Beweiswert digitaler Dokumente – eine EU-Perspektive

THOMAS HOEREN

Inhaltsverzeichnis

1. Freie richterliche Beweiswürdigung

Nach herrschender Auffassung können elektronische Dokumente **nur im Rahmen freier richterlicher Beweiswürdigung** (§ 286 ZPO) im Zivilprozess Berücksichtigung finden[1]. Dabei mehren sich die Stimmen auch innerhalb der Jurisprudenz, die einer E-Mail im Bestreitensfall keinen Beweiswert zuerkennen. So soll die Angabe einer E-Mail-Adresse selbst bei Absicherung mit einem Passwort kein ausreichendes Indiz dafür sein, dass der E-Mail-Inhaber tatsächlich an einer Internetauktion teilgenommen hat[2]. Anders argumentieren Stimmen in der Literatur, die zumindest für

---

1 Hierzu sehr ausführlich NÖCKER, 176, 180 f.; GEIS, 653 f.; HEUN, 2, 3; anderer Ansicht nur KILIAN, 607, 609.

2 AG Erfurt, Urteil vom 14. September 2001, MMR 2002, 127, mit Anm. WIEBE = CR 2002, 767, mit Anm. WINTER; ähnlich auch OLG Köln, Urteil vom 6. September 2002, MMR 2002, 813 = CR 2003, 55, mit Anm. MANKOWSKI 44 = K&R 2003, 83; mit Anm. ROSSNAGEL = TKMR 2003, 51; OLG Hamburg, Urteil vom 13. Juni 2002,

die Identität des Erklärenden bei E-Mails einen Anscheinsbeweis für möglich ansehen[3]. Auch soll ein solcher bei Vorliegen einer Lesebestätigung gegeben sein[4].

Eine Qualifizierung als Privaturkunde im Sinne von § 416 ZPO scheidet aus, da es an einer dauerhaften Verkörperung sowie an einer hinreichenden Unterschrift fehlt und darüber hinaus die Gedankenäusserung nicht unmittelbar aus sich heraus wahrgenommen werden kann. Der Verkäufer kann daher beim Abschluss eines Vertrages via Internet nicht darauf vertrauen, dass die elektronisch erstellten Unterlagen den vollen Beweis für den Abschluss und den Inhalt des Vertrages erbringen. Der Kunde kann sich problemlos darauf berufen, dass er den Vertrag nie, oder nicht mit diesem Inhalt, abgeschlossen hat. Sendeprotokolle erbringen nämlich nicht den Anscheinsbeweis für den Zugang einer Erklärung; sie haben allenfalls Indizwirkung[5]. Im übrigen sieht die Rechtsprechung Internetauktionen als Versendungskauf an, so dass die Darlegungs- und Beweislast für den Inhalt eines Pakets beim Verkäufer liegt[6].

2. Beweisvereinbarung

Dieses Problem lässt sich auch nicht vertraglich, durch Abschluss einer **Beweisvereinbarung** lösen. Zwar wäre eine Klausel denkbar, wonach der Kunde den Beweiswert der elektronischen Dokumente als Urkundsbeweis akzeptieren muss. Eine solche Klausel hätte jedoch keine Bindungswirkung für die richterliche Beweiswürdigung. Der Richter könnte es weiterhin ablehnen, die Dokumente als Urkunden zu qualifizieren. Auch die Bindung des Kunden an diese Klausel ist zweifelhaft[7].

MMR 2002, 677, mit Anm. FUNK/WENN 820; LG Bonn, Urteil vom 19. Dezember 2003, MMR 2004, 179, mit Anm. MANKOWSKI; LG Bonn, Urteil vom 7. August 2001, MMR 2002, 255, mit Anm. WIEBE = CR 2002, 293, mit Anm. HOEREN; LG Konstanz, Urteil vom 19. April 2002, MMR 2002, 835, mit Anm. WINTER = CR 2002, 609; AG Karlsruhe-Durlach, MMR 2002, 64; AG Bonn, Urteil vom 25. Oktober 2001, CR 2002, 301.

3 So MANKOWSKI, Identität, 2822 ff. und MANKOWSKI, Anscheinsbeweis, 44 ff.; VESHLAGE, 531, 533; KRÜGER/BÜTTER, 181, 186.

4 MANKOWSKI, Identität, 2822 ff.

5 BGH, NJW 1995, 665.

6 LG Berlin, Urteil vom 1. Oktober 2003, MMR 2004, 189.

7 HOEREN, CR 1995, 513, 516.

3. Gesetzesänderungen

Eine Lösung lässt sich nur gesetzgeberisch finden, indem die Gesetze entsprechend geändert werden. Eine solche Regelung findet sich zum Beispiel in Grossbritannien. Nach **dem Civil Evidence Act 1995** ist eine Computerdatei als Beweismittel zugelassen, wenn „it forms part of the records of a business and an officer of the business provides a certificate of its authenticity". Diese Regel ist allerdings m.E. nicht als Ausdruck eines erhöhten Beweiswertes zu verstehen. Sie entspricht vielmehr der Tatsache, dass elektronische Informationen nicht bereits per se von der Beweiswürdigung ausgeschlossen sind, weil sie elektronisch gespeichert sind. Von der Frage der generellen Zulassung elektronischer Beweismittel ist die Frage des konkreten Beweiswertes aber zu trennen.

Eine eindeutige Bestimmung des Beweiswertes elektronischer Dokumente findet sich nur in **Italien**. Nach Art des Gesetzes Nr. 59 vom 15. März 1997 sollen elektronische Dokumente den gleichen Beweiswert wie Papierdokumente haben. Diese enorm liberale Haltung Italiens stösst allerdings auf Skepsis bei anderen europäischen Staaten, die sich fragen, wieso jedes elektronisch generierte Dokument trotz seiner beliebigen Manipulierbarkeit einen solch hohen Beweiswert haben soll.

