Das Beweisrecht elektronischer Dokumente

Prof. Dr. Helmut Rüßmann, Universität des Saarlandes

Inhaltsübersicht:

Juristen, die der EDV-Szene nahestehen, gilt das deutsche Beweisrecht als rückständig, weil es elektronische Dokumente den Regeln des Augenscheinsbeweises unterwirft und nicht den für schriftliche Dokumente geltenden Regeln des Urkundenbeweises. Immer wieder wird der Ruf nach dem Gesetzgeber laut, dem elektronischen Dokument unter bestimmten Voraussetzungen (elektronische Unterschrift) Urkundenqualität zu verleihen(1) oder doch wenigstens dem elektronischen Dokument eine dem § 416 ZPO nachempfundene Beweisregel zur Seite zu stellen(2). Die Alternative des Augenscheinsbeweises(3) wird für unzureichend gehalten. Ja, man sieht sogar den Wirtschaftsstandort Deutschland in Gefahr, wenn nicht der Gesetzgeber im Sinne der Proponenten tätig werde (4). Und *Kilian* nennt als einen Grund für die Aufnahme der Schiedsgerichtsklausel in den deutschen EDI-Rahmenvertrag die Ungeeignetheit der Beweisregeln des staatlichen Prozesses(5) . Man verweist auch gern auf ausländische Regelungen, die die elektronischen Dokumente beweisrechtlich den Dokumenten in der traditionellen Schriftform gleichstellen(6). Leider zeichnen sich die bisher vorgelegten Analysen weder durch eine gründliche Aufarbeitung des deutschen Beweisrechts(7) noch durch eine den Ansprüchen ernsthafter Rechtsvergleichung genügende Auswertung ausländischer Beweisrechte aus. Der folgende Beitrag (8) zielt darauf ab, allfällige Mißverständnisse zum deutschen und zu ausländischen Beweisrechten auszuräumen. Sein Fazit wird sein, daß eine Änderung des deutschen Beweisrechts durch den Gesetzgeber nicht geboten ist und daß die ausdrücklichen Gleichstellungen der elektronischen und

der schriftlichen Dokumente in ausländischen Rechten der Überwindung hausgemachter Probleme dienen, die das deutsche Recht nicht kennt. Zur Inhaltsübersicht

Das elektronische Dokument im deutschen Beweisrecht

Im deutschen Beweisrecht geht es für das elektronische Dokument zunächst um die Alternative des Augenscheins- oder Urkundenbeweises. Da der Augenscheinsbeweis das Auffangbecken für alle die Beweisstücke ist, die nicht die Merkmale eines der anderen Beweismittel erfüllen, bedarf es der Analyse des Urkundenbeweises und eines Vergleichs mit den Regeln des Augenscheinsbeweises, um sich Klarheit über die Eignung des einen oder anderen Regelungskomplexes zu verschaffen. Für die Analyse des Urkundenbeweises kann man die öffentlichen Urkunden aus der weiteren Betrachtung ausscheiden. Sie erweisen sich als praktisch problemlos, weil, wenn man eine Papierdokumentation öffentlicher Stellen auf eine elektronische Dokumentation umstellt, in der Regel ausdrücklich bestimmt wird, welche Bedeutung einerseits ein Eintrag in die elektronische Dokumentation und andererseits Ausdrucke aus der elektronischen Dokumentation haben. So ist der Eintrag in das Grundbuch als automatisierte Datei materiellrechtlich die Eintragung in das Grundbuch, und prozeßrechtlich weist man den Inhalt des Grundbuchs durch Ausdrucke nach, von denen § 131 GBO bestimmt:

Wird das Grundbuch in maschineller Form als automatisierte Datei geführt, so tritt an die Stelle der Abschrift der Ausdruck und an die Stelle der beglaubigten Abschrift der amtliche Ausdruck. Die Ausdrucke werden nicht unterschrieben. Der amtliche Ausdruck ist als solcher zu bezeichnen und mit einem Dienstsiegel oder stempel zu versehen; er steht einer beglaubigten Abschrift gleich.

Für die Analyse wichtiger als die öffentlichen Urkunden sind die Privaturkunden und die ihnen korrespondierenden privaten elektronischen Dokumentationen. In einer Privaturkunde kann eine Willenserklärung(9) oder eine Wissenserklärung(10) verbrieft sein. Für das erste mag die Annahme eines Vertragsangebots, für das zweite die ärztliche Dokumentation stehen. Ob die Beweisregel des § 416 ZPO nur die eine oder die andere Art der Erklärung erfaßt, ist streitig. Was sie für die jeweilige Erklärungsart bedeutet, kann indessen ohne eine Entscheidung des Streits festgehalten werden. Zur Inhaltsübersicht

Die Bedeutung des § 416 ZPO für Wissenserklärungen

Für Wissenserklärungen bedeutet die Beweisregel des § 416 ZPO nichts. Dies zeigt das Zusammenspiel der §§ 439, 440 ZPO mit § 416 ZPO. Die Beweisregel des § 416 ZPO greift nur, wenn die Urkunde echt ist. Echtheit der Urkunde bedeutet, daß die Urkunde so, wie sie erscheint, von dem hergestellt ist, von dem sie nach der Behauptung des Beweisführers stammt. Über die Echtheit ist nach §§ 439, 440 ZPO zu befinden. Das geschieht ohne Bindung an Beweisregeln im Rahmen freier Beweiswürdigung(11). Nur wenn die Echtheit der Unterschrift feststeht, also anerkannt oder zur vollen Überzeugung des Gerichts bewiesen ist, besteht eine widerlegliche Vermutung auch für die Echtheit der Urkunde. Kommt das Gericht auf diesem Wege zu dem Ergebnis, daß die Urkunde echt ist, gilt § 416 ZPO. Schon auf Grund der Begriffsmerkmale für die Echtheit steht damit fest, daß die Urkunde mit Inhalt vom Aussteller stammt. Eine Beweisregel, die in der Rechtsfolge das anordnet, was in den Tatbestandsvoraussetzungen für das Eingreifen der Beweisregel festgestellt werden muß, ist überflüssig. Im Alternativkommentar zur Zivilprozeßordnung habe ich das im Anschluß an eine in Logik und Sprachphilosophie eingeführte Begriffsbildung so ausgedrückt, daß die Beweisregel die Geltung eines analytisch wahren Satzes anordne(12). Zur Inhaltsübersicht

Die Bedeutung des § 416 ZPO für Willenserklärungen

Für Willenserklärungen gilt das soeben für Wissenserklärungen Ausgeführte ebenso, wenn Inhalt der Beweisregel nur sein sollte, daß die Urkunde von dem stammt, der sie nach der Behauptung des

Beweisführers errichtet haben soll(13). Es könnten aber auch zwei andere Bedeutungen in Betracht kommen. Die eine geht dahin, nicht nur die Äußerung der Erklärung, den willentlichen Skripturakt, sondern auch die Tatsache, daß die Erklärung willentlich in den Verkehr gebracht wurde, als von der Beweisregel umfaßt anzusehen(14), die andere dahin, den materiellrechtlichen Tatbestand der Abgabe der Willenserklärung als jeder Widerlegung entzogen bewiesen zu betrachten(15). Das sind beides Bedeutungen, die der Beweisregel des § 416 ZPO einen über die zu ihrem Eingreifen erst festzustellende Echtheit der Urkunde hinausweisenden Regelungsgehalt geben und damit die Beweisregel überhaupt als sinnvoll erweisen. Auf den ersten Blick scheinen diese Bedeutungen deckungsgleich. Dem ist indessen nicht so. Das allerdings erschließt sich erst durch einen Blick auf die materiellrechtlichen Konsequenzen der beiden Auffassungen. Im materiellen Recht mögen im einzelnen die Rechtsfolgen umstritten sein, welche an Erklärungen geknüpft werden, die ohne Willen des Erklärenden seine Sphäre verlassen haben. Diskutiert wird insbesondere, ob eine Willenserklärung gar nicht erst abgegeben wurde, aber gleichwohl unter bestimmten Voraussetzungen Vertrauensschaden analog § 122 BGB ersetzt werden muß(16), oder aber ob die Willenserklärung vom Erklärenden durch Anfechtung beseitigt werden muß bzw. im Sinne eines Wahlrechts auch aufrechterhalten werden kann (17). Zur Inhaltsübersicht

Beweiskraft für das Inverkehrbringen der Erklärung

Die Diskussion um Anfechtungsmöglichkeit und/oder Vertrauensschadensersatz kann unter der Annahme der ersten Bedeutung der Beweisregel des § 416 ZPO nicht sinnvoll geführt werden, weil sie es nicht zuließe, im Prozeß geltend zu machen, daß die Erklärung die Sphäre des Erklärenden ohne seinen Willen verlassen habe.

Dies mag man sich an zwei Beispielen vergegenwärtigen, in denen schriftliche Erklärungen ohne Willen des Verfassers auf den Weg gebracht und später im Original im Prozeß als Gegenstand des Urkundenbeweises vorgelegt werden. Hinsichtlich des im Allgemeinen Teil des Bürgerlichen Rechts klassischen Schulfalls einer Vertragsannahme, die fertig ausgefüllt und unterschrieben über Nacht zwecks weiteren Bedenkens liegen bleiben soll und von der Sekretärin versehentlich zur Post gebracht wird, könnten die materiellrechtlichen Fragen der Abgabe, der Anfechtung und des Vertrauensschadens nicht mehr beachtlich sein. Denn § 416 ZPO ordnete im Wege einer Fiktion an, daß die Urkunde willentlich in den Verkehr gebracht worden sei. Die daran anknüpfende Subsumtion führte zwingend zu dem Ergebnis, daß eine Abgabe und kein Anfechtungsgrund wegen "abhandengekommener Willenserklärung" vorliege. Keine der Parteien könnte sich mehr auf Rechtsfolgen berufen, die tatbestandlich voraussetzen, daß die Erklärung nicht willentlich in den Verkehr gebracht wurde, selbst wenn dies mit anderen Beweismitteln sicher bewiesen werden könnte. Das gleiche Ergebnis würde eintreten im zweiten Beispiel einer Wissenserklärung im weiteren Sinne, wenn man diese nicht ohnehin aus dem Anwendungsbereich des § 416 ZPO aussondert. Auch der Schmähbrief, mit dem der Verfasser sich seine Wut vom Leib schreiben, nicht aber den Adressaten erreichen wollte, mag aufgrund derselben Eilfertigkeit sein ungeplantes Ziel erreicht haben. Zu den materiellrechtlichen Fragen, ob die Persönlichkeitsverletzung dem Schreiber kausal zugerechnet werden kann und ob er sie zu vertreten hat, käme das erkennende Gericht regelmäßig nicht, weil es ohne Wertungsmöglichkeit nach § 416 ZPO daran gebunden wäre, daß die Erklärung gerade doch mit Willen des Verfassers in den Verkehr gebracht wurde.

