Prof. Dr. Alexander Roßnagel, Kassel/Saarbrücken

Die qualifizierte elektronische Signaturen mit Einschränkungen im Besteuerungsverfahren

erscheinen in: Kommunikation und Recht 2003, Heft 8, 379 - 385

Um die ausschließlich elektronische Übermittlung von Steuererklärungen und sonstiger für das automatisierte Besteuerungsverfahren erforderlicher Daten zu ermöglichen, enthalten die durch das 3. Verwaltungsverfahrensänderungsgesetz (VwVfÄG) vom 21.8.2002 geänderte Abgabenordnung (AO) und die Steuerdaten-Übermittlungsverordnung (StDÜV) vom 28.1. 2003 entsprechende Regelungen. Um die Integrität und Authentizität elektronischer Erklärungen sicher zu stellen, sehen beide Regelungen vor, dass diese elektronisch signiert werden müssen. Allerdings fordern sie hierfür keine qualifizierte elektronische Signatur nach dem Signaturgesetz (SigG), sondern schaffen eine neue Signaturstufe eigens für Besteuerungsverfahren, für die viele Anforderungen des SigG nicht gelten sollen. Der Beitrag erläutert, welche Ausnahmen für die „qualifizierte elektronische Signatur mit Einschränkungen" ermöglicht wurden und bewertet diese Regelungen aus dem Blickwinkel des Signaturrechts.

I. Das elektronische Besteuerungsverfahren

Um Besteuerungsverfahren mit Hilfe elektronischer Medien durchführen zu können, hat das 3. VwVfÄG mit Wirkung vom 28.8.2002 die allgemeinen Regelungen der AO so geändert, dass die erforderlichen Rahmenbedingungen für eine „elektronische Akte" in der Finanzverwaltung vorliegen.[1] Hierdurch soll vor allem die Abgabe und Bearbeitung von Steuererklärungen durch den Einsatz moderner Kommunikationsmittel ermöglicht werden, für die die Finanzverwaltungen das elektronische Verfahren zur Übermittlung von Steuererklärungsdaten „ELektronische STeuerERklärung - ELSTER" entwickelt haben. Zu diesem Zweck wird in § 87a Abs. 1 AO die Übermittlung elektronischer Dokumente vom Bürger zur Behörde und umgekehrt zugelassen, wenn hierfür ein Zugang eröffnet ist.[2]

Da für viele Anträge, Erklärungen und Mitteilungen an die Finanzbehörden die Schriftform mit eigenhändiger Unterschrift gefordert wird,[3] stellt § 87a Abs. 3 Satz 1 AO die elektronische Form der Schriftform gleich. Diese Form wird gemäß § 87a Abs. 3 Satz 2 AO erfüllt, wenn das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 SigG versehen ist. Das Signieren des elektronischen Dokuments mit einer „einfachen" Signatur nach § 2 Nr. 1 SigG oder einer „fortgeschrittenen" Signatur nach § 2 Nr. 2 SigG[4] vermag die elektronischer Form nicht zu erfüllen und die Schriftform nicht zu ersetzen.[5]

---

1 S. BT-Drs. 14/9000, 35.

2 Zur Auslegung dieses Tatbestandsmerkmals s. z.B. BT-Drs. 14/9000, S. 30f.; *Schlatmann*, LKV 2002, 491; *ders*., DVBl. 2002, 1009; *ders*., in: *Roßnagel* (Hrsg.), Die elektronische Signatur in der öffentlichen Verwaltung, 2002, S. 66; *Schmitz/Schlatmann*, NVwZ 2002, 1285; kritisch *Nedden* in: *Roßnagel* (Hrsg.), Die elektronische Signatur in der öffentlichen Verwaltung, 2002, S. 111f.; *Roßnagel*, NJW 2003, 475.

3 S. z.B. § 25 Abs. 3 Satz 4 und 5 EStG, § 18 Abs. 3 Satz 3 UStG, § 14a Satz 3 GewStG.

4 S. hierzu *Roßnagel*, MMR 2003, 165.

5 S. *Roßnagel*, NJW 2003, 475.

Verwaltungsakte der Finanzbehörden können nach § 119 Abs. 2 AO grundsätzlich schriftlich, elektronisch, mündlich oder in anderer Weise erlassen werden. Ist für Verwaltungsakte durch Gesetz die Schriftform angeordnet,[6] kann sie nach § 87a Abs. 4 AO, soweit nicht durch Gesetz etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Auch hierfür muss das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 SigG versehen sein. In diesem Fall muss außerdem nach § 119 Abs. 3 Satz 3 AO das der Signatur zugrunde liegende qualifizierte Zertifikat entsprechend § 7 Abs. 1 Nr. 9 SigG oder ein zugehöriges qualifiziertes Attributzertifikat nach § 7 Abs. 2 SigG die erlassende Behörde erkennen lassen.[7] Dies erscheint angesichts der Regelung in § 119 Abs. 3 Satz 1 AO zur Angabe der erlassenden Behörde in der Erklärung überflüssig und ohne die Anforderung, das Zertifikat in die Signatur einzuschließen, auch wenig hilfreich. Außerdem ist diese Regelung mit dem Nachteil verbunden, eine weitere Verbreitung von Signaturen dadurch zu behindern, dass sie die private Nutzung der Zertifikate ausschließt.[8]

Die rechtliche Gleichsetzung von Schriftform und elektronischer Form durch die Generalklauseln des § 87a Abs. 3 und 4 VwVfG greift im gesamten Steuerrecht, unabhängig davon, mit welchen Bezeichnungen das jeweilige Gesetz die Schriftform anordnet. Damit ist die elektronische Form statt der Schriftform grundsätzlich immer zulässig, auch ohne dass dies in der jeweiligen Vorschrift erwähnt wird. Etwas anderes gilt nur dann, wenn die elektronische Form ausdrücklich ausgeschlossen ist[9] oder wenn Anträge, Anzeigen oder Ähnliches „auf“ (nicht „nach“) amtlich vorgeschriebenen Vordrucken abzugeben sind.[10]

