Beweiswürdigung elektronischer Dokumente im Zivilprozess

unter vergleichender Betrachtung

von qualifizierten elektrnonischen Signaturen nach dem

Sigaturgesetz

und dem Askemos-Verfahren

Rechtsanwalt
Markus Heinker
Dr. Fingerle Rechtsanwälte
Forststraße 2
04105 Leipzig

I. Inhaltsübersicht

II. Mission Statement

Vorliegend werden die Möglichkeiten zur Erstellung elektronischer Dokumente, die das Askemos-Verfahren bietet, auf ihren Beweiswert in einem zivilgerichtlichen Verfahren untersucht. Es wird geprüft, ob das Ziel, elektronische Dokumente zu erstellen, die hinsichtlich ihres Beweiswertes denen handschriftlich unterzeichneter Dokumente gleichwertig sind, mit dem Askemos-Verfahren zu erreichen ist.

III. Gang der Untersuchung

In einem ersten Schritt (unter IV.) werden die Grundzüge des Beweisrechts im Zivilprozess allgemein - also ohne Berücksichtigung der Besonderheiten, die sich nach dem Signaturgesetz ergeben - dargestellt.

In einem zweiten Schritt (unter V.) wird ein kurzer Überblick über die aktuelle Rechtslage gegeben, Im Mittelpunkt stehen dabei die Regelungen des Signaturgesetzes mit den drei Dokumentklassen und deren Anwendung in der Praxis.

Vor diesem Hintergrund werden dann in einem dritten Schritt (unter VI.) die allgemeinen Regeln der Beweiswürdigung unter Berücksichtigung der Erfahrungen mit dem Signaturgesetz auf das Askemos-Verfahren angewendet und zur Frage Stellung genommen, ob durch das Askemos-Verfahren unter Verwendung einfacher elektronischer Signaturen der Rechtsverkehr, insbesondere aber das Zivilgericht, in die Lage versetzt wird, die Authentizität (das Dokument stammt vom angegebenen Urheber bzw. angemeldetem Nutzer) und Integrität (das Dokument ist unverändert) eines elektronischen Dokuments als bewiesen betrachten zu können, ohne, dass es dazu der Hinzuziehung eines Sachverständigen bedarf.

Abschließend werden die Ergebnisse zusammengefasst (unter VII.) und die zentralen Aussagen in einer für pädagogische Zwecke brauchbaren Form aufbereitet (unter VIII.).

IV. Grundzüge der Beweiswürdigung im Zivilprozess

1. Beweisbedürftigkeit

Zunächst ist zu klären, unter welchen Umständen im Zivilprozess überhaupt Beweis zu erheben ist. Vorab sei dabei bemerkt, dass Beweis nur über Tatsachen erhoben werden kann.

Es gilt das Prinzip des Behauptens und Bestreitens, d. h. Tatsachen werden zunächst in den Prozess eingeführt indem sie behauptet werden. Dabei trägt jede Partei die Darlegungslast für die Tatsachen, die die von ihr gewünschte Rechtsfolge auslösen. Können vorgetragene Tatsachen die gewünschte Rechtsfolge nicht auslösen spricht man von „unschlüssigem Vortrag". Erst wenn die Gegenseite die behauptete Tatsache bestreitet wird sie beweisbedürftig. Ausnahmsweise bedürfen offenkundige Tatsachen gemäß § 291 ZPO keines Beweises. Offenkundig sind beispielsweise Entfernungsangaben oder der Lebenshaltungskostenindex, also jede Tatsache, die

> *„einer beliebig großen Anzahl von Menschen bekannt ist oder ohne weiteres zuverlässig wahrnehmbar ist"*[1]

Ist Beweis zu erheben geschieht dies durch ein förmliches Beweisverfahren. Dieses wird durch einen Beweisantrag der beweisbelasteten Partei und einen entsprechenden Beweisbeschluss des Gerichts eingeleitet.

Verzichtet die Gegenseite auf ein Bestreiten gilt die Tatsache als unstreitig bzw. zugestanden. Das Gericht hat sie dann seiner Entscheidung zugrunde zu legen, unabhängig davon, ob das Gericht die vorgetragene Tatsache für richtig hält. Dies ist Ausfluss des Grundsatzes der Herrschaft der Parteien über das Verfahren, einer der zentralen Maximen des Zivilprozesses.

2. Beweislast

Weiter ist die Frage zu klären, wer in einem Zivilprozess für welche Tatsachen den Beweis führen muss, wer die Beweislast trägt. Grundsätzlich gilt, dass jede Partei das beweisen muss,

[1] Thomas / Putzo § 291, Rn. 1

was ihr günstig ist [2]. Damit korrespondiert die Beweislast in der Regel mit der Darlegungslast. So muss der Kläger, der einen Anspruch geltend macht, alle Tatbestandsvoraussetzungen dieses Anspruchs beweisen. Beispielsweise muss ein Verkäufer, der im Prozess eine Kaufpreisforderung gegen einen Kunden geltend macht, beweisen, dass ein Kaufvertrag mit dem Kunden zustande gekommen ist, da sich regelmäßig erst aus diesem Vertrag eine Pflicht zur Kaufpreiszahlung ergibt. Ist dieser Vertragsschluss mittels elektronischen Dokuments erfolgt, obliegt dem Verkäufer der Beweis dafür, dass das Dokument authentisch und integer ist.

Will der Käufer gegen den Kaufpreisanspruch einwenden, er habe ein Zurückbehaltungsrecht, so obliegt ihm der Beweis dafür, dass die tatsächlichen Voraussetzungen des Zurückbehaltungsrecht vorliegen.

