Prof. Dr. Viola Schmid, LL.M. (Harvard)

Fachgebiet Öffentliches Recht

Informations- und Datenschutzrecht I

DATUM	MODUL	TITEL
03.01.2006	**5**	**Sektorale Betrachtung: Signaturrecht**

A. Geschichtliche Entwicklung des Signaturrechts ... 3
I. Internationale Perspektive ... 3
II. Europäische Perspektive ... 5
III. Deutsche Perspektive ... 6
IV. Regelungsansätze ... 8
B. Signaturverfahren ... 10
I. Symmetrische versus asymmetrische Kryptographieverfahren ... 10
II. Signatur und Verschlüsselung ... 12
III. Schlüsselgenerierung ... 13
IV. Signaturerstellung ... 14
V. Hashwert ... 14
VI. Signaturprüfung ... 15
VII. Schlüsselmanagement ... 15
1. Sicherheit des privaten Schlüssels ... 15
2. Sicherheit des öffentlichen Schlüssels ... 16
C. Parallelität der elektronischen Form mit Realworld-Dokumenten ... 18
I. Qualifizierte elektronische Signatur ... 19
II. Qualifizierte elektronische Signatur als Unterschriftssurrogat ... 19
1. Abschlussfunktion ... 20
2. Perpetuierungsfunktion ... 21
3. Identitätsfunktion ... 21
4. Echtheitsfunktion ... 22
5. Verifikationsfunktion ... 22
6. Beweisfunktion ... 22
7. Warnfunktion ... 24

D. Beispiel für die rechtliche Bedeutung von Signaturen: § 55aVwGO 24

I. § 55a VwGO als Teil des „Puzzles“ E-Governance 25

II. Grundsatz der Eröffnung von elektronischer Justizkommunikation (nur) durch Rechtsverordnung 26

III. Qualität der Informationstechnik 26

1. Signaturerfordernis 26
2. „andere sichere Verfahren“ als Konkurrenz zum Signaturkanon? 27
3. Sicherung von Intimität 28

E. Literaturhinweise 29

A. Geschichtliche Entwicklung des Signaturrechts

I. Internationale Perspektive

Wichtige erste Impulse für ein Signaturrecht gingen von internationalen Abkommen im Bereich des internationalen Handelsverkehrs aus. Insbesondere im Internationalen Transportrecht war schon Ende der siebziger Jahre (Hamburg Rules von 1978) eine Öffnung für elektronische Verfahren, die die handschriftliche Unterschrift ersetzen, zu beobachten. Obwohl Klarheit über konkrete Verfahrenweisen oder diesbezügliche Standards nicht herrschte, wurde die elektronische Unterschrift der handschriftlichen Unterschrift gleichgestellt:

Art. 14 United Nations Convention on the Carriage of Goods by Sea (Hamburg Rules)[1]
[Issue of bill of lading]
(3) The signature on the bill of lading may be in handwriting, printed in facsimile, perforated, stamped, in symbols, or made by any other mechanical or electronic means, if not inconsistent with the law of the country, where the bill of lading is issued.

Diese Impulse aufgreifend setzte sich die **"Working Party on Facilitation of International Trade Procedures"**[2] als Unterorgan der **"United Nations Economic Commission for Europe"(UNECE)** in ihrer 14. Empfehlung[3] 1979 mit der Frage der Authentifizierung mittels anderer Verfahren als der handschriftlichen Unterschrift auseinander.[4] Drei Funktionen der Unterschrift standen dabei im Vordergrund:

Recommendation No. 14 by the Working Party on Facilitation of International Trade Procedures
[Function of signature]
4. A signature on trade documents serves three main purposes:
(i) It identifies the source of a document, i.e. the writer;
(ii) It confirms the information of the document; and
(iii) It constitutes proof of the signatory´s responsibility for the correctness and/or completion of the information in the document.
(...)

Als Authentifizierungsverfahren, das diesen Anforderungen gerecht wird, wurde das im internationalen Zahlungsverkehr zwischen Banken schon seit 1973 angewandte Verfahren **S.W.I.F.T.**[5] anerkannt, das bis heute verwendet wird.

---

[1] United Nations Convention on the Carriage of Goods by Sea (sogenannte "Hamburg Rules") vom 30.03.1978
[2] Working Party on Facilitation of International Trade Procedures.
[3] Recommendation No. 14: „Authentication of Trade Documents by Means other than Signature" vom März 1979.
[4] Neben Telex und Fernkopie (Fax) wurde auch schon die direkte Übertragung von Computer zu Computer (E-Mail) als zu berücksichtigende aufstrebende Kommunikationsmethode erkannt.
[5] SWIFT (Society for Worldwide Interbank Financial Telecommunication) wird einerseits als Abkürzung für die Gesellschaft verwendet, andererseits auch als Abkürzung für das Netz, das die Gesellschaft bereitstellt.

Der Aspekt des internationalen Handels- und Zahlungsverkehrs blieb auch weiterhin zentral, so dass sich hauptsächlich internationale Gremien und Organisationen mit handelsrechtlichem Hintergrund mit dem Thema der elektronischen Signatur beschäftigten, etwa die „United Nations Commission on International Trade Law“(UNCITRAL)[6]. Das „UNCITRAL Model Law on Electronic Commerce“[7] von 1996 forderte die rechtliche Anerkennung und Wirksamkeit elektronischer Signaturen.

Art. 5 der Resolution 162(LI) [Legal recognition of data messages]
Information shall not be denied legal effect, validity or enforce-ability solely on the grounds that it is in the form of a data message.

Art. 7 der Resolution 162(LI) [Signature]
(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
(a) a method is used to identify that peson and to indicate that person´s approval of the information contained in the data message; and
(b) that method is as reliable as was appropriate for the purpose of which the data message was generated or communicated, in the light of all the circumsstances, including any relevant agreement.
(...)

2001 wurde ein eigenes Modellgesetz hinsichtlich elektronischer Signaturen geschaffen.[8] Während sich die Modellgesetze der UNCITRAL an Staaten wenden, richteten sich die Arbeiten anderer Foren, etwa der „Organisation for Economic Co-operation and Development“(OECD)[9] oder der „International Chamber of Commerce“(ICC)[10], gleichermaßen an Private.

Die ersten staatlichen Signaturgesetze, die in Kraft traten, stammten aus den Vereinigten Staaten. Einzelne US-Bundesstaaten[11] haben sich schon sehr früh mit der rechtlichen Regulierung elektronischer Signaturen auseinandergesetzt. Das weltweit erste Gesetz, das eine Sicherungsinfrastruktur für elektronische Signaturen implementierte, war der „Utah Digital Signature Act“ [12] vom 01.05.1995. Diese Vorreiterrolle der Vereinigten Staaten hängt mit der Größe und wirtschaftlichen Bedeutung des US-Marktes zusammen. Ein weiterer Grund könnte aber

[6] United Nations Commission on International Trade Law (UNCITRAL): “Legal aspects of automatic data processing”, A/CN.9/238, erstellt in der 16. Sitzungsperiode, 24.05.-03.06.1983.
[7] Resolution 162(LI) der Generalversammlung der Vereinten Nationen vom 16.12.1996.
[8] “Model Law on Electronic Signatures of the United Nations Commission on Internatioal Trade Law”, Resolution 80(LVI) der Generalversammlung der Vereinten Nationen vom 12.12.2001.
[9] Guidelines for Cryptography Policy vom 27.03.1997.
[10] General Usage for International Digitally Ensured Commerce (GUIDEC): GUIDEC I vom 06.11.1997 und GUIDEC II vom Oktober 2001.
[11] Nachweise bei A. Miedbrodt: “Signaturregulierung im Rechtsvergleich”, 1. Auflage 2000, S. 36 ff.
[12] Utah Digital Signature Act (Utah DSA) vom 01.05.1995.

auch in der Tatsache begründet liegen, dass die Nutzung des Internets in der US-amerikanischen Bevölkerung im internationalen Vergleich am stärksten verbreitet war.

II. Europäische Perspektive

Auch im Europarecht stand in einem ersten Schritt die kommerzielle Nutzung des elektronischen Datentransfers im Vordergrund. 1987 beschloss der **Rat (damals noch der Europäischen Gemeinschaften)** ein **„Gemeinschaftsprogramm betreffend den elektronischen Datentransfer für kommerzielle Zwecke über Kommunikationsnetze“**[13]**.** In der zweiten Phase[14] (1991 bis 1994) stand auch die juristische Analyse der elektronischen Unterschrift bei elektronischen Nachrichten auf der Agenda. In den als „Bangemann-Report“ bekannt gewordenen Empfehlungen[15] wurde die wachsende Bedeutung von Verschlüsselungs- und Signaturverfahren für den elektronischen Geschäftsverkehr hervorgehoben und die Wichtigkeit einer Regelung auf europäischer Ebene betont.

> „Encryption is particularly important for telecommerce, which requires absolute guarantees in areas such as the integrity of signatures and text, irrevocable time and date stamping and international legal recognition.(...)
> The Group recommends acceleration of work at European level on electronic and legal protection as well as security.”[16]

Das Europäische Parlament forderte 1996 Kommission und Mitgliedstaaten auf, rechtliche Regelungen für die Bereiche Informationssicherheit und Vertraulichkeit zu entwickeln.[17]
1999 erließen das Europäische Parlament und der Rat die Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (europäische Signaturrichtlinie)[18], die von den Mitgliedstaaten bis zum 19.07.2001 umzusetzen war. Deutschland ist dieser europäischen Vorgabe mit dem Signaturgesetz (SigG)[19] vom 16.05.2001 und dem Formrechtsanpassungsgesetz[20] vom 13.07.2001 nachgekommen.