Um elektronische Dokumente im Steuerverfahren auch als Beweismittel nutzen zu können, bestimmt § 87a Abs. 5 Satz 1 AO, dass der Beweis durch Vorlegung oder Übermittlung der Daten angetreten werden kann. Erfüllt das Dokument die elektronische Form ermöglicht § 87a Abs. 5 Satz 2 AO einen durch Gesetz vorweggenommenen Anscheinsbeweis.[11] Danach soll der Anschein der Echtheit einer in elektronischer Form vorliegenden Willenserklärung (§ 126a BGB), der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, nur durch Tatsachen erschüttert werden können, die ernstliche Zweifel daran begründen, dass die Erklärung mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist.

Nach § 150 Abs. 1 Satz 2 AO sind die Regelungen zur elektronischen Übermittlung allerdings nur anwendbar, soweit auf Grund eines Gesetzes oder einer nach § 150 Abs. 6 AO erlassenen Rechtsverordnung die Steuererklärung auf maschinell verwertbaren Datenträgern übermittelt werden darf.

---

6 S. z.B. § 157 Abs. 1 Satz 1 AO.

7 S. zu Attributen in Zertifikaten *Roßnagel*, in: *ders*. (Hrsg.), Recht der Multimediadienste, 1999 ff., § 7 SigG, Rn. 50 ff.

8 S. *Roßnagel*, NJW 2003, 475.

9 S. z.B. §§ 224a, 244, 309, 324 AO.

10 S. z.B. §§ 46 Abs. 3, § 138 Abs. 1 AO und § 50d Abs. 2 EStG.

11 Diese Regelung entspricht § 292a ZPO - s. hierzu *Fischer-Dieskau/Gitter/Paul/Steidle*, MMR 2002, 709; *Scheffler*/*Dressel,* CR 2000, 378; *Roßnagel*, MMR 2000, 451; *ders*., NJW 2001, 1817; *Borges,* K&R 2001, 196; *Dästner,* NJW 2001, 3469.

II. Die elektronische Übermittlung von Steuererklärungen

Die Freigabe für die elektronische Übermittlung enthält die am 28.1.2003 in Kraft getretene StDÜV.[12] Sie bestimmt in § 1 Abs. 1, dass Steuererklärungen, Freistellungsaufträge, Sammelanträge, Zusammenfassende Mitteilungen und sonstige für das Besteuerungsverfahren erforderliche Daten mit Ausnahme für Verbrauchsteuern elektronisch übermittelt werden können.

Da noch nicht alle Finanzbehörden für die sichere elektronische Kommunikation ausgestattet sind, behält sich die Finanzverwaltung allerdings vor, den Zugang für die elektronische Kommunikation zu eröffnen. Art und Einschränkungen der elektronischen Übermittlung werden nach § 1 Abs. 2 StDÜV werden in Abstimmung mit den obersten Finanzbehörden vom Bundesfinanzministerium (BMF) in einer Verwaltungsvorschrift bestimmt, die im Bundessteuerblatt zu veröffentlichen ist. Soweit Fragen der Verschlüsselung oder Sicherheit in der Informationstechnik betroffen sind, erfolgt die Bestimmung im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik.

Unterliegen Daten, die die Behörde übermittelt, dem Steuergeheimnis nach § 30 AO, so sind die Daten nach § 87a Abs. 1 Satz 3 AO mit einem geeigneten Verfahren zu verschlüsseln. Diese Regelung für Behörden weitet § 1 Abs. 3 StDÜV auf alle Übermittlungen, also auch die vom Bürger zur Behörde aus. Für sie sind dem jeweiligen Stand der Technik entsprechende Maßnahmen zu treffen, die die Vertraulichkeit der Daten gewährleisten. Werden für die Übermittlung allgemein zugängliche Netze – wie das Internet – genutzt, sind Verschlüsselungsverfahren anzuwenden.

III. Ein zusätzliches Signaturverfahren

Zwar fordert die AO für die elektronische Form – in Übereinstimmung mit den Regelungen im Privat-, Verwaltungs- und Sozialrecht – eine qualifizierte elektronische Signatur nach § 3 Nr. 3 SigG. Doch befürchtet das BMF, dass die „bei einer ‚qualifizierten elektronischen Signatur' erforderliche kostenpflichtige Einschaltung einer Zertifizierungsstelle sowie die unzureichende Verbreitung und Nutzung der dafür erforderlichen sicheren Signaturerstellungseinheit ... zumindest in der nahen Zukunft den angestrebten zügigen Aufbau der elektronischen Kommunikation zwischen den Steuerpflichtigen und der Finanzverwaltung noch erheblich behindern" und „die Weiterentwicklung des Projekts ELSTER" gefährden würde.[13] Es hat daher darauf hingewirkt, dass in § 87a Abs. 6 AO eine Sonderregelung getroffen wurde, die Ausnahmen von den Anforderungen der elektronischen Form nach § 87a Abs. 3 und 4 AO ermöglicht. Danach darf für eine Übergangszeit von den Anforderungen des SigG an eine „qualifizierte elektronische Signatur" nach Maßgabe einer nach § 150 Abs. 6 AO zu erlassenden Rechtsverordnung abgewichen werden. Damit sollen „neben den Signaturen der qualifizierten Trustcenter insbesondere auch die durch Banken und Arbeitgeber herausgegebenen Signaturen (ZKA-Karte, Mitarbeiter-, Firmenkarte, elektronischer Dienstausweis) zur rechtsverbindlichen elektronischen Kommunikation zwischen den Steuerpflichtigen und der Finanzverwaltung genutzt werden können".[14]

