Elektronische Signatur

Einleitung

Das „Gesetz über Rahmenbedingungen für elektronische Signaturen“ (Signaturgesetz, SigG) ist am 22.05.2001 in Kraft getreten. Damit wurde die Richtlinie 1999/93/EG vom 13.12.1999 des Europäischen Parlamentes und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen umgesetzt. Das frühere Signaturgesetz von 1997 trat außer Kraft.
Die Richtlinie verpflichtete den deutschen Gesetzgeber zur Neugestaltung von drei Rechtskomplexen[1]:

- Änderung der Sicherheitsinfrastruktur, die dem deutschen Signaturgesetz zugrunde liegt
- schuldrechtliche Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift
- beweisrechtliche Klarstellung des Beweiswerts der elektronischen Signatur

Richtlinienkonform wurde der Begriff „digitale Signatur“ durch „elektronische Signatur“ ersetzt.

Das SigG stellt eine einheitliche „Infrastruktur“ für elektronische Signaturen sicher. Insbesondere bestimmt es, was eine „qualifizierte elektronische Signatur“ ist. Auf Grundlage des neuen SigG wurde die am 22.11.2001 in Kraft getretene neue Signaturverordnung erlassen.

Das „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Formvorschriften an den modernen Rechtsverkehr“ (FormVAnpG)[2] führte zum 01.08.2001 zwei neue Formarten in das Privatrecht ein. Zum einen wird als Alternative zur Schriftform die elektronische Form anerkannt (§ 126 Abs. 3 BGB), zum anderen gibt es nunmehr die Textform in § 126b BGB.

Teilweise wird der elektronischen Form bereits ein Anwendungsfeld gleichberechtigt **neben** der eigenhändigen Unterschrift geschaffen. So spricht das BGB in § 309 Nr. 12 (Wirksamkeit von Beweislastregelungen in AGB) und in § 355 Abs. 2 Satz 2 (Widerrufsrecht bei Verbraucherverträgen) von „qualifizierter elektronischer Signatur“, so dass der Erklärungsempfänger sich in diesen Fällen nicht gegen die elektronische Kommunikation wehren kann[3].

---

[1] Kilian, BB 2000, 734.

[2] BGBl I, 1542.

[3] Dauner-Lieb (Noack), § 126, Rn 11.

Technische Umsetzung

Die elektronische Signatur ist – im Gegensatz etwa zur eingescannten Unterschrift – mit einer Art „Siegel" vergleichbar. Bei der elektronischen Signierung wird als „Siegel" ein einmaliger Schlüssel generiert, der dem Dokument angehängt wird.[4] Durch die Verschlüsselung einer Datei mit einem einzig und allein einer Person zurechenbaren geheimen Schlüssel werden zum einen die Datei und der Erzeuger logisch miteinander verknüpft, zum anderen kann die Datei nicht mehr unbemerkt verändert werden.[5]

Verschlüsselungsverfahren

Als Grundlage für die elektronische Signatur wird für jede Person mit Hilfe eines asymmetrischen Verschlüsselungsverfahrens ein einmaliges Schlüsselpaar generiert. Die Schlüssel werden als öffentlich und privat bezeichnet und stehen in einer speziellen mathematischen Abhängigkeit zueinander. Chiffrier- und Dechiffrierschlüssel sind nicht identisch, sie sind wie zwei Puzzleteile, die zwar unterschiedlich sind, aber von ihrem Verwender wieder zusammengefügt werden können.[6]

Der private Schlüssel wird vom rechtmäßigen Inhaber dazu verwendet, die elektronische Signatur zu erzeugen. Der Schlüssel selbst wird dabei nicht sichtbar. Er befindet sich ausschließlich auf einer Chipkarte, die zur Kategorie der Smartcards zählt und äußerlich einer Telefonkarte ähnelt. Der Schlüssel ist in dieser Karte so geschützt, dass noch nicht einmal der rechtmäßige Besitzer ihn „auslesen" kann. [7]

Mit dem öffentlichen Schlüssel kann jeder Empfänger die Signatur und das Dokument auf die Echtheit und Unversehrtheit überprüfen. Der öffentliche Schlüssel wird in einem öffentlich zugänglichen Verzeichnis zum jederzeitigen Abruf bereitgehalten.

Die Schlüsselpaare können für unterschiedliche Zwecke verwendet werden. Zum einen kann dadurch, dass der Absender mit dem öffentlichen Schlüssel des Empfängers eine Nachricht verschlüsselt, die dann nur der Empfänger mit seinem privaten Schlüssel dechiffrieren kann, gewährleistet werden, dass keine Dritter die Nachricht liest. Zum anderen kann man mit dem Schlüsselpaar die Authentizität der Nachricht sichern.

---

[4] Schicker, JurPC Web-Dok. 139/2001, Abs. 8.

[5] Roßnagel, NJW 2001, 1817.

[6] Hoeren, Rechtsfragen im Internet, S. 234.

[7] Schicker, JurPC Web-Dok. 139/2001, Abs. 12.

Zum Erzeugen einer Signatur wird der private Schlüssel verwendet. Der zu unterschreibende Text wird zunächst mit einem nicht umkehrbaren sog. Hash-Verfahren komprimiert, es wird ein Art Quersumme gebildet, der sog. Hash-Code. 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.[8]

Nach der Signierung besteht die komplette Datei nun aus der ursprünglichen Datei selbst, der angehängten elektronischen Signatur und dem (den) Signaturschlüssel-Zertifikat(en) des Unterschreibenden, also seinen persönlichen Angaben.[9]

Nach derzeitigem theoretischem Stand ist es nicht möglich, das Verschlüsselungsverfahren zu brechen, mit Ausnahme einer „Brute-Force"-Attacke (=systematisches Probieren aller Möglichkeiten).[10] Durch hinreichend große Schlüssellängen übersteigt der erforderliche Aufwand jedoch die derzeit weltweit verfügbare Rechenkapazität. Zudem kann die Schlüssellänge bei Bedarf variabel erhöht werden.

