

ALEXANDER ROßNAGEL / STEFANIE FISCHER-DIESKAU

## Automatisiert erzeugte elektronische Signaturen

*Von großer wirtschaftlicher Relevanz dürften künftig elektronische Signaturen sein, die für Massenanwendungen in automatischen Prozessen erzeugt werden. Solche Signaturen sind jedoch weder im Signaturgesetz (SigG) noch in der Signaturverordnung (SigV) geregelt worden. Vielmehr orientieren sich deren Vorschriften ausschließlich an der „eigenhändig“ erzeugten elektronischen Si-*

*gnatur. Der Beitrag untersucht daher, ob automatisiert erzeugte elektronische Signaturen (I.) als fortgeschrittene (II.) oder qualifizierte elektronische Signaturen anerkannt werden können (III.) und welche Rechtsfolgen mit ihnen verbunden sind (IV.). Abschließend wird die Frage nach einer Reform einschlägiger Regelungen gestellt (V.).*

### I. Automatisiert erstellte Signaturen

Die Automatisierung von Datenverarbeitungs-(DV)-Prozessen ist ein wesentlicher Ansporn für die Weiterentwicklung der Informationstechnik und ihren Einsatz in immer mehr Anwendungen. Die Automatisierung wird vor allem zur Rationalisierung von Massenverfahren eingesetzt. Sie kann ihre rationalisierende Wirkung aber meist nur dann entfalten, wenn der gesamte Prozess automatisiert ist. Soweit Integrität und Authentizität der automatisch erzeugten Daten durch elektronische Signaturen abgesichert werden sollen, streben die Verantwortlichen demgemäß auch eine Automatisierung der Signaturerzeugung an. Müsste

die Signatur jedes Mal „von Hand“ erzeugt werden, gingen im Regelfall die Rationalisierungsgewinne durch die Automatisierung des sonstigen Prozesses verloren. Aus rechtlicher Sicht sind mit der automatisierten Erzeugung von elektronischen Signaturen jedoch einige Fragen verbunden, denen sich dieser Beitrag widmet.

Als automatisierte elektronische Signatur wird im Folgenden eine Signatur verstanden, die von einem automatischen Prozess ohne Zutun eines Menschen erzeugt wird. Dabei wird davon ausgegangen, dass ein Mensch diesen Prozess bewusst angestoßen hat, dass er aber weder die zu signierenden Daten im Einzelfall vor der Signatur überprüft noch den geheimen Schlüssel im Einzelfall freischaltet noch den Befehl zur Erzeugung der Signatur im Einzelfall gibt.

Automatisierte elektronische Signaturen werden in der Praxis bereits erstellt. Signaturkomponenten sind mit DV-

■ 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. Stefanie Fischer-Dieskau ist wissenschaftliche Mitarbeiterin in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet).

Prozessen in einer Form verbunden, dass die aus dem Prozess entstehenden Daten mit einer ausreichenden Performance signiert werden. Sie finden Einsatz zum Beispiel in der Erstellung von Rechnungen,<sup>1</sup> Zertifikaten,<sup>2</sup> Auskünften aus Verzeichnisdiensten,<sup>3</sup> Zeitstempeln<sup>4</sup> und erneuten Signaturen nach § 17 SigV.<sup>5</sup> Es ist damit zu rechnen, dass sie zukünftig z.B. auch für Bestätigungen, Beglaubigungen, automatisierte Bescheide, Quittungen und Eingangsbestätigungen, aber auch für eingescannte Unterlagen<sup>6</sup> zum Einsatz kommen.

Weitgehend gelöst ist das Problem, ob durch eine automatisiert erzeugte elektronische Signatur eine dem Autor zurechenbare Willenserklärung hergestellt werden kann. Eine von einer DV-Anlage hergestellte Erklärung ist dem Betreiber dieser Anlage zuzurechnen, wenn der Einsatz der Anlage auf dessen Willen beruht und er sich die von der DV-Anlage hergestellten Erklärungen als „eigene“ zurechnen lassen will.<sup>7</sup> Es gibt keinen Grund anzunehmen, dass dies bei einer automatisiert erzeugten elektronischen Signatur anders sein sollte. Dies sah auch der Gesetzgeber so, der in der Begründung zum SigG 1997 ausführte: „Da letztlich immer eine natürliche Person über den Einsatz von Rechnern und die Verarbeitung von Daten sowie die jeweiligen Anwendungsprogramme entscheidet, können auch automatisch erstellte Signaturen auf eine menschliche Handlung zurückgeführt werden.“<sup>8</sup>

Weiterhin dürfte die Feststellung auf allgemeine Zustimmung stoßen, dass die automatisiert erstellte elektronische Signatur eine elektronische Signatur i.S.d. SigG ist. Sie erfüllt nämlich die Definition des § 2 Nr. 1 SigG, da sie Daten enthält, die anderen Daten beigefügt sind und der Authentifizierung dienen sollen.

Fraglich ist jedoch, ob eine automatisierte elektronische Signatur die Definition der fortgeschrittenen elektronischen Signatur nach § 2 Abs. 2 SigG erfüllt oder gar als qualifizierte elektronische Signatur nach § 2 Nr. 3 SigG angesehen werden kann. Für viele elektronische Dokumente, die in Massenverfahren erzeugt werden, verlangt das Gesetz inzwischen eine fortgeschrittene<sup>9</sup> oder eine qualifizierte elektronische Signatur.<sup>10</sup> Die dogmatische Einordnung der automatisierten elektronischen Signatur ist somit von hoher praktischer und wirtschaftlicher Relevanz. Sie soll im Folgenden näher untersucht werden.