Ursprünglich war eine Regelung des Beweiswertes im Rahmen des **deutschen Informations- und Kommunikationsdienstegesetzes (IuKDG)** vorgesehen. Frühe Entwürfe des in diesem Gesetzespaket enthaltenen Signaturgesetzes sahen vor, dass ein elektronisches Dokument als Urkunde anerkannt werden könne, wenn die Echtheit einer dabei verwendeten elektronischen Unterschrift mit einem öffentlichen Schlüssel überprüft werden kann, der durch ein zum Zeitpunkt der Unterschrift gültiges Zertifikat einer zugelassenen Zertifizierungsinstanz bestätigt ist. Allerdings verliess den Gesetzgeber dann der Mut. Zwar fanden sich im IuKDG ausführliche Regelungen zur digitalen Signatur im Rahmen des Signaturgesetzes und der dazu gehörigen Signaturverordnung. Doch präjudizierte die Einhaltung der komplizierten Verfahrensbestimmungen für die digitale Signatur nicht mehr deren Beweiswert. Jeglicher Bezug zwischen Signaturregulierung und ZPO wurde nachträglich eliminiert. Dies schloss allerdings nicht aus, dass der digitalen Signatur im Rahmen der freien richterlichen Beweiswürdigung (§ 286 ZPO) ein besonderer Beweiswert zukommt, auch wenn damit die Frage des Beweiswertes digitaler Dokumente weiterhin dem Ermessen und letztendlich damit auch der Willkür einzelner Richter überlassen wird.

4. Signaturrichtlinie und das neue Signaturgesetz

Hier hat allerdings die Europäische Union mit der Ende 1999 in Kraft **verabschiedeten Signaturrichtlinie** Abhilfe geschaffen[8]. In der Richtlinie wird **zwischen „elektronischen Signaturen"** und **„fortgeschrittenen digitalen Signaturen"** unterschieden. Einer (einfachen) elektronischen Signatur darf nach Art. 5 Abs. 2 nicht generell die Rechtsgültigkeit und die Zulässigkeit als Beweismittel abgesprochen werden. Eine „fortgeschrittene digitale Signatur" hat darüber hinaus auch einen erhöhten Beweiswert. Dazu ist erforderlich, dass die Signatur ausschliesslich dem Unterzeichner zugeordnet ist, die Identifizierung des Unterzeichners ermöglicht, mit Mitteln erstellt wird, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann und so mit den Daten, auf die sie sich bezieht, verknüpft ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann. „Fortgeschrittene" elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen[9], sollen das rechtliche Erfordernis einer Unterschrift erfüllen (Art. 5 Abs. 1). Es dürfte damit feststehen, dass zumindest dann, wenn die hohen Sicherheitsanforderungen des deutschen Signaturgesetzes erfüllt sind, der Beweiswert eines dergestalt signierten Dokuments dem einer Privaturkunde gleichkommt. Gleiches dürfte auch für Signaturverfahren anderer Staaten gelten, sofern die dortigen Zertifizierungsstellen die in Anhang II der Richtlinie festgelegten Voraussetzungen erfüllen. Zertifizierungsstellen, die ein qualifiziertes Zertifikat ausstellen, müssen gegenüber jeder Person, die vernünftigerweise auf das Zertifikat vertraut, haften. Sie können den Anwendungsbereich von Zertifikaten und den Wert der Transaktionen, für die ein Zertifikat gültig ist, begrenzen. Die Zertifizierungsstelle ist in diesen Fällen nicht für Schäden verantwortlich, die sich aus einer über den Anwendungsbereich oder die Höchstgrenze hinausgehenden Nutzung eines Zertifikats ergeben.

Die Signaturrichtlinie ist der richtige Weg. Sie lässt aber noch Fragen offen. Insbesondere das Verhältnis der „fortgeschrittenen digitalen Signatur" zu den Sicherheitsanforderungen einzelner nationaler Signaturregelungen ist unklar. Es sollte sehr schnell Planungssicherheit dahingehend hergestellt werden, welche Sicherheitsinfrastruktur welchen Beweiswert für ein digital signiertes Dokument mit sich bringt. Die Planungssicherheit lässt sich aber nur dadurch herstellen, dass einzelne Akteure anfangen, die Signatur einzusetzen. Gefordert ist hier der Staat, mit gutem Vorbild voranzugehen. Auch die grossen Unternehmen sind gefordert, den klassischen Vertrieb um einen virtuellen Distributionsweg mittels digitaler Signaturen zu ergänzen und hierzu dem Versicherungsnehmer eine entsprechende Hardware (Chipkarte und Lesegerät) kostengünstig zur Verfügung zu stellen. Ansonsten droht das spieltheoretische Dilemma, dass niemand aus Angst der erste sein will und die digitale Signatur aus diesem Grund nie zum effektiven Einsatz kommt.

Das Bundeskabinett hat am 15. Februar 2001 den Entwurf eines Gesetzes über die Rahmenbedingungen für elektronische Signaturen und die Umsetzung der Richtlinie verabschiedet. Dieser Entwurf hat am 9. März 2001 auch den Bundesrat passiert. Am 22. Mai 2001 ist das Gesetz dann im Bundesgesetzblatt veröffentlicht worden[10].

Nach dem neuen Signaturgesetz kommen **verschiedene Stufen** der Signaturerzeugung zum Tragen. Da ist zum ersten die **einfache Signatur**. Es handelt sich um eine digitale Unterschrift, deren Erzeugung nicht nach den Vorgaben des Signaturgesetzes erfolgt. Solche Signaturen sind nicht verboten. Sie sind aber nicht der Schriftform gleichgestellt (§ 126 Abs. 3 BGB). Auch kommt ihnen kein erhöhter Beweiswert im Sinne von § 292a ZPO zu. Es fehlt ihnen schliesslich auch die Sicherheitsvermutung nach § 15 Abs. 1 SigG.

Im neuen Signaturgesetz sind lediglich die Anforderungen an eine **„qualifizierte elektronische Signatur"** geregelt. Erst eine solche Signatur erfüllt die Anforderungen des Signaturgesetzes (vgl. § 2 Abs. 3 SigG). Als „qualifiziertes Zertifikat" gilt jede elektronische Bescheinigung, mit denen Signaturprüfschlüssel einer natürlichen Person zugeordnet werden und die die Identität dieser Person bestätigen (§ 2 Ziff. 6 und 7 SigG). Das Zertifikat muss bestimmte Mindestangaben enthalten (§ 7 SigG) und den gesetzlichen Vorgaben des SigG entsprechen. Erlaubt sind – im Unterschied zum alten SigG – auch softwarebasierte Signatursysteme (§ 2 Nr. 10 SigG). Der Betrieb eines Zertifizierungsdienstes für solche Zertifikate

8 Richtlinie 1999/93/EG des europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Abl. L 13 vom 19. Januar 2000, 12. Parallel dazu sind die Arbeiten zum UNCITRAL-Modellgesetz für den elektronischen Geschäftsverkehr zu beachten, die auch die Entwicklung einheitlicher Regeln für elektronische Signaturen umfassen (www.un.or.at/ uncitral/index.htm). Auch die OECD arbeitet an einer Übersicht über Formvorschriften im Bereich elektronischer Signaturen.

