Professor Dr. Alexander Roßnagel, Kassel/Saarbrücken*

Elektronische Signaturen mit der Bankkarte?

Das Erste Gesetz zur Änderung des Signaturgesetzes

Der Aufsatz wurde veröffentlicht in: Neue Juristische Wochenschrift, 58. Jg. (2005), Heft 7, 385 – 388.

Am 11.1.2005 trat das Erste Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) in Kraft. Es ermöglicht vor allem den Vertrieb von Signaturkarten im Fernabsatz. Damit soll Kreditinstituten erleichtert werden, Signaturverfahren mit ihren Bankkarten zu verbinden. Der Beitrag beschreibt die Bedeutung der neuen Regelungen für qualifizierte Signaturverfahren (I.), das Gesetzgebungsverfahren (II.), die wesentlichen Neuregelungen (III.) sowie die Folgen für Regelungen, die auf das Signaturgesetz Bezug nehmen (IV.). Ein kurzer Ausblick beschließt den Beitrag (V.).

I. Bedeutung der Neuregelungen

Elektronische Signaturen sind die Basistechnologie für den elektronischen Rechts- und Geschäftsverkehr. Nur mit ihrer Hilfe können Integrität und Authentizität elektronischer Daten nachgewiesen werden.[1] Soweit die Beweiseignung elektronischer Daten bedeutsam sein kann, sehen daher viele Rechtsvorschriften des Privat-,[2] Verwaltungs-[3] und Prozessrechts[4] qualifizierte elektronische Signaturen vor. Nur für qualifiziert signierte elektronische Dokumente erkennt das Recht eine Äquivalenz zur Schriftform an und sieht Beweiserleichterungen vor.[5]

Trotz dieser enormen Bedeutung werden qualifizierte elektronische Signaturen bisher nur für wenige IT-Anwendungen von bestimmten professionellen Kreisen genutzt. Eine breite Nutzung im elektronischen Geschäfts- und Verwaltungsverkehr konnte nicht erreicht werden. Diese Durchsetzungsschwäche besteht in der gesamten EU.[6] Deutschland ist noch das Land, das den weitesten Durchbruch erzielt hat. Da der rechtliche Rahmen in den Mitgliedstaaten – soweit die Signaturrichtlinie dies zulässt – sehr unterschiedlich ist, dürfte dies nicht dem jeweiligen Rechtsrahmen anzulasten sein. Vielmehr liegt es an ungeeigneten Geschäftsmodellen und vor allem einer Verkennung des gesamtwirtschaftlichen Infrastrukturcharakters elektronischer Signaturverfahren.[7]

Um elektronische Signaturen zu fördern und hierfür ihre Aktivitäten zu koordinieren, haben am 3.4.2003 vier Bundesministerien zusammen mit einigen kartenausgebenden Organisationen ein „Signaturbündnis“ gegründet, dem seitdem weitere Unternehmen und Organisationen

---

* Der Autor ist Universitätsprofessor für öffentliches Recht und Vizepräsident der Universität Kassel, Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR) in Saarbrücken.

1 S. z.B. *Roßnagel*, in: ders. (Hrsg.), Recht der Multimediadienste, 1999, 6. EL 2004, Einl. ins SigG, Rn. 7 ff.

2 S. FormanpassG v. 13.7.2001, BGBl. I, S. 1542; näher *Roßnagel*, NJW 2001, 1817.

3 S. 3. VwVfÄG v. 21.8.2002, BGBl. I, S. 3322; näher *Roßnagel*, NJW 2003, 469.

4 S. RegE für ein JKomG vom 28.10.2004, BT-Drs. 15/4067.

5 S. ausf. Nachw. in *Roßnagel* (Fn. 1), Rn. 277- 307.

6 S. Bericht zur Evaluation der Richtlinie von *Dumortier et al*., The Legal and Market Aspects of Electronic Signatures, 2003, sowie die Übersicht in *Roßnagel* (Fn. 1), Rn. 239 ff.