## II. Fortgeschrittene elektronische Signatur?

Um fortgeschrittene elektronische Signaturen zu sein, müssen elektronische Signaturen die vier Definitionsmerkmale des § 2 Nr. 2 SigG erfüllen. Sie müssen

- lit. a) die ausschließliche Zuordnung der Signatur zum Signaturschlüsselinhaber gewährleisten,
- lit. b) die Identifizierung des Signaturschlüsselinhabers ermöglichen,
- lit. c) mit Mitteln erzeugt werden, die der Signaturschlüsselinhaber unter seiner alleinigen Kontrolle halten kann und
- lit. d) mit den Daten, auf die sie sich beziehen, so verknüpft sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Kein Problem dürfte im Regelfall das Definitionsmerkmal (lit. d) bereiten. Dieses wird jedenfalls dann erfüllt, wenn die Signatur auf geeigneten asymmetrischen Kryptographieverfahren beruht und mit sicherheitsgeeigneten Hash- und Signaturalgorithmen und -parametern<sup>11</sup> erzeugt wurde.<sup>12</sup>

Für die anderen drei Definitionsmerkmale ist die Bewertung jedoch nicht so einfach. Gegen die Einordnung der automatisierten elektronischen Signatur als fortgeschrittene Signatur könnte nämlich geltend gemacht werden, sie stünde der konzeptionellen Idee der elektronischen Signatur als Unterschriftenersatz entgegen. Insbesondere die zwingende Zuordnung zu einer natürlichen Person stehe im Widerspruch zu ihrer Erzeugung durch einen automatisierten Prozess. Weiterhin könnte geltend gemacht werden, eine fortgeschrittene elektronische Signatur setze im Einzelfall die Eingabe des persönlichen Identifikationsdatums des Signaturschlüsselinhabers voraus.

### 1. Ausschließliche Zuordnung zum Signaturschlüsselinhaber

Die ausschließliche Zuordnung zum Signaturschlüsselinhaber könnte dadurch in Frage gestellt sein, dass die einzelne Signatur nicht vom Signaturschlüsselinhaber, sondern von dem automatisierten Prozess erzeugt wird. Unter Signaturschlüsselinhaber versteht § 2 Nr. 9 SigG eine natürliche Person, die den Signaturschlüssel besitzt und der die zugehörigen Signaturprüfchlüssel durch qualifizierte Zertifikate zugeordnet sind. Diese Definition trifft eigentlich nur auf qualifizierte elektronische Signaturen zu. Jedoch verwendet § 2 Nr. 2 SigG diesen Begriff auch für fortgeschrittene elektronische Signaturen. Trotz dieser Ungeheimtheit ist aus der Definition jedenfalls zu folgern, dass für fortgeschrittene elektronische Signaturen zwar kein qualifiziertes Zertifikat verlangt werden kann, dass aber die anderen Definitionsmerkmale, nämlich der Besitz des Signaturschlüssels durch eine natürliche Person und die Zuordnung des Signaturprüfchlüssels zu dieser Person durch ein Zertifikat erforderlich sind.<sup>13</sup>

Die Beschränkung auf natürliche Personen rechtfertigt die Begründung zum SigG 2001 – nur für qualifizierte elektronische Signaturen<sup>14</sup> – mit dem Hinweis, dies sei durch die in Art. 5 Abs. 1 RLeS vorgesehene rechtliche Gleichstellung qualifizierter elektronischer Signaturen mit der handschriftlichen Unterschrift vorgegeben.<sup>15</sup> Allgemeiner wurde dies in der Begründung zum SigG 1997<sup>16</sup> und in der Literatur<sup>17</sup> damit begründet, dass eine digitale Signatur „wie eine eigenhändige Unterschrift“ immer an eine natürliche Person gebunden sei.<sup>18</sup> Dies könnte zu dem Schluss verleiten, dass das Konzept elektronischer Signaturen, wie es im SigG ausgestaltet ist, die Erzeugung von Signaturen – ebenso wie die Erzeugung von eigenhändigen Unterschriften –

1) PM von *t-mobil* zur elektronischen Telefonrechnung v. 24.1.2003.

2) S. z.B. *Roßnagel*, in: ders. (Hrsg.), *Recht der Multimediadienste*, § 2 SigG Rdnr. 67.

3) S. z.B. *Roßnagel* (o. Fußn. 2), § 2 SigG Rdnr. 67.

4) S. z.B. *Roßnagel* (o. Fußn. 2), § 2 SigG Rdnr. 67, 79; [www.authentidate.de](http://www.authentidate.de).

5) S. z.B. *Brandner/Pordesch*, DuD 2003, 354; *Roßnagel/Fischer-Dieskau/Pordesch/Brandner*, CR 2003, 301.

6) Dies wird z.Zt. insb. im Zusammenhang mit der virtuellen Poststelle diskutiert.

7) S. für die h.M. z.B. *Mehrings*, in: *Hoeren/Sieber*, *Handbuch Multimedia-Recht*, 13.1 Rdnr. 48.

8) BT-Drs. 13/7385, S. 27.

9) § 87 Abs. 6 AO und § 7 StDÜV – s. hierzu *Roßnagel*, K&R 2003, 379.

10) § 14 Abs. 4 UStG; § 33 Abs. 4 Nr. 4 b) VwVfG.

11) S. Anh. I, Nr. 1.2 zur SigV.

12) S. näher *Roßnagel*, MMR 2003, 166.

13) S. *Roßnagel*, MMR 2003, 165.

14) Dass diese Einschränkung durch Verweis auf den Signaturschlüsselinhaber auch für fortgeschrittene Signaturen gilt, wird in der amtl. Begr. nicht thematisiert.

15) BT-Drs. 14/4662, S. 19.

16) BR-Drs. 966/96, S. 29, 29 f., 31 f.

17) S. z.B. *Bieser/Kersten*, *Chipkarte statt Füllfederhalter*, 1998, S. 50.

18) So auch die *Reg TP*, [www.regtp.de](http://www.regtp.de), FAQ 19.

durch natürliche Personen vorsehe und ihre Erzeugung durch automatische Prozesse ausschließe.