9 Die an ein qualifiziertes Zertifikat zu stellenden Voraussetzungen finden sich in Anhang III der genannten Richtlinie.

10 Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, Bundesgesetzblatt am 21. Mai 2001, BGBl 2001 Teil I Nr. 22, 876 ff.

ist genehmigungsfrei nach entsprechender Anzeige möglich (4 Abs. 1 und 3 SigG). Die Anzeige erfolgt bei der Regulierungsbehörde für Telekommunikation und Post; die RegTP nimmt auch die allgemeine Missbrauchsaufsicht hinsichtlich der Einhaltung der technischen Standards vor. Nach § 11 Abs. 1 SigG haftet eine Zertifizierungsstelle einem Dritten für den Schaden, den dieser dadurch erleidet, dass er auf die Angaben in einem qualifizierten Zertifikat vertraut. Diese Haftung entfällt nur dann, wenn der Anbieter beweisen kann, dass er nicht schuldhaft gehandelt hat (§ 11 Abs. 2 SigG). Ein qualifiziertes Zertifikat hat nach § 292a ZPO den Anschein für sich, dass die zertifizierte elektronische Willenserklärung echt ist. Dieser Anschein kann nur durch Tatsachen erschüttert werden, die es ernsthaft als möglich erscheinen lassen, dass die Erklärung nicht mit dem Willen des Signatur-Schlüssel-Inhabers abgegeben worden ist. Der Kunde kann also immer noch vortragen, die Chipkarte mit dem Signaturschlüssel sei ihm entwendet worden. Allerdings trifft ihn dann eine Obliegenheit, diesen Fall unverzüglich dem Vertragspartner anzuzeigen; ansonsten verliert er sein Rügerecht. Im Übrigen bleibt ihm die Behauptung, ihm seien nicht die Daten angezeigt worden, die er signiert habe (etwa weil ein anderes als das signierte Dokument im Hintergrund signiert worden ist). Gelingt dem Anwender der Nachweis einer solch falschen Präsentation, ist die signierte Erklärung nicht authentisch. In der Forschung wird zu Recht von der „Achillesferse" des Signaturrechts gesprochen[11].

Eine freiwillige Akkreditierung ist für Zertifizierungsdiensteanbieter möglich, die von der zuständigen Behörde ein zusätzliches Gütesiegel erhalten (§ 15 SigG). Zu diesen Anbietern zählt die Deutsche Telekom AG mit ihrer Tochter „T-Telesec Crypt" (http://www.telesec.de). Die Deutsche Post AG mit ihrem Dienst „Signtrust" (http://www.signtrust. deutschepost.de) hat sich Mitte 2002 aus dem Geschäft zurückgezogen.

Seit Inkrafttreten des neuen Signaturgesetzes sind **13 Zertifizierungsstellen** akkreditiert; drei weitere stehen kurz vor der Akkreditierung. Den auf diese Weise generierten Zertifikaten kommt ein noch höherer Beweiswert als den normalen qualifizierten Signaturen zu, ohne dass man weiss, wie hoch der Beweiswert zu bemessen ist. Für das Zivilrecht stehen qualifizierte und akkreditierte Signaturverfahren auf einer Stufe; für Behörden erscheint allerdings eine Verpflichtung zur Nutzung akkreditierter Verfahren möglich[12].

11 So FISCHER-DIESKAU/GITTER/PAUL/STEIDLE, 709, 713. Siehe dazu auch PORDESCH, 89 ff.

12 Siehe ROSSNAGEL, Signatur, 225 f.; ROSSNAGEL, Unterschiede, 215, 221.

Zu klären ist noch die **Interoperabilität der Signaturen**, insbesondere im Hinblick auf die Nutzung im Ausland. Ende September 2001 wurden erste Interoperabilitätsspezifikationen (ISIS-MTT) seitens des BMWi veröffentlicht. Im Übrigen ist inzwischen auch das 3. Verwaltungsverfahren-Änderungsgesetz am 1.2.2003 in Kraft getreten[13]. Hiernach kann für den Bereich des Verwaltungsverfahrens eine durch Rechtsvorschrift angeordnete Schriftform, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Diese Form wird gem. § 3a II VwVfG erfüllt, wenn das elektronische Dokument mit einer qualifizierten elektronischen vorheriger Signatur nach dem Signaturgesetz versehen ist. Zu beachten sind ferner die Pläne für ein Justizkommunikationsgesetz. Hiernach soll künftig bei elektronischen Dokumenten, soweit die ZPO und das ArbGG für gerichtliche Dokumente die Schriftform und die handschriftliche Unterschrift verlangen, diese Anforderung durch Hinzufügung des Namens und einer qualifizierten elektronischen vorheriger Signatur erfüllt werden[14].

5. Digitale Signatur: Technische Umsetzung

Um das Signaturrecht zu verstehen, bedarf es einer kurzen Einführung in die technischen Grundlagen. Eine Verschlüsselung von elektronischen Nachrichten lässt sich auf zwei Wegen bewerkstelligen: symmetrisch und asymmetrisch.

5.1 Die symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung erfolgt **die Chiffrierung und Dechiffrierung über einen einheitlichen Schlüssel.** Beispiele einer solchen Verschlüsselung findet sich in der Kindheit, wenn Kinder z.B. eine Geheimsprache erfinden: Wer A sagt, meint B. Wer B sagt, meint C. Solche Abreden können und müssen natürlich nach einem komplizierteren Muster verfahren, wenn es um den Austausch von Geheiminformationen zwi-

13 BGBl I, 3322. Dazu auch SCHMITZ/SCHLATMANN, 1281; SCHLATMANN, 489; ROSSNAGEL, Verwaltungsverfahren, 469; zu den Entwürfen SCHMITZ, 1238; CATREIN, Kommunikation, 50; CATREIN, Entwurf, 413; ROSENBACH, 332; ROSSNAGEL, Signatur, 221; ROSSNAGEL, DVBl 2002, 1005; STORR, 579.