7 S. z.B. *Roßnagel*, MMR 2003, 1f.; *Gesellschaft für Informatik/Informationstechnische Gesellschaft*, DuD 2003, 763.

beigetreten sind.[8] In dessen Rahmen wurde intensiv diskutiert, wie die vorhandenen Karteninfrastrukturen für die weitere Verbreitung von Signaturverfahren genutzt werden könnten[9] und welche Anforderungen des SigG und der SigV dafür den Prozessabläufen für die Ausgabe von Bankkarten angeglichen werden müssten.[10]

Das 1. SigGÄndG passt das SigG den Bedingungen der Kreditinstitute an. Um die „im Wirtschaftsleben bereits seit langem eingeführten und bewährten Verfahrensprozesse z.B. bei der Registrierung und Ausgabe von EC-, Bankkunden- oder Versichertenkarten auch für die Ausgabe von Signaturkarten mit qualifizierten elektronischen Zertifikaten mit den entsprechenden Synergieeffekten (Verwaltungsvereinfachung, Kostenreduzierung)“ nutzen zu können,[11] werden Vorschriften, die diesen Verfahrensprozessen entgegenstanden, so abgeändert, dass die Beantragung und Ausgabe von Signaturkarten ohne persönlichen Kontakt und ohne Unterschrift möglich ist. Dadurch soll ein durchgängig elektronischer Verfahrensprozess für Antrag und Ausgabe von Signaturkarten ermöglicht werden. Außerdem wird die Bedingung der Kreditinstitute erfüllt, das von ihnen favorisierte Gültigkeitsmodell durchsetzen zu können. Mit dieser Anpassung verbindet die Bundesregierung die Hoffnung, mit Hilfe der Kreditinstitute Signaturverfahren so zu vervielfachen, dass der elektronische Geschäfts-, Verwaltungs- und Gerichtsverkehr auf diese aufsetzen kann.[12]

II. Das Gesetzgebungsverfahren

Nach umfangreichen Abstimmungen im Signaturbündnis legte das Bundesministerium für Wirtschaft und Arbeit am 1.4.2004 einen Referentenentwurf vor.[13] Ohne formelle Beteiligung der Öffentlichkeit folgte bereits am 30.4.2004 der Gesetzentwurf der Bundesregierung.[14] Nach der Stellungnahme des Bundesrats[15] und der Gegenäußerung der Bundesregierung[16] wurde der Gesetzentwurf am 24.6.2004 in den Bundestag eingebracht. Er wurde in erster Lesung federführend an den Ausschuss für Wirtschaft und Arbeit und mitberatend an den Innenausschuss, den Rechtsausschuss, den Ausschuss für Gesundheit und Soziale Sicherung und den Ausschuss für Kultur und Medien überwiesen. In den Ausschussberatungen wurden von den Koalitionsfraktionen Bedenken von Datenschützern, Verbraucherschützern und Notaren[17] aufgegriffen, die eine Behinderung im Erwerb pseudonymer Zertifikate, eine unsichere Identifizierung und eine unzureichende Aufklärung der Signaturschlüssel-Inhaber bemängelten.[18] Diese führten in den Ausschussempfehlungen zu Änderungen hinsichtlich der Identifizierung und Belehrung der Antragsteller für ein Zertifikat sowie zur Beibehaltung des Anspruchs auf ein pseudonymes Zertifikat.[19] Am 12.11.2004 verabschiedete der Bundestag das Gesetz ohne

---

8 S. www.signaturbuendnis.de: z.Z. 7 Ministerien und Behörden, 7 Verbände, 25 Unternehmen.

9 Zu den technischen Voraussetzungen s. *Zitzelsberger/Hogen*, DuD 2002, 271.

10 S. zur Sicht der Kreditinstitute *Bürger/Esslinger/Koy*, DuD 2004, 133.

11 Breg., BT-Drs. 15/3417, S. 6.

12 Breg., BT-Drs. 15/3417, S. 6.

13 S. zu diesem *Skrobotz*, DuD 2004, 410.

14 BR-Drs. 327/04; BT-Drs. 15/3417.

15 BT-Drs. 15/3417, S. 9.

16 BT-Drs. 15/3417, S. 10.

17 S. z.B. MMR 11/2004, Vf.

18 Ausschuss für Wirtschaft und Arbeit, Drs. 15(9)1499.

19 BT-Drs. 15/3471.

größere Aussprache[20] und am 26.11.2004 der Bundesrat.[21] Das 1. SigÄndG vom 4.1.2005 wurde am 10.1.2005 verkündet[22] und trat am 11.1.2005 in Kraft.