Eine tatsächliche Vermutung für die willentliche Absendung der Erklärung mag daher bestehen, wenn der Beweisführer die Urkunde in Händen hält. Der Beweis, daß die Erklärung nicht willentlich in Umlauf gebracht wurde, muß aber, gleich wie man die materiellen Rechtsfolgen einer derartigen Sachlage genau ausgestaltet, prozessual zulässig sein. Daraus folgt, daß von der Beweisregel des § 416 ZPO nicht umfaßt sein kann, daß der Aussteller die Erklärung im tatsächlichen Sinne in den Verkehr gebracht hat. Zur Inhaltsübersicht

Beweiskraft für die Abgabe der Erklärung

Wenn die Beweisregel des § 416 ZPO überhaupt einen sinnvollen Anwendungsbereich haben soll, bleibt als einzige Deutung der Beweis für den materiellrechtlichen Abgabetatbestand.

Mit der soeben abgelehnten Deutung der Beweisanordnung, daß unwiderleglich die Erklärung willentlich in den Verkehr gebracht wurde, ist die Regelung einer Abgabe im Sinne von § 130 BGB nicht identisch. Denn nach diesem Normverständnis wird dem Aussteller, dem im Prozeß die von ihm stammende Privaturkunde vorgehalten wird, nur der Einwand abgeschnitten, er habe die hierin verkörperte Willenserklärung nicht abgegeben. Soweit es aus anderen Gründen als denen der Abgabe der Willenserklärung auf die Tatfrage ankäme, ob die Erklärung "abhandengekommen" sei, könnte dieser Einwand nicht an § 416 ZPO scheitern. Insbesondere bliebe diese Tatsache als Voraussetzung der Anfechtbarkeit der als abgegeben geltenden Willenserklärung beweisbar.

Allerdings verändert ein Verständnis, wonach § 416 ZPO die materiellrechtliche Abgabe fingiert, die methodische Struktur der Beweisregel. Denn bewiesen wird nicht mehr eine Tatsache - "der Aussteller hat diese Erklärung geäußert (und in den Verkehr gebracht)" -, auf die aufgrund einer anderen Tatsachenbasis - "echte unterschriebene Urkunde" - kraft formeller Regel und ohne Wertungsmöglichkeit geschlossen wird. Vielmehr handelt es sich nunmehr um den unwiderleglichen Schluß von der Tatsachenbasis auf die festgestellte Erfüllung eines gesetzlichen Tatbestandsmerkmals ("Abgabe einer Willenserklärung"). Die Beweisregel entzieht demnach nicht (nur) die richterliche Befugnis zur freien Beweiswürdigung, sondern ersetzt auch die Subsumtion. Diese Normstruktur ist aber bei Vermutungen und Beweisregeln keineswegs ungewöhnlich. Auch § 417 ZPO umfaßt mit dem vollen Beweis des Inhalts amtlicher Entscheidungen nicht nur den Schluß auf eine Tatsache - "eine Entscheidung ist niedergeschrieben worden" -, sondern füllt damit einen rechtlichen Tatbestand aus - "die Entscheidung ist ergangen". Im übrigen bleibt die so verstandene Regel trotz ihrer methodischen Erweiterung im Umfang hinter dem reinen Tatsachenschluß zurück. Denn die den Tatbestand ausfüllenden Tatsachen werden ja gerade nicht fingiert und stehen daher für andere Subsumtionsvorgänge zur Disposition. Dagegen bezieht die andere Ansicht(18) zwar den Tatbestand der Abgabe nicht (ausdrücklich) in die Beweisregel ein; eine Beschränkung auf die Beweistatsache - "willentlich in den Verkehr gebracht" - führte aber konsequenterweise und wie soeben exemplifiziert dazu, daß bei der an sich noch freien Subsumtion nicht nur bei der tatbestandlichen Abgabe der Willenserklärung(19) keine andere Entscheidung mehr möglich wäre, sondern auch beim daran anschließenden § 119 Abs. 1 BGB die Voraussetzungen einer Anfechtung zwingend abzulehnen wären. Zur Inhaltsübersicht

Zwischenergebnis für das Beweisrecht der Privaturkunde

Fassen wir die beweisrechtliche Situation für Privaturkunden zusammen, so ergibt sich:

- der Echtheitsbeweis (§§ 439, 440 ZPO) unterliegt der freien Beweiswürdigung, es besteht lediglich eine widerlegliche Vermutung für die Echtheit der Urkunde, wenn die Unterschrift unstreitig oder nachweislich echt ist;
- für die echte Urkunde gilt die Beweisregel des § 416 ZPO, wenn die Urkunde unterschrieben oder mittels notariell beglaubigten Handzeichens unterzeichnet ist; für eine echte, aber nicht in dieser Weise gezeichnete Urkunde gilt keine Beweisregel, sondern der Grundsatz der freien Beweiswürdigung;
- enthält die echte und im Sinne des § 416 ZPO gezeichnete Urkunde keine Willenserklärung, so geht die Beweisregel ins Leere, weil die "Abgabe" der Erklärung schon zur Feststellung der Echtheit zur Überzeugung des Gerichts bewiesen sein muß; der Wahrheitsgehalt der Wissenserklärung unterliegt immer der freien Beweiswürdigung;
- enthält die echte und im Sinne des § 416 ZPO gezeichnete Urkunde eine Willenserklärung, so steht aufgrund der Beweisregel des § 416 ZPO der materiellrechtliche Tatbestand der Abgabe der Willenserklärung unwiderleglich fest. Daß die Urkunde ohne Willen des Ausstellers in den Verkehr gebracht worden ist, kann zur Begründung von Rechtsfolgen außerhalb des Abgabetatbestands immer noch bewiesen werden. Zur Inhaltsübersicht

Der Ertrag für elektronische Dokumente

Was läßt sich aus diesen Regeln für elektronische Dokumentationen gewinnen, wenn wir sie *de lege lata* oder *de lege ferenda* den Urkunden gleichsetzen? Wenig!

- der Echtheitsbeweis des elektronischen Dokuments unterliegt der freien Beweiswürdigung; allenfalls bei einem elektronisch signierten Dokument könnte entsprechend § 440 Abs. 2 ZPO eine Vermutung auch für die Echtheit des Dokumentes gelten, wenn die elektronische Unterschrift nachweislich echt ist. Unter dieser Voraussetzung wird ein verständiger Richter aber auch ohne die gesetzliche Vermutung kaum zu einem anderen Ergebnis kommen können, als vom Beweisgegner den Nachweis des Mißbrauchs der echten Unterschrift zu verlangen;
- wollte man in der elektronischen Unterschrift ein Analogon zur Zeichnungsvoraussetzung des § 416 ZPO sehen, so käme die Beweisregel des § 416 ZPO nur für elektronisch dokumentierte Willenserklärungen zum Zuge. Sie entzöge den materiellrechtlichen Abgabetatbestand dem prozeßrechtlichen Zweifel, ließe es aber durchaus offen, das Inverkehrbringen des elektronischen Dokuments für Rechtsfolgen jenseits des Abgabetatbestandes zu bestreiten und zur Überzeugung des Gerichts zu widerlegen;
- für Wissenserklärungen ist die "Abgabe" schon mit dem Echtheitsbeweis, d.h. vor Eingreifen der Beweisregel geführt;
- der Inhalt der Wissenserklärung unterliegt ohnehin der freien Beweiswürdigung.

Stellt man diesen Regeln der "urkundsähnlichen Behandlung" elektronischer Dokumente die Regeln gegenüber, die sich bei einer Behandlung elektronischer Dokumente als Gegenstände des Augenscheinsbeweises ergeben, so sind die Unterschiede minimal und für alle praktischen Zwecke vernachlässigbar. Das elektronische Dokument unterliegt insgesamt der freien Beweiswürdigung, nicht nur die Fragen, ob das Dokument von dem durch den Beweisführer angegebenen Aussteller stammt, und ob denn das richtig ist, was im Inhalt des Dokuments dokumentiert wird, sondern auch die Frage, ob, wenn es denn einmal zu einer elektronischen Unterschrift kommt, die Voraussetzungen für den materiellrechtlichen Abgabetatbestand erfüllt sind. Das Hauptaugenmerk der Praxis wird dem Echtheits- und dem Inhaltsproblem einer elektronischen Dokumentation gewidmet sein. Sind die mit ihm zusammenhängenden Fragen zur Überzeugung des Gerichts gelöst, so fällt, wenn eine Willenserklärung dokumentiert wird, der materiellrechtliche Abgabetatbestand regelmäßig als Nebenprodukt dieser Lösung ab, ohne daß es dafür einer eigenständigen Beweisregel bedürfte.

Die Befürchtung, ein unzureichendes Beweisrecht könne sich als Investitionshindernis riesigen Ausmaßes erweisen(20), findet nach alledem im geltenden Beweisrecht keine Stütze. Auch im materiellen Recht der Rechtsgeschäftslehre verfügt die Rechtsdogmatik über hinreichende Möglichkeiten, dem elektronischen Rechts- und Geschäftsverkehr einen sicheren Boden zu bereiten (21). Ob Formvorschriften sie stehen in der Tat einem Vertragsschluß mittels EDV und Telekommunikation im Wege den Siegeszug des elektronischen Geschäftsverkehrs hindern, müßte erst noch belegt werden. Für Grundstückskaufverträge und Bürgschaftserklärungen via Btx und EDI sehe ich keinen Bedarf. Ihr Ausschluß aus den telekommunikativ abzuschließenden Rechtsgeschäften kann doch kaum für die Zurückhaltung von Investitionen in Milliardenhöhe verantwortlich sein. Vor Psychosen kann allerdings auch die Rechtsdogmatik Unternehmen nicht bewahren, die schlecht beraten vor Investitionsentscheidungen zurückschrecken.