14 Vgl. dazu FISCHER-DIESKAU, 701 ff.

schen Erwachsenen über das Internet geht. IBM hat hierzu z.B. schon in den achtziger Jahren das Verfahren DES entwickelt (Data Encryption Standard). Erforderlich ist bei einer solchen Verschlüsselung, dass das Geheimverfahren vorab zwischen den Kindern angesprochen worden ist. Im Internet sind solche Absprachen aber nur selten möglich. Man müsste eine solche Absprache regelmässig über das Netz selbst vornehmen, was den Sicherheitswert der „Geheimsprache" deutlich herabsetzt. Auch kommunizieren zu viele Personen miteinander, als das man in kleiner Runde noch Geheimverfahren sicher verabreden könnte. Man kann im Internet daher solche Verfahren sinnvollerweise nur bei einer geschlossenen Nutzergruppe einsetzen.

5.2 Die asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung (public key crytography) **werden zwei unterschiedliche Schlüsselpaare** generiert und verwendet. Chiffrier- und Dechiffrierschlüssel sind nicht identisch; sie sind wie zwei Puzzleteile, die zwar unterschiedlich sind, aber von ihrem Verwender wieder zusammengefügt werden können. Die Schlüsselpaare können aufgrund dessen für unterschiedliche Zwecke verwendet werden. Zum einen kann man damit gewährleisten, dass eine Nachricht den Empfänger erreicht, ohne dass ein Dritter (etwa ein Hacker oder Strafverfolgungsbehörden) sie liest. Hierzu wird der Chiffrierschlüssel des Empfängers öffentlich bekannt gemacht; sein Dechiffrierschlüssel bleibt geheim. Der Absender verschlüsselt seine Botschaft mit dem öffentlichen Schlüssel des Empfängers und verschickt die Nachricht. Der Empfänger kann die Nachricht dann mit seinem privaten Schlüssel entschlüsseln und lesen. **Für Dritte ist die Nachricht nicht lesbar**.

Zum anderen kann man mit dem Schlüsselpaar die **Authentizität einer Nachricht** sichern. Hierzu wird der Dechiffrierschlüssel des Absenders öffentlich bekannt gegeben, sein Chiffrierschlüssel aber geheim gehalten. Der Absender chiffriert seine Nachricht und schickt sie den Empfänger. Dieser kann nun mit Hilfe des öffentlichen Dechiffrierschlüssels die Botschaft entschlüsseln und weiss, dass nur der Absender die Botschaft verschickt haben kann. Insofern wirkt das Schlüsselpaar wie eine digitale Unterschrift.

Wichtig ist hierbei eine Schlüsselgenerierung, die zwar eine schnelle Berechnung der Schlüssel in einer Richtung, nicht aber in umgekehrter

Richtung ermöglicht. Dazu verwendet man den sog. **RSA-Algorithmus** (benannt nach deren Entwicklern Rivest, Shamir und Adleman). Es werden sehr grosse Zahlen gebildet, die in Primfaktoren zu zerlegen sind. Die grosse Zahl kann sehr leicht mittels der Primzahlen berechnet werden. Wer aber nur die grosse Zahl kennt, hat so viele Möglichkeiten, diese aus den Primzahlen zu errechnen, dass er auch mit EDV-Hilfe nicht auf die korrekte Berechnung kommt.

Einfach lässt sich die Anwendung solcher Verfahren am Beispiel von **eTrust** demonstrieren. eTrust ist das Signaturmodell der Deutschen Post Signtrust auf der Basis des qualifizierten Zertifikats (siehe oben)[15]. Der Kunde erhält in einer Filiale der Deutschen Post auf Vorlage seines Personalausweises Chipkarte, Chipkartenlesegerät und PIN-Nummer. Signtrust weist ihm dann ein Schlüsselpaar zu, mit dessen Hilfe der Nutzer seine Mails signieren kann. eTrust wandelt die Nachricht beim Versenden in einen Zahlencode um. Dieser sog. „Hash-Wert", der für jede Mail unterschiedlich ist wird noch einmal verschlüsselt und dem Empfänger zusammen mit der Originalnachricht und dem öffentlichen Schlüssel übersandt. Aus diesen Eckdaten kann der Empfänger feststellen, wer die Nachricht verschickt hat (über den öffentlichen Schlüssel) und ob diese unverändert übermittelt worden ist (über den Hash-Wert).

5.3 Alice und Bob

Traditionell werden zur Erklärung kryptografischer Abläufe die **Charaktere Alice und Bob** verwendet. Die beiden wollen über einen Kanal wie z.B. das Internet Nachrichten austauschen, genau genommen will Alice eine elektronische Nachricht an Bob unterzeichnen. Ins Spiel kommen später ein Bösewicht namens Mallory und die Zertifizierungsstelle Trent.

Sinnvoll ist im Allgemeinen lediglich der **Einsatz asymmetrischer Verfahren**. Verwendet werden zwei Schlüssel: ein privater und ein öffentlicher Schlüssel. Beide sind einer bestimmten Person wie z.B. Alice ausschliesslich zugeordnet. Sie sind voneinander abhängig, können aber einzeln benutzt werden. Der private Schlüssel ist ausschliesslich dem Inhaber bekannt. Er dient der Verschlüsselung der Daten. Der öffentliche Schlüssel sollte möglichst breit bekannt gemacht werden. Mit ihm kann ein Empfänger von Daten, wie z.B. Bob, die Signatur prüfen.

15 Siehe dazu http://www.signtrust.de.

Zunächst muss Alice einmalig ein Schlüsselpaar, also **einen privaten und einen öffentlichen Schlüssel**, erzeugen. Zum Erzeugen einer Signatur benutzt Alice ihren privaten Schlüssel. Der zu unterschreibende Text wird dazu zunächst mit einem nicht umkehrbaren so genannten Hash-Verfahren komprimiert. Das so entstandene Komprimat (Hash-Wert) stellt den „Fingerabdruck" des Textes dar. Es wird dann mit dem privaten Schlüssel codiert. Die daraus entstehende Signatur wird dem zu übertragenden Dokument angehängt. Dieser Vorgang wird heute automatisch von entsprechender Software übernommen.