Neben diesen allgemeinen Beweislastregeln regelt der Gesetzgeber für bestimmte Einzelfälle die Beweislastverteilung ausdrücklich und abweichend. Er bedient sich dabei der „gesetzlichen Vermutung“. Beispielsweise stellt § 1006 BGB zugunsten des Besitzers einer beweglichen Sache die Vermutung auf, dass dieser Eigentümer ist. Gemäß § 292 ZPO ist diese Vermutung jedoch widerleglich, allerdings nur durch den Beweis des Gegenteils.

In bestimmten Bereichen hat auch die Rechtsprechung Beweislastregelungen aufgestellt, die bis hin zu einer Umkehr der Beweislast reichen. Ein klassisches Beispiel ist die Haftung des Arztes bei groben Behandlungsfehlern. Nach den allgemeinen Regeln hätte der geschädigte Patient zu beweisen, dass der Fehler des Arztes kausal ist für den eingetretenen Schaden. Diese Regel hat der Bundesgerichtshof (BGH) zum Zweck eines besseren Interessenausgleichs aufgehoben[3]. Danach muss nun der Arzt die Nichtursächlichkeit seines Fehlers beweisen.

Zum Problemkreis Beweislast gehört auch der Sonderfall des prima-facie-Beweis, des Beweises des ersten Anscheins. Bestimmte Zusammenhänge sind nach der Lebenserfahrung so typisch und häufig, dass man dem ersten Anschein nach auf eine bestimmte Ursache oder Wirkung schließen darf[4], es besteht eine „tatsächliche Vermutung“. Diese kehrt die Beweislast nicht vollständig um, zwingt aber die Gegenpartei die ernsthafte Möglichkeit einer anderen Ursache oder Wirkung zu beweisen, um so die tatsächliche Vermutung zu erschüttern.

[2] für viele (am Beispiel einer Internetauktion): LG Bonn, CR 2002, 293
[3] NJW 1995, 778
[4] BGH NJW 1986, 2829

3. Beweismaß

Grundsätzlich hat die beweisbelastete Partei den so genannten Vollbeweis gemäß § 286 ZPO zu erbringen. Dies bedeutet Herstellen der Überzeugung des Gerichts von der Richtigkeit der Tatsache. Er ist zu unterscheiden von der Glaubhaftmachung gemäß § 294 ZPO (etwa im einstweiligen Rechtschutz), bei der nur eine überwiegende Wahrscheinlichkeit gefordert wird.

Bei seiner Überzeugungsbildung lässt das Gesetz dem Gericht einen breiten Spielraum:

> *§ 286 I ZPO (Freie Beweiswürdigung)*
> *Das Gericht hat unter Berücksichtigung des gesamten Inhalts der Verhandlungen und des Ergebnisses einer etwaigen Beweisaufnahme nach freier Überzeugung zu entscheiden, ob eine tatsächliche Behauptung für wahr oder nicht wahr zu erachten sei. In dem Urteil sind die Gründe anzugeben, die für die richterliche Überzeugung leitend gewesen sind.*

Der BGH hat versucht diese allgemeine Formel zu präzisieren:

> *Hierfür genügt, da eine absolute Gewissheit nicht zu erreichen und jede Möglichkeit des Gegenteils nicht auszuschließen ist, ein für das praktische Leben brauchbarer Grad an Gewissheit[5] … ein für einen vernünftigen, die Lebensverhältnisse klar überschauenden Menschen so hoher Grad von Wahrscheinlichkeit, dass er den Zweifeln Schweigen gebietet ohne sie völlig auszuschließen[6].*

4. Beweismittel

Als Beweismittel kommen im Zivilprozess ausschließlich die so genannten Strengbeweismittel in Betracht:

Zeugen: Eine andere Person gibt eine eigene Wahrnehmung vom Beweisthema wieder.

Parteieinvernahme: Eine Partei gibt eine eigene Wahrnehmung vom Beweisthema wieder.

[5] NJW 93, 935
[6] NJW 00, 953

Augenschein: Der Richter überzeugt sich von einer Tatsache durch Ansicht.

Sachverständigengutachten: Ein Fachmann nimmt zum Beweisthema Stellung.

Urkunden: Eine verkörperte Gedankenerklärung mit Ausstellerangabe belegt die Abgabe einer Erklärung durch den Aussteller.

Dem Strengbeweis steht der so genannte Freibeweis gegenüber, der mit allen Mitteln geführt werden kann (etwa Telefonanruf des Richters). Er ist nur für Nebenfragen des Verfahrens zulässig.

V. Beweiswürdigung elektronischer Dokumente mit Signaturen nach dem Signaturgesetz

1. Signaturgesetz und die drei Qualitätsstufen elektronischer Signaturen

Das Signaturgesetz ist die Antwort des Gesetzgebers auf das Bedürfnis breiter Verkehrskreise nach elektronischen Dokumenten, die hinsichtlich Authentizität und Integrität denen herkömmlicher Urkunden gleichstehen oder diesen überlegen sind. Der Weg des Gesetzgebers ist die elektronische Signatur, ein System aus zwei Algorithmen, die sich in einer einmaligen Kombination zu einem Algorithmenpaar ergänzen. Dabei bleibt ein Algorithmus (gemeint ist der numerische Schlüssel) geheim, der andere ist öffentlich. Unter diesem kann der Inhaber des Algorithmus identifiziert werden[7].