---

[13] Beschluss 87/499/EWG vom 05.10.1987, ABl L 285, 35.
[14] Beschluss 91/385/EWG des Rates zur Durchführung der zweiten Phase des Programms TEDIS (Trade Electronic Data Interchange Systems) vom 22.07.1991, ABl L 208, 066.
[15] „Europe and the global information society“(Bangemann-Report), Empfehlungen einer Expertengruppe an den Europäschen Rat vom 26.05.1994.
[16] Bangemann-Report, 3. Kapitel.
[17] Entschließung zu der Empfehlung an den Europäischen Rat „Europa und die globale Informationsgesellschaft“ und zu der Mitteilung der Kommission „Europas Weg in de Informationsgesellschaft: Ein Aktionsplan“ vom 28.10.1996, ABl C 320, S. 164, Ziffer 106.
[18] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl L 013, 12 vom 19.01.2000.
[19] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001, BGBl I 876.
[20] Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr (Formrechtsanpassungsgesetz) vom 13.07.2001, BGBl I 1542.

III. Deutsche Perspektive

Deutschland hatte das erste Signaturgesetz in Europa. Das frühere Signaturgesetz von 1997[21] regelte nur die Anforderungen an die „digitale Signatur". Die Definition der „digitalen Signatur" zeigt, dass es sich um die „qualifizierte elektronische Signatur" nach heute geltendem Signaturrecht[22] handelte.[23]

§ 2 SigG 1997 [Begriffsbestimmungen]
(1) Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde nach § 3 versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt.
(…)

§ 2 SigG [Begriffsbestimmungen]
Im Sinne dieses Gesetzes sind
1. „elektronische Signaturen" Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,
2. „fortgeschrittene elektronische Signaturen" elektronische Signaturen nach Nummer 1, die
a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,
3. „qualifizierte elektronische Signaturen" elektronische Signaturen nach Nummer 2, die
a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
b) mit einer sicheren Signaturerstellungseinheit erzeugt werden,
(…)

Ein wichtiger Unterschied zwischen dem SigG 1997 und dem SigG 2001 lag in der Ausweitung des Regelungsbereichs des Signaturrechts. Während das SigG 1997 nur Regelungen für einen Signaturtyp – die unter Sicherheitsgesichtspunkten der Unterschrift entsprechende Signatur – enthielt, erfasst das SigG 2001 alle Arten elektronischer Signaturen und unterscheidet zwischen drei Signaturtypen: („einfacher") elektronischer Signatur, fortgeschrittener elektronischer Signatur und qualifizierter elektronischer Signatur. Damit wird beispielsweise auch eine eingescannte Unterschrift vom Signaturrecht umfasst[24] – obwohl sie keine sichere Auskunft über den Aussteller zu geben vermag. Dieses weite Verständnis des Begriffs elektronische Signatur lag auch der europäischen Signaturrichtlinie zugrunde. Auch die fortgeschritte-

[21] Gesetz zur digitalen Signatur (SigG 1997) vom 22.07.1997, BGBl I 1870.
[22] Signaturgesetz (SigG 2001) vom 16.05.2001, in der durch das Erste Signaturänderungsgesetz vom 04.01.2005 modifizierten Fassung.
[23] So auch der Gesetzesentwurf der Bundesregierung: BR-Drucks 496/00 S. 31.
[24] BR-Drucks 496/00, S. 30.

ne elektronische Signatur des SigG 2001 entspricht hinsichtlich Terminologie und Definition der europäischen Signaturrichtlinie. Das deutsche SigG 2001 trifft lediglich noch eine weitere Unterscheidung zwischen fortgeschrittener und qualifizierter elektronischer Signatur. Inhaltlich findet sich die qualifizierte elektronische Signatur auch in der europäischen Signaturrichtlinie wieder (Art. 5 Abs. 1 europäische Signaturrichtlinie) – es wurde aber kein eigenständiger Begriff für diese besondere Form der fortgeschrittenen elektronischen Signatur etabliert.

Art. 5 Signaturrichtlinie [Rechtswirkung elektronischer Signaturen]
(1) Die Mitgliedstaaten tragen dafür Sorge, daß fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und die von einer sicheren Signaturerstellungseinheit erstellt werden,
a) die rechtlichen Anforderungen an eine Unterschrift in bezug auf in elektronischer Form vorliegende Daten in gleicher Weise erfuellen wie handschriftliche Unterschriften in bezug auf Daten, die auf Papier vorliegen, und
b) in Gerichtsverfahren als Beweismittel zugelassen sind.

Die europäische Signaturrichtlinie schuf außerdem Anpassungsbedarf hinsichtlich der Verwirklichung der europäischen Binnenmarktprinzipien. Weiter enthält das SigG 2001 im Gegensatz zum SigG 1997 eine eigene Haftungsregelung (§ 11 SigG).

§ 11 SigG [Haftung]
(1) Verletzt ein Zertifizierungsdiensteanbieter die Anforderungen dieses Gesetzes oder der Rechtsverordnung nach § 24 oder versagen seine Produkte für qualifizierte elektronische Signaturen oder sonstige technische Sicherungseinrichtungen, so hat er einem Dritten den Schaden zu ersetzen, den dieser dadurch erleidet, dass er auf die Angaben in einem qualifizierten Zertifikat, einem qualifizierten Zeitstempel oder einer Auskunft nach § 5 Abs. 1 Satz 2 vertraut. Die Ersatzpflicht tritt nicht ein, wenn der Dritte die Fehlerhaftigkeit der Angabe kannte oder kennen musste.
(2) Die Ersatzpflicht tritt nicht ein, wenn der Zertifizierungsdiensteanbieter nicht schuldhaft gehandelt hat.
(3) Wenn ein qualifiziertes Zertifikat die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt, tritt die Ersatzpflicht nur im Rahmen dieser Beschränkungen ein.
(4) Der Zertifizierungsdiensteanbieter haftet für beauftragte Dritte nach § 4 Abs. 5 und beim Einstehen für ausländische Zertifikate nach § 23 Abs. 1 Nr. 2 wie für eigenes Handeln. § 831 Abs. 1 Satz 2 des Bürgerlichen Gesetzbuchs findet keine Anwendung.

Unter dem SigG 1997 galt noch ausschließlich das allgemeine Haftungsrecht, wie es im Bürgerlichen Gesetzbuch (BGB) geregelt ist.

Die europäische Signaturrichtlinie forderte darüber hinaus die grundsätzliche Genehmigungsfreiheit von Zertifizierungsdiensten (Art. 3 Abs. 1 europäische Signaturrichtlinie). Dies wird jetzt auch im deutschen Signaturrecht gewährleistet (§ 4 Abs.1 SigG).

§ 4 SigG [Allgemeine Anforderungen]
(1) Der Betrieb eines Zertifizierungsdienstes ist im Rahmen der Gesetze genehmigungsfrei.
(…)

Der deutsche Gesetzgeber hat von der in der europäischen Signaturrichtlinie eingeräumten Möglichkeit der Schaffung eines freiwilligen Akkreditierungssystems Gebrauch gemacht.

§ 15 SigG [Freiwillige Akkreditierung von Zertifizierungsdiensteanbietern]
(1) Zertifizierungsdiensteanbieter können sich auf Antrag von der zuständigen Behörde akkreditieren lassen; die zuständige Behörde kann sich bei der Akkreditierung privater Stellen bedienen. Die Akkreditierung ist zu erteilen, wenn der Zertifizierungsdiensteanbieter nachweist, dass die Vorschriften nach diesem Gesetz und der Rechtsverordnung nach § 24 erfüllt sind. Akkreditierte Zertifizierungsdiensteanbieter erhalten ein Gütezeichen der zuständigen Behörde. Mit diesem wird der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen (qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung) zum Ausdruck gebracht. Sie dürfen sich als akkreditierte Zertifizierungsdiensteanbieter bezeichnen und sich im Rechts- und Geschäftsverkehr auf die nachgewiesene Sicherheit berufen.
(…)

IV. Regelungsansätze

Für das Signaturrecht[25] können zwei Regelungsstrategien unterschieden werden:

- Modelle, die nur bestimmte Kommunikationsbeziehungen regeln und
- Modelle, die eine Regelung aller Kommunikationsbeziehungen anstreben.

Darüber hinaus können drei Substrategien unterschieden werden:

- **Technikrechtlicher Ansatz**

Signaturnormen, die einem technikrechtlichen Ansatz folgen, regeln die Voraussetzungen der Infrastruktur für elektronische Signaturen en détail, um beweissichere Kommunikation zu ermöglichen. Dieses Konzept wurde vom „Utah Digital Signature Act“ und vom „Washington Electronic Authenication Act“[26] verfolgt Auch das deutsche Signaturrecht ist stark von diesem Ansatz geprägt, indem Anforderungen an

- **Technische Sicherheit,**

  z. B. durch regelmäßige Festlegung, welche Signatur- und Hashverfahren geeignet sind

- **Anwendungssicherheit,**

  etwa durch das für Signaturanwendungskomponenten bestehende Erfordernis der Erkennbarkeit von Existenz und nicht erfolgter Sperrung des geprüften qualifizierten Zertifikats

[25] Kategorisierung folgend A. Miedbrodt: “Signaturregulierung im Rechtsvergleich”, 1. Auflage 2000, S. 36 ff.
[26] Washington Electronic Authentication Act (Washington EAA) vom 29.03.1996.

