Erläuterungen zum Gesetz zur digitalen Signatur (Signaturgesetz – SigG)

Vom 22. Juli 1997 (BGBl. I S. 1872)[1)]
(BGBl. III 9020-8)

Von
Prof. Dr. Georgios Gounalakis
Philipps-Universität Marburg

Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
CR	Computer und Recht
KuR	Kommunikation und Recht
NJW	Neue Juristische Wochenschrift
SigG	Gesetz zur digitalen Signatur (Signaturgesetz)
TDG	Gesetz über die Nutzung von Telediensten (Teledienstegesetz – abgedruckt unter VI H 10 q)
TDDSG	Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz – abgedruckt unter VI H 10 b)
TKG	Telekommunikationsgesetz (abgedruckt unter VI H 11)
ZUM	Zeitschrift für Urheber- und Medienrecht

Schrifttum

Bröhl, CR 1997, 73ff.
Engel-Flechsig/Maennel/Tettenborn, NJW 1997, 2981ff.
Geis, NJW 1997, 3000ff.
Gounalakis/Rhode, KuR 1998, Heft 2

Einführung

I. Regelungsgegenstand und Entstehungsgeschichte

In Anbetracht steigender gewerbsmäßiger Nutzbarkeit der neuen Medien, vor allem des Internets durch E-Mail oder Telebanking, erschien eine utilitäre rechtliche Rahmensetzung notwendig, welche der geschäftlichen Inanspruchnahme dieser Dienste Rechnung trug. Es galt Gefahren zu bannen, die sich in Form technischer Manipulierbarkeiten versandter Daten oder Unverläßlichkeit der Absenderkennung niederschlugen und daher den unaufhaltsamen, wirtschaftlichen Siegeszug jener neomedialen Angebote nachhaltig zu behindern drohten. Demgemäß will dieses von der Wirtschaft geforderte Gesetz mit »Pilotfunktion« eine administrative Grundlage für elektronische Unterschriften schaffen, auf deren Fundament weitere Normen und technische Verfahren zur digitalen Signatur aufbauen können. Geregelt wurde die Vergabe einzigartiger wie fälschungssicherer Signaturschlüssel unter behördlich kontrolliertem Ablauf, nicht aber die Änderung zivil- oder öffentlich-rechtlicher Schriftformerfordernisse. Deren Anpassungsbedürftigkeit soll vorerst nur beobachtet werden. Ebenso vom SigG ausgenommen blieb die rechtliche Flankierung der Verschlüsselung und Unkenntlichmachung

1) Verkündet als Artikel 3 des Informations- und Kommunikationsdienste-Gesetzes vom 22. 7. 1997 (BGBl. I S. 1870). In Kraft ab 1. 8. 1997.

ganzer Datensätze, die zu Überlegungen hinsichtlich eines eigenen Kryptographiegesetzes führten. Eingebettet ist das SigG in ein Bündel multimediagerechter Regelungen, wozu auch die ebenfalls vom Informations- und Kommunikationsdienste-Gesetz (IuKDG) eingeführten Normwerke TDG und TDDSG gehören. Auf deren einleitende Erläuterungen sei an dieser Stelle ausdrücklich hingewiesen (abgedruckt unter VI H 10 a und VI H 10 b).

II. Grundkonzeption

Um ein digitales Dokument verläßlich zu signieren, steht dem Nutzer ein individuelles Schlüsselpaar zur Verfügung, das sich aus einem privaten und einem paßgenauen öffentlichen Schlüssel zusammensetzt. Der private Schlüssel ist geheim und auf – beispielsweise – einer Chipkarte so gespeichert, daß er nicht ausgelesen werden kann. Mit dem öffentlichen Schlüssel gelingt es jederzeit, Unverfälschtheit der Daten und Identität seines Inhabers festzustellen. Technisch besehen handelt es sich bei der elektronischen Unterschrift um Datencodes, die auf Algorithmen beruhen, mit deren Hilfe sich jede beliebige Datei elektronisch besiegeln läßt. Die Zuteilung der Schlüsselpaare erfolgt durch anerkannte Zertifizierungsstellen, welche die Verknüpfung zwischen Unikat und Benutzer auf einem (digitalen) Zertifikat verbriefen (§§ 2 Abs. 2; 5 Abs. 1; 7). Jenes kann vom Nutzer seinen Dokumenten zur besonderen Verifikation beigefügt und bei seiner Zustimmung auch von jedermann öffentlich über Telekommunikationsverbindung eingesehen werden (§ 5 Abs. 1 S. 2).