---

12 BGBl. I, 139; s. auch die amtl. Begr. in BR-Drs. 892/02

13 S. BT-Drs. 14/9000, 36; BR-Drs. 892/02, 13f.

14 Amtl. Begr., BR-Drs. 892/02, 14.

Damit wird bis zum 31.12.2005 neben den im SigG bereits geregelten Signaturstufen[15] „einfache“, „fortgeschrittene“, qualifizierte“ und „akkreditierte“ Signatur eine zusätzliche zeitlich auf drei Jahre befristete und sachlich auf Steuerverfahren begrenzte Signaturstufe geschaffen. Diese „qualifizierte elektronische Signatur mit Einschränkungen“ ist nach § 7 Abs. 1 Satz 1 StDÜV eine „fortgeschrittene elektronische Signatur“ im Sinn des § 2 Nr. 2 SigG, weil sie die Anforderungen an eine qualifizierten elektronischen Signatur nicht erfüllt. Die zulässigen Einschränkungen gegenüber dem von § 87a Abs. 3 Satz 2 AO geforderten Niveau beschreibt § 7 StDÜV. Alle anderen Anforderungen an eine qualifizierte elektronische Signatur müssen ausnahmslos erfüllt sein, damit das jeweilige Signaturverfahren als Ersatz der Schriftform im Steuerverfahren rechtsgültig verwendet werden kann.

Nach § 87a Abs. 6 Satz 2 AO kann in der Rechtsverordnung bestimmt werden, dass die „qualifizierte elektronische Signatur mit Einschränkungen“ auch für Verwaltungsakte abweichend von § 87a Abs. 4 Satz 2 AO eingesetzt werden kann. Diese Regelung hat die StDÜV jedoch nicht getroffen. Sie regelt nach § 7 Abs. 1 Satz 1 ausdrücklich nur die Voraussetzungen für „elektronische Signaturen im Sinne des § 87a Abs. 6 Satz 1 AO“. Sie gilt daher nur für Steuererklärungen, Freistellungsaufträge, Sammelanträge, Zusammenfassende Mitteilungen und sonstige für das Besteuerungsverfahren erforderliche Daten mit Ausnahme für Verbrauchsteuern, nicht aber für elektronische Verwaltungsakte, für die Schriftform gefordert wird.

IV. Die qualifizierte elektronische Signatur mit Einschränkungen

Die qualifizierte elektronische Signatur mit Einschränkungen muss eine fortgeschrittene Signatur nach § 2 Nr. 2 SigG sein, die zwar den Merkmalen der qualifizierten Signatur in § 2 Nr. 3 SigG nahe kommt, sie aber nicht ganz erfüllen muss. Bestimmte – vor allem formelle - Anforderungen an die Signaturerstellungseinheit, das Zertifikat und den Zertifizierungsdiensteanbieter werden nicht gefordert. Technisch-organisatorisch muss sie jedoch „weitgehend“ die „gleichen Sicherheiten wie die qualifizierte elektronische Signatur“ bieten.[16] Zwischen dem Ziel qualifizierte elektronische Signatur (§ 87a Abs. 3 AO) und den Erleichterungen des § 7 StDÜV besteht ein eindeutiges Regel-Ausnahme-Verhältnis. Daher ist bei der Auslegung des § 7 StDÜV zu beachten, dass grundsätzlich die Anforderungen des SigG an qualifizierte elektronische Signaturen gelten,[17] es sei denn, die Vorschrift regelt spezifische Ausnahmen. Diese sind als Ausnahmen eng auszulegen. Im Zweifel muss sich die Auslegung an dem Ziel der Vorschrift orientieren, „weitgehend die gleichen Sicherheiten wie die qualifizierte elektronische Signatur“ gewährleisten zu wollen.

1. Ausnahmen für die sichere Signaturerstellungseinheit

Nach § 7 Abs. 1 Nr. 1 StDÜV muss die fortgeschrittene elektronische Signatur[18] „mit einer Signaturerstellungseinheit erzeugt werden, die die wesentlichen Anforderungen an eine sichere Signaturerstellungseinheit“ im Sinn des § 2 Nr. 10 SigG erfüllt. Der sehr unbestimmte Begriff der „wesentlichen Anforderungen“ zielt materiell auf „die Nutzung technisch gleichwerti-

---

15 S. zu diesen ausführlich *Roßnagel*, MMR 2002, 215; *ders*., in: *ders.* (Hrsg.), Die elektronische Signatur in der öffentlichen Verwaltung, 2002, S. 31 ff.

16 Amtl. Begr., BR-Drs. 982/02, 14.

17 Dies gilt z.B. für die Anforderungen an Verzeichnisdienste nach § 5 Abs. 1 SigG und § 4 SigV, an das Gültigkeitsmodell (Kettenmodell) der Zertifikate, an den Einsatz zuverlässigen Personals nach § 5 Abs. 5 SigG und § 4 Abs. 3 SigV und an den Datenschutz nach § 14 SigG.

18 S. zu den Anforderungen an diese *Roßnagel*, MMR 2003, 165.

ger Produkte“, ohne dass diese jedoch – wie für qualifizierte elektronische Signaturen – in dem formellen Verfahren nach Anlage 1 der SigV nachgewiesen sein muss. Vielmehr sind auch alternative Nachweisverfahren wie eine „Zertifizierung entsprechend FIPS 140-1, mindestens Level 2“ zulässig.[19] Die wesentlichen Anforderungen an die Signaturerstellungseinheit ergeben sich somit aus den Zielanforderungen des § 17 Abs. 1 SigG und des § 15 Abs. 1 SigV. Danach müssen die Signaturerstellungseinheiten Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen. Sie dürfen den Signaturschlüssel nicht preisgeben und müssen gegen unberechtigte Nutzung der Signaturschlüssel schützen. Sie müssen gewährleisten, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder alternativ durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann.