- **Personelle Sicherheit,**

  etwa durch die Unterrichtungspflicht der Zertifizierungsdiensteanbieter über Sicherheitsmaßnahmen und die rechtlichen Wirkungen einer qualifizierten elektronischen Signatur

- **Organisatorische Sicherheit**

  beispielsweise mittels behördlicher Aufsichts- und Kontrollmaßnahmen

formuliert werden.

Während das SigG 1997 noch für einen rein technikrechtlichen Ansatz stand, wird dies im SigG 2001 mit der durch die europäische Signaturrichtlinie notwendigen Anpassung und Harmonisierung etwas aufgeweicht hin zu einem hybriden Ansatz. Gleichwohl sind die technikrechtlichen Wurzeln unverkennbar und dominieren auch weiterhin das deutsche Signaturrecht.

- **Marktwirtschaftlicher Ansatz**

Signaturnormen, die einem marktwirtschaftlichen Ansatz folgen, regeln nur die gesetzlichen Rahmenbedingungen, innerhalb derer es den Kräften des Marktes überlassen bleibt, die Anforderungen an die Anbieter elektronischer Signaturverfahren zu spezifizieren. Dieser Ansatz findet sich im Modellgesetz „Uniform Electronic Transactions Act“[27] der „National Conference of Commissioners on Uniform State Laws“[28] (NCCUSL) vom 30.07.1999, auf dessen Basis viele Bundesstaaten entsprechende Gesetze erlassen haben, und im „E-Sign Act“[29] des US-amerikanischen Bundesgesetzgebers vom 30.06.2000.

- **Hybrider Ansatz**

Einen solchen kombinierten Ansatz, der Regelungselemente sowohl des technikrechtlichen wie des marktwirtschaftlichen Ansatzes enthält, haben z. B. die europäische Signaturrichtlinie oder der „Illinois Electronic Commerce Security Act“[30] gewählt. In der europäischen Signaturrichtlinie wird der marktwirtschaftliche Ansatz durch die (einfache) elektronische Signatur repräsentiert.

Art. 2 Europäische Signaturrichtlinie [Begriffsbestimmungen]
Im Sinne dieser Richtlinie bezeichnet der Ausdruck
1. "elektronische Signatur" Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen;
2. "fortgeschrittene elektronische Signatur" eine elektronische Signatur, die folgende Anforderungen erfüllt:

[27] Uniform Electronic Transactions Act (UETA) vom 30.07.1999.
[28] National Conference of Commissioners on Unifrom State Law (NCCUSL).
[29] Electronic Signatures in Global and National Commerce Act (E-Sign Act) vom 30.06.2000, United States Public Laws 106-229 (S. 761).
[30] Illinois Electronic Commerce Security Act (Illinois ECSA) vom 14.08.1998.

a) Sie ist ausschließlich dem Unterzeichner zugeordnet;
b) sie ermöglicht die Identifizierung des Unterzeichners;
c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;
d) sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, daß eine nachträgliche Veränderung der Daten erkannt werden kann;
(…)

An die (einfache) elektronische Signatur werden keine technischen, personellen, organisatorischen oder anwendungsbezogene Anforderungen gestellt. Mit der Übernahme der Definition der (einfachen) elektronischen Signatur aus der Richtlinie fanden erstmals Elemente des marktwirtschaftlichen Ansatzes Eingang ins deutsche Signaturrecht.

Mit der fortgeschrittenen elektronischen Signatur folgt die europäische Signaturrichtlinie dem technikrechtlichen Ansatz. Für diese Signatur werden technische, organisatorische, personelle und anwendungsbezogene Sicherheitsanforderungen formuliert.[31]

B. Signaturverfahren

I. Symmetrische versus asymmetrische Kryptographieverfahren

Das deutsche Signaturgesetz geht von der Verwendung eines asymmetrischen kryptographischen Verfahrens aus. Für diese Perspektive gibt es folgende Anhaltspunkte:

§ 2 SigG [Begriffsbestimmungen]
Im Sinne dieses Gesetzes sind (…)
4. „Signaturschlüssel“ einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden,
5. „Signaturprüfschlüssel“ elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden,
(…)

§ 15 SigV[32] [Anforderungen an Produkte für qualifizierte elektronische Signaturen]
(1) Sichere Signaturerstellungseinheiten nach § 17 Abs. 1 Satz 1 des Signaturgesetzes müssen gewährleisten, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann. Der Signaturschlüssel darf nicht preisgegeben werden. Bei Nutzung biometrischer Merkmale muss hinreichend sichergestellt sein, dass eine unbefugte Nutzung des Signaturschlüssels ausgeschlossen ist und eine dem wissensbasierten Verfahren gleichwertige Sicherheit gegeben sein. Die zur Erzeugung und Übertragung von Signaturschlüsseln erforderlichen technischen Komponenten nach § 17 Abs. 1 Satz 2 oder Abs. 3 Nr. 1 des Signaturgesetzes müssen gewährleisten, dass aus einem Signaturprüfschlüssel oder einer Signatur nicht der Signaturschlüssel errechnet werden kann und die Signaturschlüssel nicht dupliziert werden können.

[31] Insbesondere durch die Anhänge I-IV der Richtlinie.
[32] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001, BGBl. I 3074.

(2) Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass
1. bei der Erzeugung einer qualifizierten elektronischen Signatur
a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,
b) eine Signatur nur durch die berechtigt signierende Person erfolgt,
c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird und
2. bei der Prüfung einer qualifizierten elektronischen Signatur
a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und
b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.
(…)

Die Verwendung eines symmetrischen Signaturverfahrens setzt zwei Dinge voraus, zum einen, dass die Kommunikationspartner schon vorher miteinander in Kontakt gestanden haben, um einen Schlüssel zu vereinbaren, und zum anderen eine gewisse Vertrauensbeziehung, da sich jeder darauf verlassen muss, dass der jeweils andere den Schlüssel geheim hält. Die Vorteile des asymmetrischen Verfahrens für den elektronischen Rechts- und Geschäftsverkehr liegen somit auf der Hand: Während bei einem symmetrischen Verfahren immer nur jeweils zwei Kommunikationspartner den Schlüssel kennen sollten, um Authentizität, Identität und Integrität tatsächlich zu gewährleisten, ist mithilfe eines asymmetrischen Verfahrens die Kommunikation einer Person mit beliebig vielen verschiedenen Kommunikationspartnern möglich, ohne dass der Zweck der Signatur gefährdet wird. Damit wird die Sicherheit von elektronischen Signaturen entscheidend erhöht. Schließlich kann gegenüber jedem denkbaren Kommunikationspartner eine Identitätsausweisung mittels derselben elektronischen Signatur erfolgen.

Anders als das deutsche Recht ist dem US-amerikanischen E-Sign Act die Struktur der asymmetrischen Verschlüsselung nicht zu entnehmen.

Sec. 106 E-Sign Act [Definitions]
(5) ELECTRONIC SIGNATURE. – The term „electronic signature“ means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with intent to sign the record.
(...)

Im Hinblick auf die deutsche Rechtslage und die deutlichen Vorteile von asymmetrischen Kryptographieverfahren für den Rechtsverkehr wird sich die Darstellung der Ver- und Entschlüsselungstechnik auf asymmetrische Verfahren beschränken. Schließlich darf vermutet werden, dass bereits jetzt die asymmetrischen Verfahren das Signaturrecht in der Praxis dominieren – soweit es um der traditionellen Unterschrift gleichgestellte Signaturen geht.

II. Signatur und Verschlüsselung

Neben der elektronischen Signatur basieren auch Verschlüsselungstechniken auf Kryptographieverfahren. Zur Verdeutlichung des Wesens der elektronischen Signatur erscheint eine Abgrenzung von der Verschlüsselung hilfreich:

- Die **Verschlüsselung** schützt die **Vertraulichkeit** von Kommunikationsinhalten (Schutz der **Intimität**).
- Die **elektronische Signatur** schützt **Authentizität**, **Integrität** und **Identität** von Kommunikation.
- Nur weil ein Dokument signiert ist, bedeutet das nicht, dass das Dokument auch vertraulich ist. Wird zur Entschlüsselung ein öffentlicher Schlüssel verwendet, ist diese Erkenntnis trivial: Jeder kann auf den Schlüssel zugreifen und das Dokument lesen.
- Nur weil ein Dokument verschlüsselt und damit vertraulich ist, bedeutet das nicht, dass das Dokument auch authentisch ist: Zwar mag ein Dritter die Information nicht entschlüsseln und lesen können, trotzdem kann er sie manipulieren. Mit der Veränderung durch Dritte verliert eine Information die Authentizität, denn sie ist nicht mehr unverfälscht und stammt so inhaltlich auch nicht mehr vom Absender der Information, sondern vom manipulierenden Dritten.

Im Recht findet sich die Unterscheidung von elektronischer Signatur und Schutz gegen unbefugte Kenntnisnahme durch Verschlüsselung etwa in § 174 Abs. 3 S. 3 ZPO.

