Die elektronische Signatur und das deutsche Signaturgesetz

Steffen Wettig, Ref. jur.
wettig@informatik.uni-jena.de

Lehrstuhl für Rechnerarchitektur und –kommunikation
Friedrich-Schiller-Universität Jena
07740 Jena

Betreuer der Arbeit: Prof. Dr. Eberhard Zehendner, P.D. Dr. Stefan Storr
Art der Arbeit: Seminararbeit
Fachbereich GI: Sicherheit

Zusammenfassung

Die Informationsübermittlung über das Internet hat heutzutage eine erhebliche Bedeutung. Dabei kann es sich um E-Mail, Telefongespräche, Videokonferenzen, medizinische Daten, Bank - bzw. Firmendaten und vieles mehr handeln. Für den „elektronischen Handel“ wie überhaupt für jede rechtsverbindliche Kommunikation über das Netz wird es von entscheidender Bedeutung sein, die Abgabe von Willenserklärungen beweisen zu können. Elektronische Signaturen, vergleichbar der natürlichen Unterschrift, können für Verträge bedeuten, dass diese ohne Einbuße an Beweissicherheit geschlossen werden können. [1] Dazu sind jedoch sowohl technische Vorkehrungen (Kryptographie), als auch rechtliche Regelungen (z.B. Signaturgesetz) erforderlich, die dem Stand der Technik entsprechen.

I. Einleitung

Für rechtlich relevantes Handeln in offenen Datennetzen sind folgende Punkte wichtig:
Geheimhaltung/Vertraulichkeit: Nur befugte Personen sollen den Inhalt eines Dokuments lesen können.
Datenintegrität: Der Inhalt eines Dokuments soll nicht unbemerkt verändert werden können.
Authentifizierung: Der Urheber eines Dokuments soll klar sein; kein anderer soll sich als Urheber ausgeben können.
Verbindlichkeit: Der Urheber eines Dokuments soll seine Urheberschaft nicht abstreiten können.
Ein weiteres Ziel ist in manchen Situationen **Anonymität**, also die Vertraulichkeit des Kommunikationsvorgangs.

Eine Lösung für die sich ergebenden Problemfelder und Angriffsszenarien bietet die Kryptographie. Mit Hilfe von mathematischen Verfahren können Informationen verschlüsselt oder elektronisch signiert werden. Während es bei der Verschlüsselung darauf ankommt, dass kein Unbefugter die Nachricht lesen kann, ist Ziel der elektronischen Signatur, dass ein signiertes Dokument nicht mehr verändert werden kann, ohne dass man dies bemerkt. Bei der Signatur kommt es also darauf an, ein elektronisches Dokument einer bestimmten Person rechtsverbindlich zuordnen zu können. Den Unterschied zwischen beiden Systemen kann man sich folgendermaßen verdeutlichen:
Bei der **Verschlüsselung** wird das Dokument in einen verschließbaren Aktenkoffer gelegt und nur derjenige kann den Inhalt des Dokumentes lesen oder verändern, der den Schlüssel zu diesem Aktenkoffer besitzt.
Bei der **elektronischen Signatur** wird das Dokument zwar auch in einen solchen Aktenkoffer gelegt, aber dieser besteht jetzt aus Glas. Jeder kann von außen in das Dokument einsehen, aber keiner kann daran etwas verändern, ohne den Aktenkoffer zu beschädigen.
Man kann diese beiden Absichten natürlich auch kombinieren, indem man den gläsernen Aktenkoffer für die Signatur in einen undurchsichtigen Aktenkoffer einschließt. Nur der Empfänger kann ihn öffnen und den Inhalt einsehen. Er kann aber nicht unbemerkt etwas an dem signierten Dokument ändern, da er den gläsernen Koffer nicht öffnen kann.

Es dürfte daher nicht übertrieben sein, die Kryptographie als Schlüsseltechnologie für die Entwicklung des Internet und der Informationsgesellschaft zu bezeichnen.

