Frage nach der Einführung eines einheitlichen „Europäischen Erbscheins". Momentan scheinen dem Verfasser diese Schritte noch als zu gewagt, die Differenzen zwischen den einzelnen nationalen materiellen erbrechtlichen Regelungen als zu groß, um schon eine derartig weitgehende Regelung zu verabschieden.

Wenn es geschafft werden könnte, ein für alle Mitgliedstaaten der EU akzeptables einheitliches Kollisionsrecht und einheitliche Regelungen für die Zuständigkeit in Erbsachen zu schaffen, würde der Verfasser schon viel für erreicht halten, da damit eine ganze Reihe von Schwierigkeiten, die mit transnationalen Erbfällen zur Zeit in der notariellen Praxis verbunden sind, beseitigt werden könnten.

Angesichts des Enthusiasmus, mit dem die anderen EU-Institutionen das Grünbuch der Kommission zum Erb- und Testamentsrecht jedoch begrüßt haben, und der Eile, zu der insbesondere die Mitgliedstaaten und das Europäische Parlament die Kommission zu drängen scheinen, ist demgegenüber wohl zu erwarten, dass die Kommission sich wohl schon sehr bald an einer „großen Lösung" in diesem Bereich versuchen wird. Aus notarieller Sicht wird also insoweit die Entwicklung auch auf europäischer Ebene weiter genau zu verfolgen sein.

Der Einfluss signaturrechtlicher Anforderungen auf die Wirksamkeit der elektronischen notariellen Urkunde

(von Notarassessor Dr. Jens Bormann, LL.M. (Harvard), und Notarassessor Dr. Sebastian Apfelbaum, Berlin)

I. Elektronischer Rechtsverkehr und notarielles Berufs- und Verfahrensrecht

Grundlage für die Erstellung elektronischer notarieller Urkunden sind die §§ 39 a, 42 Abs. 4 BeurkG, 15 Abs. 3 BNotO, die durch das am 1. 4. 2005 in Kraft getretene Justizkommunikationsgesetz[1] eingeführt wurden. Gemäß § 15 Abs. 3 BNotO erstreckt sich der Urkundsgewährungsanspruch bereits seit dem 1. 4. 2006 auch auf Vermerkurkunden nach § 39 a BeurkG. Ein breites Anwendungsfeld hierfür ist durch den elektronischen Handelsregisterverkehr ab dem 1. 1. 2007 eröffnet. Nach § 12 HGB in der Fassung des Gesetzes über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister (EHUG)[2] dürfen Handelsregisteranmeldungen und ihre Anlagen nur noch in elektronischer Form eingereicht werden. Hiermit kommt den Notaren im elektronischen Rechtsverkehr insofern eine Vorreiterrolle zu, als eine Verpflichtung zur Einreichung von elektronischen öffentlichen Urkunden (§§ 371 a Abs. 2 ZPO, 39 a BeurkG) besteht, was unter anderem die Verwendung qualifizierter elektronischer Signaturen nach § 2 Nr. 3 SigG voraussetzt. Dagegen ist in gerichtlichen Verfahren die Einreichung von elektronischen Dokumenten, die eine qualifizierte elektronische Signatur tragen, bislang nur fakultativ vorgesehen (vgl. §§ 130 a ZPO, 46 b ArbGG, 65 a SGG, 52 a FGO, 55 a VwGO).

Die Fertigung von notariellen Urkunden in elektronischer Form stellt das notarielle Berufs- und Verfahrensrecht vor neue Herausforderungen, da die herkömmlichen Vorschriften und ihre Interpretation auf die notarielle Urkunde in Papierform zugeschnitten sind. Für die elektronische öffentliche Urkunde müssen sich ein vergleichbares Regelungsniveau und ein gesicherter Bestand an Rechtsprechung und Literatur erst herausbilden. Ein Beispiel für solche neuartigen Probleme ist die Darstellung der von einem Notarvertreter errichteten elektronischen notariellen Urkunde.[3] Gegenstand dieses Beitrags ist eine andere wichtige Fragestellung, die die Verwendung von qualifizierten elektronischen Signaturen mit sich bringt. Es stellt sich das Problem, welche Auswirkungen Verstöße gegen das Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) auf die Wirksamkeit der notariellen Urkunde haben. Bevor hierauf im Einzelnen näher eingegangen wird (vgl. Abschnitt VI.), erscheint eine nähere Darstellung der Funktion und der Wirkungsweise qualifizierter elektronischer Signaturen (Abschnitt II.), des Normzwecks und des Regelungsgehalts von § 39 a BeurkG (Abschnitt III., IV.) sowie der Regelungen zur Beschaffenheit von papiergebundenen notariellen Urkunden (Abschnitt V.) sinnvoll.