Das Signaturgesetz unterscheidet drei Qualitätsstufen elektronischer Signaturen: die einfache, die fortgeschrittene und die qualifizierte elektronische Signatur.

a. (einfache) elektronische Signatur

Eine (einfache) elektronische Signatur sind nach § 2 Nr. 1 SigG alle Daten, die anderen Daten beigefügt sind und zur Authentifizierung dienen. Dazu gehören Daten aus biometrischen Verfahren genauso, wie die Namenswiedergabe oder eine Bilddatei, etwa mit der eingescanten Unterschrift[8].

b. fortgeschrittene elektronische Signatur

Bereits deutlich aufwändiger ist die fortgeschrittene elektronische Signatur. Nach § 2 Nr. 2 SigG muss zusätzlich zu den Anforderungen an (einfache) elektronische Signaturen noch weitere Voraussetzungen erfüllen: Sie muss ausschließlich dem Signaturinhaber zugeordnet sein und seine Identifizierung ermöglichen. Sie muss mit Mitteln erstellt sein, die der Signaturschlüsselinhaber unter seiner alleinigen Kontrolle halten kann. Und schließlich muss sie mit den Daten auf die sie sich bezieht so verknüpft sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

[7] Spindler/Schmitz/Geis, Seite 434
[8] Spindler/Schmitz/Geis, Seite 436

c. qualifizierte elektronische Signatur

Erst für die qualifizierte elektronische Signatur stellt das Gesetz nach § 2 Nr. 2 SigG Anforderungen auch an die Sicherheit der organisatorischen Prozesse, der Schlüsselverwaltung und der technischen Komponenten. Danach sind qualifizierte elektronische Signaturen fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen. Das sind nach § 2 Nr. 6 SigG elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigen. Diese Zertifikate werden nur von qualifizierten Zertifizierungsdiensten vergeben. Die Qualifizierung der Zertifizierungsdienste erfolgt durch Akkreditierung durch die Regulierungsbehörde oder durch Anzeige der Tätigkeit bei der Behörde. Ferner verlangt das Gesetz eine sichere Signaturerstellungseinheit.

Es müssen also bei qualifizierten elektronischen Signaturen solche unterschieden werden, die von einem akkreditierten Zertifizierungsdienst stammen und solche von einem „nur“ angezeigten Zertifizierungsdienst.

2. Beweiswert von elektronischen signierten Dokumenten im Zivilprozess

Hinsichtlich ihres Beweiswertes muss wieder zwischen den drei Qualitätsstufen von Signaturen unterschieden werden:

a. Einfache Signaturen

Elektronische Dokumente mit (einfacher) Signatur können im Prozess als Augenscheinsbeweisobjekt eingeführt werden:

> *§ 371 I ZPO (Beweis durch Augenschein)*
> *Der Beweis durch Augenschein wird durch Bezeichnung des Gegenstandes des Augenscheins und durch die Angabe der zu beweisenden Tatsachen angetreten. Ist ein elektronisches Dokument Gegenstand des Beweises, wird der Beweis durch Vorlegung oder Übermittlung der Datei angetreten.*

Der Beweiswert ist jedoch aufgrund der Möglichkeiten Authentizität und Integrität des Dokuments zu verfälschen gering. So haben zahlreiche Gerichte[9] (zumeist für die Abgabe von Geboten in Internet-Auktionen) entschieden, dass demjenigen, der sich auf ein (einfaches) elektronisches Dokument beruft, der Vollbeweis von Authentizität und Integrität obliegt. Beispielhaft ein Auszug aus der Begründung eines Urteils des LG Bonn[10]:

> *Grundsätzlich trägt jede Partei die Beweislast dafür, dass der Tatbestand der ihr günstigen Rechtsnorm erfüllt ist. Danach musste der Kläger hier das Zustandekommen eines Vertrages mit dem Beklagten, d.h. auch die Abgabe der vertragsbegründenden Willenserklärung durch diesen beweisen … Eine davon abweichende Verteilung der Beweislast aus Billigkeitsgesichtspunkten ist auch im Hinblick auf die dem Vertragsschluss zugrunde liegenden Gefahrenbereiche nicht geboten …*

Der erforderliche Vollbeweis ist durch Vorlegen der Datei oder eines Ausdrucks nicht erbracht. Beispielhaft ein Auszug aus der Begründung eines Urteils das AG Bonn[11]:

> *Es ist allgemein bekannt, dass E-Mail-Dateien manipulierbar sind. Selbst wenn die entsprechenden E-Mails grundsätzlich vom Beklagten abgesandt worden sein sollten, wäre es möglich, dass einzelne Worte oder einzelne Sätze dieser E-Mails von Dritten abgeändert worden sind. Soweit kann diesen vom Kläger vorgelegten E-Mail-Ausdrucken keinerlei Beweiswert beigemessen werden.*

b. fortgeschrittene Signatur

Dieselbe Problematik stellt sich bei fortgeschrittenen Signaturen. Zwar erlaubt die fortgeschrittene Signatur den Nachweis, dass bestimmte Angriffe gegen die Echtheit des Dokuments nicht zutreffen[12]. Jedoch muss derjenige, der sich auf das Dokument beruft den Nachweis führen, dass die Signatur technisch und organisatorisch sicher ist. Die dazu erforderlichen Informationen wird der in der Regel nicht haben und selbst, wenn sie vorliegen, bedarf es eines Sachverständigen, um eine entsprechende Einschätzung vorzunehmen.

[9] so auch LG Konstanz, CR 2002, 609 und OLG Köln, CR 2003, 55
[10] vom 07.08.2001, Az. 2 O 450/00
[11] vom 25.10.2001, Az. 3 C 193/01
[12] Roßnagel, Elektronische Dokumente als Beweismittel, NJW 2006, 806

c. qualifizierte Signatur

Erst die qualifizierte elektronische Signatur vermag diese Probleme zu überwinden. Allerdings auch nicht aus sich selbst heraus. Mit dem Justizkommunikationsgesetz[13] im Jahr 2005 und der Novelle des Signaturgesetzes hat der Gesetzgeber Beweiserleichterungen in Form der gesetzlichen Vermutung für elektronische Dokumente mit qualifizierter Signatur formuliert.