2. Ausnahmen für das qualifizierte Zertifikat

Nach § 7 Abs. 1 Nr. 2 StDÜV muss die Signatur „auf einem zum Zeitpunkt ihrer Erzeugung gültigen Zertifikat beruhen, das die Anforderungen an qualifizierte Zertifikate“ im Sinn des § 2 Nr. 7 SigG erfüllt. Von diesen Anforderungen lässt § 7 Abs. 1 Nr. 2 a) StDÜV die Ausnahmen zu, dass das Zertifikat die Angaben nach § 5 Abs. 2 und 3 sowie § 7 Abs. 1 Nr. 7 bis 9 SigG nicht enthalten muss. Dies bedeutet, dass der Zertifizierungsdiensteanbieter den Prüfaufwand für Attribute, insbesondere für eine Vertretungsmacht oder für berufsbezogene Angaben, und für Einschränkungen in der Nutzung des Signaturschlüssels nicht erbringen muss. Allerdings wird es in vielen Fällen notwendig oder zumindest hilfreich sein, wenn im Zertifikat Angaben zu einer Vertretungsmacht oder zu berufsbezogenen Eigenschaften enthalten sind – etwa wenn das Organ oder der Vertreter einer juristischen Person für diese handelt. In § 7 Abs. 1 Nr. 2 StDÜV wird daher nur die Pflicht aufgehoben, diese Angaben ins Zertifikat aufzunehmen, nicht jedoch verboten, dies zu tun.

3. Ausnahmen für qualifizierte Zertifizierungsdiensteanbieter

Für qualifizierte Zertifikate ist nach § 2 Nr. 7 SigG erforderlich, dass die Zertifizierungsdiensteanbieter, die sie ausstellen, alle Anforderungen des SigG und der SigV erfüllen. Hiervon erlaubt § 7 Abs. 1 Nr. 2 b) i.V.m Abs. 2 StDÜV elf genau definierte Ausnahmen, die eng auszulegen sind und letztlich keine Sicherheitseinbußen erlauben. Die Ausnahmen gestatten nämlich nur die „Nutzung technisch gleichwertiger ... Betriebsabläufe“. Ansonsten müssen die „weiteren Anforderungen“ des SigG und der SigV, „insbesondere … die gesicherte Identifizierung des Antragstellers sowie der Einsatz von Sperrlisten, ... erfüllt werden“. „Die Verwendung von Signaturen“ im Sinn des § 87a Abs. 6 AO soll damit „für die Übergangszeit technisch weitgehend die gleichen Sicherheiten wie die qualifizierte elektronische Signatur“ bieten.[20]

V. Die Ausnahmen des § 7 Abs. 2 StDÜV

Durch § 7 Abs. 2 StDÜV werden folgende Ausnahmen von den Anforderungen des SigG und der SigV zugelassen:

---

19 Alle Zitate aus der Amtl. Begr., BR-Drs. 982/02, 14.

20 Amtl. Begr., BR-Drs. 982/02, 14.

1. Eingeschränktes Sicherheitskonzept und Verzicht auf die Anzeige des Betriebs

Nach Nr. 1 kann auf eine „Abschätzung und Bewertung der verbleibenden Sicherheitsrisiken im Sicherheitskonzept und die Anzeige des Betriebs“ nach verzichtet werden. Diese Ausnahme entlastet die Anbieter von Verfahren für qualifizierte elektronische Signaturen mit Einschränkungen von zwei Pflichten.

Nach § 4 Abs. 3 Satz 1 SigG muss jeder, der den Betrieb eines Zertifizierungsdienstes aufnimmt, diesen in der in § 1 SigV beschriebenen Form der Regulierungsbehörde für Telekommunikation und Post (RegTP) anzeigen. Diese Anzeigepflicht entfällt ersatzlos.

Nach § 4 Abs. 2 Satz 4 SigG ist eine Voraussetzung für den Betrieb eines Zertifizierungsdienstes, dass die Maßnahmen zur Erfüllung der Sicherheitsanforderungen in einem Sicherheitskonzept entsprechend § 2 SigV aufgezeigt und umgesetzt sind. Ein solches Sicherheitskonzept muss auch für qualifizierte elektronische Signaturen mit Einschränkungen aufgestellt werden. Allerdings verzichtet Nr. 1 auf den Bestandteil der Abschätzung und Bewertung verbleibender Sicherheitsrisiken. Dieses abgespeckte Sicherheitskonzept muss auch nicht der RegTP vorgelegt werden.