II. Funktion und Wirkungsweise qualifizierter elektronischer Signaturen

Die Technik der qualifizierten elektronischen Signatur begegnet zwei Grundproblemen, die sich im elektronischen Rechtsverkehr stellen.

1. Nachweis von Veränderungen des zu signierenden Dokuments

Ein Grundproblem elektronischer Dokumente besteht darin, dass ihr Inhalt von unbefugten Dritten grundsätzlich ohne Hinterlassung jeglicher Spuren verändert werden kann.[4] Dieses Risiko ist besonders ausgeprägt, wenn sie ohne weiteren Schutz über offene Netzwerke wie das Internet versendet werden. Für einen Empfänger ist die inhaltliche Unverändertheit im Vergleich zum abgesendeten Ausgangsdokument regelmäßig nicht feststellbar.

---

1 BGBl I 2005, 837.

2 BGBl I 2006, 2553.

3 Vgl. hierzu das Rundschreiben 25/2006 der Bundesnotarkammer sowie BNotK-Intern 6/2006, 5 f. Beide Quellen sind unter www.bnotk.de abrufbar.

4 Bettendorf, RNotZ 2005, 277, 278; ders., in: Erber-Faller (Hrsg.), Elektronischer Rechtsverkehr, 2000, Kap. I.B.2.; ders., in: Berichte der deutschen Delegation, XX. Internationaler Kongress des Lateinischen Notariats, Cartagena/Kolumbien, 1992, 29, 47; Gassen, Digitale Signaturen in der Praxis – Grundlagen, Sicherheitsfragen und normativer Rahmen, 2003, 1. Teil I.

Hier schafft die qualifizierte elektronische Signatur Abhilfe, indem sie über ein verlässliches mathematisches Verfahren jede spurlose Veränderung sichtbar macht. Zu diesem Zweck wird aus den elektronischen Daten, also dem Urkundstext, ein unverwechselbarer „Datenfingerabdruck“ (sog. *Hash-Wert*) generiert, der verschlüsselt wird.[5] Das mathematische Ergebnis dieses Verschlüsselungsverfahrens ist die qualifizierte elektronische Signatur. Das derart verschlüsselte Komprimat wird an die „im Klartext“ vorliegende Originalnachricht angehängt. Sowohl das verschlüsselte Komprimat als auch die Originalnachricht werden verschickt.[6]

Bei der Verschlüsselung bedient man sich des sog. asymmetrischen Verschlüsselungsverfahrens.[7] Bei den herkömmlichen, sog. symmetrischen Verschlüsselungsverfahren[8] wird zur Ver- und Entschlüsselung einer Nachricht derselbe Schlüssel verwendet. Die Schwäche dieses Verfahrens liegt in Folgendem: Da beide Kommunikationspartner den gleichen geheimen Schlüssel verwenden und kennen, kann nicht nachgewiesen werden, wer von beiden die Nachricht erzeugt hat. Diese Schwierigkeit wird im asymmetrischen Verschlüsselungsverfahren umgangen, indem mit zwei verschiedenen Schlüsseln gearbeitet wird. Die Verschlüsselung des *Hash-Wertes* des Ausgangsdokuments erfolgt mit einem sog. „privaten“ oder „geheimen“ Schlüssel (*private key*), der nur dem Schlüsselinhaber selbst bekannt ist, also keinesfalls für Dritte zugänglich sein darf.[9] Der private Schlüssel wird nicht auslesbar auf einer nur mit einer Geheimzahl (PIN) frei zu schaltenden Signaturkarte[10] gespeichert. Diese Signaturkarte wird von einer Zertifizierungsstelle, dem Zertifizierungsdiensteanbieter, herausgegeben.[11]

Der Empfänger einer derartig signierten Nachricht (z. B. beim elektronischen Handelsregisterverkehr das Registergericht) entschlüsselt die Signatur mittels eines zweiten sog. „öffentlichen“ Schlüssels (*public key*), der im öffentlich zugänglichen Zertifikatsverzeichnis des Zertifizierungsdiensteanbieters – ähnlich wie in ein Telefonbuch – eingestellt wird.[12] Dieser Schlüssel korrespondiert mathematisch mit dem vom Signierenden benutzten privaten Schlüssel. Durch die bei Erstellung des Schlüsselpaares verwendete mathematische Funktion wird gewährleistet, dass man den privaten Schlüssel auch dann nicht berechnen kann, wenn man im Besitz des öffentlichen Schlüssels ist.[13]

Das bei der Entschlüsselung durch den Empfänger eingesetzte Softwareprogramm bildet aus dem mit gesendeten Originaltext (Klartext) einen zweiten *Hash-Wert* und vergleicht diesen mit dem in der elektronischen Signatur enthaltenen, ursprünglichen *Hash-Wert*, der mit Hilfe des öffentlichen Schlüssels entschlüsselt worden ist. Dieser Vergleich der *Hash-Werte* lässt einen eindeutigen Rückschluss darauf zu, ob die Nachricht inhaltlich unverändert übermittelt worden ist oder ob nach dem Signieren durch den Verwender Änderungen (absichtlich oder durch Übertragungsfehler) vorgenommen worden sind.[14] Die Feststellung einer Veränderung des Dokuments ist damit sichergestellt.