Als Zertifizierungsstelle dürfen dabei natürliche oder juristische Personen tätig werden, die von der nach § 3 zuständigen Behörde hierfür die Genehmigung (§ 4) erhalten. Schlüssel-Inhaber können nur natürliche Personen sein. Zu betonen ist, daß auch eine nicht unter diesen Maßgaben erzeugte Signierung durch den Nutzer gestattet ist, soweit sie nicht durch andere Rechtsvorschriften vorgeschrieben wurde (§ 1 Abs. 2).

III. Technische Flexibilität

Da durch weitere technische Veränderungen algorithmische Verschlüsselungsverfahren längerfristig betrachtet an Wirksamkeit verlieren können, will dieses Gesetz entwicklungsoffen bleiben. Nach § 16 ist die Bundesregierung ermächtigt, Näheres zu den technischen Anforderungen durch Rechtsverordnung zu regeln.

IV. Haftungsfragen

Soweit eine Zertifizierungsstelle die ihr obliegenden Pflichten verletzt, bestimmt sich die Haftung gegenüber Dritten (insb. solchen, die auf die Gültigkeit der Signatur vertraut haben) nach den allgemeinen zivilrechtlichen Grundsätzen. Da von speziellen Haftungstatbeständen im SigG Abstand genommen wurde, können hier bedenkliche Lücken im Rahmen der Regreßansprüche entstehen (s. hierzu BT-Drs. 13/7934, S. 34, 36 und 39; BR-Drs. 966/96 [Beschluß], S. 22; *Gounalakis/Rhode*, KuR 1998, Heft 2).

Zu § 1 [Zweck und Anwendungsbereich]:

Zu *Absatz 1* s. Punkt I der Einführung, zu *Absatz 2* deren Punkt II.

Zu § 2 [Begriffsbestimmungen]:

Die Begriffe »digitale Signatur« und »Zertifizierungsstelle« sind dem internationalen Sprachgebrauch entlehnt und werden aus Gründen der Rechtssicherheit legaldefiniert. Zur Erläuterung

der Zertifizierung und Signierung s. auch Punkt II obiger Einführung. *Attribut-Zertifikate* können Angaben über die Vertretungsmacht des Schlüsselinhabers für dritte Personen enthalten (vgl. § 5 Abs. 2 und § 7 Abs. 2) und gehören zum Signaturschlüssel-Zertifikat, sind also auch wie ebendieses zu behandeln. *Zeitstempel* dienen als temporales Fixativ, indem sie ein Vor- oder Rückdatieren von digitalen Dokumenten verhindern. Solch eine veritas documenti toti ad tempus wird schon durch bloßes Stempeln der digitalen Signatur erreicht, weil diese einen »digitalen Fingerabdruck« der signierten Daten enthält und somit die zeitliche Echtheit des gesamten Inhaltes bezeugt.

Zu § 3 [Zuständige Behörde]:

Die gem. § 66 TKG bereits für die Erteilung der Lizenzen nach dem TKG zuständige Behörde ist aus verwaltungsrechtlichen wie -praktischen Zweckmäßigkeitserwägungen auch im Rahmen des SigG mit Wahrnehmung der genannten Aufgaben betraut.

Zu § 4 [Genehmigung von Zertifizierungsstellen]:

Der *Absatz 1* ist Anspruchsgrundlage für den um eine Genehmigung Ersuchenden. Näheres bestimmt sich nach der gem. § 16 Nr. 1 erlassenen Rechtsverordnung; im übrigen finden die Vorschriften des Verwaltungsverfahrensgesetzes (abgedruckt unter I B 25) Anwendung. Eine Übertragung der Genehmigung auf Dritte ist nicht vorgesehen.

