedenen Zertifikatstypen die von der AC erstellt werden können.[278] Dies sind acht verschiedene Typen, verteilt auf zwei Gruppen. In einer Gruppe sind die Zertifikate ohne Verschlüsselungsfunktion, das heißt Zertifikate, die nur die Authentizitätsfunktion besitzen, die so genannten „digitalen Signaturzertifikate“ (certificados de assinatura digital oder Zertifikate des Typs A). In der anderen Gruppe sind die digitalen Zertifikate mit Verschlüsselungsfunktionen[279], die hauptsächlich dem Zweck der Vertraulichkeit dienen (certificados de sigilo oder Zertifikate des Typs S).[280] Diese Unterteilung wurde so getroffen, damit die verschiedenen Funktionen eines Zertifi-

277 Minimalen Anforderungen der Certificate Policy.

278 Art. 1.1.3.

279 Über die Verbreitung und Benutzung von Verschlüsselungsverfahren hat in Brasilien keine umfangreiche Diskussion stattgefunden, wie etwa in Deutschland, in Frankreich oder in den USA. Näher zum Thema Kryptokontroverse: *Bizer*, DuD 1997, 203; *Hamm*, DuD 1997, 186; *Hortmann*, DuD 1997, 214; *Blaze*, DuD 1997, 209.

280 Es ist auch zu erwähnen, dass die Vertraulichkeit auch durch die Verschlüsselung der Nachricht mit dem öffentlichen Schlüssel des Empfängers gewährleistet werden kann.

kats beliebig vom Nutzer getrennt gewählt werden können. Für die Zertifikate mit Verschlüsselungsfunktion besteht grundsätzlich die Möglichkeit der Wiedergewinnung von Schlüsseln (Key Recovery), besonders für den Zweck der Reaktion auf den möglichen Verlust von privaten Schlüsseln.[281] Wenn das geschieht, ist der Zugang zum verschlüsselten Dokument ohne die Möglichkeit der Wiedergewinnung des privaten Schlüssels unmöglich. Daher hat der Schutz des Dokuments vor unautorisierten Dritten seinen Preis, indem bei Verlust oder Nicht-Verfügbarkeit des Schlüssels der Inhaber der verschlüsselten Daten seine eigene Information nicht wiedergewinnen kann.[282] Deswegen kann die Möglichkeit eines Key Recovery von großer Bedeutung sein, besonders für die Unternehmen und öffentlichen Stellen, die sich für die Verschlüsselung von Informationen entscheiden.[283]

Das vorgesehene Verfahren zur Wiedergewinnung von Schlüsseln innerhalb des brasilianischen Signaturrechts ist das so genannte Key Backup.[284] Dabei wird eine Sicherheitskopie des privaten Schlüssels erstellt und diese entweder vom Signaturschlüsselinhaber selber gespeichert oder bei dem entsprechenden Zertifizierungsdiensteanbieter hinterlegt. Die Wiedergewinnung privater Schlüssel von Zertifikaten für elektronische Signaturen, die der Authentifizierung und Integrität von elektronischen Dokumenten dienen, ist allerdings von der Regulierung ausdrücklich ausgeschlossen.[285] Denn diese haben vor allem Identitäts-, Echtheits- und Beweisfunktionen, die erheblich beeinträchtigt werden können, wenn eine Kopie des privaten Schlüssels auch bei einem Dritten gespeichert wird. So eine Möglichkeit würde an sich schon zu Unsicherheiten führen, denn bei einer Streitigkeit um die Authentizität einer elektronischen Willenserklärung wäre die Behauptung des Signaturschlüsselinhabers, er habe das Dokument nicht signiert, von vornherein nicht völlig auszuschließen, was die Rechtslage deutlich komplizieren könnte.

Jede Untergruppe von Zertifikaten enthält vier verschiedene Zertifikatsstufen. Die Zertifikate werden angesichts bestimmter Aspekte ihrer Sicherheitsattribute in zunehmender Ordnung gruppiert. Die folgende Tabelle gibt die Merkmale der verschiedenen Zertifikatsstufen an:

281 Diese Möglichkeit ist im zweiten Satz des Art. 6.2.4.2, Resolução Nr. 41 vorgesehen.

282 *Blaze*, DuD 1997, 209.

283 *Wiesner*, DuD 2000, 703.

284 Neben dem Key Backup, sind auch die Verfahren von Key Escrow, Trusted Third Party und Key Encapsulation, möglich. Näher zum Thema: *Wiesner*, DuD 2000, 698.

285 Erster Satz Art. 6.2.4.2, Resolução Nr. 41.

Zertifikatstyp	Kryptographischer Schlüssel			Maximale Gültigkeit (Jahr)	Häufigkeit der Erstellung der Sperrliste (in Stunden)	Maximale Zeit für die Sperrung (in Stunden)
	Länge (bits)	Erzeugungsverfahren	Speichermittel			
A1 und S1	1024	Software	Speichermittel mit Passwort oder biometrischem Merkmal geschützt und von einer Software verschlüsselt.	1	6	12
A2 und S2	1024	Software	Smart Card oder Token ohne Prozessor, mit Passwort oder biometrischem Merkmal geschützt.	2	6	12
A3 und S3	1024	Hardware	Smart Card oder Token, beide mit Prozessor zur Schlüsselgenerierung und mit Passwort oder biometrischem Merkmal geschützt.	3	6	12
A4 und S4	2048	Hardware	Smart Card oder Token, beide mit Prozessor zur Schlüsselgenerierung und mit Passwort oder biometrischem Merkmal geschützt.	3	6	12

2.2.9.1.1.2 Speichermittel

Was das Speichermittel betrifft, sieht man in der Tabelle, dass es beim Zertifikat der Kategorie A1 prinzipiell möglich ist, den privaten Schlüssel beispielsweise auf einer Festplatte zu speichern. Als 2001 die brasilianische Infrastruktur für öffentliche Schlüssel implementiert wurde, galt diese Möglichkeit ausdrücklich als vorläufige Maßnahme. Der Grund dafür bestand darin, dass manche Anwendungen, wie das damals neu eingeführte brasilianische Zahlungssystem, unbedingt mit einem sichereren Authentizitätsmechanismus als den vorhandenen Verfahren verwendet werden sollten. Allerdings waren die Speicherkarten nicht flächendeckend verbreitet. Dieser unsichere Weg innerhalb einer erwünschten Sicherheit ist dann gewählt worden. Was ursprünglich nur provisorisch gelten sollte, ist aber noch immer in Kraft. Das Problem dieser Lösung liegt in der fehlenden Möglichkeit der alleinigen Kontrolle über den Signaturschlüssel durch den Zertifikatinhaber. Softwarelösungen alleine sind nicht geeignet, um die notwendige Sicherheit des Nutzers zu schaffen.[286] Hierzu wären zusätzliche Schutzmechanismen erforderlich, wie das Einschließen der Diskette in einem Safe oder das Isolieren des PCs ohne Netzanschluss in einem Zimmer, zu dem nur der Schlüsselinhaber Zutritt hat.[287] Das alles wäre realisierbar, aber unpraktisch für den Nutzer.

2.2.9.1.1.3 Angaben des akkreditierten Zertifikats

Da Zertifikate den Zusammenhang zwischen dem öffentlichen Schlüssel und einem Teilnehmernamen herstellen, ist auch die Bestimmung der obligatorischen und gegebenenfalls fakultativen Angaben eines Zertifikats eine zentrale Vorschrift jeder PKI-Regulierung. Die Resolução Nr. 41, Artikel 7.1 regelt die Anforderungen zu Struktur und Inhalt von digitalen Zertifikaten. Als obligatorisches Zertifikatformat innerhalb der akkreditierten Verfahren ist der Standard X.509 der *International Telecommunication Union* in der Version 3, wie in RFC 3280 definiert.

Dadurch, unabhängig vom Zertifikatstyp, muss ein Zertifikat folgende Informationen enthalten: 1) den Namen des Signaturschlüssel-Inhabers, 2) den Namen des Ausstellers, 3) Informationen zu Beginn und Ende der Gültigkeitsdauer des Zertifikats, 4) den zugeordneten öffentlichen Schlüssel, 5) Geburtsdatum des Signaturschlüssel-Inhabers (falls es sich um ein Zertifikat für eine natürliche Person handelt) und 6) Internetadresse der Sperrliste des Ausstellers.

Was die persönlichen Daten des Signaturschlüsselinhabers betrifft, sind nur der vollständige Name und das Geburtsdatum erforderlich. Möglich ist auch die Eintragung von mehreren Identifikationsnummern in das Zertifikat, um sich gegenüber den verschiedenen Behörden oder Berufskammern zu identifizieren. Dies können

286 Hierzu *Geis*, MMR 2000, 668.

287 *Roßnagel*, MMR 2003, 165.

zum Beispiel die Nummern von folgenden Identifikationsmitteln sein: Personalausweis, Sozialversicherungsausweis, Steuerpflichtigenausweis, Stimmberechtigtenausweis oder Rechtsanwaltsausweis. Alle oder manche dieser nicht obligatorischen Angaben können in das Zertifikat nach Wunsch des Antragstellers eingetragen werden. Bei der Beantragung des Zertifikats füllt der Interessent ein Formular aus, worin er erklärt, welche von diesen personenbezogenen Daten ins Zertifikat eingetragen werden sollen.[288] Dabei wird er aber auch darauf hingewiesen, dass je weniger Daten im Zertifikat enthalten sind, desto eingeschränkter seine Verwendungsmöglichkeiten sein können. Dies erfolgt angesichts der Tatsache, dass Anwendungen wie die elektronische Steuererklärung oder die für den Zugang zu Sozialversicherungsinformationen des Bürgers seit langem – bereits vor Einführung der Signaturverfahren – nur anhand der entsprechenden Ausweisnummer bei der Behörde möglich waren.

2.2.9.1.2 Aufbewahrung akkreditierter Zertifikate

Gemäß Art. 6.3.1 Resolução Nr. 42 müssen akkreditierte Zertifizierungsdiensteanbieter sowohl ihre Zertifikate und die Zertifikate ihrer Kunden als auch die ausgestellten Sperrlisten nach dem Ablauf der entsprechenden Zertifikate aufbewahren. Diese Pflicht ist unbefristet zu erfüllen, damit im Laufe der Zeit Signaturen überprüfbar bleiben. Ursprünglich galt in der ICP-Brasil eine Aufbewahrungspflicht von 30 Jahren ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates endete. Strenger hingegen ist die Vorschrift geworden, welche die unbeschränkte Überprüfbarkeit signierter Dokumente gewährleistet.

2.2.9.1.3 Sperrung von Zertifikaten

In der obigen Tabelle sieht man auch, dass der Zertifizierungsdiensteanbieter die Sperrung der Zertifikate innerhalb einer maximal festgelegten Zeit durchzuführen hat. Diese Zeit beträgt zwölf Stunden für alle Zertifikatstypen, berechnet ab dem Eingang des Sperrantrags.[289] In der geltenden Regelung ist schon ein bedeutender Fortschritt im Vergleich zu der aufgehobener Bestimmung der Resolução Nr. 7, die Reaktionszeiten von 18 bis 72 Stunden vorsah, zu sehen. Als Gegengewicht zu der Vorschrift über die Sperrfrist von maximal zwölf Stunden sieht der Art. 4.4.3.5 Resolução Nr. 42 vor, dass die AC für den Missbrauch des Signaturschlüssels in der Zeit zwischen dem Eingang des Sperrantrags und dem Eintritt der Sperrwirkung haftet. Diese Regel schützt den Signaturschlüsselinhaber und versucht die möglichen negativen Auswirkungen einer solchen maximalen Zeitspanne von 12 Stunden für die Sperrung der Zertifikate zu vermindern.

288 Gemäß Art. 3.1.9.2.2. der Resolução Nr. 42.

289 Gemäß Art. 4.4.3.3 der Resolução Nr. 42.

2.2.9.1.3.1 Sperrlisten versus OCSP-Dienst

Der Abschluss des Sperrverfahrens stellt die Eintragung des zu sperrenden Zertifikats in eine Sperrliste dar. Dies folgt aus Art. 4.4.3.2, d, der Resolução Nr. 42. In dieser Liste werden alle Zertifikate eines Zertifizierungsdiensteanbieters eingetragen, die als ungültig betrachtet werden sollen. Solche Listen werden Negativlisten genannt, denn sie enthalten nur die gesperrten Zertifikate. Die Integrität und Authentizität der Sperrliste wird durch eine Signatur des Zertifizierungsdiensteanbieters gewährleistet. Bei der Anwendung eines Signaturverfahrens wird dann zunächst die Signatur vom Empfänger geprüft und zusätzlich festgestellt, ob das Zertifikat nicht in der dazugehörigen gültigen Sperrliste verzeichnet ist. Und nur wenn das Zertifikat nicht in dieser Liste eingetragen ist - deswegen Negativliste - wird es akzeptiert.

Das Problem der Sperrlisten ist in der Tatsache begründet, dass sie in der Regel nur in regelmäßigen Abständen erstellt werden. Wird das Beispiel der hier erörterten brasilianischen Infrastruktur betrachtet, nach welchem die Sperrlisten in Abständen von 12 Stunden aktualisiert und veröffentlicht werden dürfen, dann wird klar, wie unsicher ein solches Modell sein kann. Beispielsweise hat der Zertifizierungsdiensteanbieter noch 11 Stunden um das Sperrverfahren abzuschließen, wenn der Antrag auf Sperrung eines oder mehrerer Zertifikate bereits eine Stunde nach der letzten Veröffentlichung erfolgte. Dabei ist der Sperrwunsch dem Zertifizierungsdiensteanbieter bekannt, aber nicht veröffentlicht. Falls keine weiteren Listen während des Zeitraumes der Gültigkeit erstellt werden, kann die Überprüfung des Zertifikats zu falschen Ergebnissen führen.[290]

Als Alternative zu den Sperrlisten sind die Positivlisten, wie etwa ein Online-Auskunftsdienst nach dem Online Certificate Status Protocol (OCSP), zu sehen. Diese sind durch allgemeine Richtlinien von der IETF durch die RFC 2560 spezifiziert worden. Wie der Name schon verrät, ermöglicht dieser Auskunftsdienst dem Signaturempfänger, den aktuellen Status des Zertifikats zu verifizieren. Bei einer Anfrage werden die Aussagen *gültig*, *gesperrt* oder *nicht ausgestellt* vom Dienst gegeben. Ihr besonderes Merkmal und ihr Vorteil ist dann die Aktualität. Bei der Verifizierung des Zertifikats wird nicht nur ermittelt, ob es zu dem bestimmten Zeitpunkt gesperrt war, sondern auch ob es überhaupt existierte (Existenznachweis), was für die langfristige und nachhaltige Überprüfung von Zertifikaten von Bedeutung ist.[291] Dieser Dienst soll allmählich eingeführt werden, auch um den „langsamen und umständlichen Mechanismus der Certificate Revocation Lists (CRLs) abzulösen“[292]. Im Vergleich zu den Sperrlisten ist zu erwähnen, dass diese normalerweise einen großen Umfang von Zertifikaten beinhalten. Dieses Informationsvolumen wird, angesichts der im Laufe der Zeit steigenden Anzahl an Sperrungen, mit der Zeit immer umfangreicher. Beim OCSP-Dienst, der auf einem Protokoll basiert und nicht

290 *Berger*, DuD 1999, 209.

291 *Nitschke*/*Dahm*, DuD 2005, 142; *Fischer-Dieskau*, 2006, 209.

292 *Nitschke*/*Dahm*, DuD 2005, 142.

einfach als Datenformat definiert ist (wie die CRLs), fragt eine Anwendung nach dem Sperrstatus zu einem oder mehreren Zertifikaten auf einmal.[293] Darauf reagiert der Dienst mit einer kurzen elektronisch signierten Antwort zu jedem angefragten Zertifikat.

Die Resolução Nr. 42, Art. 4.4.3.2, d, sieht die Aufstellung von Sperrlisten als Pflicht für die akkreditierten Zertifizierungsdiensteanbieter vor, indem sie bestimmt, dass das Widerrufsverfahren eines Zertifikates mit seiner Eintragung in einer Sperrliste und im Fall der Anwendung eines OCSP-Dienstes mit der Aktualisierung der Information über das Zertifikat endet. Dieser Artikel, in Verbindung mit dem Art. 2.1, j,[294] der Resolução Nr. 42, lässt das fakultative Merkmal der Durchführung eines OCSP-Dienstes durch die Zertifizierungsdiensteanbieter zu. Die Pflicht der Zertifizierungsstellen im Rahmen der ICP-Brasil ist allerdings lediglich das Führen einer Sperrliste.

2.2.9.1.3.2 Form und Bearbeitung des Sperrantrags

Die Form des Sperrantrags und des Authentisierungsverfahrens bleibt der Zertifizierungsstelle überlassen. Geregelt ist lediglich die Pflicht zur Bereitstellung eines Dienstes, der „leicht und jederzeit" die Sperrung des Zertifikats durch die Berechtigten ermöglicht.[295] Vorgesehen ist auch die Identifizierung des Antragstellers und die Dokumentierung und Archivierung des Verfahrens sowie die Begründung zur Sperrung durch den Zertifizierungsdiensteanbieter. Die AC Certisign[296] und die AC Serasa[297] beispielsweise verwenden ein Sperrverfahren, das durch ein Webformular durchgeführt wird. Der Zertifikatinhaber benutzt hierzu als Authentisierungsmittel einen Satz als Passwort, der ihm bei der Zertifikatserzeugung von der Zertifizierungsstelle übergeben wird. Fraglich ist, ob die Konkretisierung des Sperrverfahrens dem Zertifizierungsdiensteanbieter überlassen bleiben sollte, obwohl es sich um ein derart entscheidend wichtiges Verfahren innerhalb einer regulierten PKI handelt.

2.2.9.1.4 Zertifikatsinhaber

Gemäß Artikel 1.1.5 der Resolução Nr. 41 ist die Zuordnung eines Zertifikats zu natürlichen Personen, juristischen Personen, Automaten und funktionalen Einheiten,

293 *Nitschke*/*Dahm*, DuD 2005, 143.

294 Der Artikel bestimmt, dass dem Zertifizierungsdiensteanbieter die Ausstellung, Verwaltung und Veröffentlichung einer Sperrliste obliegt, und wenn dies der Fall ist, soll er die on-line Anfrage über die aktuelle Sperrauskünfte der Zertifikate zur Verfügung stellen.

295 Art. 4.4.3.1, Resolução Nr. 42.

296 S. dazu http://icp-brasil.certisign.com.br/repositorio/index.htm.

297 S. dazu http://publicacao.certificadodigital.com.br/repositorio/pc/politica-a2.pdf.

wie Servern, möglich. Zertifikate für juristische Personen und Automaten können eine wichtige Rolle spielen, wenn man bedenkt, dass Attributszertifikate im brasilianischen Signaturrecht nicht vorgesehen sind. Somit können diese Zertifikate einen Beitrag zur transparenten Unterscheidung zwischen persönlichen und automatisierten Signaturen leisten. Denn es ist zu erwarten, dass die Mehrzahl der elektronischen Signaturen nicht durch Personen, sondern in automatisierten Verfahren erzeugt wird.[298] Von großer Bedeutung sind auch die so genannten Serverzertifikate, die eine sichere verschlüsselte Verbindung zwischen E-Commerce Webserver und Kunden ermöglichen und gleichzeitig als „Ausweis" der Internetadresse dienen, damit der Kunde sicher ist, dass er sich auf der richtigen Webseite befindet und nicht auf einer gefälschten. Obwohl in solchen Zertifikaten der Name einer natürlichen Person nicht eingetragen wird, muss immer eine Person für ihre Nutzung verantwortlich sein, da letztlich immer eine natürliche Person über den Einsatz von Rechnern entscheidet. Diese muss ein entsprechendes Formular unterschreiben, indem sie die Verantwortung für die Nutzung des Zertifikats übernimmt.

Art. 2.1.3 Resolução Nr. 41 stellt eine Reihe von Anforderungen an den Zertifikatsinhaber. Vordergründig muss er alle notwendigen Informationen zu seiner Identifikation in einer richtigen und präzisen Weise abgeben (Art. 2.1.3, a). Ferner muss der Signaturschlüssel-Inhaber Sicherungsmaßnahmen treffen, welche die Geheimhaltung seines privaten Schlüssels gewährleisten (Art. 2.1.3, b). Darüber hinaus sind das Zertifikat sowie der private Schlüssel gemäß den Bestimmungen des Dokuments „Política de Certificados" vom Zertifikatsinhaber zu benutzen (Art. 2.1.3, c). Der Zertifikatsinhaber hat zudem Kenntnis von seinen Rechten und Pflichten in den Dokumenten „Política de Certificados" und „Declaração de Práticas de Certificação" zu nehmen (Art. 2.1.3, d). Schließlich hat er den Zertifizierungsdiensteanbieter von einer Kompromittierung seines privaten Schlüssels zu informieren und die Sperrung des entsprechenden Zertifikats zu beantragen (Art. 2.1.3, d).

Nach dem Wortlaut der Vorschrift („obrigações") sind die Anforderungen an den Zertifikatsinhaber als Rechtspflichten zu verstehen.[299] Fraglich ist aber, ob in diesen Fällen die Anforderungen an den Zertifikatsinhaber tatsächlich Rechtspflichten darstellen. Hierbei zeigt sich jedoch, dass die meisten Anforderungen lediglich Verhaltensanforderungen darstellen. Freilich sind die Anforderungen zur Geheimhaltung des privaten Schlüssels sowie zur Kenntnisnahme und Beachtung der Dokumente „Política de Certificados" und „Declaração de Práticas de Certificação" Obliegenheiten (ônus), deren Missachtung dem Verpflichteten Nachteile bringen. Das gleiche betrifft die Maßnahmen zur Informierung und Beantragung einer Sperrung bei der Kompromittierung des privaten Schlüssels. Unternimmt der Signaturschlüssel-Inhaber in diesem Fall keine Maßnahme, um einen Antrag auf Sperrung seines Zertifikats gegenüber dem Zertifizierungsdiensteanbieter zu übermitteln, dann erlei-

298 *Roßnagel*, DuD 1997, 79.

299 Die Formulierung des Art. 2.1.3 Resolução Nr. 41 benutzt den für den Fall irreführenden Begriff „obrigação" (Schuldigkeit).

det er alleinig die Schäden angesichts seines passiven Verhaltens. Der Unterschied zwischen Pflicht („dever“) und Obliegenheit („ônus“) ist, dass die Letztere anders als die Rechtspflicht im Verhältnis zum Verpflichteten selbst und nicht gegenüber dem Gläubiger besteht.[300] Die Obliegenheit hat keine Auswirkung auf das Schuldverhältnis und der Obliegenheitsbelastete kann nicht zum geforderten Verhalten gezwungen werden. Darüber hinaus begründet die Nichtbeachtung einer Obliegenheit keine Schadenersatzpflicht, sondern nur die Verschlechterung einer günstigen Rechtsposition.[301]

Anders zu behandeln ist die Anforderung zur korrekten und präzisen Informationsangabe bei der Identifikation des Antragstellers für die Ausstellung des Zertifikats. Hierbei kann eine vorsätzliche inkorrekte Angabe von Daten zur Zertifikatsausstellung die Voraussetzungen des Tatbestandes des Art. 299 „Código Penal“ (Strafgesetzbuch) erfüllen. Diese Vorschrift sieht das Verbrechen „Falsidade Ideológica“ vor. Danach wird, wer beim Ausstellen eines privaten oder öffentlichen Dokuments eine unechte Erklärung abgibt – oder es unterlässt für den Zweck des Dokuments erhebliche Erklärungen abzugeben –, mit einer Freiheitsstrafe von ein bis fünf Jahren und Geldstrafe bestraft.[302] Somit begründet die Anforderung des Art. 2.1.3, a, Resolução Nr. 41 für den Antragsteller eine Rechtspflicht, wahre Daten und Informationen dem Zertifizierungsdiensteanbieter zum Zweck der Zertifikatsausstellung abzugeben.

2.2.9.1.5 Schlüsselpaargenerierung

Im Public Key System ist der Prozess der Schlüsselpaargenerierung besonders kritisch. Im Interesse aller Beteiligten sollen die Schlüssel so sicher wie möglich erzeugt werden. Falls in diesem Prozess der unberechtigte Zugriff auf den privaten Schlüssel gelingt, kann der Duplikatinhaber gültige Signaturen erzeugen und somit unautorisierte Handlungen im Namen des berechtigten Signaturschlüsselinhabers vornehmen.

Es gibt grundsätzlich zwei Möglichkeiten für die Schlüsselgenerierung: Einmal beim Interessenten selbst oder durch den Zertifizierungsdiensteanbieter (Trustcenter). Beide Varianten haben Vor- und Nachteile. Wenn das Trustcenter die Schlüssel erzeugt, kann der Teilnehmer in Streitfällen argumentieren, das Trustcenter hätte seinen privaten Schlüssel kopiert und missbraucht.[303] Für Signaturschlüssel, die hauptsächlich Authentizitätsfunktionen erfüllen, kann dieser Einwand nicht ausge-

300 *Miranda* 2000, 457.

301 *Fischer-Dieskau* 2006, 52 ff.

302 Der Tatbestand setzt zudem den Vorsatz des Täters voraus, das Recht eines anderen zu beeinträchtigen, ein Schuldverhältnis zu begründen oder die Wahrheit über eine rechtserhebliche Tatsache zur Täuschung zu verändern.

303 *Federrath*, DuD 1997, 98.

schlossen werden. Für Schlüssel, deren Hauptaufgabe in der Verschlüsselungsfunktion liegt, ist die Schlüsselerzeugung in Trustcenter nicht so problematisch. Die Schlüsselerzeugung beim Teilnehmer hat ihren größten Vorteil darin, dass es keinen Raum für solche Behauptungen gibt, denn der Zertifizierungsdiensteanbieter bekommt lediglich den öffentlichen Schlüssel und erstellt mit ihm das Zertifikat. Doch die Schlüsselgenerierung beim Anwender kann aber deshalb kritisch sein, weil er in der Regel nichts von Computersicherheit versteht. Es kann offen bleiben, welche Schlüsselgenerierungsprogramme er verwendet hat und wie er seinen Rechner gegen Angriffe von virulenter Software und Bedrohungen aus dem Internet sichert.[304] Entscheidend ist aber, dass die Generierung von Schlüsseln durch technische Komponenten realisiert werden kann. Dies gewährleistet einerseits die Einmaligkeit und Geheimhaltung der privaten Schlüssel und schließt andererseits seine Speicherung außerhalb des Speichermittels aus.[305] Das Beispiel hierfür ist die bereits erwähnte Chipkarte, auf der das Schlüsselerzeugungsverfahren ausschließlich erfolgt, geschützt vor fremden Zugriff.

Das brasilianische Signaturrecht hat ausdrücklich die erste Alternative gewählt, das heißt, schon im einzigen Paragraphen des Art. 6 der MP 2.200-2 wird vorgesehen, dass das Schlüsselpaar „immer von seinem Inhaber erzeugt wird“. Die Bedeutung dieser Norm lässt sich in der Tatsache erkennen, dass sie nicht erst durch die Befugnisse des Regulierungsausschusses eingeführt wurde, sondern bereits schon mit der MP 2.200-2 und daraus folgend mit höheren Status, erlassen wurde. Dabei muss sich aber der Zertifizierungsdiensteanbieter überzeugen, dass der Antragsteller die Signaturerstellungseinheit mit dem zugehörigen privaten Schlüssel zu dem im Zertifikat aufgeführten öffentlichen Schlüssel besitzt. Der Nachweis des Besitzes des privaten Schlüssels kann laut Art. 3.1.9 Resolução Nr. 42 durch das im RFC 2510 beschriebenem *Proof of Possession* - Verfahren durchgeführt werden. Der RFC 2510 empfiehlt im Art. 2.3.1 das Signieren eines Dokuments seitens des Zertifikatsantragstellers, das dem Zertifizierungsdiensteanbieter den Nachweis des Besitzes ermöglicht. Handelt es sich um Schlüssel mit Verschlüsselungsfunktionen, kann der Zertifikatsantragsteller dem Zertifizierungsdiensteanbieter den entsprechenden privaten Schlüssel bereitstellen. Hierbei wäre eine andere Möglichkeit, den Besitz des privaten Schlüssels nach Art. 2.3.2 RFC 2510 durch die Entschlüsselung einer mit dem öffentlichen Schlüssel verschlüsselten Datei nachzuweisen.

2.2.9.1.6 Sichere Produkte

Auch von großer Bedeutung für die Sicherheit der Signaturverfahren sind die Produkte für die akkreditierten Signaturen. Diese Produkte beziehen die Signaturspeicherungs- und Signaturerstellungseinheiten, Produkte für die Prüfung und Anzeige

304 *Nehl*, DuD 1997, 101.

305 *Nehl*, DuD 1997, 101.

der Ergebnisse von Signaturen und Zertifikaten und Softwareprodukte für die Darstellung von zu signierenden Daten ein.

2.2.9.1.6.1 Signaturspeicherungs- und Signaturerstellungseinheiten

In der brasilianischen Regulierung sind drei mögliche Signaturerstellungseinheiten vorgesehen.[306] Die erste, für Zertifikatstyp A1, wird von einer Software erzeugt und das Speichermittel wird mit Passwort oder biometrischem Merkmal geschützt und von einer Software verschlüsselt. Das bedeutet, dass der private Schlüssel für die Zertifikate dieser Kategorie beispielsweise auf einer Festplatte oder Stick gespeichert werden kann. Die zweite und dritte Variante von Signaturerstellungseinheiten sind die Sicherheitstoken und Chipkarten, beide mit eingebauten Prozessoren.[307]

Darüber hinaus ist der private Schlüssel nach Art. 6.1.1.4 Resolução Nr. 41 verschlüsselt, mittels symmetrischen Algorithmus der Spezifikationen „Padrões e algoritmos criptográficos da ICP-Brasil", zu generieren[308]. Gemäß Art. 6.1.1.5 Resolução Nr. 41 muss der private Schlüssel während der Erzeugung und während der Übertragung auf einen Datenträger verschlüsselt transportiert werden. Ferner muss die Signaturspeicherungseinheit sicherstellen, dass der private Schlüssel einmalig ist, sowie geheim gehalten wird und dass er in einem relevanten Zeitraum aus dem öffentlichen Schlüssel nicht berechnet werden kann. Des Weiteren darf der private Schlüssel nicht für Unberechtigte zugänglich sein.

2.2.9.1.6.2 Komponenten für die Anzeige der zu signierenden Daten

Die Komponenten für die Dokumentenanzeige unterliegen ebenso als tragende Säule beim Benutzen von elektronischen Signaturen sehr hohen Sicherheitsanforderungen. Neben den Eigenschaften des Anscheins der Echtheit und Unversehrtheit ist auch eine gewisse Sicherheit der richtigen Präsentation der zu signierenden Daten von Bedeutung. Der Signierer muss eindeutig wahrnehmen, auf welche Daten sich die abzugebende Signatur bezieht. Elektronische Dokumente können nicht wie Papierdokumente unmittelbar, sondern nur über Bildschirmanzeigen oder Ausdrucke angesehen werden. Dabei kann es geschehen, dass der Signierer Daten signiert, die er nicht signieren wollte.[309] Gründe hierfür wären technische Fehler und Manipulati-

306 Siehe hierzu bereits in diesem Teil Gliederungspunkt 2.2.9.1.2.1.

307 Hierzu die Tabelle oben im Gliederungspunkt 2.2.9.1.2.1.

308 Veröffentlicht unter www.iti.br.

309 In der deutschen Literatur wird auf das so genannte „Präsentationsproblem" verwiesen. Pordesch, DuD 2000, 89, bezeichnet es als der Fall, bei dem „mindestens zwei Präsentationen derselben signierten Daten so voneinander abweichen, dass sie von Menschen unterschiedlich interpretiert werden".

onen der zum Präsentieren genutzten Anwenderinfrastruktur, aber auch Varianten der verwendeten Systeme und deren Bedienung. Beispielsweise könnte ein Angreifer mit der Einstellung oder Manipulation der für die Anzeige notwendigen Komponente erreichen, dass Dokumententeile nicht oder nicht richtig sichtbar sind.[310] Dies kann bereits auch durch die Einstellung von Bildschirmfarben der Anwendungsprogramme erfolgen, wobei besonders formatierte Textteile unsichtbar vorgezeigt werden können.[311]

Darum sind in diesem Zusammenhang Maßnahmen zu treffen, die das Risiko der mehrdeutigen Präsentationen reduzieren. Eine dieser Maßnahmen ist die Standardisierung von Datenformaten, die die Präsentation festlegen (Präsentationsformat).[312] Dadurch soll erreicht werden, dass der Signierer sowie der Verifizier aus signierten Daten dieselbe Willenserklärung ermitteln kann. Festgelegt werden sollen Spezifikationen bezüglich des Layouts (Anordnung, Zeichenformate), der Fenstergröße und anderen äußeren Aspekten der Darstellung und der Funktionen (besonders die zur Navigation und Inhaltserschließung).[313]

Im brasilianischen Signaturrecht werden keine Komponenten für die Dokumentenanzeige gefordert.

2.2.9.1.6.3 Komponenten für die Überprüfung signierter Daten

Signaturanwendungskomponenten für die Überprüfung signierter Daten spielen ebenfalls eine bedeutende Rolle in der Sicherheitsinfrastruktur. Wenn elektronische Signaturen nicht oder nicht richtig geprüft werden, bleiben Fälschungen und Verfälschungen unentdeckt.[314]

Was die Anwendung von Komponenten für die Überprüfung zu signierender Daten betrifft, legt das brasilianische Signaturrecht keine formalen Anforderungen fest. Für die Überprüfung signierter Daten wird dem Konzept der europäischen Signaturrichtlinie gefolgt, demgemäß die Verwendung von geeigneten Signaturanwendungskomponenten keine Voraussetzung für die Erzeugung einer elektronischen Signatur ist, die als Ersatz für die Unterschrift dient. Gemäß Art. 2.1.4.2 Resolução Nr. 42 braucht der Signatur-Empfänger (in den Vorschriften als „Relying Party“ genannt) nicht geeignete Darstellungs- und Prüfkomponenten zu verwenden, vielmehr kann er eine Signatur und das entsprechende Zertifikat ohne sichere Signaturanwendungskomponenten überprüfen und verifizieren. Wie er diese Überprüfungen durchführt, bleibt ihm überlassen.

310 *Pordesch*, DuD 1993, 565.
311 *Pordesch*, DuD 1993, 565.
312 *Pordesch*, DuD 2000, 93.
313 *Pordesch*, DuD 2000, 93.
314 *Pordesch*, DuD 1993, 566.

2.2.9.1.6.4 Prüfung und Bestätigung von Produkten

Obwohl die Verwendung von Signaturanzeige- und Signaturprüfkomponenten nicht konstitutiv für den Begriff „akkreditiertes Verfahren“ ist, bleibt das Thema von der Regulierung nicht unbeachtet. Die Resolução Nr. 36 aus dem Jahr 2004 legt ein Verfahren zur Evaluierung und Prüfung von Produkten für akkreditierte elektronische Signaturen fest. Diese Normierung wird durch eine Reihe von konkretisierenden Spezifikationen und Empfehlungen ergänzt.[315] Bestätigt werden Signaturerstellungseinheiten, wie Chipkarten oder Sicherheitstoken; Chipkartenlesegeräte und alle Signaturanwendungskomponenten, das heißt, Software- oder Hardwareprodukte, die zur Erzeugung, Prüfung und Darstellung von elektronischen Signaturen verwendet werden.

Die Aufsichtsbehörde erkennt Bestätigungsstellen an, die verantwortlich für die Evaluierung und das Überprüfen von Produkten, insbesondere bei Laboruntersuchungen und Praxistests sind. Bestätigungsstellen dürfen nur juristische Personen sein, die Fachkunde und Zuverlässigkeit nachweisen. Eine weitere Anforderung ist, dass die Stelle als Forschungsinstitution von einem Ausschuss des Bereichs der Informationstechnologie anerkannt sein muss. Bislang ist nur das Laboratório de Sistemas Integráveis Tecnológico (LSI-TEC), angesiedelt an der Universität von São Paulo, als Prüf- und Bestätigungsstelle von der Aufsichtsbehörde anerkannt worden.[316]

2.2.9.1.7 Haftung

In der MP 2.200-2 sind keine Haftungstatbestände vorgesehen. Diese Materie wird nur in den Nebenregelungen des Regulierungsausschusses behandelt. Die Resolução Nr. 41, Art. 2.2 regelt die Verantwortung, indem sie (Art. 2.2.1.1.) die Pflicht der Zertifizierungsstellen zur Ersetzung der von ihnen verursachten Schäden bestimmt. Diese Pflicht erstreckt sich auch auf die anderen an den Zertifizierungsdiensteanbieter vertraglich gebundenen Dienstleister wie Identifikationsstellen und sogar auf virtuelle Zertifizierungsstellen. Dabei besteht eine gesamtschuldnerische Haftung (Art. 2.2.1.2) zwischen dem Hauptzertifizierungsdiensteanbieter und den an ihn gebundene Dritte. Wichtig ist auch die Haftungsregelung des Art. 4.4.3.5 Resolução Nr. 42. Diese sieht vor, dass die AC für den Missbrauch des Signaturschlüssels in der Zeit zwischen dem Eingang des Sperrantrags und dem Eintritt der Sperrwirkung haftet.

Diese Haftungsregelungen sind grundsätzlich vertragsrechtlicher Natur und sind deswegen prinzipiell nur innerhalb der rechtlichen Beziehung zwischen Zertifizie-

315 Abrufbar unter http://www.lea.gov.br → Manual de Condutas Técnicas.

316 Für weitere Informationen: http://www.lea.gov.br/.

rungsdiensteanbieter (und an ihn gebundene Dritte) und Zertifikatsinhaber anwendbar.

Zwischen dem Zertifizierungsdiensteanbieter und einem Signaturempfänger[317], der die Dienstleistungen in Anspruch nimmt, weil er Zertifikate überprüft, besteht keine Vertragsbeziehung. Grundsätzlich steht nicht nur dem Signaturempfänger, sondern auch jeder anderen Person die Möglichkeit zur Überprüfung eines Zertifikats offen, und der Zertifizierungsdiensteanbieter ist wiederum zur Bereitstellung dieses Dienstes verpflichtet. Da alle Normierungen des Regulierungsausschusses prinzipiell auch keine Anwendung in der Beziehung Zertifizierungsdiensteanbieter und Signaturempfänger finden, bleiben lediglich andere Gesetze als Alternative für die Haftung übrig. Es ist dann zu überprüfen, inwieweit andere Rechtssätze im Verhältnis von Zertifizierungsdiensteanbieter und Signaturempfänger anwendbar sein können.

2.2.9.1.7.1 Verbraucherschutzgesetzbuch als Haftungsquelle

Denkbar wäre die Anwendung des brasilianischen Verbraucherschutzgesetzbuches, Código de Defesa do Consumidor (CDC)[318], das unter anderem die Haftung bei der Lieferung von fehlerhaften Produkten und Diensten normiert. Klarer Zweck dieses Gesetzbuches ist der Ausgleich der wirtschaftlichen, informativen und sozialen Unterlegenheit des Verbrauchers gegenüber dem Lieferanten. Nach diesem Gesetz haftet der Hersteller eines Produktes oder der Dienstleister für die Schäden, die von fehlerhaften oder mangelhaften Produkten oder Dienstleistungen verursacht werden. Im Rahmen des Código de Defesa do Consumidor gilt in der Regel[319] eine objektive Haftung (Gefährdungshaftung), für die kein Verschulden des Schädigers gefordert wird.[320] Er haftet lediglich für das Inverkehrbringen des Produkts oder der Dienstleistung auf den Markt. Vorgesehen wird im Código de Defesa do Consumidor auch die Beweislastumkehr im Zivilprozess zu Gunsten des Verbrauchers. Voraussetzungen hierfür sind gemäß Art. 6, VIII entweder die Wahrscheinlichkeit (verossimilhança) seiner Behauptungen oder seine eigene Unterlegenheit (hipossuficiência).[321]

317 Der Signaturempfänger wird auch Zertifikatsnutzer oder *relying party* genannt.

318 Lei Nr. 8.078, aus dem Jahr 1990.

319 Nach Art. 14, § 4 CDC gilt eine Verschuldenshaftung im Rahmen der Haftung von Freiberuflern. Zu dieser Kategorie gehören in Brasilien Ärzte, Zahnärzte, Buchführer, Rechtsanwälte u.a.

320 TJRS, Ap. Civ. 70016897753, Rel. Des. *Odone Sanguiné*, v. 10.01.2007 ; Ap. Civ. 70016785453, Rel. Des. *Odone Sanguiné*, v. 10.01.2007 ; Ap. Civ. 70014638308, Rel. Des. *Paulo Antônio Kretzmann*, v. 02.8.2006.

321 Die Rechtsprechung und die Literatur untergliedern diese Unterlegenheit (hipossuficiência) in zwei Kategorien. Die technische Unterlegenheit (hipossuficiência técnica) bezieht sich auf die fehlende Kenntnis des Verbrauchers über das Funktionieren eines Produktes oder einer

Eine andere Sonderregelung des Código de Defesa do Consumidor (Art. 88) ist das Verbot der Interventionsklage zum Zweck der Zügigkeit und der Vereinfachung des Prozesses. Der Código de Defesa do Consumidor bietet überdies dem Verbraucher die Möglichkeit an, die Haftungsklage in seinen eigenen Gerichtsstand vorzubringen (Art. 101, I). Diese Regel nimmt die allgemeine Klausel des brasilianischen Código de Processo Civil[322] (CPC) aus, die den Wohnsitz der beklagten Partei als allgemeinen Gerichtsstand bestimmt.[323]

Laut Art. 3 CDC ist Lieferant jede in- oder ausländische, natürliche oder juristische Person des öffentlichen Rechts oder des Privatrechts sowie auch jede Vereinigung ohne eigene Rechtspersönlichkeit, die im Bereich der Produktion, Montage, Gestaltung, Konstruktion, Umwandlung, Einfuhr, Ausfuhr des Vertriebs oder der Vermarktung von Produkten oder Dienstleistungen tätig ist.

Verbraucher im Sinn des Código de Defesa do Consumidor ist jede natürliche oder juristische Person, die ein Produkt oder eine Dienstleistung als Endverbraucher erwirbt oder nutzt. Umstritten an diesem Begriff ist, inwieweit gewerblich handelnde juristische oder natürliche Personen von einem Schutzgesetz wie dem Código de Defesa do Consumidor geschützt werden sollen. In der Literatur werden zwei Theorien artikuliert, welche sich mit der Tragweite des Verbraucherbegriffs befassen. Auf der einen Seite ist die so genannte *teoria maximalista*[324] welche behauptet, Verbraucher ist derjenige, der das Produkt oder die Dienstleistung aus dem Markt nimmt, sodass eine Weiterveräußerung nicht vorgesehen ist. Bei diesem breiten Begriff von Verbraucher spielt es keine Rolle, ob er das Produkt weiter in seinem Produktionsablauf nutzt und dadurch einen wirtschaftlichen Gewinn erzielt. Entscheidend ist nur die faktische Herausnahme der Dienstleistung oder des Produktes aus dem Markt. Auf der anderen Seite steht die *teoria finalista*[325], eine teleologische Theorie, wonach ein Verbraucher die „Endstation" in der wirtschaftlichen Kette sein muss, das heißt, der Gebrauch des Produktes oder die Nutzung des Dienstes darf lediglich seinen privaten Zwecken dienen. Nach dieser Theorie soll immer überprüft werden, ob der angebliche Verbraucher eigentlich den besonderen Schutz dieses so genannten rechtlichen Mikrosystems verdient.[326] In der brasilianischen Rechtsprechung wird diese Problematik nicht einheitlich behandelt. Das Superior Tribunal de Justiça folgt mit seiner vierten und sechsten Kammer zunächst der Tendenz der

Dienstleistung. Die wirtschaftliche Unterlegenheit (hipossuficiência econômica) bezieht sich auf die in der Regel vorliegende finanzielle Schwäche des Verbrauchers. 70016474207, Rel. Des. *Adao Sérgio do Nascimento Cassiano*, v. 20.12.2006; Ap. Civ. 70015346687, Rel. Des. *Odone Sanguiné*; STJ, AI 517.152-RJ, Rel. Min. *Nancy Andrighi*, v. 18.9.2003; TJRS, Ap. Civ 2003. In der Literatur: *Marques*, 2005, 133.

322 Das Zivilprozessgesetzbuch, Lei nº 5.869, aus dem Jahr 1973.

323 Gemäß Art. 94 des CPC.

324 *Van Marsen Faren* 2002, 42; *Alvim* 1995, 43.

325 *Marques* 2005, 123; *Comparato* 2002, 32; *Mukai* 1999, 132.

326 *Marques* 2005, 348.

engeren Auslegung des Verbraucherbegriffs.[327] Aber gleichzeitig entschieden die erste und die dritte Kammer desselben Gerichtshofs in Richtung der *teoria maximalista*.[328] Ein wichtiges Element für den Verbraucherbegriff in der Rechtsprechung ist auch die Verwundbarkeit des Endverbrauchers gegenüber dem Lieferanten.[329]

Angesichts dieser umstrittenen Auffassungen, was den Verbraucherbegriff angeht, ist davon auszugehen, dass der Zertifikatsinhaber nicht immer mit dem speziellen Haftungsschutz des Verbraucherschutzgesetzbuches rechnen darf. Ein Händler, der seine Waren durch die Internetpräsenz vertreiben will und elektronische Zertifikate für die Authentifizierung seiner Internetseite erwirbt, wird möglicherweise keinen Schutz als Verbraucher in der Beziehung zum Zertifizierungsdiensteanbieter bekommen, denn die Verwendungen von Zertifikaten gehört in diesem Fall zu der wirtschaftlichen Tätigkeiten des Unternehmens.

Der Dritte, der als Signaturempfänger auf die Information eines Zertifikates und auf die entsprechende Sperrliste (oder OCSP-Dienst) vertraut, kann auch nicht sicher sein, ob er vom Código de Defesa do Consumidor geschützt ist. Zunächst könnte er als Verbraucher angesehen werden, denn Verbraucher ist nicht nur, wer Produkte und Dienstleistungen erwirbt, sondern auch wer sie nutzt. Es bleibt aber die Unsicherheit in Bezug auf die mögliche Anwendung des eingeschränkten Verbraucherbegriffs für die gewerblich handelnden natürlichen oder juristischen Personen. Einer natürlichen Person, die in ihrer privaten Sphäre auf ein Zertifikat vertraut, wird sicherlich die Verbrauchereigenschaft stets zuerkannt. Es ist somit festzustellen, dass nur natürliche Personen, in ihren privaten Geschäften oder Kommunikationen, entweder als Signaturempfänger oder als Zertifikatinhaber, immer vom Schutzbereich des Código de Defesa do Consumidor gedeckt sein werden.

327 Hierzu beispielsweise REsp 218.505-MG, Rel. Min. *Barros Monteiro*, v. 14.2.2000, REsp 264.126-RS, Rel. Min. *Barros Monteiro*, v. 27.8.2000, REsp 475.220-GO, Rel. Min. *Paulo Medina*, v. 15.9.2003.

328 Siehe beispielsweise REsp 208.793-MT, Rel. Min. *Carlos Alberto Menezes Direito*, v. 01.8.2000, REsp 329.587-SP, Rel. Min. *Carlos Alberto Menezes Direito*, v. 24.6.2000, REsp. 468.148-SP, Rel. Min. *Antonio de Pádua Ribeiro*, REsp. 488.274-MG, Rel. Min. *Nancy Andrighi*, v. 23.6.2003, REsp. 445.854-MS, v. 19.12.2003, REsp. 263.229-SP, Rel. Min. *José Delgado*, v. 09.4.2001.

329 Einem Landwirt, der eine Maschine für seine Arbeit erwarb, wurde die Verbraucherseigenschaft zugesprochen, obwohl die Maschine im Kernbereich seiner Geschäftstätigkeit genutzt wurde. STJ, REsp 142042-RS, Rel. Min. *Ruy Rosado de Aguiar*, v. 11.11.1997. In diesem Fall war die ökonomische und technische Unterlegenheit des Landwirts entscheidend. *Carvalho* 2005, 72.

2.2.9.1.7.2 Código Civil als Haftungsquelle

Unbestritten soll die ergänzende Anwendbarkeit der Haftungstatbestände des Zivilgesetzbuches[330] in den signaturrechtlichen Verhältnissen Anwendung finden. Als allgemeine Regel wird in diesem Gesetz eine klassische Verschuldenshaftung normiert.[331] Der klagende Verletzte trägt den Nachweis für die Erfüllung des Tatbestands. Das Verschulden des Schädigers muss er nachweisen, grundsätzlich ohne die Möglichkeit einer Beweislastumkehr.

Im Rahmen des Zivilgesetzbuches ist auch nicht auszuschließen, dass die Wirkung der Vertragsklauseln zwischen Zertifizierungsdiensteanbieter und Signaturschlüsselinhaber sich auf das Verhältnis zwischen Zertifizierungsdiensteanbieter und Signaturempfänger erstreckt. Dies wäre mittels einer veränderten Auslegung des Grundsatzes der Relativität der Schuldverhältnisse denkbar.[332]

Nach der ursprünglichen Fassung dieses Grundsatzes besteht lediglich eine zweipolige Beziehung zwischen Gläubiger und Schuldner.[333] Dritte werden prinzipiell nicht in dieses Verhältnis einbezogen. Einerseits können sie aus dem fremden Schuldverhältnis keinen Ansprüchen ausgesetzt werden und zum anderen stehen ihnen keine Forderungsrechte zu.[334] Diesem Grundsatz entspricht die liberale – eher individualistische – Weltanschauung, welche im 19. Jahrhundert den *Code Civil* sowie später das erste brasilianische Zivilgesetzbuch aus dem Jahr 1916 geprägt hat.

Im neuen brasilianischen Código Civil aus dem Jahr 2002 wurde besonders Wert auf sozial ausgerichtete Grundsätze wie die „função social do contrato“ (soziale Funktion des Vertrags) und boa-fé objetiva (Treue und Glauben) gelegt.[335] Art. 421 CC bestimmt, dass die Freiheit, Rechtsgeschäfte abzuschließen an den Grenzen der sozialen Funktion des Vertrags auszuüben ist. Art. 422 CC normiert, dass sich die Vertragsparteien nach dem Grundsatz von Treue und Glauben zu verhalten haben, sowohl beim Vertragsabschluss als auch bei der Vertragserfüllung. Dieses für das

330 Das neue brasilianische Zivilgesetzbuch wurde durch Lei nº 10.406, vom 10.1.2002 eingeführt, und trat am 10.1.2003 in Kraft.

331 So lautet Art. 187 des CC: „derjenige, der aus vorsätzlicher Handlung, Unterlassung, Fahrlässigkeit oder Unvorsichtigkeit ein Recht verletzt und einem anderen einen Schaden verursacht, begeht eine unerlaubte Handlung“.

332 In der brasilianischen Rechtsprechung sind mehrere Fälle bekannt, in welchen der Grundsatz der Relativität der Schuldverhältnisse ausgenommen wurde, hierzu STJ, REsp 97.590-RS, Rel. Min. *Ruy Rosado de Aguiar*, v. 18.11.1996; STJ EREsp 70.684, Rel. Min. *Garcia Vieira*, v. 14.2.2000; STJ, EDcl/REsp 573.059-RS, Rel. Min. *Luiz Fux*, v. 30.5.2005.

333 Der Grundsatz stammt aus der römischen Vertragslehre und wird im Rechtsspruch „res inter alios acta allius neque nocere neque prodesse potest“ zusammengefasst (was die Parteien abgeschlossen haben, darf Dritte weder begünstigen noch beeinträchtigen); hierzu siehe *Miragem* 2005, 33.

334 *Kramer*, in: MüKO-BGB, Band 2a, Einl., Rn. 15.

335 S. Hierzu *Negreiros* 2002, 229; *Ferreira da Silva* 2006, 133.

kodifizierte brasilianische Privatrecht relativ neue Konzept wirkt sich allgemein auf die vertragsrechtliche Dogmatik aus. Betroffen wird dadurch auch der Grundsatz der Relativität der Schuldverhältnisse, der eine Milderung erfährt. Hierbei wird der Vertrag nicht mehr als geschlossene Abmachung – nur zwischen den ursprünglichen Parteien – verstanden, sondern als ein Rechtsinstrument, das potenziell die Interessen und sogar die Rechtssphäre von anderen betrifft.[336] Dies bedeutet zu einem, dass Dritte die noch geltenden Verträge anderer Parteien respektieren sollen.[337] Zum anderen bedeutet die Flexibilisierung des Grundsatzes der Relativität des Schuldverhältnisses aber auch, dass der Dritte auch von den Auswirkungen des fremden Vertrages begünstigt sein kann.

Aufgrund dieser Entwicklung des Grundsatzes der Relativität der Schuldverhältnisse wird dann die Möglichkeit gegeben, dass der Zertifizierungsdiensteanbieter basierend auf dem mit dem Signaturschlüssel-Inhaber abgeschlossen Vertrag gegenüber Dritten haftet. Voraussetzung hierfür ist aber eine deutliche Leistungsnähe des Dritten zum wirksamen vertraglichen Verhältnis zwischen Zertifizierungsdiensteanbieter und Signaturschlüssel-Inhaber. Der Dritte muss hierbei aber den Ursachenzusammenhang konkret nachweisen. Er muss Tatsachen anführen, die zum einen die Schäden bei einem elektronischen Rechtsverhältnis zum Signaturschlüssel-Inhaber beweisen. Zum anderen muss er auch den Beweis erbringen, dass die von ihm erlittenen Schäden auf eine Pflichtverletzung seitens des Zertifizierungsdiensteanbieters zurückzuführen sind. Die Beweiserbringung wäre beispielsweise im Falle einer Verletzung der Pflicht, ein Zertifikat rechtzeitig zu sperren und die Sperrliste zu aktualisieren, dann notwendig, wenn aufgrund dieser Verletzung ein Dritter, der auf das Zertifikat vertrauen durfte, Schäden erleidet.

2.2.9.1.7.3 Haftung im Rahmen des Gesetzesentwurfs Nr. 7.316/2002

Art. 38 Gesetzentwurf Nr. 7.316/2002 sieht eine Haftungsregelung vor, welche bestimmt, dass alle Teilnehmer der ICP-Brasil – einschließlich der Aufsichtsbehörde – für die von ihnen verursachten Schäden haften. Art. 39 legt des Weiteren eine subsidiäre Haftung der Zertifizierungsdiensteanbieter fest. Sie haften auch für von ihnen beauftragte Dritte. Art. 41 Gesetzesentwurf 7.316/2002 erklärt es für nichtig, wenn Vertragsklauseln und Bestimmungen der Dokumente „Declaração de Práticas de

336 Ein Beispiel des deutschen Rechts für eine Vorschrift, die den Grundsatz der Relativität der Schuldsverhältnisse relativiert ist § 311 Abs. 3 BGB, demgemäß ein Schuldverhätnis mit Pflichten nach § 241 Abs. 2 auch zu Personen entstehen kann, die nicht selbst Vertragspartei werden sollen. Ein solches Schuldverhältnis entsteht insbesondere, wenn der Dritte in besonderem Maße Vertrauen für sich in Anspruch nimmt und dadurch die Vertragsverhandlungen oder den Vertragsschluss erheblich beeinflusst.

337 Wie *Azevedo* darauf hinweist, dürfen sich Dritte nicht verhalten, als ob der Vertrag zwischen den ursprünglichen Vertragsparteien nicht existiere. *Azevedo* 2004, 142.

Certificação“ und „Políticas de Certficado“ die Haftung von Zertifizierungsdiensteanbietern vermindern oder ausschließen. Der einzige Paragraph des Art. 41 lässt die Hinzufügung von Schadenersatzlimitierungen ausnahmsweise in den Fällen zu, in welchen es sich beim Signaturschlüssel-Inhaber um eine juristische Person handelt.

2.2.9.1.7.4 Versicherung

Eine sehr wichtige Anforderung innerhalb der akkreditierten Verfahren in der brasilianischen Regulierung ist die Pflicht der Zertifizierungsdiensteanbieter, über eine Versicherung zu verfügen, die im Haftungsfall eingreifen muss. Haftungsregelungen alleine sind wertlos, wenn die Zertifizierungsstellen nicht über ausreichende Geldmittel oder andere Vermögensgegenstände verfügen, um verursachte Schäden auszugleichen.[338]

In den Bestimmungen der Pflichten von Zertifizierungsdiensteanbietern, die Resolução Nr. 41, Art. 2,1,1,t, wird auf die Verpflichtung zum Abschluss eines Versicherungsvertrages zur Deckung aller Schäden, die aus ihrer Tätigkeit verursacht werden können, verwiesen. Eine Mindestsumme wird nicht bestimmt, sondern nur festgelegt, dass die Versicherung geeignet und kompatibel zu den Risiken der Tätigkeit des Zertifizierungsdiensteanbieters sein muss. Mit der Offenheit dieser Bestimmung stellt sich die Frage, was als „geeignet und kompatibel zu den Risiken der Tätigkeit“ angesehen werden soll. Diese Beurteilung obliegt derjenigen Aufsichtsbehörde, welche über die Zuständigkeit für die Entscheidungen innerhalb des Akkreditierungsverfahrens verfügt. Es ist festzustellen, dass es erhebliche Schwierigkeiten bei der Behandlung der Versicherungsgestaltung einer Zertifizierungsstelle gibt. In diesem Bereich ist es schwierig, die möglichen Schäden im Vorfeld zu kalkulieren.[339] Ein Zertifikat, das als Ersatz für die handschriftliche Unterschrift verwendet wird, darf prinzipiell für alle Anwendungen genutzt werden.[340] Darüber hinaus fehlen aufgrund der mangelnden Verbreitung und Verwendung der Signaturverfahren die Erfahrungen bezüglich der Schadensverläufe. Trotzdem muss die Aufsichtsbehörde eine Entscheidung über die angemessene Versicherungspolice treffen.

Um ein zumutbares Urteil darüber zu fällen, berücksichtigt die Aufsichtsbehörde mehrere Kriterien. Ein Maßstab hierfür wären die Zertifikatstypen, die von der Zertifizierungsstelle ausgestellt werden. Von einem Zertifizierungsdiensteanbieter, der Zertifikate nur mit Verschlüsselungsfunktionen oder Zertifikate nur für eine bestimmte Anwendung ohne große finanzielle Auswirkung erstellt, soll eine zu den niedrigeren Risiken entsprechende Deckung der Versicherungspolice verlangt wer-

338 *Thomale* 2003, 230.