Zur Überprüfung der elektronischen Signatur wird das gleiche Verfahren wie zur Verschlüsselung in umgekehrter Richtung mit dem öffentlichen Schlüssel durchgeführt. Die elektronische Signatur wird entschlüsselt, so dass der ursprüngliche Hash-Code wieder vorliegt. Dann wird von den übermittelten Daten wieder der Hash-Code gebildet und mit dem entschlüsselten Hash-Code verglichen. Bei Übereinstimmung steht fest, dass die Signatur mit dem dazugehörigen Signaturschlüssel erzeugt und die Daten nicht verändert wurden.[11]

Die Signaturerstellung basiert auf dem Einsatz von Chipkarte (Smartcard) und PIN.[12] Man hat sich diesbezüglich aus Sicherheitsaspekten für eine Hardwarelösung entschieden. Ein auf der Smartcard gespeicherter privater Schlüssel verlässt niemals die Karte und ist daher besonders sicher verwahrt. Diese Sicherheit können softwarebasierte Lö-

---

[8] Hoeren, Rechtsfragen im Internet, S. 236.

[9] Schicker, JurPC Web-Dok. 139/2001, Abs. 17.

[10] Hoeren, Rechtsfragen im Internet, S. 237.

[11] Schicker, JurPC Web-Dok. 139/2001, Abs. 19.

[12] Müglich, MMR 2000, 10f.

sungen nicht bieten.[13] Der private Schlüssel ist auf der Speicherplatte, auf der er gespeichert ist, für Unberechtigte unzugänglich.[14]

Verfahren zur Erlangung einer qualifizierten elektronischen Signatur

Der Signierwillige muss zunächst mit einem Zertifizierungsdiensteanbieter (§ 4 SigG) einen Vertrag schließen, um ein qualifiziertes Zertifikat (§§ 5, 7 SigG) zu erhalten. Zertifizierungsdiensteanbieter sind gem. § 2 Nr. 8 SigG natürliche oder juristische Personen, „die qualifizierte Zertifikate oder qualifizierte Zeitstempel anbieten". Das (zeitlich nur begrenzt gültige) Zertifikat bestätigt die Zuordnung des Schlüsselpaares ausschließlich auf die Person des Inhabers.

Ein qualifiziertes Zertifikat kann als Attribut Angaben über die Vertretungsmacht einer dritten Person enthalten. Dieses Zertifizierungsattribut steht wertungsmäßig einer Vollmachtsurkunde gleich.[15]

Um der Missbrauchsgefahr an den öffentlichen Schlüsseln zu entgehen, muss der Nutzer eine Zertifizierung seines öffentlichen Schlüssels erlangen. Hierzu muss der öffentliche Schlüssel bei einer Zertifizierungsstelle eingereicht werden. Diese unterschreibt den öffentlichen Schlüssel nun mit dem eigenen privaten Schlüssel. Dieses Verfahren kann mehrstufig wiederholt werden, was zu einer Zertifizierungshierarchie führt. Sie wird auch als Public Key Infrastructure (PKI) bezeichnet. Daneben gibt es ähnliche, aber nicht hierarchische Verfahren wie z.B. das populäre bei PGP verwendete „Web of Trust". [16]

Auf diese Weise kann ein Empfänger, der über den öffentlichen Schlüssel einer Zertifizierungsstelle verfügt, eine Signatur prüfen. Er muss lediglich sicher sein, dass der ihm bekannte Schlüssel einer möglichst hohen Stelle in der Zertifizierungshierarchie korrekt ist, um ggf. über mehrere Stufen zu prüfen, ob das Zertifikat des Absenders eines Dokuments und damit der öffentliche Schlüssel korrekt ist.

---

[13] Geis, MMR 2000, 668.

[14] vertiefend: Roßnagel in: Roßnagel (Hrsg.), Recht der Multimediadienste, 1999, 5.Teil, § 14 Rn 79.

[15] Dauner-Lieb (Noack), § 126a, Rn 24.

[16] Hoeren, Rechtsfragen im Internet, S. 238.

Anwendung in der Praxis

Zur Anwendung einer qualifizierten elektronischen Signatur werden ein Chipkartenleser und spez. Signatursoftware benötigt, die einer bestimmten Sicherheitsstufe („hoch“) en t-sprechen. Außerdem muss ein Online-Zugang zu Datenbanken der Trust-Center hergestellt werden.

Problematisch ist hierbei die Kompatibilität der Software-Produkte der verschiedenen Anbieter und auch der verschiedenen Trust-Center.

Der Empfänger muss nicht nur mit Nutzung der elektronischen Form einverstanden sein, er muss auch hinreichende Darstellungsmöglichkeiten besitzen, da sonst der Zugang mangels Möglichkeit der Kenntnisnahme nicht gegeben ist[17]. Grund hierfür ist die Qualifizierung einer online übermittelten Willenserklärung als Erklärung unter Abwesenden[18], § 130 BGB. Aus diesem Grund ist auch eine Kombination von schriftlich und elektronisch vermitteltem Vertragsschluss denkbar.

Im Hinblick auf die dauerhafte Lesbarkeit eines signierten Textes kommt es auf die dauerhafte Verfügbarkeit der Mittel zu Lesbarkeit an. Gerade die stetige Weiterentwicklung der Softwarekomponenten kann dazu führen, dass für die Erfüllung der Überprüfungsfunktion das Vorhalten an sich nicht mehr im Einsatz befindlicher Software in Betracht kommen kann.