Zuverlässigkeit und Fachkunde des Antragstellers sind nach den *Absätzen 2 und 3* konstitutive Voraussetzungen für die Erteilung der Genehmigung. Damit soll einer Ausfertigung gefälschter Zertifikate entgegengewirkt werden. Das Vorliegen der übrigen Voraussetzungen hat der Antragsteller durch ein von einer unabhängigen Stelle überprüftes *Sicherheitskonzept* nachzuweisen. Die zuständige Behörde dürfte dabei insbesondere solche Prüfstellen anerkennen, die vom BSI für tauglich befunden wurden.

Möglich ist die Nebenbestimmung, nach der dem Betrieb der Zertifizierungsstelle erst nach Prüfung des Sicherheitskonzeptes und Prüfberichtes zugestimmt wird (s. *Abs. 4*).

Gemäß *Absatz 5 Satz 1* bildet die zuständige Behörde (§ 3) gleichzeitig die oberste nationale Zertifizierungsstelle, die ihrerseits den privaten und von ihr kontrollierten Zertifizierungsstellen (§ 2 Abs. 2 i. V. m. § 4 Abs. 1) die zur Signierung der Nutzerzertifikate erforderlichen Zertifikate zuteilt (»Wurzelzertifikate« bzw. »Zertifizierungszertifikate«), wobei allerdings die private Zertifizierungsstelle ihre *Signaturschlüssel* selbst erzeugen kann. Ferner stellt sich die Behörde das Zertifikat für ihre eigenen Schlüssel aus. Für sie gelten gem. *Satz 2* die gleichen Sicherheitsanforderungen, wie sie auch den (privaten) Zertifizierungsstellen abverlangt werden (§ 5 und Überprüfung des eigenen Sicherheitskonzeptes durch externe Stellen).

Die Kostenerhebung erfolgt auf Grundlage des *Absatzes 6* i. V. m. § 16.

Zu § 5 [Vergabe von Zertifikaten]:

Absatz 1 sieht für die Zertifizierungsstelle keinen Kontrahierungszwang vor. Schließt sie aber Verträge mit Nutzern, so hat sie diese z. B. durch Vorlage des Personalausweises zuverlässig zu identifizieren. Die Veröffentlichung des Zertifikates hängt von der Zustimmung des Nutzers ab. Vgl. ferner Punkt II der Einführung.

Absatz 2 trägt dem Umstand Rechnung, daß Signaturschlüssel an *natürliche* Personen gebunden sind, auch wenn diese für juristische Personen tätig werden möchten. Zum Nachweis der Vertretungsmacht durch Attribut-Zertifikate s. auch die Erläut. zu §§ 2, 7.

Zum Begriff des Pseudonyms in *Absatz 3* vgl. die Erläut. zu § 4 Abs. 1 TDDSG (abgedruckt unter VI H 10 b). Die Möglichkeit zur Pseudonymisierung des Schlüssels dient der Vermeidung von Daten und Persönlichkeitsprofilen. Pseudonyme sind gem. § 7 Abs. 1 Nr. 1 als solche kenntlich zu machen, damit sich Dritte auf die erschwerte Identifikation des Nutzers einstellen können (vgl. § 12 Abs. 2).

Die Integrität der Signaturschlüssel und der ihnen zugeordneten Personendaten soll *Absatz 4 Satz 1* aufrechterhalten. *Satz 2* fordert die absolute Geheimhaltung des privaten Schlüssels, von dem *niemand* (auch nicht der Schlüssel-Inhaber, BR-Drs. 966/96, S. 34) Kenntnis erhalten darf. Die Einmaligkeit privater Signaturschlüssel unterstreicht *Satz 3*.

Neben zuverlässigem Personal hat die Zertifizierungsstelle gem. *Absatz 5* auch technische Komponenten (§ 14) einzusetzen, deren Verwendung ihr – im Gegensatz zu den Schlüssel-Inhabern (vgl. § 6) – vorgeschrieben ist.