Die einzige Frage, die sich ernsthaft stellt, ist die, wie das Gericht das Echtheits- und Inhaltsproblem bei elektronischen Dokumenten im Rahmen der freien Beweiswürdigung lösen kann. Zur Inhaltsübersicht

Der Beweiswert von elektronischen Dokumenten

Die Antwort auf die Frage hängt von den Gefahren ab, die die Verläßlichkeit der elektronischen Dokumentation bedrohen. Letztendlich ist das Gericht daran interessiert, daß das, was dokumentiert ist, auch der Wahrheit entspricht. Teilaspekte dieses Interesses sind die Authentizität und die Integrität der Dokumentation. Zur Inhaltsübersicht

Die elektronische Lüge

Die Gefahren für die Verläßlichkeit der Dokumentation können von dem ausgehen, der die Dokumentation erstellt. Erstellt er die Dokumentation von vornherein so, daß sie nicht das dokumentiert, was tatsächlich geschehen ist, so enthält die Dokumentation eine Lüge oder auch eine irrtümliche Abweichung von der Wahrheit. Dagegen ist bei elektronischen Dokumentationen so wenig ein Kraut gewachsen wie gegen die schriftliche Lüge oder den Irrtum in an die Schriftform gebundenen Dokumentationen. Ob der Behandlungsverlauf bei einem Arzt schriftlich oder elektronisch dokumentiert wird, spielt für die Ursprungsverfälschung keine Rolle. Die Bewertung kann sich ändern, wenn eine ursprüngliche Fassung der Dokumentation nachträglich korrigiert wird. Während man das der schriftlichen Dokumentation unter Umständen ansehen oder durch besondere Analyseverfahren feststellen kann, sind nachträgliche Änderungen einer elektronischen Dokumentation prinzipiell spurenlos und der Dokumentation als solcher nicht anzusehen. Hier können Urkunden im Rahmen der freien Beweiswürdigung mehr Sicherheit gewähren als elektronische Dokumente einschließlich ihrer Ausdrucke. Das sei an einem einfachen Beispiel erläutert.

Wenn ich meinem PC einen Bericht anvertraue und dieser Bericht in einem Beweisverfahren eine Rolle spielen sollte, kann der Bericht zum Zwecke der Vorlage an das Gericht manipuliert werden, ohne daß das Gericht oder ein gerichtlicher Sachverständiger diese Manipulation nachweisen könnte. Für den Ausdruck versteht sich das von selbst, weil man dem Ausdruck nicht ansehen kann, wann der Bericht verfaßt worden ist und ob in ihn nachträglich Änderungen eingefügt worden sind. Man kann das aber nicht nur dem Ausdruck nicht ansehen, man kann es auch durch eine Untersuchung der Datei auf der Platte, dem elektronischen Speichermedium, nicht feststellen. Obwohl das Betriebssystem des Computers den Zeitpunkt der Speicherung nach Datum und Zeit sekundengenau registriert und die Datei mit einem entsprechenden Zeitstempel versieht, ist diese Information nicht verläßlich für den wirklichen Zeitpunkt der Speicherung, weil ein kleiner Handgriff genügt, um die Systemzeit des Rechners umzustellen und einen Zeitstempel für die Speicherung zu erhalten, der mit dem tatsächlichen Zeitpunkt der Speicherung nichts gemein hat. Niemand kann dem elektronischen Speichermedium diese Manipulation ansehen. Das nur in dieser Form ohne weitere Vorkehrungen Gespeicherte erweist sich im Streitfalle als wertlos. Die Situation ändert sich, wenn das Gespeicherte einem nicht änderbaren Datenträger anvertraut oder der änderbare Datenträger einem vertrauenswürdigen Dritten zur Verwahrung übergeben und auf diese Weise sichergestellt wird, daß die unter Umständen an Änderungen interessierte Partei keine Möglichkeit zu Änderungen hatte. Sie ändert sich auch, wenn System-, Programm- und Dateizugriffe lückenlos dokumentiert werden und sich dieser Zusatzdokumentation entnehmen läßt, wann wer mit welchem Programm auf eine Datei zugegriffen hat(22). Die uns aus dem PCBereich vertrauten Betriebssysteme und Programme bieten solche Funktionen nicht standardmäßig an. Zur Inhaltsübersicht

Unberechtigte Dateizugriffe Dritter

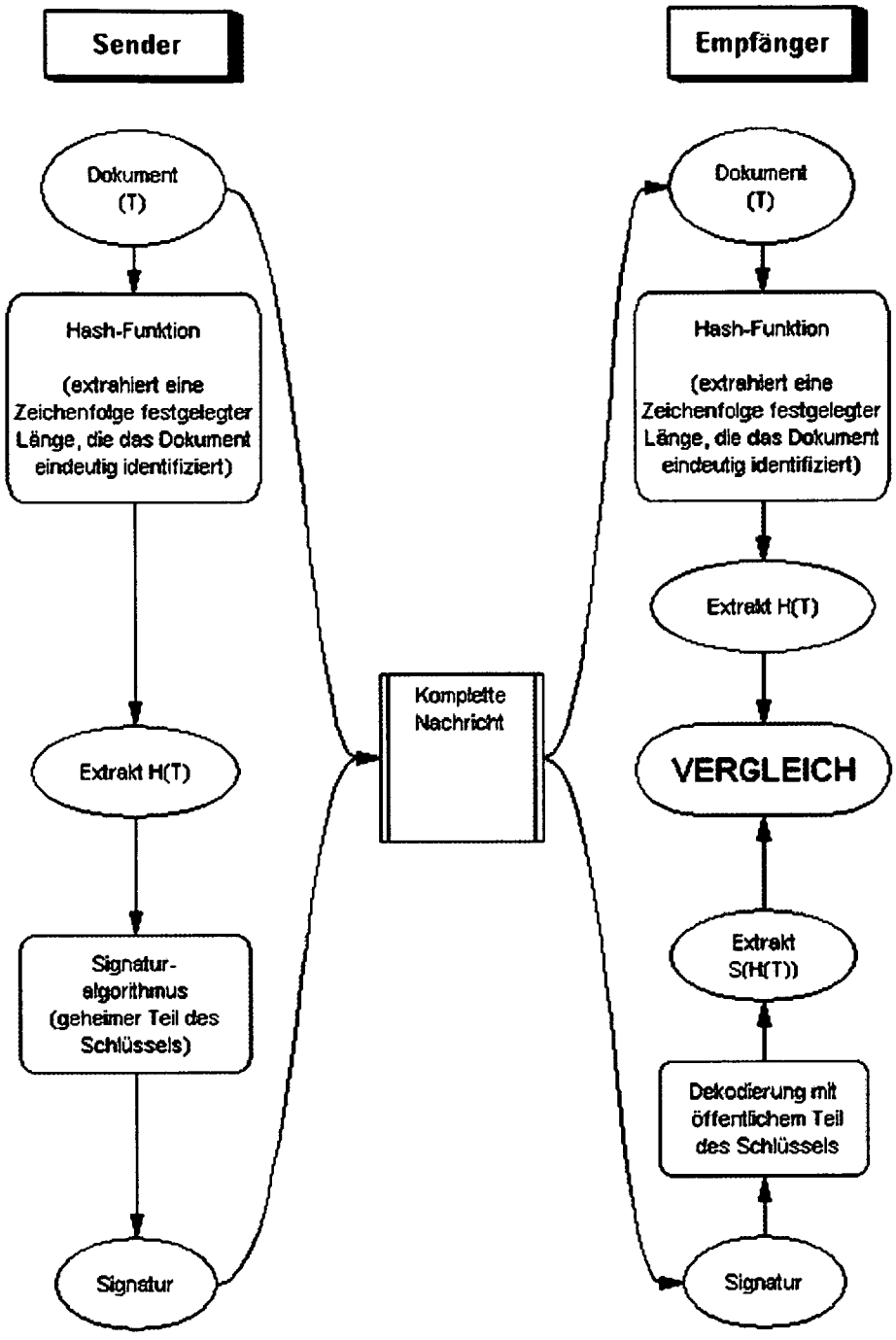
Die Gefahren können aber auch von Dritten ausgehen, die an sich mit der Erstellung der Dokumentation nichts zu tun haben. Die Dritten können am dokumentierenden Rechner selbst oder bei vernetzten Rechnern über das Netz in das Rechnersystem eindringen und die Dokumentation verändern. Sie können sich aber auch in eine Leitung hängen, das auf dem Transport befindliche Dokument abfangen, es ändern und in der geänderten Fassung wieder auf den Transportweg bringen. Das elektronische Dokument ist um so vertrauenswürdiger, je stärker die Vorkehrungen sind, um solche Verfälschungen oder Unterschiebungen von dritter Seite zu verhindern: paßwortgeschützter Rechnerzugang bei Einzelrechnern und in Rechnernetzen, Verteilung der Plattenzugriffs- sowie der

Programm- und Dateinutzungsrechte nach Sachzuständigkeit und Zugriffsnotwendigkeit, Schutz einzelner Dateien durch Verschlüsselung mit Hilfe kryptografischer Methoden, Geheimhaltung der zur Verschlüsselung verwendeten Kennwörter, Schutz der Dateien durch elektronische Signaturen, Protokollierung aller Rechner-, Programm- und Dateizugriffe. Zur Inhaltsübersicht