Eine solche Sicht würde jedoch mehreren Trugschlüssen erliegen. Zum einen erlaubt die Möglichkeit, die qualifizierte elektronische Signatur der eigenhändigen Unterschrift gleichzustellen, nicht den Umkehrschluss, dass alle qualifizierten elektronischen Signaturen ein Substitut der Unterschrift sind. Für viele Bereiche, in denen eine qualifizierte elektronische Signatur gefordert wird, wie z.B. für die Rechnung nach § 14 Abs. 4 UStG und für die erneute Signatur nach § 17 SigV, ist die Signatur kein Ersatz für eine Unterschrift, da diese gar nicht gefordert ist.<sup>19</sup> Zum anderen gilt die Forderung nach einer ausschließlichen Zuordnung der Signatur zu einer natürlichen Person auch für fortgeschrittene elektronische Signaturen, mit deren Hilfe zwar eine gewillkürte, nicht aber eine gesetzliche Schriftform ersetzt werden kann.<sup>20</sup> Für diese Signaturen gilt in noch stärkerem Maß, dass sie nicht in allen Fällen ein Ersatz für die Unterschrift sind. Drittens ist an die grundsätzliche Konzeption des SigG zu erinnern. Es soll Rahmenbedingungen für die Sicherungsinfrastruktur und die technischen Komponenten von Signaturverfahren schaffen, bei deren Erfüllung elektronische Signaturen eine hohe faktische Sicherheit erlangen und bei deren Verwendung im elektronischen Rechts- und Geschäftsverkehr der Urheber und die Integrität der Daten zuverlässig festgestellt werden können. Dies wird zwar als eine notwendige Voraussetzung dafür angesehen, dass die elektronische Signatur ein Substitut zur handschriftlichen Unterschrift darstellen und hierdurch eine entsprechende Rechtswirkung entfalten kann. Im SigG selbst werden jedoch keine Rechtsfolgen des Einsatzes von Signaturen geregelt. Ob eine Signatur als Ersatz einer Unterschrift oder zu anderen Zwecken vorgesehen wird, soll vielmehr besonderen Gesetzen überlassen werden.<sup>21</sup>

Schließlich wäre es auch unzulässig, ein Konzept in das SigG hineinzulesen, das so im Text keine Ausprägung gefunden hat. Der notwendige Bezug zu einer natürlichen Person wird im SigG nur hinsichtlich der Zuordnung eines Zertifikats hergestellt. Eine grundsätzliche Beschränkung, dass Signaturen immer nur im Einzelfall durch natürliche Personen erzeugt werden müssen, ist dem SigG nicht zu entnehmen.<sup>22</sup>

Gegen einen grundsätzlichen Ausschluss von automatisierten elektronischen Signaturen aus dem Bereich der fortgeschrittenen oder qualifizierten Signaturen sprechen

auch die amtlichen Begründungen zum SigG und zur SigV. Bereits die amtliche Begründung zum SigG 1997 erkannte die Möglichkeit automatisierter elektronischer Signaturen an. Zwar sollten für diesen Fall „personenbezogene Signaturschlüssel eingesetzt werden“. Da aber „letztlich immer eine natürliche Person über den Einsatz von Rechnern und die Verarbeitung von Daten sowie die jeweiligen Anwendungsprogramme entscheidet, können auch automatisch erstellte Signaturen auf eine menschliche Handlung zurückgeführt werden.“<sup>23</sup> Dies wird durch die amtliche Begründung zur SigV 2001 bestätigt, die ausdrücklich die „automatische Erzeugung von Signaturen (Massensignaturen)“ erwähnt und besonderen Anforderungen unterstellt.<sup>24</sup> Auch die zuständige Behörde hält automatisierte elektronische Signaturen für mit dem SigG vereinbar.<sup>25</sup>

Somit kann festgehalten werden, dass es für die ausschließliche Zuordnung der Signatur zum Signaturschlüsselinhaber ausreicht, wenn eine personalisierte und im alleinigen Besitz des Signaturschlüsselinhabers befindliche Signaturerstellungseinheit<sup>26</sup> sowie ein auf eine natürliche Person ausgestelltes Zertifikat verwendet werden. Die Erzeugung von Signaturen durch einen automatischen Prozess steht dem nicht entgegen.

## 2. Identifizierung des Signaturschlüsselinhabers

Die Voraussetzung der Identifizierung des Signaturschlüsselinhabers ist nach der amtlichen Begründung dann erfüllt, wenn der öffentliche Prüfschlüssel durch ein Zertifikat dem Signaturschlüsselinhaber zugeordnet ist.<sup>27</sup> Dies gilt auch dann, wenn zur Erzeugung von Signaturen durch automatisierte Prozesse Pseudonyme (etwa „Rechnungsstelle 12“) eingesetzt werden.<sup>28</sup> Auf diese Weise kann dem Rechtsverkehr signalisiert werden, dass es sich um eine automatisierte elektronische Signatur und nicht um eine persönlich vom Signaturschlüsselinhaber erstellte Signatur handelt.<sup>29</sup> Die Verwendung solcher pseudonymen Zertifikate sieht insbesondere auch § 3a Abs. 2 VwVfG vor.<sup>30</sup> Probleme könnten sich allenfalls aus dem fehlenden bzw. begrenzten und umständlichen Aufdeckungsanspruch ergeben.<sup>31</sup>

## 3. Alleinige Kontrolle durch den Signaturschlüsselinhaber

Um die Mittel, mit denen die Signatur erzeugt wird, unter alleiniger Kontrolle zu halten, muss der Signaturschlüsselinhaber seine Signaturerstellungseinheit vor unbefugter Nutzung schützen können.<sup>32</sup> Dieses Definitionsmerkmal kann auch bei automatischer Erzeugung der Signatur entweder dadurch erfüllt werden, dass bei einer Hardwarelösung geeignete Chipkarten oder andere vergleichbare Datenträger verwendet werden, die auch über Schutzmechanismen verfügen, oder bei einer Softwarelösung dadurch, dass der Rechner durch hohe Sicherheitsmechanismen vor einem Zugriff Unberechtigter geschützt ist.<sup>33</sup> Wie diese Schutzmechanismen ausgestaltet sind, um eine unberechtigte Nutzung des Signaturschlüssels auszuschließen, lässt die Definition offen. Ob hierfür PIN, biometrische Merkmale oder sonstige Mechanismen genutzt werden, ist nicht festgelegt. Um die alleinige Kontrolle durch den Signaturschlüsselinhaber sicherzustellen, kann es erforderlich sein, die „Freischaltung“ des Signaturschlüssels auf einen kontrollierbaren Zeitrahmen oder eine kontrollierbare Anzahl von Signaturen zu beschränken.

## 4. Die automatisierte elektronische Signatur als fortgeschrittene elektronische Signatur

Zusammenfassend kann festgehalten werden, dass die automatische Erzeugung einer elektronischen Signatur ihrer

19) S. z.B. *Bunjes/Geist*, Komm. zum UStG, 7. Aufl. 2003, § 14 Rdnr. 8 und 13 ff.; *Roßnagel/Fischer-Dieskau/Pordesch/Brandner*, CR 2003, 301.