Zu § 6 [Unterrichtungspflicht]:

Die Zertifizierungsstelle hat z. B. durch Aushändigung von Informationsblättern oder Beratungsgespräch den Schlüssel-Inhaber zu unterrichten über:
- die in seinem eigenen Interesse liegenden Maßnahmen,
- aktuelle und geeignete technische Komponenten (§ 14),
- die Signatur als ein seiner Person zurechenbares Zeichen und
- Aktualisierungserfordernisse bei alten und daher u. U. unsicheren Signaturen.

Zu § 7 [Inhalt von Zertifikaten]:

Die zur Feststellung der Urheberschaft und Authentizität einer digitalen Signatur erforderlichen Mindestangaben listet *Absatz 1* auf. Nach dessen *Nummer 7* müssen dem Zertifikat solche Informationen beigefügt werden, aus denen Beschränkungen der Schlüssel-Nutzung auf bestimmte Rechtsgeschäfte oder für einen vorgegebenen Rahmen hervorgehen.

Dies kann mit Angaben zu Beschränkungen der Vertretungsmacht zusammenfallen, für die *Absatz 2* zu beachten ist, der den § 5 Abs. 2 ergänzt (s. auch dessen Erläut.).

Aus der Zweckbestimmung des Signaturschlüssel-Zertifikates folgt, daß nicht zur Zertifizierung notwendige Daten nur mit Einwilligung des Nutzers in das Zertifikat aufgenommen werden dürfen. Das stellt der nach Empfehlung des Technologieausschusses eingefügte *Absatz 3* klar (BT-Drs. 13/7934, S. 15 und 41).

Zu § 8 [Sperrung von Zertifikaten]:

Die immer nur *ex nunc* wirkende Sperrung von Signaturschlüssel-Zertifikaten erstreckt sich zwangsläufig auch auf etwaige Attribut-Zertifikate. Umgekehrt folgt aus dieser Akzessorietät, daß aber die Sperrung solcher Nebenzertifikate das »Stammzertifikat« unberührt läßt.

Unter den Varianten der Sperrungsmöglichkeiten nach *Absatz 1* dürfte erstgenannte – Sperrung auf Nutzerverlangen – die in der Praxis am häufigsten gebräuchliche sein. Dafür wird es in der Regel zwei Anlässe geben: Der Nutzer möchte nach Schlüsselverlust einen möglichen Mißbrauch verhindern, oder er will von seinem Recht auf jederzeitigen Rückzug aus dem elektronischen Geschäftsverkehr Gebrauch machen. Eine Sperrung ex officio kommt in Betracht, wenn und soweit der Schlüssel bei Straftaten Verwendung gefunden hat (vgl. §§ 74ff. Strafgesetzbuch – abgedruckt unter II G 2).

Absatz 2 trägt dem Selbstbestimmungs- und Allgemeinen Persönlichkeitsrecht Dritter Rechnung, wenn er diese zur Sperrung solcher Zertifikate befugt, die Angaben (d. h. Daten) zu ihrer Person enthalten. (Zu eng die Begr. zum SigG in BR-Drs. 966/96, S.35, die von Drittbefugnis nur bei Änderung der Vertretungsmacht oder Entziehung der Zulassung i. S. d. § 5 Abs. 2 i. V. m. § 7 Abs. 2 ausgeht. Dies mag daran liegen, daß bei Abfassung der Begr. § 7 Abs. 3 noch nicht im Entwurf vorgesehen war.)

Absatz 3 stellt auf die Funktion der Behörde als Zertifizierungsstelle ab (s. § 4 Abs. 5).

Zu § 9 [Zeitstempel]:

Hiernach kann jedermann diese *Pflichtdienstleistung* verlangen, der Daten erzeugt oder dem fremde Daten vorliegen. Im übrigen s. § 2 Abs. 4 und dessen Erläut.

Zu § 10 [Dokumentation]:

Die Dokumentation der Sicherheitsmaßnahmen hat die Durchführung wirksamer Kontrollen und Feststellung ggf. haftungsrelevanter Pflichtverletzungen zum Zweck. Zertifikate sind zu dokumentieren, damit digitale Signaturen überprüfbar bleiben.