§ 174 ZPO [Zustellung gegen Empfangsbekenntnis]
(1) Ein Schriftstück kann an einen Anwalt, einen Notar, einen Gerichtsvollzieher, einen Steuerberater oder an eine sonstige Person, bei der aufgrund ihres Berufes von einer erhöhten Zuverlässigkeit ausgegangen werden kann, eine Behörde, eine Körperschaft oder eine Anstalt des öffentlichen Rechts gegen Empfangsbekenntnis zugestellt werden.
(2) An die in Absatz 1 Genannten kann das Schriftstück auch durch Telekopie zugestellt werden. Die Übermittlung soll mit dem Hinweis „Zustellung gegen Empfangsbekenntnis“ eingeleitet werden und die absendende Stelle, den Namen und die Anschrift des Zustellungsadressaten sowie den Namen des Justizbediensteten erkennen lassen, der das Dokument zur Übermittlung aufgegeben hat.
(3) An die in Absatz 1 Genannten kann auch ein elektronisches Dokument zugestellt werden. Gleiches gilt für andere Verfahrensbeteiligte, wenn sie der Übermittlung elektronischer Dokumente ausdrücklich zugestimmt haben. Für die Übermittlung ist das Dokument mit einer elektronischen Signatur zu versehen und gegen unbefugte Kenntnisnahme Dritter zu schützen.
(…)

Mit der Kryptographiesoftware „GNU Privacy Guard“[33], die als Open-Source-Software vom Bundeswirtschaftsministerium im Rahmen des „GNU Privacy Projekts“[34] gefördert wird, ist

[33] GNU Privacy Guard (GnuPG).
[34] GNU Privacy Projekt (GnuPP).

beispielsweise Verschlüsselung wie auch Signierung möglich, jeweils isoliert oder in Kombination miteinander.

III. Schlüsselgenerierung

Ein Schlüsselpaar besteht aus einem geheim zu haltenden privaten Schlüssel (Private Key) und einem allgemein zugänglichen öffentlichen Schlüssel (Public Key). Es gibt verschiedene Verfahren zur Generierung dieser Schlüsselpaare, in Deutschland werden von der Bundesnetzagentur[35] zurzeit folgende Verfahren als geeignet zur Erzeugung rechtlich verbindlicher Signaturen angesehen:[36]

- RSA-Verfahren[37]
- DSA (Digital Signature Algorithm)
- DSA-Varianten, basierend auf elliptischen Kurven, insbesondere EC-DSA (Elliptic Curve Digital Signature Algorithm), EC-KDSA, EC-GDSA sowie Nyberg-Rueppel-Signaturen.

Allen Verfahren ist gemeinsam, dass sie auf einem mathematischen Problem beruhen, das zwar grundsätzlich lösbar ist, hierfür aber so viel Zeit notwendig ist, dass die Informationen dann nicht mehr wertvoll sind.[38] Damit besteht die grundsätzliche Möglichkeit, dass schon morgen ein neues Verfahren zur Lösung des jeweiligen Problems gefunden wird, das schnell genug ist, um die Signaturverfahren unsicher werden zu lassen. Letztlich wird diese Möglichkeit jedoch eher als theoretisch eingestuft, so dass die Signaturverfahren als sicher angesehen werden (können). Diese Einschätzung beruht auf dem in der modernen Kryptographie anerkannten Kerckhoffs-Prinzip[39], wonach ein sicheres Kryptographieverfahren auf der Geheimhaltung des (privaten) Schlüssels und nicht auf der Geheimhaltung des Signaturalgorithmus beruhen soll.[40] Auf dieser Idee baut das heutige Paradigma der Kryptographie auf, wonach die Robustheit eines kryptographischen Verfahrens gegen bekannte Angriffe für seine Sicherheit spricht.[41] Der dennoch bestehenden Möglichkeit des Unsicherwerdens wird dadurch Rechnung getragen, dass die genannten Verfahren zunächst nur für den Zeitraum von sechs

---

[35] Die Bundesnetzagentur entspricht der früheren Regulierungsbehörde für Telekommunikation und Post (RegTP), die im Hinblick auf einen Aufgabenzuwachs in den Bereichen Elektrizität/Gas und Eisenbahn seit dem 13.07.1005 in Bundesnetzagentur umbenannt ist.

[36] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) der Regulierungsbehörde für Telekommunikation und Post (RegTP) vom 02.01.2005, Bundesanzeiger Nr. 59, 4695.

[37] Das Verfahren ist nach seinen Entwicklern Rivest, Shamir und Adleman benannt.

[38] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): E-Government-Handbuch, Kapitel II, Modul „Verschlüsselung und Signatur“, S. 23 f.

[39] Benannt nach dem niederländischen Militär-Kryptologen Auguste Kerckhoffs von Nieuwenhof (1835-1903).

[40] Eine gegenteilige Vorgehensweise ist etwa „Security by Obscurity“, also Sicherheit durch Verschleierung der verwendeten Verfahren.

[41] BSI: E-Government-Handbuch, Kapitel II, Modul „Verschlüsselung und Signatur“, S. 16 f.

Jahre als geeignet eingestuft werden. Zentral für die Eignung eines Signaturalgorithmus ist jeweils, dass aus dem öffentlichen Schlüssel nicht der private Schlüssel errechnet werden kann.

IV. Signaturerstellung

Grundsätzlich wird ein elektronisches Dokument signiert, indem der Aussteller das Dokument mit seinem privaten Schlüssel verschlüsselt. Der Empfänger kann das Dokument mit dem öffentlichen Schlüssel entschlüsseln und stellt damit sicher, dass das Dokument tatsächlich vom Aussteller und Schlüsselinhaber stammt. Die Daten sind authentisch, aber nicht vertraulich (wegen der Öffentlichkeit des Schlüssels zur Entschlüsselung).
Um noch einmal den Unterschied zur Verschlüsselung (zur Gewährleistung von Vertraulichkeit) zu verdeutlichen: Will der Aussteller eines elektronischen Dokuments, dass dieses vertraulich ist und tatsächlich nur vom vorgesehenen Empfänger gelesen werden kann, dann müsste der Aussteller das Dokument mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Nur der Empfänger ist im Besitz der „anderen Hälfte“ des Schlüsselpaares und kann damit die Nachricht entschlüsseln. Die Daten sind vertraulich, aber nicht authentisch (da der Aussteller keinen ihm zugeordneten Schlüssel verwendet, der ihn eindeutig als Aussteller ausweist).

V. Hashwert

Da das zu signierende Dokument sehr lang sein kann und damit auch der Signaturvorgang (zu) lange dauern würde, wird nicht das gesamt Originaldokument signiert, sondern zunächst ein Fingerabdruck (oder Hashwert) des Dokuments erstellt, der dann signiert wird. Das ursprüngliche Dokument wird mit der Signatur (dem signierten Hashwert) zusammen an den Empfänger übermittelt.
Das Hashverfahren muss zwei wesentliche Sicherheitsanforderungen erfüllen:

- Das Verfahren muss **kollisionsresistent** sein.

  Das bedeutet nicht, dass es keine zwei Dokumente geben darf, aus denen derselbe Hashwert gebildet wird. Das ist unmöglich bei einem derzeitigen Standard von 160 Bits für den Hashwert. Die Kollisionsresistenz verlangt nur, dass es praktisch unmöglich sein muss, zwei Eingaben zu **finden**, die auf den gleichen Hashwert abgebildet werden.

- Das Hashverfahren muss des Weiteren **irreversibel** sein.
  Aus einem Hashwert darf nicht die dem Hashwert zugrunde liegende Eingabe zurückgewonnen werden können.

Die in Deutschland als geeignet eingestuften Hashverfahren sind:

- SHA-1 (Secure Hash Algorithm)
- RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest)

Beide sind 160-Bit-Hashfunktionen, die für die nächsten sechs Jahre als sicher gelten. Die Hashfunktionen SHA-224, SHA-256, SHA-384 und SHA-512 mit jeweils entsprechender Bitzahl gelten auch längerfristig als sicher und damit geeignet.

VI. Signaturprüfung

Der Empfänger, der ein signiertes Dokument erhält, ermittelt zunächst den Hashwert des Dokuments. Mit dem öffentlichen Schlüssel des Absenders entschlüsselt er die Signatur. Damit wird die Person des Absenders eindeutig identifiziert. Nach der Entschlüsselung der Signatur verbleibt der Hashwert des Dokuments, so wie er beim Absender vor der Versendung gebildet wurde. Der Empfänger prüft die Übereinstimmung dieses Hashwerts mit dem von ihm gebildeten Hashwert: Stimmen beide überein, wurden die Daten nicht verändert. Das Dokument ist authentisch.

VII. Schlüsselmanagement

Unter dem Begriff Schlüsselmanagement können alle Verhaltensweisen und Maßnahmen zusammengefasst werden, die die Sicherheit von Schlüsseln gewährleisten. Hiervon umfasst sind etwa die Bereiche Generierung, Speicherung, Transport, Veröffentlichung, Sperrung, Wiedergewinnung nach Verlust, Nutzung und Vernichtung von Schlüsseln.

1. Sicherheit des privaten Schlüssels

Zentraler Aspekt für die Sicherheit des Private Key ist die Geheimhaltung. Als sichere Methode gilt derzeit die Erzeugung und Speicherung des Private Key auf einer Chipkarte, die wiederum durch eine PIN (Persönliche Identifikationsnummer), ein Passwort oder am besten durch eine Passphrase geschützt wird. Möglich ist auch die verschlüsselte Speicherung des Private Key auf der Festplatte oder einem sonstigen Medium.

Der Private Key muss auch vor Modifikationen geschützt werden. Wichtige Einzelaspekte sind etwa die Generierung starker Schlüssel, die sichere Speicherung und die zuverlässige Vernichtung, falls der Private Key nicht mehr genutzt werden soll.