20) S. näher *Roßnagel*, MMR 2003, 168.

21) BT-Drs. 14/4662, S. 14.

22) Ob einzelne Vorschriften zusätzliche Anforderungen stellen, wird unter III. geprüft.

23) BR-Drs. 966/96, S. 29 f.; s. hierzu näher *Roßnagel* (o. Fußn. 2), § 2 SigG Rdnr. 64, 67 f.; *Bieser/Kersten* (o. Fußn. 17), S. 51.

24) Amtl. Begr. zu § 15 Abs. 2 SigV.

25) *Reg TP*, www.regtp.de, FAQ 18.

26) S. näher *Roßnagel*, MMR 2003, 165.

27) BT-Drs. 14/4662, S. 18; s. näher *Roßnagel*, MMR 2003, 165.

28) S. *Reg TP*, www.regtp.de, FAQ 18.

29) S. hierzu näher *Roßnagel* (o. Fußn. 2), § 2 SigG Rdnr. 68.

30) BT-Drs. 14/9000, S. 31; s. auch *Schlatmann*, DVBl. 2002, 1010; *Roßnagel*, NJW 2003, 472.

31) S. hierzu *Roßnagel*, NJW 2001, 1821; *ders.*, Datenschutz in Signaturverfahren, in: *ders.* (Hrsg.), Handbuch Datenschutzrecht, 2003, S. 1246 ff.; *Scholz*, Datenschutz beim Internet-Einkauf, 2003, S. 216 ff.; *Yildirim*, Datenschutz im eGovernment, 2004, i.E.

32) BT-Drs. 14/4662, S. 18.

33) Außerdem darf der Signaturschlüssel allein in der Signaturerstellungseinheit enthalten sein und kein zweites Mal existieren – s. näher *Roßnagel*, MMR 2003, 165.

Einordnung als fortgeschrittene elektronische Signatur nach § 2 Nr. 2 SigG nicht entgegensteht, wenn trotz dieser Erzeugungsform die vier Definitionsmerkmale erfüllt werden.

### III. Qualifizierte elektronische Signatur?

Zu prüfen bleibt nun, ob eine automatisierte elektronische Signatur auch die zusätzlichen Definitionsmerkmale einer qualifizierten elektronischen Signatur erfüllen kann. Eine qualifizierte elektronische Signatur ist nach § 2 Nr. 3 SigG eine fortgeschrittene Signatur mit den vier bereits genannten Definitionsmerkmalen, die aber darüber hinaus zwei weitere Merkmale aufweist. Sie muss zusätzlich

- lit. a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
- lit. b) mit einer sicheren Signaturerstellungseinheit erzeugt werden.

Beide Definitionsmerkmale verweisen auf weitere Definitionen des § 2 SigG. Ein qualifiziertes Zertifikat ist gem. § 2 Nr. 7 SigG eine elektronische Bescheinigung nach § 2 Nr. 6 SigG für natürliche Personen, die die Voraussetzungen des § 7 SigG erfüllt und von einem Zertifizierungsdiensteanbieter ausgestellt wird, der mindestens die Anforderungen nach den §§ 4 bis 14 oder 23 SigG und der sich darauf beziehenden Vorschriften der SigV erfüllt. Sichere Signaturerstellungseinheiten sind nach § 2 Nr. 10 SigG Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die mindestens die Anforderungen nach §§ 17 oder 23 SigG und der sich darauf beziehenden Vorschriften der SigV erfüllen und die für qualifizierte elektronische Signaturen bestimmt sind.

Durch diese Verflechtung von Definitionen sind qualifizierte elektronische Signaturen fortgeschrittene elektronische Signaturen, für die zusätzlich die spezifischen Anforderungen des SigG und der SigV an Zertifikate, Zertifizierungsdiensteanbieter und technische Komponenten erfüllt werden. Daher ist im Folgenden zu prüfen, welche dieser Anforderungen einer automatisierten elektronischen Signatur entgegenstehen. Gegen solche Signaturen könnte geltend gemacht werden, dass vor jeder Erzeugung einer qualifizierten elektronischen Signatur in die sichere Signaturerstellungseinheit die einschlägigen Identitätsdaten eingegeben werden müssten, die zu signierenden Daten angezeigt werden müssten und vor der Erzeugung einer Signatur ein Warnhinweis gegeben werden müsste.

#### 1. Eingabe von Identitätsdaten

Für eine qualifizierte elektronische Signatur konstitutiv ist nach § 2 Nr. 3 b) SigG die Verwendung einer sicheren Signaturerstellungseinheit. Diese muss gem. §§ 2 Nr. 10 und 17 Abs. 1 SigG gegen unberechtigte Nutzung der Signaturschlüssel schützen und darf entsprechend § 15 Abs. 1 Satz 1 SigV die Anwendung des Signaturschlüssels erst nach Identifikation des Inhabers durch Besitz und Wissen<sup>34</sup> ermöglichen.<sup>35</sup>

Aus den Anforderungen, die an eine sichere Signaturerstellungseinheit gestellt werden, lässt sich nur entnehmen, dass zur Nutzung des Signaturschlüssels eine Aktivierung der Signaturerstellungseinheit durch Identitätsdaten erforderlich ist. Ob dies vor der Erzeugung jeder einzelnen Signatur zu erfolgen hat, lassen SigG und SigV offen. Sie lassen daher dem Hersteller von sicheren Signaturerstellungseinheiten die Gestaltungsmöglichkeit, die Wirkung

der Eingabe von Identitätsdaten selbst zu bestimmen. Die Forderung, die Signaturerstellungseinheit so zu konstruieren, dass eine langfristige Aktivierung gar nicht möglich ist, lässt sich weder dem SigG noch der SigV entnehmen und ist weder mit dem Wortlaut noch mit dem Sinn und Zweck der Regelung des § 17 Abs. 1 SigG und § 15 Abs. 1 SigV vereinbar.