II. Technische Grundlagen

Da es aus rechtlicher Sicht hauptsächlich um Beweisbarkeit des Inhalts und Zuordnung eines Dokuments zu einer Person geht, soll hier nur etwas näher auf die elektronische Signatur eingegangen werden.
Technisch funktioniert diese mit zwei unterschiedlichen mathematischen Methoden. Zum einen benötigt man Hashfunktionen und zum anderen sog. asymmetrische Kryptoverfahren. Mit den **Hashfunktionen**, auch Einwegfunktionen genannt, berechnet man aus der Nachricht einen vergleichsweise kleinen Datenblock, den Hashwert. Die Funktion wirkt wie eine Art Trichter. Am Ende ergibt sich daraus ein Wert, der von der eingegebenen Nachricht abhängt. Ändert sich nur ein Zeichen der Nachricht, ändert dies auch der dazugehörige Hashwert. Der Hashwert stellt somit eine Art Fingerabdruck der Nachricht dar. Die **asymmetrischen Kryptoverfahren** beruhen darauf, dass es einen öffentlichen und einen geheimen Schlüssel gibt (public key und secret key). Nachrichten, die mit dem secret key verschlüsselt werden, können nur mit dem public key entschlüsselt werden. Die verwendeten Schlüssel sollten so komplex sein, dass es kaum möglich ist aus dem öffentlichen Schlüssel den geheimen Schlüssel zu berechnen.

Die elektronische Signatur funktioniert nun folgendermaßen: Will der Sender eine Nachricht als von ihm erstellt ausweisen ("unterzeichnen"), so berechnet er den Hashwert der Nachricht und verschlüsselt diesen mit seinem privaten Signaturschlüssel (er „signiert“ also den Hashwert). Da nur er im Besitz dieses privaten Signaturschlüssels ist (z.B. gespeichert auf einer Smartcard), kann dies auch kein anderer. Jeder Empfänger, der sich den zugehörigen öffentlich verfügbaren Prüfschlüssel beschafft, kann nun die Echtheit der Nachricht überprüfen, sie somit verifizieren.

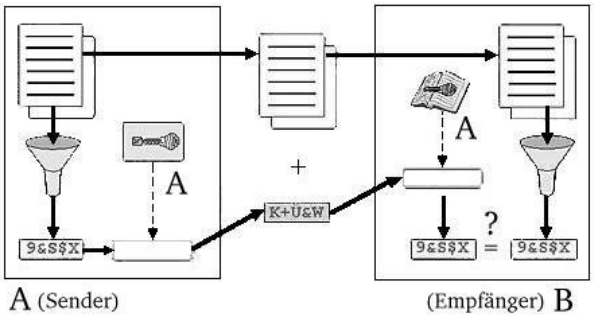

Abbildung: Signatur und Überprüfung der Signatur (ohne Datenverschlüsselung)[1]

Integrität, Authentifikation und Verbindlichkeit (also drei der oben genannten vier Punkte) können somit realisiert werden. Solchermaßen authentifizierte Nachrichten ähneln in ihren Eigenschaften unterschriebenen Schriftstücken, weshalb in diesem Zusammenhang auch von **digitalen bzw. elektronischen Signaturen**[2] die Rede ist. [6] Der Begriff der Signatur ist in diesem Zusammenhang möglicherweise etwas irreführend, da man ja nicht wie bei der „normalen“ Unterschrift etwas unterzeichnet. Vielmehr stellt die Signatur eher ein „elektronisches Siegel“ dar.

Bisher ist es so jedoch möglich die Identität einer anderen Person vorzutäuschen, indem z.B. Z ein Schlüsselpaar erstellt und den public key unter dem Namen des A veröffentlicht. Jeder der diesen für den echten Schlüssel des A hält, würde somit Z für A halten. Auch könnte z.B. A, der einen Vertrag wirklich unterschrieben hat, im Nachhinein vorgeben, dass dies überhaupt nicht sein öffentlicher Schlüssel sei. In sozialen Strukturen wird das Problem des Vortäuschens einer anderen Identität dadurch gelöst, dass ein vertrauenswürdiger Dritter eingeschaltet wird, der sich für die Identität einer Person verbürgt. Dies kann z. B. ein Freund oder Bekannter, eine Organisation, ein Wirtschaftsunternehmen oder eine staatliche Stelle[3] sein. Dieses „Verbürgen“ lässt sich mit Hilfe digitaler Signaturen auch im Rahmen kryptographischer Systeme realisieren. [4; 6] Der vertrauenswürdige Dritte unterzeichnet eine Nachricht, in der er zusichert, dass ein bestimmter öffentlicher Schlüssel zu der bezeichneten natürlichen Person gehört. Jeder, der dem Dritten vertraut und diese Unterschrift liest, kann sich sicher sein, dass eine zu dem genannten Prüfschlüssel passende Nachricht tatsächlich von dieser Person unterzeichnet wurde. Bei dem vertrauenswürdigen Dritten spricht man von einer Zertifizierungsinstanz (teilw. auch Trustcenter, Trusted Third Party oder Certification Authority). Die Zusicherung des Dritten wird Zertifikat genannt. Es kommt also einzig und allein darauf an, dass ein Benutzer eine Zertifizierungsinstanz finden kann, die sowohl er als auch sein Kommunikationspartner für vertrauenswürdig hält.