2. Sicherheit des öffentlichen Schlüssels

Besondere Bedeutung gewinnt im Signaturrecht die erforderliche Gewährleistung der Zuordnung eines Public Key zu einem Absender. Hierzu gibt es im Wesentlichen zwei Optionen:

- **„Web of trust"**

Das System basiert auf der Möglichkeit der „Beglaubigung" fremder öffentlicher Schlüssel. Ist Teilnehmer X von der korrekten, unverfälschten Zuordnung eines öffentlichen Schlüssels zu einer Person Y überzeugt, spricht X durch die Beglaubigung des öffentlichen Schlüssels von Y diesem das Vertrauen aus. Möchte Z, der X kennt und vertraut, mit Y kommunizieren, kann er sich auf das Vertrauensnetz verlassen, das dadurch entsteht, dass Z dem X vertraut und X seinerseits dem Y vertraut. Da sich nur Teilnehmer des Verfahrens gegenseitig Zertifikate ausstellen und keine sonstige Stelle involviert ist, ist das „Web of trust"-Verfahren sehr kostengünstig. Daher wird es z.B. von der Open-Source-Kryptographie-Software OpenPGP (Pretty Good Privacy) genutzt Jedenfalls innerhalb einer kleineren Gruppe, deren Mitglieder sich untereinander kennen, kann das Verfahren als sicher angesehen werden, auch wenn nicht jeder Einzelne jedem anderen persönlich seinen öffentlichen Schlüssel übergeben hat. Für die Kommunikation mit unbekannten Dritten ist das Verfahren nur bedingt geeignet.

- **„Public Key Infrastruktur" (PKI)**

Die qualifizierte elektronische Signatur nach deutschem Recht greift auf eine eigene Infrastruktur zur Gewährleistung der Zuordnung des Public Key zurück: die Zertifizierungsdiensteanbieter (ZDA). Diese erfüllen zwei Aufgaben: Sie dienen als Zertifizierungsinstanz (*Certification Authority* – CA) und als Registrierungsinstanz (*Registration Authority* – RA).[42] Registrierung bedeutet dabei die Aufnahme und Prüfung von Teilnehmerdaten, Zertifizierung bedeutet die Ausstellung des Zertifikats.

§ 5 SigG [Vergabe von qualifizierten Zertifikaten]
(1) Der Zertifizierungsdiensteanbieter hat Personen, die ein qualifiziertes Zertifikat beantragen, zuverlässig zu identifizieren. (…)

[42] Hier soll im Folgenden – im Sinne besserer Verständlichkeit und Übersichtlichkeit - auf die Unterscheidung von Zertifizierungs- und Registrierungsinstanz verzichtet und einheitlich vom Zertifizierungsdienstanbieter gesprochen werden, da dieser beide Aufgaben ausführt.

§ 7 SigG [Inhalt von qualifizierten Zertifikaten]
(1) Ein qualifiziertes Zertifikat muss folgende Angaben enthalten und eine qualifizierte elektronische Signatur tragen:
1. den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit.mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muss,
2. den zugeordneten Signaturprüfschlüssel,
3. die Bezeichnung der Algorithmen, mit denen der Signaturprüfschlüssel des Signaturschlüssel-Inhabers sowie der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann,
4. die laufende Nummer des Zertifikates,
5. Beginn und Ende der Gültigkeit des Zertifikates,
6. den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist,
7. Angaben darüber, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt ist,
8. Angaben, dass es sich um ein qualifiziertes Zertifikat handelt, und
9. nach Bedarf Attribute des Signaturschlüssel-Inhabers.
(…)

Der Schlüsselinhaber wird durch den Zertifizierungsdiensteanbieter (ZDA) identifiziert und dieser stellt dann eine elektronische Bescheinigung, ein Zertifikat, aus, das auch den öffentlichen Schlüssel enthält. Das Zertifikat trägt seinerseits eine qualifizierte elektronische Signatur, die mittels des öffentlichen Schlüssels des Zertifizierungsdiensteanbieters überprüft werden kann. Der Empfänger muss also nur einem Zertifizierungsdiensteanbieter, die in Deutschland zudem staatlich kontrolliert werden, vertrauen. Zertifizierungsdiensteanbieter haben außerdem die Möglichkeit, ein staatliches Gütesiegel ausgestellt zu bekommen, wenn sie bei einer freiwilligen Sicherheitsüberprüfung den vorgesehenen Standards genügen (so genannte „freiwillige Akkreditierung“).

§ 15 SigG [Freiwillige Akkreditierung von Zertifizierungsdiensteanbietern]
(1) Zertifizierungsdiensteanbieter können sich auf Antrag von der zuständigen Behörde akkreditieren lassen; die zuständige Behörde kann sich bei der Akkreditierung privater Stellen bedienen. Die Akkreditierung ist zu erteilen, wenn der Zertifizierungsdiensteanbieter nachweist, dass die Vorschriften nach diesem Gesetz und der Rechtsverordnung nach § 24 erfüllt sind. Akkreditierte Zertifizierungsdiensteanbieter erhalten ein Gütezeichen der zuständigen Behörde. Mit diesem wird der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen (qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung) zum Ausdruck gebracht. Sie dürfen sich als akkreditierte Zertifizierungsdiensteanbieter bezeichnen und sich im Rechts- und Geschäftsverkehr auf die nachgewiesene Sicherheit berufen.
(2) Zur Erfüllung der Voraussetzungen nach Absatz 1 muss das Sicherheitskonzept nach § 4 Abs. 2 Satz 4 durch eine Stelle nach § 18 umfassend auf seine Eignung und praktische Umsetzung geprüft und bestätigt sein. Die Prüfung und Bestätigung ist nach sicherheitserheblichen Veränderungen sowie in regelmäßigen Zeitabständen zu wiederholen.
(…)

C. Parallelität der elektronischen Form mit Realworld-Dokumenten

Mit dem Formrechtsanpassungsgesetz hat der Gesetzgeber im Jahr 2001 für das bürgerliche Recht die elektronische Form der Schriftform gleichgestellt.

§ 126a Bürgerliches Gesetzbuch (BGB) [Elektronische Form]
(1) Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.
(2) Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren.

Die Schriftform verlangt die eigenhändige Unterschrift des Ausstellers oder ein notariell beglaubigtes Handzeichen.

§ 126 BGB [Schriftform]
(1) Ist durch Gesetz schriftliche Form vorgeschrieben, so muss die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden.
(…)

Nicht jede denkbare elektronische Form kann die Schriftform ersetzen. Erforderlich sind die Hinzufügung des Namens des Ausstellers und eine qualifizierte elektronische Signatur nach dem Signaturgesetz.

Im Öffentlichen Recht ist für Behörden ebenfalls die qualifizierte Signatur vorgeschrieben.

§ 3a Verwaltungsverfahrensgesetz [Elektronische Kommunikation]
(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.
(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, ist nicht zulässig.
(3) Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, hat sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück zu übermitteln.

Bisweilen lässt der Gesetzgeber die elektronische Form nicht zu.

§ 143 Hessische Gemeindeordnung (HGO) [Genehmigung]
(1) Die Genehmigung der Aufsichtsbehörde ist schriftlich zu erteilen; die elektronische Form ist ausgeschlossen. (…)

I. Qualifizierte elektronische Signatur

Die qualifizierte elektronische Signatur baut auf anderen, einfacheren Signaturformen auf.

„elektronische Signatur“	§ 2 Nr. 1 SigG	„Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“
„fortgeschrittene elektronische Signatur“	§ 2 Nr. 2 SigG	Signaturen nach Nr. 1, „die a) ausschließlich dem Schlüsselinhaber zugeordnet sind, b) die Identifizierung des Schlüsselinhabers ermöglichen, c) mit Mitteln erzeugt werden, die der Signaturschlüsselinhaber unter seiner alleinigen Kontrolle halten kann, und d) die mit den Daten auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann“
„qualifizierte elektronische Signatur“	§ 2 Nr. 3 SigG	Signaturen nach Nr. 2, „die a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und b) mit einer sicheren Signaturerstellungseinheit erzeugt werden“

II. Qualifizierte elektronische Signatur als Unterschriftssurrogat

Da die qualifizierte elektronische Signatur denselben Wert im Rechtsverkehr erhalten und dieselben Folgen nach sich ziehen soll wie die handschriftliche Unterschrift, muss sie die Funktionen der handschriftlichen Unterschrift im Rechtsverkehr ebenfalls erfüllen. Diese Parallelität zwischen elektronischer und handschriftlicher Signatur kann aufgrund der tatsächlichen Unterschiede zwischen beiden keine vollständige Gleichheit sein, sondern nur eine funktionelle Entsprechung. Folgende Funktionen des Schriftformerfordernisses lassen sich unterscheiden – wenn sie auch zum Teil eng miteinander verknüpft und nicht eindeutig gegeneinander abgrenzbar sind:

Entwurfsbegründung eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr[43]

- *Abschlussfunktion*

Die eigenhändige Unterschrift ist der räumliche Abschluss eines Textes und bringt zum Ausdruck, dass die Willenserklärung abgeschlossen ist. Dadurch wird das Stadium der Vorverhandlungen und des bloßen Entwurfs von dem der rechtlichen Bindung abgegrenzt.

- *Perpetuierungsfunktion*

Das Schriftformerfordernis führt dazu, dass die Unterschrift und vor allem der Text fortdauernd und lesbar in einer Urkunde wiedergegeben werden und einer dauerhaften Überprüfung zugänglich sind. Hierdurch wird gewährleistet, dass eine Information über die Erklärung nicht nur flüchtig möglich ist und die Erklärung dokumentiert werden kann.