Zwar könnten bei einem längerfristigen Aktivieren der Karte z.B. andere Dokumente leichter untergeschoben und signiert werden. Doch ist dies vorrangig ein Problem, wie der Prozess der automatischen Generierung von Daten und deren Signierung sicher gestaltet werden kann, und nicht unmittelbar Ausfluss der längerfristigen Aktivierung der Signaturerstellungseinheit. Rechtlich gesehen betrifft dies die Frage, ob die Ergebnisse automatischer Prozesse ihrem Initiator zugerechnet werden können – eine Frage, die das SigG gerade nicht regeln und schon gar nicht als Aufgabe des Herstellers formulieren wollte.<sup>36</sup> Vielmehr sehen § 6 SigG und § 6 SigV eine sachgerechte Aufklärung über Möglichkeiten und Gefahren der Verwendung elektronischer Signaturen und der für sie erforderlichen technischen Komponenten durch den Zertifizierungsdiensteanbieter vor. Die Beachtung dieser Hinweise ist Sache des Signaturschlüsselhabers.

Dass eine sichere Signaturerstellungseinheit auch für mehrere Signaturen freigeschaltet werden kann, wird durch die amtliche Begründung zu § 15 Abs. 2 SigV bestätigt. Hier heißt es zu der Anforderung an die Signaturanwendungskomponente, dass eine Signatur nur durch die berechtigt signierende Person erfolgen darf: „Die Signaturkomponente darf nicht ohne Anwendung der Identifikationsdaten genutzt werden können, es sei denn, die Signaturen sollen für ein festes Zeitfenster oder eine bestimmte Anzahl ohne jeweilige Identifizierung erzeugt werden. In diesem Fall ist sicherzustellen, dass Unberechtigte keine Signaturen veranlassen können.“

#### 2. Anzeige zu signierender Daten

Die Signaturerstellungskomponenten müssen nach § 17 Abs. 2 Satz 1 SigG feststellen lassen, auf welche Daten sich die Signatur bezieht, und entsprechend § 17 Abs. 2 Satz 3 SigG nach Bedarf den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Diese Anforderungen sollen einen Missbrauch durch Unterschieben von Daten<sup>37</sup> oder durch geschickte Präsentation der Daten<sup>38</sup> erschweren. Die Anzeige dient damit auch als vorbereitende Maßnahme zur Umsetzung der Warnfunktion elektronischer Signaturen.<sup>39</sup> Diese Anforderungen an den Hersteller von Signaturerstellungskomponenten sollen diesen zwingen, die Kenntnisnahme der zu signierenden oder signierten Daten „nach Bedarf“ zu ermöglichen, nicht aber den Signaturschlüsselhaber, von dieser Möglichkeit auch immer Gebrauch zu machen. Dies gilt nicht

34) Unter bestimmten Umständen kann Wissen auch durch biometrische Merkmale ersetzt werden – s. zu diesen z.B. *Albrecht*, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, 2003, S. 78 ff.

35) Diese Forderung wird noch durch die Anforderung des § 15 Abs. 2 Nr. 1 b) SigV an die Signaturanwendungskomponente unterstützt, dass eine Signatur nur durch die berechtigt signierende Person erfolgen darf.

36) S. zur bewussten Nichtregelung von Rechtsfolgen für die Verwendung von Signaturen BT-Drs. 14/4662, S. 17.

37) S. hierzu z.B. *provet/GMD*, Die Simulationsstudie Rechtspflege, 1994, S. 126 ff.

38) S. hierzu ausführlich *Pordes*, Die elektronische Form und das Präsentationsproblem, 2002.

39) BT-Drs. 13/7385, S. 35, aml. Begr. § 15 SigV.

nur für § 17 Abs. 2 Satz 3 SigG, der ausdrücklich die Kenntnisnahme nur „nach Bedarf“ erwartet, sondern auch für § 17 Abs. 2 Satz 1 SigG. Nach dieser Vorschrift muss die Signaturerstellungskomponente die Möglichkeit der Kenntnisnahme nur zulassen, verpflichtet aber nicht den Signierenden zur Kenntnisnahme. Ist der Signierprozess so gestaltet, dass z.B. ein Unterschieben von zu signierenden Daten oder eine manipulierte Präsentation ausgeschlossen werden kann und verzichtet der Signierende bewusst auf die Kenntnisnahme des Inhalts, so besteht kein weiterer Bedarf ihrer Anzeige. Ob ein Bedarf besteht, entscheidet der Signierende. Dies ist auch sachgerecht: Die Anzeige soll nicht zum reinen Selbstzweck erfolgen,<sup>40</sup> sondern vielmehr möglichen „Bedrohungen“ entgegenwirken. Liegen diese nicht vor bzw. wird diesen auf andere Art und Weise sachgerecht entgegengewirkt, würde das Bestehen auf der Anzeige und ihrer Wahrnehmung keinen weiteren Sicherheitsmehrwert bringen und wäre daher überflüssig und sinnlos.

Die Anforderung, den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen zu lassen, steht somit einer automatisierten elektronischen Signatur nicht entgegen. Der Signierende kann auf die Anzeige der Daten verzichten. Er muss sich allerdings die dennoch signierten Daten als von ihm signiert anrechnen lassen. Er sollte daher den Risiken, denen durch die Anzeige entgegengewirkt werden soll, durch andere Maßnahmen entgegenwirken.

### 3. Warnhinweis

Nach § 17 Abs. 2 Satz 1 SigG sind für die Darstellung zu signierender Daten Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen. Nach der Konkretisierung dieser Anforderung in § 15 Abs. 2 Nr. 1 c) SigV muss „bei der Erzeugung einer qualifizierten elektronischen Signatur die Erzeugung einer Signatur vorher eindeutig angezeigt“ werden. Die Verpflichtung zur vorherigen eindeutigen Anzeige einer Signaturerzeugung könnte gegen die Zulässigkeit einer automatisierten Signaturerstellung sprechen.

Die eindeutige vorherige Anzeige der Signaturerzeugung dient ebenfalls als Warnhinweis und soll Fehlbedienungen, die zu ungewollten Signaturen führen, verhindern. Sie verlangt, auch wenn gesetzlich nicht geregelt, denklologisch zumindest eine Abbruchmöglichkeit. Die Warnung ist dabei nicht auf die zu signierenden Daten gerichtet, sondern betrifft allein den Signaturvorgang. Zweck der Anforderung ist somit allein der Hinweis, dass eine rechtserhebliche und verbindliche qualifizierte Signatur erstellt wird. Das Gesetz verlangt, die Erzeugung „vorher“ anzuzeigen, ohne eine weitere konkrete zeitliche Einordnung dessen vorzunehmen, was „vorher“ ist. Maßgeblich ist, dass vor jedem In-Gang-Setzen eines Signaturprozesses die damit verbundene Folge klar erkennbar wird. Eindeutig ist die Anzeige dann, wenn die signierende Person unmissverständlich erkennen kann, dass im nächsten Schritt ein Prozess zur Signaturerzeugung erfolgt.