Dabei wird nach privaten (Abs. I) und öffentlichen (Abs. II) Dokumenten unterschieden.

> *§ 371a ZPO (Beweiskraft elektronischer Dokumente)*
> *(1) Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.*
> *(2) Auf elektronische Dokumente, die von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind (öffentliche elektronische Dokumente), finden die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Ist das Dokument mit einer qualifizierten elektronischen Signatur versehen, gilt § 437 entsprechend.*

> *§ 437 I ZPO Echtheit inländischer öffentlicher Urkunden*
> *Urkunden, die nach Form und Inhalt als von … einer mit öffentlichem Glauben versehenen Person* (u.a. Notar) *sich darstellen, haben die Vermutung der Echtheit für sich.*

Der Beweiswert öffentlicher und privater Urkunden unterscheidet sich damit folgendermaßen:

Zunächst erfasst die Beweiskraft bei privaten Dokumenten im Gegensatz zu öffentlichen nicht die Begleitumstände (Zeit und Ort usw.).

Ferner unterscheiden sich private und öffentliche Dokumente bezüglich des Maßes der

[13] BGBl I, Seite 837

Vermutung. Während qualifiziert signierte private Dokumente nur einen Anscheinsbeweis auf ihrer Seite haben, der bereits durch ernstliche Zweifel[14] erschüttert werden kann, streitet für öffentliche qualifiziert signierte Dokumente eine Vermutung der Echtheit (§ 437 ZPO), die nur noch durch den Beweis des Gegenteils (§ 292 ZPO) entkräftet werden kann.

Gemeinsam ist beide Urkundenarten, die formelle (äußere) Beweiskraft (Beweis, von Authentizität und Integrität). Beide Urkundenarten haben keine materielle (innere) Beweiskraft (Beweis, dass der Inhalt richtig ist).

Zu beachten ist, dass die Beweiserleichterungen eine erfolgreiche technische Prüfung der verwendeten Signatur mit einer nach §§ 17 II und 15 II SigG geprüften Prüfsoftware voraussetzen[15]. Ferner darf bei privaten Dokumenten der so erzeugte Anschein von der Gegenseite nicht erschüttert werden, etwa indem die Sicherheit des Zertifizierungsdiensteanbieters bestritten wird. Hier hilft § 15 I 4 SigG (nur) bei der Verwendung akkreditierter Signaturen mit einer weiteren gesetzlichen Vermutung[16]. Diese bezieht sich auf die im Akkreditierungsverfahren von der Bundesnetzagentur bestätigte technisch-organisatorische Sicherheit des Zertifizierungsdiensteanbieters. Diese Vermutung kann nicht mehr durch schlichtes Bestreiten der technisch-organisatorischen Sicherheit erfolgen, sondern bedarf des Vortrages von Tatsachen, die ernstliche Zweifel an der Sicherheit begründen[17].

Ein weiterer Problemkreis betrifft die Authentizität. Zwar vermag die Signatur zu beweisen - jedenfalls kraft gesetzlicher Beweiserleichterung -, dass die Erklärung in der vorliegenden Form mit dem entsprechenden Signaturschlüssel „gezeichnet“ wurde. Die Frage, ob der Schlüssel auch vom berechtigten Inhaber verwendet wurde ist jedenfalls solange ein Problem wie nicht durch biometrische Verfahren zusätzliche Sicherheit geschaffen ist.

Fraglich ist deshalb, wie mit dem Einwand, die Signatur sei missbräuchlich angebracht worden, umzugehen ist.

Die Rechtsprechung hat für den unbefugten Gebrauch von EC-Karten mit PIN schon einmal eine ähnliche Problematik entschieden[18]. Will man mit dem BGH davon ausgehen, dass es auch mit größtmöglichem finanziellem Aufwand ausgeschlossen ist, die PIN zu errechnen, so gelangt

[14] an die nach Roßnagel (NJW 2001, 1826) „keine hohen Anforderungen“ zu stellen sind
[15] Schemmann, ZZP 2005, 161
[16] Rossnagel, NJW 2001, 1817
[17] Roßnagel / Fischer-Dieskau, NJW 2006, 806

[18] NJW 2004, 3623

man konsequenterweise zu dem Ergebnis, dass der Einwand des EC-Karten-Besitzers, ihm sei die Karte abhanden gekommen und er habe die Nummer vertragsgemäß geheim gehalten ausgeschlossen ist. Die Tatsache, dass die Karte eingesetzt wurde lässt damit nur zwei Schlussfolgerungen zu: Entweder der berechtigte Inhaber hat selbst verfügt oder er hat die PIN nicht sorgfältig geheim gehalten. In beiden Fällen ist es sachgerecht den Nutzer der Karte dafür haften zu lassen. Eine Ausnahme will der BGH nur dann machen, wenn die Karte im zeitlichen und räumlichen Zusammenhang mit der Benutzung eines öffentlichen Terminals abhanden gekommen ist.

Jedoch setzt dies für die hier gegenständliche Problematik zu spät an[19]. Ließe man zu, durch die Behauptung eines Diebstahls des Signaturschlüssels als ultima-ratio, einen Quasi-Rücktritt vom Vertrag zu ermöglichen, wäre das System entwertet. Man wird also davon auszugehen haben, dass solange ein Diebstahl nicht bewiesen ist, die Signatur als vom rechtmäßigen Inhaber abgegeben zu gelten hat[20].