339 *Thomale* 2003, 234.

340 Das brasilianische Recht sieht keine Vorschriften vor, die die Anwendung der elektronischen Form ausdrücklich ausschließt.

den. Einem anderen Zertifizierungsdiensteanbieter, der alle Zertifikatstypen anbietet, inklusive solcher Zertifikate für andere Zertifizierungsdiensteanbieter, obliegt logischerweise die Pflicht zum Abschluss eines Versicherungsvertrages mit einer erheblich höheren Deckung hinsichtlich des Umfangs der möglichen Risiken. Ein anderer Aspekt ist die Anzahl der ausgestellten Zertifikate. Da in der ICP-Brasil alle Zertifizierungsdiensteanbieter monatlich die Aufsichtsbehörde über die Anzahl der von ihnen ausgestellten Zertifikate zu informieren haben[341], kann sie auch diese Daten zur Evaluierung und ständigen Kontrolle der Angemessenheit der Versicherung zu den involvierten Risiken nutzen.

Nach der brasilianischen Normierung für akkreditierte Zertifikate ist es beispielsweise möglich, einen Vertrag von 1 € oder 1 Milliarde € zu signieren. Aber ein solcher Handlungsspielraum des Signaturschlüsselinhabers hat auch seinen Preis, weil er selber, Zertifizierungsdiensteanbieter, Identifikationsstellen und die Aufsichtsbehörde potenziell für entstandene Schäden haften können. Das Risiko erstreckt sich somit auf die ganze Hierarchie der Teilnehmer der PKI. Und je höher die Summe der abgewickelten Transaktionen, desto größer die Risiken und daraus folgend die erforderliche Deckung für den Versicherungsvertrag.

Die Vorschrift, die die Anforderung zum Abschluss eines Versicherungsvertrags bestimmt, beschränkt nicht den Geltungsumfang der Versicherung. Es wird nicht festgesetzt, ob die Versicherung die Schäden für die vertragliche Haftung gegenüber dem Schlüsselinhaber und gegenüber Dritten, die auf das Zertifikat vertrauen, decken muss. Aus diesem Grund ist Artikel 2,1,1,t der Resolução Nr. 41 so zu verstehen, dass die Versicherung Schäden, die Dritten (Signaturempfänger) sowie dem Schlüsselinhaber entstehen, abdecken muss.

2.2.9.2 Die sonstigen Verfahren

Der Gesetzestext definiert andere Signaturverfahren nicht. Über die sonstigen Signaturverfahren wird im § 2 Art. 10 MP 2.200-2 lediglich darauf verwiesen, dass im Prinzip neben den akkreditierten Verfahren jedes andere elektronische Identifikationsmittel verwendet werden darf, wenn die Parteien ihre Verwendung vereinbart haben oder der Erklärungsempfänger nichts unternimmt, um ein solches Verfahren anzufechten. Beispiele dieser sonstigen Verfahren sind u.a. die eingescannte Unterschrift, das Passwort, die einfache E-Mail und die frei verfügbaren Implementierungen von Pretty Good Privacy (PGP). Diese sonstigen Signaturverfahren sind mit keinen Sicherheitsanforderungen verbunden. Die PGP benutzt schon das Public-Key Verfahren, ohne aber die meisten Sicherheitsmaßnahmen der akkreditierten Verfahren zu erfüllen. Bei Verfahren wie PGP und anderen, die auf dem Markt zur Verfügung stehen, wird z.B. kein Zertifizierungspfad festgelegt. Das Instituto Nacional de Tecnologia da Informação übernimmt dabei keine Funktion als Wurzelzertifizie-

341 Art. 2.1.1, v, Resolução Nr. 42.

rungsstelle. Die nicht-akkreditierten Zertifizierungsdiensteanbieter sind frei, sich ihre Zertifizierungsstruktur zu schaffen und können ihr Wurzelzertifikat selbst signieren. Anders als in der Infrastruktur der Aufsichtsbehörde, wo sich die Zertifikate aller akkreditierten Zertifizierungsdiensteanbieter in derselben Zertifikatstruktur befinden und dadurch ohne weiteres geprüft werden können, kann bei dem Selbstzertifikat nicht verlässlich überprüft werden, ob das Zertifikat tatsächlich vom dem darin namentlich angegeben Zertifizierungsdiensteanbieter ausgestellt worden ist. Zu Interoperabilitätszwecken haben die nicht akkreditierten Zertifizierungsdiensteanbieter dafür Sorge zu tragen, dass sie die gegenseitige Anerkennung ihrer Zertifikate durch andere Zertifizierungsdiensteanbieter erreichen.

2.2.10 Zeitstempel

Bei vielen Tätigkeiten des Rechtsverkehrs ist das Nachweisen des Zeitpunkts einer Wissens- oder Willenserklärung von großer Bedeutung. Die Zeitstempel verhindern das Vor- und Rückdatieren von elektronischen Dokumenten. Sie sind stets erforderlich, wenn ein bestimmter Zeitpunkt im Streitfalle beweiserheblich sein kann.[342]

In diesem Kontext ist die genutzte Zeitquelle wichtig. Sie darf nicht manipulierbar sein und muss eine eindeutige Zeitzone verwenden. In Brasilien ist die Institution Observatório Nacional[343] für das „Liefern der Zeit" in das ganze Land verantwortlich. Das Observatório Nacional ist im Geschäftsbereich des föderalen Ministeriums für Wissenschaft und Technologie angesiedelt. In der ICP-Brasil müssen die Zertifizierungsdiensteanbieter und die Regulierungsbehörde für ihre Tätigkeiten die offizielle Zeit des Observatório Nacional benutzen.

In Brasilien sind bezüglich der Zeitstempel sowie Zeitstempeldienste noch keine Reglungen normiert worden. Art. 2 Abs. 13 Gesetzentwurf Nr. 7316/2002 regelt diese Materie, indem er die Möglichkeit der Akkreditierung von Zeitstempeldiensteanbietern vorsieht. Als Voraussetzungen dafür werden grundsätzlich diejenigen, welche dem Zertifizierungsdiensteanbieter obliegen, übernommen. Somit muss der Zeitstempeldiensteanbieter folgende Bedingungen erfüllen:

a) die Einhaltung aller Beschlüsse des Regulierungsausschusses;
b) Verpflichtung zum Abschluss eines Versicherungsvertrages zur Deckung alle Schäden die aus ihrer Tätigkeiten verursacht werden;
c) Angestellte einsetzen, die nachweislich für diese Tätigkeit die notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen;
d) die Anwendung von Systemen, die die unberechtigte Nutzung von Daten, Informationen und Dokumente des Zertifikatsinhabers verhindern;

342 *Roßnagel*, RMD, § 2 SigG a. F. Rn. 77.

343 Analog in Deutschland ist die Physikalisch-Technische Bundesanstalt (PTB).

e) über die geeigneten Einrichtungen für die Durchführung ihrer Tätigkeiten verfügen. Diese müssen auch in Brasilien angesiedelt sein;
f) ihre finanzielle Leistungsfähigkeit muss auch nachgewiesen werden.

Die notwendige Darstellung der brasilianischen Verhältnisse im Bereich der technisch-organisatorischen Vorschriften ist damit abgeschlossen. Sie soll als Grundlage dafür dienen, um wie bereits angekündigt im Kern der Arbeit einen Rechtsvergleich zu führen, welcher sich später in Kapitel 6 mit der Gegenüberstellung des Beweisrechts beider Nationen verdichtet und zum Schluss gebracht wird.

3. Vergleich und Vorschläge zur Rezeption als Ergebnis der Vergleichsanalyse

Im ersten Teil dieser Arbeit wurden die Regelungen zu den technisch-organisatorischen Eigenschaften der Sicherungsinfrastruktur für elektronische Signaturen beschrieben, welche nun folgend zur Synthese gebracht werden. Dafür werden hier die vergleichenswürdigen Aspekte der Darstellung des deutschen sowie des brasilianischen Signaturrechts diskutiert sowie anschließend – wenn passend – Vorschläge unterbreitet.

3.1 Allgemeines und Akkreditierung

Sowohl im deutschen als auch im brasilianischen Signaturrecht spielt die Akkreditierung eine wichtige Rolle. Dies ergibt sich bereits aus der Nachfrage an das Akkreditierungsverfahren in beiden Ländern. Die Anzahl von akkreditierten Anbietern ist seit der Einführung der brasilianischen PKI kontinuierlich gestiegen.[344] Auch in Deutschland lassen sich regelmäßig Interessenten bei der Bundesnetzagentur akkreditieren.[345] Es gibt kaum nicht akkreditierte Anbieter.

In beiden Ländern ist der Betrieb eines Zertifizierungsdienstes genehmigungsfrei. Dies ist in Deutschland durch § 4 Abs. 1 SigG bestimmt, welcher den Art. 3 Abs. 1 der Signaturrichtlinie umsetzt. In Brasilien wird dieses Merkmal aus Art. 10 § 2 MP 2.200-2 entnommen, wonach es den Parteien grundsätzlich frei steht, andere als die akkreditierten Signaturverfahren zu nutzen. Folglich ist die Akkreditierung in beiden Ländern als Angebot zur Steigerung des Sicherheitsniveaus der erbrachten Zertifizierungsdienste zu bezeichnen.

Der größte Unterschied zwischen den beiden Systemen liegt aber in den verschiedenen Verknüpfungen mit privilegierten Rechtsfolgen. In Deutschland gilt der Anscheinsbeweis des § 371a Abs. 1 Satz 2 ZPO grundsätzlich für qualifizierte elektro-

344 Angaben hierzu unter www.iti.br.

345 Nach Angaben der Bundesnetzagentur erfolgte die letzte Anbieterakkreditierung für qualifizierte Zertifikate am 9.8.2007; www.bundesnetzagentur.de.

nische Signaturen. Eine Anbieterakkreditierung ist hierzu nicht erforderlich. In Brasilien dagegen gilt die beweisrechtliche Privilegierung nach Art. 10 § 1 MP 2.200-2 nur zugunsten akkreditierter Signaturverfahren. Der brasilianische Ansatz liegt somit zwischen dem Ansatz des aktuellen Signaturgesetzes und dem Ansatz, welcher noch im Rahmen des SigG 1997 galt, wonach der Betrieb einer Zertifizierungsstelle an eine Genehmigung der zuständigen Behörde gebunden war.[346] Verdrängt wurde der Genehmigungsansatz des SigG 1997 durch die europäische Signaturrichtlinie, welche das Gebot der Niederlassungsfreiheit von Art. 43 EGV desartikulierte.[347] Die Signaturrichtlinie stellt hierbei im zehnten Erwägungsgrund klar, dass auch sonstige Maßnahmen mit der gleichen Wirkung einer Genehmigung unzulässig sind. Darüber hinaus müssen die Anforderungen zur Akkreditierung nach Art. 3 Abs. 2 Signaturrichtlinie objektiv, transparent, verhältnismäßig und nicht diskriminierend sein.

Die Anbieterakkreditierung im deutschen Signaturrecht zeichnet sich durch höhere Sicherheitsanforderungen im Vergleich zu den qualifizierten Zertifizierungsdiensteanbietern aus. Akkreditierte Anbieter dürfen nach § 15 Abs. 7 Satz 1, Satz 2 Nr. 1 SigG nur geprüfte und bestätigte Komponenten einsetzen. Sie müssen darüber hinaus die Zertifikate der Signaturschlüssel-Inhaber laut § 4 Abs. 2 SigV für einen Mindestzeitraum von 30 Jahren aufbewahren. Dem Signaturschlüssel-Inhaber eines akkreditierten Zertifikats wird zudem gewährleistet (§ 15 Abs. 6 SigG), dass im Fall der Einstellung der Anbietertätigkeiten entweder ein anderer Zertifizierungsdiensteanbieter oder im Ausnahmefall die zuständige Behörde die Dokumentation des scheidenden Zertifizierungsdiensteanbieters übernimmt. Diese Übernahme dient der Nachprüfbarkeit der Zertifikate für die bereits erwähnten 30 Jahre nach Ablauf des Gültigkeitszeitraums des Zertifikats.[348]

Ein weiterer Unterschied zwischen den beiden Akkreditierungssystemen liegt in der Verpflichtung der Zertifizierungsdiensteanbieter, die Zertifikate der Signaturschlüssel-Inhaber für einen gewissen Zeitraum in einem Zertifikatsverzeichnis vorzuhalten. Während in Deutschland ein Mindestzeitraum von 30 Jahren vorgesehen wird, bestimmt das brasilianische Signaturrecht[349] eine unbefristete Aufbewahrungspflicht. Dies bedeutet, dass Zertifizierungsdiensteanbieter in Brasilien einer unbefristeten Aufbewahrungspflicht nachkommen müssen. Ursprünglich galt im brasilianischen Signaturrecht die gleiche Aufbewahrungspflicht wie in Deutschland. Die entsprechende Vorschrift (Art. 6.3.1 Resolução Nr. 42) ist jedoch in jüngster

346 *Roßnagel*, NJW 1998, 3312. Hierzu auch die Begründung zum deutschen Signaturgesetz aus dem Jahr 2001, das die im Rahmen des Signaturgesetzes 1997 geltende Sicherheitsvermutung anerkennt; BT-Drs. 14/4662, 28.

347 Nach dieser Vorschrift sind Beschränkungen der freien Niederlassung von Staatsangehörigen eines Mitgliedstaats im Hoheitsgebiet eines anderen Mitgliedstaats grundsätzlich verboten.

348 Der Wortlaut des § 15 Abs. 6 SigG, wonach die Bundesnetzagentur die Abwicklung der Verträge mit den Signaturschlüssel-Inhabern sicherstellen muss, wird somit restriktiv ausgelegt. Hierzu, *Fischer-Dieskau* 2006, 155.

349 Hierzu bereits in diesem Teil Gliederungspunkt 2.2.9.1.3.

Zeit geändert worden, um eine kontinuierlich unbeschränkte Möglichkeit der Überprüfung von elektronischen Signaturen zu gewährleisten. Hierbei stärkt das brasilianische Signaturrecht zweifellos die Rechtssicherheit bei der Überprüfung von „alten" Signaturen. Fraglich ist dennoch bei genauerer Betrachtung, ob eine generell unbefristete Aufbewahrungspflicht als sachgerecht zu bewerten ist. In diesem Zusammenhang darf nicht außer Acht gelassen werden, dass nicht alle Anwendungen – wie etwa Bankapplikationen – eine langzeitige Aufbewahrung der öffentlichen Schlüssel für eine spätere Überprüfung der Signatur benötigen. Als Folge implizierte dies unnötige Kosten und wäre unter wirtschaftsrechtlichen Gesichtspunkten somit fehlgeleitet. Als Beispiel hierfür ist das brasilianische Zahlungssystem zu nennen. Akkreditierte Zertifikate werden dabei grundsätzlich für die gegenseitige Identifizierung der Bankanwendungen genutzt.[350] Die Funktion des Schriftformersatzes und die Aufbewahrung signierter Daten kommen dabei jedoch nicht in Frage.

Des Weiteren spielt für manche Signaturanwendungen eine unbefristete Aufbewahrung von Zertifikaten nach Ablauf ihrer Gültigkeit keine ausschlaggebende Rolle. Die Festsetzung einer derartigen Frist soll sich möglichst an den üblichen Verjährungsfristen von Rechtsgeschäften und den wichtigsten strafrechtlichen Vermögensdelikten orientieren. Der neue brasilianische Código Civil bestimmt diesbezüglich Verjährungsfristen von 1 bis zu 10 Jahren. Der brasilianische Código Penal setzt wiederum Verjährungsfristen von 2 bis zu 20 Jahren. Infolgedessen kann die pauschale, ständige Pflicht, Zertifikate verfügbar zu halten, dem Zertifizierungsdiensteanbieter unnötigen Aufwand und damit Zeitverlust sowie Kosten verursachen. Sachgerechter wären somit die alte Lösung der brasilianischen Regulierung und die aktuelle des deutschen Signaturrechts, wonach eine mindestens 30-jährige Aufbewahrungsfrist für akkreditierte Zertifikate gilt. Dem Zertifizierungsdiensteanbieter, wie auch dem Nutzer bleibt dann vorbehalten, je nach Bedarf und aufgrund freiwilliger Absprachen längere Fristen zu setzen oder solche für bestimmte Bereiche gesondert zu vereinbaren.[351]

Anders als in Deutschland existiert im brasilianischen Signaturrecht keine qualifizierte oder sogar fortgeschrittene Stufe. Dadurch besteht eine große Kluft zwischen den akkreditierten und den sonstigen Verfahren. Nach einem Alles-oder-Nichts Ansatz wird den Verbrauchern entweder der volle Schutz der höheren Sicherheitsanforderungen angeboten oder gar kein Schutz. Denn die Vorschriften der gesamten ICP-Brasil betreffen nur akkreditierte Zertifizierungsdiensteanbieter[352] sowie deren Kunden. Dazwischenliegende alternative Lösungen lassen sich in Brasilien auf dem

350 Hierzu s. Art. 1.3.5.2 des Dokuments „Política de Certificado" vom brasilianischen Zertifizierungsdiensteanbieter AC Certisign SPB, abrufbar unter http://icp-brasil.certisigncom.br → Repositório → PC – Política de Certificado.

351 Hierzu amtliche Begründung zu § 4 Abs. 1 SigV.

352 Auch akkreditierte Identifikationsstellen, akkreditierte dritte Dienstleister und die zuständige Behörde liegen im Geltungsbereich der ICP-Brasil.

Markt für elektronische Signaturen nur durch isolierte Initiativen des Marktes finden.

Sowohl in Brasilien als auch in Deutschland sind die Dienste akkreditierter Zertifizierungsdiensteanbieter angesichts der mit der Akkreditierung verbundenen Pflichtdienstleistungen teurer als diejenigen, welche von sonstigen Anbietern zu erwarten sind.[353] In Deutschland existiert wenigstens eine nennenswerte Zahlungsbereitschaft sowohl für akkreditierte als auch für qualifizierte elektronische Signaturen.[354]

3.2 Neusignierung

Eine Schwäche des brasilianischen Signaturrechts ist[355], dass kein Verfahren zur Neusignierung signierter Daten normiert wird. Wie bei der Darstellung des deutschen Signaturrechts erwähnt[356], ist eine Neusignierung für Dokumente erforderlich, die langfristig beweiskräftig aufzubewahren sind.[357] Grund hierfür ist, dass – anders als bei eigenhändig unterschriebenen Papierdokumenten – technische Fortschritte oder neue wissenschaftliche Erkenntnisse zu einem Verlust der Sicherheitseignung der bei der ursprünglichen Signatur eingesetzten Algorithmen und zugehörigen Parametern führen können. Anhand der neuen Algorithmen sowie den zugehörigen Parametern, werden die Signaturen der alten Dokumente durch die neue Signatur, basierend auf dem so genannten Prinzip der Verschachtelung, umfasst. Darüber hinaus bringt die Neusignierung den Vorteil mit sich, dass der Beweiswert des ursprünglich signierten Dokuments erhöht wird. Ansonsten bestünde die Möglichkeit, Signaturen des alten Dokuments ohne erkennbare Spuren zu entfernen.

Aufgrund der klaren Vorteile sowie der Notwendigkeit der Existenz einer Vorschrift zur erneuten Signatur, zeigt sich die Übernahme einer des deutschen Signaturrechts ähnlicher Regelung in das brasilianische Signaturrecht als passend.

Zu betonen ist, dass zur maximalen Nutzbarkeit und Bedeutung einer Vorschrift über die Neusignierung, eine Verknüpfung des Verfahrens an Zeitstempel zu empfehlen wäre. Nur dann werden die schon dargestellten Vorteile der erneuten Signatur maximiert. Da das brasilianische Signaturrecht sowohl Zeitstempeldienste als auch

353 *Fischer-Dieskau* 2006, 133; *Roßnagel*, MMR 1999, 265.

354 *Roßnagel*/*Hinz*, in: Oberweis et al. 2007, 173.

355 Auch innerhalb der Mitgliedstaaten der europäischen Union hat außer Deutschland nur Österreich das Thema signaturrechtlich behandelt. Die Richtlinie für elektronische Signaturen ließ die Problematik der Notwendigkeit einer neuen Signierung unberührt. Hierzu *Fischer-Dieskau* 2006, 178.

356 Siehe hierzu bereits im diesen Teil Gliederungspunkt 1.3.5.5.2.

357 Wie die Begründung zum § 17 SigV: „Unterbleibt bei einer vorhandenen qualifizierten elektronischen Signatur mit Ablauf der Eignung der Algorithmen und zugehörigen Parameter eine erneute Signatur, so verliert sie damit die vorgegebene Sicherheit“.

die Anwendung von Zeitstempeln noch nicht geregelt hat, zeigt sich auch diesbezüglich ein Normierungsbedarf.[358]

Die Normierung zur erneuten Signatur wird im deutschen Signaturrecht im Rahmen der Unterrichtungspflicht seitens des Zertifizierungsdiensteanbieters gegenüber dem Zertifikatsinhaber geregelt (§ 6 Abs. 1 Satz 2 SigG). Wie das Verfahren zur Neusignierung zu gestalten ist, bestimmt § 17 SigV. Dieser Ansatz ist grundsätzlich richtig. Den Signaturschlüssel-Inhaber mit der erneuten Signatur zu verpflichten wäre ungeeignet, denn ein Verstoß gegen diese „Pflicht" würde in der Regel keinen Dritten benachteiligen. Ein solches Vorgehen des Zertifikatsinhabers – ohne eigentlichen Schuldcharakter – begründet für ihn somit keine Pflicht, sondern eine Obliegenheit, deren Nichterfüllung Rechtsnachteile, wie die Verschlechterung der Beweiskraft seiner empfangenen elektronisch signierten Dokumente, mit sich bringt. Sowohl im deutschen[359] als auch im brasilianischen[360] Signaturrecht werden keine Rechtspflichten an den Signaturschlüssel-Inhaber gestellt.

Deshalb zeigt sich auch in diesem Aspekt, die Rezeption seitens des brasilianischen Signaturrechts von einer autonomen Vorschrift über die Neusignierung passend. Die Norm könnte überdies – wie in Deutschland – auch als Teil der Unterrichtungspflicht für den Zertifizierungsdiensteanbieter gegenüber dem Zertifikatsinhaber normiert werden.

3.3 Signaturerstellungseinheiten

Wie bereits in dieser Arbeit dargelegt[361], besteht im brasilianischen Signaturrecht die Möglichkeit, private Schlüssel einer bestimmten Zertifikatskategorie auf einer Festplatte zu speichern. Dies sollte nur vorläufig erlaubt werden, als im Jahr 2001 ein neues Zahlungssystem, basierend auf elektronischer Signaturen für die Banken, entwickelt wurde, ohne dass sichere Signaturkarten verbreitet waren. Jedoch gilt diese Vorschrift immer noch und daraus ergibt sich die Möglichkeit, dass privilegierte Rechtsfolgen eines unsicheren akkreditierten Verfahrens das Vertrauen der Nutzer gefährdet. Denn mit dieser Lösung kann nicht mehr gewährleistet werden, dass der Signaturschlüssel-Inhaber die alleinige Kontrolle über den privaten Schlüssel verfügt.

358 Zur Zeitstempelregulierung in Brasilien siehe bereits in diesem Teil Gliederungspunkt 2.2.10.

359 Über die Sicherungsmaßnahmen seitens des Signaturschlüssel-Inhabers als Obliegenheiten, siehe *Roßnagel*, MMR 2008, 28.

360 Hierzu siehe bereits in diesem Teil Gliederungspunkt 2.2.9.1.5 Eine Ausnahme bildet in diesem Zusammenhang die Rechtspflicht im brasilianischen Signaturrecht zur korrekten, wahren und präzisen Abgabe von Informationen und Daten an den Zertifizierungsdiensteanbieter für die Ausstellung des Zertifikats.

361 Siehe hierzu im 2. Teil Gliederungspunkt 2.2.9.1.2.1.

Aus diesen Gründen ist zu erwarten, dass in naher Zukunft diese unsichere Möglichkeit der Speicherung eines privaten Schlüssels aufgehoben wird und von da an nur geeignete Prozessor-Chipkarten, Security-Token oder vergleichbare Datenträger verwendet werden. Bei der aktuellen Situation, was die wichtigsten Sicherheitspunkte einer PKI betrifft, ist die Ausgangsposition Brasiliens oder brasilianischer Zertifizierungsdiensteanbieter für Verhandlungen mit anderen Staaten oder internationalen Organisationen über die gegenseitige Anerkennung von elektronischen Zertifikaten schwierig. Obwohl die Anforderungen der Europäischen Union gemäß Art. 7 der Signaturrichtlinie keine Überprüfung der Sicherheit der ausländischen Signaturverfahren vorsehen, müssen entweder das Zertifikat oder der Zertifizierungsdiensteanbieter im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der EU und dem Drittland oder internationalen Organisationen anerkannt werden.[362] Die konkreten Voraussetzungen für diese Anerkennung werden nicht in der Signaturrichtlinie bestimmt und müssen daher fallweise ausgehandelt werden. Es ist aber vorhersehbar, dass die Möglichkeit der Speicherung des Signaturschlüssels auf einer Diskette oder Festplatte als nicht geeignet für Signaturverfahren, welche die Unterschrift ersetzen sollen, eingestuft wird. In Deutschland beispielsweise werden ausländische elektronische Signaturen nach § 23 Abs. 2 SigG akkreditierten Signaturen nur dann gleichgestellt, wenn sie nachweislich eine gleichwertige Sicherheit aufweisen.[363]

3.4 Signaturanwendungskomponenten

Ein notwendig zu betrachtender Themenkreis einer Public Key Infrastruktur sind die erforderlichen Signaturanwendungskomponenten, die die Erzeugung einer elektronischen Signatur vorher eindeutig anzeigen und damit ermöglichen, die Daten auf welche sich die Signatur bezieht, festzustellen. Diesbezüglich sieht das brasilianische Signaturrecht (Resolução Nr. 36) lediglich die Möglichkeit, Produkte für die Sicherheit akkreditierter Signaturen zu prüfen und zu bestätigen.[364] Inbegriffen sind die Produkte für die Darstellung zu signierender Daten. Das deutsche Signaturgesetz enthält auch eine solche Vorschrift, geht aber einen Schritt weiter, indem es dem Signaturschlüssel-Inhaber sichere Signaturanwendungskomponenten zu verwenden empfiehlt (§ 17 Abs. 2 Satz 3 SigG), da der Einsatz solcher Komponenten – anders

362 Laut Art. 7 Abs. 1 a) und b) RLeS sind zwei andere Möglichkeiten für die Anerkennung internationaler Zertifikate vorgesehen: Entweder muss der Zertifizierungsdiensteanbieter die Anforderungen der Richtlinie erfüllen und im Rahmen eines freiwilligen Akkreditierungssystems eines Mitgliedstaats akkreditiert sein oder ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen der Richtlinie erfüllt, muss für das Zertifikat einstehen.

363 *Roßnagel* 2002a,157.

364 S. hierzu bereits in diesem Teil Gliederungspunkt 2.2.9.1.7.4.

als bei Zertifizierungsdiensteanbietern – nicht kontrollierbar ist.[365] Somit stellen die sicheren Komponenten keine Wirksamkeitsvoraussetzung für die mittels ihrer Anwendung erzeugten Signaturen dar.[366] Verstärkt wird diese Soll-Vorschrift durch die Pflichtdienstleistung des Zertifizierungsdiensteanbieters, den Signaturschlüssel-Inhaber über die erforderlichen Maßnahmen zur Sicherheit von qualifizierten elektronischen Signaturen und deren Prüfung zu unterrichten (§ 6 Abs. 1 Satz 1 SigG). Da im brasilianischen Signaturrecht die Signaturanwendungskomponenten noch nicht einmal als Empfehlungen geregelt sind, zeigt es sich als opportun, eine auf dem deutschen Modell des § 17 Abs. 2 Satz 3 SigG basierende Norm zu übernehmen.

3.5 Unterrichtungspflicht

Wie bereits in dieser Arbeit dargelegt[367], verfügt das brasilianische Signaturrecht über keine spezielle Vorschrift, welche die Unterrichtungspflicht des Zertifizierungsdiensteanbieters zur Information des Antragstellers im ausreichenden Umfang behandelt.[368] Vielmehr muss diese aus den allgemeinen Vorschriften des Verbraucherschutzgesetzbuchs hergeleitet werden. Die Regelungen des Verbraucherrechts sind jedoch für das Signaturrecht unzureichend. Benötigt werden spezifische Bestimmungen, angeglichen an die technische Komplexität der Verwendung elektronischer Signaturen und an die Tatsache, dass die Unterrichtung des Antragstellers als „notwendiger Bestandteil des Gesamtkonzepts zur Gewährleistung der Sicherheit des gesetzlichen Signaturverfahrens“ angesehen wird.[369] Hierbei kommt als mögliches Rezeptionsmodell für das brasilianische Signaturrecht die Unterrichtungspflicht des § 6 SigG in Betracht. Nach dieser Vorschrift hat der Zertifizierungsdiensteanbieter den Antragsteller über Folgendes zu unterrichten:

1) über die bereits erwähnten erforderlichen Maßnahmen zur Sicherheit von qualifizierten elektronischen Signaturen und deren Prüfung (§ 6 Abs. 1 Satz 1 SigG);
2) über die oben erwähnte Notwendigkeit Daten mit einer qualifizierten Signatur neu zu signieren, bevor der Sicherheitswert der vorhandenen Signatur geringer wird (§ 6 Abs. 1 Satz 2 SigG) sowie

365 *Fischer-Dieskau* 2006, 123; BT-Drs. 14/4662, 30.

366 S. dazu bereits in diesem Teil Gliederungspunkt 1.3.5.7.

367 S. hierzu bereits in diesem Teil Gliederungspunkt 2.2.7.

368 Art. 2.1.1, h, Resolução Nr. 42 sieht lediglich vor, dass der Zertifizierungsdiensteanbieter den Antragsteller über die Ausstellung des Zertifikats informieren muss. Darüber hinaus bestimmt Art. 2.1.1, u, Resolução Nr. 42 die Pflicht zur Information gegenüber dem Zertifikatsinhaber über die Vertragsbedingungen der Haftpflichtversicherung zum Ersatz von Schäden.

369 *Roßnagel*, RMD, § 6 SigG 1997, Rn. 18.

3) darüber, dass eine qualifizierte elektronische Signatur im Rechtsverkehr die gleiche Wirkung wie eine eigenhändige Unterschrift hat, wenn durch Gesetz nichts anderes bestimmt wird.

Während das geltende brasilianische Signaturrecht keine Vorschrift über die Unterrichtungspflicht enthält, sieht Art. 35 Gesetzentwurf Nr. 7.316/2002 als Pflicht für akkreditierte Zertifizierungsdiensteanbieter vor, den Teilnehmer über die Rechtswirkungen elektronischer Signaturen und über die notwendigen Sicherheitsmaßnahmen zum Schutz des privaten Schlüssels sowie zur Erzeugung elektronischer Signaturen zu unterrichten. Diese Vorschrift greift das Thema kurz auf. Wie es im deutschen Signaturrecht der Fall ist, könnte sich die Unterrichtungspflicht auch auf die erforderlichen Maßnahmen zur Prüfung elektronischer Signaturen erstrecken. Ferner könnte die Unterrichtungspflicht die Neusignierung enthalten. Wie bereits dargelegt, spielt die Neusignierung eine wichtige Rolle für Nutzer, die ihre Dokumente langfristig beweiskräftig aufbewahren müssen. Da die Neusignierung keine Selbstverständlichkeit ist, wird vorgeschlagen, sie als Inhalt der Unterrichtungspflicht zusammen mit den erforderlichen Sicherheitsmaßnahmen zur Prüfung einer elektronischen Signatur zu übernehmen. Mit diesen Ergänzungen könnte somit Art. 35 Gesetzentwurf Nr. 7.316 die Unterrichtungspflicht ausreichend normieren.

3.6 Identifikationsaufgaben

Bereits in dieser Arbeit herausgestellt wurde das erhebliche Gewicht der Identifikationsaufgaben innerhalb der gesamten Sicherheitskette einer Public Key Infrastruktur.[370] Zur Notwendigkeit einer persönlichen Mitwirkung bei der Identifizierung des zukünftigen Signaturschlüsselinhabers weist Martínez Nadal zu Recht darauf hin, dass nur mit dieser Prozedur eine sichere Identifikation des Antragstellers geschaffen wird.[371] Diese Sicherheit ist naturgemäß nicht absolut, möglich bleibt als Beispiel immer noch die fehlende Identifikation des Interessenten durch den Zertifizierungsdiensteanbieter. Deswegen ist es sinnvoll, dass Schulungen für Mitarbeiter der Identifikationsstellen zur Erkennung von gefälschten Dokumenten, die bei der Identifikation von Interessenten vorgezeigt werden, stattfinden. Die Anforderung zur persönlichen Mitwirkung des Antragstellers bei seiner Identifizierung gab es schon in dem Entwurf der Signaturrichtlinie. Diese ist aber im Laufe ihrer Bearbeitung gestrichen worden.[372]

Das brasilianische wie das deutsche Signaturrecht unterscheiden sich leicht in den vorgesehenen Verfahren zur Identifikation des Antragstellers. Brasilien verfügt über eine strenge Norm, welche die Identifikation des zukünftigen Signaturschlüssel-

370 Siehe bereits in diesem Teil Gliederungspunkte 1.3.5.4 und 2.2.7.

371 *Nadal* 2004, 115.

372 *Nadal* 2001, 158.

Inhabers nur durch seine persönliche Mitwirkung zulässt (Art. 7 MP 2.200-2). Ausgenommen bleibt nur die Möglichkeit des erneuten Antrags auf ein Zertifikat, wenn der Zertifikatsinhaber vor der Ablauffrist des noch gültigen Zertifikats den Antrag mittels einer akkreditierten, elektronischen Signatur signiert. In Deutschland hingegen gilt die Anforderung des § 5 Abs. 1 SigG, wonach der Zertifizierungsdiensteanbieter verpflichtet wird, den Antragsteller zuverlässig zu identifizieren. Die Konkretisierung der Zuverlässigkeit wird durch das Verfahren des § 3 SigV gegeben. Demgemäß überprüft der Zertifizierungsdiensteanbieter die Identität des Antragsstellers anhand des Personalausweises oder Reisepasses. Ursprünglich bestimmte das SigG, dass die Identifizierung nur durch einen persönlichen Kontakt erfolgen musste. Mit dem Inkrafttreten des ersten Gesetzes zur Änderung des Signaturgesetzes wird aber erlaubt, die vom Zertifizierungsdiensteanbieter zu einem früheren Zeitpunkt erhobenen Daten für die Identitätsprüfung des Antragstellers unter der Voraussetzung zu nutzen, dass diese Daten die zuverlässige Identifizierung des Antragstellers gewährleisten. Eine zuverlässige Identifizierung ist dann gegeben, wenn die Daten gemäß § 3 I SigV anhand eines gültigen Ausweises erhoben wurden und noch aktuell sind.[373] Dies bedeutet, dass die Beantragung sowie die Ausgabe von Signaturerstellungseinheiten ohne persönlichen Kontakt und ohne Unterschrift in Deutschland zugelassen sind.[374] Hierbei genügt zum Beispiel ein mittels PIN und TAN gesicherter elektronischer Antrag.[375] Hauptgrund für die Gesetzesänderung war der Versuch, elektronische Signaturen zu fördern. Dabei wurde gezielt auf die „Herstellung des sicheren elektronischen Rechts- und Geschäftsverkehrs“ geachtet und versucht eine „erforderliche Zahl an Anwendungen und Nutzern zu schaffen.“[376]

Es ist fraglich, ob die Herabsetzung des Sicherheitsniveaus des Identifizierungsverfahrens tatsächlich einen Beitrag für die gewollte Verbreitung der elektronischen Signatur leistet. Wird dem Ansatz gefolgt, liegt der Trugschluss nahe, dass durch weniger Regulierung die Chancen der Verbreitung steigen. Es ist jedoch bereits bekannt, dass die breite Nutzung elektronischer Signaturen sowohl in der gesamten Europäischen Union[377] als auch in der ganzen Welt nicht erreicht wurde, unabhängig von der Regulierungsdichte der einzelnen Länder. Die Durchsetzungsschwächen elektronischer Signaturen sind beispielsweise in Uruguay oder in der Schweiz zu finden, wo die Regulierungsdichte geringer ist. Aber auch in Ländern wie Brasilien oder Deutschland – beide mit einem umfangreicheren Rechtsrahmen – ist der erwünschte Durchbruch von Signaturverfahren nicht erzielt worden. Das Problem dafür liegt vornehmlich in den von Markt und Regierung[378] implementierten Ge-

373 BT.Drs. 15/3417, 4.

374 *Roßnagel*, MMR 2005, 385.

375 *Roßnagel*, MMR 2005, 386.

376 BT-Drs. 15/3417, 6.

377 *Dumortier*/*Kelm*/*Nilsson*/*Skouma*/*van Eecke*, DuD 2004, 141.

378 *Roßnagel*, RMD, SigG Einl., Rn. 326, erwähnt das widersprüchliche Verhalten der deutschen Bundesregierung im Rahmen der Aktionen zur elektronischen Signatur. Auf der einen Seite

schäftsmodellen. Diese bestehen in der Regel aus Insellösungen, welche meistens nur an bestimmte Anwendungen von geschlossenen Nutzergruppen gerichtet sind und somit diametral entgegengesetzt zu dem stehen, was eine Infrastruktur zum Wachsen benötigt.[379]

Das Problem der fehlenden Verbreitung elektronischer Signaturen darf nicht auf Kosten einer Sicherheitsreduzierung bei der Identifikation getragen werden. Das Argument, wonach die persönliche Identifikation des Antragstellers ein unnötiges und bürokratisches Hemmnis sei, läuft fehl und lässt vergessen, dass diese persönliche Mitwirkung lediglich nur einmal im Leben des Zertifikatsinhabers erfolgen muss. Dies wird durch § 3 Abs. 1 Satz 2 SigV ermöglicht. Nach dieser Vorschrift kann der Zertifizierungsdiensteanbieter von einer erneuten Signatur absehen, soweit ein Antrag auf ein qualifiziertes Zertifikat mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments des Antragstellers gestellt wird. Die einmalige persönliche Mitwirkung bei der Identifikation und Signaturkarteausgabe stellt sich infolgedessen als eine absolut zumutbare Anforderung dar. Der Reisepass zum Beispiel wird in Deutschland nach § 6 Abs. 1 Satz 6 PassG nur bei persönlichem Erscheinen des Passbewerbers ausgestellt. Die Gültigkeitsdauer beträgt in der Regel zehn Jahre, jedoch ist bei Personen, welche das 24. Lebensjahr noch nicht vollendet haben, der Reisepass sechs Jahre gültig (§ 5 Abs. 1 PassG). Bei einem erneuten Passantrag wäre dann die persönliche Anwesenheit nochmals erforderlich. Die Sicherheitsanforderungen an die Identifizierung bei der Beantragung eines qualifizierten Zertifikats mit dem Argument des „bürokratischen Hemmnisses“ zu senken, ist deshalb als unangemessen zu bewerten. Insbesondere angesichts der an die qualifizierte elektronische Signatur geknüpften Rechtsfolgen – in Deutschland Schriftformäquivalenz sowie vorweggenommener Anscheinsbeweis –, welche es dem Signaturschlüssel-Inhaber grundsätzlich ermöglichen, unzählige Rechtsgeschäfte im Internet abzuschließen.

Einen Beitrag, das Problem der mangelnden Verbreitung elektronischer Signaturen zu lösen, könnten deutsche Zertifizierungsdiensteanbieter leisten, indem sie mehr Gebrauch von der Möglichkeit des § 4 Abs. 5 SigG machen. Demgemäß kann der Zertifizierungsdiensteanbieter unter Einbeziehung in sein Sicherheitskonzept Aufgaben an Dritte übertragen. Dadurch können die Identifizierungsaufgaben an Dritte ausgelagert werden. Kreditinstitute könnten sich dann beispielsweise als Iden-

schaffe die Bundesregierung einen Rechtsrahmen für qualifizierte Signaturen und deren Anwendung, wie im Fall des Media@Komm-Programms. Auf der anderen Seite aber forciere die Bundesverwaltung mit „SPHINX“ die Nutzung einer parallelen Infrastruktur, die auf einem Sicherheitsniveau weit unterhalb des gesetzlichen und europäischen Standards basiere.

379 Siehe z. B. der Infrastruktur-Begriff von *Hammer*: „ein sozio-technisches System…, das in einer Region oder einem organisatorischen Komplex für viele Nutzer (Anwenderkreis) einen einheitlichen Satz von Leistungsmerkmalen oder Dienstleistungen bereitstellt. Die Nutzer können weitgehend frei entscheiden, wann, wie und zu welchem Zweck sie die von der Infrastruktur bereitgestellten Nutzungsoptionen einsetzen“, *Hammer* 1995, 42.

tifikationsstellen eines bestimmten Zertifizierungsdiensteanbieters präsentieren und von der bereits vorhandenen – in manchen Fällen sogar landesweit verbreiteten – Filialeninfrastruktur profitieren. Eine erste Identifizierung mit persönlichem Kontakt zur Signaturkartenausgabe bliebe aber erforderlich. Diese Variante schafft Transparenz und Nachvollziehbarkeit für den Antragsteller. So kann er bewusst entscheiden und ist informiert, dass die bei der Gelegenheit erhobenen Daten zur Ausstellung eines Zertifikats dienen. Darüber hinaus erhält er einen opportunen Anlass, über die Rechtswirkung und Sicherheitsmaßnahmen bei der Nutzung seines Zertifikats vom Identifikationsdienstleister unterrichtet zu werden.

In diesem Punkt zeigen sich folglich die Lösungen des ursprünglichen SigG 2001 und des brasilianischen Signaturrechts geeigneter, um die notwendige Sicherheit einer Public Key Infrastruktur mit beweisrechtlichen Folgen zu gewährleisten.

3.7 Zertifikatsinhaber

Ein weiteres dem Rechtsvergleich zwischen deutschem und brasilianischem Signaturrecht zugängliches Thema ist die Unterscheidung der möglichen Zertifikatsinhaber. Die brasilianische Regulierung (Art. 1.1.5 Resolução Nr. 41) lässt die Zuordnung eines Zertifikats zu natürlichen Personen, juristischen Personen, Anwendungen, Automaten und funktionalen Einheiten wie z.B. Servern zu. In Deutschland hingegen werden ausnahmslos Zertifikate nur für natürliche Personen ausgestellt. Der Grund für diese Beschränkung, gemäß der amtlichen Begründung zum Signaturgesetz, liegt in der von der Signaturrichtlinie (Art. 5 Abs. 1 RLeS) vorgegebenen rechtlichen Gleichstellung der qualifizierten elektronischen Signatur mit der eigenhändigen Unterschrift.[380] Argumentiert wird folglich, dass wie eine handschriftliche Unterschrift auch die elektronische Signatur immer an eine natürliche Person gebunden sein soll.[381] Hierbei wird aber außer Acht gelassen, dass elektronische Signaturen nicht immer und nicht nur als Schriftformersatz zum Einsatz kommen.[382] Für eine Rechnung gemäß § 14 Abs. 4 UStG sowie die Neusignierung nach § 17 SiGV ist die Signatur kein Substitut für die eigenhändige Unterschrift.[383] Hierbei zeichnen sich die Unveränderbarkeit und die Echtheit der elektronisch signierten Rechnung als die wichtigsten Eigenschaften aus.[384]

Ein weiteres Beispiel dafür sind die SSL-Server-Zertifikate-Signaturen, welche eine zuverlässige Authentifizierung von Webservern im Browser des Websitebesuchers ermöglichen, um einen Beitrag zur Erhöhung der Sicherheit elektronischer

380 BT-Drs. 14/4662, 19; hierzu auch S. www.bundesnetzagentur.de → elektronische Signatur → FAQ → Frage 19.

381 *Bieser*/*Kersten* 1998, 50.

382 *Viefhues*/*Hoffmann*, MMR 2003, 76.

383 *Roßnagel*/*Fischer-Dieskau*, MMR 2004, 135.

384 *Schröder*, DuD 2004, 666.

Rechtsgeschäfte zu leisten. Dadurch können Verbraucher erkennen, dass sie sich auf der gesuchten und nicht auf einer gefälschten Website befinden. Dieses Zertifikat gewinnt immer mehr an Bedeutung angesichts der wachsenden Verbreitung der so genannten „Phishing"- Angriffe[385], bei denen versucht wird, über gefälschte Internetadressen Daten eines Internetanwenders – vor allem Benutzernamen und Passwörter – zu erlangen.[386] Darüber hinaus schafft das SSL-Server-Zertifikat eine sichere Verbindung zwischen Kundenbrowser und Server, indem der ausgetauschte Inhalt nur verschlüsselt über das Netz geht.[387]

Die elektronische Signatur, basierend auf einem SSL-Server-Zertifikat, stellt somit keine Funktionsäquivalenz zur eigenhändigen Unterschrift dar. Sie dient grundsätzlich der sicheren Feststellung der Identität des Servers durch den Browser des Besuchers sowie der verschlüsselten Kommunikation zwischen diesen beiden.[388] Die Online-Banking-Anwendung der brasilianischen Bank Banrisul ist ein Beispiel dafür. Dieses Zertifikat wird für die juristische Person „Banco Banrisul" von dem akkreditierten Zertifizierungsdiensteanbieter AC Serasa ausgestellt. Im allgemeinen Feld des Zertifikats „ausgestellt für" steht der Domainname der Online-Banking-Anwendung „www.banrisul.com.br". Unter „Details" des Zertifikats steht unter dem Feld „Antragsteller" sowohl der erwähnte Domainname als auch der vollständige Name der juristischen Person „Banco do Estado do Rio Grande do Sul". Die Ausstellung eines solchen Zertifikats ist im deutschen Signaturrecht – zumindest auf den fortgeschrittenen und qualifizierten Ebenen – nicht möglich. Die Lösung nach geltendem Recht wäre die Ausstellung eines Zertifikats für einen Mitarbeiter und ein weiteres Attributszertifikat mit der Information der Server- oder Anwendungsbezeichnung (z.B. Internetbanking der Bank „x"). Problematisch wären aber im Falle eines Stellenwechsels dieses Mitarbeiters die gegebenenfalls notwendige Anpassung und der Rückruf des Zertifikats. Eine andere ebenfalls unbefriedigende Lösung wäre der Einsatz von Pseudonymen mit Angaben der Anwendung bei normalen, für natürliche Personen ausgestellten Zertifikaten. Bei beiden Lösungen wird die erforderli-

385 Zum Thema „Phishing"-Angriffe, siehe http://www.technicalinfo.net/papers/Phishing.html und *Karper*, DuD, 2006, 215.

386 Laut einer nicht repräsentativen Umfrage der Arbeitsgruppe Identitätsschutz im Internet, einer nationalen Forschungsgruppe, die sich mit der Problematik des Identitätsdiebstahls beschäftigt, gaben 2% der Befragten an, dass ein Schaden durch Missbrauch ihrer Zugangsdaten entstanden ist; hierzu *Gajek*/*Schwenk*/*Wegener*, DuD, 2005, 639.

387 Hierzu siehe auch http://www.ssl.de/ssl.html.

388 Bei der Anwendung von Zertifikaten über das SSL-Protokoll wird nur die Übertragung zwischen der Webserverdomain und dem Besucher gesichert. Was danach mit den gesicherten übertragenen Daten passiert, ist von dem was durch das SSL-Protokoll geregelt ist, abhängig bzw. davon, wie der Shop-Betreiber die Information weiterverarbeitet. Siehe hierzu http://www.ssl.de/ssl.html.

che Transparenz beeinträchtig.[389] Bei den so genannten automatisierten Signaturen ist ebenfalls die Transparenz gefährdet. Ohne ein spezifisches Zertifikat für Automaten lässt sich die automatisierte Erzeugung von Signaturen nicht erkennen.[390]

Zu berücksichtigen ist auch, dass die Signaturrichtlinie die Ausstellung von Zertifikaten auf juristische Personen nicht ausschließt.[391] Nach Art. 2, Nr. 3 RLeS ist Unterzeichner 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. Die Definition eines Zertifikats (Art. 2 Nr. 9 RLeS) schließt ebenfalls nicht die Zuordnung einer juristischen Person aus. Innerhalb der Europäischen Union hat beispielsweise u.a.[392] Spanien die Möglichkeit von Zertifikaten für juristische Personen geregelt (Art. 7 Ley 59/2003).[393] Die Gesetzesbegründung betont die steigende Bedeutung und Verbreitung solcher Zertifikate in den letzten Jahren.[394] Besonders hervorgehoben wird, dass die Streitigkeiten und die Rechtsunsicherheit nach der Einführung der Zertifikate für juristische Personen nicht gestiegen seien.[395] Dies begründe auch ihre fast unbeschränkte Zulässigkeit.[396]

Da keine europarechtlichen Hindernisse der Einführung von Zertifikaten für juristische Personen ins deutsche Signaturrecht im Weg stehen, ist diese zu empfehlen. Des Weiteren ist zu betonen, dass die Literatur in Deutschland schon seit langem kontinuierlich Zertifikate für juristische Personen fordert. [397] Hierbei könnte das deutsche Signaturrecht den Ansatz der brasilianischen Regulierung befolgen, wonach Zertifikate grundsätzlich für natürliche Personen, juristische Personen, Auto-

389 Sogar die Bundesnetzagentur erkennt an, dass in diesen Fällen ein Pseudonym zur Verwirrung der Anwender beiträgt. S. www.bundesnetzagentur.de → elektronische Signatur → FAQ → Frage 19.

390 *Roßnagel*/*Fischer-Dieskau*, MMR 2004, 139.

391 *Nadal* 2004, 120; *Skrobotz*, DuD 2004, 411; *Kunstein* 2005, 183.

392 Österreich, Dänemark und die Niederlande haben ebenso die Möglichkeit für Zertifikate juristischer Personen vorgesehen. Hierzu *Skrobotz*, DuD 2004, 411.

393 Zum Gesetztext und -Begründung: S. http://www.mityc.es/ → Legislación → Legislación Industria, Turismo y Comercio → Sociedad de la Información → Internet y firma electrónica.

394 Im Rahmen des von Ley 59/2003 aufgehobenen Real Decreto Ley 14/1999 waren Zertifikate für juristische Personen nur für die Verbindung zwischen Unternehmen und der Finanzverwaltung zulässig; hierzu Begründung zu Ley 59/2003, 45330.

395 Begründung zu Ley 59/2003, 45330.

396 Fast unbeschränkte Zulässigkeit, denn Art. 7 Nr. 3 beschränkt die Nutzung des Zertifikats einer juristischen Person auf die Verhältnisse zur öffentlichen Verwaltung und auf die Anwendungen, die in Bezug auf ihre normalen Tätigkeiten stehen. Zur Notwendigkeit einer extensiven Auslegung des Begriffs „normale Tätigkeiten“, *Nadal* 2004, 132.

397 *Roßnagel*, DuD 1997, 79; *Fox*, DuD 1999, 510; *Roßnagel*, NJW 1999, 1594 f.; *Roßnagel*/*Fischer-Dieskau*, MMR 2004, 139; *Skrobotz*, DuD 2004, 411; *Kunstein* 2005, 183; *Fischer-Dieskau* 2006, 284. Hierzu auch § 9 Abs. 2 Satz 3 des Gesetzentwurfs von provet 1996, abrufbar unter: http://www.provet.org/bib/mmge/er-g.htm.

maten und funktionale Einheiten ausgestellt werden können (Artikel 1.1.5 Resolução Nr. 41). Obwohl in solchen Zertifikaten der Name einer natürlichen Person nicht eingetragen wird, muss immer eine Person für seine Nutzung verantwortlich sein, da letztlich immer eine natürliche Person über den Einsatz von Rechnern entscheidet. Diese muss ein entsprechendes Formular unterschreiben, indem sie die Verantwortung für die Nutzung des Zertifikats übernimmt. Wird ein Stellenwechsel des verantwortlichen Mitarbeiters für das Zertifikat erforderlich, dann muss dieses nicht gesperrt werden, sondern nur die Verantwortlichkeit für die Nutzung vom alten an den neuen Mitarbeiter übertragen werden.

3.8 Limitierung im Zertifikat

Das deutsche Signaturrecht sieht in § 7 Abs. 1 Nr 7 SigG die Möglichkeit des Eintrags von Angaben im Zertifikat vor, welche die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt.[398] In Brasilien dagegen wird keine Möglichkeit normiert, Beschränkungen im Zertifikat einzutragen.[399] Die einzige Möglichkeit nach dem brasilianischen Signaturrecht, die Nutzung eines privaten Schlüssels zu beschränken, basiert auf der Grundlage einer vertraglichen Klausel zwischen Zertifizierungsdiensteanbietern und Signaturschlüssel-Inhabern. Dass ein Dritter, welcher auf ein solches Zertifikat vertraut, Kenntnis von der Vereinbarung bekommt, ist fraglich.[400] Auch wenn die Beschränkung im „Certification Practice Statement" des Zertifizierungsdiensteanbieters enthalten sein kann, darf nicht davon ausgegangen werden, dass der Signaturempfänger ohne weiteres, Kenntnis davon nimmt. Das „Certification Practice Statement" ist in der Regel ein äußerst ausführliches Dokument, mit bis zum Teil über vierzig Seiten, welches sich nicht so einfach für den normalen Nutzer zugänglich[401] und verständlich machen lässt. Diese Lösungen reichen folglich nicht aus, die Nutzung eines Zertifikats auf die notwendige Transparenz zu beschränken.

Die Möglichkeit, eine Limitierung im Zertifikat einzutragen, würde nicht nur für den Signaturschlüssel-Inhaber von Vorteil sein, sondern auch indirekt zur gesamten Sicherheit der brasilianischen PKI beitragen. In erster Linie dient die Begrenzung dem Selbstschutz des Signaturschlüssel-Inhabers dadurch, dass das Risiko im Fall des Verlustes oder des Diebstahls der Signaturkarte limitiert würde. In diesem Fall

398 Zur Beschränkung im Zertifikat siehe oben in diesem Teil 1.3.5.8.2.

399 Der Gesetzentwurf Nr. 7.316/2002 enthält keine Vorschrift zur Zertifikatsbeschränkung.

400 Über die Bedeutung einer Zertifikatsbeschränkung für potenzielle Vertragspartner des Signaturschlüssel-Inhabers siehe *Fischer-Dieskau*/*Gitter*/*Hornung*, MMR 2003, 385.

401 Im am weitesten verbreitet Zertifikatsformat – X.509v3 – besteht die Möglichkeit im Feld „Allgemein" → Ausstellererklärung, von dem „Certificate Practice Statement" oder von der „Certificate Policy" Kenntnis zu nehmen. Fraglich ist hierbei aber, ob sich der normale Nutzer dieser Information überhaupt bewusst ist.

hat die Beschränkung einen verbraucherschützenden Charakter.[402] Zum anderen schützt die Beschränkung vor der übereilten Abgabe einer elektronischen Erklärung.[403] Die Funktion der Risikokalkulation für den Zertifizierungsdiensteanbieter wäre im brasilianischen Signaturrecht von der Beschränkung nur teilweise erfüllt. Anders als in Deutschland tritt die Schadenersatzpflicht für brasilianische Zertifizierungsdiensteanbieter nicht innerhalb von Grenzen ein[404], sondern ist prinzipiell unbeschränkt.[405] Dies bedeutet eine leichte Erschwerung der Kalkulierbarkeit einer Begrenzung, schließt sie aber nicht vollständig aus. In der Regel sollen Einschränkungen aus dem Zertifikat jedermann und jeder Anwendung ersichtlich sein.[406] Haftungsansprüche aus überschrittenen Nutzungen sind daher kaum zu erwarten. In diesem Zusammenhang wäre die Möglichkeit des Eintrages einer Beschränkung im Zertifikat auch für die Einschätzung der erforderlichen Mindestdeckungssumme der Versicherung hilfreich. Stellt ein Zertifizierungsdiensteanbieter nur Zertifikate mit eingetragenen Limitierungen aus, sind die Risiken vorhersehbarer. Dies würde den Abschluss eines Versicherungsvertrages und die Einschätzung der erfordernden Deckungssumme durch die Aufsichtsbehörde erheblich erleichtern.[407]

Darüber hinaus kann die Beschränkung bei der dienstlichen Nutzung des Zertifikats eine wichtige Rolle spielen. Hier bietet sich dem Arbeitgeber die Alternative an, das Zertifikat des Arbeitnehmers ausschließlich für berufsmäßige Zwecke zu beschränken.[408] Ferner kann das Zertifikat für Vertretungszwecke beschränkt werden. Der Signaturschlüssel-Inhaber könnte eine Handlungsvollmacht seitens Dritter erhalten, welche beschränkt werden soll. Es bietet sich somit den Vertretenen die Möglichkeit, durch die Eintragung einer Beschränkung, welche sich auf das Handeln

402 *Malzer* 2002, 195.

403 *Fischer-Dieskau*/*Gitter*/*Hornung*, MMR 2003, 385.

404 Gemeint hier ist die Haftungsbeschränkung des § 11 Abs. 3 SigG, wonach die Ersatzpflicht nur im Rahmen der auf das qualifizierte Zertifikat eingetragene Beschränkungen eintritt.

405 Die Einführung einer Haftungsregelung mit Haftungsgrenzen wäre für das brasilianische Recht prinzipiell undenkbar. Das brasilianische Verbraucherrecht (CDC Art. 51, I) lässt Haftungsbeschränkungen nur ausnahmsweise zu, wenn es sich bei dem Verbraucher um eine juristische Person handelt. Zudem muss die Beschränkung auch begründet sein. Hierzu STJ, REsp 348.343-SP, Rel. Min. *Humberto Gomes de Barro*, v. 26.6.2006; TJSP, ApC 892.332-0/1, Rel. Des. *Cristina Zucchi*, v. 14.3.2007; TJSP, ApC 923.468-0/6, Rel. Des. *Walter César Exner*, v. 05.6.2008.

406 Dafür aber muss der Signierende entweder das Zertifikat abrufbar halten lassen oder es jeder signierten Nachricht hinzufügen. Hierzu *Fischer-Dieskau*/*Gitter*/*Hornung*, MMR 2003, 385.