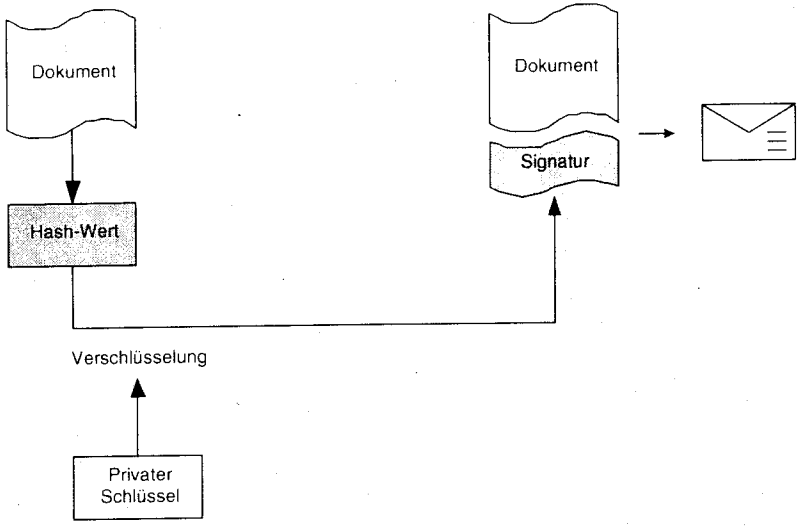

Abb.: Signieren

-----BEGIN PGP SIGNED MESSAGE-----
Informationsrecht, Prof. Dr. Thomas Hoeren
Donnerstags, 18.00 - 20.00 Uhr im S10
Beginn der Vorlesung: 15.10.1998
Klausur: 11.02.1998

-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 5.5.3i for non-commercial use <http://www.pgpi.com>
iQCVAwUBNrcWf-
XATg3nt91HBAQEyxAP/TgKI4n5FVpo5BKbg5QpbENkofXOSNAnE

qul8/ja8MqpvCafS6sPUztgGSer+BrXcBXzuUmCKt+J9OypTb3JEEJpF
V40QrdEz
Ril6eOjBP9hMWIxwUcXT6cNNoZ9EMq0BsH97ZpF6pHLO4yoJZgNa
Oy8rTAbqWacq
AkDnflcen2c=
=VMWr
-----END PGP SIGNATURE-----

Abb.: Beispiel einer PGP-signierten Nachricht

Grundsätzlich könnte anstelle des Hash-Werts auch die eigentliche Nachricht kopiert und mit dem privaten Schlüssel codiert werden und so als Unterschrift dienen. Problematisch ist hierbei die deutlich höhere Textmenge und der erhebliche Rechenaufwand, der aufgrund der Komplexität der asymmetrischen Verfahren erforderlich ist. Gängige Verfahren zum Bilden des verkürzenden Hash-Werts sind z.B. die Algorithmen RIPE-MED-160 oder SHA-1 mit einem Hash-Wert von 160 bit. Die Algorithmen zeichnen sich dadurch aus, dass sie nicht umkehrbar sind. Das heisst, dass es nach bisherigem Kenntnisstand nicht möglich ist, ausser durch Brute Force (systematisches Probieren aller Möglichkeiten) einen passenden Text zu einem gegebenen Hash-Wert zu erzeugen. Die Wahrscheinlichkeit, dass zwei Dokumente denselben 160 bit langen Hash-Wert besitzen, liegt bei 1 zu 2^{160}.

Zum Codieren kommen ebenfalls verschiedene Verfahren in Betracht. Gängig ist **RSA**, bei dem der Codierungs- bzw. Decodierungsvorgang im Ver- bzw. Entschlüsseln des Hash-Werts besteht. Dabei kommen sehr komplexe mathematische Funktionen zum Einsatz. Es ist nach derzeitigem theoretischen Stand nicht möglich, das Verschlüsselungsverfahren zu brechen mit Ausnahme einer „Brute Force"-Attacke. Bei dieser werden sämtliche möglichen Schlüssel systematisch probiert. Durch hinreichend grosse Schlüssellängen übersteigt der erforderliche Aufwand jedoch deutlich die derzeit weltweit verfügbare Rechenkapazität. Zudem kann die Schlüssellänge bei Bedarf variabel erhöht werden. Gängig ist derzeit eine Länge von 1024 Bit, zukünftig werden 2048 Bit zum Einsatz kommen.

Bob erhält nun die Nachricht. Seine Software komprimiert jetzt ebenfalls den Text und verwendet hierzu das gleiche Verfahren, das auch Alice's Software verwendet hat und das in der Signatur angegeben ist. Dies ergibt wiederum einen Hash-Wert. Dieser Hash-Wert, der öffentliche Schlüssel von Alice sowie die digitale Signatur des erhaltenen Dokuments

werden nun zur Prüfung der Signatur herangezogen. Beim RSA-Verfahren decodiert die Software dazu die Signatur mit dem öffentlichen Schlüssel von Alice und erhält den Hash-Wert zurück, den die Software von Alice erzeugt und in der Signatur beigefügt hatte. Diese beiden Hash-Werte müssen nun verglichen werden. Stimmen beide überein, so ist klar, dass gesendeter und empfangener Text identisch sind. Ausserdem steht fest, dass nur Alice, die alleine im Besitz des geheimen Schlüssels ist, die Signatur erzeugt haben kann, weil sonst der öffentliche Schlüssel nicht passen würde.