Eine Parallele zum Online-Banking mittels PIN und TAN kann nicht gezogen werden. Obwohl es bereits einige Schadensfälle beim Online-Banking gegeben hat, mangelt es an Rechtsprechung zu diesem Problemkreis. Ursache ist, dass es wohl Strategie der Banken ist, Präzedenzfälle zu vermeiden, indem eine außergerichtliche Einigung herbeigeführt wird[21]. Dies erlaubt zwar Spekulationen darüber, wie die Banken selbst die Sicherheit des Systems einschätzen, zur Rechtssicherheit trägt es jedoch nicht bei.

[19] zur Übertragbarkeit der EC-Karten-Rechtsprechung auf andere Verfahren Borges, NJW 2005, 3313
[20] so auch Roßnagel / Fischer-Dieskau, NJW 2006, 806
[21] Karper, DuD, 2006, 215

VI. Beweiswürdigung des Vertragsschluss nach dem Askemos-Verfahren

1. Intentionen

Mit dem Askemos-Verfahren soll der „klassische“ Weg des Vertragsschlusses durch wechselseitige Unterschrift unter Zuziehung eines Notars, in die moderne Kommunikationswelt transferiert werden, ohne, dass sich das in Jahrhunderten bewährte System technischen Gegebenheiten anpassen muss. Die Schwächen existierender Ansätze, wie unilateralen Signaturen und kryptografischen Systemen, sollen vermieden, die Schwächen des klassischen Weges verringert werden.

Dazu ersetzt das Askemos-Verfahren die herkömmliche elektronische Signatur durch eine multilateral abgestimmte, dynamische Signatur. Der entscheidende Unterschied besteht darin, dass die Dokumente nicht an einem Ort liegen und dort manipuliert oder vernichtet werden können, sondern verteilt gespeichert sind. Dies bietet zwei Vorteile: Zum einen ist das System deutlich unanfälliger für technische Ausfälle. Zum zweiten besteht ein wirksamer Schutz gegen Manipulationen. Mag einer (von vier) Speicherorten ausfallen oder manipuliert werden, es verbleibt eine unangetastete ¾-Mehrheit für die richtigen Daten. Durch Erhöhung der Anzahl der Speicherorte lässt sich die Sicherheit den praktischen Bedürfnissen anpassen.

2. Technischer Ablauf

Wollen zwei Parteien einen Vertrag nach dem Askemos-Verfahren schließen, so müssen sie sich zunächst auf mindestens vier Dienstleister (Provider) verständigen, die technisch und rechtlich voneinander unabhängig sind. Die Beteiligten (Parteien) müssen Benutzer eines Askemos-Netzwerkes (etwa fiXml) sein.

Zunächst muss eine Partei von den Providern identifiziert werden. Diese Authentifikation geschieht bei allen Providern unabhängig voneinander und im Idealfall nach unterschiedlichen Verfahren. Diese Verfahren sind nicht Teil des Askemos-Verfahrens.

Nun hinterlegt (speichert) eine Partei den Vertragstext (Angebot) bei allen Providern. Dies geschieht nach entsprechender Konfiguration durch einen einzigen Speicherbefehl automatisch. Bei diesem Vorgang werden dem eigentlichen Dokument Informationen (Metadaten) über den

Absender des Dokuments, die Speicherorte (Provider) und den Zeitpunkt der Hinterlegung beigefügt. Ferner wird über die Daten eine Prüfsumme gebildet (eindeutiger selbstverifizierender Identifikator, OID) und zu dem Dokument gespeichert.

Im nächsten Schritt erhält die andere Vertragspartei das Zugriffsrecht auf die bei den Providern abgelegten Daten. Sie prüft das Angebot und erklärt die Annahme indem sie ihrerseits ein Dokument bei den Providern mit der entsprechenden Erklärung nach dem oben beschriebenen Verfahren unter Bezugnahme auf das Angebot hinterlegt. Die Annahme ist mit dem Angebot verknüpft.

In einem gerichtlichen Verfahren kann Beweis über den Vertragsschluss mittels eines internetfähigen Computers und Askemos-Zugang erhoben werden. Zunächst wird Beweisantrag gestellt, indem dem Gericht der Identifikator (OID) der Annahme mitgeteilt und Zugriffsrechte darauf eingeräumt werden. Nun kann das Gericht seine Überzeugung von der Authentizität der Dokumente in Abhängigkeit vom Maß der Übereinstimmung der OID bilden.

3. Beweiswert Authentizität

Hinsichtlich der Authentizität stellt sich das Problem, dass die gesetzlichen Vermutungen zu den qualifizierten elektronischen Signaturen für diese Frage nicht greifen. Damit ist das Gericht bei der Würdigung des Sachverhaltes auf sich (bzw. seine Gutachter) gestellt.

Der Problemkreis der Authentizität muss zweigeteilt betrachtet werden. Zum einen geht es um die Frage, wie sicher ist die Zuordnung des Urhebers einer Erklärung zu dem abgelegten Dokument (a) und zum anderen um die Frage, wie sicher ist es, dass der Zugang zum System nicht missbräuchlich erfolgt (b).

a) Zuordnung Dokument - Urheber

Beim Askemos-Verfahren wird wie bei der qualifizierten elektronischen Signatur eine unauflösliche Verbindung zwischen dem Vertragstext und der Bezeichnung des Urhebers hergestellt. In Ermangelung eines öffentlichen Schlüssel-Verzeichnisses bedarf die Prüfung der Frage, ob der dann im Vertragstext bezeichnete Urheber auch derjenige ist, dem die (wie auch immer geartete) Zugangsidentität zugeordnet ist, einer Erklärung des jeweiligen Providers.