III. Die Änderungen des SigG und der SigV

Diese „kleine" Novelle[23] verfolgt letztlich zwei Ziele. Zum einen sollen eine „zügige Beantragung und Ausgabe von Signaturkarten" ermöglicht und weitere Voraussetzungen für ein Engagement der Kreditwirtschaft im Signaturmarkt geschaffen werden. Zum anderen sollen einige ‚Handwerksfehler' beseitigt werden, die sich im Gesetzesvollzug gezeigt haben.

1. Beantragung und Ausgabe einer Signaturkarte

Nach bisherigem Signaturrecht forderte die Beantragung und Ausgabe einer Signaturkarte folgende Schritte: Nach § 5 I SigG setzt die Ausgabe einer Signaturkarte einen Antrag voraus, dessen Form aber nicht vorgeschrieben ist.[24] Der Antragsteller ist nach § 3 I SigV an Hand eines Ausweises zu identifizieren. Zur Unterrichtung des Antragstellers über Rechts- und Sicherheitsfragen nach § 6 SigG ist ihm eine schriftliche Belehrung auszuhändigen. Deren Kenntnisnahme hat er nach § 6 III 1 SigG schriftlich zu bestätigen. Die auf ihn personalisierte Signaturkarte ist ihm nach § 5 II SigV persönlich zu übergeben und die Übergabe ist von ihm schriftlich oder mit qualifizierter elektronischer Signatur zu bestätigen. Im Regelfall waren somit persönliche Kontakte bei der Identifizierung, der Übergabe der Belehrung und der Kartenausgabe sowie eigenhändige Unterschriften zur Bestätigung, dass die Belehrung zur Kenntnis genommen und die Karte übergeben worden ist, notwendig. Um einen durchgängig elektronischen Antrags- und Ausgabeprozess zu ermöglichen,[25] wurden diese Erfordernisse in folgender Weise verändert:

Nach § 5 I 1 SigG wurde ein Satz eingefügt, der mit Einwilligung des Antragstellers[26] dem Zertifizierungsdiensteanbieter ermöglicht, auf – bei Kreditinstituten etwa nach § 154 AO oder §§ 2 und 9 GeldwäscheG – bereits vorliegende Identifizierungsdaten zurückzugreifen.[27] Dies ist allerdings an die Bedingung geknüpft, dass „diese Daten eine zuverlässige Identifizierung des Antragstellers gewährleisten". Dies ist dann der Fall, wenn die Daten entsprechend § 3 I SigV an Hand eines gültigen Ausweises erhoben worden[28] und noch aktuell sind.[29] Eine persönliche Mitwirkung ist für die Identifizierung des Antragstellers nicht mehr notwendig. Hierfür soll zum Beispiel ein mittels PIN und TAN gesicherter elektronischer Antrag genügen.[30]

Um die Übergabe der Belehrung zu vermeiden, sieht § 6 III 1 SigG nun vor, die Belehrung in Textform zu übermitteln. Um die schriftliche Bestätigung ihrer Kenntnisnahme zu beseitigen,

---

20 Sten.Ber. 15/12830f.

21 BR-Drs. 931/04 (Beschluss).

22 G v. 4.1.2005, BGBl. I, S. 2.

23 BT-Drs. 15/3417, S. 6.

24 Der Maßnahmekatalog für Zertifizierungsstellen der Regulierungsbehörde vom 15.7.1998 forderte eine Unterschrift.

25 S. die Forderung von *Bürger/Esslinger/Koy*, DuD 2004, 133, 138.

26 Zu datenschutzrechtlichen Bedenken ohne Einwilligung s. z.B. *Püschel*, ZBB 2002, 186.

27 Dies wurde vom BR, BT-Drs. 15/3417, S. 9, und von BT-Ausschüssen, BT-Drs. 15/4172, S. 4, gefordert, die Bundesregierung hielt dies schon nach bisherigen Recht für zulässig, BT-Drs. 15/3417, 10.