Elektronische Signaturen

In Sonderheit die elektronischen Signaturen haben in jüngerer Zeit die Aufmerksamkeit der Juristen gefunden. Ihnen widmeten sich eine Studie der Gesellschaft für Mathematik und Datenverarbeitung (GMD) "Bestandsaufnahme über die elektronischen Signaturverfahren"(23), ein von der Bundesnotarkammer in Zusammenarbeit mit TeleTrusT Deutschland e.V. veranstaltetes Forum "Elektronischer Rechtsverkehr"(24) sowie mehrere Arbeitskreise des jährlich in Saarbrücken an der Universität des Saarlandes veranstalteten Deutschen EDVGerichtstages(25). Damit hat es folgendes auf sich: Die elektronische Signatur soll sicherstellen, daß eine Datei nicht unbemerkt von dritter Seite verändert wird. Dem dienen schon immer die Vergabe von Zugriffsrechten für eine einzelne Datei wie die Verschlüsselung der Datei mit Hilfe kryptografischer Verfahren. Laden, lesen und verändern kann ein solches Dokument nur, wer über den Schlüssel, das Kennwort, verfügt, mit dessen Hilfe das elektronische Dokument verschlüsselt worden ist. Will man einem anderen als sich selbst auch nur eine Leseberechtigung erteilen, so muß man ihm das Schlüsselwort offenbaren. Das wird jedenfalls dann unpraktisch, wenn man mit vielen verschiedenen Teilnehmern im elektronischen Verkehr kommunizieren will. Dann müßte man, weil man ja nicht jedem Zugriff auf alle Dokumente erlauben will, mit jedem einzelnen ein eigenes Schlüsselwort vereinbaren, mit dem man als Ersteller die Dokumente verschlüsselt und als Leser die Dokumente entschlüsselt. Ein weiteres kommt hinzu: Der Leser, der ein Dokument entschlüsseln kann, kann dieses Dokument auch verändern. Und diese Manipulationsmöglichkeiten könnten dem Rechts- und Geschäftsverkehr abträglich sein. Hier nun kommt die elektronische Signatur ins Spiel. Sie soll die Verschlüsselung des elektronischen Dokuments ermöglichen, seine Veränderung ausschließen und zudem für eine Vielzahl von Kommunikationspartnern geeignet sein, von denen die Adressaten das Dokument lesen können, ohne das Schlüsselwort zu kennen, mit dem das Dokument verschlüsselt worden ist. Technisch funktioniert das mit einem Paar von Schlüsseln, von dem jeder der Kommunikationspartner genau eines hat. Dieses Paar besteht aus einem geheimen Schlüssel, der zum Signieren verwendet wird und ausschließlich bei der signierenden Person verbleibt, und aus einem öffentlichen Schlüssel, der zur Prüfung der Signatur verwendet wird und jedem zur Verfügung gestellt werden kann. Ist ein Dokument mit der elektronischen Signatur versehen, kann es von niemandem mehr unentdeckt verändert werden. Ein unverändertes Dokument muß mithin von dem stammen, der das Dokument mit dem geheimen Schlüssel signiert hat.

Im Ablaufmodell gewinnt das Ganze folgende Gestalt:



Ablaufmodell der Versendung einer Nachricht mit elektronischer Signatur

Die elektronische Signatur verlangt für den praktischen Einsatz die Einrichtung einer Infrastruktur, die die eindeutige Vergabe der Schlüsselpaare organisiert, jeder Person einen eindeutigen öffentlichen Schlüssel zuordnet und den öffentlichen Schlüssel verfügbar macht. Man denkt an die Einrichtung eines oder mehrerer Trustcenter, das die Schlüsselpaare erzeugt und vergibt, den öffentlichen Schlüssel zertifiziert und verfügbar macht und für die aus sicherheitstechnischen Gründen favorisierte Hardwarelösung beim geheimen Schlüssel Chipkarten mit dem geheimen Schlüssel erzeugt, die nicht ausgelesen werden können und deren Verwendung allein durch den berechtigten Schlüsselinhaber man durch Bindung an eine PIN, die deutlich länger als vier Stellen sein darf, oder durch biometrische Verfahren sichern kann.

Ein solches allgemein etabliertes Trustcenter gibt es in Deutschland bisher noch nicht. Allerdings bietet die Telekom mit Telesec einen Dienst an, der große Teile des beschriebenen

Aufgabenspektrums zu erfüllen verspricht. Ich zitiere aus der telekom-eigenen Leistungsbeschreibung(26) :

Eine der Voraussetzungen für die Kommunikationssicherheit mit Telesec ist das asymmetrische Verfahren auf Basis des RSA-Algorithmus(27) . Mit diesem Verfahren kann sowohl eine personenbezogene Verschlüsselung vorgenommen als auch eine digitale Signatur erzeugt werden. Die Kommunikationspartner erhalten dabei zunächst jeweils ein individuelles Schlüsselpaar, bestehend aus einem öffentlichen und einem dazu komplementären geheimen Schlüssel.

Die öffentlichen Schlüssel sind beiden Partnern bekannt und darüber hinaus im Prinzip auch jedem weiteren potentiellen Kommunikationspartner zugänglich. Die geheimen Schlüssel dagegen verbleiben beim einzelnen Kommunikationspartner, sicher aufbewahrt in seiner persönlichen Chipkarte.

Die Verschlüsselung einer Botschaft

Um dem Kommunikationspartner B nun eine verschlüsselte Botschaft zukommen zu lassen, muß Partner A dessen öffentlichen Schlüssel benutzen. Mit diesem öffentlichen Schlüssel von B wird nun eine Klartextbotschaft in eine nicht interpretierbare scheinbare Zufallsfolge von Zeichen verwandelt (kryptographisches Verfahren).

Der Empfänger B kann nun mittels seines geheimen Schlüssels die Botschaft wieder entschlüsseln. Daß irgendein anderer die Botschaft mit seinem geheimen Schlüssel entziffert, ist dabei ausgeschlossen.

Denn um die mit dem öffentlichen Schlüssel von B codierte Nachricht zu dechiffrieren, ist nur der zum öffentlichen Schlüssel von B komplementäre geheime Schlüssel von B in der Lage.

Die elektronische Unterschrift

Zur elektronischen Signatur, das heißt zur Sicherung der Authentizität einer Nachricht, wird folgender Prozeß benutzt: Kommunikationspartner A erstellt einen Klartext, der dann zunächst einem Komprimiervorgang zugeleitet wird, einer sogenannten Hash-Funktion. Diese hat die Eigenschaft, daß sie einen beliebig langen Text zu einem Block von 512 bit reduziert. Ein Vorgang, der aus Effektivitätsgründen erfolgt und die Menge der zu übermittelnden Daten begrenzt(28).

Das fertige Komprimat wird nun mit Hilfe des geheimen Schlüssel von A verschlüsselt und ist somit für jeden beliebigen Empfänger B zweifelsfrei dem Partner A als Absender zuzuordnen. Hierzu wird die Signatur, die dem Klartext beigefügt wurde, vom Empfänger B mit dem bekannten öffentlichen Schlüssel von A wieder entschlüsselt. So erhält B das von A gefertigte und signierte Hash-Komprimat.

Wendet nun B den gleichen Hash-Algorithmus auf den empfangenen Klartext von A an, kann er dieses Hash-Komprimat mit dem von Partner A übermittelten Komprimat vergleichen. Sind beide Komprimate identisch, so ist die Echtheit der Unterschrift und damit die Authentizität der Nachricht gewährleistet.

Wie hat der Benutzer die Gewähr, daß die ihm ausgehändigte Sicherheitstechnik, wie z.B. die Chipkarte, vertrauenswürdig ist und dem Stand der Technik entspricht?

Die Telekom läßt sowohl ihr Trust-Center für die Ausgabe der Chipkarten wie auch alle von ihr angebotenen Sicherheitsendgeräte von allseits anerkannten und unabhängigen Stellen überprüfen. Diese Überprüfungen oder Validierungen werden dabei natürlich nach den anerkannten Kriterien der Computersicherheit (COMPUSEC) und der Kommunikationssicherheit (COMSEC) durchgeführt.

Die hierzu notwendigen Grundsatzregeln hat das BSI, das Bundesamt für Sicherheit und Informationstechnik, bereits in ihrem IT-Kriterien-Katalog festgelegt. Eben diese Kriterien sind in umfangreichen Prüfspezifikationen auf die konkreten Techniken bei Endgeräten und beim Trust-Center angepaßt worden.

Auf diesem Wege erreicht Telesec alle von Telekom anvisierten Voraussetzungen einer vertrauenwürdigen Sicherheitsdienstleistung: die Transparenz der eingesetzten Sicherheitstechniken ebenso wie die Öffentlichkeit des Kryptoverfahrens und die Standardisierung der Schnittstellen zwischen Sicherheits- und Anwendungskomponenten. Die Autarkie der Ende-zu-Ende-Kommunikation genauso wie die Konzentration der zentralen Sicherheitseinrichtungen für das Schlüsselmanagement in einem Trust-Center und die Prüfung aller Sicherheitskomponenten durch den RWTÜV als neutrale technische Instanz. Zur Inhaltsübersicht

Ergebnis zum Beweisrecht elektronischer Dokumente (Deutschland)

Die beweisrechtlichen Überlegungen zur Behandlung elektronischer Dokumente lassen sich nach diesem kursorischen Überblick über die Möglichkeiten zur Sicherung von Authentizität und Integrität von elektronischen Dokumenten wie folgt zusammenfassen:

- Das deutsche Zivilprozeßrecht kennt keine rechtlichen Schranken für die Beweisführung mit Hilfe elektronischer Dokumente. Elektronische Dokumente sind zulässige Beweismittel. Sie unterfallen dem Augenscheins- und dem Sachverständigenbeweis. Der Augenscheinsbeweis ist angesprochen, soweit das Gericht den visualisierten Inhalt der elektronischen Datei selbst zur Kenntnis nimmt. Um einen Sachverständigenbeweis handelt es sich, wenn die Visualisierung oder auch die Prüfung der zur Sicherung der Authentizität und Integrität eingesetzten Verfahren besondere Kenntnisse und Fertigkeiten voraussetzen.
- Für eine Gleichstellung der elektronischen Dokumente mit den Schriftdokumenten (Urkunden) gibt es unter beweisrechtlichen Gesichtspunkten keinen Bedarf. Abgesehen davon, daß gesetzliche Beweisregeln ein anachronistisches Restbollwerk gegen den Siegeszug der freien Beweiswürdigung sind, hat die Rekonstruktion der Beweisregeln für private Dokumente ergeben, daß die in aller Regel entscheidenden Fragen nach der Echtheit, Unverfälschtheit und Vertrauenswürdigkeit eines Dokuments schon jetzt der freien Beweiswürdigung unterliegen und von keiner Beweisregel erfaßt werden. Zur Inhaltsübersicht

Rechtsvergleichende Hinweise

Rechtsvergleichende Betrachtungen stehen vor der Schwierigkeit, daß in den unterschiedlichen Rechtsordnungen ganz verschiedene Fragen zur Diskussion stehen, wenn es um elektronische Dokumentationen und den elektronischen Rechtsverkehr geht(29). Will man versuchen, die Fragen zu systematisieren, so könnte das in folgender Weise geschehen. Zunächst sind zwei Bereiche zu unterscheiden. In dem einen geht es um solche Erklärungen, die in der deutschen Diskussion um den Urkundenbeweis als Tatbestandserklärungen bezeichnet werden. In dem anderen Bereich sind die Wissens- oder Zeugniserklärungen angesprochen.