- *Identitätsfunktion*

Durch die eigenhändige Namensunterschrift wird zum einen der Aussteller der Urkunde erkennbar. Darüber hinaus soll der Erklärende identifiziert werden können, weil die unverwechselbare Unterschrift eine unzweideutige Verbindung zur Person des Unterzeichners herstellt.

- *Echtheitsfunktion*

Die räumliche Verbindung der Unterschrift mit der Urkunde, die den Erklärungstext enthält, stellt einen Zusammenhang zwischen Dokument und Unterschrift her. Hierdurch soll gewährleistet werden, dass die Erklärung inhaltlich vom Unterzeichner herrührt.

- *Verifikationsfunktion*

Die Verifikationsfunktion steht im engen Zusammenhang mit der Echtheits- und der Identitätsfunktion. Sie wird dadurch erreicht, dass der Empfänger eines Dokuments die Möglichkeit hat zu überprüfen, ob die unverwechselbare Unterschrift echt ist, z. B. durch einen Unterschriftenvergleich.

- *Beweisfunktion*

Die eigenhändige Unterschrift unter einem fixierten Text dient dem Interesse an der Beweisführung und Offenlegung des Geschäftsinhalts und führt zu dauerhafter Klarheit. Die Schriftform erleichtert dem Beweispflichtigen seine Beweisführung, sofern der Beweisgegner die Echtheit der Unterschrift nicht bestreitet (§ 439 Abs. 1, 2, § 440 Abs. 1 ZPO).

- *Warnfunktion*

Durch den bewussten Akt des Unterzeichnens wird der Erklärende hingewiesen auf die erhöhte rechtliche Verbindlichkeit und die persönliche Zurechnung der unterzeichneten Erklärung. Hierdurch soll er vor übereilten Rechtsgeschäften geschützt werden.

(…)

Dabei hat der Gesetzgeber durchaus gesehen, dass es zwischen elektronischer und handschriftlicher Signatur Unterschiede in der Gewährleistung der verschiedenen Funktionen des Formerfordernisses gibt.

1. Abschlussfunktion

Die qualifizierte elektronische Signatur bezieht sich auf das gesamte zu signierende Dokument, da aus dem Gesamttext ein individueller Hashwert gebildet wird, der mit dem privaten Signaturschlüssel signiert wird. Eine nachträgliche Veränderung – auch durch den Aussteller

[43] Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, BT-Drucks 14/4987, S. 16.

selbst – ist nicht mehr möglich, ohne die Signatur ungültig werden zu lassen. Denn mit der Veränderung des zu signierenden Dokuments ändert sich der Hashwert des Dokuments.

2. Perpetuierungsfunktion

Ein elektronisch signiertes Dokument kann gespeichert werden und steht damit dauerhaft zur Verfügung – es kann jederzeit gelesen, ausgedruckt und überprüft werden. Zwar kann ein gespeichertes Dokument zerstört werden – dieses Risiko besteht bei der traditionellen Urkunde aber gleichermaßen.

3. Identitätsfunktion

Die elektronische Form verlangt zum einen, dass der Aussteller dem Text seinen Namen hinzufügt (§ 126a Abs. 1 BGB). Damit gibt der Aussteller selbst seine Identität an. Zum zweiten muss das qualifizierte Zertifikat des Zertifizierungsdiensteanbieters (ZDA), das für eine qualifizierte elektronische Signatur erforderlich ist, den Namen des Schlüsselinhabers enthalten (§ 7 Abs. 1 Nr. 1 SigG).

§ 7SigG [Inhalt von qualifizierten Zertifikaten]
(1) Ein qualifiziertes Zertifikat muss folgende Angaben enthalten und eine qualifizierte elektronische Signatur tragen:
1. den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muss,
(…)

Das Zertifikat für den öffentlichen Schlüssel darf erst nach erfolgter Identitätsprüfung erteilt werden. Allerdings wurde mit dem 1. Signaturrechtsänderungsgesetz die Möglichkeit geschaffen, zur Identifizierung auf bereits zu einem früheren Zeitpunkt erhobene personenbezogene Daten zurückzugreifen – soweit diese Daten eine zuverlässige Identifizierung gewährleisten. Dadurch entsteht in Verbindung mit anderen Änderungen[44] die Möglichkeit, ein qualifiziertes Zertifikat zu beantragen und zu erhalten, ohne dass es zu wenigstens einem persönlichen Kontakt zwischen Antragsteller und Zertifizierungsdiensteanbieter kommt. Die daraus resultierende Missbrauchsgefahr dürfte aber als gering anzusehen sein, da eine solche heimliche Erlangung eines Zertifikats unter fremdem Namen wohl nur von nahe stehenden Personen tatsächlich realisiert werden könnte (etwa das Abfangen der Post, die Signaturkarte oder zu-

[44] Die Belehrung des Antragstellers durch den Zertifizierungsdiensteanbieter muss nur noch in Textform übermittelt werden, während zuvor eine schriftliche Belehrung auszuhändigen war. Des Weiteren konnte zwar bereits nach früherer Rechtslage die gesetzlich vorgesehene persönliche Übergabe der Signaturkarte und die Übergabebestätigung durch eine andere Vereinbarung abgeändert werden – etwa zugunsten einer Versendung der Signaturkarte. Mit dem 1. Signaturrechtsänderungsgesetz ist aber für diese abändernde Vereinbarung keine Unterschrift oder qualifizierte elektronische Signatur mehr erforderlich.

gehörige PIN enthält). Die Sicherungsinfrastruktur erschwert einen Missbrauch derart, dass die Identitätsfunktion als gewährleistet angesehen werden kann. Schließlich kann auch die handschriftliche Unterschrift gefälscht werden.

4. Echtheitsfunktion

Über die Bildung eines Hashwerts für das Dokument vor der Signierung werden Dokument und Signatur miteinander verknüpft. Mittels des Vergleichs der Hashwerte (des übermittelten Dokuments einerseits und des in der Signatur verschlüsselten andererseits) kann jede nachträgliche Veränderung des Dokuments festgestellt werden. Die durch die qualifizierte elektronische Signatur gewährleistete Sicherheit der Authentizität der Erklärung übertrifft die Sicherheit der handschriftlichen Unterschrift in dieser Hinsicht deutlich.

5. Verifikationsfunktion

Mit der Entschlüsselung einer qualifiziert elektronischen Signatur mittels des Public Key steht fest, dass die Signatur tatsächlich mit dem Private Key des Ausstellers erstellt wurde, da öffentlicher und privater Schlüssel einander eindeutig zugeordnet sind.

6. Beweisfunktion

Die Beweiskraft von Dokumenten, die mit einer qualifizierten elektronischen Signatur versehen sind, entspricht zunächst der Beweiskraft von handschriftlich unterschriebenen privaten Urkunden (für öffentliche Urkunden gelten jeweils gesonderte Regelungen, auf die hier nicht näher eingegangen werden soll).[45]

§ 371a Zivilprozessordnung (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.

[45] Die Regelunge des § 371a ZPO gilt aber nicht nur im Zivilprozess, sondern über § 98 Verwaltungsgerichtsordnung (VwGO) auch im Verwaltungsprozess.

§ 416 ZPO [Beweiskraft von Privaturkunden]
Privaturkunden begründen, sofern sie von den Ausstellern unterschrieben oder mittels notariell beglaubigten Handzeichens unterzeichnet sind, vollen Beweis dafür, daß die in ihnen enthaltenen Erklärungen von den Ausstellern abgegeben sind.

Privaturkunden, die mit einer echten handschriftlichen Unterschrift versehen sind, kommt Beweiskraft darüber zu, dass die in der Urkunde enthaltene Erklärung genau so vom Aussteller abgegeben wurde. Diese Beweiskraft wird auch der mittels qualifizierter elektronischer Signatur unterzeichneten Erklärung gegeben.
Die Echtheit der handschriftlichen Unterschrift bzw. der qualifizierten elektronischen Signatur erlangt zentrale Bedeutung, da nur der echten Unterschrift und der echten Signatur diese Beweiskraft verliehen wurde. Bei der handschriftlichen Unterschrift ist die Echtheit von demjenigen, der sich auf die in der Urkunde enthaltene Erklärung berufen will, zu beweisen (§ 440 Abs. 1ZPO).

§ 440 ZPO Beweis der Echtheit von Privaturkunden
(1) Die Echtheit einer nicht anerkannten Privaturkunde ist zu beweisen.
(…)

Demgegenüber normiert § 371a Abs. 1 S. 2 ZPO einen Anscheinsbeweis für die Echtheit eines Dokuments, das mit einer korrekten qualifizierten elektronischen Signatur versehen wurde. Ein Anscheinsbeweis ist kein endgültiger, sondern nur ein vorläufiger Beweis. Hintergrund ist ein nach der Lebenserfahrung typischer Geschehensablauf, bei dessen Vorliegen auf eine bestimmte Folge oder Ursache geschlossen werden kann. Der in § 371a Abs. 1 S. 2 ZPO festgelegte Anscheinbeweis lautet also: Ist eine Erklärung mit der qualifizierten elektronischen Signatur des X versehen, kann darauf geschlossen werden, dass die Erklärung tatsächlich von X stammt. Kann der X dem gegenüber nichts vorbringen, bleibt es endgültig dabei, dass X im Prozess als Aussteller der Erklärung gilt. Andernfalls muss X Tatsachen vortragen, die einen anderen Geschehensablauf möglich erscheinen lassen. Dadurch wird der Anscheinsbeweis erschüttert und es kann nicht von der Verwendung der Signatur des X auf die Urheberschaft des X geschlossen werden.
Da für die Echtheit der Unterschrift auf einer Privaturkunde kein Anscheinsbeweis streitet, ist dies wie jede andere Tatsache auch mit den allgemein zugelassenen Beweismitteln[46] zu beweisen.