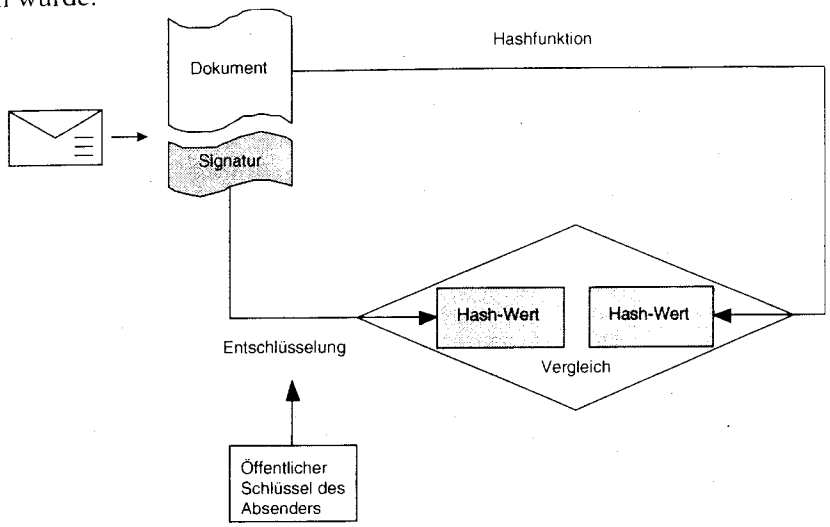

Abb.: Prüfung signierter Dokumente

Das Verfahren basiert allerdings auf der Annahme, dass der von Bob verwendete öffentliche Schlüssel von Alice „echt" ist, d.h. tatsächlich von Alice stammt. Dessen könnte sich Bob sicher sein, wenn Alice ihm ihren öffentlichen Schlüssel persönlich übergeben hätte. Dies ist häufig jedoch nicht praktikabel. Alice könnte ihren Schlüssel aber auch auf ihrer Webseite zum Abruf bereitstellen. Dies ist jedoch nicht ausreichend sicher: so könnte etwa Mallory sich in die Kommunikation über das Internet einschleusen und den abgerufenen Schlüssel verändern oder durch seinen eigenen öffentlichen Schlüssel ersetzen (Man-In-The-Middle-Attack). Mallory könnte Bob dann eine angeblich von Alice signierte Nachricht schicken. Bob's Überprüfung würde dann ergeben, dass die Nachricht tatsächlich von Alice signiert worden sei.

Stattdessen werden ***Zertifikate*** verwendet. Qualifizierte elektronische Signaturen sind elektronische Signaturen, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen. Das Zertifikat ist eine elektronische Bescheinigung, mit der ein öffentlicher Schlüssel einer Person zugeordnet und die Identität dieser Person bestätigt wird. Es enthält neben dem öffentlichen Schlüssel u.a. Angaben wie Name des Inhabers (oder ein Pseudonym), den Namen der Zertifizierungsstelle und das Ablaufdatum des Zertifikats.

Wenn Alice ein Zertifikat erhalten möchte, muss sie sich an eine Zertifizierungsstelle, etwa Trent, wenden. Sie muss ihren öffentlichen Schlüssel dort einreichen. Trent unterschreibt diesen öffentlichen Schlüssel nun mit dem eigenen privaten Schlüssel. Dieses Verfahren kann mehrstufig wiederholt werden, was zu einer Zertifizierungshierarchie führt. Sie wird auch als PKI (Public Key Infrastructure) bezeichnet. Daneben gibt es ähnliche, aber nicht hierarchische Verfahren wie z.B. das populäre bei PGP verwendete „Web of Trust".

Zertifikate werden von **Zertifizierungsdiensteanbietern** erteilt. So haben sich im Juni 1999 die vier deutschen Grossbanken an dem Sicherheitsdienstleister „TC Trust Center" beteiligt. Hierdurch ist die Grundlage für einen gemeinsamen Zertifizierungsanbieter der privaten Banken geschaffen worden. Daneben bieten beispielsweise die Deutsche Post AG mit SignTrust und die Deutsche Telekom mit Telesec die Zertifizierung an. Gleiches gilt für verschiedene Kammern. Ein aktueller Stand zu Zertifizierungsdiensteanbietern, die sich bei der Regulierungsbehörde akkreditiert oder dort ihre Tätigkeit angezeigt haben, ist unter http://www.regtp.de zu finden.

Auf diese Weise kann ein Empfänger, der über den öffentlichen Schlüssel einer Zertifizierungsstelle verfügt, eine Signatur prüfen. Daneben kann er direkt in öffentlichen Verzeichnissen der Zertifizierungsstellen prüfen, ob ein Zertifikat gültig ist. So könnte es insbesondere widerrufen worden sein, etwa weil der private Schlüssel kompromittiert wurde. So muss Bob nun lediglich sicher sein können, dass der ihm bekannte öffentliche Schlüssel einer möglichst hohen Stelle in der Zertifizierungshierarchie, etwa der der Regulierungsbehörde als Wurzelinstanz, korrekt ist. Damit kann er, gegebenenfalls über mehrere Stufen, prüfen, ob das Zertifikat von Alice und damit ihr öffentlicher Schlüssel korrekt ist. Zusätzlich sollte er aber prüfen, ob das Zertifikat nicht zwischenzeitlich widerrufen wurde, indem er in entsprechenden öffentlichen Datenbanken des Zertifikatausstellers nachschaut.

Derzeit finden Signiervorgänge noch überwiegend auf dem PC mit Hilfe spezieller Software wie z.B. PGP statt. Private Schlüssel werden dabei typischerweise auf Datenträgern wie z.B. Disketten gespeichert. Dieses Verfahren ist jedoch nicht ausreichend sicher, da der PC z.B. durch Trojanische Pferde o.ä. befallen sein und damit der private Schlüssel ausgespäht werden könnte. Zukünftig werden daher Chipkarten (SmartCards) zunehmende Verbreitung erfahren, die den privaten Schlüssel beinhalten und Codierungsvorgänge direkt auf der Karte durchführen, d.h. der private Schlüssel verlässt niemals die Karte. Benötigt werden dazu Lesegeräte. Neben den inzwischen gebräuchlichen einfachen Lesegeräten sind höherwertige Geräte mit einem Display vorzuziehen. In diesem Display wird der zu signierende Text angezeigt, um das Unterschieben unerwünschter Texte, die unterschrieben werden, zu unterbinden.