III. Rechtliche Grundlagen: Das Signaturgesetz

Es stellt sich die Frage, inwieweit die elektronische Signatur als Äquivalent zur natürlichen Unterschrift behandelt werden kann. Grundsätzlich kann ein Vertrag formfrei, d.h. auch mündlich geschlossen werden. Nur in besonders gesetzlich festgelegten Fällen ist eine bestimmte Form, z.B. Schriftform für die Wirksamkeit des Vertrages Voraussetzung. Andernfalls legen die Vertragspartner teilweise selbst Wert darauf, den Vertrag schriftlich abzuschließen, um eine bessere Beweisbarkeit des Vertragsinhalts gewährleisten zu können. Die gesetzliche Schriftform wird überall dort eingesetzt, wo der Gesetzgeber eine Urkunde als Dokumentation eines Vorgangs vorsieht. Bei der gesetzlichen Schriftform, muss der Text von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden (§126 Abs. I BGB). Die gesetzliche Schriftform wird im deutschen Recht bei den verschiedensten Willenserklärungen gefordert (z.B. Verbraucherkreditverträge und Ratenkreditgeschäfte §492 Abs. I S.1, 2 BGB, Quittungen §368 BGB und Bürgschaftserklärungen §766 BGB).

Um die elektronische Signatur mit der natürlichen Unterschrift vergleichen zu können, muss man sich die Funktionen der natürlichen Unterschrift vor Augen führen [7; 9]:
Echtheitseigenschaft: Das Dokument soll wirklich vom Unterschreibenden stammen. Indem Unterschrift und unterschriebene Erklärung auf dem selben Blatt stehen, wird ein enger Zusammenhang zwischen beiden hergestellt.

---

[1] Abbildung aus dem „Kryptoreport“ von TeleTrusT e.V. unter http://www.teletrust.de.
[2] Die Begriffe „elektronische“ / „digitale“ Signatur können synonym verwendet werden, man spricht jedoch meist von der elektronischen Signatur.
[3] Das Einwohnermeldeamt muss sicherstellen, dass sie eine Person sicher identifiziert hat, bevor ihr ein Personalausweis oder einen Pass ausgestellt wird. Dritte verlassen sich auf das Einwohnermeldeamt indem sie Ausweis oder Pass als Nachweis für die Identität gelten.

Identitätseigenschaft: Jede natürliche Unterschrift verkörpert die Identität des jeweils Unterschreibenden, d.h., die Unterschrift kann einer und nur dieser Person zugeordnet werden.
Abschlusseigenschaft: Die Unterschrift steht am Ende des Dokuments. Damit wird das Dokument abgeschlossen, so dass nachfolgende, nicht unterschriebene Äußerungen, keine Rechtsgültigkeit haben.
Warneigenschaft: Diese soll den Unterzeichnenden vor einer Übereilung bewahren. Der Akt des handschriftlichen Unterschreibens ist in der Regel ein, auch in Hinblick auf rechtliche Konsequenzen, bewusster Akt.
Verifikationseigenschaft: Jeder Empfänger kann die Unterschrift, etwa durch Unterschriftenvergleich, verifizieren.