[46] FEX: Die allgemein zugelassenen Beweismittel sind Sachverständige, Augenschein, Parteivernehmung, Urkunde und Zeuge.

7. Warnfunktion

Die Zertifizierungsdiensteanbieter sind verpflichtet, bei der Antragstellung für eine qualifizierte elektronische Signatur auf die rechtliche Bedeutung und Wirkung der qualifizierten elektronischen Signatur hinzuweisen. Durch die notwendige Nutzung der Chipkarte und die Eingabe der PIN bei der Signaturerstellung ergibt sich mindestens im gleichen Maße wie bei der handschriftlichen Unterschrift ein Moment des Innehaltens, der dem Aussteller die Bedeutsamkeit seines Verhaltens vor Augen führt. Möglicherweise ist das Bewusstsein der rechtlichen Bedeutsamkeit bei einer handschriftlichen Unterschrift traditionell stärker vorhanden, während ein vergleichbares gesellschaftliches Bewusstsein für qualifizierte elektronische Signaturen erst noch erstarken muss.

D. Beispiel für die rechtliche Bedeutung von Signaturen: § 55aVwGO

Die Gleichstellung der elektronischen Form mit der traditionellen Schriftform auch für die (Verwaltungs-)Gerichtsbarkeit wurde bereits mit dem Formrechtsanpassungsgesetz begonnen, das mit der Einführung des damaligen § 86a Verwaltungsgerichtsordnung (VwGO) die prozessualen Formvorschriften etwa bei der Einreichung von Schriftsätzen bei Gericht für die elektronische Form öffnete. Mit dem Justizkommunikationsgesetz vom 22. März 2005[47] ersetzte der neu geschaffene § 55a VwGO die Vorgängernorm des § 86a VwGO a.F..

§ 55a VwGO [Elektronische Dokumentenübermittlung]
(1) Die Beteiligten können dem Gericht elektronische Dokumente übermitteln, soweit dies für den jeweiligen Zuständigkeitsbereich durch Rechtsverordnung der Bundesregierung oder der Landesregierungen zugelassen worden ist. Die Rechtsverordnung bestimmt den Zeitpunkt, von dem an Dokumente an ein Gericht elektronisch übermittelt werden können, sowie die Art und Weise, in der elektronische Dokumente einzureichen sind. Für Dokumente, die einem schriftlich zu unterzeichnenden Schriftstück gleichstehen, ist eine qualifizierte elektronische Signatur nach § 2 Nr. 3 des Signaturgesetzes vorzuschreiben. Neben der qualifizierten elektronischen Signatur kann auch ein anderes sicheres Verfahren zugelassen werden, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt. Die Landesregierungen können die Ermächtigung auf die für die Verwaltungsgerichtsbarkeit zuständigen obersten Landesbehörden übertragen. Die Zulassung der elektronischen Übermittlung kann auf einzelne Gerichte oder Verfahren beschränkt werden. Die Rechtsverordnung der Bundesregierung bedarf nicht der Zustimmung des Bundesrates.
(2) Ein elektronisches Dokument ist dem Gericht zugegangen, wenn es in der von der Rechtsverordnung nach Absatz 1 Satz 1 und 2 bestimmten Art und Weise übermittelt worden ist und wenn die für den Empfang bestimmte Einrichtung es aufgezeichnet hat. Die Vorschriften dieses Gesetzes über die Beifügung von Abschriften für die übrigen Beteiligten finden keine Anwendung. Genügt das Dokument nicht den Anforderungen, ist dies dem Absender unter

[47] Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG) vom 22.03.2005, BGBl. I 837.

Angabe der für das Gericht geltenden technischen Rahmenbedingungen unverzüglich mitzuteilen.
(3) Soweit eine handschriftliche Unterzeichnung durch den Richter oder den Urkundsbeamten der Geschäftsstelle vorgeschrieben ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn die verantwortenden Personen am Ende des Dokuments ihren Namen hinzufügen und das Dokument mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 des Signaturgesetzes versehen.

I. § 55a VwGO als Teil des „Puzzles“ E-Governance

§ 55a VwGO dient der Unterstützung von Electronic Governance Konzepten (E-Governance oder E-Government) auf Bundes- und Länderebene.[48] Die Option elektronischer Dokumentenübermittelung ist das entsprechende Gegenstück zu den Vorschriften zur elektronischen Zustellung (§ 174 Abs. 3 S. 3 ZPO, der über § 56 Abs. 2 VwGO auch für die Verwaltungsgerichtsbarkeit gilt). Ergänzt wird beides durch § 55b VwGO, der mit der Implementierung der elektronischen Aktenführung die Verwaltungsgerichte in die Lage versetzt, ein gerichtliches Verfahren vollständig auf elektronischem Weg abzuwickeln.[49]

§ 55b VwGO [Elektronische Aktenführung]
(1) Die Prozessakten können elektronisch geführt werden. Die Bundesregierung und die Landesregierungen bestimmen jeweils für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an die Prozessakten elektronisch geführt werden. In der Rechtsverordnung sind die organisatorisch-technischen Rahmenbedingungen für die Bildung, Führung und Verwahrung der elektronischen Akten festzulegen. Die Landesregierungen können die Ermächtigung auf die für die Verwaltungsgerichtsbarkeit zuständigen obersten Landesbehörden übertragen. Die Zulassung der elektronischen Akte kann auf einzelne Gerichte oder Verfahren beschränkt werden. Die Rechtsverordnung der Bundesregierung bedarf nicht der Zustimmung des Bundesrates.
(2) Dokumente, die nicht der Form entsprechen, in der die Akte geführt wird, sind in die entsprechende Form zu übertragen und in dieser Form zur Akte zu nehmen, soweit die Rechtsverordnung nach Absatz 1 nichts anderes bestimmt.
(3) Die Originaldokumente sind mindestens bis zum rechtskräftigen Abschluss des Verfahrens aufzubewahren.
(4) Ist ein in Papierform eingereichtes Dokument in ein elektronisches Dokument übertragen worden, muss dieses den Vermerk enthalten, wann und durch wen die Übertragung vorgenommen worden ist. Ist ein elektronisches Dokument in die Papierform überführt worden, muss der Ausdruck den Vermerk enthalten, welches Ergebnis die Integritätsprüfung des Dokuments ausweist, wen die Signaturprüfung als Inhaber der Signatur ausweist und welchen Zeitpunkt die Signaturprüfung für die Anbringung der Signatur ausweist.

[48] Siehe etwa die Initiative Deutschland-Online, die E-Government Strategien von Bund, Ländern und Kommunen bündeln und interoperabel gestalten will.
[49] Den §§ 55a, 55b VwGO entsprechende Vorschriften wurden etwa auch in die Finanzgerichtsordnung (§§ 52a, 52b FGO) und das Sozialgerichtsgesetz (§§ 65a, 65b SGG) eingefügt. Im Zivilprozess galt schon mit dem Formrechtsanpassungsgesetz der dem § 86a VwGO a.F. entsprechende § 130a ZPO. Mit dem JKomG wurde ebenfalls die elektronische Aktenführung zugelassen, § 298a ZPO. Schließlich erfolgte auch für den Strafprozess eine Öffnung für die elektronische Form, nach § 41a Strafprozessordnung (StPO) ist zunächst aber nur die Einreichung von elektronischen Dokumenten möglich.

(5) Dokumente, die nach Absatz 2 hergestellt sind, sind für das Verfahren zugrunde zu legen, soweit kein Anlass besteht, an der Übereinstimmung mit dem eingereichten Dokument zu zweifeln.

II. Grundsatz der Eröffnung von elektronischer Justizkommunikation (nur) durch Rechtsverordnung

Elektronischer Rechtsverkehr nach § 55a VwGO findet nur dort statt, wo der jeweilige Gesetzgeber dies ausdrücklich durch Rechtsverordnung[50] gestattet und näher ausgestaltet hat (§ 55a Abs. 1 S. 1 VwGO).[51] Auf Bundesebene gibt es bereits Rechtsverordnungen für den Bundesgerichtshof[52], das Marken- und Patentamt sowie den Bundesgerichtshof in Patent- und Markensachen[53] und das Bundesverwaltungsgericht wie den Bundesfinanzhof[54]. Hinsichtlich der auf Länderebene bestehenden Rechtsverordnungen[55] soll hier nur auf die Rechtslage in Hessen eingegangen werden: Mit Verordnung[56] vom 30.11.2005 wurde die Einreichung von elektronischen Dokumenten für alle Gerichte und Staatsanwaltschaften in Frankfurt am Main gestattet. Im Übrigen ist die Einreichung von Dokumente in elektronischer Form bei der hessischen Justiz noch nicht vorgesehen.

Die Rechtsverordnungen legen jeweils die zur Übermittlung zulässigen Dateiformate und die für die qualifizierte elektronische Signatur zu verwendende Software oder einzuhaltenden Standards fest. Teilweise werden weitere Regelungen getroffen, etwa über Verschlüsselungsmöglichkeiten, Dateigröße und/oder –anzahl, erwünschte Dateibenennung etc.