Soweit es die Verbindung zwischen Text und Urheberbezeichnung angeht besteht wegen der oben dargestellten Verfahrensweise kein Grund anzunehmen, die Wertung des Gesetzgebers bezüglich der qualifizierten elektronischen Signatur, könne nicht auch für das Askemos-Verfahren gelten. Wohlgemerkt besteht insoweit keine gesetzliche Beweiserleichterung. Das Gericht hat nur die Möglichkeit sich durch sachverständige Beratung von dem gleichwertigen Sicherheitsniveau zu überzeugen und entsprechend zu urteilen.

Praktisch problematisch ist die Beweiserhebung über die Zuordnung des mit dem Dokument genannten Urhebers zu der Zugangsidentität. Soweit ersichtlich, muss diese durch Zeugnis des Providers bewiesen werden, was angesichts von mindestens vier beteiligten Providern - selbst bei einer schriftlichen Befragung (§ 377 III ZPO) - einen unwirtschaftlichen Aufwand bedeuten dürfte.

b) Zuordnung Nutzer - Zugangsdaten

Den Problemkreis missbräuchliche Verwendung der Zugangsdaten teilt das Askemos-Verfahren mit der qualifizierten elektronischen Signatur. Insoweit kann auf die oben gemachten Ausführungen, insbesondere zur BGH-Rechtsprechung zur EC-Karte mit PIN, verwiesen werden[22].

Für die hier gegenständliche Fragestellung geht es jedoch nicht primär um die Haftungsverteilung zwischen zwei Parteien, sondern um, die Frage, ob durch den Einwand, das Identifizierungsverfahren sei „geknackt“ worden, die Tür zu einem Quasi-Rücktritt geöffnet werden darf. Die Rechtsprechung zur EC-Karte kann deshalb nicht direkt übertragen werden.

Beim Askemos-Verfahren ist vorbehaltlich der technischen Ausgestaltung im Einzelnen wohl davon auszugehen, dass die zu verwendenden Identifizierungsverfahren das gleiche Sicherheitsniveau aufweisen werden wie die EC-Karte mit PIN. Hinzu kommt ein zusätzlicher erheblicher Sicherheitsgewinn durch das Erfordernis der mehrfachen Anmeldung. Erfolgt die praktische Ausgestaltung entsprechend, dürfte sich eine erhebliche Erhöhung des Sicherheitsniveaus ergeben, die es „mit einem für das praktische Leben brauchbaren Grad an Gewissheit“ ausschließt, dass die Verfahren zugleich „geknackt“ werden. Zu berücksichtigen ist ferner, dass das Askemos-Verfahren einen Verlaufsspeicher beinhaltet, der die jederzeitige -

[22] siehe V. 2. c.

auch nachträgliche - Transparenz jeder einzelnen Aktion sicherstellt. Diese Umstände rechtfertigen es, anzunehmen, dass der Beweis des ersten Anscheins für eine Nutzung des Systems durch den berechtigten Verwender besteht[23], jedenfalls solange die Prüfung des OID entsprechend ausfällt.

Allerdings muss wiederum davon ausgegangen werden, dass die Gerichte diese Frage nicht aus eigener Sachkunde entscheiden, sondern regelmäßig Sachverständige hinzuziehen werden. Erst nach Bestehen einer entsprechenden, gefestigten höchstrichterlichen Rechtsprechung ist es denkbar, dass es Gerichte wagen ohne Sachverständige zu entscheiden. Wegen ihrer Dynamik dürften die technischen Entwicklungen die Rechtsprechung in diesen Fragen jedoch immer wieder überholen.

An dieser Stelle ist ausdrücklich darauf hinzuweisen, dass die Rechtsprechung sich zu diesem Themenkreis noch im Fluss befindet, insbesondere, dass die letztinstanzlichen Gerichte zu dieser Frage - auch hinsichtlich qualifizierter elektronischer Signaturen - noch nicht abschließend Stellung genommen haben und damit auch krasse Kurswechsel möglich sind.

Damit bliebe schließlich die Möglichkeit, beide angesprochenen Problemkreise einer gesetzlichen Regelung zuzuführen. Hierüber kann jedoch nur spekuliert werden.

4. Beweiswert Integrität

Der Gesetzgeber hat sich mit dem Signaturgesetz für einen Weg entschieden, den elektronischen Rechtsverkehr zu fördern, der bestimmte, zum Teil als willkürlich empfundene Grundentscheidungen beinhaltet. Dies drückt sich auch in den Verbindungen ins Zivilprozessrecht aus. Die Beweiserleichterungen des § 371a ZPO gelten - für die hier vor allem interessierenden privaten Dokumente - ausdrücklich nur für solche mit qualifizierter elektronischer Signatur. Selbst die nahe liegende Möglichkeit, diesen Tatbestand zu öffnen, indem etwa die Formulierung „und ihnen gleichwertige Verfahren“ angefügt wird, wurde unterlassen. So wäre es ohne weiteres möglich gewesen, jedenfalls im Zivilprozessrecht, auch andere gleichwertige Verfahren an den Beweiserleichterungen teilnehmen zu lassen. Dies ist jedoch unterblieben, weshalb nochmals zu konstatieren ist: Das Asekmos-Verfahren wird von den Beweiserleichterungen nicht erfasst.

[23] vgl. auch Roßnagel / Fischer-Dieskau, NJW 2006, 806

Im Zuge der Verbreitung des Verfahrens obläge damit - wie oben dargestellt - den Gerichten die Bewertung mit der damit verbundenen Inanspruchnahme von Gutachtern.