2. Identifizierung nach § 154 AO

Nach Nr. 2 kann auf eine Identifizierung des Antragstellers nach § 5 Abs. 1 SigG und § 3 SigV verzichtet werden, soweit die Identifizierung entsprechend § 154 Abs. 2 AO erfolgt ist oder erfolgt. Nach § 5 Abs. 1 SigG und § 3 Abs. 1 SigV ist der Antragsteller „zuverlässig“ „anhand des Personalausweises oder eines Reisepasses ...“ zu identifizieren. Auf die Identifizierung des Antragstellers als solche soll auch nach Nr. 2 nicht verzichtet werden. Allerdings soll diese nach § 154 Abs. 2 AO erfolgen dürfen. § 154 Abs. 2 AO fordert von demjenigen, der ein Konto führt, sich „zuvor Gewissheit über die Person und Anschrift des Verfügungsberechtigten zu verschaffen und die entsprechenden Angaben in geeigneter Form ... festzuhalten“. Seit Inkrafttreten des Geldwäschegesetzes (GwG) sind die Regelungen des § 154 AO auch im Zusammenhang mit der Bekämpfung der Geldwäsche zu sehen. Auch die Identifizierung nach § 154 AO muss die Anforderungen des § 1 Abs. 5 GwG erfüllen. Dabei ist grundsätzlich vom Gebot der persönlichen und dokumentenmäßigen Identifizierung auszugehen. „Gewissheit über die Identität einer natürlichen Person besteht deshalb nur, wenn der vollständige Name anhand eines Personalausweises oder Reisepasses festgestellt wird.“[21]

Insofern stellt § 154 Abs. 2 AO vergleichbare Anforderungen an die Identifizierung wie § 5 Abs. 1 SigG und § 3 Abs. 1 SigV. Auch die Möglichkeit, auf eine bereits erfolgte Identifizierung Bezug zu nehmen und eine erneute Identifizierung zu ersparen, entspricht den Vorgaben des Signaturrechts. Dieses erlaubt auch eine Identifizierung durch Dritte, wenn diese nach § 4 Abs. 5 SigG in das Sicherheitskonzept des Zertifizierungsdiensteanbieters eingebunden sind. Dagegen ermöglicht § 154 Abs. 2 AO bei wichtigem Anlass[22] auch eine Identifizierung durch zuverlässige Dritte ohne diese formelle Voraussetzung.[23]

---

21 Nr. 8 der Verlautbarung des Bundesaufsichtsamtes für das Kreditwesen über Maßnahmen der Kreditinstitute zur Bekämpfung und Verhinderung der Geldwäsche vom 30.3.1998.

22 Als solcher gilt nach dem „Leitfaden zur Bekämpfung der Geldwäsche“ des Zentralen Kreditausschusses, der mit dem (damaligen) Bundesaufsichtsamt für das Kreditwesen abgestimmt ist, Rn. 7a, 3. Alternative etwa auch eine größere räumlichen Distanz zur Zweigstelle des Kreditinstituts.

23 S. Nr. 10 der Verlautbarungen (Fn. 21).

3. Erleichtertes Ausgabeverfahren

Nach Nr. 3 kann auf eine „Übergabe der Signaturschlüssel und Identifikationsdaten sowie Vorkehrungen zur Geheimhaltung der Identifikationsdaten“ nach § 5 Abs. 4 SigG und § 5 SigV verzichtet werden, „soweit ein von der Bundesanstalt für Finanzdienstleistungsaufsicht oder den Spitzenverbänden der deutschen Kreditwirtschaft für den Versand von ec-Karten und zugehörigen PIN-Briefen gebilligtes vergleichbares Verfahren eingesetzt wird“. Auch diese Regelung erlaubt zwei Ausnahmen von den Anforderungen an qualifizierte elektronische Signaturverfahren.

Nach § 5 Abs. 1 Satz 2 SigV hat der Zertifizierungsdiensteanbieter Vorkehrungen zu treffen, um die Geheimhaltung von Identifikationsdaten zu gewährleisten. Von dieser Pflicht wird er zwar nicht entbunden. Er muss aber nicht genau die Vorkehrungen treffen, die sich bisher im Verwaltungsvollzug der SigV als geeignet herausgestellt haben. Er kann diese vielmehr durch Sicherheitsvorkehrungen ersetzen, die den in Nr. 3 genannten Verfahren entsprechen. Sie müssen nicht von den genannten Instanzen im Einzelfall genehmigt sein.

Nach § 5 Abs. 2 Satz 1 SigV hat der Zertifizierungsdiensteanbieter dem Signaturschlüssel-Inhaber die vom ihm erzeugten Signaturschlüssel und Identifikationsdaten persönlich zu übergeben und die Übergabe von diesem schriftlich oder mit qualifizierter elektronischer Signatur bestätigen zu lassen. Von diesen Vorgaben entbindet die StDÜV insoweit, als diese Form der Übergabe durch ein in Nr. 3 genanntes Verfahren ersetzt wird. Eine persönliche Übergabe und eine schriftliche Bestätigung sind danach nicht notwendig, wohl aber die getrennte Versendung von Karte und PIN-Brief.

2.4.4 Ungeprüfte technische Komponenten

Nach Nr. 4 kann auf einen Einsatz von Produkten gemäß §§ 5 Abs. 5, 15 Abs. 7 SigG sowie §§ 5 Abs. 1, 15 und der Anlage 1 SigV verzichtet werden.

Für qualifizierte elektronische Signaturen fordert § 5 Abs. 5 SigG im zweiten Halbsatz, dass der Zertifizierungsdiensteanbieter Produkte für qualifizierte elektronische Signaturen einsetzt, die mindestens die Anforderungen nach §§ 4 bis 14 SigG sowie § 17 oder § 23 SigG und der Signaturverordnung erfüllen. Damit können aber nicht alle Produkte für qualifizierte elektronische Signaturen nach § 2 Nr. 13 SigG gemeint sein, sondern entsprechend § 7 Abs. 1 Nr. 2 b) StDÜV nur diejenigen, die Zertifizierungsdiensteanbieter benutzen. Für Signaturerstellungseinheiten sind die Anforderungen bereits in § 7 Abs. 1 Nr. 2a StDÜV beschrieben. Für Signaturanwendungskomponenten enthalten § 17 Abs. 2 SigG und § 15 Abs. 2 SigV und für technische Komponenten für Zertifizierungsdienste § 17 Abs. 3 SigG und § 15 Abs. 3 SigV funktionale Anforderungen. Die Einhaltung der Anforderungen an die Komponenten zur Schlüsselerzeugung und -personalisierung ist nach § 17 Abs. 4 SigG durch Bestätigungsstellen, die Einhaltung der Anforderungen an technische Komponenten für Verzeichnis- und Sperrdienste, für Zeitstempeldienste und für die Signaturanwendung ist durch Herstellererklärungen zu bestätigen.