Materiellrechtliche Umsetzung

Im Signaturgesetz ist nur die Sicherheitsinfrastruktur geregelt, die Umsetzung im Privatrecht regelt das Gesetz zur Anpassung der Formvorschriften.

verschiedene Arten elektronischer Signaturen

Eine elektronische Signatur besteht aus Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und zur Authentifizierung dienen (§ 2 Nr. 1 SigG). Diese Beifügung oder Verknüpfung reicht aber für einen sicheren Rechtsverkehr nicht aus, da sich hierbei weder die Authentizität noch die Inte-

---

[17] Dauner-Lieb (Noack), § 126a, Rn 16.

[18] Müglich, MMR 2000, 9.

grität des Dokuments gewährleisten lässt. Daher verlangen gesetzliche Bestimmungen durchweg nach der „qualifizierten elektronischen Signatur“.

Die Qualität der elektronischen Signatur bestimmt die Beweisqualität.[19] Zu unterscheiden sind drei "Qualitätsstufen", die sich durch unterschiedlich hohe Sicherheits-, Nachweis- und Kontrollniveaus auszeichnen.[20]

einfache elektronische Signatur

Hierbei handelt es sich um eine digitale Unterschrift, deren Erzeugung nicht nach den Vorgaben des Signaturgesetzes erfolgt. Elektronische Signaturen sind nach § 2 Nr. 1 SigG alle Daten, die anderen elektronischen Daten beigefügt werden und zur Authentifizierung dienen. Sie müssen nicht fälschungssicher und auch nicht mit den anderen Daten fest verknüpft sein. Selbst eine jederzeit fälschbare und entfernbare eingescannte Unterschrift genügt dieser Definition.[21]

Solche Signaturen sind nicht verboten, allerdings der Schriftform auch nicht gleichgestellt (§ 126 Abs. 3 BGB). Auch kommt ihnen kein erhöhter Beweiswert im Sinne von § 292a ZPO zu. Schließlich fehlt auch die Sicherheitsvermutung nach § 15 Abs. 1 SigG.[22]

fortgeschrittene elektronische Signatur

Diese Signaturart ist geregelt in § 2 Nr. 2 SigG und muss zumindest vier Funktionen erfüllen: sie muss ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sein, seine Identifizierung ermöglichen, mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann und mit den Daten, auf die sie sich bezieht, so verknüpft sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Hierbei entfällt also die Authentifizierung über das Zertifikat eines Dritten, materiellrechtlich sind mit dieser Signaturart keine Rechtsfolgen verknüpft. Es handelt sich trotzdem um eine weit verbreitete technische Signaturart (etwa Pretty-good-privacy-Software).[23]

---

[19] Geis, BB2001, Heft 21, Die erste Seite.

[20] Roßnagel, NJW 2001, 1819.

[21] Roßnagel, NJW 2001, 1819.

[22] Hoeren, Rechtsfragen im Internet, S. 232.

[23] http://www.pgp.com

qualifizierte elektronische Signatur

Qualifizierte elektronische Signaturen sind elektronische Signaturen, die auf einem zum Zeitpunkt der 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.[24]

Diese Signaturart stellt die gesetzliche elektronische Form dar; § 126 a BGB. Qualifizierungskriterien sind:

- ausschließliche Zuordnung zu dem Signaturschlüssel-Inhaber (§ 2 Nr. 2a SigG)
- Ermöglichung der Identifizierung des Signaturschlüssel-Inhabers (§ 2 Nr. 2b SigG)
- Erzeugung mit Mitteln, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann (§ 2 Nr. 2c SigG)
- Verknüpfung mit den Daten, auf die sich die Signatur bezieht dergestalt, dass eine nachträgliche Veränderung der Daten erkannt werden kann (§ 2 Nr. 2d SigG)
- die Signatur muss auf einem zum Zeitpunkt der Erzeugung gültigen Zertifikat (§ 7 SigG) beruhen (§ 2 Nr. 3a SigG)
- die Signatur muss mit einer sicheren Signaturerstellungseinheit (§ 2 Nr. 10 SigG) erzeugt werden (§ 2 Nr. 3b SigG)

§§ 126, 126a BGB

§ 126a BGB definiert die elektronische Form, deren materieller Anwendungsbereich durch § 126 Abs. 3 BGB in Verbindung mit den die Schriftform anordnenden Normen bestimmt wird. Dort wo das Gesetz das hergebrachte Schriftformerfordernis *ausdrücklich* vorsieht, findet aber die neue elektronische Form auch in Zukunft keine Anwendung. Dies wird mir der besonderen Schutzfunktion des Schriftformerfordernisses begründet[25] und ergibt sich aus der Formulierung „wenn sich nicht aus dem Gesetz ein anderes ergibt“ (§ 126 Abs. 3 2. Halbsatz BGB). Zu finden sind solche Ausnahmevorschriften etwa Arbeitsrecht und bei der Bürgschaft. Die Verwendung der elektronischen Form führt hier wegen § 125 Abs. 1 Satz 1 BGB zur Nichtigkeit.

Die Neuregelung durch das FormVAnpG bestimmt die elektronische Form als Äquivalent zur Schriftform. Immer dann, wenn das BGB und andere privatrechtliche Gesetze nach der Schriftform verlangen, kann künftig auch die elektronische Form verwandt

---

[24] Hoeren, Rechtsfragen im Internet, S. 238.