Der Formzwang dient also unterschiedlichen Zwecken, die sich aus dem spezifischen rechtlichen Kontext der Willenserklärung ergeben. Neben diesen Funktionen ergeben sich aber auch noch andere Motive für die Festlegung der gesetzlichen Schriftform. Dies wären z.B. für Grundbucheinträge die Publizitätswirkung[4], für Testamente die Beweissicherheit und für schriftliche Akten der Verwaltungsbehörden die Kontrollfunktion. [7]

Aufgrund der neuen technischen Möglichkeiten wurde in Deutschland im Jahre 1997 das Signaturgesetz (SigG) und die Signaturverordnung (SigV) geschaffen. Deutschland hatte in Europa eine Art Vorreiterrolle in diesem Bereich. Um eine europaweite Vereinheitlichung der Regelungen voranzutreiben wurden den Mitgliedsstaaten von der EU in der **Signatur-Richtlinie** und der **E-Commerce-Richtlinie** Vorgaben gemacht, die diese in ihren nationalen Gesetzen umzusetzen hatten. Das SigG, die SigV aber auch andere Gesetze wurden daraufhin im Jahre 2001 novelliert. Insbesondere mussten Rechtswirkungen festgelegt, sowie Haftungs- und Datenschutzregelungen getroffen werden.[2] Zweck des SigG 2001 ist es, Rahmenbedingungen für die elektronischen Signaturen zu schaffen (§1 Abs. I SigG). In §2 SigG ist ein Katalog von spezifischen Begriffen definiert, der das Verständnis des Gesetzes erleichtern soll. Zu erwähnen ist hier, dass der Gesetzgeber eigene Bezeichnungen für die benutzten Schlüssel vornimmt. Er bezeichnet den **geheimen Schlüssel** (secret key) als **Signaturschlüssel** (§2 Nr. 4 SigG) und den **öffentlichen Schlüssel** (public key) als **Signaturprüfschlüssel** (§2 Nr. 5 SigG). Der Gesetzgeber definiert in §2 SigG außerdem vier Signaturtypen:

1. Elektronische Signaturen (§2 Nr. 1 SigG)
Signaturen i. S. d. §2 Nr. 1 SigG sind solche Daten, die „anderen elektronischen Daten in elektronischer Form beigefügt oder logisch mit ihnen verknüpft“ sind. Dies ist die einfachste Form und bedarf keiner weiteren Sicherheitsanforderungen. [2] Zur „Authentifizierung“ soll dies ausreichen. Als Beispiel wird in der Gesetzesbegründung die eingescannte Unterschrift benannt. Sie kann unter beliebig viele Dateien kopiert werden und kann somit allenfalls subjektiv zu einer Zuordnung der benannten Person führen. [8]

2. Fortgeschrittene elektronische Signaturen (§2 Nr. 2 SigG)
Fortgeschrittene elektronische Signaturen sind solche der Nr. 1, die gem. § 2 Nr. 2 SigG zusätzliche Merkmale aufweisen können. [8] Im Wesentlichen muss der Signaturschlüssel ausschließlich dem identifizierbaren Inhaber zugeordnet sein und dieser muss alleinige Kontrolle über die Mittel zur Erzeugung einer Signatur haben. Auch eine spätere Veränderung der signierten Daten muss erkannt werden können. Ein mögliches Beispiel hierfür ist das Verfahren, das von Pretty Good Privacy (PGP) verwendet wird. Hierbei wird der geheime Signaturschlüssel ohne weitere Sicherheitsanforderungen auf einem Datenträger abgelegt.[5]

3. Qualifizierte elektronische Signaturen (§ 2 Nr. 3 SigG)
§2 Nr. 3 SigG definiert qualifizierte elektronische Signaturen (eines angezeigten Zertifizierungsdiensteanbieters). Durch weitere zusätzliche Anforderungen soll eine gewisse Sicherheitsstufe erfüllt werden. Das qualifizierte Zertifikat muss von einem Zertifizierungsdienstanbieter ausgestellt sein, der den Anforderungen der §§4 bis 14 bzw. 23 SigG genügt und der seine Tätigkeit bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) angezeigt hat. Die Komponenten zur Speicherung und Anwendung des Signaturschlüssels (Software und Hardware) müssen den Anforderungen des §17 oder 23 SigG genügen. Dies berechtigt dazu das „Prädikat der Qualifizierung“ [2] zu tragen. Gerade an diese Qualifizierung werden in anderen Gesetzen spezielle Rechtsfolgen geknüpft (z.B. §126a BGB, §292a ZPO). Im Ergebnis kann man durch die notwendige Anzeige bei der RegTP von **vermuteter Sicherheit** sprechen.

4. Qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung (§§2 Nr. 15, 15 Abs. I SigG)
Qualifizierte elektronische Signaturen eines akkreditierten Zertifizierungsdiensteanbieters, wohl besser „akkreditierte Signaturen“, [2; 5] zeichnen sich dadurch aus, dass sich der Zertifizierungsdiensteanbieter einer freiwilligen Überprüfung (Akkreditierung) unterzieht. An Stelle der Anzeige nach § 4 Abs. II, III SigG nimmt der Anbieter also zusätzliche Pflichten auf sich. Dabei hat er der zuständigen Behörde (RegTP, §3 SigG, §66 TKG) vorab (und dann in regelmäßigen Abständen) nachzuweisen, dass er die Anforderungen des Gesetzes bzw. der SigV nach § 24 SigG erfüllt (§ 15 Abs. I S. 2 SigG). Dafür erhält er, wenn dies gelungen ist, ein Gütezeichen, dass ihn als akkreditierten Zertifizierungsdiensteanbieter ausweist (§15 Abs. I S. 3-5). [3] Die von ihm ausgestellten Signaturen erfüllen somit den höchsten Sicherheitsstandard, ermöglichen also die größte Rechtssicherheit. Es liegt **geprüfte Sicherheit** vor.

---

[4] Die Glaubwürdigkeit des Inhalts bewirkt juristische Konsequenzen: Das Vertrauen auf die Richtigkeit der Eintragungen wird geschützt.
[5] Näheres zum Verfahren bzw. eine Downloadmöglichkeit unter http://www.pgpi.org.

Das SigG regelt hauptsächlich nur die qualifizierte und akkreditierte elektronische Signatur. Die Anforderungen an beide Signaturen sind beinahe gleich, aber bei der akkreditierten Signatur findet eben eine Vorabprüfung statt. Die wesentlichen Pflichten der Zertifizierungsdienstanbieter für diese beiden Signaturen nach dem SigG sind:
Identifizierung der Antragsteller (§5 Abs. I S.1, 2 SigG, §3 Abs. I SigV)
Sicherstellung der Zuordnung der Schlüssel zu den Personen (Ausstellung der Zertifikate) (§5 Abs. IV SigG)
Zertifikatsverzeichnis und Sperrverzeichnis führen (jederzeitige Abrufbarkeit) (§5 Abs. I SigG)
Dokumentation des Sicherheitskonzepts (§10 SigG, §8 SigV)
Aufbau und Unterhaltung der Public-Key-Infrastruktur (PKI)

IV. Sonstige rechtliche Regelungen: Das Formgesetz 2001 (§§126 Abs. II, 126a BGB und §§130a, 292a ZPO)

Um die Rechtswirksamkeit der elektronischen Signatur gewährleisten zu können, wurde im BGB die **elektronische Form** eingeführt (§§126 Abs. III, 126a BGB).[6] Sie ist nach §126a BGB erfüllt, wenn der Aussteller seinen Namen zugefügt und das Dokument mit einer **qualifizierten** elektronischen Signatur nach dem SigG versehen hat. Bei einem Vertrag müssten beide Vertragspartner ein gleichlautendes Dokument elektronisch signieren. §126 Abs. III BGB erlaubt die Anwendung der elektronischen Form, wenn sich aus dem Gesetz nicht ein anderes ergibt. Solche Ausnahmeregelungen hat der Gesetzgeber zugleich festgelegt.[7] Die elektronische Form ist z.B. ausgeschlossen bei der Kündigung des Arbeitsvertrages (§623 BGB), bei der Bürgschaft (§766 S.2 BGB) und bei Schuldversprechen und –anerkenntnis (§§780f. BGB). Die Ausnahmen sind in den umfassenden rechtlichen Konsequenzen dieser Handlungen begründet.