Das beschriebene Verfahren der qualifizierten elektronischen Signatur basiert demnach auf dem „*Prinzip von Besitz und Wissen*“.[15] Nur der Besitz der Signaturkarte und zusätzlich das Wissen um die PIN ermöglichen eine Verwendung des privaten Schlüssels und die Erzeugung einer qualifizierten elektronischen Signatur. Da diese das elektronische Äquivalent zur eigenhändigen Unterschrift des Notars darstellt (vgl. §§ 126 Abs. 3, 126 a BGB und § 6 Abs. 2 SigG), ist sie ihm höchstpersönlich zugeordnet. Die zur Erzeugung der qualifizierten elektronischen Signatur erforderliche Signaturkarte darf nicht Mitarbeitern oder Dritten zur Verwendung überlassen werden und ist zudem vor Missbrauch zu schützen. Eine entsprechende Ergänzung der Richtlinienempfehlungen der Bundesnotarkammer in Abschnitt IV. um eine neue Ziffer 2. hat die 92. Vertreterversammlung der Bundesnotarkammer am 28. 4. 2006 in Berlin beschlossen.[16]

Um sicherzustellen, dass der geheime private Schlüssel aufgrund technischer Fortschritte bei der Erhöhung von Rechnerleistungen trotz Kenntnis des öffentlichen Schlüssels nicht errechnet werden kann, wird das Zertifikat nach vom Bundesamt für Sicherheit und Informationstechnik (BSI) festgelegten Zeiträumen automatisch gesperrt. Daher ist der regelmäßige Erwerb neuer, technisch verbesserter Signaturkarten in den vom BSI festgelegten Abständen erforderlich.

2. Zuordnung der Nachricht zu einer bestimmten Person

Ein zweites Grundproblem des elektronischen Rechtsverkehrs stellt die rechtssichere Zuordnung einer Nachricht zu einem bestimmten Absender dar.[17] Denn bei einer elektronischen Kommunikation ist es beispielsweise ohne Probleme möglich, eine E-Mail-Nachricht unter

5 Bettendorf, RNotZ 2005, 277, 279 f.; Gassen, Digitale Signaturen in der Praxis – Grundlagen, Sicherheitsfragen und normativer Rahmen, 2003, 1. Teil III. 4.; Rapp, Rechtliche Rahmenbedingungen und Formqualität elektronischer Signaturen, 2002, 1. Kap. A. II. 3. a) bb).

6 Instruktiv hierzu Gassen, Digitale Signaturen in der Praxis – Grundlagen, Sicherheitsfragen und normativer Rahmen, 2003, 1. Teil III. 2. b).

7 Bettendorf, RNotZ 2005, 277, 279 f.; Fischer-Dieskau, Das elektronisch signierte Dokument als Mittel zur Beweissicherung, 2006, 1. Teil 2.2.1.1; Gassen, Digitale Signaturen in der Praxis – Grundlagen, Sicherheitsfragen und normativer Rahmen, 2003, 1. Teil III. 3.; Rapp, Rechtliche Rahmenbedingungen und Formqualität elektronischer Signaturen, 2002, 1. Kap. A. II.

8 Rapp, Rechtliche Rahmenbedingungen und Formqualität elektronischer Signaturen, 2002, 1. Kap. A. I.

9 Bettendorf, RNotZ 2005, 277, 279 f.; Gassen, Digitale Signaturen in der Praxis – Grundlagen, Sicherheitsfragen und normativer Rahmen, 2003, 1. Teil III. 2., 3.; Rapp, Rechtliche Rahmenbedingungen und Formqualität elektronischer Signaturen, 2002, 1. Kap. A. II.

10 In der Terminologie des Signaturgesetzes handelt es sich um eine sog. „sichere Signaturerstellungseinheit“ nach § 2 Nr. 10 SigG.

11 Gassen, Digitale Signaturen in der Praxis – Grundlagen, Sicherheitsfragen und normativer Rahmen, 2003, 1. Teil III. 5. b); Rapp, Rechtliche Rahmenbedingungen und Formqualität elektronischer Signaturen, 2002, 1. Kap. A. II. 3. c); Reisen/Mrugalla, in: Erber-Faller (Hrsg.), Elektronischer Rechtsverkehr, 2000, Kap. II. A.