407 Wie schon im Gliederungspunkt 2.2.9.1.8.4 dargelegt, besteht in Brasilien keine Mindestsumme für die Versicherung für Zertifizierungsdiensteanbieter. Die Mindestsumme wird von der Aufsichtsbehörde im Einzelfall bestimmt.

408 *Fischer-Dieskau*/*Gitter*/*Hornung*, MMR 2003, 384.

im Rahmen dieser Vollmacht bezieht, die Folgen des Handelns in seinem Namen zu begrenzen.[409]

Aufgrund der hier dargestellten Vorteile ist die Einführung einer Vorschrift zur Möglichkeit eines Beschränkungseintrags im Zertifikat in das brasilianische Signaturrecht zu empfehlen.

3.9 Zertifikatssperrung

Bezüglich der Zertifikatssperrung legt das brasilianische Signaturrecht einen maximalen Zeitraum fest, in welchem der Zertifizierungsdiensteanbieter das Sperrverfahren abzuschließen hat. Nach Art. 4.4.3.3 Resolução Nr. 42 beträgt dieser maximale Zeitraum zwölf Stunden für alle Zertifikatstypen, gerechnet ab dem Eingang des Sperrantrags. Diese einheitliche maximale Reaktionszeit bis zum Wirksamwerden des Sperrantrags kann große Unsicherheiten mit sich bringen. Dies ist besonders dann der Fall, wenn es sich um einen dringlichen Rückrufgrund handelt, wie etwa bei einem Diebstahl oder Abhandenkommen der Signaturkarte. Angenommen der Signaturschlüsselinhaber wird überfallen und seine Signaturkarte von Unberechtigten missbraucht, so könnten diese in dem Zeitraum von 12 Stunden erheblichen Schaden verursachen. Die Vorschrift erfüllt höchstens die Sicherheitsbedürfnisse der weniger dringlichen Rückrufgründe[410], wie unter anderem der Defekt des mit dem Datenspeichers zugehörigen geheimen Schlüssel, das Vergessen durch den Schlüsselinhaber der PIN, das Verlassen des Unternehmens, das ihm das Schlüsselpaar für berufliche Zwecke ausgestellt hat oder wenn er seine Zertifikatsdaten ändern muss.[411] In allen diesen Fällen mag die maximale Zeit für die Sperrung von 12 Stunden ausreichend sein. Zu erwähnen ist ebenso das Beispiel von *Pordesch* und *Bertsch*[412], wonach der Signaturschlüssel-Inhaber selbst als Angreifer in Frage kommen könnte. Im skizzierten Fall könnte der Signaturschlüssel-Inhaber eine Zertifikatssperrung beantragen und kurz danach riskante Kaufaufträge mittels seines privaten Schlüssels an der Börse abgeben. Falls die Kursentwicklung ihn nicht favorisiert, könnte er seine nach dem Sperrantrag abgegebenen Signaturen bestreiten.

Die Regel (Art. 4.4.3.5 Resolução Nr. 42), wonach der Zertifizierungsdiensteanbieter für den Missbrauch des privaten Schlüssels in der Zeit zwischen dem Eingang des Sperrantrags und dem Eintritt der Sperrwirkung haftet, ist aus diesem Grunde

409 *Fischer-Dieskau*/*Gitter*/*Hornung*, MMR 2003, 385.

410 Als verpflichtende Rückrufgründen sieht Art. 4.4.1.2 der Resolução Nr. 42 folgende Fälle vor: a) defekte Erstellung des Zertifikats; b) Notwendigkeit der Änderung der Zertifikatsangaben; c) Auflösung des Zertifizierungsdiensteanbieters; d) Kompromittierung des privaten Schlüssels oder des Speichermittels.

411 Für die Beispiele und die Unterscheidung zwischen dringlichen Rückrufgründen und weniger dringlichen Rückrufgründen, *Fox*, DuD 2001, 485.

412 *Bertsch*/*Pordesch*, DuD 1999, 515.

unzureichend. Sie mildert zwar die negativen Auswirkungen der übertrieben zulässigen Reaktionszeit, behebt aber nicht die daraus resultierenden Unsicherheiten. Die Chancen eines erfolgreichen Missbrauchs von Signaturschlüsseln mit Schaden für Signaturempfänger, Signaturschlüsselinhaber und Zertifizierungsdiensteanbieter bleiben groß. Obwohl im Endeffekt die Zertifizierungsdiensteanbieter in der Regel für die Schäden haften werden, wird eine unnötige Atmosphäre von Unsicherheit und Misstrauen geschaffen, bei einer Infrastruktur, die gerade das Gegenteil verspricht. Dies gilt insbesondere, wenn berücksichtigt wird, dass die Signaturen innerhalb der ICP-Brasil praktisch zu allen möglichen Verwendungszwecken gebraucht werden können. Hinzu kommt, dass noch keine Möglichkeit einer Beschränkung im Zertifikat besteht.[413]

Vernünftiger in diesem Zusammenhang stellt sich die deutsche Norm zur Sperrung von qualifizierten Zertifikaten dar. Laut § 8 SigG hat der Zertifizierungsdiensteanbieter ein qualifiziertes Zertifikat unverzüglich zu sperren, wenn ein Signaturschlüssel-Inhaber oder sein Vertreter dies verlangt. Aus der generalklauselartigen Formulierung des Ausdrucks „unverzüglich", ist nichts anderes als eine Aufforderung zur Durchführung der Sperrung in wenigen Minuten nach dem Eingang des Sperrantrags zu entnehmen. Diesbezüglich empfiehlt der Maßnahmenkatalog des BSI[414], dass die Reaktionszeit bis zum Wirksamwerden des Sperreintrags zehn Minuten nicht überschreiten darf.[415] Obwohl die Maßnahmenkataloge des BSI seit dem Inkrafttreten des Signaturgesetzes nur einen empfehlenden Charakter besitzen[416], sind sie als wertvolle Dokumente zu betrachten. Die Angaben der Maßnahmenkataloge sind von Experten aus Wirtschaft und Wissenschaft erarbeitet und abgestimmt worden.[417]

Es wird somit für das brasilianische Signaturecht empfohlen, die bestehende einheitliche maximale Reaktionszeit zur Durchführung einer Sperrung von zwölf Stunden zu streichen. Dies sollte aufgrund der Unsicherheiten geschehen, die ein solch übertriebener Zeitraum für ein so ausschlaggebendes Verfahren beinhaltet. Weiter-

413 Für eine dogmatische Analyse des Eintrags einer Beschränkung im Zertifikat s. *Fischer-Dieskau*/*Gitter*/*Hornung*, MMR 2003, 384. Die vorliegende Doktorarbeit schlägt vor, dass in Brasilien die Möglichkeit geregelt wird Beschränkungen im Zertifikat einzutragen; siehe hierzu oben Gliederungspunkt 3.8.

414 BSI-SigI-B4.

415 Das Handbuch des BSI erklärt hierzu aber, dass diese Zeit nicht der Zeitpunkt ist, bis zu der der Sperreintrag online verfügbar sein soll, sondern der Zeitpunkt, ab dem die Sperrung gelten soll; BSI-SigI-B4, 65.

416 BSI-GeS, 6.

417 Denn im Rahmen des § 12 Abs. 2 Satz 1 SigV 1997 war die Bundesnetzagentur verpflichtet, einen Katalog von geeigneten Sicherheitsmaßnahmen im Bundesanzeiger zu veröffentlichen. Die Maßnahmen sollten von den Zertifizierungsdiensteanbietern bei der Erstellung des Sicherheitskonzeptes berücksichtigt werden. Die Angaben hierfür waren vom Bundesamt für Sicherheit mit Beteiligung aus Wirtschaft und Wissenschaft erstellt worden.

hin wird empfohlen, eine Formulierung wie „imediatamente“ (sofortig oder umgehend) in diesem Zusammenhang zu übernehmen. Diese Wortwahl würde klarstellen, dass die Reaktionszeit zur Erzeugung eines Sperreintrages ohne Verzögerungen und innerhalb von Minuten durchzuführen ist. Eine zweite denkbare Formulierung wäre die des Maßnahmenkatalogs des BSI, wonach die Reaktionszeit zum Wirksamwerden eines Sperreintrags zehn Minuten nicht überschreiten darf.[418] Diese Variante wäre aber weniger flexibel. Wird der Wortlaut „imediatamente“ übernommen, dann bleibt ein gewisser Spielraum, indem der Zertifizierungsdiensteanbieter in den konkreten Umständen so schnell wie möglich reagieren muss. Beide signalisieren jedoch, dass das Sperrverfahren innerhalb von wenigen Minuten abzuschließen ist und wären im Ergebnis gleich effektiv.

3.9.1 Die Frage der Sperrlisten x OCSP

Hinsichtlich des Abschlusses des Sperrverfahrens unterscheiden sich die verglichenen Signaturregelungen ebenfalls. Während in Brasilien gesperrte Zertifikate in der Regel in eine Sperrliste eingetragen werden, verlangt das deutsche Signaturrecht die Führung eines Verzeichnisses, welches eine Aussage über die Gültigkeit von Zertifikaten ermöglicht. In Deutschland ist somit eine Auskunftsmöglichkeit darüber erforderlich, ob der Zertifizierungsdiensteanbieter das Zertifikat tatsächlich ausgestellt hat. Dies ist derzeit nur über eine OCSP-Abfrage technisch realisierbar.[419] Der OCSP-Dienst gibt Auskunft darüber, ob das Zertifikat gültig ist, gesperrt oder sogar nicht ausgestellt wurde (Existenznachweis). Das Risiko, dass ein Zertifikat beim Zertifizierungsdiensteanbieter gar nicht existiert, kann somit vom Prüfenden nur mittels einer OCSP-Abfrage ausgeschlossen werden.[420] Ein weiterer Vorteil der OCSP-Abfrage liegt in ihrer Aktualität, da sie im Gegensatz zu Sperrlisten, die Möglichkeit bietet, eine zeitnahe Statusüberprüfung durchzuführen. Dagegen werden die Sperrlisten meistens in regelmäßigen Zeitabständen – in Brasilien alle sechs Stunden – aktualisiert. Dies bringt eine beachtlich hohe Ungenauigkeit bei der Statusabfrage mit sich, was wiederum zu Unsicherheiten führen kann.[421] Insbesondere kritisch zu beurteilen ist dies angesichts der bereits oben erwähnten übertriebenen maximalen Reaktionszeit von zwölf Stunden zum Wirksamwerden einer Sperrung innerhalb der brasilianischen Public Key Infrastruktur. Werden die maximale Reaktionszeit zum Wirksamwerden der Zertifikatssperrung mit dem maximalen Zeitabstand für die Aktualisierung der Sperrlist addiert, dann resultiert eine mögliche ma-

418 *Bertsch* und *Pordesch* schlagen auch die Festsetzung „zumindest garantierter Maximalbearbeitungszeiten“ bezüglich des Sperrverfahrens vor. *Bertsch*/*Pordesch*, DuD 1999, 515.

419 S. dazu bereits in diesem Teil Gliederungspunkt 1.3.5.6.2.

420 *Fischer-Dieskau* 2006, 100.

421 *Roßnagel* bewertet die Sperrlisten als nur begrenzten Schutz gegen das Erstellen echter Signaturen, *Roßnagel* 1995, 274.

ximale Zeitspanne für den Abschluss des gesamten Verfahrens von 18 Stunden. Darüber hinaus stellt die Schnelligkeit der Antwort bei der OCSP-Abfrage einen Pluspunkt gegenüber den Sperrlisten dar. Diese enthalten in der Regel einen großen Umfang von Zertifikaten, welche im Laufe der Zeit mit den durchgeführten Sperrungen immer umfangreicher werden.[422] Anders beim OCSP-Dienst, der auf einem Internet-Protokoll basiert und auf die Abfrage einer Anwendung mit einer kurzen elektronisch signierten Antwort zu jedem angefragten Zertifikat reagiert.[423] Was die Kosten anbelangt, ist der OCSP-Dienst bei Einzelabfragen sogar billiger als das Herunterladen der Sperrlisten, die in der Regel mit höherem Administrationsaufwand verbunden sind. Darüber hinaus verursacht das häufige Publizieren zur Verteilung der Sperrinformationen mittels einer Sperrliste eine hohe Netzbelastung.

Für das brasilianische Signaturrecht wird deshalb empfohlen, die Onlineanfrage des Zertifikatsstatus und die entsprechende Antwort bezüglich der Gültigkeit durch das Online Certificate Status Protocol (OCSP) zu implementieren. Obwohl die Führung eines OCSP-Dienstes im Rahmen der brasilianischen Regulierung bereits vorgesehen ist, spielt sie angesichts ihres fakultativen Merkmals keine praktische Rolle. Sie sollte daher zur Erhöhung der gesamten Sicherheit als Pflicht für den Zertifizierungsdiensteanbieter eingeführt werden.

3.9.2 Form des Sperrantrags

Wie schon dargestellt, bleiben die Form des Sperrantrags und die in diesem Verfahren notwendige Authentisierung im brasilianischen Signaturrecht offen.[424] Geregelt ist lediglich die Pflicht des Zertifizierungsdiensteanbieters, einen Dienst bereitzustellen, der „leicht und jederzeit" die Sperrung des Zertifikats durch die Berechtigten ermöglicht.[425] Die Vorschrift spricht nicht von Schnelligkeit, was bei diesem Verfahren jedoch ausschlaggebend ist. Der Zertifizierungsdiensteanbieter muss dabei den Antragsteller identifizieren und das Verfahren sowie die Begründung zur Sperrung dokumentieren. Vorhergehend wurden bereits zwei Beispiele erwähnt, wie Zertifizierungsdiensteanbieter das Sperrverfahren durchführen können. Die AC Certisign[426] und die AC Serasa[427] realisieren ein Sperrverfahren, bei dem der Antragsteller ein Webformular ausfüllt. Zur Authentisierung benutzt der Zertifikatsinhaber einen Satz als Passwort, der ihm bei der Zertifikatserzeugung von der Zertifi-

422 Um dem erheblichen Umfang der Sperrlisten entgegenzuwirken, besteht die Möglichkeit, diese in Teillisten - nach bestimmten Kriterien wie beispielsweise Zertifikatstypen zu ordnen – und aufgespaltet zu veröffentlichen, s. *Fox*, DuD 2001, 485.

423 *Nitschke*/*Dahm*, DuD 2005, 143.

424 Hierzu bereits in diesem Teil Gliederungspunkt 2.2.9.1.4.2.

425 Art. 4.4.3.1, Resolução Nr. 42.

426 S. dazu http://icp-brasil.certisign.com.br/repositorio/index.htm.

427 S. dazu http://publicacao.certificadodigital.com.br/repositorio/pc/politica-a2.pdf.

zierungsstelle übergeben wurde. Fraglich ist, ob die Konkretisierung des Sperrverfahrens dem Zertifizierungsdiensteanbieter völlig überlassen bleiben sollte, obwohl es sich um ein derartig entscheidend wichtiges Verfahren innerhalb einer PKI handelt.

Das deutsche Signaturrecht sieht hierfür die Pflicht des Zertifizierungsdiensteanbieters vor, eine Rufnummer bereit zu stellen, unter der die Sperrung der qualifizierten Zertifikate durchgeführt wird (§ 7 Abs. 1 SigV). Die deutsche Lösung scheint sachgemäßer als die brasilianische. Besser geeignet wäre die Übernahme einer Vorschrift, welche wenigstens als Alternative zu einem Webformular[428] – besonders für die dringenden Sperrgründe – die Bekanntgabe einer Telefonnummer vorsieht, durch die der Zertifizierungsdiensteanbieter zur Sperrung aufgefordert werden kann. Werden keine Anforderungen zur Form des Sperrantrags festgelegt, können sowohl effizientere als auch weniger effiziente Mittel zu diesem Zweck verwendet werden. Gilt eine Mindestbearbeitungszeit bis zum Wirksamenwerden der Sperrung von 12 Stunden, dann kann ein Webformular allein möglicherweise ausreichend sein. Wird aber die in dieser Arbeit vorgeschlagene Reduzierung der Reaktionszeit zur Bearbeitung des Sperrantrags realisiert, dann wird die Bedeutung des gesamten Verfahrens signalisiert. Damit verbunden ist folglich eine breitere Auswahl von Wegen für den Signaturschlüssel-Inhaber zur Sperrung des Zertifikats. Die Möglichkeit einer Rufnummer als Alternative zum Webformular kann bei den Fällen des Abhandenkommens der Signaturerstellungseinheit und eines mobilen Gerätes wie etwa eines Notebooks behilflich sein. Für einen schnellen Sperrantrag bleibt dem Signaturschlüssel-Inhaber das Telefon als die beste Wahl. Hierzu ist die amtliche Begründung des § 7 Abs. 1 SigV zu erwähnen, wonach im Gegensatz zu anderen Netzverbindungen das Telefon nach dem aktuellen Stand der Technik praktisch überall und jederzeit rasch verfügbar ist. Die Begründung zur Signaturverordnung bezieht sich auf den Stand der Technik in Deutschland vor mehr als zehn Jahren. Sowohl in Brasilien als auch in Deutschland hat sich das Internet mittlerweile beinahe flächendeckend verbreitet. Ein Internetanschluss lässt sich heutzutage viel eher als vor zehn Jahren in beiden Ländern finden.[429] Trotz dieser Entwicklung ist jedoch das Telefon als Kommunikationsmittel – besonders in Brasilien – noch deutlicher verbreitet.[430] Verliert man seine Signaturkarte, dann benutzt man entweder sein Mobiltelefon oder

428 Auch im brasilianischen Signaturrecht sind Webformulare nicht vorgesehen, werden aber wie erwähnt von den meisten akkreditierten Zertifizierungsdiensteanbietern verwendet.

429 17% der brasilianischen Haushalte verfügen über einen Internetzugang; Comitê Gestor da Internet no Brasil, 2008,138. Im 1. Quartal 2006 waren 61,4% der deutschen Haushalte mit Internetzugang ausgerüstet; Statistisches Bundesamt 2007, 17.

430 Das zeigt zum Beispiel die Statistik über mobile Telefone. Im Februar 2008 betrug die Zahl der Anschlüsse 122,86 Millionen bei ca 180 Millionen Einwohnern in Brasilien; Comitê Gestor da Internet no Brasil, 2008, 218. Siehe hierzu auch http://www.anatel.gov.br/Portal/exibirPortalInternet.do#.

man findet sowohl in Brasilien als auch in Deutschland immer noch eine Telefonzelle eher und leichter – besonders in kleinen Ortschaften –als ein Internetcafé.

Es wird mithin für das brasilianische Recht vorgeschlagen, die Pflicht für die Zertifizierungsdiensteanbieter, eine Telefonverbindung zum Zweck einer unverzüglichen Zertifikatssperrung einzuführen.

3.10 Haftung

Wie in dieser Arbeit bereits angeführt[431], können Haftungsregelungen in Sicherungsinfrastrukturen vergleichbar einer PKI eine bedeutende Rolle spielen. Sie leisten einen Beitrag dabei, den Verbraucherschutz, das Vertrauen sowie die Akzeptanz von Signaturverfahren zu fördern.

Die Haftung wird in beiden Ländern unterschiedlich behandelt.[432] Das Signaturgesetz legt eine deliktische Haftungsnorm fest, wonach Ersatzberechtigte nur Dritte sind, die kein vertragliches Verhältnis zum Zertifizierungsdiensteanbieter haben. Werden die Anforderungen des Signaturgesetzes oder der Signaturverordnung verletzt, müssen Zertifizierungsdiensteanbieter nach § 11 Abs. 1 Satz 1 SigG die daraus resultierenden Schäden den Dritten ersetzen. Es handelt sich hierbei um eine Verschuldenshaftung mit Beweislastumkehr. Gegenüber dem Signaturschlüssel-Inhaber haftet der Zertifizierungsdiensteanbieter aufgrund des zwischen beiden abgeschlossenen Vertrags. Im brasilianischen Signaturrecht ist die Situation anders. Hier finden sich keine Haftungstatbestände in der MP 2.200-2, sondern diese werden lediglich in den Beschlüssen des Regulierungsausschusses vorgesehen. Art. 2.2.1.1 Resolução Nr. 41 regelt die Haftung, indem sie die Pflicht der Zertifizierungsstellen zur Ersetzung der von ihnen verursachten Schäden bestimmt. Diese Pflicht erstreckt sich auch auf die anderen an den Zertifizierungsdiensteanbieter vertraglich gebundenen Dienstleister wie Identifikationsstellen und virtuelle Zertifizierungsstellen. Dabei besteht eine gesamtschuldnerische Haftung (Art. 2.2.1.2) zwischen dem Hauptzertifizierungsdiensteanbieter und dem an ihn gebundenen Dritten. Der Unterschied zu Deutschland ist, dass während die Haftungsvorschriften des Signaturgesetzes nur im Verhältnis von Zertifizierungsdiensteanbietern zu Dritten anwendbar sind, gelten die brasilianischen Vorschriften ausschließlich im vertraglichen Verhältnis zwischen Zertifizierungsstelle und Signaturschlüssel-Inhaber. Als mögliche Haftungsquellen im Verhältnis zwischen dem Dritten und dem Zertifizierungsdiensteanbieter kommen der Código de Defesa do Consumidor und der Código Civil in Betracht. Diese Gesetze können auch subsidiär in der Beziehung zwischen Zertifizierungsdiensteanbieter und dem Signaturschlüssel-Inhaber geltend gemacht werden.

431 Siehe hierzu bereits in diesem Teil Gliederungspunkt 1.3.5.8.

432 Siehe hierzu oben in diesem Teil Gliederungspunkte 1.3.5.8 und 2.2.9.1.8.

Das deutsche Modell bezüglich der Haftung des Zertifizierungsdiensteanbieters ist bereits konsolidiert und wird sogar in der Literatur begrüßt.[433] Für Brasilien wird vorgeschlagen, die Haftungsvorschriften des Gesetzentwurfes Nr. 7.316/2002 zu übernehmen. Dieser Ansatz enthält einige nennenswerte wichtige Vorschriften. Art. 38 Gesetzentwurf Nr. 7.316/2002 sieht eine Haftungsregelung vor, welche bestimmt, dass alle Teilnehmer der ICP-Brasil – einschließlich der Aufsichtsbehörde – für die von ihnen verursachten Schäden haften. Wichtig hierbei ist, dass nach der Formulierung dieser Vorschrift der Zertifizierungsdiensteanbieter gegenüber jedem Dritten für Schäden haftet. Der Dritte bleibt somit nicht unbeschützt. Art. 39 legt des Weiteren eine subsidiäre Haftung der Zertifizierungsdiensteanbieter fest. Sie haften auch für von ihnen beauftragte Dritte. Nach Art. 41 Gesetzentwurf Nr. 7.316/2002 müssen Vertragsklauseln zwischen Zertifizierungsdiensteanbietern und Signaturschlüssel-Inhabern für nichtig erklärt werden, wenn diese Klausel die Haftung der Zertifizierungsstellen vermindern oder ausschließen. Das gleiche gilt für die Bestimmungen der „Declaração de Práticas de Certificação“ und „Políticas de Certficado“.

3.11 Deckungsvorsorge

Bezüglich der notwendigen Deckungsvorsorge für Zertifizierungsdiensteanbieter, um den gesetzlichen Verpflichtungen zum Ersatz von Schäden nachzukommen, unterscheiden sich die beiden Signaturregelungen geringfügig.[434] § 12 SigG bestimmt, dass Zertifizierungsdiensteanbieter über eine geeignete Deckungsvorsorge verfügen müssen. Satz 2 dieser Vorschrift legt weitergehend eine Mindestsumme von jeweils 250.000 Euro fest, für einen durch ein haftungsauslösendes Ereignis verursachten Schaden. Die gesetzliche Mindestdeckungssumme basiert auf einem Ausgleich zwischen einer Prognose des hinreichenden Gesamtschutzes für alle Geschädigten und den Möglichkeiten des Versicherungsmarktes. Diese Norm wird von § 9 Abs. 2 Nr. 2 SigV ergänzt, nach welcher die Summe 2,5 Millionen Euro für den einzelnen Versicherungsfall betragen muss. Anders wird in Brasilien normiert, hier wird keine konkrete Mindestsumme festgelegt. Gemäß Art. 2,1,1,t, Resolução Nr. 41 müssen Zertifizierungsdiensteanbieter eine geeignete und kompatible Versicherung haben, welche Risiken der Tätigkeit des Zertifizierungsdiensteanbieters abdeckt. Was unter „geeigneter“ Versicherungssumme zu verstehen ist, entscheidet die Aufsichtsbehörde fallbezogen im Laufe des Akkreditierungsverfahrens. Dabei kann sich das Instituto Nacional de Tecnologia da Informação an Maßstäben orientieren, wie z.B. den verschiedenen Zertifikatstypen, die von Zertifizierungsdiensteanbietern angeboten werden, oder die Anzahl von Zertifikaten, welche ausgestellt werden. Der Vorteil der deutschen Lösung liegt in der Klarheit und Vorhersehbarkeit durch Fest-

433 *Thomale* 2003, 251.

434 Siehe hierzu bereits im diesen Teil Gliederungspunkte 1.3.5.2 und 2.2.9.1.8.4.

setzung einer Mindestsumme als Deckungsvorsorge. Dies schafft Rechtssicherheit und ermöglicht, dass Zertifizierungsdiensteanbieter und Versicherungsunternehmen oder Banken keine großen Schwierigkeiten bei der Vertragsgestaltung haben. Auf der anderen Seite ermöglicht das Nicht-Festlegen einer Mindestsumme, wie im brasilianischen Signaturrecht praktiziert, dass im Einzelfall eine zumutbare Summe vom Zertifizierungsdiensteanbieter verlangt wird, welche seinen Tätigkeiten sowie eingegangenen Risiken entspricht. Angesichts dieser Ausführungen wird kein Rezeptionsvorschlag unterbreitet, eine Mindestdeckungssumme in das brasilianische Signaturrecht einzuführen.

Ein weiterer Unterschied liegt in den Ausgestaltungsmöglichkeiten für die Deckungsvorsorge. Während das deutsche Signaturrecht die flexible Formulierung „Deckungsvorsorge“ verwendet, sieht die brasilianische Regelung eine Versicherung als einzige Möglichkeit vor. Die deutsche Deckungsvorsorge kann laut § 9 Abs. 1 Nr. 1 und 2 SigV entweder durch eine Haftpflichtversicherung bei einem Versicherungsunternehmen oder durch eine Freistellungs- oder Gewährleistungsverpflichtung eines Kreditinstituts (insbesondere durch eine Bankbürgschaft) übernommen werden, wenn diese eine vergleichbare Sicherheit einer Haftpflichtversicherung gewährleistet.[435] Eine Änderung des brasilianischen Signaturrechts, um die Ausgestaltungsmöglichkeiten der Schadenersatzdeckung nach dem deutschen Modell flexibler zu machen ist nicht notwendig. Das Angebot an Haftpflichtversicherungen der brasilianischen Versicherungsunternehmen reicht für Zertifizierungsdiensteanbieter aus. In einer Anfangsphase herrschte Ratlosigkeit und Unsicherheit angesichts des fehlenden Bewusstseins für die Benutzung und die Risiken elektronischer Signaturen. Diese Phase ist noch nicht ganz beendet. Allmählich jedoch entwickelt sich ein gewisses Verständnis für die Eigenschaften und Rolle einer Public Key Infrastruktur. Dies haben ebenfalls die betreffenden Versicherungsunternehmen registriert und bieten deswegen den Zertifizierungsdiensteanbietern ihre Dienstleistungen ohne große Probleme an. Darüber hinaus können brasilianische Versicherungsunternehmen eine Versicherungsvariante anbieten, welche als so genannte „seguro-garantia“[436] über einen umfassenderen Versicherungsschutz gegenüber einer normalen Versicherung verfügt. Versichert werden durch die „seguro-garantia“ sämtliche Vertragspflichten eines Unternehmens.

3.12 Datenschutz

Aus der Darstellung des Signaturrechts von beiden Ländern ist auch zu entnehmen, dass Brasilien anders als Deutschland über keine spezielle Vorschrift zum Daten-

435 Der Abschluss einer Haftpflichtversicherung ist nur eine beispielhafte Möglichkeit der Deckungsvorsorge gemäß den Vorgaben des Anhangs II, Buchst. h) RLeS.

436 Diese Versicherungsvariante wird durch den Beschluss Circular Nr. 232 vom 03.6.2003 der brasilianischen Aufsichtsbehörde für Versicherungen - Susepe - normiert.

schutz verfügt. Der Entwicklungsstand und die Bedeutung des Datenschutzes in Deutschland sind erheblich höher als in Brasilien. In Deutschland sind sowohl in Landes- als auch auf der Bundesebene zahlreiche Datenschutzgesetze verabschiedet worden. Überdies erkennt das höchste Rechtssprechungsorgan Deutschlands – das Bundesverfassungsgericht – das Recht auf informationelle Selbstbestimmung des Einzelnen an, welches als Datenschutz-Grundrecht gilt. Zudem hat das Bundesverfassungsgericht am 27.2.2008 sogar ein weiteres Grundrecht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" im Rahmen der umstrittenen Frage der Zulässigkeit von Online-Durchsuchungen bestimmt.[437] Brasilien dagegen hat nur wenige Gesetze, die das Thema auch nur ansatzweise behandeln.[438]

Zum Thema Datenschutz regelt der Gesetzentwurf Nr. 7.316/2002 den Sachverhalt jedoch ausreichend. Als allgemeine Regel bestimmt Art. 37 Gesetzentwurf Nr. 7.316/2002, dass der Zertifizierungsdiensteanbieter jede, nicht im Zertifikat enthaltene, erhobene Information und Daten des Signaturschlüssel-Inhabers geheim zu halten hat. Basierend auf dem Vorbild des Art. 8 Abs. 2 der europäischen Signaturrichtlinie[439] bestimmt Art. 37 § 1 des Entwurfs, dass personenbezogene Daten nur unmittelbar bei Betroffenen erhoben werden dürfen, wenn diese ausschließlich für Zwecke der Tätigkeiten des Zertifizierungsdiensteanbieters (Zertifizierung) verwendet werden. Die Vorschrift bestimmt zudem, dass Daten für andere Zwecke als die der Zertifizierung nur verwendet werden dürfen, wenn der Betroffene einwilligt. Die Einwilligung muss ausdrücklich in einer hervorgehobenen Klausel abgegeben werden.

Nicht vorgesehen im Gesetzentwurf Nr. 7.316/2002 ist die Möglichkeit des Selbstdatenschutzes durch ein Pseudonym. Selbstdatenschutz ergänzt den Systemdatenschutz des Staates, da dieser nicht in der Lage ist, den gebotenen Datenschutz in vollem Umfang zu gewährleisten.[440]Die Verwendung von Pseudonymen bietet den Vorteil, dass beim rechtsgetreuen Verhalten des Handelnden, dieser keine Datenspuren bei seinen Transaktionen im Netz hinterlassen muss. Im Ausnahmefall – bei der Verletzung von Vertragspflichten oder allgemein zur Rückabwicklung von Verträgen – muss der Personenbezug des unter Pseudonym Signaturschlüssel-Inhabers hergestellt werden.[441] Dass die Verantwortlichkeit des Teilnehmers gewährleistet wird, ist eine Voraussetzung damit sich Pseudonyme durchsetzen. Ein mit unverhältnismäßigem Aufwand verbundenes Aufdeckungsverfahren kann praktisch zur Anonymität führen und gleichzeitig die Ansprüche eines Vertragspartners des Sig-

437 *Hornung*, CR 2008, 299.

438 Beispiel hierfür ist Art. 43 des Código de Defesa do Consumidor, welcher dem Verbraucher den Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten gewährleistet und auf die Herkunft dieser Daten hinweist.

439 Die Signaturrichtlinie basiert wiederum auf § 12 SigG 1997.

440 *Roßnagel*/*Scholz*, MMR 2000, 722.

441 *Scholz* 2003, 213.

naturschlüssel-Inhabers vereiteln. Es ist an dieser Stelle anzumerken, dass die Anonymität im Art. 5 IV der brasilianischen Verfassung grundsätzlich ausgeschlossen wird. Das Aufdeckungsverfahren muss somit in der Form gestaltet sein, dass der Vertragspartner die Information über die Identität des Signaturschlüssel-Inhabers schnell und zuverlässig erhält. Dabei muss er sich identifizieren und konkrete Angaben über eine mögliche, nicht erfüllte Vertragspflicht seitens des Signaturschlüssel-Inhabers abgeben. Um die für das Aufdeckungsverfahren erforderliche Schnelligkeit zu erreichen, wäre der Einsatz von Zertifizierungsdiensteanbietern denkbar.[442] Sie verfügen über die Identifikationsangaben der Signaturschlüssel-Inhaber und könnten für diesen Zweck beispielsweise dieselbe Rufnummer für Aufdeckungsanträge zur Verfügung stellen, unter der die Sperrung eines Zertifikats beantragt wird. Die Aufdeckung generell von einer gerichtlichen Anordnung abhängig zu machen, wäre eine ungeeignete Lösung, besonders für das brasilianische Recht, wo Datenschutz noch nicht so eine erhebliche Rolle wie in Deutschland spielt. Dies würde eine unnötige, mit hohen Kosten- und Zeitaufwand verbundene Verkomplizierung verursachen. Unberührt soll hingegen die Möglichkeit der Übermittlung der Identifikationsdaten auf Ersuchen einer zuständigen Stelle gemäß § 14 Abs. 2 SigG bleiben. Es handelt sich hierbei um Daten für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung, sowie für die Erfüllung der gesetzlichen Aufgaben der in der Vorschrift genannten Stellen.[443] Auch dass im Rahmen gerichtlicher Verfahren die Gerichte eine Aufdeckung anordnen können, sollte der Gesetzgeber beibehalten.

Bei der Gestaltung des Aufdeckungsverfahrens könnte man sogar eine maximale Zeitdauer, von z. B. achtundvierzig Stunden einführen, innerhalb welcher die Identifikation oder ihre Ablehnung dem Interessenten gegenüber mitgeteilt werden muss. Im Rahmen des Aufdeckungsverfahrens wäre auch denkbar, eine Frist zu bestimmen, binnen derer der Signaturschlüssel-Inhaber die Gelegenheit bekommt, sich über den Aufdeckungsanspruch zu äußern.[444] Wird bestätigt, dass er mit seinem Vertragspartner in Widerspruch steht, sollte diese Tatsache bereits Anlass zur Aufdeckung geben. Zudem könnte die Unterrichtungspflicht des Zertifizierungsdiensteanbieters gegenüber dem Antragsteller eines Zertifikats auf ein Pseudonym erweitert werden. Der Antragsteller könnte hierbei von der Möglichkeit eines Aufdeckungsverfahrens ausführlich informiert werden, damit er zum einen rücksichtsloses Verhalten im elektronischen Geschäftsverkehr vermeidet und zum anderem nicht überrascht ist, dass sein Pseudonym aufgedeckt wurde.

442 Hierzu *Roßnagel*, NJW 2001, 1821.

443 Siehe oben in diesem Teil Gliederungspunkt 1.3.5.10.2.

444 *Roßnagel*, RMD, § 14 SigG Rn. 71. Zur Anhörung des Signaturschlüssel-Inhabers siehe auch der Vorschlag zur Änderung des § 14 SigG von *Roßnagel*/*Pfitzmann*/*Garstka*: „… Vor der Übermittlung unterrichtet der Zertifizierungsdiensteanbieter den Signaturschlüssel-Inhaber über den Antrag und Identität des Antragstellers und gibt ihm die Gelegenheit, innerhalb einer angemessenen Frist Stellung zu nehmen.“, *Roßnagel*/*Pfitzmann*/*Garstka* 2001, 152.

Für das brasilianische Signaturrecht wird angesichts dieser Ausführungen empfohlen, am bestehenden Ansatz der datenschutzrechtlichen Bestimmungen des Gesetzentwurfes Nr. 7.316/2002 festzuhalten. Diese können aber erweitert werden, indem die Möglichkeit des Selbstdatenschutzes durch die Ausstellung eines Zertifikats auf ein Pseudonym vorgesehen wird. Damit jedoch die Nutzung von Pseudonymen keine Rechtsunsicherheit oder Misstrauen verursacht, muss ein effektives und unbürokratisches Aufdeckungsverfahren implementiert werden. Wie ausgeführt, sind Zertifizierungsdiensteanbieter für die Durchführung der Aufdeckung geeignet. Neben Behörden und Gerichten sollen Private die Möglichkeit haben, ein Aufdeckungsverfahren anzustoßen.[445] Diese Möglichkeit wird auch für das deutsche Signaturrecht empfohlen, wie schon mehrmals in der deutschen Literatur gefordert.[446]

Wie die Ausführungen des Vergleichs gezeigt haben, ist eine Gegenüberstellung vor dem Hintergrund nutzbringender Verbesserungen im Bereich der technisch-organisatorischen Vorschriften für beide Länder sinnvoll. Gleiches gilt für das Beweisrecht, wie im Folgenden dargestellt werden wird.

445 In diesem Zusammenhang wäre der Vorschlag von provet zu erwähnen, Vorschläge zur Regelung von Datenschutz und Rechtssicherheit in Online-Multimedia-Anwendungen (2. Teil, § 9 Abs. 6 und Abs. 7), Gutachten für das BMBF. Demgemäß kann die glaubhafte Darlegung einer Partei, „dass sie die Aufdeckung zur Verfolgung eines Rechtsanspruchs benötigt und der Antrag nicht offensichtlich rechtsmissbräuchlich ist, insbesondere nicht nur dem Zweck dient, ein Pseudonym aufzudecken“, zur Erteilung der Identifikationsdaten des Signaturschlüssel-Inhabers führen. So ist die Aufdeckung für Private offen.

446 Zur Forderung nach einem Aufdeckungsverfahren für Private *Roßnagel*, DuD 1997, 79; *Rieß*, DuD 2000, 533; *Fischer-Dieskau* 2006, 121.

3. Teil: Vergleich der Beweisregelungen

1. Das deutsche Beweisrecht und das elektronische Dokument

Im ersten Teil dieser Arbeit sind die technisch-organisatorischen Eigenschaften der Sicherungsinfrastruktur für elektronische Signaturen dargestellt und verglichen worden. Um den weiteren Vergleich für das Beweisrecht und die Beweisführung zu ermöglichen, wird auch in der zweiten Hälfte der Arbeit der Systematik der bisherigen Gliederung gefolgt werden. Hier wird zuerst wieder der gegenwärtige Stand der deutschen Rechtsdogmatik näher betrachtet. Dafür scheint es sinnvoll, mit der Definition des Beweises aus deutscher Sicht zu beginnen. Danach wird das brasilianische Beweisrecht beschrieben und anschließend folgt ein Vergleich, in dem der Schwerpunkt auf der Empfehlung einer neue Beweisvorschrift für das brasilianische Recht liegt.

1.1 Beweis - Allgemeines

Der Beweis dient der Überzeugungsbildung des Richters. Er benutzt diesen, um den Untersatz des Urteilssyllogismus zu erzeugen, denn den Obersatz bildet er anhand seiner Kenntnisse von der anwendbaren Rechtsordnung. Den Parteien obliegt im Zivilprozess, gemäß dem Verhandlungsgrundsatz, die Beweisführung für die umstrittenen Tatsachen, die den zu beweisenden Tatbestand erfüllen und somit über Erfolg oder Misserfolg des Prozesses entscheiden können. Der Verhandlungsgrundsatz (auch Beibringungsgrundsatz) zeichnet sich dadurch aus, dass die Lieferung der Tatsachen im Laufe eines Prozesses den Parteien obliegt. Die Parteien beschaffen den Streitstoff und breiten diesen Streitstoff vor dem Gericht aus.[447] Im Strafverfahren dagegen gilt der Untersuchungsgrundsatz (Inquisitionsmaxime)[448], wonach die Ermittlung der materiellen Wahrheit von Amtes wegen untersucht wird. Eine Auflockerung des Verhandlungsgrundsatzes findet durch § 139 ZPO statt, also durch die richterliche Frage- und Aufklärungspflicht.[449] In manchen Bereichen des Zivilprozesses gilt der Untersuchungsgrundsatz, wie zum Beispiel in den Ehe- und Kindschaftsverfahren sowie auch im Insolvenzverfahren.

447 *Baumann* 1989, 502.

448 *Reichhold*/*Putzo*, in: Thomas/Putzo, Einl. Rn. 7.

449 *Baumann* 1989, 502.

In der Regel ist ein Beweisverfahren erforderlich, denn der Tatsachenvortrag der Parteien stimmt in den meisten Fällen nicht überein[450], das heißt, sehr selten gesteht eine Partei die vom Gegner vorgetragenen Tatsachen zu[451] und häufig werden diese Tatsachen bestritten.[452]

Bevor die Beweisfragen hinsichtlich der Verwendung elektronischer Dokumente untersucht werden, sind die grundlegenden Begriffe des deutschen Zivilprozessrechts zu erklären, die im Zusammenhang mit der vorliegenden Arbeit stehen.

1. 2 Beweisarten

Man unterscheidet nach dem Ziel der Beweistätigkeit zwischen dem Vollbeweis und der Glaubhaftmachung. Nach dem Zweck des Beweises kann wiederum zwischen Haupt- und Gegenbeweis sowie Beweis des Gegenteils unterschieden werden.[453]

1.2.1 Vollbeweis

Der Begriff des vollen Beweises bringt zum Ausdruck, dass das Gericht von der Wahrheit oder Unwahrheit einer Behauptung vollständig zu überzeugen ist. In der ZPO ist der Ausdruck in den §§ 415, 416, 417 und 418 zu finden. Voll beweisen bedeutet, die Aufforderung an die beweisbelastete Partei die Vollständigkeit des zu beweisenden Tatbestandes darzulegen, oder anders betrachtet, den schon erbrachten Beweis vollständig zu entkräften, damit jede Möglichkeit des Zutreffens der vom Gegner nachgewiesenen Tatsachen ausgeschlossen wird. Der Begriff des vollen Beweises bezieht sich auch auf die richterliche Überzeugungsbildung, welche in den Fällen, in denen der Vollbeweis verlangt wird, völlig erreicht werden muss. Einerseits ist die Darlegung der bloßen Wahrscheinlichkeit einer Tatsache nicht ausreichend, andererseits ist jedoch die absolute Gewissheit des Gerichts, die jede andere Möglichkeit ausschließt, nicht erforderlich.[454] Vielmehr kommt es für die Annahme der Wahrheit auf die „freie Überzeugung“ des Richters an. Es genügt lediglich ein

450 Nach einer empirischen Untersuchung von Nack ist in ca. 70% aller Fälle ein Beweisverfahren notwendig. *Nack*, MDR 1986, 366.

451 § 288 ZPO sieht das gerichtliche Geständnis vor. Nach Abs. 1 dieser Vorschrift bedürfen die von einer Partei behaupteten Tatsachen insoweit keines Beweises, als sie im Laufe des Rechtstreits von dem Gegner bei einer mündlichen Verhandlung oder zum Protokoll eines beauftragten oder ersuchten Richters zugestanden sind.

452 Nach § 138 Abs. 3 ZPO sind Tatsachen, die nicht ausdrücklich bestritten werden, als zugestanden anzusehen, wenn nicht die Absicht, sie bestreiten zu wollen, aus den übrigen Erklärungen der Partei hervorgeht.

453 *Rosenberg*/*Schwab*/*Gottwald* 2004, 743.

454 *Oberheim*, JuS 1996, 636.

für das praktische Leben brauchbarer Grad von Gewissheit, der die Zweifel beseitigt, ohne sie völlig auszuschließen.[455]

1.2.2 Glaubhaftmachung

Bei der Glaubhaftmachung muss die Partei einen geringeren Überzeugungsgrad als bei einem Vollbeweis erreichen. Der Ausdruck „die gute Möglichkeit", dass die behaupteten Tatsachen der Wahrheit entsprechen, wird oft mit dieser Beweisart verbunden.[456] Eine Erklärung lediglich glaubhaft zu machen, ist nur dann ausreichend, wenn das Gesetz es zulässt.[457] Die ZPO trifft in § 294 nur zwei Regelungen zur Glaubhaftmachung: Wer etwas glaubhaft zu machen hat, darf alle Beweismittel verwenden, sogar die eidesstattliche Versicherung, aber die Beweisaufnahme muss sofort erfolgen können.

1.2.3 Hauptbeweis

Der Hauptbeweis ist der Beweis, der von der beweisbelasteten Partei erbracht werden muss.[458] Durch diesen Beweis will die Partei die Tatbestandsmerkmale deutlich machen, die für das Eingreifen der entsprechenden Anspruchsnorm erforderlich sind. Der Beweis ist erst dann erbracht, wenn das Gericht von der Wahrheit der vorgebrachten Tatsachen voll überzeugt ist.

1.2.4 Gegenbeweis

Einen Gegenbeweis zu führen, ist Aufgabe der nicht beweisbelasteten Partei. Ihr Ziel ist, die Unwahrheit des Hauptbeweises darzulegen. Erfolgreich geführt wird der Gegenbeweis, wenn die Überzeugung des Richters von den bereits von der beweisbelasteten Partei vorgebrachten und unter Beweis gestellten Tatsachenbehauptungen ausreichend erschüttert wird, um ihr Anliegen abzulehnen.[459] Ziel des Gegenbeweises ist also nicht die völlige Neutralisation des Hauptbeweises, sondern seine Entkräftung. Für diesen Zweck werden die Anforderungen der Rechtsprechung nicht so

455 BGH, NJW-RR 1994, 567.

456 S. z.B. *Jauernig*, 2002, 198; *Rosenberg*/*Schwab*/*Gottwald* 2004, 743.

457 Wie bei diesen Tatbestände der ZPO: §§ 44 Abs. II, 104 Abs. II, 236 Abs. II 1, 251a Abs. II 4, 296 Abs. IV, 511 Abs. III, 530, 531 Abs. II 2, 532 S. 3, 920 Abs. II.

458 *Laumen*, NJW 2002, 3740.

459 *Baumgärtel* 1996, 13.

hoch gesetzt.[460] Die bloße Erschütterung der vom Gegner geführten Beweise reicht zum Erfolg des Gegenbeweises aus, wie etwa das Darlegen eines anderweitigen Geschehensablaufs. Ein erfolgreicher Gegenbeweis verursacht das Fällen eines *non liquet*-Urteils zu Lasten der hauptbeweisbelasteten Partei.[461]

1.2.5 Beweis des Gegenteils

§ 292 Satz 1 ZPO fordert einen Beweis des Gegenteils, wenn ein Gesetz für das Vorhandensein einer Tatsache eine Vermutung aufstellt und das Gesetz nichts Anderes vorschreibt. Die Lehre spricht von einer Gleichstellung mit dem Hauptbeweis in dem Sinn, dass beide die volle Überzeugung des Richters erforderlich machen.[462] Zur Widerlegung der gesetzlichen Vermutung muss die Unwahrheit der vermuteten Tatsache voll bewiesen werden. Hier reicht nicht die bloße Erschütterung der schon von der beweisbelasteten Partei vorgelegten Tatsachen aus, sondern es ist die vollständige Entkräftung der bereits gebildeten richterlichen Überzeugung erforderlich.[463] Gefordert wird von der Partei eine völlige Neutralisierung des Hauptbeweises in einem höheren Grad als bei der Erbringung des Gegenbeweises.

1.2.6 Anscheinsbeweis

Das Rechtsinstitut des Anscheinsbeweises wurde in Deutschland zunächst mit dem Ziel von der Rechtsprechung entwickelt, befriedigende Prozessergebnisse zu ermöglichen.[464] Der Anscheinsbeweis wird in der Phase der Beweiswürdigung angewandt, als Hilfsmittel zur richterlichen Überzeugungsbildung.[465] In dem ersten Fall aus dem Jahre 1888, in welchem der Anscheinsbeweis zu Anwendung kam, ging es um die Frage, wer für eine Schiffskollision haftet. Das Reichsgericht entschied damals, dass *prima facie* der Kapitän zu belasten war, der eine Verhaltensvorschrift verletzt hatte.[466] Der Anscheinsbeweis wurde damals – und wird oft immer noch – prima-facie-Beweis genannt.

460 NJW 1983, 1740: „Der Gegenbeweis ist bereits geglückt, wenn die Überzeugung des Gerichts von der zu beweisenden Tatsache erschüttert wird; dass sie als unwahr erwiesen wird oder sich auch nur eine zwingende Schlussfolgerung gegen sie ergibt, ist nicht nötig".

461 *Laumen*, NJW 2002, 3741.

462 *Reichhold*, in: Thomas/Putzo, § 292 Rn. 9.

463 NJW 2002, 3028.

464 *Lepa*, NZV 1992, 129.

465 S. hierzu *Schemman*, ZZP 118 (2005), *Rosenberg*/*Schwab*/*Gottwald* 2004, 770.

466 *Lepa*, NZV 1992, 129.

Die Besonderheit des Anscheinsbeweises ist die Möglichkeit, auf die detaillierte Feststellung des Ereignisses zu verzichten.[467] Sein typischer Anwendungsbereich ist die Feststellung von Kausalität und Verschulden.[468] Der Richter zieht einen Erfahrungssatz heran und nutzt diesen als Brücke zwischen den Tatsachen und den Konsequenzen des Ereignisses bei der Suche nach der Ursache des Schadens. Ein Beispiel ist die erfolgte Bluttransfusion vor der Diagnose einer Aids-Infektion.[469] Die allgemeine Lebenserfahrung führt hier zum Schluss, dass die Infektion auf die Bluttransfusion zurückzuführen ist. Der Anscheinsbeweis wird auch berücksichtigt bei dem Nachweis von Verschulden und Mitverschulden, insbesondere bei Verkehrsunfällen. Ist ein Auffahrunfall geschehen, trifft man die Feststellung, dass den Auffahrenden das Verschulden trifft. Die Rechtsprechung lässt aber nicht immer, wenn ein „typischer Geschehensablauf" vorliegt, den Anscheinsbeweis zu.[470] Der Bundesgerichtshof hat sich schon geweigert einen prima-facie-Beweis in Bezug auf das Eintreffen eines Einschreibebriefs beim Empfänger anzuerkennen, obschon nach Auskunft der Post auf eine Million solcher Sendungen in einem Jahr nur 266 (0,026%) in einem anderen sogar nur 50 (0,005%) gemeldete Verluste entfielen.[471] Grund für die Ablehnung war, dass die Anerkennung des Anscheinsbeweises Rechtsunsicherheit verursachen könnte, indem der „Zugang" des § 130 Abs. 1 BGB (Wirksamwerden der Willenserklärung gegenüber Abwesenden) praktisch durch den Nachweis der Absendung ersetzt wäre.[472]

Ferner ist zu beachten, dass der Anscheinsbeweis als Fall des Indizienbeweises betrachtet wird und daher die Führung eines Gegenbeweises ermöglicht wird.[473] Grundsätzlich bedeutet Anscheinsbeweis, dass Tatsachen bewiesen werden, die den ersten Anschein für das Vorliegen der behaupteten Tatsache begründen. Die Möglichkeit eines anderen Geschehensablaufs ist aber nicht zu leugnen, denn der Anscheinsbeweis bezieht sich nicht auf konkrete Beweismittel, sondern auf den typischen Geschehensablauf.[474] Fraglich ist, inwieweit der Beweisgegner die Tatsachen nachweisen muss, um den Anscheinsbeweis zu erschüttern. Die Erschütterung des Anscheinsbeweises fordert den vollen Beweis der Tatsachen, die einen anderen Geschehensablauf möglich machen.[475] Die einfache Behauptung, dass die Tatsachen geschehen sind, reicht nicht aus. Aber der zu führende Gegenbeweis muss das Gericht nicht von der Unwahrheit des typischen Geschehensablaufs überzeugen, weil

467 *Schemmann*, ZZP 118 (2005), 163.

468 *Rosenberg*/*Schwab*/*Gottwald* 2004, 770.

469 Beispiel von *Rosenberg*/*Schwab*/*Gottwald* 2004, 771. Hierzu auch BGHZ 114, 284, 290f.

470 *Leopold* 1985, 15.

471 BGHZ 24, 308; *Leopold* 1985, 15.

472 *Leopold* 1985, 16.

473 *Schemmann*, ZZP 118 (2005), 163.

474 *Leopold* 1985, 12.

475 *Baumgärtel* 1996, 178; *Roßnagel*, NJW 1998, 3317.

das zu einer Umkehr der objektiven Beweislast führen würde.[476] Erforderlich ist nicht der Beweis des Gegenteils, sondern der bloße Gegenbeweis, der den typischen Geschehensablauf erschüttert.

1.3 Beweislast

1.3.1 Grundregel der Beweislastverteilung

Es gibt Situationen, bei denen sich auch nach der gesamten Beweisaufnahme bei dem Gericht keine Überzeugung über den vorgebrachten Sachverhalt bildet. Die bestrittenen Tatsachen, die den Tatbestand erfüllen sollten, bleiben unklar. Das Gericht befindet sich in der Lage des *non liquet* (es besteht keine Klarheit) und muss trotzdem eine Entscheidung fällen, denn zu beachten sind das Rechtsverweigerungsverbot und der jedem Bürger zustehende Justizgewährungsanspruch. Letzterer wird aus dem Art. 19 Abs. 4 GG abgeleitet und hat die Gewährung eines Anspruchs auf den effektiven Rechtsschutz zur Folge.[477] Beweislastregeln existieren, damit die Gerichte ihre Entscheidungsaufgabe erfüllen können.

Die Frage der Beweislast hat auch eine erhebliche außerprozessuale Auswirkung[478], denn ihre Regeln beeinflussen das Verhalten der Parteien. Wenigstens mittelbar wird auch die eventuelle Absicht eines Klägers, ein hohes prozessuales Risiko einzugehen, um das Gericht zu „testen", vermieden.

Im deutschen Zivilprozessrecht gilt der ungeschriebene Grundsatz, nach dem jede Partei die sie begünstigenden Tatsachen beweisen muss.[479] Dementsprechend hat der Kläger die rechtsbegründenden und -erhaltenden Tatsachen seines Rechts zu beweisen,[480] während der Beklagte die rechtshindernden, rechtsvernichtenden und rechtshemmenden Elemente des von dem Gegner zu beweisenden Tatbestands vorbringen muss. Diese Regel drückt den bereits erwähnten Verhandlungsgrundsatz aus.[481] Gäbe es im Zivilprozessrecht den Vorrang der Inquisitionsmaxime (Untersuchungsgrundsatz), genauso wie im Strafverfahren, dann wäre das Thema Beweislast nicht so relevant.

Zur Klarheit der Materie unterscheidet die Dogmatik des Beweisrechts zwischen verschiedenen Unterbegriffen: Behauptungslast, objektive Beweislast und die subjektive Beweislast. Diese sind im Folgenden zu erläutern.

476 *Baumgärtel* 1996, 178.

477 *Stein*/*Frank* 2000, 423.

478 *Baumgärtel* 1996, 6.

479 *Laumen*, NJW 2002, 3741.

480 Hierzu BGH NJW 1999, 353.

481 Siehe bereits in diesem Teil Gliederungspunkt 1.1.

1.3.2 Behauptungslast

Die Behauptungs- oder Darlegungslast bezieht sich auf die Obliegenheit der Parteien, die konkreten Tatsachen, welche die entsprechenden sie begünstigenden Normen auf der Tatbestandsseite voraussetzen, vorzubringen.[482] Um Erfolg mit einem Antrag zu haben, müssen danach die Behauptungen von den jeweiligen Beweisen bestätigt werden. Deswegen besteht eine Beziehung zwischen Behauptungslast und Beweislast, denn wer eine Tatsache beweisen will, muss sie zuerst darlegen. Die Beweislast regelt in einem späteren Zeitpunkt des Prozesses die gleiche Frage wie vorher die Darlegungslast. Bei der letzteren geht es darum, zu wessen Nachteil es sich auswirkt, dass eine bestimmte Tatsache zunächst gar nicht vorgetragen wurde und deswegen vom Gericht auch nicht berücksichtig werden kann.[483] Die Relevanz der Behauptungslast wird dann spürbar, wenn entweder Kläger oder Beklagter den Vortrag einer wichtigen Behauptung versäumen und die negativen Konsequenzen hieraus erleiden. Im Versäumnisurteil (§ 331Abs. 2 ZPO) zum Beispiel ist die Klage stets abzuweisen, wenn der Klageantrag nicht schlüssig ist.

1.3.3 Objektive Beweislast (Feststellungslast)

Die objektive Beweislast oder Feststellungslast steht im Zusammenhang mit der Frage, wer durch die Unklarheit von relevanten Tatbestandsmerkmalen belastet wird.[484] Bestimmt werden somit die objektiven Folgen der mangelnden Beweisführung.[485] Grundsätzlich stellen die Regelungen der objektiven Beweislast keine prozessuale Sanktion dar, sondern dienen lediglich der Überwindung der Situation, in der das Gericht mit den erbrachten Beweisen keine Entscheidung treffen kann (*non liquet*). Voraussetzung des *non liquet* ist das Verbleiben der Unklarheit bei Gericht trotz der Erschöpfung aller zulässigen Beweismittel.[486] Hauptsächlich wendet sich dann die Regelung der objektiven Beweislast an das Gericht[487], und obwohl die Regelungen der objektiven Beweislast die oben erwähnte außer- und vorprozessuale Auswirkung auf das Verhalten der Partei ausüben, kommen sie erst am Schluss des Prozesses zur Anwendung.[488] Die Regel der objektiven Beweislast liegt nicht im freien Ermessen des Gerichts, sondern wird einerseits vom Gesetz (wie z. B. in §§ 345, 476, 611a BGB) aufgestellt und andererseits auch von der ungeschriebenen Regel bestimmt, die besagt, dass es jeder Partei obliegt, die ihr günstigen Tatsachen

482 *Rosenberg*/*Schwab*/*Gottwald* 2004, 789.
483 *Oberheim*, JuS 1996, 637.
484 *Laumen*, NJW 2002, 3741.
485 *Rosenberg*/*Schwab*/*Gottwald* 2004, 780.
486 *Baumgärtel* 1996, 7.
487 *Baumgärtel* 1996, 6.
488 *Baumgärtel* 1996, 8.

zu beweisen.[489] Daher ist die abstrakt vorliegende gesetzliche Festsetzung der Regeln der objektiven Beweislast aus Gründen der Rechtssicherheit wichtig.