[25] Müglich, MMR 2000, 10.

werden. So ist es nunmehr möglich, den elektronischen Rechtsverkehr auch in Bereichen zu etablieren, die bislang wegen der papierschriftlichen Fixierung ausgespart blieben. Die meisten Verträge, die im E-Commerce eine Rolle spielen, konnten allerdings auch bereits vor der FormVAnpG-Reform durch den Austausch elektronisch transportierter Willenserklärungen abgeschlossen werden, da die Schriftform nicht vorgeschrieben ist.[26]

Durch die Signatur wird die **Abschlussfunktion** der eigenhändigen Unterschrift gewährleistet, der private Signaturschlüssel „siegelt" den Text. Die **Identitätsfunktion** wird durch den öffentlichen Schlüssel erfüllt. Letztliche Sicherheit über die Identität kann der Empfänger nur dann erhalten, wenn er die Möglichkeiten der Identifizierung des Ausstellers mit der digitalen Signatur auch nutzt. Das bekannte Problem des Missbrauchs von Chipkarte und PIN findet sich somit auch in diesem Bereich wieder. In der Gesetzesbegründung zu § 126 BGB wird davon gesprochen, dass man sich ein Mehr an Sicherheit vorstellen könne, so etwa den Einsatz ergänzender biometrischer Verfahren.[27] Welche Sorgfaltsobliegenheiten den Schlüsselinhaber somit aufgrund der Vermutungsregelung des § 126a Abs. 3 BGB treffen wird langfristig wohl nur durch die Rechtsprechung entwickelt werden.[28] Durch den Zusammenhang von Text und Unterschrift wird aufgrund mathematisch-logischer Verbindung zwischen Text und Signierung auch die **Echtheitsfunktion** der eigenhändigen Unterschrift erfüllt.

Bei der vereinbarten elektronischen Form des § 126 Abs. 3 BGB sind auch andere Signaturarten als die der qualifizierten elektronischen Signatur ausreichend. Die Ersetzung der Schriftform durch die elektronische Form ist abhängig vom ausdrücklichen oder konkludenten Willen der Beteiligten. Bei (empfangsbedürftigen) Erklärungen gehört nicht nur die elektronische Signierung, sondern auch die Möglichkeit der Kontrolle zur Formvollendung.[29]

§ 126a Abs. 2 BGB verweist hinsichtlich der qualifizierten elektronischen Signatur auf das Signaturgesetz. Zum Vertragsschluss nach § 126a Abs. 2 BGB ist es erforderlich, dass die Parteien je ein gleichlautendes Dokument elektronisch signieren, es ist nicht

---

[26] Noack, DStR 2001, 1894.

[27] Begründung zu § 126a BGB-E, S. 15, vgl. hierzu auch unten „Technische Weiterentwicklung".

[28] Müglich, MMR 2000, 11.

[29] Dauner-Lieb (Noack), § 126a, Rn 5.

ausreichend, wenn jeder Vertragspartner seine Angebots- bzw. Annahmeerklärung elektronisch signiert.[30]

Zum Anwendungsbereich der Formvorschriften zählen grundsätzlich auch geschäftsähnliche Handlungen und nicht nur Willenserklärungen. Darauf weist die Formulierung „Aussteller der Erklärung" in § 126a BGB hin. [31]

In § 126a Abs. 3 BGB sind darüber hinaus zwei widerlegliche Vermutungsregeln enthalten: einmal die Vermutung der Zurechnung einer Willenserklärung zum Signaturschlüsselinhaber, zum anderen eine Sonderausprägung einer vermuteten Anscheins- bzw. Duldungsvollmacht.[32] Bei der Abgabe von elektronisch signierten Erklärungen durch Dritte die ein fremden privaten Schlüssel benutzen wird vermutet, dass der Dritte vom Inhaber des Schlüssels zur Abgabe der Erklärung bevollmächtigt war. Dem Grunde nach geht es hierbei um Vertrauensschutz bei Nicht-Vorliegen der erforderlichen Vollmacht und gleichzeitiger Unzumutbarkeit der Nachprüfung der Bevollmächtigung. Ein besonderes Vertrauen gründet das Gesetz allein auf ein tatsächliches Verhalten, wobei grundsätzlich die Gutgläubigkeit des Empfängers unterstellt wird. Dies wirft wiederum die Frage auf, wie dem Signaturschlüssel-Inhaber bei Missbrauchsfällen der Nachweis der Bösgläubigkeit gelingen soll. Damit wird dem Belasteten ein weiteres erhebliches Maß an Vorsorge abverlangt.[33]

Auch die Warnfunktion gem. § 6 Abs. 2 SigG soll von der elektronischen Signatur allein durch das zur Signierung notwendige Prozedere ausgefüllt werden können. Allerdings ist diese Funktion je nach der technischen Ausgestaltung erhöht oder gemindert. Wird bspw. die Signiersoftware als automatisch startendes Zusatzmodul in die einschlägigen E-Mail-Programme integriert, wird der Nutzer nach einiger Zeit kaum mehr daran denken, dass er einer handschriftlichen Unterzeichnung gleichzuachtende Vorgänge vornimmt.[34]

---

[30] Dauner-Lieb (Noack), § 126a, Rn 26, Müglich, MMR 2000, 11.

[31] Dauner-Lieb (Noack), § 126a, Rn 11.

[32] Müglich, MMR 2000, 10.

[33] Müglich, MMR 2000, 11.

[34] Dauner-Lieb (Noack), § 126a, Rn 9.

§ 126b BGB

Neu im deutschen Recht ist die „Textform" des § 126b BGB. Diese ist als Fixierung e iner Erklärung in lesbar zu machenden Zeichen zu verstehen.[35] Sie erfordert keine Verkörperung, keine eigenhändige Unterschrift und keine qualifizierte elektronische Signatur und steht somit unterhalb der hergebrachten Schriftform und der neuen elektronischen Form.

Akkreditierung

Bei den Zertifizierungsdiensteanbietern sind zwei Qualitätsstufen zu unterscheiden: sog. „angemeldete Zertifizierungsdienste" (§ 4 Abs. 3 Satz 1 SigG) und „freiwillig akkred itierte Zertifizierungsdienste" (§ 15 Abs. 1 Satz 1 SigG).