6. Schriftform und digitale Signatur

Die deutsche Zivilrechtsordnung sieht an zahlreichen Stellen die Einhaltung einer besonderen Schriftform vor. Digital signierte Dokumente und Erklärungen genügen jedoch dem Schriftformerfordernis nach derzeitiger Rechtslage schon naturgemäss nicht[16]. Denn nach § 126 BGB muss bei einer gesetzlich vorgesehenen Schriftform der Text von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden. Das Erfordernis der Schriftform ist zum Beispiel vorgesehen bei Verbraucherdarlehensverträgen (§ 492 Abs. 1 S. 1 und 2 BGB), beim Grundstückskaufvertrag (§ 311b BGB), bei Quittungen (§ 368 BGB), bei der Bürgschaftserklärung (§ 766 BGB) und beim Testament (§§ 2231 Nr. 1, 2231 Nr. 2, 2247 I BGB).

6.1 E-Commerce-Richtlinie, Signaturrichtlinie und Schriftform

Auch auf europäischer Ebene hat man sich des Themas angenommen, da die bislang vorhandenen nationalen und internationalen Rechtsnormen aus mehreren Gründen keine befriedigende Lösung für die sich im Bereich des elektronischen Geschäftsverkehrs ergebenden Probleme geboten haben. Insbesondere soll der wirksame Abschluss von Verträgen über das Internet nicht an Formvorschriften des nationalen Rechts scheitern.

Ende 1999 ist die **Richtlinie für elektronische Signaturen**[17] in Kraft getreten, deren Ziel es ist, die grenzüberschreitende rechtliche Anerkennung elektronischer Signaturen sicherzustellen und dafür einen angemessenen und harmonisierten rechtlichen Rahmen zu schaffen.

Nach Art. 5 der Richtlinie sollen elektronische Signaturen die gleichen Rechtswirkungen entfalten wie handschriftliche Unterschriften und bei Gerichtsverfahren als Beweismittel zugelassen werden.

Um den Anforderungen im Vergleich zur eigenhändigen Unterschrift zu genügen, muss die Signatur auf einem von einer Signaturerstellungseinheit **qualifizierten Zertifikat** beruhen, Art. 5 I der Richtlinie. Dieses ist eine Bescheinigung in elektronischer Form, die eine Signaturprüfung einer Person zuordnet, die Identität dieser Person verifizieren kann und mit den Anforderungen in Anhang I der Richtlinie korrespondiert. In der Anlage sind die Anforderungen enthalten, die an diese qualifizierten Zertifikate zu stellen sind. Allerdings darf gemäss Art. 5 II der Richtlinie nicht schon deshalb die rechtliche Wirksamkeit einer elektronischen Signatur versagt werden, weil sie in elektronischer Form vorliegt oder nicht auf einem qualifizierten Zertifikat beruht bzw. nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht.

Neben der EU-Signaturrichtlinie ist auch die **E-Commerce-Richtlinie**[18] zu beachten. In den ihr vorangegangenen Begründungen heisst es, dass „die Mitgliedstaaten einen bestimmten Zustand herbeizuführen haben, ihre innerstaatlichen Rechtsvorschriften systematisch daraufhin zu überprüfen, ob sie die Verwendung elektronischer Verträge behindern, beschränken oder uninteressant machen." In Art. 9 der Richtlinie findet sich eine ausführliche Regelung zur Frage der Schriftform. Nach Art. 9 Abs. 1 der Richtlinie ist der Abschluss elektronischer Verträge zu ermöglichen. Insbesondere soll die Tatsache, dass ein Vertrag auf elektronischem Wege zustande gekommen ist, nicht zur Ungültigkeit oder Wirkungslosigkeit des Vertrages führen dürfen. Mit dem Inhalt des Art. 9 Abs. 1 der Richtlinie dürfte sich der komplizierte Streit zwischen Deutschland und dem

16 So auch grundlegend BGHZ 121, 224.

17 Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.

18 Geänderter Entwurf für eine Richtlinie des Europäischen Parlaments und des Rates über rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt v. 17. August 1999 – KOM (1999) 427 endg.

Korrigierend greift der in Art. 9 Abs. 2 der Richtlinie genannte Ausnahmekatalog ein, der Notarsverträge, Verträge mit Registerpflicht sowie familien- und erbrechtlichen Vereinbarungen ausnimmt[20]. Diese Vorschrift erstaunt insofern, als dass sich in dem Entwurf zur Richtlinie der „Geist des Binnenmarktes" widerspiegelt, nun aber Gedanken zu einer Reform des Zivilrechts auftauchen. Familien- und Erbrecht haben mit Binnenmarkt an sich nichts zu tun. Im Übrigen werden Vereinbarungen auf diesen Gebieten wohl kaum über das Internet oder andere Onlinedienste geschlossen. Nach Art. 9 Abs. 3 der Richtlinie sollen die jeweiligen Mitgliedstaaten der Kommission eine vollständige Liste von weiteren Ausnahmefällen vorlegen, so wie sie in Abs. 2 vorgesehen sind.

Auch wenn die EU-Signaturrichtlinie und die E-Commerce-Richtlinie das Problem der Schriftform noch nicht vollständig gelöst haben mögen und permanente Verbesserungen bei der ständig fortschreitenden technischen Entwicklung angebracht sind, dürften sie die nationalen Gesetzgeber mit Blick auf die Ausgestaltung und konkrete Formulierung von Formerfordernissen zu intensiven gesetzgeberischen Aktivitäten animieren, sofern dies nicht schon geschehen ist.

6.2 Form-Neuregelungen in Deutschland

In den frühen Entwürfen des IuKDG (Informations- und Kommunikationsdienstegesetz) versuchte man dem Problem der elektronischen Form durch Einführung einer „Testnorm" Herr zu werden. Man sah darin die Änderung einer einzelnen, praktisch kaum relevanten Formvorschrift, nämlich der Schriftform bei Fernunterrichtsverträgen im Rahmen des Fernunterrichtsschutzgesetzes, durch eine spezielle, elektronische Form vor. Dann verzichtete man jedoch auf dieses Experiment und liess die Frage der Schriftform aussen vor.

19 Siehe allgemein zur Signaturdiskussion, BERGMANN/STREITZ, 37; KUNER, 108; MALZER, 96; MERTENS, 769; ROSSNAGEL, Rechtsfragen, 75.

20 Nach dem ursprünglichen Entwurf vom 18. November 1998 sollte auch diese Liste von Ausnahmefällen von der Kommission einseitig geändert – also verlängert oder verkürzt – werden können. Im geänderten Vorschlag vom 17.08.1999 und in der verabschiedeten Richtlinie ist diese Regelung gestrichen worden.