1.3.4 Subjektive Beweislast (Beweisführungslast)

Die Frage der subjektiven Beweislast oder Beweisführungslast kommt im Prozess vor der objektiven Beweislast zur Anwendung, denn hier wird danach gefragt, welche Partei eine Tatsache beweisen muss, um eine Prozessniederlage zu vermeiden. Anders als die objektive Beweislast ist die subjektive Beweislast nur dort im Verfahren von Bedeutung, wo der Verhandlungsgrundsatz herrscht. Denn nur dort kann es zu einem Prozessverlust wegen des Untätigbleibens der beweisbelasteten Partei kommen.[490] Die objektive Beweislast steht auch mit der subjektiven Beweislast in dem Sinn in einem Verhältnis, als dass sie eine so genannte „Vorwirkung" auf diese hat. Die subjektive Beweislast wird in zwei anderen Kategorien untergliedert: die abstrakte und die konkrete Beweisführungslast.

1.3.5 Die abstrakte und die konkrete Beweisführungslast

Die abstrakte Beweisführungslast bezieht sich auf die Frage, wer aus der Sicht vor oder bei Prozessbeginn Beweis zu führen hat.[491] Die konkrete Beweisführungslast dagegen orientiert sich an der spezifischen Situation einer Partei im Laufe des Prozesses. Genauer erklärt beschäftigt sich die konkrete Beweisführungslast mit der Frage, wer in einem Prozess, in dem das Gericht eine vorläufige Überzeugung gewonnen hat, einen Beweis erbringen muss, um den Prozess zu gewinnen.[492] Dadurch ähneln sich die objektive und die abstrakte Beweislast, denn beide behandeln das prozessuale Risiko eines nicht erbrachten Beweises.

Durch die konkrete Beweisführungslast darf der Richter im Rahmen der Beweiswürdigung die Beweislast zu einer oder zu der anderen Partei verlagern. Die abstrakte Beweisführungslast ist statisch, die konkrete Beweisführungslast aber ist dynamisch. Beide stimmen zum Anfang des Prozesses überein, aber im Laufe des Verfahrens kann die konkrete Beweisführungslast variieren.

Der Begriff der konkreten Beweisführungslast hat eine praktische Bedeutung bei der Erschütterung eines Anscheinsbeweises. Bei einer solchen Gelegenheit muss der Beweisgegner Tatsachen, die einen anderen Geschehensablauf begründen, nachweisen, aber die Pfeiler der objektiven Beweislast und der abstrakten Beweisführungslast bleiben unberührt. Das bedeutet, dass eine Umkehr der Beweislast nicht stattfin-

489 *Laumen*, NJW 2002, 3741.
490 *Baumgärtel* 1996, 12.
491 *Laumen*, NJW 2002, 3742.
492 *Baumgärtel* 1996, 15.

det. Der Gegner eines Anscheinsbeweises hat folglich die konkrete Beweisführungslast, dem typischen Geschehensablauf einen anderen möglichen Geschehensablauf durch Behauptung und Nachweis entgegenzuhalten.

1.4 Beweismittel

Die deutsche Zivilprozessordnung sieht lediglich fünf verschiedene Beweismittel vor, nämlich Augenscheinbeweis, Urkundenbeweis, Zeugenbeweis, Sachverständigenbeweis und Beweis durch Parteivernehmung. Dem Ansatz entspricht der Grundsatz des Strengbeweises, wonach der Beweis weitgehend typisiert und beschränkt ist.[493] Nur mittels der im Gesetz genannten Verfahren (*numerus clausus*) kann der Beweis geführt werden. Von den erwähnten Verfahren werden nur der Augenscheinsowie der Urkundenbeweis in dieser Arbeit untersucht, da nur diese den Gegenstand berühren.

1.4.1 Augenschein

Der Beweis durch Augenschein wird in § 371 ZPO geregelt. Satz 2 des ersten Absatzes bestimmt, dass auch das elektronische Dokument Gegenstand dieses Beweises sein kann. In diesem Fall „wird der Beweis durch Vorlegung oder Übermittlung der Datei angetreten". Der wichtigste Anwendungsbereich des normalen Beweises durch Augenschein sind die Besichtigungen von Orten, beispielsweise bei Unfällen oder Nachbarschaftsstreitigkeiten.[494]

Dieses Beweismittel wird auch als „Wahrnehmungsbeweis" bezeichnet.[495] Gegenstände des Augenscheins können verschiedene Objekte sein, wie eine elektronische Aufzeichnung oder ein elektronisches Dokument.[496] Es ist unmittelbar von der Sinneswahrnehmung des Gerichts abhängig,[497] aber gemäß § 372 ZPO kann das Gericht auch einen oder mehrere Sachverständige hinzuziehen. In diesem Fall dienen die Sachverständigen lediglich als Gehilfen (Augenscheinsgehilfen).[498] Diese Regelung hat sich bisher bewährt und könnte sich auch für die Zukunft, in welcher elektronische Signaturen immer häufiger angewandt werden, als sehr praktisch und effektiv erweisen. Es ist zu erwarten, dass sich die Richter häufiger mit Streitigkeiten über die Authentizität und Integrität von elektronisch signierten Dokumenten beschäftigen werden. In diesem Szenario wächst sicher die Bedeutung der Rolle der

493 *Oberheim*, JuS 1996, 637.
494 *Huber*, in: Musielak, § 371 Rn. 1.
495 *Huber*, in: Musielak, § 371 Rn. 3.
496 *Borges* 2003, 453.
497 Hierzu *Schemmann*, ZZP 118 (2005), 162.
498 *Huber*, in: Musielak, § 371 Rn. 5.

Sachverständigen, wie z. B. bei der Erklärung zur Überprüfung einer Signatur.[499] Zu differenzieren ist aber der Fall, bei dem das Gericht die ganze Prozedur der Einnahme des Augenscheins dem Sachverständigen überlässt. Bei diesem Vorgehen würde es sich nicht um einen Augenscheinbeweis, sondern um einen Sachverständigenbeweis handeln.[500]

1.4.2 Beweis durch Urkunden

1.4.2.1 Begriff der Urkunde

In der deutschen Literatur herrscht Übereinstimmung, was den Begriff einer Urkunde im Zivilprozessrecht betrifft. Im Sinn der ZPO verstehen Literatur und Rechtsprechung unter diesem Begriff die Verkörperung einer Gedankenerklärung durch Schriftzeichen, die allgemein bekannt sind oder dem Gericht verständlich gemacht werden können.[501] Das Material der Urkunde spielt in der Definition keine Rolle. Es kann aus Papier, Stoff, Holz, Stein oder einem anderen Material bestehen.[502] Wichtig ist aber, dass das Material mit Händen greifbar ist. Drei Merkmale einer Urkunde sind zu betonen: Lesbarkeit, Verkehrsfähigkeit und Schriftlichkeit. Die Lesbarkeit fehlt manchen Beweismitteln wie Fotografien[503], Zeichnungen und Tonaufnahmen, die deswegen nur Objekt des Augenscheinsbeweises sein können. Die Verkehrsfähigkeit ist die Qualität des Beweisobjekts, jederzeit ohne Einsatz technischer Hilfsmittel verfügbar zu sein.[504] Die Schriftlichkeit betrifft die Möglichkeit, Verkörperungen von Gedankenäußerungen zu enthalten. Kfz-Kennzeichen, Plomben, Siegelabdrucke, aber auch Tonbandaufnahmen, Schallplatten und Fotografien sind keine Urkunde, weil sie nichtschriftlich sind, und werden deshalb lediglich als Augen-

499 *Roßnagel*, NJW 1998, 3315, weist zu Recht darauf hin, dass es das Problem des Augenscheinbeweises ist, dass nur die Bildschirmdarstellung der digital signierten Daten sowie des Ergebnisses der programmgesteuerten Signaturprüfung zur Kenntnis genommen werden kann. Die eigentlichen Sicherheitsmechanismen der digitalen Signatur können so nicht geprüft werden.

500 *Huber*, in: Musielak, § 371 Rn. 5.

501 *Huber*, in: *Musielak*, § 371 Rn. 4.

502 *Rosenberg*/*Schwab*/*Gottwald* 2004, 814.

503 Zum Beweiswert digitaler Fotos und dessen Möglichkeit der Steigerung siehe *Knopp*, ZRP 2008, 158 f.

504 *Huber*, in: Musielak, § 371 Rn. 5.

scheinsobjekt betrachtet.[505] Ein elektronisches Dokument[506] ist ebenfalls keine Urkunde, weil ihm die Verkörperung fehlt.[507]

1.4.2.2 Öffentliche Urkunde und private Urkunde

Nach der Form unterscheidet die ZPO zwischen öffentlichen und privaten Urkunden. Der Begriff der öffentlichen Urkunde findet sich in § 415 ZPO. Sie wird definiert als dasjenige Dokument, das von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises erzeugt wird. Beispiele für mit öffentlichem Glauben versehene Personen sind Notare, Gerichtsvollzieher und Urkundsbeamte.[508] Gemäß § 415 Abs. 1 ZPO begründen öffentliche Urkunden den vollen Beweis des durch die Behörde oder die Urkundsperson beurkundeten Vorganges wie beispielsweise der Vorgänge vor dem Notar, dem Nachlassgericht, oder dem Standesamt bei der Eheschließung. Dabei ist nach § 415 Abs. 2 ZPO nur der Beweis der Fälschung oder der unrichtigen Beurkundung zulässig. § 437 ZPO sieht auch eine Vermutung der Echtheit für öffentliche Urkunden vor. Diese gesetzliche Vermutung umfasst Form und Inhalt,[509] sofern die Urkunde keine sonstigen äußeren Mängel im Sinn des § 419 ZPO[510] enthält. Nach § 417 ZPO begründen öffentliche Urkunden, die eine amtliche Anordnung, Verfügung oder Entscheidung enthalten, vollen Beweis ihres Inhalts. Darüber hinaus begründen nach § 418 Abs. 1 ZPO öffentliche Urkunden, die einen anderen als den in den §§ 415, 417 bezeichneten Inhalt haben, den vollen Beweis der darin bezeugten Tatsachen. Hierbei handelt es sich um öffentliche Urkunden über Wahrnehmungen oder Handlungen einer Behörde oder Urkundsperson, die weder Erklärungen Dritter (§ 415) noch Willenserklärungen der Behörde selbst (§ 417) bezeugen.[511] Der Beweis der Unrichtigkeit der bezeugten Tatsachen ist nach § 418 Abs. 2 ZPO zulässig, sofern nicht die Landesgesetze diesen Beweis ausschließen oder beschränken.

Privaturkunden sind im Grunde genommen alle Urkunden, die nicht unter die Gruppe der öffentlichen Urkunde fallen. Zur Definition von Privaturkunden gehört nicht unbedingt das Vorhandensein einer Unterschrift. Handelsbücher, Tabellen und Rechnungen können auch als Privaturkunden betrachtet werden, allerdings wird in

505 Der strafrechtliche Urkundsbegriff umfasst auch Beweiszeichen und technische Aufzeichnungen auf Ton-, Bild- und Schriftträgern. Hierzu *Bergfelder* 2006, 120.

506 Für das elektronische Dokument als Beweismittel siehe unten Gliederungspunkt 1.6.

507 Zu der Einstimmigkeit dieser Aussage *Britz* 1996, 25.

508 *Rosenberg*/*Schwab*/*Gottwald* 2004, 815.

509 *Huber*, in: Musielak, § 437 Rn. 3.

510 Äußere Mängel wie Durchstreichungen, Radierungen, Einschaltungen oder sonstige, die die Beweiskraft einer Urkunde ganz oder teilweise aufheben oder mindern.

511 *Geimer*, in: Zöller, § 418 Rn. 1.

dieser Situation die Beweiskraft der Urkunde von der gerichtlichen freien Beweiswürdigung abhängen.[512] Der volle Beweis, dass die in den Privaturkunden enthaltenen Erklärungen von den Ausstellern stammen, hat als Voraussetzung die echte Unterschrift des Erklärenden, entweder durch seine stillschweigende oder ausdrückliche Anerkennung oder mittels einer notariellen Beglaubigung. In einem Verfahren muss sich der Gegner des Beweisführers nach § 439 ZPO über die Echtheit der Privaturkunde erklären. Wenn diese Erklärung nicht abgegeben wird oder wenn der Beweisgegner die Echtheit der Urkunde anerkennt, darf das Gericht davon ausgehen, dass die Urkunde echt ist. Wenn jedoch die Echtheit der Urkunde nicht anerkannt wird, hat die beweisbelastete Partei gemäß § 440 Abs. 1 ZPO die volle Überzeugung des Gerichts darüber herzustellen.[513] Für diesen Zweck kann die beweisbelastete Partei alle normalen Beweismittel oder den Schriftvergleich des § 441 ZPO nutzen.[514] Beweiserleichterungen zugunsten des Beweisführers sind nicht vorgesehen.

1.5 Die Beweiserleichterung

Die Beweiserleichterung ist ein von der deutschen Rechtsprechung entwickelter Begriff.[515] In einer Reihe von Fällen in den 70er und 80er Jahren des letzten Jahrhunderts hat der Bundesgerichtshof die Merkmale dieses Rechtsinstituts festgelegt.[516] Die Rechtsprechung hierzu nahm ihren Anfang bei Entscheidungen im Gebiet der zivilrechtlichen ärztlichen Haftung, in denen der BGH aus nachlässigem Verhalten von Ärzten bei der Führung der ärztlichen Dokumentation Konsequenzen für die Beweislast zog, auch im Umwelthaftungsrecht lassen sich dazu Parallelen finden.[517] In Fällen, in denen normalerweise der Patient die volle Beweislast zum Nachweis eines ärztlichen Fehlers getragen hätte, wurde zu seinen Gunsten eine Beweislastverminderung, die bis zur Umkehr[518] gehen kann, zuerkannt.[519]

Beweiserleichterungen haben nichts mit der Verteilung der Feststellungslast zu tun. Denn wie Laumen zu Recht feststellt: „Erleichtern kann man nur die Beweis-

512 *Huber*, in: Musielak, § 416 Rn. 1., BGH, NJW 1998, 58.

513 *Roßnagel*/*Pfitzmann*, NJW 2003, 1212.

514 *Reichhold*, in: Thomas/Putzo, § 440 Rn. 1.

515 Zur Entstehung des Begriffs *Laumen*, NJW 2002, 3739.

516 BGH, NJW 1972, 1520; BGH, NJW 1978, 2337; BGH, NJW 1986, 2365.

517 Siehe hierzu: *Hager*, NJW 1986, 1961; *Dombert*, in: Landmann/Rohmer, §24 Rn. 42. *Hager*, in: Landmann/Rohmer, § 6 Rn. 17 betrachtet § 6 Abs. 1 UmweltHG als Beweiserleichterung.

518 *Laumen* vertritt die Auffassung, dass die „Beweiserleichterungen bis hin zur Beweislastumkehr nur in Form von Beweiserleichterungen bis zur Umkehr der konkreten Beweisführungslast möglich sind“. Das heißt, die Feststellungslast bleibt unberührt.

519 *Laumen*, NJW 2002, 3740.

führung“, und über die Feststellungslast darf der Richter nicht entscheiden.[520] Eher gehören Beweiserleichterungen zum Bereich der Beweiswürdigung.[521] Der Unterschied ist wichtig, denn die Beweislastnormen kommen erst zur Anwendung, wenn nach der gesamten Auswertung der erbrachten Beweise die Sache noch unklar bleibt, das bedeutet nach der Beweiswürdigung.

1.6 Das private elektronische Dokument als Beweismittel

Im Folgenden wird das private elektronische Dokument untersucht. Es werden sowohl der Begriff als auch die Beweisführung mit elektronisch signierten privaten Dokumenten untersucht. Die folgenden Ausführungen legen überdies Wert auf den Anscheinsbeweis des § 371a Abs. 1 Satz 2 ZPO.

1.6.1 Begriff des elektronischen Dokuments

Weil elektronischen Dokumenten das Wesensmerkmal der Verkörperung fehlt, müssen sie immer mit einem Trägermedium verbunden werden, damit sie lesbar bleiben. Anders als in der Welt der Urkunden, in der Änderungen und Fälschungen des Originals normalerweise leicht bemerkt werden, haben elektronische Dokumente keine Geschichte. Eine charakteristische Eigenschaft von Urkunden ist ihre relative Sicherheit im Vergleich zum elektronischen Dokument. Einschaltungen, Radierungen und Durchstreichungen sind in der Regel leicht erkennbar. Die Fälschung einer Unterschrift lässt sich nicht leicht verstecken und wird normalerweise durch grafologische Gutachten entdeckt. Dagegen hinterlassen Manipulationen an elektronischen Dokumenten keine auf den ersten Blick zu konstatierenden Spuren.[522] Das Beispiel der einfachen E-Mail zeigt, dass praktisch jeder in der Lage ist, ohne großen Aufwand die Authentizität des Absenders zu verändern und die Integrität der Erklärung zu stören. Auch nach dem Empfang oder während der Übermittlung kann die E-Mail gefälscht werden.[523]

Und deshalb profitiert das elektronische Dokument[524] normalerweise nicht von dem hohen Beweiswert des Urkundenbeweises, denn ihm fehlt das Merkmal der Verkörperung. Weil es nur mithilfe von technischen Geräten und Programmen verständlich ist,[525] gelten zugunsten einfacher elektronischer Dokumente die gesetzli-

520 *Laumen*, NJW 2002, 3743.

521 *Laumen*, NJW 2002, 3743.

522 *Roßnagel*, NJW 2001, 1817; *Pordesch* 2002, 35.

523 *Roßnagel*/*Pfitzmann*, NJW 2003, 1210.

524 Über die Einigkeit darüber, dass elektronische Dokumente die Wesensmerkmale der Urkunden nicht erfüllen können, *Fischer-Dieskau* 2006, 84.

525 *Roßnagel*, NJW 1998, 3316.

chen Vermutungen nicht, die mit der eigenhändig unterschriebenen Urkunde assoziiert werden. Dagegen sind sie Gegenstände des Augenscheins. Ihnen werden keine spezifischen Beweisregeln über ihre Echtheit zuerkannt, daher unterliegen sie in diesem Fall der freien Beweiswürdigung des Richters.[526]

1.6.2 Das elektronische Dokument und die freie Beweiswürdigung

Grundsätzlich bedeutet „freie Beweiswürdigung" die Freiheit des Richters, die gesamten mit dem Prozess in Zusammenhang stehenden Beweise auszuwerten, um Tatsachen festzustellen. Diesen Grundsatz enthält § 286 Abs.1 ZPO.[527] Hierdurch wird dem Richter erlaubt, frei „über das Gewicht einer Beweisaufnahme im Verhältnis zur eigenen Lebenserfahrung"[528] zu entscheiden. Aber selbst wenn der Richter Entscheidungsfreiheit bei seiner Beweiswürdigung hat, ist er immer noch an die rationale Argumentation gebunden[529], denn „frei heißt nicht willkürlich".[530] Gemäß § 286 Abs. 2 ZPO kann die Rechtsordnung auch Ausnahmen von diesem Grundsatz schaffen, wenn ein Gesetz eine Beweisregelung oder Vermutung bestimmt, die den Richter bindet.[531] In diesem Sinn limitieren einerseits die Rechtsordnung und andererseits die richterliche Begründungspflicht das Prinzip der freien Beweiswürdigung.[532]

Die Rolle und Bedeutung der freien Beweiswürdigung hat sich im Laufe der Rechtsgeschichte verändert. Britz weist auf die Variationen ihrer Geltung gegenüber den festen Beweisregeln schon im römischen Zivilprozess hin.[533] In der Frühzeit des Legisaktionsprozesses herrschten strenge Förmlichkeiten und dadurch feste Beweisnormen, während im klassischen Formularverfahren die freie Beweiswürdigung an Einfluss gewann. Im deutschen Rechtsgebiet war das kanonische Recht wichtig für die Entwicklung der freien Beweiswürdigung, da es die Möglichkeit einführte, die

526 *Borges* 2003, 415.

527 „§ 286 Freie Beweiswürdigung (1) Das Gericht hat unter Berücksichtigung des gesamten Inhalts der Verhandlungen und des Ergebnisses einer etwaigen Beweisaufnahme nach freier Überzeugung zu entscheiden, ob eine tatsächliche Behauptung für wahr oder für nicht wahr zu erachten sei. In dem Urteil sind die Gründe anzugeben, die für die richterliche Überzeugung leitend gewesen sind". Die brasilianische Zivilprozessordnung enthält einen gleichartigen Rechtssatz im Artikel 131.

528 *Foerste*, in: Musielak, § 286 Rn. 9.

529 Wie der letzte Satz des § 286: „In dem Urteil sind die Gründe anzugeben, die für die richterliche Überzeugung leitend gewesen sind." Hierzu auch BGW, NJW 1991,1894.

530 *Britz* 1996, 94.

531 Wie die Bestimmung der Beweiskraft öffentlicher Urkunden § 415 ZPO.

532 Zu diesen beiden Aspekten als Limitierung der freien Beweiswürdigung, *Portanova* 1995, 246.

533 *Britz* 1996, 91.

Wahrheit mit den Aussagen von Zeugen zu beweisen.[534] Eine Renaissance der Bindung des Richters an strenge Beweisregeln fand mit der Rezeption des römischen Rechts statt. Die freie Beweiswürdigung konsolidierte sich innerhalb des deutschen Rechtssystems durch die Einflüsse der Aufklärung[535] und definitiv mit dem in Kraft treten des § 286 Abs. 1 der ZPO im Jahre 1898.[536]

Die Beweisführung mittels elektronischer Dokumente benötigt deutliche Beweisregeln über den Wert von elektronischen Daten, um ein gewisses Maß an Rechtssicherheit und Vorhersehbarkeit zu schaffen, wie es das Rechtsstaatsprinzip[537] erfordert. Dies ist auch von besonderer Bedeutung für den Geschäftsverkehr, bei dem Willenserklärungen eine wesentliche Rolle spielen. Manche Tatsachen von juristischer Relevanz dürfen nicht allein der relativen Unsicherheit der freien Beweiswürdigung überlassen werden. Obwohl es sicher ist, dass die freie Beweiswürdigung immer eine Rolle im Interesse der Einzelfallgerechtigkeit spielen darf, müssen Fragen wie die, was als Beweis im elektronischen Verkehr akzeptiert werden kann, vom Rechtssystem beantwortet werden. Es ist wenigstens eine gesetzliche Regelung der Voraussetzungen zur Gleichstellung von handschriftlichen Unterschriften zu elektronischen Signaturen und hinsichtlich des Beweiswertes von elektronischen Dokumenten zu erwarten.[538] Die Rechtssicherheit im Beweisrecht ist ein erwünschter Wert. Diesen hat der deutsche Gesetzgeber vornehmlich durch die Verabschiedung des Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13.7.2001 zu fördern gesucht.[539] Durch dieses Gesetz wird zugunsten qualifiziert elektronisch signierter Dokumente eine Beweiserleichterung im § 292a der Zivilprozessordnung vorgesehen. Mit Inkrafttreten des Justizkommunikationsgesetzes vom 22.3.2005 wurde § 292a ZPO aufgehoben, doch sein Inhalt ist mit wenigen Änderungen in § 371a Abs. 1 Satz 2 ZPO übernommen worden. Das Justizkommunikationsgesetz führte überdies die Gleichstellung der prozessualen Wirkung echter elektronischer Dokumente und Urkunden ein.

534 Britz 1996, 92.

535 Hierzu *Heinrich* 1996, 5.

536 *Britz* 1996,93.

537 Hierzu *Roßnagel*, NJW 1998, 3318.

538 Hierzu Artikel 5 der europäischen Richtlinie für elektronische Signaturen (1999), mit dem Ziel, die Mitgliedstaaten zur Gleichstellung der elektronischen Form durch elektronische Signaturen mit handschriftlichen Unterschriften in ihrem Rechtssystem zu verpflichten.

539 So die Begründung des Formanpassungsgesetz, BT-Drs. 14/4987, 44.: „Da mit Blick auf den vergleichbaren Fall des sorglosen Umgangs mit EC-Karten und der hierzu ergangenen divergierenden Rechtsprechung zum Vorliegen der Voraussetzungen des Anscheinsbeweises (vgl. OLG Hamm, WM 1997, 1203) eine uneinheitliche Rechtsprechung zur Beweiskraft einer qualifizierten elektronischen Signatur nicht ausgeschlossen ist, erscheint es zur Gewährleistung der für die Teilnehmer am elektronischen Rechtsverkehr unerlässlichen Rechtssicherheit geboten, eine Beweisregel in die Zivilprozessordnung aufzunehmen“.

1.6.3 Beweiswirkung echter privaten qualifizierten signierten Dokumente

Gemäß § 371a Abs. 1 Satz 1 ZPO finden auf private qualifiziert signierte Dokumente die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Echte private qualifiziert signierte Dokumente begründen dann nach § 416 ZPO vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen vom Aussteller abgegeben worden sind. Somit entspricht die prozessuale Wirkung echter elektronischer Dokumente denen echter Urkunden. Die Gleichstellung durch das Justizkommunikationsgesetz wird begrüßt, denn im Grunde genommen unterscheiden sich elektronische Dokumente und Urkunden lediglich in der Form, in der sie vorliegen.[540] Folgerichtig ist es nicht sachgerecht, eine unterschiedliche Behandlung zur beweisrechtlichen Wirkung zuzulassen, wenn die Echtheit feststeht. Zugunsten echter Urkunden gilt eine Vermutung, die nach § 292 ZPO nur durch den Beweis des Gegenteils widerlegbar ist.

1.6.4 § 371a Abs. 1 Satz 2 ZPO als Anscheinsbeweis und seine Voraussetzungen

Neu für das deutsche Zivilprozessrecht war einerseits die gesetzliche Anerkennung des bis dahin nur von der Rechtsprechung entwickelten und in der Lehre erörterten Rechtsinstituts des Anscheinsbeweises.[541] Andererseits stellte auch der Bezug einer prozessualen Vorschrift auf eine materiell rechtliche Vorschrift, nämlich auf die elektronische Form des § 126a BGB, eine Neuigkeit dar.[542] Ferner war das Schaffen eines Anscheinsbeweises in diesem Bereich nicht unumstritten. Es bestand zwar Einigkeit darüber, dass für die Durchsetzung elektronisch signierter Dokumente als sichere Beweismittel ein der Urkunde vergleichbar hoher Beweiswert nötig war. Umstritten war aber, inwiefern die Beweisvorschrift gestaltet werden sollte, ob in Form eines Urkundenbeweises oder eher in die Richtung eines Anscheinsbeweises.[543]

Wäre das qualifiziert elektronisch signierte Dokument der unterschriebenen Privaturkunde gleichgestellt, würde das bedeuten, dass der Erklärungsempfänger als beweisbelastete Partei schutzlos gegenüber einem unbegründeten Einwand des Beweisgegners sein würde, die Erklärung sei nicht von dem Signaturschlüssel-Inhaber abgegeben worden.[544] So ein rücksichtsloser Einwand ist in der Papierwelt eher selten, denn dem Beweisgegner ist mit an Sicherheit grenzender Wahrscheinlichkeit klar, dass sich die Echtheit der von ihm geleisteten Unterschrift in den häufigsten Fällen erfolglos bestreiten lässt. Der Grund hierfür ist, dass die Echtheit oder Un-

540 *Fischer-Dieskau* 2006, 144.

541 Hierzu Gliederungspunkt 1.2.6.

542 *Schemmann*, ZZP 118 (2005), 165.

543 *Fischer-Dieskau* 2006, 124.

544 BR-Drs. 14/4987, 25.

echtheit einer Urkunde in der Regel unproblematisch durch Schriftvergleichung festgestellt werden kann. Es bringt dann dem Beweisgegner nichts, die Echtheit seiner eigenen Unterschrift zu bestreiten, wenn er weiß, dass die beweisbelastete Partei ihm ohne größeren Aufwand widersprechen kann. Etwas anderes gälte bei elektronisch signierten Dokumenten, sollten sie den Beweisregelungen von Urkunden unterworfen werden. Dann hätte der Beweisführer praktisch keinen Ausweg, sollte der Prozessgegner behaupten er habe das Dokument nicht signiert. Um dieser schwierigen prozessualen Situation zu entgehen, wäre ein unzumutbarer Aufwand notwendig, denn er müsste den vollen Beweis der Echtheit der vom Beweisgegner nicht anerkannten Signatur erbringen, gemäß § 439 Abs. 1 und 2, § 440 Abs. 1 ZPO.

Aus diesem Grunde hat sich der deutsche Gesetzgeber für die Etablierung einer Beweiserleichterung in Form eines Anscheinsbeweises zugunsten des Empfängers eines qualifizierten elektronisch signierten Dokuments entschieden.[545] Die Rechtstellung des Signaturempfängers im Prozess wird wesentlich gestärkt mit dem Ziel der Gewährleistung des Vertrauens und der Rechtssicherheit im elektronischen Geschäftsverkehr.[546]

Der Unterschied zwischen dem klassische Anscheinsbeweis und der Regelung des § 371a Abs. 1 Satz 2 ZPO ist, dass dieser sich nicht auf alltägliche Lebenserfahrung bezieht, sondern auf eine Sicherheitsvermutung des Signaturgesetzes.[547] Die Voraussetzung ist hier die bereits in dieser Arbeit dargestellte „flächendeckende IT-Sicherheitsinfrastruktur, Einrichtung gesetzeskonformer Zertifizierungsdienste, technischer Komponenten und geeigneter Prüf- und Bestätigungsstellen“, über die Deutschland schon verfügt.[548] Weil die qualifizierten elektronischen Signaturen als sicher gelten, wurden sie vom deutschen Gesetzgeber als Ersatz der handschriftlichen Unterschrift anerkannt und die elektronischen Dokumente, die mit einer solchen Signatur versehen werden, bekommen einen besonderen Beweisstatus.
Der Text des § 371a Abs. 1 Satz 2 ZPO lautet: „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 nicht vom Signaturschlüssel-Inhaber abgegeben worden ist“. Aus der Vorschrift können grundsätzlich zwei konstitutive Voraussetzungen des Anscheinsbeweises entnommen werden: Das Vorliegen einer Erklärung in elektronischer Form und die Prüfung der entsprechenden

545 BR-Drs. 14/4987, 24.

546 BR-Drs. 14/4987, 13.

547 Zur Sicherheitsvermutung des § 1 Abs. 1 SigG 1997 vor der Erschaffung des Formanpassungsgesetz, *Roßnagel*, NJW 1998, 3312; *Fischer-Dieskau* 2006, 81, weist darauf hin, dass sich hinter dem von *Roßnagel* erstmalig in dem Aufsatz „Die Sicherheitsvermutung des Signaturgesetzes“, NJW 1998, 3312, verwendeten Begriff der Sicherheitsvermutung schon eine Art vorgezoger Anscheinsbeweis verborgen hat.

548 BR-Drs. 496/00, 18.

Signatur nach dem Signaturgesetz. Die beiden Voraussetzungen sind im Folgenden darzustellen.

1.6.4.1 Erklärung in elektronischer Form

Die elektronische Form ist als alternative Option zu der Schriftform des § 126 BGB in das deutsche Bürgerliche Gesetzbuch (BGB) durch das Formanpassungsgesetz eingeführt worden. Dabei wurde § 126a hinzugefügt, wonach gilt: „Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen". Da die elektronische Form als Ersatz für die eigenhändige Unterschrift im elektronischen Rechtsverkehr dienen soll, wurde sie so konzipiert, dass soweit wie möglich die mit der Schriftform bezweckten Leistungsfunktionen sichergestellt werden.[549]

Die *Abschlussfunktion* der elektronischen Form wird dadurch gewährleistet, dass die Technik der elektronischen Signatur eine logische Verbindung zwischen signiertem Dokument und Signatur ermöglicht. Das wird im Verfahren des Signierens durch die Zuordnung eines mit dem privaten Schlüssel des Signaturschlüssel-Inhabers gebildeten Hashwertes zum Dokument erreicht.

Die *Perpetuierungsfunktion* lässt sich auch durch die elektronische Form reproduzieren, indem sie die dauerhafte Lesbarkeit des Textes und seine dauerhafte Überprüfung ermöglicht. Zwar könnten – abhängig davon, für wie lange das elektronische Dokument aufbewahrt werden soll – zusätzliche Maßnahmen erforderlich sein, wie die Transformation des Dokumentes[550] oder die erneute Signatur[551]. Aber prinzipiell ist die Perpetuierungsfunktion auch im elektronischen Rechtsverkehr reproduzierbar.

Die *Identitätsfunktion* wird durch das einmalige Signaturschlüsselpaar gewährleistet, das durch den Zertifizierungsdiensteanbieter einer bestimmten natürlichen Person zugeordnet wird. Das vom Zertifizierungsdiensteanbieter ausgestellte öffentliche Schlüsselzertifikat bestätigt dann die Zuordnung zum Signaturschlüssel-Inhaber. Weitere technische und organisatorische Maßnahmen wie u.a. sichere Signaturerstellungseinheiten, PIN und ergänzende biometrische Verfahren zur Aktivie-

549 BR-Drs. 14/4987, 15.

550 Eine Transformation kann in diesem Zusammenhang notwendig sein, da angesichts der fortschreitenden technologischen Entwicklung, die Software, die zum Lesen eines bestimmten Dokumentenformats erforderlich ist, schon nach einer relativ kurzen Zeit obsolet wird und vom Markt verschwindet. Hierzu, *Roßnagel*/*Fischer-Dieskau*/*Wilke*, CR 2005, 903. Auch hierzu siehe unten Gliederungspunkt 1.8.1.

551 Zu der erneuten Signatur siehe im zweiten Teil Gliederungspunkt 1.3.5.5.2.

rung des geheimen Schlüssels und die zuverlässige Identifizierung des Teilnehmers sollen auch einen Beitrag zur Erfüllung der Identitätsfunktion leisten.[552]

Die *Echtheitsfunktion*, das heißt, der enge Zusammenhang zwischen Erklärung und Signierung, wird durch die mathematisch-logische Verbindung zwischen dem signierten Dokument und dem dazu angehängten Hashwert gesichert. Hierbei wird die Echtheitsfunktion gegenüber dem Papierdokument sogar verbessert, denn gewährleistet wird nicht nur die Echtheit der Erklärung, sondern auch die Echtheit des Dokuments. Es ist aber auch daran zu erinnern, dass sich die Echtheitsfunktion beim elektronisch signierten Dokument auf die Bestätigung, ob die signierten Daten manipuliert oder nicht manipuliert worden sind, beschränkt.

Die *Beweisfunktion* der elektronischen Form wird durch das angewandte Signaturverfahren gewährleistet und durch alle organisatorischen und technischen Sicherheitsmaßnahmen, die ihm zu Grunde liegen. Handelt es sich um ein qualifiziertes Verfahren, dann kommt der signierten Erklärung der hier thematisierte besondere Beweisstatus zu.

Die *Warnfunktion* wird durch die besonderen Schritte zur Erzeugung einer Signatur erfüllt, die vom Signaturschlüssel-Inhaber unternommen werden. Der erste Schritt ist schon das Erstellen des Dokuments. Dann muss der Signierer seine Chipkarte in das Kartenlesegerät einlegen und seine PIN und gegebenenfalls biometrische Daten eingeben, damit die Signaturfunktion der Karte aktiviert wird. Durch diese gesamte Prozedur wird dem Teilnehmer klar, dass die Anwendung einer qualifiziert elektronischen Signatur eine der eigenhändig unterschriebenen Urkunde vergleichbare Beweiswirkung zukommt. Wichtig ist in diesem Zusammenhang auch die Erfüllung der Unterrichtungspflicht des § 6 SigG seitens des Zertifizierungsdiensteanbieters gegenüber dem Signaturschlüssel-Inhaber, damit der letztere von der rechtlichen Wirkung einer qualifizierten elektronischen Signatur informiert wird.[553] Es ist aber nicht zu verkennen, dass es noch eine Weile dauern wird, bis sich die Warnfunktion der elektronischen Form im Bewusstsein der Bevölkerung konsolidiert. Hierbei ist zu beachten, dass die allgemein verbreitete Bedeutung der Schriftlichkeit auch dank einer Entwicklung von mehreren Jahrhunderten existiert. Wahrscheinlich wird die verbreitete Akzeptanz der elektronischen Form wohl nicht Jahrhunderte brauchen, aber mit Jahrzehnten ist schon zu rechnen.

Der Wortlaut des § 371a Abs. 1 Satz 2 ZPO spricht von der Notwendigkeit einer „Erklärung“ und nicht einer „Willenserklärung“ wie die frühere engere Formulierung des § 292 ZPO. Von der Vorschrift werden somit nicht nur Willens-, sondern auch Wissenserklärungen erfasst, das heißt, alle in elektronischer Form vorliegende Erklärungen inklusive derer, die keinen rechtsgeschäftlichen Erklärungsinhalt aufweisen.[554]

552 BR-Drs. 14/4987, 16.

553 Zu der Unterrichtungspflicht siehe im zweiten Teil Gliederungspunkt 1.3.5.5.

554 BR-Drs. 15/4067, 34.

Bestimmte Erklärungen dürfen aber laut dem Gesetz zur Anpassung der Formvorschriften nicht in elektronischer Form abgegeben werden und fordern weiterhin die Schriftform und damit die urkundliche Verkörperung und die eigenhändige Unterschrift.[555] Beispiele hierfür sind die Leibrente, die Bürgschaft, das Schuldversprechen und die Schuldanerkenntnis sowie der Verbraucherkreditvertrag. Beim Leibrentenversprechen etwa ist die elektronische Form ausgeschlossen aufgrund seiner äußerst weitreichenden Auswirkungen und dem erhöhten Bedürfnis nach Schutz des Erklärenden vor Übereilung.[556] Die Bestimmungen des deutschen Gesetzes in diesem Zusammenhang greifen auf die Richtlinie 2000/31/EG[557] über den elektronischen Geschäftsverkehr zurück, wonach die Schriftform bei bestimmten Geschäften vorbehalten wird, namentlich Verträge über Immobiliarrechte, Verträge, bei denen die Mitwirkung von Gerichten, Behörden oder öffentliche Befugnisse ausübenden Berufen gesetzlich vorgeschrieben ist, Bürgschaftsverträge und Verträge über Sicherheiten, die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit eingegangen werden und Verträge im Bereich des Familien- oder Erbrechts.

1.6.4.2 Hinzufügung des Namens

Gemäß § 126a BGB muss der Aussteller der Erklärung dieser seinen Namen hinzufügen. Bei dem Hinzufügen des Namens handelt es sich somit um ein konstitutives Merkmal der elektronischen Form.[558] In der Literatur wird aber auch die Ansicht vertreten, dass das Tatbestandsmerkmal des Hinzufügens des Namens nicht notwendig ist. Grund hierfür sei, dass die Zielsetzung der Regelung schon mit der Anforderung des § 7 Abs. 1 Nr. 1 SigG erreicht wäre, wonach das Zertifikat den Namen des Signaturschlüssel-Inhabers beinhalten muss.[559] Da das Zertifikat ohnehin dem Signaturempfänger übermittelt wird, ist ihm der Name des Ausstellers bekannt und dadurch ein Hinzufügen des Namens überflüssig.

Die Vorschrift wurde andererseits dahingehend kritisiert, dass sie den Weg zu datenschutzfeindlichen Auslegungen eröffne, da die Anforderung des Hinzufügens des Namens ein pseudonymisiertes Handelsverfahren ausschließen könnte.[560] Gegen diese Interpretation spricht der Einwand, dass § 12 BGB auch ein aufdeckbares Pseudonym als Namen anerkennt.[561] Dadurch könnte der Aussteller der Erklärung

555 *Oertel*, MMR 2001, 421.

556 BR-Drs. 14/4987, 43.

557 Art. 9, Abs. 2, Buchstaben a), b), c) und d).

558 *Jungermann*, DuD 2003, 71.

559 *Jandt* 2008, 283.

560 Gesellschaft für Informatik, DuD 2001, 38.

561 *Heinrichs*, in Palandt, § 12 Rn. 8.

sein Pseudonym hinzufügen und mit einem Schlüssel für ein pseudonymes Zertifikat signieren.[562]

1.6.4.3 Prüfung nach dem Signaturgesetz

§ 371a Abs. 1 Satz 2 ZPO setzt als Anforderung des Anscheinsbeweises zudem die erfolgreiche Prüfung der elektronischen Signatur nach dem Signaturgesetz voraus. Wird im Prozess die Vorlage der qualifizierten elektronischen Signatur und das Ergebnis ihrer Prüfung nicht bestritten, so sind diese Tatsachen vom Gericht als nicht streitig anzunehmen.[563]

Umstritten ist in der Literatur, ob für die Begründung des Anscheinsbeweises nur die Vorlage des Ergebnisses der Signaturprüfung ausreichend ist, oder ob der Nachweis der einzelnen Voraussetzungen einer qualifizierten Signatur erforderlich wird. Zu den zu beweisenden Voraussetzungen gehören die mathematische Sicherheit des Algorithmus, die Gültigkeit des Zertifikats zum Signaturerstellungszeitpunkt und der Nachweis, dass das zur Signatur zugeordnete Zertifikat von einem bei der Bundesnetzagentur angezeigten Zertifizierungsdiensteanbieter ausgestellt war. Diese sind die von Fischer-Dieskau genannten unmittelbaren prüfbaren Voraussetzungen einer qualifizierten elektronischen Signatur.[564] Dass diese Voraussetzungen vom Beweisführer nachgewiesen werden müssen, ist unstreitig. Anderes gilt bei den so genannten mittelbar prüfbaren Voraussetzungen.[565] Diese Voraussetzungen stehen in Verbindung mit der grundsätzlich bestehenden Qualifizierung des Zertifizierungsdiensteanbieters, der angeblich das der streitigen Signatur zugeordnete Zertifikat ausgestellt hat. Es stellt sich dann die Frage, ob die Partei, die sich auf die Qualifizierung beruft, die Erfüllung der signaturrechtlichen Anforderungen seitens des Zertifizierungsdiensteanbieters nachweisen muss, und wenn ja, welche Anforderungen zu beweisen sind oder ob der Tatbestand nur die erfolgreiche technische Signaturprüfung verlangt.[566]

Hierbei wird auf die Tatsache verwiesen, dass eine Reduzierung der tatbestandlichen Anforderungen den Grundsätzen des Institutes des Anscheinbeweises widerspräche, welche das Beibringen des vollen Beweises des typischen Geschehensverlaufs durch den Beweisführer verlangen. Ferner wird argumentiert, dass die notwendigen Erfahrungen im Umgang mit qualifizierten elektronischen Signaturen fehlen. Es besteht z. B. keine Sicherheit darüber, ob das zu prüfende Zertifikat tatsächlich von einem qualifizierten Zertifizierungsdiensteanbieter ausgestellt wurde oder ei-

562 *Roßnagel*, NJW 2001, 1825.

563 Hinweise zur Beweisbedürftigkeit im Prozessverfahren von Reichhold, in: Thomas/Putzo, vor § 284 Rn. 1.

564 *Fischer-Dieskau* 2006, 130.

565 *Fischer-Dieskau* 2006, 130.

566 *Fischer-Dieskau* 2006, 130.

gentlich missbräuchlich von einem Dritten, der sich als qualifizierter Anbieter ausgibt. Außerdem bestehen auch keine Erfahrungen was die Einhaltung der Sicherheitsanforderungen des Signaturgesetzes und der Signaturverordnung durch die bei der Bundesnetzagentur nur angemeldeten Zertifizierungsdiensteanbieter betrifft. In der Literatur kommt man somit zu dem Ergebnis, dass diese fehlenden Erfahrungswerte nicht zu Lasten des scheinbaren Signaturerstellers gehen dürfen, das heißt, der Beweisführer muss, neben den so genannten unmittelbaren prüfbaren Voraussetzungen, die Einhaltung der signaturrechtlichen Anforderungen seitens des Zertifizierungsdiensteanbieters nachweisen.[567]

Anderes gilt bei den akkreditierten Zertifizierungsdiensteanbietern, die vor ihrer Betriebaufnahme von der Bundesnetzagentur und von einer von der Bundesnetzagentur anerkannten Prüf- und Bestätigungsstelle überprüft werden. Dabei kommt der beweisbelasteten Partei – in der Regel der Signaturempfänger – die technisch-organisatorische Sicherheitsvermutung des § 15 Abs. 1 Satz 4 SigG zugute.[568] Während der Beweisführer, der über ein mit einer qualifizierten elektronischen Signatur versehenes Dokument verfügt, gegebenenfalls die bereits erwähnten Anbieteranforderungen mit Hilfe von Sachverständigen beweisen muss, befindet sich der Empfänger einer akkreditierten Signatur in einer besseren Beweislage. Dieser muss lediglich nachweisen, dass sich das Signaturverfahren des Signierers auf ein akkreditiertes Zertifikat stützt.

Im Ergebnis kann festgestellt werden, dass sich die vom Gesetzgeber erwünschte Beweiserleichterung zu Gunsten der qualifizierten Signaturverfahren im deutschen Recht nur durch den Einsatz akkreditierter Signaturen erreichen lässt.[569] Wie oben dargelegt, hat der Beweisführer, wenn er nur über eine qualifizierte Signatur als Beweismittel verfügt, die Einhaltung einer Reihe von Anforderungen seitens des Zertifizierungsdiensteanbieters nachzuweisen, was sicherlich keine einfache Aufgabe darstellt und vielmehr mit einem gewissen prozessualen Aufwand verbunden ist.

Schließlich ist anzumerken, dass die Signaturprüfung bezogen auf die Frage, ob der Signaturschlüssel-Inhaber tatsächlich die Sicherheitsmaßnahmen (wie das Einsetzen von geeigneten Komponenten) zur Erzeugung der Signatur getroffen hat, keinen Aufschluss bringen kann. Hierbei ist die Beweislage jedoch unkritisch, da die Anwendung von geeigneten Signaturkomponenten nach § 17 Abs. 2 Satz 2 SigG keine konstitutive Voraussetzung einer qualifizierten elektronischen Signatur darstellt.

567 *Fischer-Dieskau* 2006, 132.

568 *Roßnagel*, NJW 2001, 1826.

569 Hierzu *Gesellschaft für Informatik*, DuD 2001, 39.

1.6.5 Erschütterung der Beweiserleichterung des § 371a Abs. 1 Satz 2 ZPO

Die Regel der Beweiserleichterung des § 371a Abs. 1 Satz 2 ZPO begünstigt besonders den Erklärungsempfänger. Den Anschein der Echtheit zu erschüttern, obliegt im Falle des Bestreitens dem Signaturschlüssel-Inhaber.[570] Kritisiert wird an der beweisrechtlichen Begünstigung des Signaturempfängers, dass sie in der Praxis zu Lasten des Kunden (Signaturschlüssel-Inhabers) sei.[571] Eine solche Argumentation gegen beweisrechtliche Regelungen, die dem Erklärungsempfänger in einer privilegierten Beweislage versetzen, stützt sich auf die Tatsache, dass, wenn in der Papierwelt eine Unterschrift vom Beweisgegner nicht anerkannt wird, sie nach § 440 Abs. 1 ZPO von der beweisbelasteten Partei, in der Regel dem Erklärungsempfänger, zur vollen Überzeugung des Gerichts nachzuweisen ist. In diesem Fall sind keine Beweiserleichterungen zu Gunsten des Beweisführers vorgesehen. In der virtuellen Welt ist die Lage anders, wenn ein elektronisches Dokument, das mit einer qualifizierten Signatur versehen ist, vorgelegt wird. Im Fall der schlichten Nicht-Anerkennung der Echtheit des elektronischen Dokuments seitens des Erklärenden trägt nicht der Erklärungsempfänger, wie in der Papierwelt, die Beweislast zur vollen Überzeugung des Gerichts. Vielmehr gilt zu seinen Gunsten eine Beweiserleichterung, die von ihm, falls er über ein mittels einer akkreditierten elektronischen Signatur signiertes Dokument verfügt, nur den Bezug auf die Akkreditierung des Signaturverfahrens verlangt. Will der Erklärende dagegen die Authentizität der ihm zur Last gelegten Erklärung bestreiten, muss er nach § 371a Abs. 1 Satz 2 ZPO Tatsachen vortragen, die ernstliche Zweifel daran begründen, dass er diese nicht abgegeben hat.

Eine solche Beweisbegünstigung ist aber im elektronischen Geschäftsverkehr notwendig, sonst könnte der Signaturschlüssel-Inhaber beliebig die von ihm abgegebenen Erklärungen bestreiten und dann wäre der Beweisführer in eine beweisrechtliche Notlage versetzt.[572] Eine elektronische Signatur verfügt nicht über das biometrische Identifikationsmerkmal der eigenhändigen Unterschrift, deswegen wird eine solche Erleichterung erforderlich.[573] Sie schafft Rechtssicherheit. Der per Unterschrift Erklärende bestreitet normalerweise nicht die Authentizität seiner Erklärung,

570 BR-Drs. 14/4987, 13.

571 *Bizer*, DuD 2002, 279.

572 Gegen die Notwendigkeit einer gesetzlichen Beweisregelung für elektronisch signierte Dokumente *Fischer-Dieskau* 2006, 140. Nach der Autorin könnten „die Gerichte im Rahmen der freien Beweiswürdigung einen Anschein für die Signaturerstellung durch den Berechtigten durch Rückgriff auf die Diskussion und Rechtsprechung zur PIN-Problematik bei EC-Karten annehmen".

573 Gemäß der Gesezbegründung „würde eine Behandlung nach den Vorschriften über den Urkundenbeweis bedeuten, dass der Erklärungsempfänger als beweispflichtige Partei schutzlos wäre gegenüber einem unbegründeten Einwand des Beweisgegners, die Erklärung sei nicht von dem Signaturschlüssel-Inhaber abgegeben worden". BR-Drs. 14/4987, 25.

weil es ihm bewusst ist, dass ein Schriftvergleich in der Regel ohne weiteres die Urheberschaft der Urkunde bestätigen würde. Werden die Signaturverfahren, wie erwartet, verbreitet und würden sie ohne eine Beweiserleichterung zu Gunsten des Signaturempfängers angenommen, dann wäre es für den Signaturersteller ganz einfach seiner abgegebenen Erklärung zu entkommen.

Damit aber der Signaturschlüssel-Inhaber nicht vollkommen ungeschützt vor einer vom ihm nicht bewirkten Signaturerzeugung bleibt, sieht § 371a Abs. 1 Satz 2 ZPO die Möglichkeit der Erschütterung der abgegebenen Erklärung vor, indem Tatsachen vorgetragen werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüsselinhaber abgegeben worden ist. Dadurch entsteht mit dem Anscheinsbeweis im deutschen Beweisrecht in Bezug auf die qualifiziert elektronisch signierten Dokumente eine sachgerechte Risikoverteilung, wonach zu Gunsten des Erklärungsempfängers eine Beweiserleichterung gilt, die aber durch ernstlich nachgewiesene Gründe entkräftet werden kann. In diesem Zusammenhang liegt die große Herausforderung des Gerichts darin, das Gleichgewicht zwischen dem Anscheinsbeweis und den Anforderungen seiner Entkräftung zu etablieren.

Es ist umstritten, ob bei der Erschütterung des Anscheinsbeweises der Signaturschlüssel-Inhaber lediglich seine Gründe vortragen oder sie vielmehr sogar beweisen muss. Rapp erwähnt, „dass er (der Signaturschlüsselinhaber) die ernsthafte Möglichkeit vorträgt, dass die Erklärung nicht mehr mit seinem Willen abgegeben worden ist“[574]. *Schemmann*[575] deutet an, dass der bloße Vortrag von Tatsachen nicht ausreicht, was überzeugender erscheint. Vielmehr muss der Signaturschlüssel-Inhaber die Tatsachen beweisen. Noch überzeugender ist das Argument Fischer-Dieskaus, demzufolge der Signaturverwender konkrete Tatsachen vortragen und sie nötigenfalls beweisen müsse.[576] Diese Position scheint angemessen und zumutbar. Sie bietet dem Richter einen breiteren Spielraum zur Entscheidung. Daher ist dann von Fall zu Fall zu entscheiden, inwieweit und mit Blick auf den Streitigkeitsgrad des Arguments sich der Beweisaufwand des Beweisführers erstrecken soll.

Dabei genügt der Gegenbeweis zur Erschütterung des Anscheins.[577] Mittels des Gegenbeweises versucht die nicht beweisbelastete Partei die Unwahrheit des Hauptbeweises darzulegen.[578] Es gilt nicht die Regelung des § 292 ZPO, bei der der volle Beweis des Gegenteils erforderlich wird. Für die Entkräftung des § 371a Abs. 1 Satz 2 ZPO reicht der Nachweis von Fakten, die andere ernsthafte Geschehensabläufe darstellen.[579] Diese Tatsachen aber müssen im Streitfall voll bewiesen werden.

Besonders entscheidend bei dem Tatbestand von § 371a Abs. 1 Satz 2 ZPO ist die Frage, welche Tatsachen vorgebracht werden können, um die ernstlichen Zweifel

574 *Rapp* 2002, 151.

575 *Schemmann*, ZZP 118 (2005), 171.

576 *Fischer-Dieskau* 2006, 118.

577 *Fischer-Dieskau* 2006, 138.

578 *Reichhold*, in: Thomas/Putzo §284, Rn. 8. Siehe hierzu bereits Gliederungspunkt 1.2.4.

579 Hierzu *Roßnagel*, NJW 1998, 3319.

daran zu begründen, dass die Erklärung vom Signaturschlüsselinhaber abgegeben worden ist. Bei der Anfechtung einer elektronisch signierten Erklärung wird die Interpretation dieses Rechtsatzes für den Richter eine Herausforderung. Es ist nicht zu verkennen, dass § 371a ZPO ein gewisses Maß an freier Beweiswürdigung schon in sich trägt, denn der Wortlaut des Textes verwendet die Begriffe „Tatsachen" die „ernstliche Zweifel daran begründen", was dem Richter einen Spielraum überlässt. Dem Gericht obliegt dann die Entscheidung über die Tatsachen, die diese Tatbestandsmerkmale erfüllen können. Im Folgenden sind die denkbaren Erschütterungsgründe zu überprüfen.

1.6.5.1 Diebstahleinwand

Ein praktisches Problem, das bei der Anwendung elektronischer Signaturen sehr wahrscheinlich vorkommen wird, ist das des Diebstahls oder Raubes der Signaturkarte, so wie bei den unzähligen Fällen von Bankkartenmissbrauch. Hier ist zu fragen, ob das Gericht dies in solchen Fällen als Grund zur Erschütterung des Anscheins der Echtheit annehmen soll. § 371a Abs. 1 Satz 2 ZPO schützt den Signaturschlüsselinhaber in den Fällen, in denen es klar wird, dass die Erklärung nicht von ihm abgegeben wurde. In diesem Sinne ist das Ausreichen der Diebstahlsbehauptung des Signaturschlüssel-Inhabers vertretbar, sie wird als zumutbar und akzeptabel angesehen, obschon ein Diebstahl schwer zu beweisen sein kann.

Von Bedeutung ist aber die Feststellung des Zeitpunkts, ab dem der Zertifikatinhaber von dem Diebstahl Kenntnis hatte und ob er dann den notwendigen Aufwand, um das Zertifikat so schnell wie möglich zu sperren, betrieben hat.[580] Denn ab diesem Zeitpunkt ist der Zertifikatinhaber verpflichtet[581], den Zertifizierungsdienstanbieter von dem Signaturkartenverlust zu informieren, damit dieser das Zertifikat sperren kann. Als Argument von Nutzen in diesem Zusammenhang kann auch die Möglichkeit zur PIN-Ausspähung beispielsweise durch die Manipulation der Hard- oder Softwareumgebung sein.[582] Es muss ebenfalls ermittelt werden, ob der Signaturschlüssel-Inhaber den Diebstahl angezeigt hat. Das Verhalten des Zertifikatinha-

580 Laut § 6 Abs. 1 SigV soll die Zertifizierungsstelle dem Signaturschlüssel-Inhaber von den geeigneten Maßnahmen im Verlustfalle unterrichten. Zur Unterrichtungspflicht der Zertifizierungsdiensteanbieter: *Roßnagel*, RMD, § 6 SigG, Rn. 24 ff.; außerdem bereits im 2. Teil Gliederungspunkt 1.3.5.5.

581 Nach § 6 Nr. 1 und 2 SigV wird der Signaturschlüssel-Inhaber von den zu treffenden geeigneten Maßnahmen im Verlustfalle oder bei Verdacht des Missbrauchs und von den Maßnahmen über die Geheimhaltung von persönlichen Identifikationsnummern oder anderen Daten zur Identifikation unterrichtet. Der Signaturschlüssel-Inhaber verpflichtet sich in der Regel mittels eines Vertrags gegenüber dem Zertifizierungsdiensteanbieter, diese Maßnahmen einzuhalten.

582 *Schemmann*, ZZP 118 (2005), 173.

bers nach der Feststellung des angeblichen Diebstahls ist daher von großer Relevanz, damit dieses Argument nicht als einfache Ausflucht dient. In jedem Fall muss der Richter den Geschehensablauf unter strengen Kriterien neu betrachten, denn der Diebstahleinwand darf nicht zu einer üblichen Ausrede werden.

Im Rahmen dieser Diskussion muss jedoch betrachtet werden, dass die Auseinandersetzung über den Anscheinsbeweis bei der Nutzung von Bankkarten nicht als Parameter für den Missbrauch von Signaturkarten eingesetzt werden soll. Dabei ist die Warnung von *Schemmann* zu beachten, wonach es bei den Bankkarten um die Verletzung von Pflichten seitens des Bankkunden auf der Grundlage eines mit der Bank abgeschlossenen Vertrags geht.[583] Im Verhältnis zwischen Signaturkarteinhaber und dem Empfänger der betrügerischen Erklärung besteht meistens keine vertragliche Beziehung. Ob die Verletzung der Sorgfaltspflichten seitens des Signaturschlüssel-Inhabers beim Umgang mit der PIN und Signaturkarte für seine Haftung entscheidend sein wird, ist noch von der Rechtsprechung zu bestimmen. Für die Erschütterung des Anscheinsbeweises kommt es aber nicht auf die Frage an, wie der Dieb Kenntnis von der PIN erlangt hat, da Voraussetzung für den Diebstahl die Wegnahme der Signaturkarte gegen den Willen des Signaturschlüssel-Inhabers ist.[584]

Zusammenfassend kommt man zu dem Ergebnis, dass der Diebstahleinwand das Tatbestandsmerkmal „Tatsachen" des § 371a Abs.1 Satz 2 ZPO begründen kann. Ob der Vortrag des Signaturschlüssel-Inhabers vom Gericht angenommen wird, ist von Fall zu Fall und aufgrund der gesamten Fakten zu entscheiden.