28 Dies wird auch von § 1 V GeldwäscheG gefordert.

29 BT-Drs. 15/4172, S. 4.

30 Deren Sicherheit bitten allerdings die BT-Ausschüsse zu evaluieren, BT-Drs. 15/4172, S. 3; zu Phishing-Angriffen s. z.B. *Popp*, NJW 2004, 3517 m.w.Nachw.

wollte der Regierungsentwurf diese Anforderung streichen.[31] Der Bundestag hielt jedoch an der in der Bestätigung liegenden Warnfunktion für den Verbraucher fest. Um eine Bestätigung z.B. durch E-Mail zu ermöglichen, forderte er für diese jedoch nur Textform nach § 126b BGB.[32]

Die Übergabe der Signaturkarte und deren handschriftliche Bestätigung konnte bereits bisher dadurch umgangen werden, dass der Zertifizierungsdiensteanbieter mit dem Antragsteller eine andere Übergabe vereinbart. Hierfür war jedoch eine eigenhändige oder signierte Vereinbarung erforderlich. Diese Formvorgabe entfällt nun im geänderten § 5 II 1 SigV.

Nach diesen Änderungen kann etwa zu einer bereits beim Nutzer vorhandenen vorpersonalisierten Bankkarte mit Hilfe einer Webanwendung ein Zertifikat beantragt werden, indem sich der Antragsteller per PIN und TAN ausweist. Bei dieser Gelegenheit wird die Belehrung als Datei zur Verfügung gestellt, die Einwilligung zur Verwendung vorhandener Identifizierungsdaten eingeholt[33] und eine andere Art der Übergabe vereinbart. Die Übergabe der bereits vorhandenen Karte wird durch Versenden des PIN-Briefs und durch einen Download des Zertifikats vervollständigt.[34] Deren Empfang und die Kenntnisnahme der Belehrung bestätigt der Antragsteller per E-Mail.

Sofern es sich um eine Bestellung durch einen Verbraucher handelt, unterfällt diese Form des Vertragsabschlusses allerdings den Regeln über Fernabsatzverträge nach §§ 312b – e BGB.[35] Für sie gelten die Informationspflichten nach §§ 312c und e BGB sowie der BGB-InfoV, die Bestätigungs- und Gestaltungspflichten nach § 312e BGB und das Widerrufsrechts nach § 312d BGB.[36]

2. Gültigkeitsmodell

Für die Sperrung eines Zertifikats sind bisher in § 8 I SigG vier Gründe vorgesehen. Aufgrund eines neuen Satzes 2 können nun die Zertifizierungsdiensteanbieter weitere Sperrgründe vertraglich vereinbaren. Da die Kreditinstitute ein anderes Gültigkeitsmodell (Schalenmodell) für ihre Zertifikate praktizieren wollen,[37] als die Regulierungsbehörde fordert[38] und die bereits tätigen Zertifizierungsdiensteanbieter praktizieren (Kettenmodell), soll diese Regelung vor allem den Kreditinstituten ermöglichen, das ihnen passende Gültigkeitsmodell mit den daraus sich ergebenden Sperrmöglichkeiten zu vereinbaren.[39] Allerdings stellt die Regierungsbegründung klar, dass auch das von den Kreditinstituten favorisierte modifizierte Schalenmodell nur in der Form zulässig ist, in der es die aus § 19 V SigG sich ergebende Anforderung erfüllt, dass eine Signatur dann gültig ist, wenn zum Zeitpunkt ihrer Erzeugung und nicht ihrer Prüfung das Schlüsselzertifikat gültig war.[40]

---

31 BT-Drs. 15/3417, S. 8.

32 BT-Drs. 15/4172, S. 4; ebenso BR, BT-Drs. 15/3417, S. 9. Eine Pflicht zur Eingangsbestätigung des Antrags besteht nach § 312e I Nr. 3 BGB.