Im Vergleich mit der qualifizierten elektronischen Signatur darf wohl davon ausgegangen werden, dass die Integrität, die die qualifizierte elektronische Signatur durch die Verknüpfung des Textes mit den Signaturdaten erhält, mindestens der entspricht, die die Bildung des OID beim Askemos-Verfahren gewährleisten kann. Dies ist letztlich jedoch eine technische Frage. Entscheidend ist aber, dass durch das Prinzip der verteilten Speicherung und des Verlaufsspeichers ein massiver Sicherheitsgewinn entsteht, den die Gerichte werden zu würdigen haben.

Aufgrund der Sicherheitsvermutung die zugunsten qualifizierter elektronischer Signaturen besteht, kommen die Gerichte nicht in die Lage, die qualifizierte elektronische Signatur ohne diese Stütze zu bewerten. Deshalb fehlt es an einer Parallele aus der gerichtlichen Praxis, die die hier zu treffende Einschätzung absichern könnte.

Jedoch verdeutlicht die Parallele zur „nicht-elektronischen Welt“ den Grad des Zugewinns. Das Gesetz billigt bereits der einzelnen (herkömmlichen) Privaturkunde Beweiskraft zu, s.o. Der Eindruck der Integrität wird in der Regel gesteigert, wenn (allerdings in der forensischen Praxis untypisch) beide Seiten übereinstimmende Dokumente vorlegen. Ist - wie beim Askemos-Verfahren - die Integrität vierfach oder zumindest mehrheitlich belegt, kann für das sachverständig beratene Gericht wohl kein vernünftiger Zweifel daran bestehen, dass die Wertungen des Gesetzgebers zur herkömmlichen Urkunde auf sie zu übertragen sind.

Eine weitere Überlegung erhärtet diese Einschätzung. § 371 II ZPO (s. o.) spricht aus, dass die öffentliche elektronische Urkunde bereits ohne qualifizierte elektronische Signatur an den gesetzlichen Beweiserleichterungen teilnimmt. Grund dieser Privilegierung ist die Annahme, dass durch die Beteiligung der genannten Stellen von einer erhöhten Zuverlässigkeit ausgegangen werden kann. Überträgt man die ratio legis nun auf das Askemos-Verfahren findet sich ein weiterer Anhaltspunkt dafür, von einem erhöhten Beweiswert auszugehen. Denn anders als viele Dokumente, aus denen im Prozess Rechte abgeleitet werden sollen, befinden sich die Askemos-Dokumente in den Händen von unabhängigen Dritten. Nun kann deren Vertrauenswürdigkeit sicher nicht mit Behörden oder Notaren verglichen werden. Eine Verbesserung des Sicherheitsniveaus wird aber auch durch sie sichergestellt und rechtfertigt ein weiteres mal die Annahme jedenfalls eines Anscheinsbeweises für die Integrität des Askemos-Dokuments.

VII. Zusammenfassung

Das Askemos-Verfahren überträgt die herkömmlichen Wege des Vertragsschlusses auf die elektronische Kommunikation.

Dabei gelingt es hinsichtlich des Beweiswertes teilweise gegenüber der qualifizierten elektronischen Signatur und dem herkömmlichen Verfahren Verbesserungen zu erreichen.

Hinsichtlich der Identifizierung des Nutzers teilt das Askemos-Verfahren naturgemäß die Probleme der qualifizierten elektronischen Signatur, weil es dazu keinen eigenen Ansatz verfolgt. Allerdings führt die Vervierfachung der Identifizierung, zumal bei der Verwendung unterschiedlicher Verfahren, zu einem erhöhten Maß an Sicherheit, weshalb die Annahme - zumindest eines Anscheinsbeweises - gerechtfertigt erscheint.

Hinsichtlich der weiteren Aspekte der Authentizität und Integrität des Dokuments führt die Verwendung des OID und das Prinzip der verteilten Speicherung zu einem Sicherheitsniveau, dass es den Gerichten erlauben dürfte, von der Authentizität und Integrität des Dokuments im Wege des Anscheinsbeweises auszugehen, jedenfalls soweit die oben beschriebenen, technischen, organisatorischen und rechtlichen Rahmenbedingungen bestehen.

Jedoch ist nicht zu erwarten, dass Gerichte, die komplizierten technischen Abläufe im Hintergrund, aus eigener Sachkunde beurteilen werden. Insofern ist für einen längeren Zeitraum davon auszugehen, dass die Beweiserhebung und -würdigung nicht ohne sachverständige Beratung des Gerichts erfolgten wird.

Schließlich ist festzuhalten, dass in der forensischen Praxis das Askemos-Verfahren vor allem dadurch benachteiligt ist, dass die gesetzlichen Beweiserleichterungen - jedenfalls für Privaturkunden - nur den qualifiziert elektronisch signierten Dokumenten zugute kommen. Gründe für diese Entscheidung des Gesetzgebers sind nicht ersichtlich.

VIII. Pädagogische Aufbereitung

Nachfolgend sind die zentralen Aussagen in sieben Übersichten zusammengefasst.

Übersicht 1

Grundfragen des Beweisrechts

- Beweisbedürftigkeit

  Wann muss Beweis erhoben werden?

  Beweislast

  Wer muss den Beweis erbringen?

- Beweismaß

  Wann kann eine Tatsache als bewiesen gelten?

- Beweismittel

  Welche Methoden stehen zur Beweisführung zur Verfügung?

Übersicht 2

Beweisbedürftigkeit

- Zunächst behauptet der Kläger Tatsachen, die den Tatbestand der von ihm gewünschten Rechtsfolge ausfüllt. Er trägt die Darlegungslast.

  Beispiel:
  - Tatsache: Abgabe von Willenserklärungen
  - gewünschte Rechtsfolge: Vertragsschluss (§§ 145ff BGB) und damit Pflicht zur Kaufpreiszahlung (§ 433 II BGB)

- Bestreitet der Beklagte die Tatsache, muss Beweis erhoben werden.