Zu § 11 [Einstellung der Tätigkeit]:

Diese Norm will die Interessen der Schlüssel-Inhaber wahren. In Anlehnung an § 13 Abs. 4 soll die zuverlässige Kontrolle bereits erzeugter digitaler Signaturen auch nach Einstellung des Zertifikationsbetriebes sichergestellt werden.

Zu § 12 [Datenschutz]:

In *Absatz 1 Satz 1* kommt der Grundsatz der engen Zweckbindung bei der Erhebung personenbezogener Daten zum Ausdruck. Die »Einwilligung des Betroffenen« in *Satz 2* meint Einwilligung des betroffenen Dritten. Nach *Satz 3* erstreckt sich die Zweckbindung auch auf die Datenverwendung; sie wird aber mit Einwilligung des Betroffenen gelöst.

Der im Gesetzgebungsverfahren als unverhältnismäßig und mit dem Recht auf informationelle Selbstbestimmung (s. *BVerfGE* 65, 1ff.) als unvereinbar gerügte *Absatz 2 Satz 1* (BT-Drs. 13/7934, S. 36f. und 38) hat mit der vom Technologieausschuß empfohlenen Erweiterung um seinen *Satz 3* (vgl. BT-Drs. 13/7934, S. 16 und 41) eine nutzerfreundliche Entschärfung erfahren. Zwar muß die Zertifizierungsstelle Daten zur Identität des pseudonym signierenden Nutzers unter näherer Maßgabe der genannten Zwecke auf Ersuchen an die zuständigen Stellen übermitteln. Doch wird die Behörde den Schlüssel-Inhaber über die Aufdeckung seines Pseudonyms in Kenntnis zu setzen haben, soweit dem nicht wichtige öffentliche Belange

entgegenstehen. Im übrigen dürfte durch Satz 1 das Selbstbestimmungsrecht im Kern nicht beeinträchtigt sein, da hier nur *identitätsbezogene* Daten weitergegeben werden (näher zu § 12 Abs. 2 *Gounalakis/Rhode*, KuR 1998, Heft 2).

Die datenschutzrechtliche Kontrolle soll nach *Absatz 3* nicht der gem. § 3 zuständigen Stelle, sondern vielmehr der Behörde nach § 38 Bundesdatenschutzgesetz (abgedruckt unter I B 80) obliegen, deren Überprüfungsbefugnis im Rahmen des SigG zugleich erweitert wird.

Zu § 13 [Kontrolle und Durchsetzung von Verpflichtungen]:

Diese Norm enthält eine Reihe von Eingriffsermächtigungen für die nach § 3 zuständige Behörde, um die Einhaltung der Rechtsvorschriften durch die Zertifizierungsstellen zu gewährleisten. Vgl. auch § 91 Abs. 1, 3 TKG.

Absatz 1 eröffnet als »Kann-Regelung« hinsichtlich der genannten Rechtsfolgen behördliches Ermessen; *Satz 1* ist Generalklausel. Die Untersagungsverfügung nach *Satz 2* ist für eine befristete Zeit bis zur Beseitigung des rechtswidrigen Verhaltens bestimmt, wobei die Untersagung nach Satz 2 oder *3* ultima ratio bleiben soll und nur auszusprechen ist, wenn mildere Maßnahmen keinen Erfolg zeitigen.

Die zur Überwachung nach Absatz 1 erforderlichen prozessualen Befugnisse der Behörde sowie das Auskunftsverweigerungsrecht der in Zertifizierungsstellen Tätigen regelt *Absatz 2*.

Der Behörde steht nach *Absatz 3* insoweit ein Beurteilungsspielraum zu, als die Geeignetheit der Maßnahmen nach § 13 Abs. 1 S. 2 einzuschätzen ist. Dagegen wird die Verwaltung auf der Rechtsfolgenseite gebunden (»hat« zu widerrufen).