33 Ob dies als datenschutzrechtliche Einwilligung nach § 4a BDSG ausreicht, erscheint jedoch fraglich.

34 Oder es werden Karte und PIN-Brief getrennt übersandt.

35 S. zu den Voraussetzungen *Brönneke*, in Roßnagel (Fn. 1), § 312b BGB, Rn. 39 ff.

36 S. hierzu auch BT-Drs. 15/3417, 7f.

37 *Bürger/Esslinger/Koy*, DuD 2004, 138: ein modifiziertes Schalenmodell, das zwar zum Signaturzeitpunkt prüft, aber zur Ungültigkeit einer Signatur gelangt, wenn das CA- oder Root-Zertifikat ungültig ist. Dies erfordert einen zusätzlichen Sperrgrund.

38 *Regulierungsbehörde*, www.regtp.de →Elektronische Signatur→FAQ, Frage 14.

39 Dies übersieht *Skrobotz*, DuD 2004, 412.

40 S. BT-Drs. 15/3417, 8.

3. Pseudonyme Zertifikate

Nach § 5 III 1 SigG hat der Zertifizierungsdiensteanbieter auf Verlangen des Antragstellers in einem qualifizierten Zertifikat an Stelle seines Namens ein Pseudonym aufzuführen. Diese Regelung räumt dem Antragsteller die Möglichkeit ein, ein Pseudonym zu verwenden, um sich gegen das Erstellen von Persönlichkeitsprofilen zu schützen. Da diese Vorschrift entsprechend ihrem Wortlaut einen Rechtsanspruch gewährleistet,[41] die Kreditinstitute einem solchen Anspruch aber nicht ausgesetzt sein wollten,[42] schlug der Regierungsentwurf vor, die Verpflichtung zu Erteilung von Pseudonymen dadurch zu beseitigen, dass § 5 III 1 SigG um den Halbsatz, „soweit vertraglich nichts anderes bestimmt ist", ergänzt wird.[43] Dadurch hätte das in § 3a BDSG, § 4 VI TDDSG und § 18 VI MDStV verfolgte Konzept des Selbstdatenschutzes durch pseudonymes Handeln,[44] einen herben Rückschlag erfahren. Die Möglichkeit einer breiten Verwendung von Pseudonymen ist jedoch verfassungsrechtlich der notwendige Ausgleich für den Aufbau einer umfassenden Identifizierungsinfrastruktur durch elektronische Signaturen.[45] In den Ausschussberatungen wurde diese Änderung gestrichen. Es bleibt bei der Verpflichtung zur Ausstellung eines Zertifikats auf ein Pseudonym, wenn der Signaturschlüssel-Inhaber dies beantragt.

4. Auskunft über Zertifikatinhaber

Das Zertifikat enthält nach § 7 I Nr. 1 SigG nur den Namen oder das Pseudonym des Signaturschlüssel-Inhabers. Aus ihm lässt sich dessen vollständige Identität – insbesondere bei Namensgleichheit – nicht ersehen. In § 14 II 1 SigG war bisher geregelt, dass die dort genannten staatlichen Stellen von Zertifizierungsdiensteanbietern Angaben über die Identität eines Signaturschlüssel-Inhabers anfordern konnten, wenn das Zertifikat auf ein Pseudonym ausgestellt war – nicht aber, wenn es auf einen echten Namen lautete.[46] Diese systematische Ungereimtheit wird nun beseitigt. Für den Umfang der Identitätsdaten gilt das Erforderlichkeitsprinzip, es sind grundsätzlich nur Name, Geburtsdatum und Anschrift zu übermitteln, weitere Daten (z.B. Attribute) nur, wenn es für die Aufgabenerfüllung der Behörden unumgänglich ist.

Der Regierungsentwurf sah vor, dass die Auskunft unentgeltlich sein sollte. Der Bundestag beschloss jedoch, das Wort „unentgeltlich" zu streichen, weil durch die Erweiterung der Auskunftspflichten erhebliche Kosten entstehen können. Angemessene Entschädigungen sollen im Kontext einer umfassenden Regelung nach § 110 IX TKG festgelegt werden.[47] Dies wird verhindern, dass der Auskunftsanspruch zu extensiv genutzt wird.