Die Zertifizierungsdiensteanbieter fungieren dabei als Garanten des Sicherheitssystems der elektronischen Signatur. Sie müssen bei der Vergabe des Zertifikats den Antragsteller zuverlässig identifizieren, Vorkehrungen treffen, damit die Daten für qualifizierte Zertifikate nicht unbemerkt gefälscht werden und außerdem gewährleisten, dass der Signaturschlüssel geheim gehalten wird.[36]

Dienstleister auf dem Gebiet der Zertifizierung bedürfen grds. keiner Genehmigung (§ 4 Abs. 1 SigG). Die Aufnahme der Tätigkeit ist nach entsprechender Anzeige bei der RegTP möglich. Dies stellt eine durch die Richtlinie im Gegensatz zum früher geltenden Signaturgesetz geänderte Lage dar. Nach § 1 Abs. 2 SigG galt dies bereits für das Angebot aller sonstiger Signaturverfahren (untere Stufe), gilt nun aber auch für das Angebot qualifizierter Signaturverfahren (mittlere Stufe).[37] Der Grundsatz der Anmeldung der Zertifizierungsdienste sieht allerdings auch Ausnahmen vor.

Dem Zertifizierungsdiensteanbieter steht es frei, den Betrieb seines Zertifizierungsdienstes nach § 4 Abs. 3 SigG nur anzuzeigen oder sich nach § 15 SigG akkreditieren zu lassen.[38] Aber nur wenn sich die Zertifizierungsdienste freiwillig einer umfassenden technischen und administrativen Sicherheitsprüfung unterzogen haben (=Akkreditierung), können sie Zertifikate für die qualifizierte elektronische Signatur ausstellen. Die Prü-

---

[35] Noack, DStR 2001, 1896.

[36] Geis, MMR 2000, 670.

[37] Roßnagel, MMR 2000, 452.

[38] Roßnagel, NJW 2001, 1821.

fung und Bestätigung sind nach sicherheitserheblichen Veränderungen sowie in regelmäßigen Zeitabständen zu wiederholen.

Akkreditierte Zertifizierungsdiensteanbieter erhalten ein Gütezeichen, § 15 Abs. 1 Satz 3 SigG. Mit diesem Gütezeichen wird der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen zum Ausdruck gebracht. Die so erteilten Signaturen können am Wurzelzertifikat der RegTP erkannt werden.[39] Die RegTP nimmt auch die allgemeine Missbrauchsaufsicht hinsichtlich der Einhaltung technischer Standards vor.[40]

Zu den akkreditierten Anbietern sog. "Trust Center" zählen:
- 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.de)
- die DATEV und eine Vielzahl von Steuerberater- und Rechtsanwaltskammern[41]

Seit Inkrafttreten des neuen Signaturgesetzes sind 13 Zertifizierungsstellen akkreditiert; drei weitere stehen kurz vor der Akkreditierung (Stand: März 2002).

Die "Trust Center“ können gem. § 4 Abs. 5 SigG wiederum mit Dritten, sog. „Unter-Trust-Centern“, zusammen arbeiten, indem sie Aufgaben an diese übertragen und sie in ihr Sicherheitskonzept einbinden. Für den Dritten haftet das „Trust Center“ nach § 11 Abs. 4 SigG ohne die Exkulpationsmöglichkeit des § 831 Abs. 1 Satz 2 BGB.[42] Auch für diese „Unter-Trust-Center“ übernimmt die RegTP die Funktion der Wurzel-Zertifizierungsstelle.

Unterschiede der Signaturverfahren

Akkreditierte unterscheiden sich von qualifizierten Signaturverfahren vor allem dadurch, dass nur akkreditierte Zertifizierungsdiensteanbieter vor der Betriebsaufnahme behördlich überprüft werden. Qualifizierte Verfahren verfügen hingegen nur über eine behauptete, nicht über eine nachgewiesene organisatorische Sicherheit.

---

[39] Roßnagel, MMR 2000, 454.

[40] Hoeren, Rechtsfragen im Internet, S. 232.

[41] Noack, DStR 2001, 1893.

[42] Roßnagel, NJW 2001, 1820.

Nur akkreditierte Signaturen sind langfristig, nämlich über 30 Jahre, online prüfbar. Im Konkurs des Zertifizierungsdiensteanbieters übernimmt die RegTP nach § 15 Abs. 4 SigG die Zertifikate und hält sie für die restliche Zeit vorrätig. Dagegen müssen bei qualifizierten Verfahren die Zertifikate nur für die Dauer ihrer Gültigkeit plus zwei Jahre aufbewahrt werden. Danach können sie vernichtet werden. Geht der Anbieter in Konkurs, können sie noch früher verloren gehen.[43]

Sicherheit

Sofern Dritte mit dem Willen des Signaturschlüsselinhabers tätig werden, liegt ein Handeln unter fremdem Namen vor, das für und gegen den Geschäftsherrn wirkt, so dass eine entsprechende Anwendung der §§ 164 ff BGB geboten ist.[44]

Datenschutz

Teilweise wird als problematisch angesehen, dass auch die Hinzufügung eines Wahlnamens (Pseudonyms) zu einer qualifizierten elektronischen Signatur möglich ist. Dementgegen hat aber bereits die Gesellschaft für Informatik darauf hingewiesen, dass pseudonymes Handeln als Möglichkeit des Datenschutzes zu fördern ist.[45] Voraussetzung hierfür ist allerdings, dass die als Aussteller in Betracht kommende Person erkennbar sein muss. In § 12 BGB kommt auch ein aufdeckbares Pseudonym als Name in Betracht.[46] Diese Aufdeckung ist bei einer qualifizierten elektronischen Signatur immer möglich, da das Zertifikat für bestimmte Person ausgestellt wird.