- Andernfalls gilt die Tatsache als zugestanden bzw. unstreitig.

- Vermag die behauptete Tatsache die gewünschte Rechtsfolge nicht herbeizuführen ist der Vortrag unschlüssig.

- Ausnahmsweise ist die Erhebung des Beweises unnötig, wenn die Tatsache offenkundig ist.

Übersicht 3

Beweislast

- Jede Partei muss das beweisen, was ihr günstig ist

  In der Regel:
  - der Kläger: Tatsachen, die den Tatbestand des Anspruchs ausfüllen
  - der Beklagte: Tatschen, die den Tatbestand von Einwendungen ausfüllen
  -

- Es sei denn: Gesetzliche Vermutung

  Beispiel:
  § 1006 BGB: „Zu Zugunsten des Besitzers einer beweglichen Sache wird vermutet, dass er Eigentümer der Sache sei."

  nur durch Beweis des Gegenteils zu widerlegen

- Es sei denn: Beweislastumkehr

  Beispiel:
  BGH zur Arzthaftung: Bei groben Behandlungsfehlern muss der Arzt beweisen, dass sein Behandlungsfehler für einen Schaden beim Patienten nicht ursächlich war

- Es sei denn: Anscheinsbeweis (tatsächliche Vermutung)

  Ein bestimmter Zusammenhang ist nach der Lebenserfahrung so typisch und häufig, dass man auf eine bestimmte Wirkung schließen darf

  bereits durch Erschütterung des Anscheins zu widerlegen

Übersicht 4

Beweismaß

o Vollbeweis, § 286 ZPO

Grundsätzlich ist die volle Überzeugung des Gerichts von der Richtigkeit der Tatsache zu beweisenden herzustellen.

o Glaubhaftmachung, § 294 ZPO

Vor allem im einstweiligen Rechtschutz genügt die überwiegende Wahrscheinlichkeit

Übersicht 5

Beweismittel

o Strengbeweismittel (Regelfall)

- Zeugen
  Eine andere Person gibt eine eigene Wahrnehmung vom Beweisthema wieder.

- Parteieinvernahme
  Eine Partei gibt eine eigene Wahrnehmung vom Beweisthema wieder.

- Augenschein
  Der Richter überzeugt sich von einer Tatsache durch Ansicht.

- Sachverständigengutachten
  Ein Fachmann nimmt zum Beweisthema Stellung.

- Urkunden
  Eine verkörperte Gedankenerklärung mit Ausstellerangabe belegt die Abgabe einer Erklärung durch den Aussteller.

o Freibeweis (für “unwesentliche” Verfahrensfragen)

Übersicht 6

Beweiswert von elektronischen Signaturen

- o privates Dokument mit *(einfacher) Signatur*:
  als Augenscheinsobjekt im Prozess zulässig, aber in der gerichtlichen Praxis ohne Beweiswert

- o Dokument mit fortgeschrittener Signatur:
  wie Dokument mit einfacher Signatur

- o privates Dokument mit *qualifizierter Signatur*:
  gemäß § 371a I ZPO Nachweis von Authentizität und Integrität kraft Anscheins, der durch ernstliche Zweifel widerlegt werden kann

- o öffentliches Dokument mit *qualifizierter Signatur*:
  gemäß §§ 371a II, 437 ZPO Nachweis von Authentizität und Integrität kraft gesetzlicher Vermutung, die nur durch den Beweis des Gegenteils zu widerlegen ist.

Übersicht 7

Beweiswert von Askemos-Dokumenten

Erheblicher Sicherheitsgewinn gegenüber qualifizierter elektronischer Signatur durch:

- verteilte Speicherung
- Verlaufsspeicher
- OID
- vierfache Anmeldung
- ggf. unterschiedliche Anmeldeverfahren

deshalb

Gerichtliche Anerkennung zu erwarten

aber

Keine Anwendung der gesetzlichen Beweiserleichterungen

deshalb

Urteilsfindung ohne Sachverständigengutachten in absehbarer Zeit nicht zu erwarten

IX. Literaturverzeichnis

Balzer, Beweisaufnahme und Beweiswürdigung im Zivilprozess, Erich Schmidt, 2001

Baumbach / Lauterbach / Albers / Hartmann, ZPO-Kommentar, C.H. Beck, 65. Auflage, 2007

Becker, Elektronische Dokumente als Beweismittel im Zivilprozess, Peter Lang, 2003

Bieser / Kersten, Elektronisch unterschreiben, Hüthig, 2. Auflage, 1999

Britz, Urkundenbeweisrecht und Elektrotechnologie, C.H. Beck, 1996

Gounalakis, Rechtshandbuch Electronic Business, C.H. Beck, 2003

Koch, Internet-Recht, Oldenbourg, 2. Auflage, 2005

Schellhammer, Zivilprozess, C.F. Müller, 11. Auflage, 2004

Sigrun / Erber-Faller, Elektronischer Rechtsverkehr, Luchterhand, 2000

Spindler / Schmitz / Geis, Teledienstegesetz, C.H. Beck, 2004

Thomas / Putzo, Kommentar zur Zivilprozessordnung, C.H. Beck, 27. Auflage, 2005

Zeitschrift, CR, Computer und Recht, Verlag Schmidt

Zeitschrift, DSB, Datenschutzberater, Verlag Handelsblatt

Zeitschrift, DuD, Datenschutz und Datensicherung, Verlag Vieweg

Zeitschrift, JuS, Juristische Schulung, Verlag C.H. Beck

Zeitschrift, NJW, Neue Juristische Wochenschrift, Verlag C.H. Beck

Zeitschrift, ZZP, Zeitschrift für Zivilprozess, Verlag Heymann