Im Mai 1999 hat sich das Bundesjustizministerium diesem Anliegen angenommen, angestossen auch durch die oben skizzierte E-Commerce-Richtlinie[21]. Das Ministerium legte einen Gesetzesentwurf zur Anpassung der Formvorschriften des Privatrechts an den modernen Geschäftsverkehr vor[22]. Zu diesem Entwurf legte am 20. Juni 2001 der Vermittlungsausschuss eine Beschlussempfehlung vor, die dann am 22. Juni 2001 vom Bundestag angenommen worden ist[23]. Das Gesetz ist zum 1. August 2001 in Kraft getreten[24].

Das Gesetz sieht, neben der notariellen Beurkundung, als weiteren Ersatz der durch Gesetz vorgeschriebenen Schriftform die **„elektronische Form"** vor (§ 126 III BGB). In § 126a BGB werden die Voraussetzungen der elektronischen Form festgelegt. Hier wird die Natur des SigG als Referenzgesetz deutlich, denn zur Wahrung der elektronischen Form ist eine qualifizierte elektronische Signatur nach dem SigG erforderlich. Gestrichen wurden zwei im ersten Entwurf aus dem Jahre 1999 enthaltenen widerlegliche Vermutungsregeln, zum einen die Zurechnung einer Willenserklärung zum Signaturschlüsselinhaber (§ 126a III 1 BGB-E a.F.) und zum anderen eine Sonderausprägung einer vermuteten Anscheins- bzw. Duldungsvollmacht (§ 126a III 2 BGB-E a.F.)[25]. Die Schriftform bleibt allerdings bei bestimmten Konstellationen bestehen, z.B. bei

- § 623 BGB (Kündigung des Arbeitsvertrages)
- § 630 BGB, § 73 HGB (Zeugnis)
- § 766 S. 2 BGB (Bürgschaft)
- §§ 780, 781 BGB (Schuldversprechen und -anerkenntnis)

Mit der **„Textform"** als neuer, „verkehrsfähiger" Form, wird in § 126b BGB ein erleichtertes Formerfordernis gegenüber der Schriftform vorgesehen, das den Bedürfnissen des modernen Rechtsverkehrs entgegen kommt. Ursprünglich war vorgesehen, dass die Textform bereits eingehalten ist, wenn der Text in Schriftzeichen lesbar, die Person des Erklärenden erkennbar ist und der Abschluss der Erklärung erkennbar gemacht wird.

21 Siehe dazu auch den japanischen Omnibus Act for the Use of Information and Communications Technology relating to the Delivery of Papers, Act. No. 126 of 2000, effective on 1 April 2001.

22 Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr vom 19. Mai 1999 – BMJ I B 1 – 3414/2.

23 Bundesrats Drucksache 497/01. Siehe den Entwurf unter http://www.bmj.bund.de/ggv/ggv_i.htm/bgbrege1.pdf.

24 Gesetz zur Anpassung der Formvorschriften im Privatrecht vom 13. Juli 2001, BGBl 2001 I Nr. 35, 1542.

25 Abschluss-, Identitäts-, Echtheits-, Warn- und Beweisfunktion.

Dann protestierte allerdings der Bundesrat und wies darauf hin, dass diese Formulierung zu weit sei und § 126b BGB ersatzlos gestrichen werden müsse[26]. Dieser Widerspruch war insofern problematisch, als das am gleichen Tag vom Bundesrat gebilligte Mietrechtsreformgesetz bereits Verweise auf die Textform enthielt. Die Regelung wurde eilig neu formuliert und passierte dann Ende Juni 2001 den Vermittlungsausschluss[27]. Nach dem jetzt geltenden § 126b BGB wird die Textform eingehalten, wenn die Erklärung

- in einer Urkunde oder andere „zur dauerhaften Wiedergabe in Schriftzeichen geeigneten Weise" abgegeben worden ist,
- die Person des Erklärenden genannt ist und
- der Abschluss der Erklärung durch Nachbildung der Namensunterschrift oder anders erkennbar gemacht wird.

Auf die eigenhändige Unterschrift soll dann verzichtet werden können. Problematisch ist hier der Verweis auf die dauerhafte Wiedergabe und die Parallele zur Namensunterschrift. Die Textform ist für solche, bislang der strengen Schriftform unterliegenden Fälle gedacht, in denen das Erfordernis einer eigenhändigen Unterschrift unangemessen und verkehrserschwerend ist. Typische Anwendungen betreffen Massenvorgänge mit sich wiederholenden, meist gleichlautenden Erklärungen ohne erhebliche Beweiswirkung. Dazu zählt auch das Computerfax von PC zu PC. In dem Gesetz ausgewiesene Fälle sind z.B. §§ 355 I, 356 I Nr. 3, 410 II, 416 II, 556b Abs. 2 Nr. 1 und 651g II 3 BGB.

Anders ist die Neuregelung der ZPO. Nach dem **Zustellungsreformgesetz**[28] kann die Zustellung in Zivilverfahren auch durch ein Fax oder ein elektronisches Dokument erfolgen (§ 174 Abs. 2 und 3 ZPO n.F.). Welche Formerfordernisse das elektronische Dokument erfüllen muss, lässt das Gesetz offen. Eine qualifizierte Form ist allerdings notwendig, wenn gesichert werden soll, dass der Inhalt der Nachricht bei der Übertragung unverändert geblieben ist. Das elektronische Dokument gilt als zugestellt, wenn der Adressat bestätigt, die Datei erhalten und zu einem bestimmten Zeitpunkt entgegengenommen zu haben. Das Empfangsbekenntnis kann auch elektronisch übermittelt werden, wobei eine Verschlüsselung oder Signatur nicht erforderlich ist. Für die Rücksendung des Bekenntnisses

26 BT-DrS 14/6044 vom 15. Mai 2001.
27 BT-DrS 14/6353 vom 20. Juni 2001.
28 Gesetz zur Reform des Verfahrens bei gerichtlichen Zustellungen vom 25. Juni 2001, BGBl I 1206, in Kraft seit dem 1. Juli 2002. Siehe dazu auch VIEFHUES/SCHERF, 596 und VIEFHUES, 556.

wird die ZPO noch einmal geändert werden, um auch eine elektronische Rücksendung zu ermöglichen.