§ 15 Abs. 2 Nr. 1 c) SigV fordert, dass die vorherige Anzeige vor Erstellung „einer“ Signatur erfolgt. Diese im Singular stehende Formulierung muss jedoch nicht in der Form ver-

standen werden, dass die Anzeige vor der Erzeugung „jeder“ Signatur erfolgen muss. Hätte die Verordnung diese Anforderung stellen wollen, hätte präziser statt des unbestimmten Artikels „einer“ die präzise Bestimmung „jeder“ verwendet werden müssen. Zusammen mit der Zielsetzung der Vorschrift, die Herstellung von Signaturanwendungskomponenten zu steuern, kann die Formulierung der Vorschrift nur so verstanden werden, dass die Komponenten eine Einstellung ermöglichen müssen, bei der die Erzeugung jeder einzelnen Signatur angezeigt wird. Die Vorschrift fordert aber nicht Signaturanwendungskomponenten, die ausschließlich eine solche Ausgestaltung aufweisen. Vielmehr sind auch Komponenten zulässig, die es in das Belieben ihres Nutzers stellen, als Ausfluss ihrer Privatautonomie die Einstellung der Anzeige selbst zu bestimmen.

Erforderlich ist also eine Anzeige vor dem In-Gang-Setzen des Erzeugungsprozesses. Wie viele Signaturen der Signaturschlüsselinhaber durch diesen Prozess oder für welchen Zeitraum er Signaturen erzeugt, liegt in seinem Ermessen. Entscheidet sich der Signaturschlüsselinhaber für die Erzeugung mehrerer Signaturen durch einen automatischen Prozess, benötigt er die erforderliche Kenntnisnahme des Warnhinweises nur vor dem Beginn dieses Prozesses. Weitere Warnhinweise während des ungestörten Ablaufs dieses Prozesses wären widersinnig und nicht vom Zweck des § 15 Abs. 2 Nr. 1 c) SigV umfasst.

Diese Interpretation entspricht auch der amtlichen Begründung dieser Anforderung. Danach muss „die Erzeugung einer Signatur ... durch einen Warnhinweis vorher angezeigt werden. Insbesondere bei der automatischen Erzeugung von Signaturen (Massensignaturen) muss sichergestellt sein, dass Signaturen nur zu dem voreingestellten Zweck (z.B. Signaturen zu Zahlungsanweisungen bei Großanwendern) und durch eine zuvor geprüfte und abgenommene Anwendung vorgenommen werden können.“ Für den Ordnungsgeber kann danach die Anzeige sogar durch andere Sicherungen, die eine Fehlbedienung ausschließen, ersetzt werden. Ob eine so weite Auslegung, die den Wortlaut vollkommen obsolet macht, zulässig ist, kann dahingestellt bleiben. Jedenfalls erwartet der Ordnungsgeber bei automatisierten elektronischen Signaturen keine Anzeige zu jeder einzelnen Signatur.

Nur nebenbei sei bemerkt, dass die Anforderungen an Signaturanwendungskomponenten nach § 17 Abs. 2 SigG und § 15 Abs. 2 SigV für den Signaturschlüsselinhaber keine Muss-Vorschriften sind und daher auch nicht in die Definition einer qualifizierten elektronischen Signatur in der Weise eingehen, dass ihre Verletzung die Erfüllung der Definition ausschließt. Vielmehr wird ihre Verwendung von § 17 Abs. 2 Satz 3 SigG nur i.S.e. Soll-Vorschrift dringend empfohlen.<sup>41</sup> Alternativ zur Verwendung solcher Komponenten lässt das SigG auch geeignete andere Maßnahmen – etwa die Erzeugung von Signaturen in einer gesicherten Umgebung – zu. Schon aus diesem Grund können Anforderungen an die Signaturanwendungskomponenten einer Einordnung automatisierter elektronischer Signaturen des normalen Signaturschlüsselinhabers als qualifizierte elektronische Signaturen nicht entgegenstehen.

Anders ist jedoch die Situation für akkreditierte Zertifizierungsdiensteanbieter. Diese sind gem. §§ 15 Abs. 7 SigG verpflichtet, geprüfte und bestätigte Signaturanwendungskomponenten einzusetzen. Für sie ist die hier vorgenommene Auslegung der § 17 Abs. 2 SigG und § 15 Abs. 2 SigV entscheidend.

40) S. hierzu *Schreiber*, Elektronisches Verwalten, 2002, S. 168.

41) Diese Regelung trägt dem Umstand Rechnung, dass die Einhaltung dieser Vorschrift nicht überprüfbar ist, weil aus der erstellten Signatur die verwendeten Signaturanwendungskomponenten nicht ersichtlich sind – s. BT-Drs. 14/4662, S. 30; s. auch *Bovenschulte/Eifert*, DuD 2002, 77.

#### 4. Automatisierte elektronische Signatur als qualifizierte elektronische Signatur

Zusammenfassend kann festgehalten werden, dass die automatisierte elektronische Signatur unter bestimmten Voraussetzungen als qualifizierte elektronische Signatur anzuerkennen ist. Der Umstand, dass sie nicht durch persönliches Handeln des Signaturschlüsselnehmers, sondern durch einen von diesem initiierten und kontrollierten automatischen Prozess erzeugt worden ist, schließt diese Anerkennung nicht aus. Allerdings müssen auch für diese Form der Signaturerzeugung die Anforderungen des SigG und der SigV erfüllt werden.

Da das größte Rationalisierungspotenzial in Massenprozessen zu erwarten ist, wird die auch „Massensignatur“ genannte automatisierte elektronische Signatur künftig die Form der weit überwiegenden Zahl elektronischer Signaturen sein. Die Prüfung hat ergeben, dass das SigG diese Mehrzahl von Signaturen nicht grundsätzlich aus seinem Anwendungsbereich ausschließen wollte. Vielmehr gelten die Anforderungen des SigG auch für diese – und damit auch die mit der Anerkennung als fortgeschrittene oder qualifizierte elektronische Signatur verbundenen Rechtsfolgen.