Für den Bereich der Tatbestandserklärungen können wir drei Fragenkomplexe unterscheiden:

- Wird für die Wirksamkeit von Rechtsgeschäften die Einhaltung einer Formvorschrift verlangt? Welche Beweise sind für die Einhaltung der Formvorschrift zugelassen?
- Wird für die Durchsetzung von rechtsgeschäftlichen Verpflichtungen die Einhaltung einer Formvorschrift verlangt?
  Welche Beweise sind für die Einhaltung der Formvorschrift zugelassen?
- Wird für den Nachweis einer vertraglichen Verpflichtung ein bestimmtes Beweismittel

vorgeschrieben?
Welche Ausnahmen gibt es für den Beweis mit dem bestimmten Beweismittel?

Für den Bereich der Wissens- oder Zeugniserklärungen bleibt ein Fragenkomplex:

- Gibt es Beweismittelbeschränkungen oder Beweisregeln für den Nachweis mit Hilfe elektronischer Dokumente?

Im Rahmen meines Beitrags zur Jahrestagung der Wissenschaftlichen Vereinigung für Internationales Verfahrensrecht(30) habe ich unter diesem Fragenraster die Beweisrechte der Schweiz, Österreichs, Frankreichs, Belgiens, Griechenlands, Englands und der Vereinigten Staaten von Amerika untersucht. Hier will ich mich auf die Wiedergabe der Ergebnisse mit einigen erläuternden Hinweisen beschränken und darf den an Einzelheiten interessierten Leser auf die Veröffentlichung des Tagungsbandes verweisen.

Das Recht der Bundesrepublik Deutschland enthält mit Blick auf das Beweisrecht für elektronische Dokumente die liberalste aller nur erdenklichen Regelungen. Selbst wo materiellrechtlich die Wirksamkeit eines Rechtsgeschäfts von der Einhaltung der Schriftform abhängt, kann die Einhaltung der Schriftform mit allen nur erdenklichen Beweismitteln bewiesen werden. Über die Tauglichkeit der Mittel wird im Rahmen der freien Beweiswürdigung und nicht bei der Zulassung als Beweismittel befunden. Vergleichbar liberale Gestaltungen finden wir in der Schweiz und in Österreich. Andere Rechte sind dagegen durch mehr oder weniger große Beschränkungen bei der Zulassung der Beweismittel gekennzeichnet.

Zum ersten Bereich der Tatbestandserklärungen verlangt das common law unter dem Aspekt der best evidence rule(31) den Nachweis mit dem Original. Das gilt sowohl dort, wo die materiellrechtliche Wirksamkeit eines Rechtsgeschäfts von der Einhaltung der Form abhängt, als auch dort, wo durch das statute of frauds(32) für die gerichtliche Durchsetzung von rechtsgeschäftlichen Verpflichtungen die Einhaltung einer Formvorschrift verlangt wird(33). Das französische Recht und ihm nachgebildete Rechte schreiben ab einem bestimmten Streitwert den Beweis vertraglicher Verpflichtungen mit schriftlichen Urkunden vor(34). In dem einem wie dem anderen Komplex stellt sich die Frage, welche Ausnahmen von den jeweiligen Geboten gemacht werden und wie sich in diesem Rahmen elektronische Dokumente ausmachen.

Zum zweiten Bereich der Wissens- und Zeugniserklärungen wird nur im angloamerikanischen Rechtskreis die Zulassungsfrage für elektronische Dokumente unter dem Gesichtspunkt des hearsay Verbots und der best evidence rule aufgeworfen. Für das US-amerikanische Bundesrecht etwa finden sich die einschlägigen Regeln in den Federal Rules of Evidence(35). Sie sind durch das Bemühen gekennzeichnet, die durch das hearsay Verbot und die best evidence rule errichteten Zulassungsschranken nach Möglichkeit zu überwinden.

Festzuhalten bleibt, daß es sich bei den Erfordernissen des schriftlichen Beweises und bei den Zulassungsbeschränkungen um hausgemachte Probleme handelt. Wenn zur Überwindung der hausgemachten Probleme elektronische Dokumente den schriftlichen Dokmenten gleichgestellt werden, so trägt das nichts für das Beweisrecht eines Landes aus, dem die Zulassungsbeschränkungen fremd sind. Im Gegenteil: Die rechtsvergleichenden Untersuchungen belegen, daß für die beweisrechtliche Behandlung elektronischer Dokumente das von Zulassungsbeschränkungen und Beweisregeln freie Recht der Bundesrepublik Deutschland Vorbildcharakter hat. Zur Inhaltsübersicht

Fußnoten

(1) Seidel, Signaturverfahren und elektronische Dokumente. Rechtliche Bewertung und Regelungsvorschläge, in: Bestandsaufnahme über die elektronischen Signaturverfahren (Veröffentlichung der Gesellschaft für Mathematik und Datenverarbeitung - GMD), St. Augustin 1992, S. 80 ff.; ders., Zertifizierung rechtsverbindlicher und urkundensicherer Dokumentverarbeitung, in: Bundesnotarkammer (Hrsg.), Elektronischer Rechtsverkehr, Digitale Signaturverfahren und Rahmenbedingungen, Köln 1995, S. 89, 94; ders., Dokumentenschutz im elektronischen Rechtsverkehr, CR 1993, Teil I S. 409 ff., Teil II S. 484 ff.; Geis, Zivilprozeßrechtliche Aspekte des elektronischen Dokumentenmanagements, CR 1993, 653, 656; Bergmann/Streitz, Beweisführung durch EDV-gestützte Dokumentation, CR 1994, 77, 79. Zurück zum Text

(2) So regt etwa die Arbeitsgemeinschaft für Wirtschaftliche Verwaltung e.V. (AWV) in ihrer Projektgruppe "Prozeßrechtliche Aspekte des Dokumenten-Managements auf der Basis elektronischer Speichersysteme" einen § 416a ZPO mit folgender Fassung an: "Gleich einer privaten Urkunde im Sinne von § 416 ZPO werden auf Datenträgern gespeicherte Dokumente und deren Ausdruck behandelt, wenn es sich um eine Gedankenäußerung handelt, die nach dem Stand der Technik geeignete Verfahren der Datenauthentizität und die Identität des Ausstellers erkennen läßt und durch geeignete Techniken und organisatorische Maßnahmen vor Verfälschung gesichert ist" (AWV-Schrift 06 531, Eschborn 1993, S. 17 f.). Zurück zum Text

(3) Für den Augenscheinsbeweis Baumbach/Lauterbach/Albers/Hartmann, 52. Aufl., München 1994, Übers § 415 Rdnr. 3; Thomas/Putzo, 17. Aufl., München 1991, Vorbem § 371 Anm. 3; Geimer in: Zöller, 18. Aufl., Köln 1993, Vor § 415 Rn 3; AK-ZPO/Rüßmann, Neuwied und Darmstadt 1987, vor § 415, RN 2; MünchKommZPO-Schreiber, Band 2, München 1992, § 415 Rdnr. 6; Schumann in: Stein-Jonas, 20. Aufl., Zweiter Band, Teilband 2, Tübingen 1989, vor § 371 Rdnr. 4; Rosenberg/Schwab/Gottwald, 15. Aufl., München 1993, § 121 (S. 697); vgl. auch Redeker, Geschäftsabwicklung mit externen Rechnern im Bildschirmtext, NJW 1984, 2390, 2394. Zurück zum Text

(4) So Seidel in einem Diskussionsbeitrag in: Bundesnotarkammer (a.a.O. Fußnote 1), S. 170: "Es geht hier wirklich um die Beweissicherheit und die Rechtsverbindlichkeit der elektronischen Kommunikation. Es befinden sich bereits Milliarden-Investitionen in der Pipeline, die gestaut werden, weil die Rechtslage so unsicher ist. Das muß man sich überlegen, und unter dem Aspekt 'Wirtschaftsstandort Deutschland' meine ich, daß wir diese rechtlichen Regelungen wirklich brauchen." Zurück zum Text

(5) Kilian, Zweck und Inhalt des deutschen EDI-Rahmenvertrages, CR 1994, 657, 660. Zurück zum Text

(6) AWV-Schrift 06 531 (a.a.O. Fußnote 2), S. 15 ff. Nahezu wortgleich mit der AWV-Schrift Geis (a.a.O. Fußnote 1). Zurück zum Text

(7) Geradezu ärgerlich sind Eigenheiten der Begriffsbildung, wenn ohne Not der "Formalbeweis" des Urkundenbeweisrechts (§ 416 ZPO) dem "Freibeweis" des § 286 ZPO gegenübergestellt wird, statt sich der eingeführten Begriffsbildung "Beweisregel" auf der einen Seite und "Freie Beweiswürdigung" auf der anderen Seite zu bedienen. So durch Seidel, GMD-Dokumentation (a.a.O. Fußnote 1), S. 18 f. und ders. (a.a.O. Fußnote 1), CR 1993, 411. Der Begriffsverwirrung sitzt auch Kilian (a.a.O. Fußnote 5) auf. Zurück zum Text

(8) Es handelt sich um die gekürzte Fassung eines Vortrags, den ich unter dem Titel "Moderne Elektroniktechnologie und Informationsbeschaffung im Zivilprozeß" auf der Jahrestagung der Internationalen Vereinigung für Internationales Verfahrensrecht e.V. im April 1995 in Rostock gehalten habe. Die ungekürzte Fassung des Vortrags wird in der vom Gieseking Verlag verlegten Schriftenreihe der Vereinigung (herausgegeben von Schlosser) zusammen mit den anderen