Davon zu unterscheiden ist die Haftung aufgrund des Rechtsscheins. Drei sind die Voraussetzungen der Rechtsscheinhaftung.[585] Sie wirkt nur zugunsten des Vertrauenden (in dem Fall der Signaturempfänger). Sie fordert einen objektiven Scheintatbestand an, das heißt, der Schein einer wirklich bestehenden Rechtslage (das positive Prüfergebnis der Signatur schafft dies). Die dritte Voraussetzung ist die Zurechenbarkeit des Schuldners (hier der Signaturschlüssel-Inhaber). Bei der Rechtsscheinhaftung muss der Signaturschlüssel-Inhaber die Schäden ersetzen, obwohl er die zugrunde liegende Erklärung nicht abgegeben hat. Er haftet aber für die Handlung eines Dritten, der etwa anhand seiner Signaturkarte und die auf der Karte geschriebene PIN, die elektronische Nachricht signiert hat. Die Zurechenbarkeit des Signaturschlüssel-Inhabers zur Willenserklärung des Dritten ergibt sich somit aus der Verletzung von Sorgfaltspflichten beim Umgang mit der Signaturkarte und PIN.[586]

583 *Schemmann*, ZZP 118 (2005), 174.

584 *Fischer-Dieskau* 2006, 138.

585 *Reese* 2006, 49.

586 Siehe hierzu *Spiegelhalder* 2007, 164.

1.6.5.2 Das Präsentationsproblem

In Bezug auf dieses Thema weist die Literatur auf die Möglichkeit von mehrdeutigen Präsentationen von Daten bei der Signierung eines elektronischen Dokuments hin.[587] Gemeint ist die Möglichkeit, dass elektronische Willenserklärungen gar ohne eine Veränderung der signierten Daten, alleine durch Umstände der Präsentation, verfälscht werden können.[588] Mit anderen Worten, es kann sein, dass der Signaturschlüssel-Inhaber Daten signiert, die er gar nicht signieren wollte. *Pordesch* geht von einem Begriff des Präsentationsproblems aus, zu dem mindestens zwei Präsentationen derselben signierten Daten so voneinander abweichen, dass sie von Menschen unterschiedlich interpretiert werden.[589]

Die Ursachen dieses Problems seien technische Fehler und Manipulationen der zum Präsentieren genutzten Anwenderinfrastruktur.[590] Eine andere mögliche Ursache seien auch die Varianten der verschiedenen Systeme, die verwendet werden und deren Bedienung.[591]

In dieser Problematik ist auch das Verhalten des Nutzers während der Präsentation von Bedeutung. Die gewählte Ansicht des Dokuments, die Art, wie er durch das Dokument navigiert, und die Eingaben, die er vornimmt, können sich auf die Wahrnehmung der Erklärung auswirken. *Pordesch* zitiert das Beispiel der Vielfalt von Ansichtsmöglichkeiten eines Word-Dokuments.[592] Es variiert von der druckerorientierten Seitenansicht über Normal-, Online-, Gliederungs- und Seitenlayoutansicht, Überarbeitungsmodus mit Kennzeichnung von Änderungen und weiteren Einstellungen. Dies sei eine auch für Experten kaum verständliche Fülle von abweichenden Ansichtsmöglichkeiten der Daten. Es könne leicht geschehen, dass ein ungeübter Nutzer die „Normal-Ansicht" wählt, bei der Grafiken und Textrahmen ausgeblendet sind. Wenn diese erhebliche Informationen in Bezug auf das Hauptdokument enthalten, kann das Ignorieren von diesen einen Schaden verursachen. Das Risiko erhöht sich besonders bei der Anwendung von fremden Signaturanwendungskomponenten.[593] Nach den Ergebnissen der Simulationsstudien von *provet* haben diejenigen, die die zum Verifizieren und Signieren verwendete Anwenderinfrastruktur wenigs-

587 *Gesellschaft für Informatik*, DuD 2001, 39; *Fox*, DuD 1998, 387.

588 *Pordesch*, DuD 2000, 89.

589 *Pordesch* 2002, 20; *ders.*, DuD 2000, 89.

590 *Pordesch*, DuD 2000, 89.

591 *Pordesch*, DuD 2000, 89; *ders.* 2002, 51 ff.

592 *Pordesch*, DuD 2000, 91.

593 *Fischer-Dieskau* 2006, 136. Die Definition von Signaturanwendungskomponenten gemäß § 2, Nr. 11 des Signaturgesetzes lautet: Software- und Hardwareprodukte, die dazu bestimmt sind, a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signatur zuzuführen oder b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen.

tens teilweise kontrollieren, Möglichkeiten „Systeme unerkannt zu manipulieren und den Nutzer zu täuschen“.[594]

Um die möglichen Schäden durch das Präsentationsproblem zu vermeiden, sind Maßnahmen zu treffen, die genereller Natur sind. Die Standardisierung von Präsentationsdatenformaten z.B. ist eine notwendige Aktion.[595] Erforderlich sind Bestimmungen in Bezug auf Anordnung und Zeichenformat des Layouts, auf die Fenstergröße und auf andere Funktion wie z. B. die zur Navigation. Wichtig ist die Anwendung von Signaturerstellungskomponenten gemäß §17 Abs. 2 Satz 1 SigG, die feststellen lassen, auf welche Daten sich die Signatur bezieht, und entsprechend § 17 Abs. 2 Satz 3 SigG nach Bedarf den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Hierbei ist jedoch anzumerken, dass aufgrund der Natur der Normen, die den Einsatz von sicheren Komponenten regeln (so genannte „Soll-Vorschriften“), es dem Nutzer überlassen bleibt, ob er die dort beschriebenen sicheren Komponenten einsetzt.[596]

Trotz dieser möglichen Maßnahmen ist und bleibt das Präsentationsproblem eine Achillesferse bei der Anwendung elektronischer Signaturen.[597] Eine noch offene und besonders schwierige Frage ist, inwieweit das Argument der fehlerhaften Präsentation als mögliche Erschütterung des Anscheins der Echtheit des § 371a Abs. 1 Satz 2 ZPO dienen kann. Grundsätzlich kann das Argument vom Gericht angenommen werden, da zu seinem Kern der Zweifel an der Willentlichkeit der Erklärung gehört, was genau das Tatbestandmerkmal des § 371a Abs. 1 Satz 2 ZPO erfüllt. So wie das Argument des Diebstahls darf aber auch das Präsentationsproblem nicht als Ausflucht für den Signaturschlüsselinhaber dienen. Um dies zu vermeiden, wird das Gericht vor eine schwierige Aufgabe gestellt, in der das Hinzuziehen von Sachverständigen sehr wahrscheinlich wird. Die Signaturanwendungskomponenten und die Umgebung, in der die strittige Signatur erstellt wurde, müssen begutachtet werden, um die Behauptungen des Signaturanwenders zu überprüfen.

Bei der Erschütterung des Anscheinsbeweises aufgrund des Präsentationsproblems sollte das Gericht in der Regel nicht so hohe Anforderungen an den Gegenbeweis des Signaturschlüssel-Inhabers ansetzen. Es muss darauf geachtet werden, dass der Erklärende üblicherweise und trotz der vom Zertifizierungsdiensteanbieter geleisteten Unterrichtung zur Sicherheitsmaßnahmen über kein Wissen von den Gefahren einer Falschpräsentation verfügt.[598]

594 *Pordesch*, DuD 2000, 92. *Gesellschaft für Informatik*, DuD 2001, 39.

595 *Pordesch* 2002, 190.

596 *Gesellschaft für Informatik*, DuD 2001, 39.

597 *Fischer-Dieskau*/*Gitter*/*Paul*/*Steidle*, MMR 2002, 713.

598 *Roßnagel*, NJW 2001, 1826; *Fischer-Dieskau* 2006, 106.

1.6.5.3 Signaturkarteweitergabe

Zu überprüfen ist auch ob, das Gericht das Argument annehmen soll, wonach der Signaturschlüssel-Inhaber willentlich seine Signaturkarte und PIN an einen Dritten weitergegeben hat. Vorstellbar wäre, dass der Dritte sich nicht an die von Signaturschlüssel-Inhaber angegebenen Weisungen einer möglichen versteckten Stellvertretung hält. Beweist der Signaturkarteinhaber seinen abweichenden ursprünglichen Willen gegenüber der vom Dritten abgegebenen Erklärung, ist von der Erschütterung des Anscheinsbeweises auszugehen.[599]

Auch in diesem Fall bleibt die Haftung des Signaturschlüssel-Inhabers gegenüber dem Geschädigten nach Rechtsscheintatbeständen unberührt.

1.6.6 Nicht von § 371a Abs. 1 Satz 2 ZPO umfasste Themen

Bisher sind die beachtlichen Argumente einer Entkräftung des Anscheinsbeweises des § 371a Abs. 1 Satz 2 ZPO dargestellt worden. Wie gezeigt, beschränken sich diese möglichen Themen des Gegenbeweises auf den Diebstahleinwand, auf das Präsentationsproblem und auf die Kartenweitergabe. Es gibt aber auch ungeeignete Argumente für die Erschütterung, die aus rechtsdogmatischer Perspektive nicht vom § 371a Abs. 1 Satz 2 ZPO umfasst werden. Diese Argumente sind im Folgenden zu überprüfen.

1.6.6.1 Falsche Übermittlung und Irrtum (§§ 119, 120 BGB)

Mit der Verabschiedung und dem Inkrafttreten des Formanpassungsgesetzes wurde auch § 120 des BGB (Anfechtbarkeit der Willenserklärung wegen falscher Übermittlung) verändert. Der Begriff „Anstalt“ wurde durch die Formulierung „Einrichtung“ ersetzt. Gemäß der Begründung sollte diese neue Fassung umfangreicher sein, denn die alte zielte auf die Anfechtung der Übermittlung per Post oder Telegraf.[600] Mit dem Ausdruck „Einrichtung“ soll der Wortlaut des Gesetzes an die Realität des elektronischen Verkehrs angepasst werden, in der eine Vielfalt von privaten Dienstleistungsanbietern tätig sind.

Anzufechten ist die Willenserklärung, die falsch übermittelt worden ist. Anders als beim Präsentationsproblem, in dem die Unrichtigkeit noch in den Machtbereich des Erklärenden fällt (eigentlich im Softwarebereich), handelt es sich hier um einen

599 *Fischer-Dieskau* 2006, 139.

600 BR-Drs. 14/4987, 14.

Fehler auf dem virtuellen Weg, nach dem Versand und vor dem Empfang[601], das so genannte „Transportrisiko“[602].

Problematisch für den Erklärenden ist, dass er hauptsächlich das Risiko einer unrichtigen Übermittlung trägt, obwohl ihm die Anfechtungsmöglichkeit zur Verfügung steht. Beispielsweise im Fall eines Eingriffes mit Datenmanipulationen hat er gemäß § 122 BGB „jedem Dritten den Schaden zu ersetzen, den der andere oder der Dritte dadurch erleidet, dass er auf die Gültigkeit der Erklärung vertraut“.

Der Irrtum bezieht sich auf die Fehlerhaftigkeit der Willensäußerung. Der Erklärende setzt ein anderes Erklärungszeichen als er wollte (Erklärungsirrtum) oder er erklärt zwar, was er wollte, aber dies bedeutet etwas anderes als ursprünglich gemeint war (Inhaltsirrtum).[603] Soll der Irrende das Rechtsgeschäft anfechten, dann wird dieses gemäß § 142 BGB rückwirkend vernichtet. Er haftet dann laut § 122 BGB für den Schaden, den der andere oder der Dritte dadurch erleidet, dass er auf die Gültigkeit der Erklärung vertraut.

Daher kommt im Fall einer falschen Übermittlung oder eines Irrtums die Anwendung des § 371a Abs. 1 Satz 2 ZPO überhaupt nicht in Frage, sondern die Regelungen zur Anfechtung fehlerhafter Willenserklärungen (§§ 119 ff. BGB).

1.6.6.2 Fehlende Sicherheit in der technisch-organisatorischen Infrastruktur

Auch ist zu untersuchen, ob ein Verstoß gegen die dem Zertifizierungsdiensteanbieter vom Signaturgesetz auferlegten Pflichten Auswirkungen auf den Beweiswert eines elektronisch signierten Dokuments haben oder ob ein solcher Verstoß als Argument zur Erschütterung des Anscheinsbeweises vom Signaturschlüssel-Inhaber angewandt werden darf.

In diesem Kontext kämen Verstöße, wie die fehlerhafte Identifizierung des Antragstellers nach § 5 Abs. 1 SigG oder die unzureichende Kontrolle seiner Vertretungsmacht oder beruflicher Angaben nach § 5 Abs. 2 SigG in Betracht. Auch zu erwähnen wären etwa Einbrüche in die Sicherheitsanlagen des Zertifizierungsdiensteanbieters, wo wichtige Tätigkeiten durchgeführt werden, wie etwa das Ausstellen von Zertifikaten. Weitere denkbare Verstöße könnten die unzureichende oder falsche Unterrichtung des Antragstellers nach § 6 Abs. 2 SigG oder die fehlerhafte Dokumentationsführung laut § 10 SigG oder die inkorrekte Übergabe der sicheren Signaturerstellungseinheit dem Signaturschlüssel-Inhabers nach § 5 Abs. 2 SigV sein.

Im Begriff einer qualifizierten elektronischen Signatur sind die Anforderungen einer fortgeschrittenen Signatur (§ 2 Nr. 2 SigG) enthalten und zusätzlich muss die Signatur noch auf einem, zum Zeitpunkt ihrer Erzeugung gültigen, qualifizierten

601 BR-Drs. 14/4987, 14.

602 *Mehrings*, MMR 1998, 30.

603 *Medicus* 2004, 85.

Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt werden (§ 2 Nr. 3 SigG). Ein qualifiziertes Zertifikat wiederum muss gemäß § 2 Nr. 7 SigG die Voraussetzungen des § 7 SigG erfüllen und von einem Zertifizierungsdiensteanbieter ausgestellt werden, der mindestens die Anforderungen der §§ 4 bis 14 oder § 23 SigG erfüllt. Eine Auslegung, wonach ein einziger Verstoß gegen die Anbieteranforderungen schon dazu führen würde, dass die Voraussetzung einer qualifizierten elektronischen Signatur nicht gegeben ist, wäre sicherlich drastisch. Es würde zu unerwünschter Unsicherheit führen, wenn die Teilnehmer des elektronischen Geschäftsverkehrs nach der Abgabe oder dem Empfang einer qualifiziert signierten Erklärung befürchten müssten, dass der kleinste Fehler[604] seitens des Zertifizierungsdiensteanbieters erfolgreich bestritten werden könnte. Dabei würde die elektronische Form und indirekt der Anscheinsbeweis des § 371a Abs. 1 Satz 2 ZPO davon abhängen, dass die Zertifizierungsdiensteanbieter keinen einzigen Fehler bei ihrer Tätigkeit begehen. Da es das Ziel des Signaturgesetzes und der anderen Regelungen ist, die Grundlage für das Vertrauen an den elektronischen Geschäftsverkehr zu schaffen, stände eine Auslegung, welche die kontinuierliche und fehlerfreie Einhaltung der signaturrechtlichen Anforderungen seitens des Zertifizierungsdiensteanbieter als Voraussetzung einer qualifizierten Signatur bedingt, im Widerspruch zu den angestrebten Zielen, Vertrauen und Rechtssicherheit.

In diesen Fällen ist daher § 371a Abs. 1 Satz 2 ZPO nicht anwendbar, denn die Verstöße gegen die Dienstleistungspflichten des Zertifizierungsdiensteanbieters sollen in der Regel keinen Einfluss auf die Qualität der qualifizierten elektronischen Signatur nehmen. Würde man bejahen, dass gravierende Konzeptfehler des Zertifizierungsdiensteanbieters einen Einfluss auf die Qualität der Signatur nehmen, dann käme die Anwendung des § 371a Abs. 1 Satz 2 ZPO nicht in Frage, weil die Voraussetzung für die Geltung dieser Beweiserleichterung, nämlich die qualifizierte elektronische Signatur, bereits nicht gegeben wäre. Offen ist aber immer der Weg zu einem Schadenersatzanspruch von dem Beschädigten gegen den Zertifizierungsdiensteanbieter nach § 11 SigG.

604 Denkbar wäre eine Trennung zwischen zwei Verschiedenen Gruppen von Verstößen gegen die Dienstleistungspflichten seitens eines angezeigten Zertifizierungsdiensteanbieters. Die so genannten „Konzeptfehler“ entsprechen dabei einem fehlerhaften Geschäftsmodell oder einer Prozessorganisation seitens des Zertifizierungsdiensteanbieters, welche nach dem Signaturgesetz oder der Signaturverordnung nicht gesetzkonform sind. Diese wären als gravierend einzustufen und könnten das Tatbestandmerkmal „der ernstlichen Zweifel“ erfüllen. Die zweite Gruppe besteht aus den „Einzelfehlern“, welche einmal oder auch in seltenen Fällen mehrmals von Mitarbeitern des Zertifizierungsdiensteanbieters verursacht werden. Hierbei verfügt der angezeigte Zertifizierungsdiensteanbieter über ein korrektes signaturgesetzkonformes Konzept. Der einzelne Fehler hat keinen Einfluss auf den Beweiswert der signierten Dokumente.

Anders als die privaten elektronischen Dokumente gilt für öffentliche elektronische Dokumente, die qualifiziert signiert sind, laut § 371a Abs. 2 Satz 2 ZPO die Vermutung der Echtheit des § 437 ZPO. Die Regelung stützt sich auf den Begriff der öffentlichen Urkunde des § 415 Abs. 1 ZPO, das heißt, das Dokument muss 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 werden.

Die zweite Voraussetzung der Vermutung der Echtheit ist das Vorliegen einer qualifizierten Signatur. Somit geht die Wirkung eines öffentlichen elektronischen Dokuments weiter als die des privaten elektronischen Dokuments, da die Letztere einen Anschein der Echtheit begründet. Während zur Erschütterung des Anscheins der Echtheit der Gegenbeweis genügt, ist zur Entkräftung der Vermutung der Echtheit nach § 292 ZPO der Beweis des Gegenteils nötig. Der Signaturschlüssel-Inhaber muss in diesem Fall beweisen, dass er die Erklärung nicht signiert hat, dass ihm ein anderer Text zur Signierung vorgelegen hat oder dass die Signatur von einem anderen unter Missbrauch erzeugt wurde.[605]

Dieser Behandlungsunterschied rechtfertigt sich dadurch, dass auch in der Papierwelt private und öffentliche Urkunden angesichts ihrer Eigenschaften differenziert behandelt werden. Die Echtheit einer nicht anerkannten Privaturkunde ist gemäß § 440 Abs. 1 ZPO zu beweisen, während sich bei öffentlichen Urkunden die Echtheitsvermutung meist ohne weiteres aus Inhalt und Form ergibt.[606] Ferner ist die differenzierte Behandlung in der Tatsache begründet, dass dem Bürger immer eine Abschrift der Urkunde zugestellt wird und die Urschrift von der Behörde aufbewahrt wird. Das ermöglicht das leichte Feststellen der Übereinstimmung zwischen Urschrift und Abschrift und begründet die Vermutung der geringeren Fälschungswahrscheinlichkeit.[607] Kritisch wird die favorisierte Behandlung zu Gunsten öffentlicher elektronischer Dokumente gegenüber den privaten elektronischen Dokumenten in der Literatur aufgrund der Tatsache betrachtet, dass beide im Endeffekt mit demselben Instrument zur Sicherung der Integrität und Authentizität versehen werden, nämlich der qualifizierten elektronischen Signatur.[608] Ferner seien sowohl vom Anschein als auch von der Vermutung zwei Aspekte umfasst, die eigentlich durch die qualifizierte Signatur nicht nachgewiesen werden, nämlich die Präsentation der signierten Daten und die Zurechnung der Signatur zum Signaturschlüssel-Inhaber. In Hinsicht auf die Präsentation der Daten wäre die Differenzierung zugunsten öffentlicher Dokumente gerechtfertigt, da Behörden und mit öffentlichem Glauben versehene Personen verpflichtet sind, ihre Systeme grundsätzlich sicherer zu gestalten, und

605 *Roßnagel/Fischer-Dieskau*, NJW 2006, 808.

606 *Huber*, in: Musielak, § 437 Rn. 3.

607 *Geiger*, § 98 Rn. 29.

608 *Roßnagel/Fischer-Dieskau*, NJW 2006, 808.

dadurch vermindert sich die Chance von Manipulationen und dem Unterschieben von Daten. In Bezug auf die Zuordnung der Signatur zum Signaturschlüssel-Inhaber ist aber die Differenzierung eher schwieriger zu akzeptieren, denn eine konsolidierte Rechtsprechung zu EC-Karte und PIN erkennt lediglich einen Anschein und keine Vermutung an.[609]

Schließlich ist hervorzuheben, dass nach dem Wortlaut des § 371 Abs. 2 Satz 1 ZPO die Beweiskraft öffentlicher elektronischer Dokumente der Beweiskraft öffentlicher Urkunde gleichgestellt wird und zwar selbst dann, wenn sie nicht mit einer qualifizierten elektronischen Signatur versehen sind. § 371 Abs. 2 Satz 1 ZPO verwendet nur den Ausdruck „elektronische Dokumente" anders als § 371 Abs. 2 Satz 2 ZPO, der auf die qualifizierte elektronische Signatur verweist. Das einfache elektronische Dokument begründet folglich nach §§ 415 Abs. 1, 417 und 418 Abs. 1 ZPO vollen Beweis für den Vorgang, für amtliche Anordnungen, Verfügungen und Entscheidungen sowie für die in ihnen bezeugten Tatsachen.[610] Es reicht hierbei nach § 371 Abs. 2 Satz 1 ZPO, dass das öffentliche elektronische Dokument von einer Behörde oder einer mit öffentlichem Glauben versehenen Person ausgestellt wird. Um die Vermutung der Echtheit zugunsten öffentlicher elektronischer Dokumente nach § 371 Abs. 2 Satz 1 ZPO zu widerlegen ist der Beweis des Gegenteils erforderlich.

1.8 Die Transformation und das transformierte Dokument als Beweismittel

Im Folgenden wird das bedeutsame Thema der Transformation untersucht. Es ist den Begriffen, den Grundsätzen und der Beweisproblematik um die Transformation nachzugehen.

1.8.1 Transformation von Dokumenten und ihre Notwendigkeit

Als Transformation versteht man die Übertragung eines Dokuments von einem in ein anderes Format.[611] Eine Transformation kann grundsätzlich in drei Formen erfolgen. Ein elektronisches Dokument kann von einem elektronischen Format (z.B. doc) in ein anderes Format (z.B. pdf) übertragen werden (E-to-E). Es kann auch nötig sein, ein elektronisches Dokument mittels eines Druckers in die Papierform umzuwandeln (E-to-P). Die dritte Transformationsform ist ein Papierdokument anhand eines Scanners in ein elektronisches Dokument umzuwandeln (P-to-E).[612]

609 BGH, NJW 2004, 3623; OLG Frankfurt a.M., WM 2002, 2102; OLG Stuttgart, NJW-RR 2002, 1274; OLG Hamm, NJW 1997, 1711; OLG Frankfurt a. M., NJW-RR 2002, 628.

610 *Roßnagel*/*Fischer-Dieskau*, NJW 2006, 808.

611 *Roßnagel*/*Fischer-Dieskau*/*Wilke*, CR 2005, 903.

612 *Farnbacher*/*Fischer-Dieskau*/*Hollerbach*/*Winnecke*, in: Roßnagel/Schmücker 2006, 113.

Es gibt eine steigende Tendenz, Dokumente zu transformieren. Erstens überlegen sich Behörden und Unternehmen das Umwandeln von Papierdokumenten in elektronische Formate, da sie eine Fülle von Räumen angesichts Archivierungspflichten belegen. Sollte sich die Möglichkeit ergeben, die Originale durch die mittels einer Transformation erlangten Zieldokumente zu ersetzen, würde dies eine ungeheuere Platzersparnis darstellen, denn elektronische Dokumente benötigen keinen körperlichen Transport und physische Aufbewahrung.[613] Sie können auch schneller als ein Papierdokument aufgefunden und übertragen werden und ermöglichen, dass mehrere Personen sie gleichzeitig benutzen. Zum anderen wird eine Transformation als Mittel zur langfristigen Sicherung der Lesbarkeit elektronischer Dokumente erforderlich. Dass angesichts der raschen technologischen Entwicklung die Soft- und Hardware, die zum Lesen eines bestimmten Dokumentenformats erforderlich sind, schon binnen einer relativ kurzen Zeit obsolet werden, macht es notwendig, dass diese Dokumente in aktuelle Formate transformiert werden, damit sie an jedem Rechner lesbar bleiben.[614] Ferner kann eine Transformation auch erforderlich sein, um die Bestimmungen des Daten- und Geheimnisschutzes zu gewährleisten. Das kann dann der Fall sein, wenn personenbezogene Daten in Krankenakten, die für die medizinische wissenschaftliche Forschung angewandt werden, geschwärzt werden müssen. Eine ähnliche Situation besteht, wenn die Verwaltung verpflichtet ist, allen Bürgern Einsichtsrechte in die Unterlagen zu gewähren, aber gleichzeitig dabei die informationelle Selbstbestimmung des Betroffenen achten muss. Des Weiteren besteht ein Bedürfnis nach einer Transformation, um etwa die Vorgangsbearbeitung einer Behörde, die ihre Pflichten auch auf elektronischem Weg anbietet, zu ermöglichen. Da die Dokumente in den unterschiedlichsten Formaten vorgelegt werden, wird die Transformation erforderlich, um eingehende Dokumente, die in Fremdformaten erstellt worden sind, in die Formate zu transformieren, deren Bearbeitung der Behörde möglich ist.[615]

613 *Roßnagel*/*Wilke*, NJW 2006, 2145.

614 *Roßnagel*/*Fischer-Dieskau*/*Wilke*, CR 2005, 903.

615 Nach § 3a Abs 3 VwVfG darf aber die Behörde den Zugang elektronischer Dokumente auf bestimmte Formate beschränken. Nach dieser Vorschrift soll sie, falls das der Behörde übermittelte elektronische Dokument für sie zur Bearbeitung nicht geeignet ist, dies dem Absender mit den Angaben der für sie geltenden technischen Rahmenbedingungen unverzüglich mitteilen. Der Empfänger darf aber auch geltend machen, dass das von der Behörde übermittelte elektronische Dokument von ihm nicht bearbeitet werden kann. In diesem Fall muss die Behörde es erneut in einem geeigneten elektronischen Format oder als Schriftstück übermitteln.

1.8.2 Grundsätze der rechtssicheren Transformation

In Deutschland wurden im Rahmen des Projekts Rechtssichere Transformation signierter Dokumente (Transidoc) Konzepte für die Durchführung rechtssicherer Transformation von Dokumenten entwickelt.[616] Mit Blick auf die Gefahr, dass bei der Dokumentkonvertierung zum einen Daten gelöscht oder verfälscht werden können und zum anderen der Beweiswert der entsprechenden Signatur verloren gehen kann, wurden Grundsätze der rechtssicheren Transformation vorgestellt.[617]

Die Grundsätze wurden so konzipiert, dass sie für die drei verschiedenen Transformationsformen anwendbar sind. Erstens sollen die Transformationen aus Effizienzgründen und zur Vermeidung menschlicher Fehler so weit wie möglich automatisiert durchgeführt werden. Zweitens muss die inhaltliche Übereinstimmung zwischen Ausgangs- und Zieldokument gewährleistet werden.[618] Drittens müssen die Signaturen des ursprünglichen Dokuments verifiziert und das Ergebnis der Prüfung vermerkt werden.[619] Viertens ist auch die Integrität von Ausgangs- und Zieldokument während des Transformationsverfahrens durch etwa Hashwerte zu gewährleisten. Fünftens muss die Transformation dem ausführenden Bearbeiter oder dem Verantwortlichen für das durchführende System zugerechnet werden. Sechstens sollen nur die dazu berechtigten Mitarbeiter eine Transformation durchführen, gemäß den entsprechend anwendbaren gesetzlichen Regelungen oder eigenen Berechtigungskonzepten. Zu erwähnen ist auch, dass die Berechtigung zur Transformation auch nachträglich überprüfbar sein muss, wobei das notarielle Siegel bei Papierdokumenten und die Attributszertifikate bei elektronischen Dokumenten angewandt werden können. Siebtens muss der Transformationsprozess durch geeignete organisatorische und technische Sicherheitsmaßnahmen auf Grund der Grundsätze des Daten- und Geheimschutzes vor dem Zugriff von Unberechtigten geschützt werden. Achtens ist die Verwendbarkeit und Verkehrsfähigkeit des Zieldokuments zu gewährleisten. Dabei müssen Formate ausgesucht werden, die eine langfristig eindeu-

616 Das Projekt Transidoc wurde vom Bundesministerium für Wirtschaft und Arbeit gefördert, und hatte folgende beteiligten Institutionen: Fraunhofer Institut für Sichere Informationstechnologie SIT, Darmstadt, Projektgruppe verfassungsverträgliche Technikgestaltung der Universität Kassel, Zentrum für Informations- und Medizintechnik (Uni-Klinikum Heidelberg), Intercomponentware AG, curiavant Internet GmbH, Datev e.G. und Bundesnotarkammer Berlin; siehe hierzu: http://www.transidoc.de.

617 *Roßnagel*/*Schmidt*, 2008, i.E.

618 Es ist aber hier zu behaupten, dass manchmal Veränderungen am Ausgangsdokument vorgenommen werden müssen. Das ist etwa der Fall bei der aus datenschutzrechtlichen Gründen notwendigen Schwärzung personbezogener Daten in Krankenakten, die vorgenommen werden müssen.

619 Sollte sich das Ausgangsdokument um ein elektronisch signiertes Dokument handeln, dann sind gegebenenfalls die verschiedenen Verifikationsdaten zu beschaffen, wie Zertifikate, Sperrlisten, Zertifikatsstatusabfrage, Zeitstempel, usw.

tig interpretierbare und stabile Verwendung des Dokuments ermöglichen. Neuntes soll die Nachvollziehbarkeit der Transformation ermöglicht werden, indem ihr gesamter Verlauf protokolliert wird. Es handelt sich hier um die Daten, die festzuhalten sind, wie etwa Bezeichnung der eingesetzten Systeme und Komponenten, verwendete Parameter und Prüfergebnisse. Der letzte Grundsatz ist die Zuverlässigkeit des transformierenden Systems, was durch die Benutzung von geprüften und zertifizierten Systemen erreicht werden kann.

1.8.3 Die Transformation als beweisrechtliches Problem

Die Transformation, unabhängig von ihrer Art, kann als Notwendigkeit und als Vorteil betrachtet werden. Wenn es aber der Wunsch ist, von allen praktischen Vorteilen der Transformation zu profitieren, und besonders von dem Vorteil, der sich aus dem Vernichten des Originals ergibt, muss sichergestellt werden, dass eventuelle Nachteile so weit wie möglich vermieden werden. Sollte das Zieldokument beispielsweise an Beweiswert verlieren, dann kann die Absicht eines Unternehmens, alle seine Papierdokumente ins Elektronische zu transformieren, vereitelt werden. Es stellt sich dann zunächst die Frage, was für einen Beweiswert das transformierte Dokument erlangen soll.

Erstens muss untersucht werden, ob schon vereinzelte Regelungen zur Transformation bestehen. Nach dem aktuellen Stand des deutschen Rechts sind lediglich Anforderungen an die Transformation durch spezielle Normen des unterschiedlichen Fachrechts vorgesehen. Die dazu gehörigen Beweisregeln fehlen.[620] So ist es z.B. im Handels- und Steuerrecht.[621] Nach § 257 Abs. 3 HGB und § 147 Abs. 2 AO wird die Möglichkeit gegeben, verschiedene handels- und steuerrechtlich relevante Unterlagen auf maschinenlesbaren Datenträgern zu speichern und die Originale zu vernichten. Gemäß § 110a Abs. 2 Satz 1 SGB IV können Sozialbehörde an Stelle der schriftlichen Unterlagen, eine Wiedergabe von diesen auf einem Bildträger oder auf anderen dauerhaften Datenträgern aufbewahren. Dabei sollen aber die Grundsätze der Wirtschaftlichkeit und Sparsamkeit sowie die Grundsätze ordnungsmäßiger Aufbewahrung beachtet werden.[622] Im Bereich der Justiz wird die Transformation im Rahmen der Führung elektronischer Prozessakten vorgesehen. Nach § 298a Abs. 1 Satz 2 ZPO bestimmen die Bundesregierung und Landesregierungen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Akten

620 *Roßnagel*/*Fischer-Dieskau*/*Wilke*, CR 2005, 904.

621 S. hierzu *Roßnagel*/*Fischer-Dieskau*/*Jandt*/*Knopp,* 2007, 72 f.

622 Zum Begriff der ordnungsmäßigen Aufbewahrung s. *Roßnagel*/*Fischer-Dieskau*/*Jandt*/*Knopp,* 2007, 41.

geführt werden können.[623] § 298a Abs. 2 Satz 1 ZPO regelt die Möglichkeit einer P-to-E-Transformation, indem die in Papierform eingereichten Schriftstücke und sonstige Unterlagen zur Ersetzung in ein elektronisches Dokument übertragen werden sollen. Dabei sind aber die Unterlagen, soweit sie in Papierform weiter benötigt werden, bis zum rechtskräftigen Abschluss des Verfahrens aufzubewahren (§ 298a Abs. 2 Satz 2). Wiederum öffnet § 298 Abs. 1 ZPO den Weg für die Transformation von einem elektronischen Dokument zum Papier. Der Ausdruck muss hierbei einen Vermerk enthalten, in dem eingetragen wird, welches Ergebnis die Integritätsprüfung des Dokuments ergab sowie wen die Signaturprüfung als Inhaber der Signatur und welchen Zeitpunkt sie für die Anbringung der Signatur ausweist. Im deutschen Zivilprozessrecht ist keine Regelung zur E-to-E Transformation vorgesehen.

Des Weiteren enthält § 33 VwVfG eine Regelung, die die drei verschiedenen Transformationsformen für die amtliche Beglaubigung von transformierten Dokumenten durch die Behörden zulässt. Dabei soll die jeweilige zuständige Behörde die Übereinstimmung zwischen Ausgangs- und Zieldokument überprüfen und dann einen Beglaubigungsvermerk für das Zieldokument erzeugen. Elektronische Ausgangsdokumente dürfen nur beglaubigt werden, wenn diese mit einer qualifizierten elektronischen Signatur versehen sind. Nach § 33 Abs. 5 VwVfG muss der Beglaubigungsvermerk außer der Feststellung, dass die beglaubigte Abschrift mit dem vorgelegten Schriftstück übereinstimmt, die Feststellungen enthalten, wen die Signaturprüfung als Inhaber der Signatur ausweist, welchen Zeitpunkt die Signaturprüfung für die Signaturprüfung ausweist und welche Zertifikate mit welchen Daten dieser Signatur zugrunde lagen. Schließlich enthält auch das Beurkundungsgesetz eine ähnliche Regelung in den §§ 39a, 42 Abs. 4. Dabei werden Notare ermächtigt, transformierte Dokumente zu beglaubigen. Weitere Anforderungen an den Beglaubigungsvermerk legt aber das Beurkundungsgesetz nicht fest. § 42 Abs. 4 BeurkG regelt lediglich, dass bei der Beglaubigung eines Ausdrucks eines elektronischen Dokuments, das mit einer qualifizierten elektronischen Signatur versehen ist, das Ergebnis der Signaturprüfung zu dokumentieren ist.

Was die medizinische Dokumentation anbelangt, müssen Ärzte laut § 10 Abs. 1 der Musterberufsordnung (MBO-Ä 1997) die von ihnen gemachten Feststellungen sowie alle getroffenen Maßnahmen dokumentieren. Die Dokumentation muss mindestens bis zu zehn Jahren nach Abschluss der Behandlung aufbewahrt werden. Die Aufbewahrung dient sowohl der Gedächtnisstütze des Arztes als auch dem Patienten, der damit Kenntnis über seinen Behandlungsverlauf erlangt. Der Dokumentation kommt überdies eine beweissichernde Funktion zu.[624] Gemäß § 10 Abs. 5 MBO-Ä 1997 kann die Dokumentation auch auf elektronischen Datenträgern oder anderen Speichermedien aufbewahrt werden, wenn besondere Sicherungs- und Schutzmaß-

623 Gemäß § 298a Abs. 1 Satz 3 ZPO können die Landesregierungen die Ermächtigungen zur Einführung der elektronischen Akten auf die Landesjustizverwaltungen übertragen; s. hierzu *Roßnagel*/*Fischer-Dieskau*/*Jandt*/*Knopp* 2007, 94 f.

624 *Roßnagel*/*Fischer-Dieskau*/*Jandt*/*Wilke* 2008, 74 f.

nahmen getroffen werden, damit ihre Veränderung, Vernichtung oder unrechtmäßige Verwendung verhindert wird. Eine Regelung, welche die ersetzende Transformation zulässt, enthält weder die MBO-Ä noch den Bundesmantelvertrag-Ärzte (BMV-Ä).

Die allgemeinen Beweisregelungen der ZPO ergänzen die Transformationsvorschriften. Was die beweisrechtliche Behandlung privat transformierter Dokumente betrifft, ist aber zu erwähnen, dass sie sich in keiner privilegierten Lage befinden. Laut § 420 ZPO müssen Privatdokumente immer im Original vorgelegt werden.[625] Die Beweisregel des § 416 ZPO – die den vollen Beweis der Authentizität des von Ausstellern unterschriebenen oder mittels notariell beglaubigten Handzeichens unterzeichneten Dokuments begründet – gilt nicht für die transformierten Dokumente. Sie unterliegen der freien Beweiswürdigung des § 286 Abs. 1 ZPO. Anders als die privaten Dokumente erlangen transformierte öffentliche Dokumente eine privilegierte Behandlung, da diese im Beweisverfahren gemäß § 435 ZPO[626] in der Regel ohne Beweisnachteile als Ersatz der Originaldokumente eingebracht werden können.[627]

Im Ergebnis ist festzustellen, dass die Regelungen des deutschen Rechts in Bezug auf die Transformation von Dokumenten und auf die Beweisführung mit dem Zieldokument zumindest für öffentliche Dokumente eine relative Rechtssicherheit für ihre Anwendung darstellt. Dabei wird zum einen die Inhaltstreue durch den Sichtvergleich des Ausgangs- und Zieldokuments seitens einer zuständigen Person gesichert. Zum anderen wird aber auch die Echtheit durch die Prüfung der Sicherungsmittel des Ausgangsdokuments vor der Transformation gewährleistet.[628] Letztlich besteht auch die Nachvollziehbarkeit des Zieldokuments, indem es einen Beglaubigungsvermerk enthält, welcher die wichtigsten Daten der Signatur bzw. Unterschrift dokumentiert. Werden die Originale eines öffentlichen Dokuments vernichtet, dann können die mittels der gesetzlichen vorgesehenen Transformationsverfahren resultierenden Zieldokumente einen hohen Beweiswert erlangen.

Die Literatur deutet aber einen Nachteil des Konzepts der vorliegenden Transformationsregelungen an, wonach die gesetzlichen Vorgaben zur Beglaubigung für die Transformation E-to-E und E-to-P unzureichend spezifiziert wären.[629] Dementsprechend bleiben manche Fragen hinsichtlich der Echtheit des Ausgangsdokuments offen. Es fehlen Angaben darüber, inwieweit die Zertifikatskette bis zur Wurzelinstanz überprüft werden muss. Die gesetzlichen Anforderungen legen auch nicht fest,

625 BGH, NJW-RR 1989, 1323.

626 § 435 ZPO bestimmt die Möglichkeit, die Vorlage einer öffentlichen Urkunde in Urschrift oder in einer beglaubigten Abschrift, vorausgesetzt dass die Beglaubigung die Erfordernisse einer öffentlichen Urkunde enthält. Das Gericht kann aber anordnen, dass der Beweisführer die Urschrift vorlege oder die Tatsachen angebe und glaubhaft mache, die ihn an der Vorlegung der Urschrift verhindern.

627 *Roßnagel*/*Fischer-Dieskau*/*Jandt*/*Wilke* 2008, 90.

628 *Roßnagel*/*Fischer-Dieskau*/*Wilke*, CR 2005, 905.

629 *Roßnagel*/*Fischer-Dieskau*/*Wilke*, CR 2005, 905.

ob Informationen zur Gültigkeit des Zertifikats über eine OCSP-Abfrage in den Transformationsvermerk einbezogen werden müssen. Dazu fehle noch die Anforderung an die verwendeten Algorithmen und Parameter der ursprünglichen Signatur in dem Zeitpunkt, zu dem die Transformation durchgeführt wurde. Alle diese Schwachstellen des Inhalts des Beglaubigungsvermerks hätten eine Auswirkung auf den Beweiswert des Zieldokuments, indem es geringer einzustufen sei als das Original, das eventuell vernichtet wurde.[630]

1.8.4 Das Transidoc-Konzept für die Transformation E-to-E

Um eine Lösung für solche Probleme zu finden und um mögliche Einwände gegen den Beweiswert des Zieldokuments zu vermeiden, entwickelte Transidoc besonders für die Transformation E-to-E ein Transformationsverfahren.[631] Dabei wird die elektronische Signatur des Ausgangsdokuments vor der Konvertierung geprüft und das Prüfergebnis in den Transformationsvermerk einbezogen. Die spätere Beurteilung der Integrität und Authentizität des Ausgangsdokuments wird durch ein dokumentiertes Prüfergebnis ermöglicht, das Angaben über die Zertifikatskette bis hin zur Wurzelinstanz enthält.[632] Außerdem wird die eingeholte OCSP-Antwort bezüglich dem Status des Nutzerzertifikats zum Zeitpunkt der Abfrage in den Transformationsbericht eingetragen. Die Transformation erfolgt in einem automatisierten Verfahren, was das menschliche Eingreifen bei der Konversion unmöglich macht. Geschützt wird das Transformationssystem zudem durch eine physische Zugangskontrolle. Es kann einen Netzangriff ebenso durch eine Firewall oder die Verwendung eines offline Systems verhindern. Zum Abschluss wird das Zieldokument einschließlich des Transformationsberichts nach der Transformation mit einer qualifizierten elektronischen Signatur gegen Verfälschungen gesichert.[633]

1.8.5 Das Problem der fehlenden Wirtschaftlichkeit der Transformation

Eine mögliche Hürde bei der Handhabung der transformierten Dokumente liegt in der Tatsache, dass das Transformationsverfahren des Verwaltungsverfahrensgesetzes und des Beurkundungsgesetzes eine Vergleichsprüfung voraussetzt. Das bedeutet, dass bei jedem einzelnen Beglaubigungsvermerk eine zuständige Person mitzuwirken hat. Dadurch ist eine wirtschaftliche Transformation von großen Mengen an Dokumenten praktisch ausgeschlossen. Ein automatisiertes Verfahren wäre mit den Anforderungen der amtlichen oder öffentlichen Beglaubigung aber nicht vereinbar.

630 *Roßnagel*/*Fischer-Dieskau*/*Wilke*, CR 2005, 905.

631 *Wilke*/*Jandt*/*Löwe*/*Roßnagel*, CR 2008, 609.

632 *Wilke*/*Jandt*/*Löwe*/*Roßnagel*, CR 2008, 609.

633 *Wilke*/*Jandt*/*Löwe*/*Roßnagel*, CR 2008, 609.

Um die Vorteile der Transformation in vollem Umfang zu ermöglichen, das heißt, ohne einen Beweiswertverlust, aber gleichzeitig mit Blick auf die Möglichkeit ihrer rechtssicheren massenhafte Gestaltung, wird daher eine Lösung benötig, die sowohl Beglaubigung als auch Automatisierung in Betracht zieht. Die Übereinstimmungsprüfung zwischen Ausgangs- und Zieldokument soll zu diesem Zwecke von der Sichtprüfung durch ein geprüftes technisches Transformationssystem ersetzt werden, das alle Anforderungen einer ordnungsgemäßen Transformation berücksichtigt.[634] Ein solches System muss mit einem Prüfprogramm für die Beglaubigung kombiniert werden, das alle erforderlichen Angaben in den Vermerk mit einbezieht.

1.8.6 Das Problem der Transformation P-to-E

Werden von außen Dokumente in Papierform an eine Behörde oder an ein Unternehmen gerichtet, welches die Dokumentation durchgängig elektronisch verarbeitet und aufbewahrt, dann kann es zu Medienbrüchen kommen. Um das zu vermeiden, besteht die Möglichkeit der P-to-E Transformation, indem sowohl die einkommenden als auch die schon abgelagerte Papierdokumente gescannt oder in digitale Textdokumente umgewandelt werden.[635]

Die Tatsache aber, dass bei der Konvertierung von Papierurkunden in elektronische Dokumente die Sicherheitsmerkmale des Papierdokuments verloren gehen, ist ein zentrales Problem dieser Transformationsart, wenn es das Ziel der Umwandlung ist, die Papieroriginale zu vernichten. Es ist zwar zu erwähnen, dass es bei den Fällen, in denen keine gesetzlichen oder vertraglichen Dokumentations-, Aktenführungs- oder Aufbewahrungspflichten bestehen, natürlich gestattet ist, das Ursprungsdokument aus Papier zu scannen und danach zu vernichten.[636] Besteht aber aufgrund des Gesetzes oder des Vertrages eine solche Pflicht, dann sollte das Unternehmen oder die Behörde die Originale nicht vernichten. Da, wie schon erwähnt, nach § 420 ZPO die Urschrift einer Urkunde dem Gericht vorgelegt werden muss, unterliegen gescannte Dokumente nicht dem Urkundsbeweis sondern der freien Beweiswürdigung des § 286 Abs. 1 ZPO. Eine Ausnahme dafür gilt nur in zwei Fällen.[637]

Eine erste Ausnahme gilt für den Fall, bei dem der Beweisgegner nach § 427 ZPO der Anordnung des Gerichts, eine Urkunde vorzulegen, nicht nachkommt. Dann kann die vom Beweisführer beigebrachte Abschrift der Urkunde als richtig angesehen werden, das heißt, die Behauptungen des Beweisführers über die Beschaffenheit und den Inhalt der Urkunde können als bewiesen angenommen werden. In dem Zusammenhang kann der Ausdruck des gescannten Dokuments als Abschrift be-

634 *Roßnagel*/*Fischer-Dieskau*/*Wilke*, CR 2005, 908.

635 *Roßnagel*/*Wilke*, NJW 2006, 2145.

636 *Roßnagel*/*Wilke*, NJW 2006, 2146.

637 *Roßnagel*/*Wilke*, NJW 2006, 2148.

trachtet werden, da für die Abschrift das Verfahren ihrer Erzeugung, wie etwa durch das mechanische Kopieren oder durch das Scannen, irrelevant ist.[638]

Eine zweite Ausnahme gilt für die öffentlichen Dokumente, angesichts der Bestimmung des § 435, wonach eine öffentliche Urkunde sowohl in Urschrift als auch in einer beglaubigten Abschrift, die hinsichtlich der Beglaubigung die Erfordernisse einer öffentlichen Urkunde an sich trägt, vorgelegt werden kann. Sollten aber dem Gericht Bedenken gegen die Richtigkeit der beglaubigten Abschrift kommen, kann es anordnen, dass der Beweisführer die Urschrift vorlegt oder die Tatsachen angibt und glaubhaft macht, die ihn an der Vorlegung der Urschrift hindern. Kommt dem Gericht nach der Anordnung keine Klarheit, dann entscheidet es nach freier Überzeugung über den Beweiswert der Abschrift. Den elektronischen Dokumenten, die durch das Scannen gemäß § 33 Abs. 4 Nr. 4a VwVfG und § 39a BeurkG erzeugt werden, kommt nach §§ 371a Abs.2 Satz 1, 435 ZPO der Beweiswert einer Originalurkunde zu.[639]

Kommen aber keine der erwähnten Ausnahmen in Betracht, dann unterliegt das gescannte Dokument der freien Beweiswürdigung des § 286 Abs. 1 ZPO. Soll das gescannte Dokument im Lauf des Transformationsverfahrens qualifiziert elektronisch signiert werden, hilft diese Signatur aber kaum, was den Beweiswert des Dokuments betrifft. Diese im gescannten Zieldokument enthaltene elektronische Signatur ersetzt nicht die Unterschrift des Ausgangsdokuments. Vielmehr dient diese lediglich als künftiger Integritätsschutz des Dokuments, denn das Ursprungsdokument enthält in der Regel Unterschriften, die eine andere Person oder andere Personen zu einem früheren Zeitpunkt abgegeben hat, bzw. haben, und die Transformation führt immer zum Verlust der Echtheitsprüfbarkeit des Ausgangsdokuments. Somit gilt die Beweiserleichterung des § 371a Abs. 1 Satz 2 ZPO nicht für das qualifiziert elektronische signierte gescannte Dokument. Diese erstreckt sich nur auf die Echtheit der elektronisch signierten Übereinstimmungserklärung des Transformationsvermerks.[640]

1.8.7 Notwendigkeit einer Beweisregelung?

In der aktuellen Lage des elektronischen Verwaltungs- und Geschäftsverkehrs gewinnt die Digitalisierung von Dokumenten immer mehr an Bedeutung. Noch interessanter ist die Transformation, wenn gleichzeitig die Papieroriginale vernichtet werden dürfen. Damit aber dieses praktische Bedürfnis erfüllt wird, benötigt das Beweisrecht neue Regelungen, die die Zulässigkeit des ersetzenden Scannens vorsehen. Das Scannverfahren muss auf technisch-organisatorischen Konzepten basieren.

638 *Winkler* 2003, § 42 Rn. 6.

639 *Roßnagel*/*Wilke*, NJW 2006, 2148.

640 *Roßnagel*/*Wilke*, NJW 2006, 2148; *Roßnagel*/*Fischer-Dieskau*/*Jandt*/*Wilke* 2008, 91.

Diese werden in Deutschland beispielsweise vom Informatikzentrum des Landes Niedersachsen und dem schon erwähnten Forschungsprojekt Transidoc entwickelt.

Denkbar wäre auch die gesetzliche Festlegung von Anforderungen an die Funktionalität und an die Sicherheit von automatisierten technischen Transformationssystemen. Problematisch ist in diesem Zusammenhang jedoch, dass mit der Umwandlung des Papiers in digitale Daten und der Vernichtung der Papierurkunde, die Möglichkeit der Feststellung der Authentizität der Unterschrift auf dem Scannprodukt verloren geht.[641] Durch den Einsatz qualifizierter Signaturen wird nur die vom Papierdokument erfüllte Anforderung der Integrität gewährleistet. Eine Beweisregelung für Scannprodukte würde somit angesichts des derzeitigen Stands der Technik keine sichere technisch-organisatorische Basis und Rechtfertigung finden.[642] Die Studie Transidoc ist zudem zu dem Ergebnis gekommen, dass die freie Beweiswürdigung durch den Einsatz geeigneter technisch-organisatorischer Maßnahmen im Scannverfahren ausreichen kann.

1.9 Die Fremderzeugung von elektronischen Signaturen

Unter Fremderzeugung von elektronischen Signaturen versteht man die Auslagerung der Signaturerzeugung durch den Signaturschlüssel-Inhaber an einen Dienstleister.[643] Eine solche Delegierung kann aus Gründen der Bequemlichkeit oder Rationalisierung der Ausführung von Geschäftsprozessen von Behörden oder Unternehmen stattfinden. Ein Beispiel dafür wäre die Auslagerung bei der Erstellung elektronischer Rechnungen.[644] Die Signaturauslagerung kann grundsätzlich in zwei verschiedenen Formen erfolgen: Durch das Fremdsignierungsmodell und durch das Vertretungsmodell.[645] Fraglich ist, ob beide zu qualifizierten elektronischen Signaturen führen, für die die Beweiserleichterung des § 371a Abs. 1 Satz 2 ZPO gilt.

1.9.1 Fremderzeugung durch das Fremdsignierungsmodell

Bei diesem Modell erzeugt der Dienstleister Signaturen anhand der Signaturerstellungseinheit, PIN und Zertifikat des Auftraggebers. Der Dokumentempfänger er-

641 *Roßnagel*/*Fischer-Dieskau*/*Jandt*/*Wilke* 2008, 117.

642 *Roßnagel*/*Fischer-Dieskau*/*Jandt*/*Wilke* 2008, 119; *Wilke*/*Jandt*/*Löwe*/*Roßnagel*, CR 2008, 612.

643 Der Begriff ist aus *Roßnagel*, MMR 2008, 23 herzuleiten.

644 Rechnungen sind laut § 14 Abs. 1 Satz 2 UStG auf Papier oder – sofern der Empfänger zustimmt – auf elektronischem Weg zu übermitteln. Werden Rechnungen elektronisch übermittelt, müssen sie nach § 14 Abs. 3 UStG eine qualifizierte elektronische Signatur tragen.

645 So *Roßnagel*, MMR 2008, 23.

kennt aber bei dieser Variante nicht, dass der Zertifikatsinhaber nicht selbst, sondern in seinem Namen ein Dritter die Daten signiert. Das Rechtsverhältnis zwischen Auftraggeber und Dienstleister wird durch einen Vertrag geregelt.

Argumentiert wird aber, dass die im Rahmen des Fremdsignierungsmodells erzeugten Signaturen nicht den Begriff der qualifizierten Signatur des SigG erfüllen.[646] Das ergibt sich aus der Tatsache, dass beim Fremdsignierungsmodell der Signaturschlüssel-Inhaber nicht in der Lage ist, Signaturen zu erzeugen, mit Mitteln, die unter seiner alleinigen Kontrolle gehalten werden können, wie § 2 Nr. 2 c) SigG bestimmt. Beim Fremdsignierungsmodell kann der Signaturschlüssel-Inhaber nicht seine eigene Signaturerstellungseinheit vor unbefugter Nutzung schützen. Darüber hinaus gehört zum gesamten Sicherheitskonzept des Signaturrechts, dass die Signaturerstellungseinheit erst nach der Identifikation des Inhabers durch Besitz und Wissen angewendet werden kann (§ 15 Abs. 1 SigV). Diese technische Regel ergänzt die Regelungen des § 5 Abs. 6 SigG und § 5 Abs. 2 SigV, wonach der Signaturschlüssel-Inhaber die tatsächliche unmittelbare Sachherrschaft über seine sichere Signaturkarte und ausschließlich allein über die Wissensdaten verfügen soll.[647]

Da gemäß § 126a Abs. 1 BGB eine qualifizierte Signatur mit der handschriftlichen Unterschrift rechtlich gleichgestellt wird, sollte das Fremdsignierungsmodell auch die Funktionen der Letzteren gewährleisten.[648] Das ist aber zweifelhaft bei wenigstens vier Funktionen der eigenhändigen Unterschrift.[649] Die Identitätsfunktion wird gefährdet, indem nicht mehr gewährleistet wird, dass die Person des tatsächlich Signierenden mit der des Signaturschlüssel-Inhabers übereinstimmt. Die Echtheitsfunktion ist auch nicht gegeben, da allein aus der Signatur nicht geschlossen werden kann, dass die signierten Daten tatsächlich vom Signaturschlüssel-Inhaber herrühren und nicht nachträglich verändert worden sind. Auch die Beweisfunktion wäre im Fremdsignierungsmodell beeinträchtig, da sie sich aus der Identitäts- und Echtheitsfunktion ergibt. Hierbei muss der Empfänger der signierten Daten durch andere Beweismittel als die Signatur allein beweisen, dass mit Wissen und Wollen des Signaturschlüsselinhabers tatsächlich signiert worden ist.[650] Schließlich ist auch die Erfüllung der Warnfunktion angesichts des mangelnden Bewusstseins des Zertifikatsinhabers bei der Signierung problematisch. Ohne den Begriff der qualifizierten elektronischen Signatur und die Funktionen einer eigenhändigen Unterschrift zu erfüllen[651], wird dem Fremdsignierungsmodell infolgedessen sowohl die Beweiser-

646 *Roßnagel*, MMR 2008, 28.

647 *Roßnagel*, MMR 2008, 28.

648 Zu der Funktionsäquivalenz der qualifizierten elektronischen Signatur siehe bereits in diesem Teil Gliederungspunkt 1.6.4.1.1.

649 *Roßnagel*, MMR 2008, 25.

650 *Roßnagel*, MMR 2008, 26.

651 Die Bundesnetzagentur warnt davor, dass das Fremdsignierungsmodell den Sinn des Signaturgesetzes widerspricht: „Keinesfalls im Sinne der Rechtsfiktion des Signaturgesetzes (Besitz plus Wissen äquivalent zu Unterschrift) ist es deshalb z.B., wenn der Inhaber einer Signa-

leichterung des § 371a ZPO als auch die elektronische Form des § 126a Abs. 1 BGB nicht zuerkannt.

1.9.2 Fremderzeugung durch das Vertretungsmodell

Durch das Vertretungsmodell signiert der Dienstleister die elektronischen Dokumente des Auftraggebers auf Basis einer Vollmacht und verwendet dabei seine eigene Signaturerstellungseinheit, PIN und Zertifikat. Dem Signaturempfänger wird somit klar, dass der Dienstleister die Willenserklärung im Auftrag des Auftraggebers abgibt. Die Transparenz ist somit gewährleistet. Auf diese Weise – ohne Weitergabe von Signaturkarte und PIN – bleibt der konstitutive Begriff der qualifizierten elektronischen Signatur des § 2 Nr. 2 c) SigG und die Möglichkeit der Anwendung des § 371a ZPO erhalten.[652]

1.10 Automatisiert erzeugte elektronische Signaturen

So wie bei der Fremdsignierung dient die Automatisierung der Signaturerzeugung der Rationalisierung und Effizienzsteigerung unterschiedlicher Geschäftsbereiche. Insbesondere in den Bereichen, in denen die Prozesse völlig automatisiert laufen und viele gleichartige Dokumente elektronisch signiert werden müssen, ist man auf die automatische Erzeugung von elektronischen Signaturen angewiesen. Die Massensignaturen werden zudem als ein wichtiges Mittel zur flächendeckenden Verbreitung elektronischer Signaturen betrachtet.[653]

Die automatisierte elektronische Signatur wird von einem automatischen Prozess ohne Zutun eines Menschen erzeugt.[654] Wichtig in diesem Begriff ist, dass ein Mensch zwar den Prozess bewusst anstößt, aber weder im Einzelfall vor der Signatur die zu signierenden Daten überprüft noch den privaten Schlüssel aktiviert.[655] Fraglich ist, ob mit diesen Eigenschaften die automatisierte elektronische Signatur den Begriff der qualifizierten elektronischen Signatur erfüllt und ob für automatisierte Signaturen die Beweiserleichterung des § 371a ZPO in Anspruch genommen werden kann. Besonders aufgrund der Tatsache, dass das ursprüngliche Konzept des Signaturgesetzes vom Ideal des Signaturschlüssel-Inhabers ausgeht, der als natürli-

turkarte diese – incl. Dazugehöriger PIN – an einen geschäftsmäßigen „Rechnungssteller" abgibt, damit dieser in seinem Namen Rechnungen signiert", www.bundesnetzagentur.de → Elektronische Signatur → FAQ → Frage 18.