5. Definition des Signaturschlüssel-Inhabers

Bei der Umsetzung der Signaturrichtlinie in das neue SigG ist die Definition des Signaturschlüssel-Inhabers in § 2 Nr. 9 so gewählt worden, dass sie auch für fortgeschrittene elektronische Signaturen gilt, für diese aber systemwidrig ein qualifiziertes Zertifikat voraussetzt.[48]

---

41 S. *Roßnagel* (Fn. 1), § 5 SigG 1997, Rn. 42.

42 S. *Bürger/Esslinger/Koy*, DuD 2004, 136.

43 Breg., BT-Drs. 15/3417, S. 7, nennt dies eine „Klarstellung".

44 S. *Roßnagel*, Konzepte des Selbstdatenschutzes, in: *ders*. (Hrsg.), HB Datenschutzrecht, 2003, S. 344 ff.

45 S. *Roßnagel/Wedde/Hammer/Pordesch,* Digitalisierung der Grundrechte, 1990, S. 240 ff.; *Bäumler,* in: Langenbach/Ulrich (Hrsg.), Elektronische Signaturen, 2002, S. 113 ff.; *Roßnagel* (Fn. 1), Rn. 316.

46 S. hierzu *Roßnagel*, Datenschutz in Signaturverfahren, in: *ders*. (Fn. 44), S. 1246.

47 BT-Drs. 15/4172, 4.

48 Zum Unterschied fortgeschrittener und qualifizierter Signaturen s. *Roßnagel*, MMR 2002, 215.

Da dies weder der Richtlinie entspricht noch so vom Gesetzgeber gemeint war, wurde dieser Fehler nun durch eine neue Definition in § 2 Nr. 9 SigG korrigiert.

6. Definition der zuständigen Behörde

In § 3 wurde die für das SigG zuständige Behörde bisher als die „Behörde nach § 66 TKG" bezeichnet. Um künftig von Änderungen des TKG unabhängig zu sein, wurde diese Bezeichnung in „Regulierungsbehörde für Telekommunikation und Post" geändert. Außerdem wurde der Verweis auf die Vorschriften für akkreditierte Zertifizierungsdiensteanbieter für die Vergabe von qualifizierten Zertifikate in § 16 I 2 SigG auch auf deren Sperrung ausgedehnt.

7. Hinterlegung der Herstellererklärung

Nach § 17 IV 2 SigG genügt für den Nachweis der Gesetzeskonformität bestimmter Produkte für elektronische Signaturen eine entsprechende Erklärung des Herstellers. Um die Aufsicht der Regulierungsbehörde über solche Produkte sicherzustellen, verpflichtet ein neuer Satz 3 die Hersteller, eine Ausfertigung ihrer Erklärung bei der Behörde zu hinterlegen. Erklärungen, die den Anforderungen des SigG und der SigV entsprechen, werden zum Schutz der Hersteller und Nutzer im Amtsblatt der Regulierungsbehörde veröffentlicht.

IV. Folgen der Neuregelungen

Die Bundesregierung versicherte, mit dem 1. SigÄndG sei „nicht beabsichtigt, systematische Änderungen des SigG vorzunehmen".[49] Angesichts des Konzeptwechsels beim Beantragungs- und Ausgabeprozess ist dennoch zu fragen, ob diese nachträglichen Gesetzesänderungen Auswirkungen auf Vorschriften haben, die bereits auf das SigG verweisen und das bisher geforderte Sicherheitsniveau des Identifizierungs- und Ausgabeprozesses voraussetzen.

Zu recht weisen die Bundestagsausschüsse darauf hin, dass es, „um die Sicherheit von qualifizierten elektronischen Signaturen auch langfristig sicherzustellen und angesichts der Rechtsfolgen, die sich aus dem Einsatz qualifizierter Signaturen ergeben können, insbesondere notwendig (ist), Verfahren zur zuverlässigen Identifizierung des Antragstellers zu entwickeln".[50] Während die Integrität signierter Daten technisch durch kryptographische Mechanismen gesichert werden kann, hängt deren Authentizität entscheidend von der organisatorischen Sicherheit des Identifizierungs- und Übergabeprozesses ab.