Vorträgen der Rostocker Tagung erscheinen. In ihr wird es vor allem auch um die Informationspflichten im Zusammenhang mit elektronischen Dokumenten gehen. Zurück zum Text

(9) Häufig als Tatbestandsurkunde bezeichnet. Zurück zum Text

(10) Die Wissenserklärung - häufig der Tatbestandsurkunde als Zeugnisurkunde gegenübergestellt - steht hier als Name für alle die Erklärungen, die nicht Willenserklärungen sind. Es geht dabei nicht allein um Beschreibungen dessen, was ist (Wissenserklärungen im engeren Sinne), sondern auch um schriftlich fixierte Wünsche, Drohungen, Beleidigungen, Liebeserklärungen oder Bewertungen. Zurück zum Text

(11) Von Seidel, GMD-Dokumentation (a.a.O. Fußnote 1), S. 19 verkannt. Zwar enthalten auch die §§ 439, 440 ZPO Regeln. Es handelt sich aber nicht um Beweisregeln, die die freie Beweiswürdigung ausschlössen. Zurück zum Text

(12) AK-ZPO/Rüßmann (a.a.O. Fußnote 3), § 416 Rdnr. 1. Zurück zum Text

(13) So AK-ZPO/Rüßmann (a.a.O. Fußnote 3), § 416 Rdnr. 1. Zurück zum Text

(14) So ausdrücklich Schreiber in MünchKommZPO (a.a.O. Fußnote 3), § 416 Rdnr. 10. Wohl auch Baumbach/LauterbachAlbers/Hartmann (a.a.O. Fußnote 3), § 416 Rdnr. 5; Thomas/Putzo (a.a.O. Fußnote 3), § 416 Anm. 2 b); Rosenberg/Schwab/Gottwald (a.a.O. Fußnote 3), § 121 (S. 701) jeweils mit der Annahme, von der Beweisregel sei auch umfaßt, daß die Urkunde abgesendet worden sei. Zurück zum Text

(15) Diese Deutung wird von meinem Mitarbeiter Jörg W. Britz vorgeschlagen, der die Fragen im Rahmen eines Dissertationsvorhabens untersucht. Zurück zum Text

(16) So z.B. Larenz, Allgemeiner Teil des deutschen Bürgerlichen Rechts, 7. Aufl., München 1989, § 21 (S. 419); BGHZ 65, 13, 15. Zurück zum Text

(17) So z.B. Flume, Allgemeiner Teil des Bürgerlichen Rechts, 3. Aufl., Berlin u.a. 1979, § 20 a.E. (S. 414 f.). Zurück zum Text

(18) A.a.O. Fußnote 14. Zurück zum Text

(19) So für die Tatbestandsurkunden auch ausdrücklich MünchKommZPO-Schreiber (a.a.O. Fußnote 3), § 416 Rdnr. 7. Zurück zum Text

(20) Siehe oben Fußnote 4. Zurück zum Text

(21) Vgl. dazu die umfassende und vorbildliche Ausarbeitung von Matthias Kuhn, Rechtshandlungen mittels EDV und Telekommunikation, Zurechenbarkeit und Haftung, München 1991. Zurück zum Text

(22)Vgl. zu Protokolldateien allgemein Runge, Protokolldateien zwischen Sicherheit und Rechtsmäßigkeit, CR 1994, 710. Zurück zum Text

(23) Mit den Teilstudien Seidel, Signaturverfahren und elektronische Dokumente. Rechtliche Bewertung und Regelungsvorschläge (siehe schon oben Fußnote 1); Herda, Technische und organisatorische Aspekte der digitalen Unterschrift; Struif, Die Smartcard. Signaturanwendungsfelder aus funktioneller Sicht und Signatur-Dienstleistungsinstanzen - alle dokumentiert in einer GMD-eigenen Veröffentlichung, St. Augustin 1992. Zurück zum Text

(24) In Buchform dokumentiert, a.a.O. Fußnote 1. Zurück zum Text

(25) Teilweise dokumentiert in Bergmann/Streitz (a.a.O. Fußnote 1) CR 1994, 77 ff. Zurück zum Text

(26) Hochglanzprospekt S. 4 bis 6. Die Fußnoten stammen nicht von der Telekom, sondern enthalten Erläuterungen und Anmerkungen von mir. Als Anschauungshilfe mag die Abbildung auf S. 11 dienen. Zurück zum Text

(27) Es handelt sich um eines der sogenannten "offenen Systeme" zur Verschlüsselung von Daten, welche sich dadurch auszeichnen, daß sie mit gemeinhin bekannten Verschlüsselungsmodi arbeiten. Die Sicherheit der Verschlüsselung beruht auf dem Umstand, daß die Ermittlung des "Schlüssels" - benutzt werden Primzahlen extremer Größe - auch unter Verwendung modernster Computertechnologie nur in einem Zeitraum erfolgen könnte, der schon den Versuch sinnlos erscheinen läßt. Eingeführt wurde der RSA-Algorithmus von R.L. Rivest, A. Shamir und L. Aleman in ihrem Aufsatz: A method for obtaining digital signatures and public-key cryptosystems, Comm. ACM, vol. 21 (1978), S. 120-126. Zurück zum Text

(28) Hier bedarf die Aussage der Telekom wohlwollender Interpretation. Natürlich ist es technisch ausgeschlossen, ein Dokument beliebiger Größe auf einen Umfang von 512 bit zu komprimieren. Gemeint ist vielmehr die Erstellung eines Datenextraktes aus dem zu verschickenden Dokument. Die im Wege des Hash-Algorithmus extrahierten Daten identifizieren das Dokument derart, daß jede Veränderung im Dokument sich auch in einer Veränderung des Hash-Extrakts niederschlägt. Das Hash-Extrakt dient nun als Grundlage des Signiervorgangs. Dem Empfänger wird sowohl das Dokument als auch die in diesem Wege erstellte elektronische Unterschrift zugeleitet. Zurück zum Text

(29) Darauf nimmt die AWV-Schrift (a.a.O. Fußnote 2) zu wenig Bedacht. Zurück zum Text

(30) Siehe oben Fußnote 8. Zurück zum Text

(31) Als eine Fassung der best evidence rule sei hier Section 1500 California Evidence Code (Beweisrecht für Silicon Valley) angeführt:

Except as otherwise provided by statute, no evidence other than the original of a writing is admissible to prove the content of a writing. This section shall be known and may be cited as the best evidence rule. Zurück zum Text

(32) Beispielhaft sei hier die Regelung im amerikanischen Uniform Commercial Code angeführt:

Section 2-201. Formal Requirements; Statute of Frauds.(1) Except as otherwise provided in this section a contract for the sale of goods for the price of $500 or more is not enforceable by way of action or defense unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorized agent or broker. A writing is not insufficient because it omits or incorrectly states a term agreed upon but the contract is not enforceable under this paragraph beyond the quantity of goods shown in such writing.

(2) Between merchants if within a reasonable time a writing in confirmation of the contract and sufficient against the sender is received and the party receiving it has reason to know its contents, it satisfies the requirements of subsection (1) against such party unless written notice of objection to its contents is given within 10 days after it is received.

(3) A contract which does not satisfy the requirements of subsection (1) but which is valid in other

respects is enforceable

(a) if the goods are to be specially manufactured for the buyer and are not suitable for sale to others in the ordinary course of the seller's business and the seller, before notice of repudiation is received and under circumstances which reasonably indicate that the goods are for the buyer, has made either a substantial beginning of their manufacture or commitments for their procurement; or

(b) if the party against whom enforcement is sought admits in his pleading, testimony or otherwise in court that a contract for sale was made, but the contract is not enforceable under this provision beyond the quantity of goods admitted; or

(c) with respect to goods for which payment has been made and accepted or which have been received and accepted (Sec. 2-606). Zurück zum Text

(33) An dieser Stelle noch ein Wort zum Internet als Fundgrube für Rechtsvergleicher. Der Uniform Commercial Code wird mit Annotations elektronisch vorgehalten vom Legal Information Institute der Cornell University Law School. Er ist via Datenautobahn erreichbar und abrufbar, wenn man einen Zugang zum Internet hat. Die Universität des Saarlandes stellt diesen Zugang allen ihren Mitgliedern kostenlos zur Verfügung. Das Zauberwort heißt World Wide Web. In ihm sind weltweit unzählige Informationen über sog. Hypertextlinks verbunden. Ein guter Ausgangspunkt für Rechtsinformationen im Internet ist der Rechtsweb-Server der Universität des Saarlandes (betreut vom Lehrstuhl für Rechtsinformatik, Prof. Dr. Maximilian Herberger). Wer über einen Zugang zum Internet verfügt und ein Programm zum Navigieren im World Wide Web hat, erreicht den Rechtsweb-Server der Universität des Saarlandes mit "http://www.jura.uni-sb.de/". Von hier aus kann er sich zum Legal Information Institute der Cornell University Law School weiterreichen lassen. Direkt dorthin kommt man mit "http://www.law.cornell.edu/". Dem Leser dieser Zeilen dürfte das Internet vertraut sein. So er will, kann er die Verbindungen gleich von dieser Stelle aus ausprobieren. Hier geht es nach Saarbrücken und hier nach New York! Zurück zum Text

(34) Es geht um Art. 1341 Code civil. Nach dieser Vorschrift ist außer in Handelssachen ab einem summenmäßig bestimmten Streitwert (derzeit FF 5.000) ein Beweis durch Schriftstücke erforderlich. Art. 1341 Abs. 1 und 2 Code civil lauten wörtlich:Il doit être passé acte devant notaires ou sous signatures privées de toutes choses excédant une somme ou une valeur fixée par décret, même pour dépôts volontaires et il n'est re(u aucune preuve par témoins contre et outre le contenu aux actes, ni sur ce qui serait allégué avoir été dit avant, lors et depuis les actes, encore qu'il s'agisse d'une somme ou valeur moindre.