Doch auch für die gerichtliche Praxis mussten insbesondere im Prozessrecht Regelungen getroffen werden, wie ein Richter im Sinne des Beweisrechts mit solchen elektronischen Signaturen umzugehen hat. Beispielhaft sei an dieser Stelle auf die Zivilprozessordnung (ZPO) hingewiesen, jedoch sind auch andere verfahrensrechtliche Regelungen mit dem schon erwähnten Formgesetz novelliert worden. Weitere Novellierungen stehen an (z.B. die des Verwaltungsverfahrensgesetzes [9]). Der **§130a ZPO** wurde neu geschaffen. Es ist jetzt möglich **Schriftsätze, Anträge und Erklärungen in elektronischer Form bei Gericht einzureichen**, wenn dies durch Rechtsverordnung für das jeweilige Gericht zugelassen ist. Seit November 2001 läuft z.B. am Bundesgerichtshof ein Modellversuch, in dem die Möglichkeit der Einreichung von elektronischen Schriftsätzen untersucht wird.[8] Ein weiteres aktuelles Beispiel diesbezüglich ist die Verordnung über den elektronischen Rechtsverkehr bei dem Finanzgericht Hamburg.[9] Seit Mai 2002 ist es dort möglich ein komplettes Klageverfahren per E-Mail abzuwickeln. „Zur Herstellung der rechtlichen Verbindlichkeit soll das jeweilige Dokument mit einer **qualifizierten** elektronischen Signatur versehen werden“ (Anlage zu §2 der Verordnung). Außerdem werden auf den Internetseiten des Finanzgerichts bzw. der Justizverwaltung[10] Informationen zu den zulässigen Formaten bzw. Versionen der Dokumente bereitgestellt.

Außerdem wurde der neue **§292a ZPO** eingeführt. Dieser regelt eine **Beweisvermutung** für Erklärungen in elektronischer Form mit **qualifizierter** Signatur gem. §126a BGB. Es wird aufgrund der technischen und organisatorischen Anforderungen, die an eine qualifizierte Signatur gestellt werden, davon ausgegangen, dass dies als Anschein genügt, dass die Erklärung von der Person stammt, deren Signatur die Erklärung trägt. Dieser Anscheinsbeweis ist aber, durch Tatsachen erschütterbar, „die es ernsthaft als möglich erscheinen lassen, dass die Erklärung nicht mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist“ (§292a ZPO).

Quellenverzeichnis

[1] Bizer, Johann/Fox, Dirk „Digital signierte Zukunft?”, Datenschutz und Datensicherheit (DuD), 2/1997, S.66
[2] Bizer, Johann „Elektronisch Signaturen im Rechtsverkehr“, in Gimmy, Marc André/Kröger, Detlef (Hrsg.) „Handbuch zum Internetrecht“, S.37–92, 2. Aufl., Berlin 2002
[3] Blum, Felix „Entwurf eines neuen Signaturgesetzes“, Datenschutz und Datensicherheit (DuD), 2/2001, S.71-78
[4] Fox, Dirk „Signaturschlüssel-Zertifikat”, Datenschutz und Datensicherheit (DuD), 2/1997, S.106
[5] Roßnagel, Alexander „Das neue Recht der elektronischen Signaturen“, NJW 2001, S.1817-1826
[6] Schneier, Bruce „Angewandte Kryptographie“, 1. Aufl., Bonn 1996
[7] Vierter Zwischenbericht der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft“ zum Thema „Sicherheit und Schutz im Netz”, Bundestagsdrucksache 13/11002, vom 22.06.1998
[8] „Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“, Bundestagsdrucksache 14/4662, vom 16.11.2000
[9] „Entwurf eines Dritten Gesetzes zur Änderung verwaltungsverfahrensrechtlicher Vorschriften“, Bundestagsdrucksache 14/9000, vom 13.05.2002

[6] Gesetz z. Anpassung der Formvorschriften des Privatrechts u.a. Vorschriften an den mod. Rechtsgeschäftsverkehr, v. 13.07.2001, BGBl. I, S.1542ff.
[7] Das dies möglich ist, ergibt sich aus Artikel 1 Abs. II der Signatur-Richtlinie.
[8] Für den Bundesgerichtshof ist dies in der Elektronischen Rechtsverkehrsverordnung – ERVVOBGH vom 26. Nov. 2001, BGBl. I, S.3225 geregelt. Siehe näheres zum Modellversuch unter http://www.bundesgerichtshof.de/e-rechtsverkehr.htm.
[9] HmbGesetz- und Verordnungsbl. I 2002, S. 41f., ebenfalls verfügbar unter http://www.dud.de/dud/documents/e-rechtsverkehr-hmbgvbl-020409.pdf.
[10] Unter http://www.finanzgericht.hamburg.de und http://www.justiz.hamburg.de.