### IV. Folgen der Verwendung automatisierter elektronischer Signaturen

Die Folgen, die mit dem Einsatz der elektronischen Signatur verfolgt werden, ergeben sich aus der jeweiligen Anwendung. Vor diesem Hintergrund ist für den jeweiligen Anwendungsbereich gesondert zu prüfen, ob weitere Zwecke mit der Signatur verbunden werden, die der Zulässigkeit der automatisierten elektronischen Signatur entgegenstehen könnten. Rechtsfolgen der automatisierten elektronischen Signatur können z.B. darin bestehen, dass mit ihrer Hilfe Formvorschriften erfüllt werden können, dass sie besondere Anforderungen für Massenverfahren erfüllen sollen oder dass ihre Vorlage als Beweismittel eine besondere Beweiserleichterung bewirkt.

#### 1. Erfüllung der elektronischen Form

Soweit die elektronische Form den Einsatz einer qualifizierten elektronischen Signatur erfordert, kann diese Anforderung auch durch eine automatisierte elektronische Signatur erfüllt werden. Zusätzlich fordert § 126a BGB allerdings das maschinenschriftliche Unterzeichnen mit dem Namen des Signierenden, während § 3a VwVfG auf dieses – angesichts des Zertifikats überflüssige<sup>42</sup> – Zusatzanforderung verzichtet.<sup>43</sup> Nach dem Entwurf eines Justizkommunikationsgesetzes soll für dessen Geltungsbereich die zusätzliche Unterzeichnung mit dem Namen gefordert werden.<sup>44</sup>

#### 2. Erfüllung der besonderen Anforderungen für potenzielle Massenverfahren

Viele Regelungen für potenzielle Massenverfahren fordern zwar eine qualifizierte elektronische Signatur, nicht aber die Einhaltung der elektronischen Form. Auch in diesem Fall erfüllt die automatisierte elektronische Signatur die Anforderungen dieser Vorschriften, soweit allein die Signatur in Frage steht. Zu beachten ist jedoch, dass die Rechtsordnung für Massenverfahren prädestinierte Prozessabläufe bisher nur als manuelles Prüfverfahren ausgestaltet hat, die ein Tätigwerden einer natürlichen Person in jedem Einzelfall aus anderen Gründen erforderlich macht. So erfordert z.B. die Bestätigung, dass ein Dokument von Papier zu Elektronik (z.B. § 36 SRVwV, § 110a–d SGB IV, § 33 Abs. 4 VwVfG) oder von einem elektronischen For-

mat in ein anderes (z.B. § 33 Abs. 4 VwVfG) korrekt transformiert worden ist, dass der Bestätigende den Vergleich persönlich durch Inaugenscheinnahme vorgenommen hat. In diesen Fällen scheidet die Automatisierung der Vorgänge nicht wegen der Signatur, sondern wegen dieser gesetzlichen Anforderung persönlichen Tätigwerdens aus.

#### 3. Automatisierte elektronische Signatur im Beweisrecht

Für automatisch erzeugte fortgeschrittene elektronische Signaturen ergeben sich in der freien Beweiswürdigung nach § 286 ZPO hinsichtlich Integrität und Authentizität der Signatur keine besonderen Probleme. Beide muss der Beweisführer zur Überzeugung des Gerichts ohne ausreichende Kenntnisse über die Umstände nachweisen.<sup>45</sup> Wird die Zurechnung einer automatisierten elektronischen Signatur zu der automatisch erzeugten Willenserklärung bestritten, muss nur nachgewiesen werden, dass die Signatur aus einem automatischen Prozess stammt, den der Signaturschlüsselhaber bewusst und gewollt in Gang gesetzt hat. Dass das signierte elektronische Dokument einen anderen Inhalt enthält, als der Signaturschlüsselhaber erklären wollte, dürfte in seine Risikosphäre fallen und von ihm zu beweisen sein.<sup>46</sup>

Die automatisierte elektronische Signatur kann bei Vorliegen aller Voraussetzungen eine qualifizierte elektronische Signatur sein. Werden diese Voraussetzungen nicht bestritten oder nachgewiesen,<sup>47</sup> kann die Integrität, Authentizität und Autorisierung der Signatur mit Hilfe der Beweisvermutung des § 292a ZPO nachgewiesen werden. Eine Erschütterung des Anscheins der Echtheit dieser Signatur kann nur durch Tatsachen erfolgen, die ernstliche Zweifel daran begründen, dass die Erklärung mit dem Willen des Signaturschlüsselhabers abgegeben worden ist. Diesen Nachweis kann er z.B. führen, wenn es ihm gelingt zu belegen, dass ihm seine Signaturkarte abhanden gekommen oder abredewidrig für einen (anderen) automatischen Prozess verwendet worden ist.<sup>48</sup> Wenn aber der Prozess der Signaturerzeugung mit seiner Signaturkarte und seinem Willen in Gang gesetzt worden ist, wird es ihm sehr schwer fallen nachzuweisen, dass die signierte Erklärung nicht mit seinem Willen abgegeben worden ist.<sup>49</sup> Insofern trägt er faktisch das Risiko, dass der von ihm initiierte automatische Prozess auch nach seinen Intentionen abläuft. Dieses Risiko kann er verringern, wenn er gem. § 7 Abs. 1 Nr. 7 SigG eine auf den spezifischen Zweck bezogene Beschränkung in sein Zertifikat mit aufnimmt.<sup>50</sup>

#### 4. Reformbedarf?

An gesetzlichen Regelungen, die für Massensignaturen die Verwendung fortgeschrittener oder qualifizierter elektronischer Signaturen zwingend verlangen, wurde vielfach Kritik geübt, weil sie ökonomische Lösungen verhin-

42) S. näher Roßnagel, NJW 2001, 1825; Gesellschaft für Informatik, DuD 2001, 38.

43) S. näher Roßnagel, NJW 2003, 472.

44) S. näher Fischer-Dieskau, MMR 2003, 703; Viefhues, CR 2003, 542 ff.

45) S. hierzu Roßnagel, MMR 2003, 168 f.