Le tout sans préjudice de ce qui est préscrit dans les lois relatives au commerce. Zurück zum Text

(35) Die Federal Rules werden kraft des Rules Enabling Act (28 USC § 2072) vom Supreme Court erlassen. Die Federal Rules of Evidence stammen aus dem Jahre 1975 und sind zuletzt 1993 geändert worden. Sie können ebenfalls elektronisch abgerufen werden beim Legal Information Institute der Cornell University Law School. Den direkten Zugriff hat man mit "http://www.law.cornell.edu/rules/frcp/overview.htm". Zurück zum Text

Mikrofilm und elektronische Dokumentation
- ein rechtlicher Vergleich -

Von Rechtsanwalt Dr. Ivo Geis

MIKRO BYTE HORST SINDT GMBH
DIE WELT DER TECHNIK UND DOKUMENTENSICHERHEIT
Horst Sindt
Geschäftsführer
Innungsstraße 9
21244 Buchholz i.d.N.
Telefon: (04181) 29 96 - 0
Fax: (04181) 29 96 29
info@mikrobyte.de
www.mikrobyte.de
... macht Sindt!

1.0 Übersicht

In einem rechtlichen Innovationsschub sind Europäische Richtlinien und deutsche Gesetze zur elektronischen Kommunikation und zur elektronischen Archivierung ergangen. Welches rechtliche Schicksal hat den Mikrofilm durch die Aktualisierung der „Grundsätze Ordnungsmäßiger Archivierung" (2.0) und die Gesetzgebung zur Rechtswirkung elektronischer Signaturen (3.0) getroffen? Wie weit reichen nach dem Stand der Gesetzgebung die rechtlichen Möglichkeiten für das Outsourcing von Archivdienstleistungen (4.0)? Nachdem die Gesetzgebung zum elektronischen Geschäftsverkehr 1997 mit dem „Informations- und Kommunikationsdienstegesetz" begonnen hat und diese Gesetzgebung zahlreiche Korrekturen erfahren hat, ist es Zeit eine Bilanz für den Mikrofilm zu ziehen.

2.0 Nachschau GOBS und GDPDU

Die traditionellen Grundsätze ordnungsmäßiger Archivierung mikroverfilmter Dokumente und elektronischer Dokumente (GoBS) sind um die Grundsätze zur ordnungsmäßigen Archivierung originärer elektronischer Dokumente ergänzt worden. Mit diesen „Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen" (GDPDU) werden Anforderungen an die maschinelle Auswertung von Archiven gestellt, für die das Mikrofilmarchiv nicht ausreichen soll.

2.1 Die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)

Handelsrecht und Steuerrecht verlangen mit § 257 Abs. 3 HGB (Handelsgesetzbuch) und § 147 Abs. 2 AO (Abgabenordnung) die Aufbewahrung nach den Grundsätzen ordnungsmäßiger Buchführung. Diese allgemeinen Grundsätze hat das Bundesfinanzminiserium durch die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme" (GoBS) konkretisiert.[1] Diese Grundsätze sind nach Ziffer 1.1 GoBS ein allgemein gültiges Ordnungsprinzip der handelsrechtlichen und steuerrechtlichen Aufbewahrungsvorschriften, das auch für die Mikroverfilmung als integrierte Fortsetzung des

[1] Schreiben des Bundesfinanzministeriums vom 7.11.1995 in BStBl. I 1995, S. 738 – 747.

EDV-Verfahrens gilt. Durch die GoBS wird die Integrität der Dokumente für die Phasen der Übertragung auf das Speichermedium (2.1.1), die Aufbewahrung (2.1.2) und die Wiedergabe (2.1.3) sichergestellt. Die Mikroverfilmung nach den Grundsätzen der Ordnungsmäßigkeit eröffnet die Möglichkeit, die mikroverfilmten Papieroriginale zu vernichten (2.1.4) und sichert die Beweisqualität des Mikrofilms (2.1.5).

2.1.1 Ordnungsmäßige Übertragung auf das Speichermedium

Nach § 257 Abs. 3 Nr. 1 HGB und § 147 Abs. 2 Nr. 1 AO müssen empfangene Handelsbriefe und Buchungsbelege bildlich und andere Unterlagen inhaltlich übereinstimmend mit dem Original aufbewahrt werden. Dieser Anforderung entspricht das COM-Verfahren. Nach Auswahl der zu archivierenden Dokumente, deren Konvertierung in TIF- oder PDF-Dateien mit Übernahme von Index- und Metadaten wird der Film hergestellt, indem der virtuelle Film erstellt, nach Kontrolle des Inhalts zur Belichtung freigeben und nach der Entwicklung archiviert wird. Durch dieses Verfahren wird sichergestellt, dass ein Dokument einschließlich Index- und Metadaten bildlich übereinstimmend mit dem Original in das COM-System übernommen wird und damit ordnungsmäßig auf das Speichersystem des Mikrofilms übertragen ist

2.1.2 Ordnungsmäßige Aufbewahrung

Zulässig und damit ordnungsmäßig ist die Aufbewahrung als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern, § 147 Abs. 2 AO, § 257 Abs. 3 HGB. Die damit auf Mikrofilm zulässige Archivierung muss nach § 147 Abs. 2 Nr. 2 AO, § 257 Abs. 3 Nr. 2 HGB sicherstellen, dass die Dokumente während der Aufbewahrungsfrist jederzeit verfügbar sind. Die jederzeitige Verfügbarkeit setzt voraus, dass die Dokumente vorhanden, also ordnungsmäßig aufbewahrt werden. Ordnungsmäßige Aufbewahrung erfordert nach Ziffer 5.5 GoBS die Datensicherheit der Dokumente entsprechend den im Einzelfall bestehenden Bedingungen. Das COM-Verfahren ist alterungsresistent, manipulationssicher und desastertolerant. Alterungsresistenz besteht durch die langfristige Haltbarkeit des Filmmaterials von bis zu 500 bis 1.000 Jahren. Manipulationssicherheit ist auf zwei Ebenen gegeben: die Manipulation von Filmen ist erkennbar und das Entfernen von Dokumenten ist durch das Indexverzeichnis am Anfang und am Ende eines Films ausgeschlossen. Desastertoleranz besteht durch die Unempfindlichkeit des Trägermaterials Mikrofilm.

2.1.3 Ordnungsmäßige Wiedergabe

Archivierte Dokumente müssen nach § 147 Abs. 2 Nr. 2 AO unverzüglich lesbar gemacht werden können. Hierzu müssen Dokumente nach Ziffer VIII des Begleitschreibens zu den GoBS mit einem unveränderten Index versehen sein, unter dem sie zu bearbeiten und zu verwalten sind.[2] Das COM-Verfahren entwickelt durch die Übernahme von Index- und Metadaten ein Indexierungssystem, das die ordnungsmäßige Wiedergabe ermöglicht. Durch die Indexierung können die gespeicherten Dokumente wieder aufgefunden und innerhalb angemessener Frist lesbar gemacht werden. Das COM-Verfahren entspricht damit der Anforderung der GoBS an die ordnungsmäßige Wiedergabe.

2.1.4 Die Vernichtung des Papieroriginals

Auf Grund der Ordnungsmäßigkeit des COM-Verfahrens werden die in diesem Verfahren mikroverfilmten Dokumente im Rahmen der handelsrechtlichen und steuerrechtlichen Prüfung der Jahresabschlüsse anerkannt. Damit können die Originalunterlagen grundsätzlich vernichtet werden. Auf diese Möglichkeit, das Original nach ordnungsmäßiger Archivierung zu vernichten, weist das Schreiben des Bundesfinanzministeriums vom 7.11.1995 unter VIII. c) hin und macht auf andere Rechtsvorschriften aufmerksam, nach denen eine Aufbewahrung des Originals notwendig bleibt.[3] Das Original hat eine rechtliche Bedeutung als gesetzliche Schriftform für die Kündigung des Arbeitsvertrages gemäß § 623 BGB, das arbeitsrechtliche Zeugnis gemäß § 630 BGB, die Bürgschaftserklärung gemäß § 766 BGB, das Schuldversprechen gemäß § 780 BGB und das Schuldanerkenntnis gemäß § 781 Satz 1 BGB. Das bedeutet, dass diese Dokumente auch nach ordnungsmäßiger Archivierung als Original aufbewahrt werden müssen.

2.1.5 Beweisqualität

Entsteht ein Rechtsstreit über den Inhalt eines mikroverfilmten Dokuments, kommt es auf die Beweisqualität an. Da für das Lesen des Mikrofilms technische Hilfsmittel als erforderlich angesehen werden, gelten mikroverfilmte Dokumente nicht als Urkunde, sondern als Objekt des Augenscheins, das der freien Beweiswürdigung des Gerichts unterliegt.[4] Im Rahmen der freien Beweiswürdigung sprechen die Grundsätze der Ordnungsmäßigkeit für die Beweisqualität der archivierten Dokumente. Mit der Aufbewahrung entsprechend diesen

---

[2] BStBl. I 1995, S. 740.
[3] BStBl. I 1995, S. 740.
[4] *Leipold* in Stein/Jonas, Kommentar zur Zivilprozessordnung; 21. Aufl., Tübingen 1999, Vor, § 415, Randnummer 1; ebenfalls *Schreiber* in Münchener Kommentar zur Zivilprozessordnung, 2. Aufl. München 2000, § 415, Randnummer 6

Grundsätzen soll die Dokumentation gegen Änderungen geschützt werden.[5] Deshalb gilt die entsprechende Aufbewahrung als Indiz für die Beweissicherheit.[6]

2.2 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)

Das Bundesfinanzministerium hat mit seinem Schreiben vom 16. Juli 2001 „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)"[7] die Prüfungsmethoden dem elektronischen Geschäftsverkehr angepasst, der durch elektronische Erklärungen abgewickelt wird. Grundlage ist die Neufassung des § 147 Abs. 6 Abgabenordnung (AO), wonach die Finanzbehörde im Rahmen einer Außenprüfung das Recht hat, Einsicht in die gespeicherten Daten zu nehmen und das Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen und maschinelle auszuwerten. Sie kann nach § 147 Abs. 6 AO im Rahmen einer Außenprüfung auch verlangen, dass die Daten nach ihren Vorgaben maschinell ausgewertet oder ihr die gespeicherten Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung gestellt werden. Das Bundesfinanzministerium interpretiert dieses Recht in Abschnitt I.1. Abs. 5 GDPdU als unmittelbaren Datenzugriff, als mittelbaren Datenzugriff und als Datenträgerüberlassung.