Daher sind Bedenken, dass das Namenserfordernis sich datenschutzfeindlich auswirken könnte, grundlos.[47]

Haftung der Zertifizierungsstellen

Der Gesetzgeber ist in §§ 11 und 12 SigG der Forderung nach einer spezialgesetzlichen Haftungsregelung für die Zertifizierungsstellen nachgekommen.[48] Den Zertifizierungsdienst trifft eine deliktische Verschuldenshaftung mit Umkehr der Beweislast. Er haftet

---

[43] Roßnagel, NJW 2001, 1823.

[44] Dauner-Lieb (Noack), § 126, Rn 26.

[45] Stellungnahme der Gesellschaft für Informatik, DuD 2001, 38.

[46] Roßnagel, NJW 2001, 1825.

[47] Dauner-Lieb (Noack), § 126a, Rn 13, Roßnagel, NJW 2001, 1825.

[48] vgl. hierzu Leier, MMR 2000, 13ff.

für Schäden, die durch eine fehlerhafte Zertifizierung entstehen. Zu denken ist hierbei an Fehler und Unregelmäßigkeiten bei der Ausgabe und Verwaltung von Signaturschlüssel-Zertifikaten etwa durch technische Defekte, betrügerische Manipulationen oder ein fahrlässiges Verhalten von Mitarbeitern der Zertifizierungsstelle.

In § 11 Abs. 2 SigG ist für die Fälle des nachweisbaren nicht schuldhaften Handelns eine Exkulpationsmöglichkeit für die Zertifizierungsdiensteanbieter vorgesehen. An die „im Verkehr erforderliche Sorgfalt" sind hier hohe Anforderungen zu stellen. [49] Auch ist hier noch einmal auf die bereits angesprochen Haftung für Dritte ohne Exkulpationsmöglichkeit gem. § 11 Abs. 4 SigG hinzuweisen.

Eine Haftungsbeschränkung ist ausschließlich über eine Verwendungsbeschränkung des Signaturschlüssels möglich, § 11 Abs. 3 SigG.

Zur Sicherstellung der Erfüllung der Haftungsverpflichtung sieht § 12 SigG eine geeignete Vorsorge zur Deckung der nach § 11 SigG ersatzpflichtigen Schäden vor. Die Mindestsumme beträgt jeweils 250.000 •. Die Deckungssumme ist nach § 4 Abs. 2 SigG Voraussetzung der Betriebsaufnahme und mit der Anmeldung nach § 4 Abs. 3 SigG nachzuweisen.

Prozessrecht

In den §§ 130a ZPO, 46b ArbGG, 108a SGG, 86a VwGO, 77a FGO wird die Verwendung einer elektronischen Form ermöglicht, vorbereitende Schriftsätze „sollen" mit qualifizierter elektronischer Signatur versehen werden.

Der Gesetzgeber hat darauf verzichtet, die Bestimmungen des Urkundenbeweises auf elektronische Dokumente entsprechend anzuwenden, sonder vielmehr ein eigenständiges Recht der Beweisführung mit elektronischen Dokumenten geschaffen. Dieses System enthält sowohl Elemente des Augenscheinsbeweises als auch des Urkundenbeweises und findet seine zentrale Regelung in einer in § 292a ZPO aufgestellten gesetzlichen Vermutung.[50]

Die elektronische Form ist als qualifizierte elektronische Signatur zwar der gesetzlichen Schriftform gleichgestellt worden, nicht aber der Privaturkunde des Zivilprozessrechts.

---

[49] Roßnagel, NJW 2001, 1823.

[50] Dästner, NJW 2001, 3469.

Für den E-Commerce ist entscheidend, dass damit das elektronische Dokument ein Objekt des Augenscheins ist, dessen Beweisqualität von der Qualität der elektronischen Signatur abhängig ist.[51] Der in § 371 Abs. 1 ZPO neu eingefügte Satz 2 unterstellt alle elektronischen Dokumente dem Augenscheinsbeweis, unabhängig davon, ob sie der elektronischen Form iSv § 126a BGB genügen oder nicht.

Die Vorlage eines unsignierten elektronischen Dokuments allerdings erbringt nur den Beweis dafür, dass ein solches Dokument existiert, nicht aber, von wem es stammt.[52]

Beweiswert von signierten elektronischen Dokumenten

§ 292a ZPO stellt eine Vermutungsregel zugunsten des Empfängers einer elektronischen Erklärung auf. Die Vorschrift geht von der Vermutung aus, dass das Dokument echt – im urkundenrechtlichen Sinne – ist, also tatsächlich von demjenigen herrührt, der darin als Aussteller angegeben ist, wenn eine dieser Person zugeordnete Signatur verwendet wurde.

Dem Absender ist jedoch die Möglichkeit der Exkulpation durch das Vorbringen und Beweisen von Tatsachen, die „ernstliche Zweifel" daran begründen, dass die Erklärung mit Willen des Signaturschlüssel-Inhabers abgegeben wurde, möglich. Diese Regelung stellt keine Beweislastumkehr dar, der Erklärende muss nicht beweisen, dass die Signatur nicht von ihm stammt, erforderlich ist nur das Erschüttern des gesetzlichen Anscheinsbeweises.[53]

Hier stellt sich nun aber das Problem der Haftung wegen eines fahrlässig verursachten Rechtsscheins.[54] Die Beweisfunktion eines Dokuments, das der elektronischen Form genügt, geht über die der eigenhändig unterzeichneten Urkunde hinaus.

---

[51] Geis, MMR 2000, 672; Zur Diskussion um die Gleichstellung des elektronischen Dokuments mit der Privaturkunde der ZPO vgl. Roßnagel, NJW 1998, 3315; zur Beweisqualität digital signierter Dokumente aktuell zusammenfassend: Jäger/Kussel, in: Hoeren/Schüngel (Hrsg.), Rechtsaspekte der digitalen Signatur, 1999, S. 175, 272 ff.

[52] Dästner, NJW 2001, 3469.

[53] Dauner-Lieb (Noack), § 126, Rn 27.