652 Zur Beschreibung des Vertretungsmodells im Fall der elektronischen Rechnungserstellung siehe *Roßnagel*, BB 2007, 1237.

653 *Schröder*, DuD 2004, 665.

654 *Roßnagel*/*Fischer-Dieskau*, MMR 2004, 133.

655 *Roßnagel*/*Fischer-Dieskau*, MMR 2004, 133.

che Person jedes Mal anhand seiner sicheren Signaturkarte und der zugehörigen Wissensdaten seine Signaturen erzeugt.[656]

Bereits die vier Voraussetzungen der fortgeschrittenen elektronischen Signatur werden von der automatisierten elektronischen Signatur erfüllt. Die ausschließliche Zuordnung zum Signaturschlüssel-Inhaber (§ 2 Nr. 2 a) SigG) ergibt sich aus der personalisierten und in seinem alleinigen Besitz befindliche Signaturerstellungseinheit sowie aus dem auf seine Person ausgestellte Zertifikat.[657] Hierbei ist auch zu beachten, dass sich der Bezug zu einer natürlichen Person im Signaturgesetz auf die Zuordnung des Zertifikats und nicht auf die Erzeugung der Signatur bezieht. Dass eine Signatur immer nur durch natürliche Personen und nicht von automatischen Prozessen zu erzeugen ist, kann nicht aus dem Signaturgesetz hergeleitet werden.[658] Die Identifizierung des Signaturschlüssel-Inhabers (§ 2 Nr. 2 b) SigG) wird ebenfalls mittels der Zuordnung des Zertifikats zu seiner Person ermöglicht. Die alleinige Kontrolle der Mittel zur Erzeugung der Signatur (§ 2 Nr. 2 c) SigG) wird durch den Schutz der Signaturerstellungseinheit seitens des Signaturschlüssel-Inhabers erfüllt. Geeignete asymmetrische Kryptographieverfahren gewährleisten die Erfüllung des letzten Definitionsmerkmals einer fortgeschrittenen Signatur, nämlich die Erkennung der nachträglichen Veränderung der Daten (§ 2 Nr. 2 d) SigG).

Zu diesen vier Anforderungen kommen noch die zwei zusätzlichen Definitionsmerkmale der qualifizierten elektronischen Signatur, nämlich, dass die elektronische Signatur auf einem zum Zeitpunkt ihrer Erzeugung gültigen Zertifikat beruht und dass sie mit einer sicheren Signaturerstellungseinheit erzeugt wird. Was die sichere Signaturerstellungseinheit angeht, bestimmt § 15 Abs. 1 Satz 1 SigV, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen zur Anwendung kommen kann. Offen bleibt es, ob diese Identifikation immer wieder vor der einzelnen Signaturerzeugung zu erfolgen hat. Da weder SigG noch SigV dieses verlangen, darf davon ausgegangen werden, dass die Wissensdaten nicht immer bei jedem einzelnen Signaturvorgang einzugeben sind.

Erforderlich ist aber nach § 15 Abs. 2 Nr. 1 c) SigV, dass Signaturanwendungskomponenten die Erzeugung einer[659] Signatur vorher eindeutig anzeigen. Eine Anzeige wird somit nur vor dem In-Gang-Setzen des Signaturerzeugungsprozesses erforderlich.[660]

656 *Roßnagel*, MMR 2008, 23.

657 *Roßnagel*/*Fischer-Dieskau*, MMR 2004, 133.

658 *Roßnagel*/*Fischer-Dieskau*, MMR 2004, 135.

659 Zu der Verordnungsformulierung „einer" wird von *Roßnagel*/*Fischer-Dieskau*, MMR 2004, 137, darauf hingewiesen, dass die Anzeige nicht vor „jeder" Signierung erfolgen muss. Hätte der Verordnungsgeber das gewollt, dann würde er anstelle des unbestimmten Artikels „einer" die präzise Bestimmung „jeder" verwenden.

660 *Roßnagel*/*Fischer-Dieskau*, MMR 2004, 137.

Dass elektronische Signaturen automatisch erzeugt werden können, wird ebenfalls von der Bundesnetzagentur bestätigt.[661] Dabei stellt die Aufsichtsbehörde aber klar, dass immer ein besonderer Schutz gegen Missbrauch des Signaturschlüssels implementiert werden muss. Vorgeschlagen wird die Einrichtung von Zeitfenstern, in denen alle abzusendenden Dokumente durch eine einmalige PIN-Eingabe signiert werden. Ein Zeitraum wie etwa eine Stunde kann festgelegt werden, während dessen die PIN aktiviert bleibt. Die Einrichtung von Zeitfenstern zur Signaturerzeugung und somit die Zulässigkeit automatisierter Verfahren wird auch von der amtlichen Begründung zur Signaturverordnung vorgesehen.[662]

Mit diesem Ergebnis ist die automatisierte erzeugte Signatur unter Beachtung bestimmter Anforderungen grundsätzlich zulässig.[663] Dies wird sowohl von Literatur als auch von der Bundesnetzagentur und amtlicher Begründung der Signaturverordnung bestätigt. Obwohl das Signaturgesetz ursprünglich für die einzelne Signatur konzipiert wurde, stellt die automatisch erstellte Signatur mit besonderem Schutz gegen Missbrauch kein Verstoß gegen den Begriff der qualifizierten Signatur dar. Daher sollen es keine Komplikationen bei der Beweisführung mittels automatisierter Signaturen geben. Nach § 371a Abs. 1 Satz 2 ZPO muss der Beweisgegner Tatsachen vortragen, die ernstliche Zweifel daran begründen, dass er die Erklärung abgegeben hat. Die bloße Behauptung, das Dokument sei nach der Initiierung des Prozesses gegen seinen Willen signiert worden, wird wahrscheinlich nicht ohne weiteres vom Gericht angenommen werden.

Der Systematik weiter folgend endigt an dieser Stelle die Darstellung der deutschen Situation und die Arbeit widmet sich der Sicht des brasilianischen Systems.

661 Siehe hierzu www.bundesnetzagentur.de → Elektronische Signatur → FAQ → Frage 18.

662 Gemäß der Begründung zu § 15 Abs. 1 SigV: „Sichere Signaturanwendungskomponenten können so gestaltet werden, dass optional vor jeder Signatur, nach einer zuvor festgelegten Anzahl von Signaturen oder nach bestimmtem Zeitablauf bei Nichtbenutzung der Signaturerstellungseinheit, die Identifikationsdaten erneut eingegeben werden müssen.“ Weiter in der Begründung zu § 15 Abs. 2 SigV wird die automatisierte Signatur explizit anerkannt: „Insbesondere bei der automatischen Erzeugung von Signaturen („Massensignaturen“) muss sichergestellt sein, dass Signaturen nur zu dem voreingestellten Zweck (z.B. Signaturen zu Zahlungsanweisungen bei Großanwendern) und durch eine zuvor geprüfte und abgenommene Anwendung vorgenommen werden können“.

663 Ausgeschlossen wäre die automatisierte Signatur, wo eine gesetzliche Anforderung zum persönlichen Tätigwerden zu Bestätigunszwecke verlangt wird, wie etwa bei der Bestätigung der Korrektheit einer Transformation P-to-E (§ 110a –d SGB IV und § 33 Abs. 4 VwVfG) oder bei einer Transformation E-to-E (§ 33 Abs. 4 VwVfG); siehe hierzu *Roßnagel*/*Fischer-Dieskau*, MMR 2004, 138.

2. Das brasilianische Beweisrecht und das elektronische Dokument

Die Verbindung zwischen der technisch-organisatorischen Infrastruktur für öffentliche Schlüssel und dem Beweisrecht wird durch zwei Vorschriften der Medida Provisória Nr. 2.200-2 geschaffen. Diese sind die §§ 1 und 2 MP 2.200-2, welche über die beweisrechtliche Behandlung der akkreditiert signierten Dokumente (§ 1 MP 2.200-2) und der sonstigen elektronischen Dokumente (§ 2 MP 2.200-2) bestimmen. Diese Regelungen schaffen jedoch keine neue vollständige beweisrechtliche Systematik, sondern müssen im Zusammenhang der bereits existierenden Vorschriften ausgelegt und angewandt werden. Ein Beispiel dafür ist § 1 MP 2.200-2, der auf Art. 131 des alten Código Civil verweist.

Bevor die Beweisvorschriften der Medida Provisória Nr. 2.200-2 im Einzelnen untersucht werden können, ist eine Darstellung einiger für die vorliegende Arbeit relevanter beweisrechtlicher Begriffe erforderlich.

2.1 Beweisrecht: Materielles oder formelles Recht?

Das Thema Beweisrecht wird im brasilianischen Recht nicht nur vom Zivilprozessrecht, sondern auch im Código Civil behandelt.[664] Der Ansatz hat historische Gründe, denn bei der Verabschiedung des Código Civil im Jahr 1916 gab es keine einheitliche, landesweite Zivilprozessordnung, vielmehr galten in jedem Bundesland unterschiedliche Regulierungen zum Prozessrecht. Das motivierte den Gesetzgeber dazu, eine minimale Regulierung des Beweisrechts durch das Código Civil zu etablieren, um ein gewisses Maß an Rechtssicherheit innerhalb des Landes zu schaffen.[665]

Trotz der Durchsetzung des Ansatzes dieser Variante einer gemischten Behandlung des Beweisrechts, wird besonders von zivilprozessrechtlichen Autoren Kritik in Bezug auf die Platzierung der beweisrechtlichen Regelungen im Código Civil geübt. Sie argumentieren, das Beweisrecht sei ein Thema, welches ausschließlich der Zivilprozessordnung angehöre.[666] Nach dieser Auffassung solle sich das materielle Recht nur auf die Regelung der Form von Willenserklärungen beschränken und den Rest dem Zivilprozessrecht überlassen.[667]

Eine Doppelbehandlung der Materie stützt sich jedoch nicht allein auf den Gedanken, dass der Adressat des Beweises lediglich ein Richter sei, sondern berücksichtigt vielmehr auch Vertragspartner oder Dritte. Im Beispiel von *Pontes de Miranda* ist dazu erwähnt, dass der Erbe die Erblasserschulden bei Vorlage der ent-

664 Einem vergleichbaren Ansatz wird im französischen, italienischen und portugiesischen Recht gefolgt, hierzu: *Barbosa Moreira* 2002, 189.

665 *Couto e Silva* 1979, 135.

666 *Dinamarco* 2005 46; *Moniz de Aragão* 2004, 11 ff.; *Barbosa Moreira* 2005, 97 ff.

667 *Barbosa Moreira* 2005, 45.

sprechenden Nachweise bezahlt.[668] Ebenso wird das mittlerweile veraltete Beispiel des Kaufmannes angebracht, welcher angesichts einer zu großen Geschäftsmenge von Geschäftspartnern diese immer auffordert, die Vorlage der Rechnungen mit den dazu gehörigen Nachweisen zu erbringen, um die Zahlungen gegebenenfalls durchzuführen.[669] Die Diskussion sei dahingehend unzutreffend, würde man den Beweis nur auf den Prozess reduzieren, denn der Beweis diene nicht nur der Überzeugung des Gerichts.[670]

Außerdem gelänge dem Verteidiger der ausschließlichen prozessualen Behandlung des Beweises nicht zu erklären, weshalb die Beweisregeln nur dem formellen Recht angehören können. Dies zeige sich besonders im Falle der prozessualen Regelungen auf gegenwärtige, noch nicht abgeschlossene Gerichtsverfahren, welche sofort nach in Kraft treten für die Zukunft einwirken und damit zugleich eventuell die Rechtsposition einer der Parteien beeinträchtigen könnten.[671] Dies wäre möglich, wenn etwa ein Beweismittel infolge eines neuen Gesetzes abgeschafft würde und damit die Chancen der Partei, ihr zugrunde liegendes behauptetes Recht durchzusetzen, erschwert würde.

Diese Doppelbehandlung ist im neuen Código Civil beibehalten worden. Es ist somit nicht zu verkennen – wie *Pontes de Miranda* zu Recht hinweist – , dass das Beweismaterial nicht nur der Überzeugungsbildung des Gerichts dient. Auch Vertragsparteien überzeugen sich anhand von Beweisen, die von ihren Vertragspartnern in den üblichen Geschäftsbeziehungen vorgebracht werden.

2.2 Beweismittel

Der brasilianische Código de Processo Civil (CPC) sieht sieben verschiedene Beweismittel vor[672], nämlich Parteivernehmung, Anerkenntnis, Vorlegung einer Urkunde oder Sache, Urkundenbeweis, Zeugenbeweis, Sachverständigenbeweis und richterlicher Augenschein. Trotz der Kodifizierung dieser Beweismittel, handelt es sich hier nicht um den Ansatz des Strengbeweises. Gemäß Art. 332 Código de Processo Civil sind alle rechtlichen als auch moralisch legitimierten Mittel zulässig, um die Wahrheit der behaupteten Tatsachen nachzuweisen. Selbst dann, wenn diese nicht im Código de Processo Civil festgesetzt sind. Gestattet werden somit die so genannten „provas atípicas“, das heißt Beweismittel, welche nicht ausdrücklich auf der Liste der Beweismittel vorgesehen sind. Beispiele für diese nicht gesetzlich vorgesehenen Beweismittel sind die „provas emprestadas“. Dies ist ein Beweis, der entweder von einem anderen Gericht oder durch die Polizei oder eine Finanzbehörde

668 *Pontes de Miranda* 2000, 451.
669 *Pontes de Miranda* 2000, 451.
670 *Pontes de Miranda* 2000, 451.
671 *Moreira Alves* 2003, 194.
672 Art. 332 bis Art. 443.

erhoben wurde und vom Beweisführer vorgelegt werden darf.[673] Zu den „provas emprestadas" gehören auch die Feststellungen, die vom Gerichtsvollzieher im Rahmen seiner Tätigkeiten protokolliert werden.[674] Der Código Civil zählt wiederum auch die möglichen Beweismittel der rechtserzeugenden Tatsachen in Art. 212 auf: Anerkenntnis, Urkunde, Zeuge, Vermutung und Begutachtung. Von den erwähnten Beweismitteln werden in dieser Arbeit nur die Vermutungen und der Urkundenbeweis untersucht, da nur diese den Gegenstand berühren.

2.2.1 Gesetzliche Vermutungen

Die Rede von gesetzlichen Vermutungen ist immer dann gegeben, wenn kraft eines Gesetzes bei Vorliegen von bestimmten Gegebenheiten von weiteren Gegebenheiten auszugehen ist. Die Einordnung der Vermutungen in die Aufzählung der Beweismittel des Zivilgesetzbuches stößt in der brasilianischen Literatur auf Kritik. *Barbosa Moreira* behauptet die Vermutung sei kein Beweismittel, wie das Zivilgesetzbuch bestimmt, sondern es handele sich um einen im brasilianischen Recht so genannten indirekten Beweis.[675] Im Rahmen dieser Arbeit bleibt aber die Diskussion über die rechtsdogmatische Einordnung von Vermutungen dahingestellt.

Im brasilianischen Recht existieren die gesetzlichen Vermutungen *juris tantum* und die Vermutungen *juris et de jure*. Es wird in der Literatur auf eine Abstufung der Vermutungen nach ihrer Beweiskraft hingewiesen: die stärksten seien die Vermutungen *juris et de jure* und die schwächeren die Vermutungen *juris tantum*.[676]

2.2.1.1 Vermutungen *juris et de jure*

Gegen eine Vermutung *juris et de jure* hat der Beweisgegner keine Möglichkeit, einen Gegenbeweis beizubringen. Es handelt sich um unwiderlegliche Rechtsvor-

673 Die „provas emprestadas" dürfen von einem Gericht im Ganzen angenommen werden, unter der Voraussetzung, dass das rechtliche Gehör der gegenseitigen Partei über den Inhalt des erbrachten Beweises gewährleistet wird. Siehe z.B. STF, HC 72295, Rel. Min. *Octávio Gallotti*, v. 27.10.1995.

674 *Dinamarco* 2005, 95.

675 In der brasilianischen Literatur wird, beeinflusst von der italienischen rechtsprozessualen Lehre, der Beweis nach direktem und indirektem Beweis gruppiert. Der direkte Beweis bezieht sich unmittelbar auf die zu beweisende Tatsache: Beispiel hierfür ist der Zeuge, der eine Autokollision gesehen hat. Der gleiche Zeuge kann in Bezug auf denselben Unfall auch als indirekter Beweis betrachtet werden, wenn er den Unfall nicht gesehen hat, sondern erst kurz nach dem Ereignis beim Unfallort vorbeigefahren ist. Siehe hierzu *Silva* 1998, 340; *Dinamarco* 2005, 89; *Giannico* 2005, 102.

676 *Alvim* 2001, 596.

schriften, die grundsätzlich auf Tatbestände des materiellen Rechts angewiesen sind.[677] Beispiel dafür ist die Gläubigerbenachteiligung, die vermutet wird, wenn der Konkursschuldner eine Sicherung gewährt (Art. 163 CC). *Cândido Dinamarco* weist darauf hin, dass die Vermutungen *juris et de jure* auch im Zivilprozessrecht zu finden sind, wie im Fall des Art. 12, § 3 CPC, welcher die Vermutung artikuliert, dass der Geschäftsführer einer ausländischen juristischen Person die Vertretungsmacht für den Empfang einer Vorladung zum Prozess besitze.[678]

2.2.1.2 Vermutungen *juris tantum*

Eine Vermutung *juris tantum* kann grundsätzlich angegriffen werden, das heißt, anders als bei einer Vermutung *juris et de jure* hat der Gegner hier die Möglichkeit, die Vermutungsbasis zu erschüttern. Das ist etwa der Fall des Art. 8 CC, wonach, falls zwei oder mehrere Personen beim selben Ereignis ableben und nicht festgestellt werden kann, dass einer der Mitverstorbenen vor den anderen dahingeschieden ist, vermutet wird, dass sie gleichzeitig verstorben seien. Bei der Feststellung der Erbfähigkeit eines Erbens kann jedoch als Beweis entscheidend sein, dass tatsächlich eine Person vor der anderen Person verstorben ist, was durch die widerlegliche Vermutung des Art. 8 CC als zulässig angesehen würde.

Nach herrschender Meinung[679] führe die Vermutung *juris tantum* in den häufigsten Fällen zu einer Beweislastumkehr. Dies wird von der Rechtsprechung bestätigt.[680]

2.2.2 Öffentliche Urkunde

Art. 364 des CPC regelt die Beweiskraft der öffentlichen Urkunde, indem er bestimmt, dass die öffentliche Urkunde sowohl ihr Ausstellen als auch die Tatsachen beweist, welche eine öffentliche Behörde oder eine mit öffentlichem Glauben versehene Person in ihr erklärt. Darauf gründet eine Vermutung der Wahrhaftigkeit der

677 *Dinamarco* 2005, 117; *Leonardo* 2004, 243.

678 *Dinamarco* 2005, 118.

679 *Barbosa Moreira* 1988, 43; *Alvim* 2001, 599; *Greco* 2004, 193; *Dinamarco* 2005, 119; a.A. *Leonardo* 2004, 241 ff.

680 Siehe z.B. STJ, AgRg in REsp 856.856-RJ, Rel. Min. *Humberto Martins*, v. 05.6.2007; TARS, Ap. Cível 185005113, Rel. *Lio Cezar Schmitt*, v. 26.2.1985; TARS, Ap. Cível 185068319, Rel. *Sílvio Manoel de Castro Gamborgi*, v. 19.3.1986; TARS, Ap. Cível 185005113, Rel. *Lio Cezar Schmitt*, v. 26.2.1985; TARS, Ap. Cível 196201412, Rel. *Roberto Expedito da Cunha Madrid*, v. 23.1.1997; TARS, Ap. Cível 198078495, Rel. *Ulderico Ceccato*, v. 22.10.1998.

Tatsachen, die vom Aussteller der öffentlichen Urkunde abgegeben werden.[681] Der öffentlichen Urkunde kommt zusätzlich noch die Vermutung der Echtheit *juris tantum* zu, welche durch einen konkreten Beweis ihrer Unechtheit erschüttert werden kann.[682] Im Fall des Ausstellens durch einen Beamten gelten diese Vermutungen unabhängig davon, ob der ausstellende Beamte reine Beglaubigungsfunktionen erfüllt. Ähnlich verhält sich dies etwa bei den amtlichen Beglaubigungen von Unterschriften, Abschriften und Fotokopien oder im Falle, dass der Beamte allgemein in seinen alltäglichen Tätigkeiten öffentliche Urkunden erstellt. Die Vermutungen der Echtheit und der Wahrhaftigkeit werden zudem aus der Grundrichtlinie des Verwaltungsrechts hergeleitet, wonach die Verwaltungshandlungen und -akten der Vermutung der Rechtsmäßigkeit und der Wahrhaftigkeit unterliegen.[683]

Wird die Echtheit einer öffentlichen Urkunde vom Beweisgegner bestritten, gilt die Urkunde aber bis zur Verkündung der gerichtlichen Entscheidung, welche die Unechtheit erklärt.[684]

2.2.3 Privaturkunde und die Unterschrift

Die Privaturkunde wird unter Ausschluss des Definitionsmerkmals der öffentlichen Urkunde beschrieben, das heißt, es handelt sich um eine Urkunde, welche nicht von einer Person mit öffentlichem Glauben ausgestellt wird.[685] Die Erklärungen einer unterschriebenen Privaturkunde gemäß Art. 219 CC und Art. 368 CPC werden als echt vermutet.[686] Beide Artikel enthalten wortgetreu die gleiche Formulierung, welche ursprünglich aus Art. 131 des CC 1916 stammt. Diese Regelung wird in der Literatur als Behauptung des Vertrauens für alle schriftlichen Geschäfte angesehen, um zu vermeiden, dass der Urheber einer unterschriebenen Urkunde seine eigene Unterschrift bestreitet.[687] Die Rede ist hier aber von einer Vermutung *juris tantum,* das heißt, das Gesetz stellt eine widerlegbare Vermutung auf.[688]

Im Código de Processo Civil werden aber diese Regelungen von weiteren Vorschriften ergänzt, welche die Beweisführung mittels Privaturkunden sowie die Beweislast beim Bestreiten einer Unterschrift regeln. Art. 372 CPC[689] bestimmt, dass

681 *Marinoni*/*Arenhart*, 2000, 40. Siehe z.B. TJRS, Ap. Cível 70008072688, Rel. Des. *Ney Wiedemann Neto*, v. 29.9.2004; Ap. Cível 700010436285, Rel. Des. *Orlando Heemann Júnior*, v. 30.09.2005.

682 *Marinoni*/*Arenhart* 2000, 42.

683 *Di Pietro* 1993, 62.

684 *Marinoni*/*Arenhart* 2005, 394.

685 *Marinoni*/*Arenhart* 2000, 68.

686 Für die Klassifizierung des Art. 368 CPC als Vermutung juris tantum, *Dinamarco* 2005, 121.

687 *Gama* 1927, 252; *Miranda* 1995, 99.

688 Siehe oben in diesem Teil Gliederungspunkt 2.2.1.2.

689 Die Vorschrift ist analog zu § 439 ZPO.

dem Gegner des Beweisführers die Erklärung über die Echtheit und den Inhalt einer Privaturkunde innerhalb von zehn Tagen seit der Vorlegung der Urkunde durch den Beweisführer obliegt. Soll der Gegner des Beweisführers die Urkunde bestreiten, dann wirkt diese bestrittene Urkunde solange nicht – anders als bei der öffentlichen Urkunde –, bis das Gericht eine Entscheidung über die Frage fällt.[690] Falls eine fristgerechte Erklärung nicht abgegeben wird, gilt die Urkunde als anerkannt. Wird aber die Unterschrift einer privaten Urkunde bestritten, verliert diese gemäß Art. 388, I, CPC ihre Echtheitsvermutung bis die Echtheit nachgewiesen wird. In diesem Zusammenhang trägt laut Art. 389 Abs. 2 CPC die Beweislast der Beweisführer der umstrittenen Urkunde.[691]

Es ist ebenso möglich eine beglaubigte Unterschrift zu bestreiten.[692] In der brasilianischen notariellen Praxis existieren zwei verschiedene Unterschriftsbeglaubigungen. Bei der ersten Variante – reconhecimento por autenticidade – bestätigt der Notar, dass die genannte Person die Urkunde vor ihm unterzeichnet hat. Die Unterschrift muss in diesem Fall persönlich in Gegenwart des Notars geleistet werden. Zum Vorteil dieser Beglaubigung zählt die hohe Vertrauenswürdigkeit angesichts der Voraussetzung der Anwesenheit des Unterschreibenden vor dem Notar. Bei der zweiten Variante – reconhecimento por semelhança (Legalisation durch Ähnlichkeit) – erscheint die Person nur einmal vor dem Notar, bei dem sie ihre Unterschrift hinterlegt. Hinterher besteht in diesem Falle immer die Möglichkeit, dass die in einer Urkunde abgegebene Unterschrift mit der beim Notar hinterlegten Unterschrift verglichen wird. Dieser bestätigt im Nachhinein die Urheberschaft des Dokuments durch den Vergleich der beiden Unterschriften. Der Vorteil dieser Variante liegt in der Unkompliziertheit des Verfahrens, denn die Person, von welcher die Unterschrift zu beglaubigen ist, muss nicht jedes Mal zum Notar. Es reicht, wenn ein Dritter das unterschriebene Dokument zum Notar bringt. Dieser Vorteil kann noch auf ein Höchstmaß gebracht werden, indem der Interessent seine Unterschrift bei mehreren

690 *Marinoni/Arenhart* 2005, 314.

691 Zum Thema Beweislast beim Bestreiten einer Unterschrift siehe z.B. TJRS, Ap. Cível 70020535159, Rel. Des. *Tasso Caubi Soares Delabary*, v. 6.9.2007; TJRS, Ap. Cível 70003028131, Rel. *Dr. Agathe Elsa Schmidt da Silva*, v. 12.5.2005; TJRS, Ap. Cível 70006871248, Rel. Des. *Cláudio Augusto Rosa Lopes Nunes*, v. 10.3.2005; TJRS, Ap. Cível 70004843769, Rel. *Dr. Leila Vani Pandolfo Machado*, v. 10.11.2004; TJRS, Ap. Cível 70008704553, Rel. Des. *Léo Lima*, v. 27.5.2004 ; TJRS, Ap. Cível 70002241396, Rel. Des. *Jorge Alberto Schreiner Pestana*, v. 07.3.2002.

692 Das brasilianische Recht verlangt nur selten, dass eine Unterschrift beglaubigt wird. Einer dieser Fälle ist Art. 1.120 CPC, wo die Eheleute beim Stellen eines Antrags auf einverständliche Scheidung, die nicht in Gegenwart des Richters unterschrieben wird, ihre Unterschriften beglaubigen lassen müssen. Erwähnt wird die Beglaubigung einer Unterschrift auch bei der gesetzlichen Behandlung der Vollmacht im Art. 654, § 2 CC, wonach der Dritte, der mit dem Vertreter des Vollmachtgebers verhandelt, verlangen darf, dass die Vollmacht mit einer beglaubigten Unterschrift des Vollmachtgebers versehen wird.

Notaren an verschiedenen Orten hinterlegt. Obwohl die unterschiedlichen Prozeduren und Formalitäten beider Varianten existieren, gilt nach Art. 369 CPC zugunsten beglaubigter Unterschriften eine Vermutung *juris tantum* der Echtheit des Dokuments.[693] Auch hier gilt eine widerlegbare Vermutung, welche jedoch in der Praxis schwieriger zu entkräften ist.

2.3 Die Beweislast

In der Literatur ist die Rede nicht von der Pflicht (dever) der Parteien, Beweise beizubringen, sondern von der einfachen Last (ônus).[694] Führt die beweisbelastete Partei keinen Beweis, erleidet sie möglicherweise eine prozessuale Niederlage. Im Gegensatz zur Pflicht, von welcher das Gesetz die Einhaltung fordert und deren Erfüllung erzwungen werden kann, steht die Beachtung der Last in freiem Belieben des Interessenten.

Im Rahmen des Código de Processo Civil ist eine allgemeine Beweislastregelung im Art. 333 zu finden. Laut dieser Regel trägt der Kläger die Beweislast für die rechtsbegründenden Tatsachen seines Rechts (Art. 333, Abs. 1 CPC), während der Beklagte die Beweislast für die rechtshindernden, rechtsvernichtenden und rechtshemmenden Elemente des vom Gegner zu beweisenden Tatbestands trägt (Art. 333, Abs. 2 CPC). Diese Vorschrift deckt den Grundsatz des Interesses, wonach beweispflichtig diejenige Partei ist, zu Gunsten welcher die zu beweisenden Tatsachen gelten sollen.[695] Derjenige, der Interesse am Nachweis einer bestimmten Tatsache hat, muss den Beweis führen.

2.4 Das elektronische Dokument

Schon in der Anfangsphase der Verbreitung des Internets als Medium zur Geschäftsabwicklung wurden Überlegungen über den erforderlichen Rechtsrahmen zur Beweisführung mittels elektronischer Dokumente angestellt. Bereits im Jahr 1992 deutete *Santolim* darauf hin, dass Voraussetzung zur Wirksamkeit einer im elektronischen Rechtsverkehr abgegebenen Willenserklärung zwei Anforderungen seien: Zum einen sollte das gewählte Medium (elektronisches Dokument, Formular oder ähnliches) nicht veränderbar sein, ohne dass die Veränderung Spuren hinterlässt. Zum anderen sollte das Mittel die Identifizierung des Erklärenden ermöglichen.[696] In die gleiche Richtung zielte noch im Jahr 2000 die Argumentation des Richters des

693 *Pontes de Miranda* 2001, 365.

694 *Buzaid* 1972, 60; *Karam* 1980, 52; *Alvim* 2001, 476; *Pacífico* 2001, 37 ff.

695 *Dinamarco* 2005, 72 f.

696 *Santolim* 1995, 33 (wissenschaftliche Arbeit bereits im Jahr 1992 vorgelegt, aber erst im Jahr 1995 veröffentlicht).

Superior Tribunal de Justiça[697], *Aguiar Júnior*[698], der zufolge die unzähligen elektronisch abgeschlossenen Verträge praktisch keinen Beweiswert hätten, da diese von den Verbrauchern üblicherweise aufbewahrten Ausdrucke der Transaktionen den gleichen – oftmals geringen – Beweiswert wie ein Zeugenbeweis aufwiesen.[699] Um diese Schwachstelle der Beweisführung mittels elektronischer Dokumente zu beseitigen, sollten – wie in anderen Ländern – asymmetrische kryptografische Verfahren eingeführt werden. Nur dann habe man die Möglichkeit, die Authentizität und Integrität der Wiedergabe der Vertragsklauseln eines elektronischen Vertrags zu überprüfen.[700] Tatsächlich kann, wie von *Aguiar Júnior* erwähnt, der Inhalt von elektronischen Dokumenten jederzeit von jedermann beliebig verändert werden, ohne dass eine Möglichkeit besteht, dies am Dokument zu erkennen.[701] Ebenso erfordert es bei der elektronischen Übermittlung von Dokumenten häufig nur einen geringen Aufwand, die wahre Identität des Absenders zu verschleiern oder eine falsche Identität vorzutäuschen.

Unter Beachtung dieser Manipulationsmöglichkeiten gilt für einfache elektronische Dokumente im brasilianischen Recht keine beweisrechtliche Privilegierung. Sie unterliegen lediglich, entgegen der Ansicht von *Aguiar Júnior*, der ihnen praktisch gar keinen Beweiswert zumisst, der freien Beweiswürdigung des Gerichts. Wie schon oben dargestellt[702], sind nach Art. 332 CPC alle rechtlich wie auch moralisch legitimierten Mittel zulässig, um die Wahrheit der behaupteten Tatsachen nachzuweisen, auch wenn sie nicht im CPC ausdrücklich festgesetzt werden. Darüber hinaus legt Art. 107 CC fest, dass die Gültigkeit einer Willenserklärung nicht von einer besonderen Form abhängt, es sei denn, diese wird durch ein Gesetz ausdrücklich verlangt. Es besteht somit grundsätzlich Formfreiheit.

Jedoch reicht die Tatsache, dass einfache elektronische Dokumente vom Gericht gewürdigt werden können, nicht aus, um eine ausreichende Rechtsicherheit im elektronischen Geschäftsverkehr zu etablieren. Bleibt der Gesetzgeber in diesem Bereich passiver Zuschauer der Ereignisse, dann droht hier steigende Rechtsunsicherheit. Aus diesem Grunde hat die MP 2.200-2 nicht nur die technisch-organisatorischen Rahmenbedingungen einer landesweiten Infrastruktur für öffentliche Schlüssel geschaffen, sondern gleichzeitig Beweisregelungen für elektronische Dokumente –

697 Das Superior Tribunal de Justiça (STJ) ist das oberste brasilianische Gericht auf dem Gebiet der ordentlichen Gerichtsbarkeit mit Sitz in Brasilia.

698 *Aguiar Júnior* 2000, zit. n. *Lawand* 2003, 144.

699 Gemäß Art. 227 CC und Art. 402 CPC ist der ausschließliche Zeugenbeweis nur bei Rechtsgeschäften zulässig, deren Wert unterhalb des zehnfachen Wertes des höchsten im Land gültigen Mindestmonatslohns zum Zeitpunkt des Vertragsabschlusses liegt. Der einzige Paragraph des Art. 227 CC bestimmt, dass der Zeugenbeweis nur einen ergänzenden Charakter zum Urkundenbeweis besitzt.

700 *Aguiar Júnior* 2000, zit. n. *Lawand* 2003, 144.

701 *Pordesch* 2002, 35; *Roßnagel*/*Pfitzmann*, NJW 2003, 1212.

702 Siehe bereits oben in diesem Teil Gliederungspunkt 2.2.

sowohl signiert als auch unsigniert – in die brasilianische Rechtsordnung aufgenommen. Diese Beweisregeln sind in Art. 10 §§ 1 und 2 MP 2.200-2 enthalten und werden im Folgenden dargestellt.

2.4.1 Das elektronisch signierte Dokument im Rahmen des Art. 10 § 2 MP 2200-2

Art. 10 § 2 MP 2.200-2 besagt, dass im Anwendungsbereich dieser Vorschrift grundsätzlich sämtliche Mittel zur Gewährleistung von Authentizität und Integrität elektronischer Dokumente zulässig sind. Dies umfasst auch Signaturverfahren, die außerhalb der brasilianischen Infrastruktur liegen. Den Parteien oder Kommunikationsteilnehmern steht es frei, sich nach ihrem Belieben über das zu verwendende Sicherungsmittel zu einigen. Diese Vorschrift ist ähnlich wie Art. 5 Abs. 2 RLeS und basiert fast buchstäblich auf Art. 3 Nr. 4 der portugiesischen Verordnung Decreto-Lei Nr. 290-D/1999[703] und wird auch vom Art. 6 Gesetzentwurf Nr. 7316 wiederholt.

Ziel des Art. 10 § 2 MP 2.200-2 ist die Flexibilisierung der Regelung des Art. 10 § 1 MP 2200-2. Diese soll erreicht werden, indem andere Identifikations- und Integritätsmittel für elektronische Dokumente angewandt werden können, ohne dass diese als Beweismittel vom vornherein auf Ablehnung stoßen.[704] Hierdurch wird die Privatautonomie der Vertrags- und Kommunikationspartner respektiert, die somit selbst in privatrechtlichen Absprachen frei bestimmen können, welche elektronische Signatur für die gegenseitige Kommunikation oder sogar zur Formalisierung von Rechtsgeschäften benutzt werden soll. Obwohl der elektronische Geschäftsverkehr viele Unsicherheiten mit sich bringt, kann es durchaus plausible Gründe dafür geben, dass sich Geschäftspartner, die sich schon seit langem kennen, gegen ein akkreditiertes Signaturverfahren entscheiden. Die Parteien können sich bewusst und ihrer Risikobereitschaft entsprechend frei entscheiden, ihre Geschäfte je nach Wert und Bedeutung der Transaktion etwa durch einfache E-Mails abzuwickeln. Hierbei ist zu berücksichtigen, dass digitale Signaturen und die akkreditierten Signaturverfahren im Wesentlichen zum einen für offene Netze konzipiert wurden, bei denen die Unsicherheiten des elektronischen Geschäftsverkehrs am ausgeprägtesten sind, und zum anderen für Vertragspartner, die sich im „realen“ Leben nie begegnet sind und sich höchstwahrscheinlich auch nie begegnen werden.[705]

In diesem Zusammenhang müssen die Vertragspartner trotzdem damit rechnen, dass die Authentizität oder die Integrität eines einfachen elektronischen Dokuments

703 Decreto-Lei Nr. 290-D/1999 wurde zuletzt von den Decreto-Lei Nr. 62/2003 und Nr. 165/2004 geändert. Durch diese beiden Novellierungen ist die Signaturrichtlinie ins portugiesische Recht umgesetzt worden. Zum portugiesischen signaturrechtlichen Rechtsrahmen siehe http://www.icp.pt/template16.jsp?categoryId=96799.

704 *Menke* 2005, 144.

705 *Menke* 2005, 145.

im Laufe ihrer geschäftlichen Zusammenarbeit von der anderen Vertragspartei erfolgreich bestritten werden kann. Mit wachsender Unsicherheit des von ihnen gewählten Mittels steigt jedoch auch das Risiko, dass eine der Parteien später die Authentizität oder Integrität des Dokumentes erfolgreich bestreitet. Wird die Echtheit elektronischer Dokumente im Rahmen des Art. 10 § 2 MP 2.200-2 bestritten, dann unterliegen sie der freien Beweiswürdigung. Gemäß Art. 131 CPC darf der Richter den Beweis dann frei auswerten, sofern er die Tatsachen und Sachverhalte berücksichtig, welche in den Akten enthalten sind – selbst wenn diese nicht von den Parteien vorgetragen worden sind. Er muss jedoch in dem Urteil die Gründe für seine Überzeugungsbildung angeben.

Im Fall des Bestreitens der Echtheit tauchen dann Komplikationen auf, da zur abschließenden Klärung der Streitfrage in der Regel ein Sachverständigenbeweis erhoben werden muss. Diese Sachverständigengutachten sind in vielen Fällen aufwendig und kostspielig. Die Dauer und Kosten eines Prozesses dürften deswegen zuvor nicht eindeutig absehbar sein.[706]

Art. 10 § 2 MP 2.200-2 könnte außerdem die Tür zur „Technikoffenheit" öffnen, obwohl dieses Konzept offensichtlich keine zentrale Rolle in der brasilianischen Regulierung spielt.[707] Danach könnten andere Identifikationsmittel wie biometrische Signaturverfahren, Passwörter, einfache E-Mails, freie verfügbare Implementierungen des Programms „Pretty Good Privacy" (PGP)[708] eingesetzt werden, ohne dass ihre Zulässigkeit und Wirksamkeit als Beweismittel von den Gerichten negiert werden kann. Eine Beschränkung der Beweisführung durch elektronische Dokumente ausschließlich auf akkreditierte Signaturverfahren ist so nicht möglich.

2.4.2 Das elektronisch signierte Dokument im Rahmen Art. 10 § 1 MP 2.200-2

Entscheidet sich der Teilnehmer des elektronischen Kommunikationsverkehrs aber für die akkreditierten Signaturverfahren, soll dieser von einer besseren Beweislage profitieren. Zu diesem Zwecke wurde eine Vorschrift geschaffen (§ 1 des Art. 10 MP 2.200-2), gemäß welcher die Echtheitsvermutung, die zu Gunsten unterschriebener Dokumente im Rahmen des Código Civil gilt, auf den elektronischen Rechtsverkehr übertragen wird. Voraussetzung dafür ist jedoch, dass das elektronische Dokument mit einer akkreditierten Signatur versehen wird. § 1 des Art. 10 verweist auf Art. 131 des mittlerweile außer Kraft getretenen Código Civil aus dem Jahr

706 *Roßnagel*, RMD, SigG Einl., Rn. 228.

707 Hierzu im zweiten Teil Gliederungspunkt 2.2.2, der das technologische Konzept der ICP-Brasil behandelt.

708 Im Verfahren von PGP generieren und verwahren die Anwender ihre Schlüssel selbst. Sie verteilen auch ihren öffentlichen Schlüssel selbst. Unabhängige Dritte zur Identifizierung und Ausstellung von Zertifikaten sind nicht einbezogen. Kritisch zu der fehlenden Sicherheit von PGP, Mertes 1995, 159. Zu PGP siehe auch www.pgp.de.

1916, welcher beim Erlass der MP 2.200-2 noch galt. Der brasilianische Código Civil gilt inzwischen in einer neuen Fassung aus dem Jahr 2002 und regelt in Art. 2.046, dass alle gesetzlichen Bestimmungen, die auf Vorschriften des im Jahr 2003 außer Kraft getretenem Código Civil aus dem Jahr 1916 verweisen, nun auf die entsprechenden Regelungen des geltenden Código Civil zu beziehen sind. Der neue Código Civil hat die Formulierung des Art. 131 des alten Código Civil in Art. 219 exakt übernommen.

Die Vorschrift gilt nach wie vor als wichtiges Mittel zur Gewährleistung von Rechtssicherheit im Geschäftsverkehr. Dies wird dadurch bewirkt, dass die Vorschrift den vertragsschließenden Parteien und auch der Rechtsgemeinschaft im Allgemeinen die Ernsthaftigkeit und die Rechtskraft der Unterschrift signalisiert.[709] Der Gesetzgeber will hier die Möglichkeit ausschließen, dass jeder nach dem Abschließen eines Vertrags beliebig seine Namensunterzeichnung erfolgreich bestreiten könnte und dadurch Rechtsunsicherheit verursacht würde. Das ist das zentrale Gebot dieser Vorschrift. Die MP 2.200-2 hat genau in diesem Sinne und für diesen Zweck diese Vorschrift aus dem Zivilrecht übernommen, um Rechtssicherheit für den elektronischen Geschäftsverkehr zu schaffen.

Die Rechtssicherheit stützt sich hier aber nicht etwa auf das eigenhändige Unterschreiben, sondern auf das akkreditierte Zertifizierungsverfahren (processo de certificação credenciado) im Rahmen der Infra-Estrutura de Chaves Públicas Brasileira.[710] Die Echtheitsvermutung (*juris tantum*) für elektronische Dokumente gilt somit für Dokumente mit Signaturen, die mittels akkreditierter Verfahren erzeugt worden sind. Die akkreditierten Verfahren wiederum stützen sich auf technisch-organisatorische Vorschriften, welche durch Beschlüsse des Regulierungsausschusses erlassen wurden[711] und die sich ihrerseits – was die Technik angeht – auf die von der Wissenschaft entwickelten Verschlüsselungs- und Signierverfahren stützen.

2.4.3 Das Bestreiten eines mittels akkreditierter Verfahren signierten Dokuments

Wird die Echtheit einer eigenhändigen Unterschrift bestritten,[712] relativiert Art. 389 Abs. 2 CPC die Echtheitsvermutung des Art. 219 CC, da dem Beweisführer der umstrittenen Urkunde die Beweislast dafür zugewiesen wird, die Echtheit der Unterschrift nachzuweisen. Da es im Código de Processo Civil keine analoge Regel zur Beweisführung mittels elektronischer Dokumente gibt, stellt sich die Frage, wie die Situation vom Gericht bewertet werden soll, wenn die Urheberschaft eines mit einer akkreditierten digitalen Signatur versehenen Dokuments vom Signaturschlüssel-Inhaber bestritten wird. Dürfte Art. 389 Abs. 2 CPC angewendet werden – obwohl

709 *Miranda* 1995, 99; *Gama* 1927, 252.

710 Detaillierter zu dem Thema siehe im zweiten Teil Gliederungspunkt 2.2.6.

711 Mehr hierzu siehe im zweiten Teil Gliederungspunkt 2.2.4.

712 S. hierzu die Ausführungen oben in diesem Teil 2.2.3.

er ursprünglich für die Papierwelt konzipiert wurde? Oder gilt direkt die Echtheitsvermutung des § 1 Art. 10 MP 2.200-2? Wer soll die Beweislast tragen?

2.4.3.1 Anwendung Art. 389 Abs. 2 CPC?

Die erste denkbare Alternative zur Lösung dieses Problems wäre die analoge Anwendung von Art. 389 Abs. 2 CPC auch für elektronisch signierte Dokumente. Art. 389 Abs. 2 CPC bestimmt, dass im Fall des Bestreitens einer Unterschrift (assinatura) diejenige Partei die Beweislast trägt, welche das Dokument in den Prozess eingeführt hat. Die Vorschrift enthält die Begriffe „assinatura" und „documento". Eine digitale Signatur (assinatura digital) und ein elektronisches Dokument (documento eletrônico) würden bei einer buchstabengetreuen Auslegung durchaus durch die Begriffe „assinatura" und „documento" erfasst werden. Der Begriff „documento" könnte im brasilianischen Recht sowohl für eine Urkunde im Sinn des deutschen Rechts stehen[713], als auch als Oberbegriff für alle Dokumentarten aufgefasst werden. Im brasilianischen Recht existiert keine dem deutschen Recht entsprechende Differenzierung zwischen den beiden Begriffen und ein „documento" muss nicht unbedingt eine Verkörperung darstellen, also an ein Material gebunden sein, welches mit den Händen greifbar ist. Das Gleiche betrifft den Begriff „assinatura", der auch nicht unbedingt auf eine handschriftliche Unterschrift beschränkt sein muss und eine gewisse Flexibilität aufweisen kann. Diese Auslegung wäre grundsätzlich möglich und wird von den Vertretern einer seit dem Ende der 90er Jahre in der Literatur konsolidierten Auffassung, nach der das brasilianische Recht im Allgemeinen keine große Anpassungsbedürfnisse seiner Beweis- und Formvorschriften an die neuen elektronischen Techniken aufweise,[714] auch so gesehen. Man könne und solle technische Innovationen einführen[715] – und zwar auch per Gesetz – aber gleichzeitig die schon vorhandenen Beweis- und Formvorschriften anwenden. Anstelle der Einführung neuer Beweis- und Formvorschriften sollten somit eher Auslegungsversuche unternommen werden.[716]

Würde man jedoch die Beweislastregel des Art. 389 Abs. 2 CPC für elektronisch signierte Dokumente anwenden, dann müsste der Signaturempfänger – ohne jegliche Beweiserleichterung – die Beweislast für die Authentizität und Integrität des bestrittenen signierten elektronischen Dokuments tragen. Der Erklärungsempfänger wäre dann praktisch schutzlos gegenüber dem unbegründeten Einwand seines Beweis-

713 Zur Definition einer Urkunde im deutschen Recht siehe im dritten Teil Gliederungspunkt 1.4.2.1.

714 Siehe hierzu u.a., *Santolim* 1995, 33, *Rodrigues* 2001, 83, *Castro* 2001, *Marques* 2005, 146, *Boiago Jr.* 2006, 137 ff., *Parentoni* 2007, 37 ff.

715 *Santolim* 1995, 33.

716 *Santolim* 1995, 34 ff.

gegners, dass die elektronischen Daten nicht vom ihm signiert seien.[717] Das würde zu einem ungerechten Ergebnis führen, welches das Vertrauen der Teilnehmer am elektronischen Rechtsverkehr gefährden könnte. Darüber hinaus wären Sinn und Zweck der Vorschriften über die Beweislast – ursprünglich für die Papierwelt konzipiert – vereitelt, grundsätzlich Gerechtigkeit, Vorhersehbarkeit sowie Rechtssicherheit zu erzielen.

Zu untersuchen wäre auch der Wert der Akkreditierung, die dieser im Rahmen des Art. 389 Abs. 2 CPC zugewiesen wird. Wie ist die Behauptung des Signaturempfängers, dass das von ihm beigebrachte Dokument von seinem Beweisgegner mittels eines akkreditierten Signaturverfahrens gemäß Art. 10 § 1 MP 2200-2 signiert worden sei, zu bewerten? Bei der Auseinandersetzung mit diesem Argument ist zu beachten, dass die Akkreditierung vermutlich eine erhebliche Rolle bei der richterlichen Überzeugungsbildung spielen wird. Das Verweisen auf die Sicherheit einer landesweiten Infrastruktur für öffentliche Schlüssel, die sich wiederum auf umfassende internationale technisch-organisatorische Regelungen stützt, wird sicherlich vom Gericht nicht ignoriert werden. Ob das Argument der Akkreditierung zur Überzeugung des Gerichts ausreichen würde, wäre aber eine offene Frage. Gelingt es dem möglichen Autor eines bestrittenen Dokuments, Tatsachen vorzutragen, die das Gericht zweifeln lassen, dann verliert der Signaturempfänger den Prozess im Fall des non liquet, angesichts der ihm zugewiesenen Beweislast.

Grundsätzlich ist jedoch festzustellen, dass Art. 389 Abs. 2 CPC für das Bestreiten elektronisch signierter Dokumente anwendbar ist.

2.4.3.2 Ausschließliche Anwendung der Echtheitsvermutung des § 1 Art. 10 MP 2.200-2?

Eine zweite Möglichkeit, die mittels eines akkreditierten Verfahrens signierten Daten zu bestreiten, ergibt sich durch den direkten Verweis auf den § 1 Art. 10 MP 2.200-2. Wird im Streitfall die direkte und ausschließliche Anwendung des § 1 Art. 10 MP 2.200-2 vertreten, muss aber gerechtfertigt werden, weshalb keine Anwendung der entsprechenden Regelungen des CPC – insbesondere von Art. 389 Abs. 2 – erfolgt. Dabei könnte die Partei – im Falle der Erklärungsempfänger – argumentieren, dass die MP 2.200-2 ein spezielles Gesetz (lex specialis) sei, welches das allgemeine Gesetz, hier den CPC (lex generalis), verdrängt. Speziell für elektronische signierte Daten konzipiert könnte § 1 Art. 10 MP 2.200-2 somit der allgemeinen Regelung des Art. 389 Abs. 2 CPC vorgehen. Dabei sollte man diese Regelung als prozessuale Vorschrift[718] betrachten. Die Einordnung dieser Vorschrift als pro-

717 Die gleiche Argumentation der Begründung des deutschen Formanpassungsgesetzes gilt hier. Siehe hierzu BR-Drs. 14/4987, S. 25, und auch bereits im 3. Teil Gliederungspunkt 1.6.4.

718 Im Rahmen der bei der Zeit des Erlassens der MP 2.200-2 geltenden Fassung der Constituição Federal, könnte eine Medida Provisória über Zivilprozessrecht bestimmen. Nach der

zessuale Bestimmung wäre aber auf den ersten Blick nicht ohne weiteres erkennbar, denn der Rechtssatz auf den sie verweist[719], ist im Código Civil platziert. Da jedoch der Art. 368 des CPC eine Vorschrift mit der exakten Formulierung des Art. 219 CC enthält, lässt sich dieser Schluss nicht durchsetzen. Sowohl Art. 219 CC als auch Art. 368 CPC zeichnen sich als „normas bifrontes" in der brasilianischen Literatur[720] aus, das heißt, es handelt sich um bipolare Regelungen, die weder ausschließlich der Kategorie des prozessualen Rechts noch der des materiellen Rechts angehören. Vielmehr handelt es sich hierbei um Vorschriften, welche sowohl über die Form als auch über den Beweiswert von Dokumenten bestimmen.

Zu erwähnen ist auch, dass § 1 Art. 10 MP 2.200-2 eine Vermutung *juris tantum* darstellt. Da nach Literatur und Rechtsprechung die widerleglichen Vermutungen eine Beweislastumkehr mit sich bringen[721], käme man zu dem Ergebnis, dass der Signaturschlüssel-Inhaber die Beweislast für die Behauptung trage, er habe die Erklärung nicht abgegeben. Dieser Ausgang könnte auch unzulänglich und mit ungerechten Ergebnissen verbunden sein. Ein Beispiel dafür ist der Fall des angeblichen Signaturschlüssel-Inhabers, welcher aufgrund eines ihm zugewiesenen signierten elektronischen Dokuments verklagt wird. Behauptet er aber, er habe nie ein elektronisches Zertifikat erworben und habe nichts mit dem Dokument zu tun, trägt er trotzdem die Beweislast im Fall des *non liquet*. Die Rechtsfolge der Beweislastumkehr ist schwerwiegend für den mutmaßlichen Signaturschlüssel-Inhaber, aber unvermeidbar will man einen Schutz für den Signaturempfänger in Form einer Beweisvorschrift schaffen. Dies beruht aufgrund des Mangels einer Unterteilung der Widerlegbarkeit einer Vermutung in Beweis des Gegenteils und Gegenbeweis im brasilianischen Recht.[722] Dementsprechend kann das Gericht höhere oder niedrigere Anforderungen an die Widerlegung stellen. Das erwünschte Gleichgewicht zwischen dem Schutz des Erklärungsempfängers gegen unbegründete Einwände des Beweisgegners und der Garantie der Möglichkeit einer Verteidigung des Signaturschlüssel-Inhabers für die Fälle, in denen er tatsächlich die bestrittene Erklärung nicht abgegeben hat, zu schaffen, ist keine leichte Aufgabe. Dies benötigt sicherlich eine neue Beweisregelung für elektronisch signierte Dokumente, welche beide Ziele in Einklang bringt.

Ungeachtet dessen, für die aktuelle geltende Lage selbst wenn die Anwendung des § 1 Art. 10 MP 2.200-2 mit möglichen ungerechten Ergebnissen verbunden sein kann, bleibt die Möglichkeit der Anwendung dieser Vorschrift für das Bestreiten der

Verabschiedung der Verfassungsänderung Emenda Constitucional Nr. 32 dürfen die Medidas Provisórias nicht mehr über Zivilprozessrecht verfügen. Hierzu bereits im 2. Teil Gliederungspunkt 2.1.

719 Art. 131 des alten Código Civil, der dem Art. 219 des aktuellen entspricht.

720 *Dinamarco* 2005, 46 ff.

721 Hierzu bereits in diesem Teil Gliederungspunkt 2.2.1.2.

722 Anders im deutschen Beweisrecht, wo diese Unterteilung existiert. Siehe hierzu bereits im 2. Teil Gliederungspunkte 1.2.4 und 1.2.5.

Authentizität elektronischer Dokumente erhalten, wenn diese mittels akkreditierter Verfahren signiert wurden.

2.4.3.3 Das Verbraucherschutzgesetzbuch und das Bestreiten der Authentizität einer elektronisch signierter Datei

Das Bestreiten der Authentizität einer elektronisch signierten Datei – nicht unbedingt mittels eines akkreditierten Verfahrens – wird auch teilweise vom Verbraucherschutzgesetzbuch (CDC) geregelt. Zu erwähnen ist hier die Vorschrift (Art. 6 Abs. 8 CDC)[723], wonach der Verbraucher das Recht auf eine Erleichterung bei der gerichtlichen Durchsetzung seiner Ansprüche hat. Insbesondere gilt hier die Umkehr der Beweislast im Zivilprozess, wenn nach richterlicher Ansicht die Behauptungen des Verbrauchers glaubwürdig erscheinen oder wenn der Verbraucher nach ordentlichen Erfahrungssätzen als unterlegen „hipossuficiente" betrachtet wird. Ein Verbraucher im Sinn des Art. 2 CDC ist jede natürliche oder juristische Person, die als Endnutzer ein Produkt erwirbt oder benutzt oder eine Dienstleistung in Anspruch nimmt.[724] Der Signaturschlüssel-Inhaber kann, wenn er als Verbraucher im elektronischen Geschäftsverkehr auftritt, Gebrauch von der Beweislastumkehrregel des CDC machen. Die zwei Voraussetzungen des Tatbestands sind aber zu erfüllen, nämlich erstens die Überzeugung des Gerichts von der Wahrscheinlichkeit der Behauptungen und zweitens von der Unterlegenheit des Verbrauchers.[725] Dabei kann sich der Signaturschlüssel-Inhaber auf die so genannte technische Unterlegenheit (hipossuficiência técnica) stützen, welche sich auf die fehlende Kenntnis des Verbrauchers über das Funktionieren eines Produktes oder einer Dienstleistung bezieht. Angesichts der Tatsache, dass im Umgang mit elektronischen Signaturen das Fachwissen und die Erfahrung im Allgemeinen fehlen, sind die Chancen groß, dass sich das Gericht von der Unterlegenheit des Verbrauchers überzeugen lässt. Wie von Blocher zu Recht darauf hingewiesen wird, stellt sich die komplexe Signaturtechnologie für den normalen Anwender als eine „black box" dar, auf die er sich komplett verlassen muss.[726]

Wird aber eine Entscheidung zur Umkehr der Beweislast von Gericht gefällt[727], muss diese spätestens bis zum Anfang der Beweisaufnahme erfolgen. Würde ansonsten eine solche Verfügung erst später etwa im Urteil angewiesen, dann bliebe die von ihr benachteiligte Partei praktisch schutzlos und hätte kaum eine Möglich-

723 Hierzu siehe im 2. Teil Gliederungspunkt 2.2.9.1.8.1.

724 Zu der Auseinandersetzung in der Literatur und Rechtsprechung über den Verbraucherbegriff siehe im 2. Teil Gliederungspunkt 2.2.9.1.8.1.

725 Über die Unterlegenheit des Verbrauchers siehe im 2. Teil Gliederungspunkt 2.2.9.1.8.1.

726 *Blocher* 2007, 438 f.