2.2.1 Datenzugriff der Finanzbehörde

Der Datenzugriff umfasst das Lesen, das Filtern und Sortieren der Daten gegebenenfalls unter Nutzung der im Datenverarbeitungssystem vorhandenen Auswertungsmöglichkeiten, Abschnitt I.1.a) Abs. 2 GDPdU. Das Recht des Datenzugriffs durch die Finanzbehörde ist nach Abschnitt I.1. Abs. 1 bis Abs. 4 GDPdU auf die steuerlich relevanten Daten beschränkt: die Daten der Finanzbuchhaltung, der Anlagenbuchhaltung und der Lohnbuchhaltung. Der Zugriff auf steuerlich relevante Daten in anderen Bereichen der Datenverarbeitungssysteme muss in geeigneter Weise möglich sein und bei unzutreffender Qualifizierung nachträglich ermöglicht werden.

2.2.2 Maschinelle Auswertbarkeit originär elektronischer Dokumente

Nach § 147 Abs. 2 Nr. 2 AO muss sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell

---

[5] Glanegger u.a./*Kirnberger*, HGB-Komm, Heidelberg 2002, 6. Aufl., § 257 Rdnr. 3; Münch Komm HGB/ *Ballwieser*, § 257 Rdnr. 16; Heymann/*Walz*, HGB-Komm, Berlin 1999, 2. Aufl., § 257 Rdnr. 6.
[6] Ebenroth/Bonjou/Joost/*Wiedemann*, HGB-Komm, München 2001, § 257 Rdnr. 1.
[7] BStBl. 2001 I, S. 415 ff.

ausgewertet werden können. Damit sind originär digitale Unterlagen auf maschinell verwertbaren Datenträgern während der gesamten Aufbewahrungsfrist zu archivieren. Nach Abschnitt III.1 Satz 2 GDPdU sind originär digitale Unterlagen die in das Datenverarbeitungssystem in elektronischer Form eingehenden Daten und die im Datenverarbeitungssystem erzeugten Daten. Im elektronischen Geschäftsverkehr sind dies e-Mails einschließlich Anhang. Maschinell verwertbare Datenträger sind maschinell lesbare und auswertbare Datenträger. Wenn originär digitale Unterlagen auf maschinell verwertbaren Datenträgern zu archivieren sind, dann dürfen sie nicht, so die Schlußfolgerung des Bundesfinanzministeriums, ausschließlich in ausgedruckter Form oder auf Mikrofilm aufbewahrt werden und ist die Aufzeichnung im COM-Verfahren nicht ausreichend, Abschnitt III.1. Satz 3 GDPdU.

3.0 Elektronische Signaturen

Im EU-Binnenmarkt soll nach der EG-Signaturrichtlinie die Unterschrift durch elektronische Signaturen ersetzt werden können. Entsprechend den Vorgaben der EG-Signaturrichtlinie sind durch die deutsche Gesetzgebung zur elektronischen Signatur (3.1) drei Signaturklassen entstanden (3.2). Diese Signaturen ersetzen Schriftformerfordernisse, die vertraglich vereinbart und gesetzlich bestimmt sind (3.3). Im Rechtsstreit bestimmt die Qualität der elektronischen Signaturen die Beweisqualität der elektronisch signierten Dokumente (3.4).

3.1 Die Gesetzgebung zur elektronischen Signatur

Die Gesetzgebung benötigte zur Regelung elektronischer Signaturen zwei Phasen. Am 1. August 1997 ist das Gesetz zur digitalen Signatur in Kraft getreten, das im Rahmen des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) verabschiedet worden ist.[8] Am 13. Dezember 1999 wurde die Richtlinie 1999/93/EG des europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (EGSRL) verabschiedet.[9] Ziel der Signaturrichtlinie ist es, eine EU-einheitliche Infrastruktur für elektronische Signaturen sicherzustellen, die nach Art. 5 EGSRL der Unterschrift gleichgestellt werden. Auf Grund dieser Richtlinie ist das neue deutsche Signaturgesetz

[8] Signaturgesetz – SigG, BGBl. S. 1870 ff.; aus der umfangreichen Literatur wird auf die Kommentare zu dem Signaturgesetz 1997 verwiesen: *Engel-Flechsig, Maennel/Tettenborn,* Beck'scher IuKDG-Kommentar, München, 2001 und *Roßnagel* (Hrsg.) Recht der Multimedia-Dienste, Fünfter Teil - Gesetz zur digitalen Signatur, München 2001;

[9] Abl. EG L Nr. 13 v. 19. Januar 2000, S. 12 ff.; hierzu *Geis,* MMR 2000, 667; *Redeker,* CR 2000, 455; *Roßnagel,* K&R 2000, 313.

(SigG) entstanden, das am 22. Mai 2001 in Kraft getreten ist.[10] Das Signaturgesetz wird ergänzt durch die Signaturverordnung (SigV), die von der Bundesregierung am 24. Oktober 2001 beschlossen worden ist.[11] Die dritte Phase der Signaturgesetzgebung ist zu erwarten: Am 1. April 2004 ist der „Entwurf eines Ersten Gesetzes zur Änderung des Signaturgesetzes" (1. SigÄndG) veröffentlicht worden.[12] Die wesentliche Änderung besteht in der Vereinfachung des Vergabeverfahrens.

3.2 Die drei Signaturklassen

Charakteristisch für die EG-Signaturrichtlinie und das Signaturgesetz sind die drei Signatur-Klassen der elektronischen Signatur, der fortgeschrittenen elektronischen Signatur und der qualifizierten elektronischen Signatur

3.2.1 Die elektronische Signatur

Die Anforderungen an die elektronische Signatur sind gering: Elektronische Signaturen sind nach § 2 Nr. 1 SigG alle Daten, die anderen elektronischen Daten beigefügt werden und zur Authentifizierung dienen. Dies sind biometrische Verfahren, die Namenswiedergabe und die eingescannte Unterschrift.[13] In diesen Fällen besteht lediglich eine geringwertige Authentizitätsfunktion, nicht aber eine Integritätsfunktion.

3.2.2 Die fortgeschrittene elektronische Signatur

An die fortgeschrittene elektronische Signatur wird nach § 2 Nr. 2 SigG die Anforderung gestellt, dass sie

- ausschließlich dem Signaturschlüssel-Inhaber zugeordnet ist,
- damit seine Identifizierung ermöglicht,
- mit Mitteln erstellt wird, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann,
- mit den Daten, auf die sie sich bezieht, verknüpft ist, damit eine nachträgliche Veränderung der Daten erkannt werden kann.

Die fortgeschrittene elektronische Signatur muss von Zertifizierungsdiensten als vertrauenswürdigen Dritten dem Signaturschlüssel-Inhaber zugeordnet werden. Dies ist der Fall, wenn unternehmensinterne oder unternehmensexterne Zertifizierungsdienste

---

[10] Verkündet im Bundesgesetzblatt vom 21. Mai 2001 Teil I, Nr. 22; ; Hierzu: *Bert/Fleisch/Michels,* DuD 2002, 69-74; *Roßnagel,* MMR 2001, 201 f.; *ders.*, MMR 2002, 215-222; *Tettenborn,* CR 2000, 683-691; *Schmidl,* CR 2002, 508-517; zur wirtschaftspolitischen Bedeutung digitaler Signaturen *Sandl,* CR 2000, 319.

[11] Hierzu *Geis,* K&R 2002, 59.

[12] Veröffentlicht in www.iukdg.de unter „Elektronische Signaturen".

Signatursoftware an die Berechtigten vergeben. Hierdurch ist für den Empfänger die Identifizierung des Absenders möglich. Dies bedeutet Authentizität. Durch die Verknüpfung mit den Daten soll eine nachträgliche Veränderung erkannt werden können. Keine erkennbare Veränderung ist damit ein Indiz für die Integrität. Anforderungen an die Sicherheit der organisatorischen Prozesse der Schlüsselverwaltung und der technischen Komponenten bestehen nicht.[14] Die fortgeschrittene elektronische Signatur ist also offen für die technische und organisatorische Ausgestaltung.

3.2.3 Die qualifizierte elektronische Signatur

Die qualifizierte elektronische Signatur ist eine Steigerung der fortgeschrittenen elektronischen Signatur, indem sie durch qualifizierte Zertifizierungsdienste vergeben und verwaltet wird. Mit der qualifizierten elektronischen Signatur wird die höchste Sicherheitsstufe für die Integrität und Authentizität elektronischer Erklärungen erreicht. Die qualifizierte elektronische Signatur ist charakterisiert durch die Sicherheitsanforderungen, die qualifizierten Zertifizierungsdienste, die Art der Vergabe qualifizierter elektronischer Signaturen und das Zertifikatverzeichnis. Sicherheit wird erreicht, indem die elektronische Signatur auf einer Chipkarte vergeben wird, die nur durch ein Passwort oder ein biometrisches Merkmal des Berechtigten aktiviert werden kann und durch hohe Sicherheitsqualität der technischen Komponenten, § 17 Abs. 1 SigG. Qualifizierte Zertifizierungsdienste entsprechen den gesetzlichen Anforderungen an die Zuverlässigkeit und die Fachkunde. Dies wird auf Antrag des Zertifizierungsdienstes von der Regulierungsbehörde geprüft oder ist ihr von dem Zertifizierungsdienst angezeigt worden.[15] Qualifizierte Zertifizierungsdienste vergeben die qualifizierte elektronische Signatur, wenn sie sich von der Identität des Antragstellers auf der Grundlage eines Personalausweises oder Reisepasses überzeugt haben, § 5 SigG.Der Zertifizierungsdienst hat die von ihm ausgestellten Zertifikate in ein öffentliches Zertifikatverzeichnis aufzunehmen, das online abgefragt werden kann, § 5 Abs. 1 S. 2 SigG. Damit kann sich der Empfänger einer elektronischen Nachricht mit qualifizierter elektronischer Signatur von der Authentizität des Absenders vergewissern: Aus dem Zertifikatverzeichnis ergibt sich die zuverlässig festgestellte Identität des Absenders.

---

[13] *Roßnagel,* NJW 2001, 1817, 1819.
[14] *Roßnagel,* NJW 2001, 1817, 1819; *ders.,* MMR 2003, 164 ff.
[15] Über die Zertifizierungsdienste informiert die Website der Regulierungsbehörde, www.regtp.de.