[54] eingehend: Dörner, AcP 202 (2002).

Übermittlung elektronischer Dokumente im gerichtlichen Verfahren

Nach der Rechtsprechung des BGH und der anderen Obersten Bundesgerichte entspricht die Bedeutung der Schriftform im Verfahrensrecht nicht derjenigen im materiellen Recht.

Zu differenzieren ist zunächst zwischen der Übermittlung eines Dokuments als Telekopie (=Telefax/Computerfax, § 130 Nr. 6 ZPO) einerseits, wobei auf den Übertragungsweg, nämlich die Übermittlung unter Nutzung des öffentlichen Telekommunikationsdienstes, abzustellen ist, und der Übermittlung von „Aufzeichnungen als elektronisches Dokument" (=E-Mails, § 130a ZPO) andererseits.[55] Diese Unterscheidung findet ihre Entsprechung im Zustellungsreformgesetz, das am 01.07.2002 in Kraft treten wird.

Gem. § 130a Abs. 1 Satz 2 ZPO „soll" eine E-Mail mit einer qualifizierten elektronischen Signatur versehen sein, also der elektronischen Form des § 126a BGB entsprechen. Trotz Bedenken der Länder gegen den Gesetzesentwurf ist es bei der Sollvorschrift geblieben, da andernfalls ein Auseinanderfallen der Formerfordernisse der §§ 130 und 130a ZPO die Folge gewesen wäre. Allerdings ist „soll" iSv § 130a ZPO genauso auszulegen, wie dies durch die gefestigte Rechtsprechung bereits in § 130 ZPO der Fall war, nämlich als zwingendes Erfordernis, wenn nicht die Beifügung der Unterschrift aus technischen Gründen ausgeschlossen ist.[56]

§ 130a Abs. 2 Satz 1 ZPO macht die Einreichung elektronischer Dokumente bei Gericht jedoch davon abhängig, dass die Bundes- oder Landesregierung diesen Übermittlungsweg für ihren jeweiligen Zuständigkeitsbereich freigegeben hat. Dies kann wiederum erst dann geschehen, wenn die Gerichte über eine entsprechende Ausstattung verfügen. Neben diesem Ausstattungsproblem ist die Frage des justizinternen Umgangs mit eingehenden elektronischen Dokumenten zu klären. Hierbei sind Probleme wie die Festlegung von Datei-Formaten oder die Entwicklung einer neuen Aktenordnung zu klären.[57]

Internationale Anwendung

Durch die Signaturrichtlinie werden alle qualifizierten elektronischen Signaturen in Europa gleichgestellt, egal aus welchem Mitgliedsstaat sie stammen (§ 23 SigG).

---

[55] Dästner, NJW 2001, 3470.

[56] Vgl. Zöller/Greger, ZPO, 22.Aufl. (2001), § 130 Rn 5; Musielak/Stadler, ZPO, 2.Aufl. (2000), § 129 Rn 8ff jew. m.w. Nachw.

[57] Dästner, NJW 2001, 3470.

Drittstaaten können ebenfalls einbezogen werden, indem Zertifizierungsstellen aus Drittstaaten sich in einem Mitgliedsstaat der EU akkreditieren lassen oder eine in einem Mitgliedsstaat niedergelassene Zertifizierungsstelle für eine Zertifizierungsstelle in einem Drittstaat einsteht oder entsprechende bilaterale oder multilaterale Vereinbarungen mit der EU getroffen werden.

Die amerikanische Lösung des E-Commerce entspricht der Philosophie des freien Marktes. Im Gegensatz zu der europäischen gesetzlich definierten Qualität der elektronischen Signatur, sind in den USA durch den „Electronic Signatures in Global and National Commerce Act" vom 08.06.2000 (in Kraft seit 01.10.2000) [58] elektronische Verträge mit schriftlichen Verträgen gleichgestellt. Die elektronische Signatur ist nicht gesetzlich definiert, sondern die Marktteilnehmer entscheiden über die Qualität der elektronischen Signatur.[59] Ein Public Key Infrastructure-System wird nicht verlangt[60], vielmehr ist das einzige Erfordernis einer elektronischen Signatur, dass die elektronische Form gespeichert wird und für spätere Zwecke reproduziert werden kann. Im internationalen E-Commerce bliebt somit die Wahl zwischen dem „offenen" amerikanischen System und dem „geschlossenen" europäischen System.

Ausblick

technische Weiterentwicklung

Es ist damit zu rechnen, dass in Zukunft zur sicheren und zweifelsfreien Identifikation der Nutzer digitaler Signaturen biometrische Verfahren anstelle von PINs und Passwörtern einsetzt werden. Der Vorteil dieser Verfahren liegt darin, dass die biometrischen Daten eindeutig einer Person zugeordnet werden können. Typischerweise fließen biometrische Daten nicht unmittelbar in eine Signatur ein, sondern werden zur Identifikation eines Benutzers gegenüber einem Signaturgerät verwendet.[61]

Außerdem ist bspw. die Verwendung eines Schreibpads, um das Dokument mit einer eigenhändigen Unterschrift zu versehen, denkbar.

---

[58] abrufbar unter der Website der American Bar Association: http://www.abanet.com.

[59] Geis, MMR 2000, 667.

[60] Geis, BB 2001, Heft 21, Die erste Seite.

[61] Teletrust Deutschland e.V., Trusted E-Commerce, S. 9.

Elektronische Gerichtsverfahren

Elektronischer Rechtsverkehr ist mehr als Kommunikation über das Internet. Dazu gehört letztlich auch die Ersetzung der Papierakte durch die elektronische Akte. Für eine Reihe von Verfahren, die die Gerichte in einem besonders hohen Maße beschäftigen, stellt der Verzicht auf Papier keine Utopie dar.[62] In ihnen erscheint eine Strukturierung und Formalisierung des Parteivortrags möglich, ohne dass dies zu einem Verlust an Information führt. So hat eine Arbeitsgruppe aus Richtern und Rechtsanwälten in Nordrhein-Westfalen im Rahmen einer Machbarkeitsstudie die Möglichkeit eines elektronischen Scheidungsverfahrens mit positivem Ergebnis geprüft.