727 Die Entscheidung zur Umkehr der Beweislast im Rahmen des Código de Defesa do Consumidor darf von Amts wegen getroffen werden. Hierzu: *Leonardo* 2004, 269.

keit, die prozessuale Niederlage zu vermeiden angesichts der überraschenden Wende erst am Schluss eines Prozesses. Außerdem würde eine späte Entscheidung diesbezüglich gegen das Verfassungsgebot auf rechtliches Gehör (direito ao contraditório e ampla defesa) des Art. 5, LVI, CF verstoßen.[728]

2.4.3.4 Bewertung der Optionen

Wie dargestellt sind im Fall des Bestreitens einer mittels akkreditierter Signaturverfahren signierten Datei nach der aktuellen brasilianischen Rechtslage grundsätzlich zwei Rechtsquellen anwendbar: § 1º Art. 10 MP 2.200-2 oder Art. 389 Abs. 2 CPC. Beide führen zu gegensätzlichen Ergebnissen. Während § 1º Art. 10 MP 2.200-2 eine widerlegliche Vermutung begründet, welche vom Signaturschlüssel-Inhaber neutralisiert werden muss, verlagert Art. 389 Abs. 2 CPC die Beweislast für die Authentizität des elektronischen Dokuments wiederum auf den Signaturempfänger. Eine dritte Variante wäre die Anwendung von einer der genannten Vorschriften und gegebenenfalls die parallele Handhabung des Art. 6 Abs. 8 CDC, insbesondere mit der Umkehr der Beweislast zu Gunsten des Verbrauchers.

Eine solche Gesetzeslage führt jedoch zu Rechtsunsicherheit. Da beide Wege mit sich einander widersprechenden Ergebnissen – einmal trägt der Signaturempfänger das Risiko des *non liquet*, das andere Mal der Signaturschlüssel-Inhaber – möglich sind, ist der Prozessausgang anhand der Beweissituation nicht mehr vorhersehbar und für den Entscheidenden beliebig. Die ausschließliche Anwendung des Art. 10 § 1º MP 2.200-2 mit dem Argument, dass die MP 2.200-2 nach dem Kriterium *lex specialis* den Código de Processo Civil verdrängt, wäre die beste Wahl zur Lösung dieses Normenkonfliktes. Diese Konstellation stellt jedoch keine Selbstverständlichkeit bei der Rechtsanwendung dar. Wie bereits in dieser Arbeit erwähnt[729], spielt die Beweislast auch eine sehr wichtige außerprozessuale Rolle, denn ihre Regeln beeinflussen das Verhalten der Parteien. Die Entscheidung, einen Prozess zu führen, kann nur konsequent getroffen werden, wenn Rechtsanwälte in der Lage sind, ihre Mandanten über die zu beweisenden Inhalte ausreichend zu informieren. Bei einer so undefinierten Lage, in der die Beweislast zwischen den Parteien beliebig nach dem Wunsch des Gesetzesanwenders gewählt werden kann, für den er plausible Argu-

728 Siehe hierzu: Agravo de Instrumento 14.305-5/8, Rel. Des. *José Geraldo de Jacobina Rabello*, v. 05.9.1996, TJSP; Agravo de Instrumento 121.979-4, Rel. Des. *Antonio Carlos Marcatu*, v. 07.10.1999, TJSP; Apel. Cível 70022098768, Rel. Des. *Pedro Celso Dal Pra*, v. 13.12.2007, TJRS; a.A., besonders mit dem Argument, dass die Beweislastumkehr erst am Schluss des Prozesses zu erklären ist, nach der Prüfung des unstreitigen Sachverhalts, Ap. Cível 70021794342, Rel. Des. *Iris Helena Medeiros Nogueira*, v. 11.12.2007, TJRS; Agravo de Instrumento 64.343-4, Rel. Des. *Ney Almada*, v. 23.9.1997, TJSP; Agravo de Instrumento 142.928-5, Rel. Des. *Cristo Pereira*, v. 03.9.2003, TJPR.

729 Siehe hierzu bereits im diesen Teil Gliederungspunkt 1.3.

mente und gültige Rechtssätze für eines der zwei Extreme findet, ist nicht nur der Prozessausgang schwer einschätzbar, sondern es wird auch die gesamte Sicherheit der Infrastruktur für öffentliche Schlüssel abgeschwächt. Während die Regulierung der Infrastruktur durch die MP 2.200-2 als auch die weiteren Beschlüsse des Ausschusses für eine technische sowie organisatorische Sicherheit sorgen und dabei auch recht erfolgreich sind, scheitern sie in puncto Rechtsicherheit.

Anders stellt sich die Lage bei unterschriebenen Dokumenten dar, bei denen die beweisrechtliche Lage eindeutig ist. Art. 219 CC enthält für diese eine Echtheitsvermutung. Diese Vermutung wird aber von Art. 389 Abs. 2 CPC beschränkt, indem – im Falle des Bestreitens der Unterschrift – die Beweislast auf den Beweisführer verlagert wird. Hier können sich Rechtsanwälte und Interessenten ein klares Bild über die Aussichten des Prozesses im Bezug auf die Frage der Authentizität der Urkunde machen.

Als Resultat ergibt sich somit, dass das brasilianische Beweisrecht über keine ausreichende und sachgerechte Lösung für die Beweisführung mittels elektronisch signierter Dokumente anhand akkreditierter Verfahren verfügt. Zu erwähnen ist auch die Tatsache, dass der Gesetzentwurf Nr. 7316/2002 diese Situation nicht ändert, sondern die hier dargelegte Problematik verschärft, indem er im Art. 5 regelt, dass die akkreditierten Signaturen gemäß Art. 219 des CC den gleichen Beweiswert wie die eigenhändigen Unterschriften haben. Diese gesetzliche Wertung mit einem erneuten Verweis auf die Vorschriften über die eigenhändige Unterschrift signalisiert dem Gesetzesanwender, dass die Möglichkeit, von den entsprechenden Regeln des CPC – und besonders von Art. 389 Abs. 2 – Gebrauch zu machen, weiter besteht.

2.4.3.5 Inhaltliche Einwände

Die bisherigen Ausführungen konzentrierten sich auf den Aspekt der Beweislast beim Bestreiten einer akkreditierten Signatur. Unabhängig von dieser Frage muss auch das Thema der möglichen inhaltlichen Einwände gegen die Echtheitsvermutung des Art. 10 § 1º MP 2.200-2 erörtert werden. Die Geltendmachung der Vermutung erfordert die Vorlage einer akkreditierten Signatur. Gelingt dem Beweisführer der Beweis, dass das Dokument mit einem solchen Verfahren signiert worden sei, dann gilt die Vermutung. Dieser Beweis ist durch Vorlage des passenden akkreditierten Zertifikats möglich. Bei der Widerlegung der Vermutungsbasis werden dem Beweisgegner grundsätzlich keine inhaltlichen Grenzen gesetzt. Er kann plausible Argumente beibringen, muss diese jedoch nachweisen. Hält aber das Gericht einen Gesichtspunkt für unerheblich, dann kann der entsprechende Beweis zurückgewiesen werden. Gemäß Art. 131 CPC bestimmt der Richter von Amtes wegen oder nach Parteiantrag, welche Beweise zur Aufklärung des Sachverhalts geboten erschei-

nen.[730] Er kann die unbrauchbaren oder von einer Partei zu Verzögerungszwecken gestellten Anträge zur Beweisaufnahme ablehnen.

Als möglicher Einwand gegen die Vermutung der Echtheit wäre die fehlerhafte Identifizierung des Signaturschlüssel-Inhabers durch den Zertifizierungsdiensteanbieter zu nennen. Behauptet der Beweisgegner beispielsweise er habe nie eine Chipkarte aus einem akkreditierten Signaturverfahren gehabt, wird der Richter möglicherweise gegenüber dem Zertifizierungsdiensteanbieter anordnen[731], die entsprechende Dokumentation vorzulegen. Wird die ordnungsgemäße Identifizierung des vermeintlichen Ausstellers durch Kopie des Ausweises oder durch den eigenhändig unterschriebenen Antrag nicht bewiesen, kann die Vermutungsbasis erschüttert werden.

Einwenden könnte der Signaturschlüssel-Inhaber auch, dass der private Schlüssel unberechtigt verwendet wurde. Hierbei könnte die Argumentation auf Diebstahl und Ausspähung der PIN basieren. Der Signaturschlüssel-Inhaber muss in diesem Zusammenhang den Diebstahl nachweisen und wenn ihm dies gelingt, dann kann er vielleicht die Vermutung erfolgreich erschüttern. Dabei muss auch beachtet werden, dass die Rechtsprechung beim Umgang mit Bankkarten eine Rolle bei den Gerichtsentscheidungen über Missbrauch von Signaturkarten spielen kann. Die Rechtsprechung diesbezüglich neigt dazu, angesichts der verschiedenen Manipulations- und Angriffsmöglichkeiten mit Bankkarten im elektronischen Rechtsverkehr, die technische Sicherheit der zugrunde liegenden Verfahren als nicht völlig sicher anzusehen.[732]

Fraglich ist, wie sich die Rechtsprechung angesichts der erwähnten Präjudize zu Bankkarten bezüglich des Umgangs mit Signaturkarten entwickeln wird. Eine einfache Übertragung der von der brasilianischen Rechtsprechung entwickelten Grundsätze bezüglich Bankkarten darf dabei nicht stattfinden. Grund hierfür ist, dass die Technik der digitalen Signatur sicherer als die der normalen Bankkarten ist. Während Bankkartendaten u.a. am Geldautomaten durch moderne Techniken ausspioniert werden können, sind solche Fälle bezüglich der sicheren Signaturerstellungs-

730 Anders als im § 355 Abs. 2 ZPO bestimmt, besteht im Código de Processo Civil die Möglichkeit, den Beschluss, durch die eine oder die andere Art einer Beweisaufnahme, anzufechten.

731 Der negative Beweis, er habe nie eine akkreditierte Signatur erworben, fällt dem Signaturschlüssel-Inhaber naturgemäß erheblich schwerer als dem Zertifizierungsdiensteanbieter der positive Beweis der Identifizierung eines vermeintlichen Teilnehmers. In diesem Zusammenhang würde dem Zertifizierungsdiensteanbiter laut Art. 339 CPC und Art. 341, II, CPC als Dritten angeordnet, die Dokumentation bezüglich der Identifikation vorzulegen.

732 Siehe beispielsweise REsp 833.469-RJ, Rel. Min. *Cesar Asfor Rocha*, v. 11.12.2006, REsp 727.843-SP, Rel. Min. *Nancy Andrighi*, v. 01.02.2006, REsp. 651.086, Rel. Min. *Jorge Scartezzini*, v. 20.03.2006, REsp. 784.602-RS, Rel. Min. *Jorge Scartezzini*, v. 01.02.2006, Resp 557.030-RJ, Rel. Min. *Nancy Andrighi*, v.01.02.2005.

einheiten unbekannt. Eine vergleichbare Unsicherheit der Signaturverfahren – besonders der akkreditierten Variante – darf somit nicht vorausgesetzt werden.

Ein weiterer Einwand zur Erschütterung der Vermutung könnte mit dem Argument begründet werden, dass der Signaturschlüssel-Inhaber auf Grund manipulierter Hard- und Softwareumgebung Daten signiert habe, die er nicht hätte signieren wollen. Es handelt sich hierbei um die schon erwähnte Präsentationsproblematik[733], wonach Darstellungen derselben signierten Daten so voneinander abweichen, dass Menschen verschiedene Interpretationen aus ihnen gewinnen.[734] Ursache für unterschiedliche Präsentationen können neben Manipulationen, technische Fehler sowie Varianten der verwendeten Systeme und deren Bedienung sein. Wird ein elektronisches Dokument auf einer fremden Umgebung signiert, dann kann die Wahrscheinlichkeit des Auftretens des Präsentationsproblems erhöht werden.[735] Unabhängig davon, wie dies erfolgt, wird eine Begutachtung der Systemumgebung erforderlich, in welcher das bestrittene elektronische Dokument signiert worden ist. Die Durchführung dieses Nachweises und ihre Bewertung durch das Gericht sind sicherlich keine einfachen Aufgaben. Zum einen darf das Präsentationsproblem nicht als unbegründete Exkulpationsmöglichkeit seitens des Beweisgegners von der Rechtsprechung zugelassen werden. Zum anderen dürfen die Anforderungen zur Erschütterung der Vermutung bezüglich des Präsentationsproblems angesichts der Risiken auf der Anwenderseite[736] nicht zu hoch bewertet werden[737]. Aus diesen Gründen müssen die Nachweise der Schwachstellen der Systemumgebungen des Signierenden akribisch aufgenommen und vom Richter gewürdigt werden.

2.4.3.6 Die Beweisführung mittels transformierter Dokumenten

Eine steigende Tendenz, Dokumente in den drei verschiedenen Formen[738] zu transformieren, ist auch für Brasilien festzustellen. Besonders erwünscht – sowohl bei Behörden als auch bei privaten Unternehmen – ist angesichts der Archivierungspflichten sowie der dazugehörigen Kosten die Transformationsform P-to-E.

Was die Aufbewahrungspflicht anbelangt, sind in der brasilianischen Rechtsordnung keine allgemeinen anwendungsübergreifenden Aufbewahrungsvorschriften zu finden. Einheitliche Anforderungen sind somit nicht vorgesehen. Diese ergeben sich vielmehr aus den für die jeweiligen Bereiche geltenden Regelungen. So bestimmt zum Beispiel Art. 195 als einziger Paragraph des Código Tributário Nacional (Steu-

733 Siehe hierzu bereits in diesem Teil Gliederungspunkt 1.6.5.2.

734 *Pordesch*, DuD 2000, 89.

735 *Fischer-Dieskau* 2006, 139.

736 Über die fehlende öffentliche Bewusstsein für die Risiken auf der Anwenderseite siehe *Fischer-Dieskau* 2006, 140.

737 *Roßnagel*, RMD, Einl. SigG 2001, Rn. 289.

738 Über die Transformationsformen siehe bereits in diesem Teil Gliederungspunkt 1.8.1.

ergesetzbuch), dass die Steuerpflichtigen, welche für die Steuerveranlagung relevante Urkunden nachweisen müssen, diese bis zur Verjährung der entsprechenden rechtlichen Ansprüche aufzubewahren haben. Die Verjährung beträgt gemäß Art. 150, § 4, des Código Tributário Nacional fünf Jahre. Bereits seit Inkrafttreten des Decreto Nr. 6.022 von 22.01.2007 besteht die Möglichkeit, dass Kaufleute und Handelsgesellschaften ihre Handelsbücher und die für die Steuerveranlagung relevanten Unterlagen elektronisch führen. Mit Decreto Nr. 6.022 wurde das so genannte SPED (Öffentliches System für die digitale Buchführung) in die brasilianische Rechtsordnung eingeführt. Im Rahmen des SPED werden die elektronischen Handelsbücher und Unterlagen mit akkreditierten Verfahren signiert (Art. 2, § 1). Verfahrensweisen zum Umgang mit den bereits auf Papier vorhandenen Handelsbüchern und Unterlagen sowie der Möglichkeit einer P-to-E Transformation regelt das „Decreto" jedoch nicht. Sozialversicherungsunterlagen müssen je nach Fall entweder für fünf oder zehn Jahre oder sogar unbefristet[739] aufbewahrt werden. Im Personalbereich müssen Unternehmen bestimmte Unterlagen für mindestens fünf Jahre[740], manchmal für zwanzig[741] Jahre aufbewahren. Einige der Unterlagen sind sogar unbefristet aufzubewahren.[742]

2.4.3.6.1 Gerichtsakten

Aufbewahrungsfristen hinsichtlich Gerichtsakten sind nicht landesweit einheitlich vorgegeben. Ein wichtiger Schritt in die Richtung der Modernisierung der brasilianischen Justiz war die Verabschiedung des Gesetzes Nr. 11.419 am 19.12.2006, welches die Möglichkeit eröffnet hat, dass Verfahrensbeteiligte elektronische Kommunikationsformen rechtswirksam verwenden können.[743] In Art. 11 bestimmt das Gesetz, dass alle elektronischen Dokumente, bei denen die Authentizität im Sinn des Gesetzes gewährleistet wird, als Originale zu behandeln sind. Die Authentizität

739 Wie etwa der Fall von Selbstständigen, die gemäß Art. 45, § 1, Gesetz Nr. 8.212, aus dem Jahre 1991, ihre Beitragsunterlagen bis zur Geltendmachung ihrer Versorgungsansprüche aufbewahren müssen.

740 Diese Frist betrifft etwa die arbeitsvertraglichen Unterlagen, wie im Art. 7, XXIX, CF bestimmt. Die gleiche Frist gilt für die Register, deren Aufbewahrung der Kontrolle durch die zuständige Behörde dient.

741 Wie die Unterlagen über die Krankengeschichte des Arbeitnehmers, gemäß Art. 7.4.5 Erlass SSST Nr. 24/94.

742 Wie Bücher oder Karteikarten mit den Arbeitnehmereintragungen für die zukünftige Berechnung der Arbeitszeit für Rentenzwecke.

743 Die Möglichkeit, elektronische Akten zu führen, bestand schon im beschränkten Rahmen der so genannten Juizados Especiais Federais, vereinfachte Verfahren für die Vergleichung, Verurteilung und Vollstreckung von Fällen mit geringer Komplexität und niedrigem Streitwert. Eingeführt wurde diese Möglichkeit durch das Gesetz Nr. 10.259 aus dem Jahr 2001.

elektronischer Dokumente wird gemäß Art. 1, § 2, III, a und b durch zwei mögliche elektronische Signaturen sicher gestellt. Die erste Möglichkeit (Art. 1, § 2, a) ist die digitale Signatur, welche auf einem digitalen Zertifikat eines akkreditierten Zertifizierungsdiensteanbieters beruht, wie vom speziellen Gesetz geregelt.[744] Die zweite Möglichkeit (Art. 1, § 2, b) ist die Registrierung des Verfahrensbeteiligten gegenüber den entsprechenden Rechtspflegeorganen gemäß der internen Regelungen dieser Instanzen. Diese Regelung ist an der Stelle zu kritisieren, denn als einzige mögliche Authentifizierungsform sollte nur die akkreditierte digitale Signatur akzeptiert werden. Die Variante der Registrierung des Teilnehmers wird wahrscheinlich durch Passwörter implementiert – das Gesetz lässt diese Möglichkeit offen – was zu erkennbaren Unsicherheiten führt. Die pauschale Anerkennung – besonders angesichts der Tatsache, dass die Justiz über ihren eigenen Zertifizierungsdiensteanbieter (AC Jus) verfügt – von unsicheren Identifikationsmitteln wie Passwörter für die rechtsverbindliche Kommunikation zwischen Verfahrensbeteiligten durch ein nationales Gesetz ist unakzeptabel.[745]

Dieser Ansatz stellt im Weiteren ein zusätzliches Problem dar, weil er praktisch offen lässt, wie diese Registrierung durchzuführen ist, das heißt jedes Organ der Rechtspflege entscheidet separat, wie das Verfahren gestaltet wird. Da Brasilien über 88 Gerichte (hier Landgerichte und Bundesgerichte gezählt) verfügt, ist das Entstehen von Wildwuchs sehr wahrscheinlich.[746] Außerdem werden sich Verfahrensbeteiligte bei jedem Gericht, an dem sie ihre Tätigkeiten ausüben, registrieren lassen müssen. Dies wird einen unverhältnismäßig hohen zeitlichen und finanziellen Aufwand erfordern, denn nach Art. 2, § 1 Lei Nr. 11.419 ist die persönliche Mitwirkung bei der Identifizierung und Registrierung (zur möglichen Übergabe des Identifikationsdaten) des Teilnehmers notwendig. Die persönliche Identifizierung an sich ist nicht zu kritisieren, aber gerade dieser Punkt verdeutlicht, wie überflüssig und ungünstig die Registrierung sein kann, wenn man daran denkt, dass die Verfahrensbeteiligten mit einem einzigen akkreditieren Zertifikat im Rahmen der ICP-Brasil Zugang zu den virtuellen Angeboten aller Gerichte haben könnten. Zur Erlangung eines Zertifikats ist nur ein einziger persönlicher Kontakt erforderlich, was unter wirtschaftlichen Aspekten positiv zu bewerten ist.[747] Des Weiteren könnte der Teilnehmer mit diesem Zertifikat auf alle Justizanwendungen landesweit und ohne weitere Identifizierungen zugreifen.

744 In diesem Zusammenhang kann als spezielles Gesetz nur die MP 2.200-2 in Frage kommen.

745 Auch kritisch zu der Möglichkeit der so genannten Registrierung als Authentifizierungsform, *Calmon* 2007, 62 ff.

746 *Calmon* 2007, 64.

747 Gemäß Art. 7 MP 2.200-2 und Art. 3.2.2, b, Resolução Nr. 42. Hierzu auch bereits im 2. Teil Gliederungspunkt 2.2.7.

2.4.3.6.2 Die Transformation P-to-E

Das Gesetz Nr. 11.419 hat eine Transformation P-to-E pauschal zugelassen, indem es im Art. 11 § 1 festgelegt hat[748], dass digitalisierte Dokumente, die von Organen der Rechtspflege, Staatsanwaltschaft, Polizeibehörden, Behörden und Rechtsanwälten zu den elektronischen Akten beigefügt werden, die gleiche Beweiswirkung wie Papieroriginale haben. Die begründete Behauptung der Verfälschung vor oder während des Scannprozesses bleibt aber vorbehalten. Die Vorschrift nennt nicht die Möglichkeit des Bestreitens der Echtheit des Zieldokuments nach der Transformation. Da Anforderungen zur Integritätssicherung des Zieldokuments – etwa durch Anwendung digitaler Signaturen – nicht vorgesehen sind, ist eine nach der Transformation durchgeführte Manipulation des Zieldokuments nicht nur technisch möglich, sondern auch wahrscheinlich. Das Gesetz muss somit so interpretiert werden, dass die Behauptung der Manipulation des Zieldokuments auch nach der Transformation zugelassen bleibt.

Die Möglichkeit der Vernichtung der Originale wurde vom Gesetz Nr. 11.419 sachgerecht nicht vorgesehen.[749] Nach Art. 11 § 3 sind alle in elektronische Form konvertierte Originale bis zum Eintritt der Rechtskraft des Urteils[750] oder, wenn statthaft, bis zum Ablauf der Frist zur Wiederaufnahmeklage aufzubewahren. Anzumerken ist jedoch, dass diese Vorschrift sich nur auf einen konkreten Prozess bezieht. Ein Dokument – wie etwa ein komplexer Vertrag – kann potenziell mehrere Rechtsansprüche begründen. Werden alle diese nicht auf einmal geltend gemacht, das heißt im ersten Prozess, dann soll das entsprechende Dokument auch nach dem Ablauf der Frist zur Wiederaufnahmeklage weiter aufbewahrt werden. Wird das Dokument aber vernichtet und eine zweite oder eine dritte auf das vernichtete Original begründete Klage erhoben, dann droht dem Beweisführer der Prozessverlust.

2.4.3.6.3 Andere Transformationsformen

Die zwei anderen Transformationsformen – nämlich die Transformation E-to-E und E-to-P – werden im Gesetz Nr. 11.419 nicht vorgesehen. Der Gesetzgeber hat die Chance verpasst, diese näher zu regeln. Da die Verfahrensbeteiligten immer häufiger ihre Anträge elektronisch ausfertigen und gleichzeitig elektronische Akten in der Justiz noch nicht verbreitet sind, wäre eine Vorschrift sinnvoll, welche die Möglich-

748 Die Vorschrift ändert Art. 365 CPC, indem sie die vier neuen Bestimmungen (Nr. V, VI, § 1 und § 2) einführt.

749 Hierzu bereits in diesem Teil Gliederungspunkt 1.8.7, besonders in Bezug auf die Ergebnisse der Atlas-Studie.

750 Eine ähnliche Vorschrift stellt § 298a Abs. 2 Satz 2 ZPO dar, wonach die Unterlagen, sofern sie in Papierform weiter benötigt werden, mindestens bis zum rechtskräftigen Abschluss des Verfahrens aufzubewahren sind.

keit der Fertigung von Ausdrucken elektronischer Dokumente unter bestimmten Voraussetzungen für die noch im Papier geführten Akten zulässt. Für die elektronisch geführten Akten wäre auch eine Vorschrift denkbar, welche die Transformation E-to-E zulässt. Dies dürfte erforderlich sein angesichts der verschiedenen Datenformate elektronischer Dokumente, die potenziell an die Gerichte von den Verfahrensbeteiligten überreicht werden können. Die Gerichte werden stets versuchen, alle ankommenden elektronischen Dokumente in ihr In-House-Format zu konvertieren. Um diese Problematik zu umgehen, könnten die Justizverwaltungen regeln, dass nur In-House-Formate angenommen werden. Dadurch verschöbe sich das Problem jedoch nur um wenige Jahre, denn der Formatwechsel ist unabdingbar zum Erhalt der Lesbarkeit elektronischer Dokumente angesichts der technologischen Entwicklung, welche die Lesefähigkeit der am Markt verfügbaren Software innerhalb kürzester Zeit nicht mehr deckt.

2.4.3.6.4 Der Beweiswert des transformierten Zieldokuments

Angesichts des Mangels allgemeiner anwendungsübergreifender und bereichsspezifischer Transformationsvorschriften – ausgenommen die in Bezug auf Transformation vom Papier zu einem elektronischen Dokument im Rahmen des Gesetzes Nr. 11.419 –, welche zum einem die Transformation zulassen und zum anderen konkrete Anforderungen und Formulierungen festlegen, unterliegen die aus einer Transformation resultierenden Zieldokumente der freien Beweiswürdigung des Art. 332 CPC.

Zu beachten ist hier auch Art. 383 CPC. Dem zufolge beweisen mechanische Wiedergaben, wie etwa Fotos, Filme und Töne, unter anderem die Tatsachen oder Sachen, welche sie nachbilden. Der Beweis kann aber vom Gericht nur angenommen werden, wenn der Beweisgegner ihn nicht bestreitet.[751] Nach Art. 383 Einziger Paragraph CPC ordnet das Gericht eine Begutachtung durch Sachverständige an, wenn die Authentizität der mechanischen Wiedergabe bestritten wird. Der Código Civil enthält fast die gleiche Vorschrift, aber anstelle des offenen Begriffs „unter anderem" verwendet er die modernere Formulierung „elektronische Wiedergabe", um klar zu stellen, dass diese als Beweismittel zugelassen sind. Die Beschränkung in Bezug auf das Nichtbestreiten der Wiedergabe durch den Beweisgegner bleibt jedoch. In die gleiche Richtung tendiert Art. 223 CC, der über den Beweiswert der Fotokopie eines Dokuments bestimmt. Hierbei gilt die beglaubigte Fotokopie eines Dokuments als Beweis einer Willenserklärung. Wird aber ihre Authentizität bestritten, muss das Original vorgebracht werden. Auf das gescannte Dokument könnten diese Vorschriften angewandt werden. Ihre Systematik legt aber deutlich fest, dass dem Zieldokument eine relative Beweiskraft zugeordnet wird. Grund hierfür ist die Notwendigkeit, Originale beizubringen, falls die Authentizität der mittels der Transformation erlangten digitalisierten Dokumente bestritten würde.

751 *Pontes de Miranda* 2001, 385.

Das Dokumentenbeweisverfahren sieht als Grundsatz die Vorlage des Originals vor. Das ergibt sich aus Art. 365 CPC, der die Dokumente aufzählt, deren Beweiskraft des einen Originals entspricht. Hierbei sind zahlreiche Ausnahmen vorgesehen, wie zum Beispiel Bescheinigungen der Geschäftsstellen über jegliche Aktenstücke, die zu den Akten beigefügt werden (Art. 365 Abs. 1 CPC) oder Wiedergaben öffentlicher Dokumente, es sei denn, dass diese von einer Person mit öffentlichem Glauben beglaubigt wurden (Art. 365 Abs. 3 CPC). Handelt es sich nicht um eine solche Ausnahme, dann müssen die Parteien die Originale vorlegen. Hierbei ist zu beachten, dass die Letzteren nach dem Verständnis in der Praxis immer einen höheren Beweiswert aufweisen, obwohl in diesen wenigen Fällen manche Dokumente den Originalen gleichgestellt werden.[752] Dieses basiert auf der Tatsache, dass etwa zur Ausfertigung einer Bescheinigung der Eingriff eines Dritten immer notwendig ist, da die Wiedergabe nicht immer den ganzen Inhalt nachbildet. Ein Unterschied zum Original ist häufig feststellbar.

2.4.3.7 Die automatisierte erzeugte elektronische Signatur

Zu untersuchen ist auch inwieweit die Medida Provisória Nr. 2.200-2 und ihre Nebenvorschriften die Erzeugung automatisiert hergestellter elektronischer Signaturen zulassen und was für eine Beweiswirkung diese Signaturen haben. Überfprüft werden muss, ob die automatisierte Signatur gegen konstitutive Anforderungen des akkreditierten Verfahrens verstößt. Wie schon dargestellt[753], legt das brasilianische Signaturrecht die konstitutiven Anforderungen nicht in einer übersichtlichen Weise fest, sondern verteilt diese auf verschiedene Stellen der Regulierung. Folgende Anforderungen können als konstitutiv für eine akkreditierte Signatur betrachtet werden:

- das Schlüsselpaar muss vom Signaturschlüssel-Inhaber selbst erzeugt werden (Art. 6, einziger Paragraph MP 2.200-2),
- der private Schlüssel steht in der alleinigen Kenntnis, Kontrolle und Nutzung des Signaturschlüssel-Inhabers (Art. 6, einziger Paragraph MP 2.200-2) sowie
- die Benutzung einer der im Art. 6.1.1.7 Resolução Nr. 41 ernannten Signaturerstellungs- und Signaturspeicherungseinheiten durch den Signaturschlüssel-Inhaber. [754]

In Bezug auf die erstgenannte Anforderung, nach der das Schlüsselpaar selbst vom Signaturschlüssel-Inhaber erzeugt wird, bereitet die automatisierte Signatur

752 *Marinoni*/*Arenhart* 2005, 275.

753 Siehe hierzu bereits im zweiten Teil Gliederungspunkt 2.2.9.

754 Zu den möglichen Signaturspeicher- und Signaturerzeugungsmittel im Rahmen der ICP-Brasil siehe bereits im zweiten Teil Gliederungspunkt 2.2.9.1.2.1.

kein Problem. Wie bereits dargelegt[755], wird im brasilianischen Signaturrecht großen Wert darauf gelegt, dass der Antragsteller selbst sein eigenes Schlüsselpaar erzeugt. Dass diese Regel befolgt wird, liegt nicht nur im Interesse des Zertifikatinhabers, sondern auch in dem des Zertifizierungsdiensteanbieters, denn durch die Schlüsselpaargenerierung beim Zertifikatsinhaber bleibt der Einwand, das Trustcenter habe den privaten Schlüssel des Teilnehmers bei der Schlüsselpaarerzeugung kopiert und missbraucht, praktisch ausgeschlossen. Für die Erzeugung automatischer Signaturen stellt die hier erörterte Anforderung kein Hindernis dar, da die Schlüsselpaargenerierung sowohl für normale Signaturen im Einzelfall als auch für die im automatischen Prozess erzeugten Signaturen eine Vorbedingung ist.

Die beiden letzteren Anforderungen stehen in enger Beziehung zueinander. Zur Erfüllung der Anforderung der alleinigen Kenntnis, Kontrolle und Nutzung des privaten Schlüssels muss der Zertifikatsinhaber geeignete sichere Chipkarten, Softwarelösungen[756] oder Sicherheitstoken verwenden, welche über Mechanismen verfügen, die vor dem Zugriff Unberechtigter schützten. Darüber hinaus darf die Signaturerstellungseinheit laut Art. 6.1.1.7 Resolução Nr. 41 nicht verhindern, dass die zu signierenden Daten dem Signierenden vor dem Signaturvorgang angezeigt und verändert werden können. Was nicht von den Regelungen bestimmt wird, aber zur Gewährleistung der Kontrolle der Signatur implementiert werden kann, ist die Einrichtung von Zeitfenstern, welche die Anzahl von Signaturen auf einen bestimmten Zeitraum beschränken.[757]

Zu erwähnen ist außerdem, dass das brasilianische Signaturrecht die Zuordnung eines Zertifikats zu juristischen Personen, Automaten und funktionalen Einheiten wie Servern vorsieht.[758] Dies trägt beispielsweise dazu bei, den Einsatz digitaler Signaturen innerhalb von Unternehmensabläufen zu implementieren, denn so werden Konstruktionen wie zum Beispiel der Abschluss innerbetrieblicher Haftungsübernahmeregelungen und die Weitergabe der PIN zur Aktivierung der Karte für den Fall eines Mitarbeiterwechsels vermieden.[759] Außerdem helfen Zertifikate für Automaten und Server, die Transparenz für den Empfänger elektronisch signierter Dokumente zu verstärken.

Es kann somit festgehalten werden, dass die automatisierte elektronische Signatur – erzeugt unter Anwendung akkreditierter Verfahren – auf keine Hindernisse sowohl

755 Siehe hierzu bereits im 2. Teil Gliederungspunkt 2.2.9.1.6.

756 Dass Softwarelösungen nicht geeignet sind, um die notwendige Sicherheit des Nutzers zu gewährleisten, ist nicht Gegenstand des hier erörterten Themas. Zu einer kritischen Analyse der Softwarelösungen im Rahmen der ICP-Brasil siehe bereits im zweiten Teil Gliederungspunkt 3.3.

757 Hierzu siehe die Ausführungen zur automatisierten Signatur im deutschen Signaturrecht, bereits in diesem Teil unter Gliederungspunkt 1.10.

758 Siehe hierzu bereits im 2. Teil Gliederungspunkte 2.2.9.1.5 und 3.7.

759 *Roßnagel*/*Fischer-Dieskau*, MMR 2004, 139.

von Seiten der MP 2.200-2 als auch von den Nebenvorschriften stößt. Somit kommt dieser der gleiche Beweiswert zu, wie einer normal im Einzelfall erzeugten Signatur.

3. Vergleich und Vorschlag zur Rezeption

3.1 Der unterschiedliche Urkundenbegriff

Das deutsche und das brasilianische Recht verwenden unterschiedliche Begriffe von Urkunde und Dokument. An dieser Stelle ist das deutsche Recht präziser. Anders als die deutsche kennt die brasilianische Rechtsordnung keine Differenzierung zwischen den Bezeichnungen „Dokument" und „Urkunde". In der Tat gibt es nur ein Wort: Das Wort „documento" bedeutet ein Beweismittel, durch das etwas ausgedrückt wird. Es gibt keinen Begriff wie den der Urkunde, welcher die Verkörperung der Gedankenerklärungen voraussetzt.

Eine digitale Signatur (assinatura digital) sowie ein elektronisches Dokument (documento eletrônico) würden bei einer buchstabengetreuen Auslegung durchaus durch die Begriffe „assinatura" und „documento" erfasst werden. Der Begriff „documento" könnte im brasilianischen Recht sowohl für eine Urkunde im Sinn des deutschen Rechts stehen[760], sowie auch als Oberbegriff für alle Dokumentarten aufgefasst werden können. Im brasilianischen Recht existiert keine dem deutschen Recht entsprechende Differenzierung zwischen den beiden Begriffen. Des Weiteren muss ein „documento" nicht unbedingt eine Verkörperung darstellen, also an ein Material gebunden sein, welches mit den Händen greifbar wäre. Das Gleiche gilt für den Begriff „assinatura", welcher ebenso nicht ausschließlich auf eine handschriftliche Unterschrift beschränkt sein muss. Dieser kann eine gewisse Flexibilität aufweisen und beispielsweise auch den Begriff der digitalen Signatur (assinatura digital) erfassen.

Dieser Unterschied führt zu einem prinzipiell ungleichen Ansatz zwischen beiden Ländern hinsichtlich der Notwendigkeit, eine beweisrechtliche Regelung einzuführen. Angesichts der erwähnten Offenheit der Begriffe „assinatura" und „documento" wäre in Brasilien die Einführung einer spezifischen beweisrechtlichen Vorschrift für elektronische Dokumente im Prinzip nicht notwendig. In Deutschland dagegen war von Anfang an klar, dass elektronisch signierte Daten nicht mit Urkunden gleichzusetzen sind und diese deshalb nicht im Rahmen des Urkundenbeweises gemäß §§ 415 ff. ZPO vorgelegt werden können.[761] Die beweisrechtlichen Nachteile der Signaturempfänger könnten somit entweder durch den Augenschein nach § 371 ff. ZPO[762] oder durch die Sicherheitsvermutung des § 1 Abs. 1 SigG 1997 aufgehoben

760 Zur Definition einer Urkunde im deutschen Recht siehe bereits im 3. Teil Gliederungspunkt 1.4.2.1.

761 *Roßnagel*, in: ders., RMD, Einl. SigG 2001, Rn. 39.

762 *Roßnagel* 1992, 41.

werden.[763] Dennoch wurde ein Anscheinsbeweis für qualifiziert signierte Erklärungen mit § 292a ZPO geschaffen, welcher mit dem Inkrafttreten des Justizkommunikationsgesetzes im § 371a Abs. 1 Satz 2 ZPO konsolidiert wurde. Bei der Schaffung der Beweisvorschrift wurde auf die Stärkung der Rechtssicherheit und der Verkehrsfähigkeit der elektronischen Signatur sowie auf das Vertrauen in den elektronischen Rechtsverkehr gezielt geachtet.[764]

3.2 Die Schwächen der geltenden brasilianischen Beweisvorschrift

Die Darstellung des brasilianischen Beweisrechts hat gezeigt, dass die aktuelle Rechtslage von Rechtsunsicherheit geprägt ist. Grundsätzlich sind zwei Rechtsquellen für das Bestreiten einer mittels akkreditierter Signaturverfahren signierten Datei anwendbar: § 1º Art. 10 MP 2.200-2 oder Art. 389, II, CPC. Während § 1º Art. 10 MP 2.200-2 eine widerlegliche Vermutung der Echtheit begründet, welche vom Signaturschlüssel-Inhaber entkräftet werden muss, trägt dagegen bei der Geltendmachung von Art. 389 Abs. 2 CPC der Signaturempfänger die Beweislast beim Bestreiten einer Signatur.

Weiterhin fördert die Rechtsunsicherheit die Tatsache, dass die Beweisregelungen bezüglich elektronisch signierter Daten in Form einer Medida Provisória gelten. Obschon eine solche Gesetzesart auch in Rechtsordnungen von Ländern wie Portugal, Griechenland, Spanien und Italien zu finden ist[765], stellt sie nicht die am besten geeignete Form dar, eine Beweisvorschrift einzuführen. Die strukturellen Schwächen der Medidas Provisórias werden deutlich, betrachtet man die Tatsache, dass sie zwar als formelles Gesetz gelten, jedoch allein vom Bundespräsidenten beschlossen werden. Daraus ergibt sich ein Legitimationsproblem, welches durch den exzessiven Gebrauch der Medidas Provisórias verschärft wird. Dies stößt oft auf Kritik mit dem Vorwurf eines Demokratiedefizits und der Hypertrophie der Exekutivgewalt.[766]

Mangelt es darüber hinaus einer so wichtigen Regelung wie die zum Beweiswert elektronisch signierter Daten an Übersicht[767], wird sie durch eine Medida Provisória festgesetzt und nicht in ein normales Gesetz oder Gesetzbuch eingeführt. Es ist hierbei zu berücksichtigen, dass Brasilien über mehr als 580.000 Rechtsanwälte ver-

763 *Roßnagel*, NJW 1998, 3312.

764 BT-Drs. 14/4987, 13.

765 Siehe hierzu im 2. Teil Gliederungspunkt 2.1.

766 *Paul* 1999, abrufbar unter: http://www.dbjv.de/dbjv-high/mitteilungen/99-01/text_05.html.

767 Nach der Reform zum Erlass von Medidas Provisórias aus dem Jahr 2001 hat der Präsident Fernando Henrique Cardoso monatlich im Durchschnitt 6,8 Medidas Provisórias erlassen. Der Präsident Luiz Inácio Lula da Silva erlässt monatlich im Durchschnitt 5,36 Medidas Provisórias. Hierzu *Coelho* 2007, 63.

fügt[768], ohne dass jedoch eine einheitliche hochqualitative Ausbildung zugrunde liegt. Angesichts der brasilianischen Hochschulzugangspolitik[769] sind landesweit unzählige juristische Fakultäten verbreitet[770], sodass die Qualität von Dozenten und Studenten nicht überall effektiv kontrolliert und gewährleistet wird. Diese nicht selten unvorbereiteten Studenten werden mit der Zeit Rechtsanwälte. Für sie gilt, je unübersichtlicher die Rechtsordnung, desto mehr wird ihnen die Arbeit erschwert, was zur Verschlechterung ihrer Dienstleistungen und des gesamten anwaltlichen Berufes führen kann. Die Regulierung über die technisch-organisatorischen Rahmenbedingungen für elektronische Signaturen und besonders über den Beweiswert elektronisch signierter Daten mittels einer Medida Provisória leistet keinen Beitrag zur notwendigen Vereinfachung sowie zur Übersicht der brasilianischen Rechtsordnung.

Auch der Name „medida provisória" („provisorische Maßnahme" oder „provisorischer Erlass") erzeugt kein Vertrauen. Im Gegenteil: es wird eine vorläufige Lösung signalisiert, die aber schon seit fast sieben Jahren gilt und dadurch zu Verunsicherungen führt.

Des Weiteren ist hier ebenso zu berücksichtigen, dass der von der brasilianischen Literatur vorgeschlagene Ansatz[771], Auslegungsversuche zu unternehmen statt neue Regelungen für den elektronischen Rechtsverkehr zu schaffen, nicht alle Probleme des neuen Mediums löst. Besonders im Bereich der Beweis- und Formvorschriften sind stabile und übersichtliche Rechtssätze erforderlich. Die Entwicklung dieser Vorschriften der Rechtsprechung allein zu überlassen wäre mit Unsicherheiten ver-

768 Nach Angaben der Ordem dos Advogados do Brasil (die Bundesrechtsanwaltskammer Brasiliens) verfügt das Land über 586.829 zugelassene Rechtsanwälte. Siehe hierzu http://www.oab.org.br/relatorioAdvOAB.asp. Deutschland hat nach Angaben der Bundesrechtsanwaltskammer 146.906 zugelassene Rechtsanwälte; hierzu http://www.brak.de/seiten/pdf/Statistiken/2008/gesamt50-2008.pdf.

769 Der brasilianische Hochschulzugang zeichnet sich durch die Besonderheit der Aufnahmeprüfungen aus. Der Kandidat sucht sich eine Hochschule aus, wo er die Aufnahmeprüfung ablegt. Die Prüfungen sind in der Regel schwieriger bei den öffentlich-rechtlichen Universitäten, welche vom Studenten nicht bezahlt werden.

770 In Brasilien sind laut der Statistik aus dem Jahr 2005 vom Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) 861 juristische Fakultäten für eine gesamte Bevölkerung von ungefähr 190 Millionen Einwohnern in Betrieb. Allein die Stadt Rio de Janeiro verfügt über 56 juristische Fakultäten. Zu der brasilianischen Statistik siehe http://www.publicacoes.inep.gov.br/resultados.asp?cat=6&subcat=6# → Censo da educação superior → sinopse estatística 2005 n. 3, S. 161. S. hierzu auch: http://conjur.estadao.com.br/static/text/26375,1.

In Deutschland gibt es 44 juristische Fakultäten für 82 Millionen Einwohner. In den Vereinigten Staaten aus Nordamerika sind es 180 juristische Fakultäten für eine Bevölkerung von 300 Millionen Einwohnern.

771 Siehe hierzu bereits in diesem Teil Gliederungspunkt 2.4.

bunden. In manchen Fällen dauert es Jahre oder sogar Jahrzehnte bis eine Auffassung in den Gerichten konsolidiert ist.[772] Ferner gilt eine bindende Kraft von Präjudizien im brasilianischen Recht grundsätzlich nicht. Zwar berücksichtigen brasilianische Richter die Entscheidungen anderer Gerichte, jedoch existiert wie bereits angemerkt keine einheitliche konsolidierte Vorgehensweise bei Präjudizien. Die Parteien berufen sich zwar in der brasilianischen Gerichtspraxis oft auf Präjudizien – besonders auf die Entscheidungen der höheren Gerichte. Die sind jedoch nicht bindend. Ihnen wird von Richtern oftmals gefolgt, besonders aus praktischen Gründen, die mit dem System der Rechtsmittel zusammenhängen. Da Richter üblicherweise nicht wollen, dass ihre Entscheidungen durch die höheren Instanzen aufgehoben werden, stützen sie sich auf die Autorität von Präjudizien höherer Gerichte.[773]

3.3 Vorschlag zur Novellierung des Código de Processo Civil

Empfehlenswert wäre, dass – wie Deutschland – Brasilien in diesem Zusammenhang eine beweisrechtliche Vorschrift in den Código de Processo Civil einführt, wonach klar geregelt wird, welchen Beweiswert akkreditiert signierten Dokumenten zugerechnet wird. Die Platzierung der Vorschrift in den Código de Processo Civil dient der Übersicht und Rechtssicherheit, welche bei der aktuellen gesetzlichen Lage nicht gegeben sind. Wird der Gesetzentwurf Nr. 7.316/2002 vom Parlament verabschiedet, dann verbessert sich diese Lage nur bedingt. Durch die Verabschiedung des Entwurfes wird ein spezielles Gesetz zum Signaturrecht und zum Beweiswert elektronisch signierter Daten geschaffen, was sehr wichtig als Signal für die Bedeutung der Bestimmungen ist. Zur optimalen Übersicht der Beweisvorschrift mit einem Gewinn an Rechtssicherheit wäre aber die Einführung dieser Vorschrift in den Código de Processo Civil zu empfehlen. Einen solchen Ansatz hat beispielsweise das Gesetz Nr. 11.419 zu Recht verfolgt[774], welches durch die Änderung einiger Vorschriften des Código de Processo Civil die umfassende elektronische Aktenbearbeitung innerhalb des Gerichts ermöglicht.

Nach der aktuellen Fassung des Gesetzentwurfs Nr. 7.316/2002 wird eine ähnliche Beweisvorschrift wie Art. 10 § 1 MP 2.200-2 vorgesehen. Es handelt sich um Art. 4 Gesetzentwurf Nr. 7.316, der die Gleichstellung akkreditierter elektronischer Signaturen zu handschriftlichen Unterschriften gemäß Art. 219 des Código Civil bestimmt. Die Basis der Medida Provisória wird infolgedessen mit der bereits erwähnten Problematik der Rechtsunsicherheit erhalten. Denn selbst wenn die Bestimmung des Entwurfs, so wie die der Medida Provisória einen direkten Verweis auf die Normen zur eigenhändigen Unterschrift vornimmt, bleibt die Möglichkeit

772 Beispiel hierfür ist die Diskussion innerhalb der brasilianischen Rechtsprechung über den Verbraucherbegriff.

773 Siehe hierzu *Zajtay* 1976, 81 f.

774 Siehe hierzu bereits im 3. Teil Gliederungspunkt 2.4.3.6.1.

der Anwendung der Beweisregelung des Código de Processo Civil über das Bestreiten der Unterschrift (Art. 389 Abs. 2 CPC) offen.

Um diese Rechtsunsicherheit zu beseitigen, könnte eine Vorschrift mit folgender Formulierung in den Código de Processo Civil eingeführt werden:

„Art. 368-A. Elektronische Dokumente, die mit einer als echt geprüften akkreditierten elektronischen Signatur im Rahmen der Infra-Estrutura de Chaves Públicas versehen sind, haben die Vermutung der Echtheit für sich. Die Vermutung kann durch Tatsachen widerlegt werden, die ernstliche Zweifel daran begründen, dass die zugrunde liegende Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist."[775]

Die Vorschrift wäre besser im Titel – Seção V - Da Prova Documental Subseção I, Da força probante dos documentos – über dem Beweiswert von Dokumenten platziert.

Der erste Satz des Vorschlags begründet eine Vermutung *juris tantum* der Echtheit der mittels eines akkreditierten Verfahrens signierten Erklärung. Im Vergleich zur geltenden Vermutung des Art. 10 § 1 MP 2.200-2 wird das Element der Echtheit hinzugefügt. Die vorgeschlagene Vorschrift geht infolgedessen einen Schritt weiter als die Vermutung zu Gunsten unterschriebener Dokumente, indem sie die Eigenschaft der Integrität einbezieht. Diese Erweiterung der Vermutung ist auf die Technik kryptografischer Verfahren[776] zurückzuführen, die nachträglich erkennen lässt, ob das elektronische Dokument nach der Signierung verändert wurde.

Der zweite Satz basiert auf der Formulierung des § 371a Satz 2 ZPO und signalisiert, dass zur Erschütterung der Vermutung Tatsachen erforderlich sind, die einen abweichenden Geschehensablauf als möglich begründen. Diese Formulierung ist sachgerecht und gewährleistet das notwendige Gleichgewicht zwischen dem Schutz des Erklärungsempfängers gegen unbegründete Einwände des Beweisgegners – durch den Ausdruck der „ernstlichen Zweifel" – und der Garantie der Verteidigung des Signaturschlüssel-Inhabers für die Fälle, in denen er tatsächlich die bestrittene Erklärung nicht abgegeben hat. Anders als § 292 Satz 1 ZPO gilt im brasilianischen Beweisrecht nicht das Gebot des Beweises des Gegenteils für die Neutralisierung einer gesetzlichen Vermutung.[777] Der Unterschied zwischen Beweis des Gegenteils und Gegenbeweis ist dem brasilianischen Recht fremd. Für die Widerlegung der Vermutungsbasis ist infolgedessen keine volle Überzeugung des Richters erforderlich. Was vom Beweisgegner vorgetragen wird, muss allerdings nachgewiesen werden und zu einem plausiblen Schluss auf die mangelnde Echtheit der signierten

775 In der portugiesischen Sprache würde der Vorschlag folgender Formulierung entsprechen: „Os documentos eletrônicos assinados mediante assinatura eletrônica credenciada no âmbito da ICP-Brasil têm a sua autoria e integridade presumida. Esta presunção pode ser afastada por meio de fatos que levantem dúvidas fundadas de que a declaração subjacente não tenha sido feita pelo titular da chave de assinatura".

776 Siehe hierzu bereits im 1. Teil Gliederungspunkt 4.3.

777 Zum Beweis des Gegenteils im deutschen Recht siehe im 3. Teil Gliederungspunkt 1.2.5.

Erklärung führen. Bei den möglichen Einwänden gegen die Vermutung werden folglich – so wie bei Art. 10 § 1 MP 2.200-2 – keine Grenzen gezogen.[778]

Wird die hier vorgeschlagene Vorschrift in das Código de Processo Civil eingeführt, dann wäre es nicht mehr möglich Art. 389 Abs. 2 CPC für das Bestreiten einer elektronisch signierten Erklärung anzuwenden. Denn es würde eindeutig klargestellt, dass bei der Widerlegung der Echtheit einer unterschriebenen Erklärung Art. 389 Abs. 2 CPC anwendbar wäre und dass bei der Widerlegung der Echtheit einer elektronisch akkreditiert signierten Erklärung der hier empfohlen Art. 368-A CPC beachtet werden müsse. Die heutige bestehende Möglichkeit einer Partei, sich je nach der Situation und nach dem erwünschten Ergebnis entweder auf Art. 389 Abs. 2 CPC oder auf Art. 10 § 1 MP 2.200-2 zu berufen, ist nicht mehr gegeben. Im Fall wie etwa des Diebstahls oder Raubes der Signaturkarte muss der Beweisführer (meistens der Signaturempfänger) seinen Anspruch geltend machen, indem er die signierte Erklärung einschließlich des Zertifikats dem Gericht vorlegt. Um die Signaturprüfung dem Gericht zu ermöglichen, muss der Beweisführer die Datei in einer für das Gericht lesbaren Version beibringen. Die Vermutung der Echtheit kann vom Beweisgegner (in dem Fall der Signaturschlüssel-Inhaber) entkräftet werden, wenn es ihm gelingt, Tatsachen nachzuweisen, die im konkreten Fall auf das Vorkommen eines Diebstahls oder Raubes zurückzuführen sind. Er muss dann beispielsweise nachweisen, den Diebstahl oder Raub rasch nach dem Ereignis bei der Polizei angezeigt zu haben. Zudem ist ebenso der Beweis zu erbringen, den Antrag auf Sperrung des Zertifikats schnellstmöglich abgegeben zu haben.

Als Ergebnis wird festgestellt, dass der Vorschlag gleichzeitig einen Beitrag für mehr Übersicht und Rechtssicherheit schafft, indem die Beweisvorschrift in dem Código de Processo Civil und nicht in einer Medida Provisória platziert wird. Überdies sollte der direkte Verweis auf die Normen zur eigenhändigen Unterschrift des Código Civil abgeschafft werden, um damit eine autonome Regel für die Beweiswirkung akkreditierter elektronischer Signaturen zu implementieren. Schließlich schafft der Vorschlag, durch die auf den § 371a Satz 2 ZPO basierende Formulierung „ernstliche Zweifel", einen Maßstab für die Entkräftung der widerleglichen Vermutung der Echtheit akkreditiert elektronisch signierter Erklärungen, der zwar konkretisiert werden muss, aber zugleich einen Anhaltspunkt für eine gerechte Lösung der Beweisproblematik mittels elektronischer Signaturen gibt.

4. Zusammenfassung

Die Untersuchung des brasilianischen und des deutschen Signaturrechts hat gezeigt, dass beide Systeme ähnlichen Ansätzen folgen. Beide Länder verfügen über eine breite Infrastruktur für öffentliche Schlüssel mit einer zuständigen Behörde an der Spitze der Hierarchie ihrer Zertifizierungsdienste. Sowohl die Bundesnetzagentur in

778 Für Beispiele von Einwänden siehe im 3. Teil Gliederungspunkt 2.4.3.5.

Deutschland als auch das brasilianische Instituto Nacional de Tecnologia da Informação akkreditieren nach einer entsprechenden Prüfung den Betrieb der Zertifizierungsdiensteanbieter. Weiterhin obliegen beiden Behörden Aufsichtsaufgaben in Bezug auf akkreditierte Anbieter in Brasilien sowie auf akkreditierte und angezeigte Anbieter in Deutschland.

Die Pflicht der brasilianischen akkreditierten Zertifizierungsdiensteanbieter, die Zertifikate der Signaturschlüssel-Inhaber für einen unbefristeten Zeitraum aufzubewahren, ist nicht sachgerecht. Diese kann unnötige Kosten und Aufwand verursachen, da nicht alle Anwendungen – wie etwa Bankapplikationen – die langzeitige Aufbewahrung öffentlicher Schlüssel und Zertifikate für spätere Überprüfungen von Signaturen erforderlich machen. Unter diesem Aspekt ist die Regelung des deutschen Signaturrechts für akkreditierte Verfahren vernünftiger, welche eine Aufbewahrungsfrist von mindestens 30 Jahren festlegt. Wird die Aufbewahrung für einen längeren oder sogar unbefristeten Zeitraum gefordert, kann entweder das spezielle Gesetz des Bereiches dies bestimmen oder die Interessenten können nach Bedarf gesonderte Vereinbarungen treffen.

Qualifizierte Zertifikate können nach dem deutschen Signaturrecht (§ 2 Nr. 9 SigG) nur auf natürliche Personen ausgestellt werden. Grund für diesen Ansatz ist das Argument, dass qualifizierte Signaturen die gleiche Wirkung wie eine eigenhändige Unterschrift haben und deshalb wie diese immer an eine natürliche Person gebunden werden müssen. Hierbei wird jedoch außer Acht gelassen, dass nicht in allen Anwendungen die Signatur als Schriftformersatz genutzt wird, wie das erwähnte Beispiel der SSL-Server-Zertifikate-Signaturen verdeutlicht, welche die zuverlässige Authentifizierung von Webservern im Browser des Internetnutzers ermöglichen. Da keine europarechtlichen Hindernisse auf dem Weg zu Zertifikaten für juristische Personen liegen, sollte Deutschland eine ähnliche Regelung wie Art. 1.1.5 Resolução Nr. 41 einführen, wonach die Zuordnung von Zertifikaten für natürliche und juristische Personen sowie für Anwendungen, Automaten und funktionale Einheiten möglich ist.

Das brasilianische Signaturrecht verfügt über keine spezielle Vorschrift zur Unterrichtungspflicht der Zertifizierungsdiensteanbieter gegenüber den Antragstellern für akkreditierte Signaturverfahren. Diese Pflicht muss aus den allgemeinen Vorschriften des Código de Defesa do Consumidor hergeleitet werden. Diese reichen jedoch für die Komplexität der Verwendung elektronischer Signaturen nicht aus. Die Unterrichtungspflicht des deutschen Signaturrechts könnte hierfür in das brasilianische Signaturrecht eingeführt werden. Besonders hervorzuheben in der deutschen Unterrichtungspflicht sind die Punkte, über welche der Zertifizierungsdiensteanbieter den Antragsteller informieren muss. Besonders beachtenswert sind dabei die Maßnahmen, welche zur sicheren Anwendung elektronischer Signaturen notwendig sind. Außerdem ist über die Notwendigkeit einer erneuten Signatur für signierte Dokumente, welche langfristig aufzubewahren sind, ebenso zu informieren, wie über die rechtlichen Wirkungen der generellen Anwendung elektronischer Signaturen.

Eine weitere Schwäche des brasilianischen Signaturrechts ist, dass kein Verfahren zur Neusignierung signierter Daten normiert wird. Die Darstellung der deutschen Signaturregelungen hat gezeigt, dass die Neusignierung für Dokumente, die langfristig beweiskräftig aufzubewahren sind, unabdingbar ist. Dies weil – anders als bei eigenhändig unterschriebenen Papierdokumenten – technische Fortschritte oder neue wissenschaftliche Erkenntnisse zu einem Verlust der Sicherheitseignung, der bei der ursprünglichen Signatur eingesetzten Algorithmen und zugehörigen Parametern, führen könnten. Überdies bringt die Neusignierung den Vorteil mit sich, dass der Beweiswert des ursprünglich signierten Dokuments erhöht wird. Ansonsten bestünde die Möglichkeit, Signaturen des alten Dokuments ohne erkennbare Spuren zu entfernen. Wie in der Vergleichung der Signaturregelungen erwähnt, zeigt sich aufgrund der klaren Vorteile sowie der Notwendigkeit der Existenz einer Vorschrift zur erneuten Signatur die Übernahme einer des deutschen Signaturrechts ähnlichen Regelung in das brasilianische Signaturrecht als passend. Die Regel könnte – wie in Deutschland – sowohl autonom normiert werden, als auch als Teil der Unterrichtungspflicht.