46) Grundlegend zur Zurechnung automatischer Willenserklärungen Köhler, AcP 182, 126 ff.

47) S. hierzu ausführlich Fischer-Dieskau/Gitter/Paul/Steidle, MMR 2002, 709; Jungermann, DuD 2003, 69; Borges, Verträge im elektronischen Geschäftsverkehr, 2003, S. 506.

48) S. näher Fischer-Dieskau/Gitter/Paul/Steidle, MMR 2002, 713.

49) S. zur automatisierten Willenserklärung z.B. LG Köln MMR 2003, 81 ff.

50) Beispiel für eine Beschränkung: „Nutzung beschränkt auf Telefonrechnung der Gesellschaft xy“; s. zur Beschränkung von Zertifikaten allgemein Fischer-Dieskau/Gitter/Hornung, MMR 2003, 384.

den.<sup>51</sup> Diese Kritik erscheint unberechtigt. Zum einen können – wie die Untersuchung zeigt – sowohl fortgeschrittene<sup>52</sup> als auch qualifizierte elektronische Signaturen durch automatische Prozesse erzeugt werden, die alle ökonomischen Vorteile automatischer DV-Prozesse nutzen. Zum anderen sind diese Anforderungen aus der Garantienpflicht des Gesetzgebers für einen sicheren elektronischen Rechtsverkehr<sup>53</sup> geboten. Eine einigermaßen verlässliche Sicherheit für den Rechtsverkehr bieten jedoch nur qualifizierte Signaturverfahren.<sup>54</sup> Änderungen an diesen Anforderungen sind also nicht erforderlich.

Notwendig sind jedoch Regelungen, die einerseits eine Automatisierung von Prozessen ermöglichen, andererseits aber spezifische Sicherheits- und Kontrollanforderungen an solche Automatisierungen festlegen. Dies gilt z.B. für Transformationen verschiedener Dokumentenfor-

51) S. z.B. BITKOM, Freiräume schaffen für Wachstum, Innovation und Arbeitsplätze, Ein 10-Punkte-Programm der ITK-Wirtschaft für die neue Legislaturperiode, 1.10.2002, S. 25.

52) Auch für diese sind personalisierte Signaturerstellungseinheiten zu verwenden – s. o. II.1.

53) S. z.B. Roßnagel (o. Fußn. 2), § 1 SigG Rdnr. 16 ff. m.w.Nw.

54) S. hierzu ausführlich Roßnagel, MMR 2002, 215 ff.

55) S. z.B. zu Anforderungen an die automatische Erhebung der notwendigen Verifikationsdaten für zu transformierende elektronische Signaturen Roßnagel/Fischer-Dieskau/Pordes/Brandner, CR 2003, 301.

56) Dies gilt z.B. für die Regelungen zur elektronischen Aktenführung in § 298a ZPO und zur Übertragung in elektronische Dokumente in § 110c OWiG. Dagegen soll der Ausdruck eines elektronischen Dokuments automatisiert erfolgen können – s. Viefhues, CR 2003, 544.

57) S. z.B. Fischer-Dieskau, MMR 2003, 701; Viefhues/Hoffmann, MMR 2003, 71; Viefhues, CR 2003, 545.

58) S. zu dieser rückwärtsgewandten, an der alten Erscheinung der eigenhändigen Unterschrift haftenden Sicht kritisch Roßnagel, Der Regelungsbedarf rechtsverbindlicher Telekooperation, in: Alcatel SEL Stiftung (Hrsg.), Rechtsverbindliche Telekooperation, 1996, S. 7 ff.

59) S. Roßnagel, DuD 1997, 79.

60) S. hierzu z.B. § 9 Abs. 3 und 4 des Entwurfs zum einem SigG von provet, Vorschläge zur Regelung von Datenschutz und Rechtssicherheit in Online-Multimedia-Anwendungen, Gutachten für den BMBF, Darmstadt 1996, www.provet.org/bib/mmge oder www.iid.de/iukdg/doku.html.

mate. Soll ein elektronisches Dokument ausgedruckt, ein Papierdokument eingescannt oder ein elektronisches Dokument in ein anderes elektronisches Format überführt werden, sind bei der künftig anstehenden Fülle von Dokumenten und der beschränkten Erkenntnisfähigkeit visueller Kontrollen individuelle Prüfungen „Blatt für Blatt“ anachronistisch. Vielmehr sind Regelungen erforderlich, die automatische Transformations- und Bestätigungsprozesse ermöglichen, an diese spezifische Sicherheitsanforderungen stellen,<sup>55</sup> Zertifizierungen der Prozesse fordern und die Aussagekraft der Bestätigungen an die tatsächliche Leistungsfähigkeit solcher Prozesse anpassen. Diese Regelungen sollten dann auch funktionale Anforderungen an die Erzeugung automatisierter elektronischer Signaturen enthalten. Diese Forderung sollte bereits in dem geplanten Justizkommunikationsgesetz<sup>56</sup> berücksichtigt werden.<sup>57</sup>

Schließlich wäre zu überlegen, ob das Festhalten an Zertifikaten allein für natürliche Personen für die künftige noch weitere Zunahme automatischer Prozesse vertretbar ist.<sup>58</sup> Das Festhalten an dieser Regelung hemmt den Einsatz fortgeschrittener und qualifizierter Signaturen, weil er zu Konstruktionen zwingt, die so nicht gewollt sein können, wie den Einsatz von Mitarbeiterkarten bei Verwendung von Pseudonymen, dem Abschluss innerbetrieblicher Haftungsübernahmeregelungen und der Weitergabe der PIN zur Aktivierung der Karte für den Fall eines Mitarbeiterwechsels. Zugleich fehlt dem Empfänger der Signatur die transparente Unterscheidung zwischen persönlichen und automatisierten Signaturen. Zumindest beim Verzicht auf aussagekräftige Pseudonyme werden automatisierte Erklärungen erzeugt, von denen der Empfänger annimmt, sie wären unmittelbar von natürlichen Personen abgegeben worden.<sup>59</sup> Dagegen würden Zertifikate für Automaten eine größere Flexibilität für die Verwender elektronischer Signaturen und eine größere Transparenz für die Empfänger elektronisch signierter Dokumente ermöglichen.<sup>60</sup>