Auf die in § 17 Abs. 2 und 3 SigG und § 15 Abs. 2 und 3 SigV genannten funktionellen Anforderungen kann nicht vollständig verzichtet werden, wenn die Verfahren auch nur fortgeschrittene Signaturen im Sinn des § 2 Nr. 2 SigG ermöglichen sollen.[24] Die Ausnahme der Nr.

[24] S. näher *Roßnagel*, MMR 2003, 165.

4 ist daher so zu verstehen, nicht die Nutzung unsicherer Produkte ermöglicht, sondern die „Nutzung gleichwertiger Produkte“ gestattet wird.[25] Sie behält „die wesentlichen Anforderungen“ bei, verzichtet aber auf eine buchstabengetreue Befolgung, wenn die technischen Komponenten die genannten grundlegenden Sicherheitsfunktionen erfüllen. Nr. 4 ermöglicht, auf die in § 17 Abs. 4 SigG geforderten Nachweise zu verzichten, ohne allerdings wesentliche Ausnahmen bei den materiell-funktionalen Anforderungen zuzulassen.

Die zweite Ausnahme betrifft § 15 Abs. 7 SigG. Diese Ausnahme ist unverständlich, da § 15 Abs. 7 SigG nur für Signaturverfahren akkreditierter Zertifizierungsdiensteanbieter gilt.

Die dritte Ausnahme der Nr. 4 betrifft Sicherheitsanforderungen an die Schlüsselerzeugung und -personalisierung sowie an die Geheimhaltung der Identifikationsdaten nach § 5 Abs. 1 SigV. Eine sichere Schlüsselerzeugung und eine Geheimhaltung der Identifikationsdaten sind essentiell für die Sicherheit von Signaturverfahren. Daher kann auch diese Ausnahme nicht so verstanden werden, dass sie vollständig von diesen Anforderungen befreit. Vielmehr lässt sie auch Realisierungen zu, die eine gleichwertige Sicherheit auf andere Weise bieten.

Die vierte Ausnahme der Nr. 4 betrifft die Anlage 1 SigV, die Vorgaben für die Prüfung von Produkten für qualifizierte elektronische Signaturen enthält. Sie ermöglicht die Verwendung von Produkten mit gleichwertiger Sicherheit, auch wenn deren Nachweis nicht den Anforderungen der Anlage 1 SigV entsprechen.

5. Verzicht auf die Prüfung des Besitzes der richtigen Signaturerstellungseinheit

Nach Nr. 5 kann auf eine Feststellung, dass der Antragsteller die zugehörige Signaturerstellungseinheit besitzt, verzichtet werden. § 5 Abs. 6 SigG fordert von einem Zertifizierungsdiensteanbieter, dass er sich in geeigneter Weise davon überzeugt, dass der Antragsteller für ein Zertifikat die Signaturerstellungseinheit besitzt, auf der der zum Zertifikat passende Signaturschlüssel gespeichert ist. Sofern der Antragsteller die Signaturerstellungseinheit vom Zertifizierungsdiensteanbieter erhält, hat dieser nach § 5 Abs. 2 Satz 1 SigV sich die Übergabe schriftlich oder mit Signatur bestätigen zu lassen. Diese Überprüfung oder Bestätigung kann nach Nr. 5 entfallen.

6. Verzicht auf eine Bestätigung der Belehrung

Nach Nr. 6 kann auf eine gesonderte Unterschrift des Antragstellers über die Kenntnisnahme der Belehrung verzichtet werden. Diese Ausnahme betrifft nicht die Belehrung als solche, wohl aber die von § 6 SigG und § 6 SigV geforderte unterschriebene Bestätigung ihrer Kenntnisnahme. Für eine qualifizierte elektronische Signatur mit Einschränkungen genügt es, die Belehrung mit der Signaturerstellungseinheit oder dem PIN-Brief zu versenden.

7. Verzicht auf eine Sperrung per Telefon

Nach Nr. 7 kann auf eine Bekanntgabe einer Telefonnummer zur Sperrung der Zertifikate verzichtet werden, „soweit eine Telefaxnummer bzw. eine E-Mail-Adresse zu diesem Zweck mitgeteilt wird“. Diese Ausnahme befreit nicht von der Anforderung, einen Sperrdienst „rund um die Uhr“ zu unterhalten, der die Berechtigung zur Sperrung überprüft und eine berechtigte Sperrung unverzüglich veranlasst. Sie befreit aber von der in § 7 Abs. 1 SigV vorgesehenen

[25] Amtl. Begr., BR-Drs. 982/02, 14.

Modalität des Sperrdiensts, dass der Zertifizierungsdiensteanbieter den zur Sperrung Berechtigten eine Rufnummer bekannt zu geben hat, unter der diese eine Sperrung veranlassen können. Die Rufnummer kann durch eine Telefaxnummer oder eine E-Mail-Adresse ersetzt werden. Dadurch macht Nr. 7 zugleich deutlich, dass sie keine so hohen Anforderungen an die Unverzüglichkeit der Sperrung stellt wie § 7 Abs. 1 SigV, da es bei Fax und E-Mail genügen muss, wenn in vertretbaren Intervallen der Eingang überprüft wird.