Wie die Arbeit weiter zeigt, sind Zeitstempel ein wichtiges Mittel, um ein Vor- und Rückdatieren von elektronischen Dokumenten zu verhindern. Wird im Streitfalle ein bestimmter Zeitpunkt beweiserheblich, dann sind Zeitstempel unabdingbar. Deutschland verfügt über Vorschriften im Signaturgesetz (§§ 2 Nr. 14 und 9 SigG), welche Zeitstempel normieren. Deren Nutzung ist hingegen im brasilianischen Signaturrecht nicht vorgesehen. Hier werden die Zeitstempel im Gesetzentwurf Nr. 7.136/2002 geregelt. Er bietet die Möglichkeit der Akkreditierung von Zeitstempeldiensteanbietern und normiert diese. Diese Aussicht auf eine nutzvolle Steigerung der Sicherheit des elektronischen Geschäftsverkehrs ist geboten, um Zeitstempeldienste in die brasilianische Public Key Infrastruktur einzuführen.

Die sichere und zuverlässige Identifikation des Antragstellers stellt einen wesentlichen Teil der Sicherheitskette einer Public Key Infrastruktur dar. In diesem Fall gilt in Brasilien das Gebot, die Beantragung eines akkreditierten Zertifikats nur unter persönlichem Kontakt stattfinden zu lassen. Im deutschen Signaturgesetz wird die Anforderung an den Zertifizierungsdiensteanbieter, den Antragsteller zuverlässig zu identifizieren, normiert. Als möglich gilt nach der Verabschiedung des ersten Gesetzes zur Änderung des Signaturgesetzes, Daten zu nutzen, welche der Zertifizierungsdiensteanbieter zu einem früheren Zeitpunkt erhoben hat. Es ist in Deutschland somit zugelassen, Beantragung und Ausgabe von Signaturerstellungseinheiten ohne persönlichen Kontakt und Unterschrift wie etwa mittels PIN und TAN durchzuführen. Dies schafft jedoch Rechtsunsicherheit, denn anstelle der Identität an einen sicheren persönlichen Kontakt anzuknüpfen, wird dieser durch virtuelle Aktionen ersetzt. Sachgerechter sind in diesem Zusammenhang die Lösungen des brasilianischen Signaturrechts und der aufgehobenen Fassung des Signaturgesetzes, die den persönlichen Kontakt zur Identifikation des Antragstellers erforderlich machen.

Die Möglichkeit, Beschränkungen nach Art oder Umfang einer Anwendung ins Zertifikat einzutragen, wird in Brasilien nicht vorgesehen. Anders in Deutschland,

wo das Signaturgesetz dies normiert. Eine Limitierung im Zertifikat einzutragen trägt zur gesamten Sicherheit einer Public Key Infrastruktur bei. Sie dient zum einen dem Selbstschutz des Signaturschlüssel-Inhabers und hat einen verbraucherschützenden Charakter. Zum anderen kann die Limitierung als Mittel zur Risikokalkulation in Bezug auf mögliche Haftungsansprüche behilflich sein, obwohl in Brasilien Ersatzpflichten grundsätzlich nicht eingeschränkt werden dürfen. Die Beschränkung kann eine wichtige Rolle spielen, insbesondere für die behördliche Pflicht des ITI, um die erforderliche Mindestversicherungssumme für Zertifizierungsdiensteanbieter einzuschätzen. Und schließlich schützt die Beschränkung vor Übereilung bei der Abgabe einer elektronischen Erklärung. Aus all diesen Gründen wäre es für das brasilianische Signaturrecht empfehlenswert, eine Vorschrift zu übernehmen, welche die Möglichkeit vorsieht, eine Limitierung ins Zertifikat einzutragen.

Das brasilianische Signaturrecht legt für den Zertifizierungsdiensteanbieter eine unnötige maximale Reaktionszeit von zwölf Stunden fest, um das Sperrverfahren von Zertifikaten durchzuführen. In dieser Zeitspanne können unzählige Ereignisse geschehen, welche wie etwa bei einem Diebstahl oder Abhandenkommen der Signaturkarte Schäden verursachen. Die deutsche Regel zeigt sich als sachgerechter, indem sie eine „unverzügliche“ Sperrung bestimmt. In Betracht kommt ebenfalls der Maßnahmenkatalog des BSI, welcher eine Reaktionszeit bis zum Wirksamwerden des Sperreintrags von maximal zehn Minuten empfiehlt.

Mit der Eintragung des Sperrvermerks im Zertifikatsverzeichnis als Abschluss des Zertifikatssperrverfahrens verfügt das deutsche Modell über eine sicherere Variante als das brasilianische. Während brasilianische akkreditierte Zertifizierungsdiensteanbieter in der Regel gesperrte Zertifikate in eine Sperrliste eintragen, wird von deutschen Zertifizierungsstellen die Führung eines Verzeichnisses verlangt, welches die Aussage über die Gültigkeit von Zertifikaten ermöglicht. Dessen Prüfung durch die Nutzer lässt sich derzeit nur durch OCSP-Abfragen realisieren. Der größte Vorteil von OCSP-Abfragen im Vergleich zur Abfrage von Sperrlisten liegt darin, dass der OCSP-Dienst einen Existenznachweis des Zertifikats ermöglicht. Bei der Prüfung wird folglich das Risiko ausgeschlossen, dass das betreffende Zertifikat nicht existiert. Angesichts dieses Vorteils wäre es sinnvoll, dass Brasilien die Onlineabfrage des Zertifikatsstatus sowie die entsprechende Antwort bezüglich der Gültigkeit durch das Online Certificate Status Protocol (OCSP) implementiert.

Die Form des Zertifikatssperrantrags bleibt im brasilianischen Signaturrecht offen. Wie in dieser Arbeit dargestellt, realisieren einige brasilianische Zertifizierungsdiensteanbieter ein Sperrverfahren, bei welchem der Antragsteller ein Webformular ausfüllt. Seine Identität gegenüber dem Sperrdienst weist er in diesem Fall durch ein Passwort nach, welches ihm bei der Zertifikatserzeugung von der Zertifizierungsstelle übergeben wurde. Hierzu ist die Lösung des § 7 Abs. 1 SigV angemessener. Diese Vorschrift sieht die Pflicht für Zertifizierungsdiensteanbieter vor, eine Rufnummer für die Sperrung qualifizierter Zertifikate bereitzustellen. Für die Fälle, in denen sowohl die sichere Signaturerstellungseinheit als auch das Gerät, mit dem signiert wird (wie ein Notebook), geraubt werden, muss es eine Alternative zum

Webformular geben. Der Vorteil der Telefonverbindung besteht in der Tatsache, dass sie immer noch wesentlich verbreiteter als das Internet und somit schneller ist.

Das brasilianische Gesetz Nr. 11.419 stellt einen wichtigen Schritt in Richtung Modernisierung der brasilianischen Justiz dar. In ihm wird die Möglichkeit geschaffen, dass Verfahrensbeteiligte elektronische Kommunikationsformen rechtswirksam verwenden können. Schwachpunkt dieses Gesetzes ist jedoch die Option für die Parteien, sich neben einer akkreditierten Signatur durch die Registrierung gegenüber den Anwendungen der entsprechenden Rechtspflegeorgane zu identifizieren. Diese Möglichkeit sollte aus dem Gesetz gestrichen werden, denn zum einen schafft sie einen großen Aufwand angesichts der Tatsache, dass Rechtsanwälte sich bei jedem Gericht an dem sie ihre Tätigkeiten ausüben, registrieren lassen müssen. Zum anderen wird mit der Möglichkeit der einfachen Registrierung durch möglicherweise Passwort-Verfahren die Chance verpasst, die viel sichere Variante der akkreditierten Verfahren zu verbreiten.

Art. 1.3.5.2 Resolução Nr. 41 bezweckt die Interoperabilität zu gewährleisten, indem er bestimmt, dass Anwendungen, welche einen bestimmten Zertifikatstyp zulassen, Zertifikate der gleichen oder höheren Kategorie unabhängig vom ausstellenden Zertifizierungsdiensteanbieter unterstützen müssen. Diese Regelung ist durchaus zu begrüßen, jedoch droht ihr Wirkungslosigkeit, denn im Geltungsbereich der Normen der brasilianischen PKI befinden sich ausschließlich die Zertifizierungsinstanzen und sonstige Teilnehmer der Infrastruktur für öffentliche Schüssel wie Identifikationsstellen. Dritte, die Anwendungen für akkreditierte Verfahren entwickeln, sind prinzipiell den Geboten dieser Regelungen nicht untergeordnet, weil sie der Infrastruktur nicht angehören. Die erwähnte Norm zur Gewährleistung der Interoperabilität erreicht somit ihr Ziel nur bedingt. Notwendig wäre die Bestimmung einer solchen Norm im Rahmen eines Gesetzes und nicht innerhalb der Beschlüsse des Regulierungsausschusses, wie es der aktuellen Lage entspricht. Dieser Schwachpunkt wird aber behoben, sollte der Gesetzentwurf Nr. 7.316/2002 verabschiedet werden. Art. 12 des Entwurfs gibt eine ähnliche Norm wie Art. 1.3.5.2 Resolução Nr. 41 wieder und löst folglich das hier erwähnte Problem.

In Brasilien wird die Möglichkeit gegeben, dass prinzipiell bei einem Zertifikat einer bestimmten Kategorie (A1), der private Schlüssel beispielsweise auf einer Festplatte gespeichert werden kann. Problematisch hierbei ist, dass die alleinige Kontrolle über den Signaturschlüssel durch den Zertifikatinhaber verloren geht. Softwarelösungen alleine sind nicht geeignet, um die notwendige Sicherheit des Nutzers zu gewährleisten. Hierzu wären zusätzliche manuelle Schutzmechanismen erforderlich, wie das Einschließen der Diskette in einem Safe oder das Isolieren des PCs ohne Netzanschluss in einem Zimmer, zu dem nur der Schlüsselinhaber Zutritt hat. Das alles wäre realisierbar, aber unpraktisch für den Nutzer. Aus diesen Gründen ist zu erwarten, dass in naher Zukunft diese unsichere Gegebenheit der Speicherung eines privaten Schlüssels aufgehoben wird und zukünftig nur noch geeignete Prozessor-Chipkarten, Security-Token oder vergleichbare Datenträger verwendet werden. Bei der aktuellen Situation, betreffend eine der wichtigsten Sicherheitsas-

pekte einer PKI, ist die Ausgangsposition Brasiliens oder brasilianischer Zertifizierungsdiensteanbieter für Verhandlungen mit anderen Staaten oder internationalen Organisationen über die gegenseitige Anerkennung von elektronischen Zertifikaten schwierig. Obwohl die Anforderungen der Europäischen Union gemäß Art. 7 der Signaturrichtlinie keine Überprüfung der Sicherheit der ausländischen Signaturverfahren vorsehen, müssen entweder das Zertifikat oder der Zertifizierungsdiensteanbieter im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der EU und dem Drittland oder der internationalen Organisationen anerkannt werden.[779] Die konkreten Voraussetzungen für diese Anerkennung werden nicht in der Signaturrichtlinie bestimmt und müssen daher fallweise ausgehandelt werden. Es ist jedoch vorhersehbar, dass die Möglichkeit der Speicherung des Signaturschlüssels auf einer Diskette oder Festplatte als nicht geeignet für Signaturverfahren, welche die Unterschrift ersetzen sollen, eingestuft werden würde. In Deutschland beispielsweise werden ausländische elektronische Signaturen nach § 23 Abs. 2 SigG akkreditierten Signaturen nur dann gleichgestellt, wenn sie nachweislich eine gleichwertige Sicherheit aufweisen.

In Anbetracht der Gegebenheiten der brasilianischen Signaturregulierung wird lediglich die Möglichkeit vorgesehen, Signaturanwendungskomponenten und Produkte für die Sicherheit akkreditierter Signaturen zu prüfen und zu bestätigen. Besonders wichtig ist, dass die Erzeugung einer elektronischen Signatur vorher eindeutig angezeigt wird, damit der Signierende, die Daten auf welche sich die Signatur bezieht, feststellen kann. Gemeint sind die Produkte für die Darstellung zu signierender Daten. Das deutsche Signaturgesetz enthält eine der brasilianischen Signaturregulierung ähnlichen Vorschrift, geht aber einen Schritt weiter, indem es dem Signaturschlüssel-Inhaber sichere Signaturanwendungskomponenten zu verwenden empfiehlt (§ 17 Abs. 2 Satz 3 SigG). Der Einsatz solcher Komponenten durch den Zertifikatsinhaber – anders als bei Zertifizierungsdiensteanbietern – ist nicht kontrollierbar. Somit stellen die sicheren Komponenten keine Wirksamkeitsvoraussetzung für die mittels ihrer Anwendung erzeugten Signaturen dar. Verstärkt wird diese Soll-Vorschrift durch die Pflichtdienstleistung des Zertifizierungsdiensteanbieters, den Signaturschlüssel-Inhaber über die erforderlichen Maßnahmen zur Sicherheit von qualifizierten elektronischen Signaturen und deren Prüfung zu unterrichten (§ 6 Abs. 1 Satz 1 SigG). Da im brasilianischen Signaturrecht die Signaturanwendungskomponenten noch nicht einmal als Empfehlungen geregelt sind, zeigt es sich als opportun, basierend auf dem deutschen Modell des § 17 Abs. 2 Satz 3 SigG eine Norm darüber zu übernehmen.

779 Laut Art. 7 Abs. 1 a) und b) Signaturrichtlinie wären zwei andere Möglichkeiten für die Anerkennung: die Erfüllung der Anforderungen der Signaturrichtlinie und die Akkreditierung des Zertifizierungsdiensteanbieters in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum, oder dass ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen der Signaturrichtlinie erfüllt, für das Zertifikat einsteht.

Der Datenschutz gewinnt im deutschen Recht eine höhere Aufmerksamkeit als im brasilianischen Recht. Dies hat die Darstellung beider Signaturregelungen gezeigt. Während bereits das Signaturgesetz aus dem Jahr 1997 eine datenschutzrechtliche Vorschrift enthielt, sieht das geltende brasilianische Signaturrecht keine derartige Regelung vor. Diese Lage ändert sich ein wenig in Brasilien sollte der Gesetzentwurf Nr. 7.316/2002 verabschiedet werden, welcher eine allgemeine Norm zum Datenschutz vorsieht. Diese Vorschrift könnte aber mit der Möglichkeit zum Selbstdatenschutz durch ein Pseudonym ähnlich dem deutschen Signaturgesetz ergänzt werden. Hierzu wird aber ein unbürokratisches Aufdeckungsverfahren erforderlich, welches die Verantwortlichkeit des unter einem Pseudonym handelnden Signaturschlüssel-Inhabers gewährleistet. Zu beachten ist in diesem Zusammenhang auch, dass Art. 5, IV der Constituição Federal die Anonymität untersagt.

Wie diese Arbeit zeigte, können Haftungsregelungen in Public Key Infrastrukturen eine notwendige Rolle spielen. Sie leisten einen Beitrag dabei, den Verbraucherschutz, das Vertrauen sowie die Akzeptanz von Signaturverfahren zu fördern. Das Signaturgesetz sieht eine deliktische Haftungsnorm vor, wonach Ersatzberechtigte nur Dritte sind, die kein vertragliches Verhältnis zum Zertifizierungsdiensteanbieter haben. Es handelt sich hierbei um eine Verschuldenshaftung mit Beweislastumkehr. Gegenüber dem Signaturschlüssel-Inhaber haftet der Zertifizierungsdiensteanbieter aufgrund des zwischen beiden abgeschlossenen Vertrags. In Brasilien sind keine Haftungstatbestände in der MP 2.200-2 zu finden, sondern diese werden lediglich in den Beschlüssen des Regulierungsausschusses festgesetzt. Während die Haftungsvorschriften des Signaturgesetzes nur im Verhältnis Zertifizierungsdiensteanbieter zu Dritten anwendbar sind, gelten die brasilianischen Vorschriften ausschließlich im vertraglichen Verhältnis zwischen Zertifizierungsstelle und Signaturschlüssel-Inhaber. Als mögliche Haftungsquellen im Verhältnis zwischen dem Dritten und dem Zertifizierungsdiensteanbieter kommen der Código de Defesa do Consumidor und der Código Civil in Betracht. Diese Gesetze können auch subsidiär in der Beziehung zwischen dem Zertifizierungsdiensteanbieter und dem Signaturschlüssel-Inhaber geltend gemacht werden. Für Brasilien wird vorgeschlagen, die Haftungsvorschriften des Gesetzesentwurfes Nr. 7.316/2002 zu übernehmen. Dieser Ansatz enthält einige nennenswert wichtige Vorschriften. Art. 38 Gesetzentwurf Nr. 7.316/2002 sieht eine Haftungsregelung vor, welche bestimmt, dass alle Teilnehmer der ICP-Brasil – einschließlich der Aufsichtsbehörde – für die von ihnen verursachten Schäden haften. Wichtig hierbei ist, dass nach der Formulierung dieser Vorschrift der Zertifizierungsdiensteanbieter gegenüber jedem Dritten für Schäden haftet. Der Dritte bleibt somit nicht unbeschützt. Art. 39 legt des Weiteren eine subsidiäre Haftung der Zertifizierungsdiensteanbieter fest. Sie haften auch für von ihnen beauftragte Dritte. Nach Art. 41 Gesetzentwurf Nr. 7.316/2002 müssen Vertragsklauseln zwischen Zertifizierungsdiensteanbietern und Signaturschlüssel-Inhabern für nichtig erklärt werden, wenn diese Klausel die Haftung der Zertifizierungsstellen vermindern oder ausschließen. Das gleiche gilt für die Bestimmungen der „Declaração de Práticas de Certificação“ und „Políticas de Certficado“.

Die aktuelle Rechtslage bezüglich des Beweiswerts elektronisch signierter Dokumente ist in Brasilien von Rechtsunsicherheit geprägt. Dies ist der Tatsache zu verdanken, dass grundsätzlich zwei Rechtsquellen für das Bestreiten einer mittels akkreditierter Signaturverfahren signierten Datei zum Einsatz kommen können: § 1 Art. 10 MP 2.200-2 oder Art. 389 Abs. 2 CPC. § 1 Art. 10 MP 2.200-2 begründet eine widerlegliche Vermutung der Echtheit, welche vom Signaturschlüssel-Inhaber erschüttert werden muss. Wird aber Art. 389 Abs. 2 CPC angewandt, trägt der Signaturempfänger die Beweislast zur Erschütterung einer Signatur. Darüber hinaus ist in diesem Zusammenhang auch problematisch, dass Beweisvorschriften in Form einer Medida Provisória gelten. Die in dieser Arbeit vorgeschlagene Änderung des Código de Processo Civl leistet sowohl einen Beitrag zu mehr Übersicht als auch zu mehr Rechtssicherheit. Ferner schafft der Vorschlag durch die auf den § 371a Satz 2 ZPO basierende Formulierung „ernstliche Zweifel“ einen Maßstab für die Entkräftung der widerleglichen Vermutung der Echtheit akkreditiert elektronisch signierter Erklärungen.

Literaturverzeichnis

Adams, C. / *Lloyd, S.*, Understanding Public-Key Infrastructure: concepts, standards, and deployment considerations, Indianapolis 1999.

Almeida, A. C. de, Direito e Internet, Coimbra 2002.

Alvim, A., Manual de Direito Processual Civil, vol. 2, São Paulo 2001.

Amaral Júnior, J. L. M. do, Medida Provisória e sua conversão em lei. A Emenda Constitucional n. 32 e o papel do Congresso Nacional, São Paulo 2004.

Andrade, R. A., Contrato eletrônico no novo Código Civil e no Código do Consumidor, Barueri 2004.

Azevedo, A. J. de, Os princípios do atual direito contratual e a desregulamentação do mercado. Direito de exclusividade nas relações de fornecimento. Função social do contrato e responsabilidade aquiliana do terceiro que contribui com o inadimplemento contratual. Estudos e pareceres de direito privado, São Paulo 2004.

Baptista, L. O. (Hrsg.), Novas fronteiras do Direito na Informática e Telemática, São Paulo 2001.

Barbagalo, E. B., Contratos Eletrônicos: contratos formados por meio de redes de computadores, peculiaridades jurídicas da formação do vínculo, São Paulo 2001.

Barbosa Moreira, J.C., As presunções e a prova, São Paulo 1988.

Barbosa Moreira, J.C., O novo Código Civil e o Direito Processual, RF 2002, 181.

Barbosa Moreira, J.C., Anotações sobre o Título "Da prova" do novo Código Civil, RTDC 2005, 97.

Barreto, A. C. H., Assinaturas Eletrônicas e Certificação, In: Rocha Filho, V. de O. (Hrsg.), O Direito e a Internet, Rio de Janeiro 2002.

Bauer, F. L., Entzifferte Geheimnisse – Methoden und Maximen der Kryptologie, Berlin 2000.

Baum, M., Technology Neutrality and Secure Electronic Commerce: rule making in the age of 'equivalence', Version 1.1, 1999, abrufbar unter: http://www.verisign.com/repository/techneutralityv1_1.doc.

Baumann, J., Einführung in die Rechtswissenschaft, Rechtssysteme und Rechtstechnik, München 1989.

Baumgärtel, G., Beweislast im Privatrecht – Die Schwierigkeiten der Beweislastverteilung und die Möglichkeiten ihrer Überwindung, München 1996.

Berger, A., Signatur-Interoperabilitätsspezifikation: Zertifikate und Dokumentformate, DuD 1998, 206.

Bergfelder, M. / *Nitschke, T.* / *Sorge, C.*, Signaturen durch elektronische Agenten, Informatik Spektrum 2005, 210.

Bergfelder, M., Was ändert das 1. Signaturänderungsgesetz? Die qualifizierte elektronische Signatur zwischen Anspruch und Wirklichkeit, CR 2005, 148.

Bergfelder, M., Der Beweis im elektronischen Rechtsverkehr, Hamburg 2006.

Bertsch, A., Digitale Signaturen, Berlin 2002.

Bertsch, A. / *Pordesch, U.*, Zur Problematik von Prozesslaufzeiten bei der Sperrung von Zertifikaten, DuD 1999, 514.

Bertsch, A. / *Fleisch, S.* / *Michels, M.*, Rechtliche Rahmenbedingungen des Einsatzes digitaler Signaturen, DuD 2002, 69.

Bieser, W. / *Kersten, H.*, Chipkarte statt Füllfederhalter, Heidelberg 1998.

Bieser, W. / *Kersten, H.*, Elektronisch unterschreiben – die digitale Signatur in der Praxis, Heidelberg 2002.

Bizer, J., Elektronisch signiertes Dokument, DuD 1993, 700.

Bizer, J., Rechtliche Bedeutung der Kryptographie, DuD 1997, 203.

Bizer, J., Das Wurzelzertifikat des Zertifizierungsdienstanbieters, DuD 2002, 107.

Bizer, J., Sicherheit durch Interaktion – Alternativen zu gesetzkonformen Signaturen im E-Commerce, DuD 2002, 276.

Bizer, J. / *Fox, D.*, Freiheit und Regulierung, DuD 1997, 182.

Blaze, M., Kryptopolitik und Informations-Wirtschaft, DuD 1997, 204.

Blocher, W. / *Zisak, A.*, Elektronischer Rechtsverkehr: Rechtliche Regelung und praktische Anwendung elektronischer Signaturen, RdW 2006, 612.

Blocher, W., Zur Haftung des Zertifizierungsdiensteanbieters nach § 11 Signaturgesetz 2001, in; Hänlein, A./ Rossnagel, A. (Hrsg.), Wirtschaftsverfassung in Deutschland und Europa, Festschrift für Bernhard Nagel, Kassel 2007.

Blum, F., Entwurf eines neuen Signaturgesetzes, DuD 2001, 71.

Boiago Jr., J. W., Contratos eletrônicos – aspectos jurídicos, Curitiba, 2006.

Borges, G., Verträge im elektronischen Geschäftsverkehr – Vertragsabschluss, Beweis, Form, Lokalisierung, anwendbares Recht, München 2003.

Bösing, S., Authentifizierung und Autorisierung im elektronischen Rechtsverkehr – Qualifizierte Signaturschlüssel- und Attributszertifikate als gesetzliche Instrumente digitaler Identität, Baden-Baden 2005.

Bovenschulte, A. / *Eifert, M.*, Rechtsfragen der Anwendung technischer Produkte nach Signaturgesetz, DuD 2003, 76.

Brandner, R. / *Pordesch, U.* / *Roßnagel, A.* / *Schachermayer, J.*, Langzeitsicherung qualifizierter elektronischer Signaturen, DuD 2002, 97.

Brandner, R. / *Pordesch, U.*, Konzept zur signaturgesetzkonformen Erneuerung qualifizierter Signaturen, DuD 2003, 354.

Britz, J. W., Urkundenbeweisrecht und Elektroniktechnologie, München, 1996.

Bröhl, G. / *Tettenborn, A.*, Das neue Recht der elektronischen Signaturen. Kommentierende Darstellung von Signaturgesetz und Signaturverordnung, Köln 2001.

Bundesamt für Sicherheit in der Informationstechnik (BSI), Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV – SigI Abschnitt B4 Normen und Standards, Version 1.0, Bonn 2000, abrufbar unter: http://www.bsi.de/esig/basics/techbas/interop/bsi/sigib4.pdf (zitiert als: BSI-SigI-B4)

Bundesamt für Sicherheit in der Informationstechnik (BSI), Grundlagen der elektronischen Signatur, Bonn, 2006, abrufbar unter: http://www.bsi.de/esig/esig.pdf (zitiert als: BSI-GeS)

Burnett, S. / *Paine, S.*, Criptografia e Segurança: o guia oficial RSA, Rio de Janeiro 2002.

Büger, M. / *Esslinger, B.* / *Koy, H.*, Das deutsche Signaturbündnis, DuD 2004, 133.

Buzaid, A., Estudos de Direito, v. 1, São Paulo 1972.

Calmon, P., Comentários à Lei de Informatização do Processo Judicial: Lei Nr. 11.419, de 19 de dezembro de 2006, São Paulo 2007.

Carpes, A. T., A distribuição dinâmica do ônus da prova no formalismo-valorativo, Revista da Ajuris Nr. 104, 9.

Carvalho, A. P. G., Contratos via Internet, Belo Horizonte 2001.

Carvalho, A. P. G., Verbraucherverträge im Internet: rechtsvergleichende Studie zum deutschen und brasilianischen Recht, Baden-Baden 2005.

Castro, A., A., O documento eletrônico e a assinatura digital – uma visão geral., 2001, abrufbar unter: http://jus2.uol.com.br/doutrina/texto.asp?id=2632.

Coelho, S. R. S., O excesso de Medidas Provisórias e o problema da autonomia e independência do Poder Legislativo: impasses e dilemas, Brasília, 2007, abrufbar unter: http://bdjur.stj.gov.br/dspace/handle/2011/10209.

Comitê Gestor da Internet no Brasil, Survey on the use of Information and Communication Technologies in Brazi: ICT Households and ICT Enterprises 2007, executive and editorial coordination, Mariana Balboni, São Paulo 2008.

Constantinesco, L.J., Einführung in die Rechtsvergleichung, Köln 1971.

Constantinesco, L.J., Die rechtsvergleichende Methode, Köln 1972.

Corrêa, G. T., Aspectos jurídicos da Internet, São Paulo 2002.

Couto e Silva, C. V. do, Direito material e processual em tema de prova, RP 1979, 135.

Covello, S. C., A presunção em matéria civil, São Paulo 1983.

Creifelds, C., Rechtswörterbuch, München 2002.

Dästner, C., Neue Formvorschriften im Prozessrecht, NJW 2001, 3469.

De Lucca, N., Aspectos Jurídicos da contratação Informática e Telemática, São Paulo 2003.

De Lucca, N. / *Simão Filho, A.* (Hrsg.), Direito & Internet: aspectos jurídicos relevantes, Bauru 2001.

De Lucca, N., Títulos e Contratos Eletrônicos: o advento da informática e seu impacto no mundo jurídico. In: De Lucca, N./ Simão Filho, A. (Hrsg.). Direito & Internet: aspectos jurídicos relevantes. Bauru 2001, 69.

Dietze, L. / *Gießmann, E.-G.* / *Lo Iacono, L.*, Gültigkeitsmodelle – revisited, DuD 2005, 206.

Diffie, W. / *Hellmann, M. E.*, New Directions in Cryptography, IEEE Transactions on Information Theory 1976, 644.

Diniz, D., Documentos Eletrônicos, Assinaturas Digitais, São Paulo 1999.

Dinamarco, C.R., Instituições de direito processual civil, v. 4, São Paulo 2005.

Di Pietro, M.S.Z., Direito Administrativo, São Paulo 1993.

Doña, M. L. S. F., Impacto del comercio electrónico en el derecho de la contratación, Madrid 2002.

Dumortier, J. / *Kelm, S.* / *Nilsson, H.* / *Skouma, G.* / *van Ecke, P.*, The legal and market aspects of electronic signatures, DuD 2004, 141.

Ellison, C. / *Schneier, B.*, Ten risks of PKI: What you´re not being told about Public Key Infrastructure, Computer Security Journal, v. 16, n. 1, 2000, 1.

Erber-Faller, S. (Hrsg.), Elektronischer Rechtsverkehr, Kriftel 2000.

Espínola, E., Breves Anotações ao Código Civil Brasileiro, Salvador 1918.

Federrath, H., Schlüsselgenerierung: Einseitig sicher ist nicht sicher genug, DuD 1997, 98.

Ferreira, I. S. / *Baptista, L. O.* (Hrsg.), Novas fronteiras do direito na era digital, São Paulo 2002.

Ferreira da Silva, L. R., A função social do contrato no novo Código Civil e sua conexão com a solidariedade social, in: Sarlet, I. (Hrsg.), O novo Código Civil e a Constituição

Fischer-Dieskau, S., Das elektronisch signierte Dokument als Mittel zur Beweissicherung: Anforderungen an seine langfristige Aufbewahrung, Baden-Baden 2006.

Fischer-Dieskau, S. / *Gitter, R.* / *Paul, S.* / *Steidle, R.*, Elektronisch signierte Dokumente als Beweismittel im Zivilprozess, MMR 2002, 709.

Fischer-Dieskau, S. / *Steidle, R.*, Die Herstellererklärung für Signaturanwendungskomponenten – Eine Erleichterung zur Verbreitung elektronischer Signaturen?, MMR 2006, 68.

Fischer-Dieskau, S. / *Gitter, R.* / *Hornung, G.*, Die Beschränkung des qualifizierten Zertifikats - § 7, Abs. 1 Nr. 7 SigG als wichtiges Mittel der Risikokalkulation, MMR 2003, 384.

Ford, W. / *Baum, M. S.*, Secure Electronic Commerce: building the infrastructure for digital signatures and encryption, Prentice Hall 2001.

Fox, D., Fälschungssicherheit digitaler Signaturen, DuD 1997, 69.

Fox, D., Zu einem prinzipiellen Problem digitaler Signaturen, DuD 1998, 386.

Fox, D., Eine kritische Würdigung des SigG, DuD 1999, 508.

Fox, D., Certificate Revocation List (CRL), DuD 2001, 485.

Fritsch, L. / *Rossnagel, H.*, Die Krise des Signaturmarktes : Lösungsansätze aus betriebswirtschaftlicher Sicht, in: Federrath, H. (Hrsg.): SICHERHEIT 2005, Sicherheit – Schutz und Zuverlässigkeit: Beiträge der 2. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Lecture Notes on Informatics, Regensburg 2005.

Gajek, S. / *Schwenk, J.* / *Wegener, C.*, Identitätsmissbrauch im Onlinebanking, DuD 2005, 11.

Gama, A. D., Tratado Teórico e Prático de Direito Civil Brasileiro, v. 2. Introdução ao estudo do Direito Civil, Rio de Janeiro 1927.

Garcia Mas, F. J., Comercio y Firma Electrónicos: análisis jurídico de los servicios de la Sociedad de la Información, Valladolid 2002.

Gassen, D., Digitale Signaturen in der Praxis: Grundlagen, Sicherheitsfragen und normativer Rahmen, Köln 2003.

Geis, I. (Hrsg.), Das digitale Dokument: Rechtliche, organisatorische und technische Aspekte der Archivierung und Nutzung, Eschborn 1995.

Geis, I., Die digitale Signatur, NJW 1997, 3000.

Geis, I., Die elektronische Signatur: Eine internationale Architektur der Identifizierung im E-Commerce, MMR 2000, 667.

Gesellschaft für Informatik e. V., Stellungnahme zum Gesetzentwurf „Formvorschriften des Privatrechts“, DuD 2001, 38.

Gesellschaft für Informatik e. V. / *Informationstechnische Gesellschaft im VDE*, Memorandum zur Förderung des elektronischen Rechts- und Geschäftsverkehrs vom 3.4.2003, DuD 2003, 763.

Giannico, M., A prova no Código Civil. Natureza jurídica, São Paulo 2005.

Gitter, R., Softwareagenten im elektronischen Geschäftsverkehr, Baden-Baden 2008.

Glanz, S., Consumidor e Contrato Eletrônico, RT 796, 114.

Greco, L., A prova no processo civil: do Código de 1973 ao novo Código Civil, RF 2004, 183.

Greco, M. A., Internet e Direito, São Paulo 2002.

Greco, M. A. / *Martins, I. G. da S.* (Hrsg.), Direito e Internet: relações jurídicas na sociedade informatizada, São Paulo 2001.

Hager, G., Umweltschäden – ein Prüfstein für die Wandlungs- und Leistungsfähigkeit des Deliktsrechts, NJW 1986, 1961.

Hähnchen, S., Das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, NJW 2001, 2831.

Hamm, R., Kryptokontroverse, DuD 1997, 186.

Hammer, V., Gestaltungsbedarf und Gestaltungsoptionen für Sicherungsinfrastrukturen, in: Hammer, V. (Hrsg.), Sicherungsinfrastrukturen, Darmstadt 1995.

Hammer, V., Wie nennen wir Infrastrukturen für die Schlüsselverwaltung, DuD 1998, 91.

Hammer, V. / *Petersen, H.*, Aspekte der Cross-Zertifizierung, in: Horster, P. (Hrsg.), Kommunikationssicherheit im Zeichen des Internet, Grundlagen, Strategien, Realisierungen, Anwendungen, Braunschweig, 2001, 192.

Heinrich, C., Die Beweislast bei Rechtsgeschäften, Köln 1996.

Herranz, I. R. (Hrsg.), Derecho del comercio electrónico, Madrid 2001.

Hoeren, T., Grundzüge des Internetrechts – E-Commerce/Domains/Urheberrecht, München 2001.

Holzhauer, H., Die eigenhändige Unterschrift: Geschichte und Dogmatik des Schriftformerfordernisses im deutschen Recht, Frankfurt a. M. 1973.

Hornung, G., Ein neues Grundrecht. Der verfassungsrechtliche Schutz der "Vertraulichkeit und Integrität informationstechnischer Systeme", CR 2008, 299.

Hortmann, M., Kryptoregulierung weltweit – Überblick, DuD 1997, 214.

Jauernig, O., Zivilprozessrecht, München 2002.

Jandt, S., Vertrauen im Mobile Commerce, Baden-Baden 2008.

Jones, J., PKI at the crossroads, abrufbar unter: http://www.fcw.com/print/8_24/news/77034-1.html.

Jungermann, S., Der Beweiswert elektronischen Signaturen – Zu den Voraussetzungen und Rechtsfolgen des § 292a ZPO, DuD 2003, 69.

Jungermann, S., Der Beweiswert elektronischer Signaturen, Frankfurt a. M. 2002.

Kaiser, J. H., Vergleichung im öffentlichen Recht, ZaöRV 1964, 391.

Karam, M., Ônus da prova: noções fundamentais, RP, Nr. 17, 50.

Karper, I., Sorgfaltspflichten beim Online-Banking – Der Bankkunde als Netzwerkprofi? – Zur möglichen Neubewertung des Haftungsmaßtabs, DuD 2006, 215.

Knopp, M., Digitalfotos als Beweismittel, ZRP 2008, 156.

Koehler, H., Die Problematik automatisierter Rechtsvorgänge, insbesondere Willenserklärungen, AcP 1982, 126.

Komnios, K., Die elektronische Signatur im deutschen und griechischen Recht, Frankfurt am Main 2007.

Kunstein, F., Die elektronische Signatur als Baustein der elektronischen Verwaltung, Berlin 2005.

Kumbruck, C., Digitale Sicherheit und Sicherheitskultur, in: Hammer, V. (Hrsg.), Sicherungsinfrastrukturen, Darmstadt, 1995, 217.

Kunz, T. / *Schmidt, A.U.* / *Viebeg, U.*, Konzepte für rechtssichere Transformationen signierter Dokumente, DuD 2005, 279.

Landmann, R. v. / *Rohmer, G.*, Umweltrecht, 51. Auflage, München, 2007, (zitiert als: Bearbeiter, in: Landmann/Rohmer).

Langenbach, C. J. / *Ulrich, O.* (Hrsg.), Elektronische Signaturen: Kulturelle Rahmenbedingungen einer technischen Entwicklung, Berlin-Heidelberg 2002.

Laumen, Hans-W., Die „Beweiserleichterung bis zur Beweislastumkehr" – Ein beweisrechtliches Phänomen, NJW 2002, 3739.

Lawand, J. J., Teoria geral dos contratos eletrônicos, São Paulo 2003.

Leal, S. do R. C. S., Contratos eletrônicos – validade juridical dos contratos via internet, São Paulo 2007.

Lenz, J. M. / *Schmidt, C.*, Die elektronische Signatur: Eine Analogie zur eigenhändigen Unterschrift, Stuttgart 2001.

Leonardo, R. X., Imposição e inversão do ônus da prova, Rio de Janeiro 2004.

Leopold, D., Beweislastregeln und gesetzliche Vermutungen – insbesondere bei Verweisungen zwischen verschiedenen Rechtsgebieten, Berlin 1966.

Leopold, D., Beweismaß und Beweislast im Zivilprozess, Berlin 1985.

Lepa, M., Beweiserleichterungen im Haftpflichtrecht, NZV 1992, 129.

Lessig, L., Code and Other Laws of Cyberspace. New York 1999.

Lopes, J. B., A prova no direito processual civil, São Paulo 2000.

Lorenzetti, R. L., Comercio Electrónico, Buenos Aires 2001.

Lo Iacono, L. / *Dietze, L.*, Gültigkeit von Zertifikaten und Signaturen, DuD 2005, 14.

Malzer, H. M., Neuere Gesetzgebung zur Erleichterung des elektronischer Geschäftsverkehrs und ihre Auswirkungen auf die notarielle Tätigkeit, in: Bettendorf, J. (Hrsg.), EDV und Internet in der notariellen Praxis, Köln 2002, 185.

Manssen, G. (Hrsg.), Telekommunikations- und Multimediarecht, Kommentar, Band 2, Loseblatt, Berlin Stand: November 2004, (zitiert als: Bearbeiter, in: Manssen, Band 2).

Marcacini, A. T. R. / *Costa, M.*, O apagão do comércio eletrônico no Brasil, 2001, abrufbar unter http://jus2.uol.com.br/doutrina/texto.asp?id=2284.

Marcacini, A. T. R., Direito e Informática: uma abordagem jurídica sobre a criptografia, Rio de Janeiro 2002.

Marcacini, A. T. R. / *Costa, M.*, Duas óticas, abrufbar unter http://conjur.estadao.com.br/static/text/27788,1.

Marinoni, L.G. / *Arenhart, S.C.*, Comentários ao Código de Processo Civil, v. 5, Tomo II, Do Processo de Conhecimento – arts. 364 a 443, São Paulo 2000.

Marinoni, L.G., Formação da convicção e inversão do ônus da prova segundo as peculiaridades do caso concreto, RT 862, 11.

Marques, A. T. G. L., A prova documental na internet – validade e eficácia do documento eletrônico, Curitiba 2005.

Marques, C. L., Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais, São Paulo 2005.

Marques, L. G. M., Direito da Informática, Coimbra 2000.

Martins, F., Contratos e Obrigações Comerciais, Rio de Janeiro 1999.

Martins, G. M., Contratos eletrônicos via Internet: problemas relativos à sua formação e execução. Revista dos Tribunais 776, 92.

Martins, G., Formação dos Contratos Eletrônicos de Consumo via Internet, Rio de Janeiro, 2003.

Matte, M. S., Internet: comércio eletrônico: aplicabilidade do código de defesa do consumidor nos contratos de e-commerce, São Paulo 2001.

Medicus, D., Bürgerliches Rechts, Köln, Berlin, München 2004.

Mehrings, J., Vertragsschluss im Internet. Eine neue Herausforderung für das alte BGB, MMR 1998, 30.

Meira, S., Infra-estrutura brasileira, provisória, de chaves públicas, abrufbar unter: http://www.no.com.br.

Menke, F., Assinaturas Digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a ICP alemã, RDC 48, 132.

Menke, F., Assinatura eletrônica no direito brasileiro, São Paulo 2005.

Mertes, P., Digitale Signatur – Wertlos ohne Trust Center, in: Glade, A. / Reimer, H. / Struif, B. (Hrsg.), Digitale Signatur und sicherheitsintensive Anwendungen, Braunschweig 1995, 153.

Miedbrodt, A., Signaturregulierung im Rechtsvergleich: Ein Vergleich der Regulierungskonzepte in Deutschland, Europa und in den Vereinigten Staaten von Amerika, Baden-Baden 2000.

Miragem, B., Diretrizes interpretativas da função social do contrato, RDC 56, 22.

Miranda, D. A., Anotações ao Código Civil Brasileiro, v.1., São Paulo 1995.

Moniz de Aragão, E. D., Regras de prova no Código Civil, RP 2004, 116, 10.

Moreira Alves, J. C., A parte geral do projeto de Código Civil brasileiro: subsídios históricos para o novo Código Civil brasileiro, São Paulo 2003.

Mulholland, C., Internet e contratação – panorama das relações contratuais eletrônicas de consumo, Rio de Janeiro 2006.

Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2a: Allgemeiner Teil (Auszug), §§ 241-432 BGB, 4. Auflage, München 2003.

Musielak, J., Gegenwartsprobleme der Beweislast, ZZP 1987, 385.

Musielak, J. (Hrsg.), Kommentar zur Zivilprozessordnung, mit Gerichtsverfassungsgesetz, 3. Auflage, München 2002 (zitiert als: Bearbeiter, in: Musielak).

Nadal, A. M., Comercio Electrónico, Firma Digital y Autoridades de Certificación, Madrid 2001.

Nadal, A. M., La ley de firma electrónica, Madrid 2001a.

Nadal, A. M., Comentarios a La Ley 59/2003 de firma electrónica, Madrid 2004.

Negreiros, T., Teoria do contrato: novos paradigmas, Rio de Janeiro 2002.

Nehl, R., Schlüsselgenerierung in Trust Centern?: Vertrauen durch Trust Center, DuD 1997, 100.

Nissel, R., Neue Formvorschriften bei Rechtsgeschäften: elektronische Form und Textform im Privatrechtsverkehr, Köln 2001.

Nitschke, T. / *Dahm, P.*, Die Rolle von OCSP bei Web Services – Schnelle Auskunft – Risiko oder Chance, DuD 2005, 142.

Oberheim, R., Beweiserleichterungen im Zivilprozeß, JuS 1996, 636.

Oertel, K., Elektronische Form und notarielle Aufgaben im elektronischen Rechtsverkehr MMR 2001, 419.

Ondarza, P. von, Digitale Signaturen und die staatliche Kontrolle von „Fremdeleistungen", Baden-Baden 2001.

Pacífico, L. E. B., O ônus da prova no direito processual civil, São Paulo 2001.

Palandt, O., Bürgerliches Gesetzbuch, 66. Auflage, München 2007 (zitiert als: Bearbeiter in: Palandt).

Parentoni, L. N., Documento eletrônico – aplicação e interpretação pelo Poder Judiciário, Curitiba 2007.

Paul, W., Verfassung und Justiz in Brasilien, Mitteilungen der Der Deutsch-Brasilianisch Juristenvereinigung Nr. 1/1999, abrufbar unter: http://www.dbjv.de/dbjv-high/mitteilungen/99-01/text_05.html.

Peixoto, Rodney de Castro, O Comércio Eletrônico e os Contratos. Rio de Janeiro, 2001.

Pereira, C. M. da S., Instituições de Direito Civil: Introdução ao Direito Civil, Bd. 1, 18. Aufl., Rio de Janeiro 1997.

Pontes de Miranda, F. C., Tratado de Direito Privado, v. 3, Campinas 2000.

Pontes de Miranda, F. C., Comentários ao Código de Processo Civil, tomo IV: arts. 282 a 443, Rio de Janeiro 2001.

Pordesch, U., Risiken elektronischer Signaturverfahren, DuD 1993, 561.

Pordesch, U., Der fehlende Nachweis der Präsentation signierter Daten, DuD 2000, 89.

Pordesch, U., Die elektronische Form und das Präsentationsproblem, Baden-Baden 2003.

Portanova, Rui, Princípios do processo civil, Porto Alegre 2005.

Rapp, C., Rechtliche Rahmenbedingungen und Formqualität Elektronischer Signaturen, München 2002.

Reese, N., Vertrauenshaftung und Risikoverteilung bei qualifizierten elektronischen Signaturen, Köln 2006.

Rego, H. de S., Natureza das normas sobre prova, São Paulo 1985.

Reinhardt, M., Die Umkehr der Beweislast aus verfassungsrechtlicher Sicht, NJW 1994, 93.

Reinaldo Filho, D. (Hrsg.), Direito da informática: temas polêmicos, Bauru 2002.

Rheinstein, M., Einführung in die Rechtsvergleichung, München 1987.

Rieß, J., Signaturgesetz – Der Markt ist unsicher, DuD 2000, 530.

Rezende, P. / *Marcacini, A.* / *Costa, M.*, Novos Ventos Digitais, 2003, abrufbar unter: http://www.marcosdacosta.adv.br/documento.asp?ID_Documento=455.

Rocha Filho, V. O. (Hrsg.), O Direito e a Internet, Rio de Janeiro 2002.

Rodrigues, C. A., Da desnecessidade de assinatura para a validade do contrato efetivado via Internet, RT 784, 83.

Rosenberg, L. / *Schwab, K.-H.* / *Gottwald, P.* (Hrsg.), Zivilprozessrecht, 16. Auflage, München 2004.

Roßnagel, A., Digitale Unterschriften und Verfassungsverträglichkeit, in: Reimer, H./Struif, B. (Hrsg.), Kommunikation und Sicherheit, Bad Vilbel/Darmstadt 1992.

Roßnagel, A., Digitale Signaturen im Rechtsverkehr, NJW-CoR 1994, 96.

Roßnagel, A., Rechtspolitische Gestaltungsstrategie für Sicherungsinfrastrukturen, in: Hammer, V. (Hrsg.), Sicherungsinfrastrukturen, Darmstadt 1995, 265.

Roßnagel, A., Das Signaturgesetz – kritische Bemerkungen zum Entwurf der Bundesregierung, DuD 1997, 75.

Roßnagel, A., Die Sicherheitsvermutung des Signaturgesetzes, NJW 1998, 3312.

Roßnagel, A., Aufgaben der Regulierungsbehörde nach dem Signaturgesetz, MMR 1998, 468.

Roßnagel, A., Das Signaturgesetz nach zwei Jahren – Hinweise zur Gesetzevaluierung, NJW 1999, 1591.

Roßnagel, A., Anerkennung von Prüf- und Bestätigungsstellen nach dem Signaturgesetz, MMR 1999, 342.

Roßnagel, A., Das neue Recht elektronischer Signaturen – Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO, NJW 2001, 1817.

Roßnagel, A., Der elektronische Ausweis. Notwendige und mögliche Identifizierung im E-Government, DuD 2002, 281.

Roßnagel, A., Die neue Signaturverordnung, BB 2002, 261.

Roßnagel, A., Weltweites Internet – globale Rechtsordnung? MMR 2002, 67.

Roßnagel, A., Rechtliche Unterschiede von Signaturverfahren, MMR 2002, 215.

Roßnagel, A. (Hrsg.), Die elektronische Signatur in der öffentlichen Verwaltung - Die künftigen Regelungen und ihre praktische Umsetzung, Baden-Baden 2002.

Roßnagel, A., Die europäische Richtlinie für elektronische Signaturen und ihre Umsetzung im neuen Signaturgesetz. In: Lehmann, M. (Hrsg.). Electronic Business in Europa, München 2002a.

Roßnagel, A., Das elektronische Verwaltungsverfahren, NJW 2003, 469.

Roßnagel, A., Die fortgeschrittene elektronische Signatur, MMR 2003,164.

Roßnagel, A., Rechtlicher Rahmen für den elektronischen Geschäftsverkehr, abrufbar unter http://www.unikassel.de/fb10/oeff_recht/publikationen/pubOrdner/Rahmen_fuer_den_elektronischen_Geschaeftsverkehr.pdf.

Roßnagel, A. (Hrsg.), Recht der Multimedia-Dienste, Kommentar, Loseblatt, München Stand: Juni 2004, (zitiert als: Bearbeiter, in: Roßnagel, RMD).

Roßnagel, A., Datenschutz im 21. Jahrhundert, ApuZ 2006, 9.

Roßnagel, A., Fremdsignierung elektronischer Rechnungen: Vorsteuerabzug gefährdet, BB 2007, 1233.

Roßnagel, A., Die signaturrechtliche Herstellererklärung, MMR 2007, 487.

Roßnagel, A., Fremderzeugung von qualifizierten Signaturen? Ein neues Geschäftsmodell und seine Rechtsfolgen, MMR 2008, 22.

Roßnagel, A. / *Scholz, P*., Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721.

Roßnagel, A. / *Pfitzman, A*. / *Garstka, H*., Modernisierung des Datenschutzrechts – Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001.

Roßnagel, A. / *Yonemaru, T*., Japanische Signaturgesetzgebung – Auf dem Weg zu "e-Japan", MMR 2002, 798.

Roßnagel, A. / *Pfitzman, A*., Der Beweiswert von E-Mail, NJW, 2003, 1209.

Roßnagel, A. / *Fischer-Dieskau, S*. / *Pordesch, U*. / *Brandner, R*., Erneuerung elektronischer Signaturen, CR 2003, 301.

Roßnagel, A. / *Fischer-Dieskau, S*. / *Wilke, D*., Transformation von Dokumenten – Zur Notwendigkeit einer Technik- und Rechtsgestaltung, CR 2005, 903.

Roßnagel, A. / *Schmücker, P*. (Hrsg.), Beweiskräftige elektronische Archivierung – Bieten elektronische Signaturen Rechtssicherheit? Ergebnisse des Forschungsprojekts „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente" 2006, i. E. (zitiert als: Bearbeiter, in: Roßnagel/Schmücker 2006, Seite.).

Roßnagel, A. / *Wilke, D.*, Die rechtliche Bedeutung gescannter Dokumente, NJW 2006, 2145.

Roßnagel, A. / *Stumpf, F.* / *Sacher, M.* / *Eckert C.*, Erzeugung elektronischer Signaturen mittels Trusted Platform Module, DuD 2007, 357.

Roßnagel, A. / *Fischer-Dieskau, S.* / *Jandt, S.* / *Knopp, M.*, Langfristige Aufbewahrung elektronischer Dokumente, Baden-Baden 2007.

Roßnagel, H. / *Hinz, O.*, Zahlungsbereitschaft für elektronische Signaturen, in: Oberweis, A. / Weinhardt, C. / Gimpel, H. / Koschmieder, A. / Pankratius, V. / Schizler, B. (Hrsg.), Wirtschaftsinformatik 2007 – eOrganisation: Service-, Prozess-, Market-Engineering, 8. Internationale Tagung Wirtschaftsinformatik, Karlsruhe 2007, 163.

Roßnagel, A. / *Fischer-Dieskau, S.* / *Jandt, S.* / *Wilke, D.*, Scannen von Papierdokumenten, Baden-Baden 2008.

Roßnagel, A. / *Schmidt, A.* (Hrsg.), Die rechtssichere Transformation signierter Dokumente, 2008, i. E.

Rover, A. J. / *Veiga, L. A. O.*, Documento eletrônico e certificação diferente da ICP-Brasil, September 2003, abrufbar unter: http://www.conjur.com.br/static/text/3194,1.

Santolim, C. V. M., Formação e eficácia probatória dos contratos por computador, São Paulo 1995.

Santos, J. M. d. C., Código Civil Brasileiro interpretado principalmente sobre o ponto de vista prático, Bd. 3, Rio de Janeiro 1934.

Santos, M. A., Comentários ao Código de Processo Civil, v. 4, São Paulo 1973.

Santos, M. A., Prova judiciária no cível e comercial, São Paulo 1983.

Schemmann, T., Die Beweiswirkung elektronischer Signaturen und die Kodifizierung des Anscheinsbeweises in § 371 a Abs. 1 Satz 2 ZPO, ZZP 118, 161.

Schneier, B., Segurança.com: segredos e mentiras sobre a proteção na vida digital, Rio de Janeiro 2001.

Scholz, P., Datenschutz beim Internet-Einkauf: Gefährdungen – Anforderungen - Gestaltungen, Baden-Baden 2003.

Schoueri, L. E. (Hrsg.), Internet: o direito na era virtual, Rio de Janeiro 2001.

Schröder, K.-W., Uniforme elektronische Signaturen – Zum Problem der Massensignaturen im deutschen Signaturgesetz, DuD 2004, 665.

Schwemmer, J., Frontbericht 1.0: der steinige Weg zur digitalen Unterschrift, DuD 2000, 70.

Schwemmer, J., Lösungen und Probleme: Ein langer Weg zur Interoperabilität (mögliche Erklärungen), 2001, abrufbar unter: http://www.bundesnetzagentur.de/enid/45a2c67475c25a1edbc1d241712af8d0,0/Elektronische_Signatur/Veroeffentlichungen_pg.html.

Schwintowski, H.-P., Einführung in die Rechtsvergleichung, JA 1991, 241.

Silva, O. A. B. da, Curso de Processo Civil, v. 1, São Paulo 2001.

Silva Junior, R. L. / *Waisberg, I.* (Hrsg.), Comércio Eletrônico, São Paulo 2001.

Singh, S., O Livro dos Códigos, Rio de Janeiro 2002.

Skrobotz, J., "Lex Deutsche Bank": Das 1. SigÄndG – Anmerkungen zur Änderung des Signaturgesetzes (Stand 1. April 2004), DuD 2004, 410.

Spiegelhalder, T., Rechtsscheinhaftung im Stellvertretungsrecht bei der Verwendung elektronischer Signaturen, Hamburg 2007.

Stadler, T., Mobiles Bezahlen, Baden-Baden 2006.

Statistisches Bundesamt, Entwicklung der Informationsgesellschaft, IKT in Deutschland, Wiesbaden, 2007, abrufbar unter: https://www-ec.destatis.de/csp/shop/sfg/bpm.html.cms.cBroker.cls?cmspath=struktur,vollanzeige.csp&ID=1021037.

Stein, E. / *Frank, G.*, Staatsrecht, Tübingen 2000.

Strebel, H., Vergleichung und vergleichende Methode im öffentlichen Recht, ZaöRV 1964, 405.

Stuber, W.D. / *Franco, A. C. de P.*, A Internet sob a ótica jurídica, RT 749, 60.

Suárez, J. M. A. C., La firma y el comercio electrónico en España – comentarios a la legislación vigente, Elcano 2000.

Teixeira, R. V. G., O documento eletrônico como prova no procedimento monitório, RP 132, 83.

Tettenborn, A., Die Evaluierung des Signaturgesetzes und Umsetzung der EG-Signaturrichtlinie, in: Geis, I. (Hrsg.), Die digitale Signatur – eine Sicherheitstechnik für die Informationsgesellschaft, Eschborn 2000, 231.

Thedoro Júnior, Humberto, A onda reformista do direito positive e suas implicaçoes com o princípio da segurança jurídica, RP 136, 32.

Thomale, H.-C., Haftung und Prävention nach dem Signaturgesetz, Baden-Baden 2003.

Thomas,H. / *Putzo,H.* / *Reichold, K.* / *Hüßtege, R.*, Kommentar zur Zivilprozessordnung, 24. Auflage, München 2002.

Timm, B., Signaturgesetz und Haftungsrecht, DuD 1997, 525.

Ulrich, O., Elektronische Signaturen in Zukunftsbildern: kulturelle Reflexionen. In: Langenbach, C.J. / Ulrich, (Hrsg.). Elektronische Signaturen: Kulturelle Rahmenbedingungen einer technischen Entwicklung, Berlin-Heidelberg 2002.

Van Marsen Faren, D., Notas sobre o consumo e o conceito de consumidor – desenvolvimentos recentes, Boletim Científico Escola Superior do Ministério Público da União, Brasília 2002.

Viesca, M. I. /*Ruiz de Villa, D.*, Los prestadores de servicios de certificación en la contratación eletrónica, Elcano 2001.

Viefhues, W. / *Hoffmann, H.*, Gesetz zur Verhinderung des elektronischen Rechtsverkehrs? – Praktische Auswirkungen des Diskussionsentwurfs und Anpassungsbedarf an die Regelungen bei den Gerichten der Europäischen Gemeinschaften, MMR 2003, 71.

Volpi Neto, A., Comércio eletrônico: direito e segurança, Curitiba 2002.

Wiesner, B., Key Recovery, DuD 2000, 698.

Wilke, D. / *Jandt, S.* / *Löwe, J.* / *Roßnagel, A.*, Eine Beweisführung von Format – Die Transformation signierter Dokumente auf dem Prüfstand, CR 2008, 607.

Winkler, K., Beurkundungsgesetz, 15. Auflage, München 2003.

Wohlmacher, P. / *Fox, D.*, Hardwaresicherheit von Smartcards, DuD 1997, 260.

Zajtay, I., Beiträge zur Rechtsvergleichung – Ausgewählte Schriften -, Tübingen 1976.

Zöller, R., Kommentar zur Zivilprozessordnung, 26. Auflage, Köln 2007 (zitiert als: Bearbeiter, in: Zöller).

Zweigert, R. / *Kötz, H.*, Einführung in die Rechtsvergleichung auf dem Gebiete des Privatrechts, Tübingen 1996.