III. Qualität der Informationstechnik

1. Signaturerfordernis

§ 55a Abs. 1 S. 3 VwGO und § 55a Abs. 3 VwGO stellen dynamische Rechtsgrundverweisungen auf das Signaturgesetz dar. Beide Regelungen verlangen eine qualifizierte elektronische Signatur, eine (einfache) elektronische Signatur oder eine fortgeschrittene elektronische

[50] FEX: Rechtsverordnungen sind abstrakt-generelle Rechtssätze, die nicht von der Legislative, sondern von der Exekutive erlassen werde.
[51] Gleiches gilt sowohl für die elektronische Aktenführung nach § 55b VwGO als auch für alle übrigen soeben genannten prozessualen Normen, die elektronischen Rechtsverkehr ermöglichen.
[52] Verordnung über den elektronischen Rechtsverkehr beim Bundesgerichtshof (ERVVOBGH) vom 26.11.2001, BGBl. I 3225.
[53] Verordnung über den elektronischen Rechtsverkehr im gewerblichen Rechtsschutz (ERvGewRV) vom 05.08.2003, BGBl. I 1558.
[54] Verordnung über den elektronischen Rechtsverkehr beim Bundesverwaltungsgericht und beim Bundesfinanzhof (ERVVBVerGBFH) vom 26.11.2004, BGBl. I 3091.
[55] Übersicht über die weiteren bestehenden Rechtsverordnungen unter http://www.klagenpermail.de/.
[56] Verordnung über den elektronischen Rechtsverkehr bei den in der Stadt Frankfurt am Main ansässigen Gerichten und Staatsanwaltschaften vom 30.11.2005, GVBl. I 794.

Signatur reichen nicht aus. Hintergrund ist die Ersetzung der handschriftlichen Unterschrift. Der Gesetzgeber erkennt unter den drei Signaturtypen nur die qualifizierte elektronische Signatur (mit und ohne Anbieterakkreditierung) als funktionelle Entsprechung der handschriftlichen Unterschrift an.

2. „andere sichere Verfahren“ als Konkurrenz zum Signaturkanon?

§ 55a Abs. 1 S. 4 VwGO gestattet für Dokumente, die an das Gericht übermittelt werden sollen, neben der qualifizierten elektronischen Signatur auch die Nutzung „anderer sicherer Verfahren“ – wenn und soweit dies durch eine Rechtsverordnung zugelassen wird. Voraussetzung ist die Gewährleistung von Authentizität und Integrität der übermittelten Dokumente.[57] Bisher hat kein Verordnungsgeber die Option des § 55a Abs. 1 S. 4 VwGO genutzt. Insoweit bleibt die weitere Entwicklung abzuwarten. Jedenfalls ermöglicht § 55a Abs. 1 S. 4 VwGO erstmals die Zulassung eines mit dem Signaturensystem konkurrierenden Verfahrens. Die tatsächliche Existenz eines solchen anderen technisch sicheren Verfahrens jenseits des Signaturenkanons ist nicht per se ausgeschlossen: Zum einen besteht hinsichtlich der Sicherheitsbeurteilung ein Ermessensspielraum des Normgebers, der zu respektieren ist – gerade auch wegen der Komplexität der Beantwortung sicherheitsrelevanter Fragestellungen.

Zum Zweiten zeigen die diesbezüglichen Regelungen anderer Staaten, dass anderweitige technische und rechtliche Lösungen möglich sind. Österreich setzt etwa schon seit der Einführung des elektronischen Rechtsverkehrs 1990 auf ADV-Verfahren (automationsunterstützte zeichenweise Datenübertragung).[58] Zur Authentifizierung dient ein siebenstelliger Anschriftcode. Der Kreis der Teilnehmer am elektronischen Rechtsverkehr wurde zunächst auf Rechtsanwälte, Notare etc. beschränkt. Obwohl die Breitenwirkung des elektronischen Rechtsverkehrs auch nach der Öffnung für alle interessierten Personen beschränkt zu sein scheint, wird das Angebot stark in Anspruch genommen.[59]

Die Zulassung anderer sicherer Verfahren – für bestimmte Arten von Verfahren und/oder Dokumenten – könnte die Alltagspraktikabilität und damit die Akzeptanz und Verbreitung der elektronischen Form insgesamt erhöhen. Für eine genauere Differenzierung der (Sicherheits-)

---

[57] Siehe die Begründung zum Gesetzesentwurf der Bundesregierung für das JKomG, BR-Drucks 609/04, S. 87.

[58] Verordnung des Bundesministers für Justiz über den elektronischen Rechtsverkehr vom 04.12.1989, BGBl. Nr. 600/1989.

[59] Zahlen für das Jahr 2003 nach G. Viefhues, „Elektronischer Rechtsverkehr in Österreich - Schlussfolgerungen aus deutscher Sicht“, MMR 2004, 792 ff.: 85% der Eingaben bei den Zivilgerichten 1. Instanz wurden elektronisch übermittelt. Im Bereich der Vollstreckungsverfahren wurden 60 % elektronisch eingebracht. Die Gesamtzahl der elektronischen Sendungen im Jahr 2003 (sowohl an die Gerichte als auch von den Gerichten) lag bei 6,1 Mio. Dadurch wurden 2 Mio. € an Portokosten gespart.

Anforderungen bezüglich unterschiedlicher Verfahren/Dokumente/Beweisrelevanz etc. könnte auch Art. 5 Abs. 2 europäische Signaturrichtlinie sprechen.

Art. 5 europäische Signaturrichtlinie [Rechtswirkung elektronischer Signaturen]
(2) Die Mitgliedstaaten tragen dafür Sorge, daß einer elektronischen Signatur die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen wird,
- weil sie in elektronischer Form vorliegt oder
- nicht auf einem qualifizierten Zertifikat beruht oder
- nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder
- nicht von einer sicheren Signaturerstellungseinheit erstellt wurde.

Auch der (einfachen) elektronischen Signatur und der fortgeschrittenen elektronischen Signatur muss (irgendeine) rechtliche Wirkung zukommen und sie müssen grundsätzlich als Beweismittel zulässig sein. Würde im Zusammenhang mit der Zulassung der elektronischen Form stets eine qualifizierte elektronische Signatur gefordert, dann verbliebe für die beiden anderen Signaturtypen kein (Anwendungs-)Raum mehr.

3. Sicherung von Intimität

Auffallend ist, dass - so stark Identität, Integrität und Authentizität rechtlich geschützt werden - dem Schutz von Intimität so wenig Bedeutung beigemessen wird. Im Entwurfsverfahren (Referentenentwurf) zum JKomG[60] lautete § 55a Abs. 1 S. 2 VwGO noch

§ 55a VwGO
(1) (…) Daten, die nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden müssen, sind zu verschlüsseln. (…)

Im endgültigen Gesetzesentwurf war diese Regelung nicht mehr enthalten. In der Begründung des Gesetzesentwurfs wurde Verschlüsselung nur noch mit einem Satz erwähnt.[61] Eine denkbare Ursache hierfür könnte sein, dass Vertraulichkeit von Daten als datenschutzrechtliche Anforderung verstanden wird und nicht als Element von Datensicherheit begriffen wird. Dieses Verständnis mag mit der Betonung der Parallelität zur Schriftform zusammenhängen – wo sich die Frage des Schutzes der Datenintimität nicht in diesem Maße stellt.

[60] Referentenentwurf zum JKomG vom 14.04.2003.
[61] Entwurf eines Gesetzes über die Verwendung elektronischer Kommunikationsformen in der Justiz vom 28.10.2004, BT-Drucks 15/4067, S. 24.

E. Literaturhinweise

- C. Berger, Beweisführung mit elektronischen Dokumenten, NJW 2005, 1016
- C. Eckert, IT-Sicherheit, 2005
- S. Fischer-Dieskau: Der Referentenentwurf zum Justizkommunikationsgesetz aus Sicht des Signaturrechts MMR 2003, 701
- S. Fischer-Dieskau/A. Roßnagel/ R. Steidle, Beweisführung am seidenen Bit-String? – Die Langzeitaufbewahrung elektronischer Signaturen auf dem Prüfstand, MMR 2004, 451
- S. Hähnchen, Das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, NJW 2001, 2831
- Hessen Media, Bd. 42, Digitale Signatur (von H. Baier), 2003
- Lüdemann/N. Adams, Die elektronische Signatur in der Rechtspraxis, K&R 2002, 8
- P. Mankowski, Zum Nachweis des Zugangs bei elektronischen Erklärungen, NJW 2004, 1901
- A. Roßnagel, Das neue Recht elektronischer Signaturen – Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO, NJW 2001, 1817
- derselbe, Rechtliche Unterschiede von Signaturverfahren, MMR 2002, 215
- derselbe, Elektronische Signaturen mit der Bankkarte? – Das Erste Gesetz zur Änderung des Signaturgesetzes, NJW 2005, 385
- V. Schmid, Cyberlaw – eine neue Disziplin im Recht? Jahrbuch des Umwelt- und Technikrechts, Berlin, 2003, S. 449
- W.Viefhues, Sicherheitsaspekte bei der elektronischen Kommunikation zwischen Anwalt und Gericht, K&R 2002, 170
- derselbe, Das Gesetz übe die Verwendung der elektronischen Kommunikationsformen in der Justiz, NJW 2005, 1009
- N. Yildrim, Elektronische Signaturen in der öffentlichen Verwaltung, DVBl 2002, 241