8. Dokumentation nach Handels- und Steuerrecht

Nach Nr. 8 kann auf eine Dokumentation gemäß § 10 SigG und § 8 SigV verzichtet werden, „soweit die Dokumentation des Zertifizierungsdiensteanbieters den Aufzeichnungspflichten des Handels- und Steuerrechts entspricht". Diese Erleichterung führt nicht dazu, dass die Dokumentation nach § 10 SigG und § 8 SigV entfallen kann. Sie kann auch nicht einfach durch die ohnehin vorzunehmenden Aufzeichnungen nach Handels- und Steuerrecht ersetzt werden. Denn diese dienen weitgehend anderen Zwecken. Nach Nr. 8 muss weiterhin eine „Dokumentation des Zertifizierungsdiensteanbieters" erfolgen, die zumindest den Aufzeichnungspflichten des Handels- und Steuerrechts entsprechen muss. Dies kann Erleichterungen für Form und Sicherung der Dokumentation sowie den Zeitraum ihrer Aufbewahrung bringen.[26] Die Anforderungen an den Inhalt der Dokumentation ergeben sich aus § 10 SigG und § 8 SigV.[27]

9. Haftung und Deckungsvorsorge

Nach Nr. 9 kann auf die Bestimmungen über die Haftung gemäß § 11 SigG und die Deckungsvorsorge gemäß § 12 SigG, § 9 SigV verzichtet werden, „soweit verbindliche Regelungen zur Haftung und zur besonderen Deckungsvorsorge durch den Betreiber des Zertifizierungsdienstes vorliegen". Auf die genannten Bestimmungen kann der Zertifizierungsdiensteanbieter natürlich nicht „verzichten". Mit dieser ungeschickten Formulierung ist gemeint, dass die Haftungsregelungen des § 11 SigG und die Verpflichtung zur Deckungsvorsorge durch Allgemeine Geschäftsbedingungen des Zertifizierungsdiensteanbieters ersetzt werden können, in denen er sich selbst zur Haftung und Deckungsvorsorge verpflichtet. Um ein vergleichbares Sicherheitsniveau wie bei qualifizierten Signaturverfahren zu bieten, ist dabei eine vergleichbare Haftung des Zertifizierungsdiensteanbieters und eine vergleichbar sichere „besondere Deckungsvorsorge" vorzusehen, wie sie die §§ 11 und 12 SigG und § 9 SigV fordern. Abweichungen im Detail sind zulässig.

10. Anzeige der Einstellung der Tätigkeit gegenüber der Finanzverwaltung

Nach Nr. 10 kann auf „Bestimmungen über die Einstellung der Tätigkeit" gemäß § 13 SigG, § 10 SigV verzichtet werden, „soweit die Einstellung der Zertifizierungsdienste dem Bundesministerium der Finanzen und den obersten Finanzbehörden der Länder unverzüglich angezeigt wird". Nach dieser Ausnahme kann auf die Erfüllung der Anforderungen des § 13 SigG verzichtet werden, bei einer Einstellung des Betriebs dafür zu sorgen, dass die Zertifikate von einem anderen Zertifizierungsdiensteanbieter übernommen werden, die Zertifikate zu sperren, die Signaturschlüssel-Inhaber zu informieren und die Dokumentation an den übernehmenden Zertifizierungsdiensteanbieter oder die Regulierungsbehörde zu übergeben. Als Anforderung

---

[26] Für Kreditinstitute stellt allerdings § 9 GwG vergleichbare oder sogar höhere Anforderungen an die Sicherungsmaßnahmen und den Zeitraum der Aufbewahrung.

[27] S. zu diesen *Roßnagel*, in: *ders*. (Hrsg.), Recht der Multimediadienste, 1999 ff., § 10 SigG, Rn. 26 ff. und § 13 SigV, Rn. 25 ff.

bleibt nach Nr. 10 nur die Anzeige an die zuständige Finanzbehörden. Das Sperren der Zertifikate und die Unterrichtung der Signaturschlüssel-Inhaber dürfte allerdings bereits vertragsrechtlich geboten sein, so dass faktisch nur die Suche nach einem anderen Zertifizierungsdiensteanbieter und die Übergabe der Dokumentation an diesen entfallen.

11. Auslagerung ins Ausland

Nach Nr. 11 kann auf eine „freiwillige Akkreditierung und Aufsicht bei einem teilweisen Betrieb des Zertifizierungsdienstes in Drittstaaten“ gemäß § 23 SigG verzichtet werden, „soweit ein Betreiberkonzept vorliegt und eine Vereinbarung über die Einhaltung der deutschen Regelungen zum Datenschutz getroffen wird“. Mit diesen Ausnahmen soll der „Betrieb von Teilen des Zertifizierungsdienstes in anderen Staaten“ gestattet werden.[28] Um diesen Zweck zu erreichen, ist die Ausnahmeregelung missglückt. Zum einen ist der Betrieb von Teilen des Zertifizierungsdienstes in anderen Staaten nach § 4 Abs. 5 SigG – nicht § 23 SigG – bereits zulässig.[29] Zum anderen ist eine freiwillige Akkreditierung für das Angebot von qualifizierten Zertifikaten weder für den Anbieter noch für den Betreiber der ausgelagerten Teilprozesse erforderlich. Schließlich regelt § 23 Abs. 1 SigG die Gleichstellung von Signaturen mit ausländischem qualifiziertem Zertifikat mit Signaturen mit einem Zertifikat aus Deutschland. Er regelt weder den Betrieb von Teilen des Zertifizierungsdienstes im Ausland noch die Aufsicht über diese im Ausland betriebenen Teile. Die Ausnahmeregelung ist in allen drei Fällen überflüssig. Gemeint ist, dass der Betrieb von Teilen des Zertifizierungsdienstes im Ausland keiner Aufsicht deutscher Behörden unterliegen soll, wenn ein entsprechendes Betreiberkonzept und eine Vereinbarung über die Einhaltung der deutschen Regelungen zum Datenschutz vorliegt.