Absatz 4 dient der kontinuierlichen Überprüfbarkeit digitaler Signaturen. Für diese Regelung bleibt nur dann Raum, wenn die Zertifizierungsstelle jener ihr nach § 11 obliegenden Pflicht nicht Genüge getan hat.

Eine Klarstellungsfunktion kommt *Absatz 5 Satz 1* zu. *Satz 2* verlangt die pflichtgemäße Betätigung behördlichen Ermessens.

Zu § 14 [Technische Komponenten]:

Diese Norm enthält die durch technische Komponenten umzusetzenden Zielvorgaben. Die technischen Komponenten müssen dem aktuellen Stand der Wissenschaft und Technik entsprechen. Damit das SigG entwicklungsoffen bleibt, wird Näheres per Rechtsverordnung geregelt (vgl. § 16 Nr. 6).

Zertifizierungsstellen sind verpflichtet, geeignete technische Komponenten einzusetzen (vgl. § 5 Abs. 5 S. 2, 3 und § 9 mit entsprechenden Erläuterungen) sowie die Schlüssel-Inhaber über diesbezügliche Sicherheitsmaßnahmen zu unterrichten (§ 6). Des weiteren kommt den Stellen mit Blick auf Geheimhaltung des Schlüssels und Sicherheit der Signierkomponente eine Garantenfunktion zu (vgl. § 5 Abs. 4 S. 2).

Dagegen liegt der Einsatz geeigneter technischer Komponenten bei Aufbereitung zu signierender oder zu prüfender signierter Daten (nach Unterrichtung gem. § 6) allein beim Schlüssel-Inhaber.

Die *Absätze 1 bis 3* schreiben den Einsatz technischer Komponenten vor, um beispielsweise Fälschungen digitaler Signaturen erkennbar zu machen, private Signaturschlüssel vor Mißbrauch zu schützen und eindeutig anzuzeigen, auf welche Daten sich die Signatur bezieht (die auf dem Bildschirm angezeigten Daten müssen mit den signierten Daten übereinstimmen). Auch wollen sie das unbefugte Verändern und Abrufen von Zertifikatverzeichnissen verhindern.

Als anerkannte Stelle i. S. v. *Absatz 4* wird man in erster Linie das BSI ansehen müssen, das aufgrund seiner Sachkunde gemäß der Aufgabenzuweisung nach dem BSI-Einrichtungsgesetz (abgedruckt unter I B 10 a) zur Überprüfung informationstechnischer Komponenten und zur Vergabe von Sicherheitszertifikaten befähigt und befugt ist (Näheres in der BSI-Zertifizierungsverordnung [abgedruckt unter I B 10 b] und der BSI-Kostenverordnung [abgedruckt unter I B 10 c]). Allerdings kann die zuständige Behörde auch andere Stellen anerkennen, wenn diese auf vergleichbarem Sach- und Sicherheitsniveau arbeiten.

Absatz 5 stellt Produkte sowie deren Bewertungen aus den genannten europäischen Staaten den technischen Komponenten i. S. v. Absatz 4 unter Vorbehalten gleich.

Zu § 15 [Ausländische Zertifikate]:

Mit dieser Äquivalenzklausel nach *Absatz 1* werden in Ergänzung zu § 14 Abs. 5 digitale Signaturen aus dem genannten europäischen Ausland den deutschen gleichgestellt, wenn und soweit sie ähnliche Sicherheitsmerkmale aufweisen.

Die globale und supranationale Nutzbarkeit neuer Medien sowie die damit verbundenen zwischenstaatlichen Übereinkommen finden in *Absatz 2* Berücksichtigung. Er soll im Falle bi- oder multinationaler Vereinbarungen den Absatz 1 erweitern.

Zu § 16 [Rechtsverordnung]:

S. hierzu Punkt III obiger Einführung sowie insbesondere auch die §§ 4 und 14 mit ihren entsprechenden Erläuterungen. Nach Maßgabe dieser Ermächtigungsgrundlage wurde am 8.10.1997 die Verordnung zur digitalen Signatur (Signaturverordnung – SigV – abgedruckt unter VI H 10 c a) erlassen.