Um diese zu gewährleisten, sahen das SigG und die SiGV die gesicherte persönliche Mitwirkung bei der Identifizierung und Übergabe vor. Um auch noch nach Jahren oder Jahrzehnten die Einhaltung dieser Anforderungen überprüfen zu können, war die Kopie des aktuell geprüften Ausweises sowie die eigenhändig unterschriebene Bestätigung der Übergabe und der Kenntnisnahme der Belehrung zur Dokumentation nach § 10 SigG zu nehmen. Damit war die Identität in der virtuellen Welt durch mehrere – nachweisbare – Kontakte mit der Identität in der körperlichen Welt verknüpft. Auf diese Garantien bauten die Regelungen zur Schriftformäquivalenz der qualifizierten Signatur (z.B. § 126 III BGB, § 3a II VwVfG, § 87a III, IV AO und § 36a II SGB I) sowie die in allen Prozessordnungen geltende Beweiserleichterung des § 292a ZPO auf.

Die Frage ist berechtigt, ob all diese Kontakte zwischen der körperlichen und der virtuellen Welt und ihre urkundlichen Nachweise erforderlich sind, um die Rechtsfolgen der Formäquivalenz und des vorweggenommenen Anscheinsbeweises zu rechtfertigen. Aber ebenso ist die Frage berechtigt, ob diese Rechtsfolgen noch zu rechtfertigen sind, wenn auf alle diese Kontakte und Nachweise für das ohnehin schwächste Glied in der Sicherheitskette der elektroni-

---

[49] BT-Drs. 15/3417, 6.

[50] BT-Drs. 15/4172, 3.

sche Signatur verzichtet wird und die Voraussetzung für eine virtuelle Identität ausschließlich an virtuelle Aktionen geknüpft wird.[51] Kann durch solche Prozesse und Nachweise noch die tatsächliche Identität des Inhabers eines Signaturschlüssels gewährleistet und bestätigt werden? Zweifel daran sind angebracht: Nehmen wir die Beispiele des Ehemannes kurz vor einer Trennung oder des Pflegers einer älteren Dame.[52] Er kennt ihre persönlichen Daten, PIN und TAN oder kann sie sich ebenso wie die Bankkarte beschaffen. Er beantragt für sie ein Zertifikat und bestätigt den Antrag und alle Vereinbarungen mit ihren TAN. Das Kreditinstitut greift auf ihre vor mehreren Jahren erhobenen Identifikationsdaten zurück und stellt ein Zertifikat aus, das er auf ihre Bankkarte lädt. Der PIN-Brief[53] wird per Post zugeschickt und von ihm abgefangen. Den Empfang der PIN und die Kenntnisnahme der Belehrung bestätigt er mit einer E-Mail von ihrem Account aus. Danach regelt er mit ihrer Karte ihre Vermögensverhältnisse zu seinen Gunsten. Haben die Ehefrau oder die Erben der alten Dame eine Chance, sich zu wehren?

Da der Gesetzgeber des 1. SigÄndG sich der Rechtsfolgen qualifizierter Signaturen bewusst war und diese weiterhin wollte, als er die Sicherheitsanforderungen an den Identifizierungs- und Ausgabeprozess senkte, ist davon auszugehen, dass die Rechtsfolgen auch gelten, wenn es sich um diese in ihrem Sicherheitsniveau veränderten qualifizierten elektronischen Signaturen handelt. Dies gilt jedenfalls hinsichtlich ihrer Formäquivalenz[54] und grundsätzlich auch hinsichtlich des Anscheins der Echtheit nach § 292a ZPO. Etwas anderes ist jedoch anzunehmen, soweit der Gesetzgeber Rechtsfolgen ausdrücklich vom Vorliegen „ernstlicher Zweifel" an der Authentizität des Signierenden abhängig macht. Dies ist für den Anscheinsbeweis nach § 292a ZPO der Fall. Aufgrund systematischer Defizite des Identifizierungs- und Übergabeprozesses und mangels prüfbarer Nachweise und bezeugbarer Kontakte dürfte es einem Gericht leichter fallen, ernstliche Zweifel zu hegen, wenn die Urheberschaft einer signierten Erklärung mit guten Gründen bestritten wird. Entfällt der Anschein des § 292a ZPO, ist der Beweiswert einer signierten Erklärung nach § 286 ZPO zu bestimmen. Dieser hängt jedoch wesentlich von der durch den Identifizierungs- und Ausgabeprozess gewährleisteten Sicherheit der Zuordnung des Signaturschlüssels zum Erklärenden ab. Er ist ohne eine gesicherte persönliche Mitwirkung des Erklärenden deutlich geringer.