VI. Bewertung

§ 87a Abs. 6 AO und die StDÜV sind aus signaturrechtlicher Sich kein gelungener Wurf – nicht nur wegen der vielen Handwerksfehler – diese wird die Rechtswissenschaft korrigieren und mit diesen wird die Praxis leben lernen, sondern vor allem wegen der wirtschaftspolitischen Folgen. Allein kurzfristiger Ressortvorteile wegen für das Steuerverfahren eine eigene – fünfte – Stufe elektronischer Signaturen einzuführen, ist nicht nur verwirrend, sondern für die Entwicklung des E-Government, aber auch des E-Commerce und des gesamten elektronischen Rechtsverkehrs und letztlich für den Wirtschaftsstandort Deutschland schädlich.

Die Finanzverwaltung mag hiervon gewisse Vorteile haben: Wer ohnehin und aus anderen Gründen eine Signaturkarte hat – etwa als Karte für das Online-Banking oder als Dienst- und Unternehmensausweis – kann diese auch für die elektronische Steuererklärung verwenden. Insofern kann ELSTER durch diese Regelung einen kleinen Aufschwung erfahren. Dieser dürfte aber begrenzt sein, weil außer den Verfahren der Kreditinstituten – an deren Signaturverfahren die Regelung des § 7 StDÜV orientiert ist – wohl nur wenige sonstige Signaturverfahren genau diese Anforderungen erfüllen.

Die qualifizierte elektronische Signatur mit Einschränkungen ist einfunktional – für sie gibt es neben ELSTER keine gesetzlich geregelte Verwendungsmöglichkeit. Kaum jemand wird eine Signaturkarte kaufen, allein um damit Steuerdaten zu signieren. E-Government, E-Commerce und der gesamte elektronische Rechtsverkehr sind jedoch darauf angewiesen, dass

---

[28] Amtl. Begr., BR-Drs. 982/02, 14.

[29] Dies im Fall des akkreditierten Zertifizierungsdiensteanbieters Authentidate bereits praktiziert.

für möglichst viele Anwendungen nutzbare Signaturverfahren zur Anwendung gelangen.[30] Hierfür hätte ELSTER – neben anderen Anwendungen – ein Anreiz sein können. Wenn aber jeder – wie die Finanzverwaltung – nur ihre Ressortinteressen verfolgt, wird es nie zu einer breiten Nutzung eines Signaturverfahrens kommen, das in vielen Anwendungen eingesetzt werden kann.

Ist die zeitliche Befristung für qualifizierte elektronische Signaturen mit Einschränkungen ernst gemeint, werden jetzt Public-Key-Infrastrukturen aufgebaut und Signaturkarten ausgegeben, die spätestens nach drei Jahren nicht mehr für den Zweck der Steuerdatenübermittlung verwendet werden können. Sie müssen dann weggeworfen und durch Karten und Infrastrukturen für qualifizierte elektronische Signaturen ersetzt werden. Für die für viele andere Anwendungen erforderliche qualifizierte elektronische Signatur sind dies drei verlorene Jahre.

§ 87a Abs. 6 AO und § 7 StDÜV sind kein Vorbild für eine Fortentwicklung des Signaturrechts. Sie sind nicht an Anforderungen eines offenen Rechtsverkehrs orientiert, sondern an den bestehenden Verfahren der Kreditinstitute,[31] die andere Zielsetzungen haben – nämlich die Absicherung des Verkehrs zwischen Kunde und Bank. Durch die Ausnahmen des § 7 StDÜV bleiben zu viele unverantwortbare Lücken hinsichtlich der technischen und organisatorischen Sicherheit für eine verlässliche Zuordnung des Signaturschlüssels zum Signaturschlüssel-Inhaber. Diese sind vielleicht für das Steuerverfahren akzeptabel, in dem es eine kontinuierliche Beziehung zwischen Verwaltung und Bürger gibt, aus der viele weitere Anhaltspunkte für die Integrität und Authentizität einer Erklärung genommen werden können und in der sich viele Korrekturmöglichkeiten bieten. Dies gilt aber nicht für die Zurechnung einer signierten Willenserklärung in einem offenen Netz mit unbekannten Kommunikationspartnern. Daher besteht keine Chance, den Anwendungsbereich für die qualifizierte elektronische Signatur mit Einschränkungen zu erweitern.

Die vorübergehende Einführung der qualifizierten elektronischen Signatur mit Einschränkungen gibt das falsche Signal an den Markt, der ohnehin auf positive Impulse für die Verwendung von qualifizierten elektronischen Signaturen nach dem SigG angewiesen ist. Richtig wäre es gewesen, mit den Banken und anderen über eine sofortige Migration ihrer Verfahren auf das Niveau qualifizierter elektronischer Signaturen zu sprechen und sie dabei zu unterstützen. Dabei könnte bei funktionaläquivalenter Sicherheit auf die bisherigen internen Prozesse der Kreditinstitute Rücksicht genommen werden. Dies darf aber nicht die für rechtlich relevante Erklärungen notwendige Sicherheit von Signaturen untergraben – wie in der Richtlinie für elektronische Signaturen und zu deren Umsetzung im SigG festgelegt worden ist.

Zum Autor: Prof. Dr. Alexander Roßnagel ist Universitätsprofessor für öffentliches Recht an der Universität Kassel, dort Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR), Saarbrücken.

30 S. näher *Roßnagel*, MMR 2003, 1f.

31 In Fachkreisen wird diese Regelung daher auch „Lex Deutsche Bank“ genannt.