Öffentliches Recht

Die gesetzliche Verwendung qualifizierter elektronischer Signaturen, in weiten Bereichen, namentlich im öffentlichen Recht steht zu erwarten. Nach dem Entwurf eines Gesetzes zur Änderung verwaltungsverfahrensrechtlicher Vorschriften[63] sollen im VwVfG als Alternative zur Schriftform die elektronische Form mit qualifizierter elektronischer Signatur[64] und der „elektronische Verwaltungsakt“ eingeführt werden. [65]

Gem. Art. 3 Abs. 7 der Richtlinie können die Mitgliedstaaten an die Verwendung elektronischer Signaturen in den öffentlich-rechtlichen Beziehungen zwischen Staat und Bürger zusätzliche Anforderungen stellen, solange diese objektiv, transparent, verhältnismäßig und nicht diskriminierend sind. Damit haben die Mitgliedstaaten die Möglichkeit, für das öffentliche Recht akkreditierte Zertifizierungsdienste vorzuschreiben.[66]

---

[62] Dästner, NJW 2001, 3471.

[63] http://www.bmi.bund.de/Anlage8126/Gesetzentwurf_als_PDF-Downoad.pdf.

[64] Metternich, GRUR 2001, 650.

[65] Noack, DStR 2001, 1893, Rosenbach, DVBl 2001, 332; Catrein, NWVBl 2001, 50; Groß, DÖV 2001, 159.

[66] Geis, MMR 2000, 669.

Literatur

- **Dästner**, Neue Formvorschriften im Prozessrecht; NJW 2001, 3469
- **Dauner-Lieb**, Das neue Schuldrecht; §§ 126, 126a BGB
- **Hoeren,** Rechtsfragen im Internet, S. 227-240
- **Geis**, Das neue Signaturgesetz: Die deutsche Sicherheitsordnung für den E-Commerce; http://www.ivo-geis.de/documents/neuessig.php.3
- **Geis**, Die elektronische Signatur: Eine internationale Architektur der Identifizierung im E-Commerce; MMR 2000, 667
- **Geis**, Elektronische Signatur: Sichere Kommunikation im E-Commerce; BB 2001, Heft 21, Die erste Seite
- **Kilian**, EG-Richtlinie über digitale Signaturen in Kraft; BB 2000, 733
- **Leier**, Haftung der Zertifizierungsstellen nach dem SigG; MMR 2000, 13
- **Metternich**; Rechtsfragen im Zusammenhang mit der elektronischen Anmeldung; GRUR 2001, 647
- **Miedbrodt/Mayer**, E-Commerce-Digitale Siganturen in der Praxis; MDR 2001, 432
- **Müglich**, Neue Formvorschriften für den E-Commerce – Zur Umsetzung der EU-Signaturrichtlinie in deutsches Recht; MMR 2000, 7
- **Noack**, Digitaler Rechtsverkehr: Elektronische Signatur, elektronische Form und Textform; DStR 2001, 1893
- **Oertel**, Elektronische Form und notarielle Aufgaben im elektronischen Rechtsverkehr; MMR 2001, 419
- **Rapp**, Rechtliche Rahmenbedingungen und Formqualität elektronischer Signaturen; München 2002
- **Redeker**, EU-Signaturrichtlinie und Umsetzungsbedarf im deutschen Recht; CR 2000, 455
- **Rosenbach**, Erläuterungen und Anmerkungen zum Entwurf eines Gesetzes zur Änderung des Verwaltungsverfahrensgesetzes; DVBl 2001, 332
- **Roßnagel**, Das neue Recht der elektronischen Signaturen – Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO; NJW 2001, 1817
- **Roßnagel**, Ein Kulturumbruch: Digitale Signaturen; BB 2000, Heft 10, Die erste Seite
- **Roßnagel**, Auf dem Weg zu neuen Signaturregelungen – Die Novellierungsentwürfe für SigG, BGB und ZPO; MMR 2000, 451
- **Scheffler/Dressel**, Vorschläge zur Änderung zivilrechtlicher Formvorschriften und ihre Bedeutung für den Wirtschaftszweig E-Commerce; CR 2000, 378
- **Schicker**, Die elektronische Signatur – Eine praktische Einführung; JurPC Web-Dok. 139/2001(http://www.jurpc.de)

- **Schröter**, Rechtssicherheit im elektronischen Geschäftsverkehr; WM 2000, 2134
- **Schulzki-Haddouti**, Markt- oder Staatsmacht – Streit um digitale Signaturen; c't 1999, Heft 1
- **Schulzki-Haddouti**, Digitale Übereinkunft – EU-Richtlinie zur digitalen Signatur verabschiedet; c't 1999, Heft 8
- **Schulzki-Haddouti**, Unterschriftsüberreif – Digitale Signaturen brauchen Anwendung; c't 1999, Heft 21
- **Schuppan**, eGovernment: von der Mode zur Modernisierung; LKV 2002, 105
- **Stellungnahme zum Gesetzentwurf** „Formvorschriften des Privatrechts"; DuD 2001, 38
- **Teletrust Deutschland e.V.**, Trusted E-Commerce (http://www.teletrust.de)
- **Tettenborn/Bender**, Rechtsrahmen für den elektronischen Geschäftsverkehr; BB 2001, Beilage 10
- **Weigel**, Klagen per E-Mail – Möglichkeiten und Grenzen der Vereinfachung des juristischen Schriftverkehrs; c't 2000, Heft 10