Den künftigen Zertifizierungsdiensteanbietern ist daher zu empfehlen, – schon zur Vermeidung einer Haftung nach § 11 I SigG für ein Falschzertifizierung – in ihren Ablaufprozessen wenigstens *einen* gesicherten persönlichen Kontakt mit dem Antragsteller vorzusehen und dabei eine Unterschrift von ihm einzuholen.[55]

V. Die Zukunft elektronischer Signaturverfahren

Der Gesetzgeber ist mit dem 1. SigÄndG der Kreditwirtschaft sehr weit entgegen gekommen.[56] Er hat damit den Beantragungs- und Ausgabeprozess erleichtert. Nun wird sich zeigen müssen, ob dies tatsächlich das Engagement der Kreditwirtschaft und den Erfolg in der Verbreitung von Signaturverfahren so erhöht, dass es zumindest in dieser Hinsicht das Risiko einer Reduzierung des Sicherheitsniveaus qualifizierter elektronischer Signaturen wert war.

---

51 Schon bisher bestanden erhebliche Zweifel an der Rechtfertigung – s. z.B. BR, BT-Drs. 14/4987, S. 36f.; *Roßnagel*, MMR 2000, 459; *Gesellschaft für Informatik*, DuD 2001, 38.

52 Ähnliches gilt für Familienangehörige oder Arbeitskollegen.

53 Falls nicht die vorhandene Bankkarte aktiviert wird, wird die Signaturkarte mit getrennter Post zugeschickt.

54 Auch wenn die Zuordnung nicht nachprüfbar ist wie bei einer eigenhändigen Unterschrift.

55 Die mit einer bei Kontoeröffnung hinterlegten Unterschrift verglichen werden kann.

56 S. auch *Skrobotz*, DuD 2004, 410.

Zweifel daran sind angebracht. Zum einen sind die beseitigten Sicherheitsanker nicht der Grund für die geringe Verbreitung. Diese liegen vielmehr im Fehlen eines gerechten Kosten(verteilungs)modells, in der mangelnden Ausgestaltung der Signaturverfahren als eine einheitliche Infrastruktur und in der fehlenden Koordinierung der verschiedenen Anwendungen für Signaturen. Zum anderen sind andere Initiativen der Bundesregierung viel Erfolg versprechender. Dies gilt einmal für das Anwendungsprojekt JobCard, das für die Funktion als Zugangsinstrument zu den zentral gespeicherten Verdienstnachweisen eines Antragstellers auf Arbeitslosengeld eine beliebige qualifizierte Signaturkarte erfordert.[57] Hierfür könnten auch Bankkarten mit Signaturfunktion genutzt werden. Ob diese allerdings die notwendige Verlässlichkeit für einen solchen Infrastrukturträger bieten, ist noch offen. Die Kreditinstitute werden als marktwirtschaftlich agierende Einheiten ihre Signaturprojekte nicht beginnen oder sofort einstellen, wenn sie nicht die von ihnen erhofften Gewinne abwerfen. Die notwendige Investitionssicherheit für diejenigen, die in Anwendungen des elektronische Rechts-, Geschäfts- und Verwaltungsverkehr investieren sollen, bietet nur eine verlässliche Infrastruktur, wie sie ein digitaler Personalausweis mit Signaturfunktion darstellt.[58] Bei diesem wären auch die Identifizierung und die Übergabe der Karte gesichert.

---

[57] S. *Hornung/Roßnagel*, K&R 2004, 263; *Ernestus*, DuD 2004, 404.

[58] S. näher *Reichl/Roßnagel/Müller*, Machbarkeitsstudie Digitaler Personalausweis, 2005; BReg., BT-Drs. 15/4616.