12 Gassen, Digitale Signaturen in der Praxis – Grundlagen, Sicherheitsfragen und normativer Rahmen, 2003, 1. Teil III. 5. c).

13 Fischer-Dieskau, Das elektronisch signierte Dokument als Mittel zur Beweissicherung, 2006, 1. Teil 2.2.1.2.1.

14 Bettendorf, RNotZ 2005, 277, 280.

15 Bettendorf, RNotZ 2005, 277, 281; Bieser, in: Erber-Faller (Hrsg.), Elektronischer Rechtsverkehr, 2000, Kap. III. A. 3. b).

16 DNotZ 2006, 561. Ausführlich zum Verbot der Weitergabe von Signaturkarte und PIN auch Bettendorf, in: Beck'sches Notar-Handbuch, 4. Aufl. 2006, Kap. M Rn. 154.

17 Bettendorf, RNotZ 2005, 277, 278; ders., in: Erber-Faller (Hrsg.), Elektronischer Rechtsverkehr, 2000, Kap. I.B.3.; ders., in: Berichte der deutschen Delegation, XX. Internationaler Kongress des Lateinischen Notariats, Cartagena/Kolumbien, 1992, 29, 49 ff.

einem fremden Namen zu versenden, ohne dass für den Empfänger die fehlende Authentizität erkennbar ist. Deshalb sieht das Institut der qualifizierten elektronischen Signatur vor, dass eine Signaturkarte nur nach einer zuverlässigen Identifikation des Antragstellers ausgegeben werden darf (§ 5 Abs. 1 SigG). Diese Zuordnung eines Schlüsselpaares zu einer bestimmten Person macht die Einschaltung einer vertrauenswürdigen Drittinstanz erforderlich, die die Identitätsüberprüfung und Identitätsverknüpfung übernimmt und garantiert. Dieser vertrauenswürdige Dritte ist die Zertifizierungsstelle (Trust Center).[18] In dem bereits erwähnten, von der Zertifizierungsstelle herausgegebenen öffentlichen Zertifikatsverzeichnis erscheint – vergleichbar zum Telefonbuch – auch der Name des Zertifikatsinhabers. Im Rahmen der Prüfung der Signatur durch den Empfänger einer signierten Nachricht wird dieser automatisch abgefragt.

3. Zuordnung der Nachricht zu einem Notar

Bei elektronischen notariellen Urkunden stellt sich zudem die Aufgabe, dass gemäß § 39 a Satz 4 BeurkG mit der elektronischen Vermerkurkunde zugleich eine Bestätigung der Notareigenschaft verbunden werden muss. Technisch wird die Anforderung gelöst, indem die Signatur des Notars eine zusätzliche Information, das sog. Notarattribut enthält, das Bestandteil der Signaturdatei ist. Dieses regelmäßig ebenfalls auf der Signaturkarte gespeicherte Notarattribut darf die Zertifizierungsstelle gemäß § 5 Abs. 2 Satz 2 SigG erst nach einer Bestätigung der Notareigenschaft durch die zuständige Stelle in das Signaturzertifikat aufnehmen.

Nach dem gegenwärtig von der Zertifizierungsstelle der Bundesnotarkammer praktizierten Verfahren wird das Notarattribut nach einer Bestätigung der Notareigenschaft durch die regionale Notarkammer aufgenommen. Zwar werden Notare gemäß § 12 BNotO förmlich von der Landesjustizverwaltung bestellt. Nach § 12 BNotO geschieht dies jedoch erst nach Anhörung der zuständigen regionalen Kammer, so dass diese in den Bestellungsprozess eng eingebunden wird. Zudem sind nach § 65 Abs. 1 Satz 1 BNotO die Notare kraft Gesetzes Mitglied der regionalen Kammern. Diese sind regelmäßig über den Status des einzelnen Notars in ihrem Kammerbezirk informiert und somit nach Normzweck und Funktion des § 5 Abs. 2 Satz 2 SigG geeignet, die Bestätigung zu erteilen. Eine Zuständigkeit der Berufskammern bei der Bestätigung der Notareigenschaft nach § 5 Abs. 2 Satz 2 SigG entspricht zudem der Vorstellung des Gesetzgebers.[19] Diese Kompetenz der regionalen Notarkammern zu einer Bestätigung der Notareigenschaft hat der Gesetzgeber in § 67 Abs. 5 BNotO nunmehr auch ausdrücklich anerkannt.[20]

4. Rolle der Zertifizierungsstelle

Insgesamt kommt damit im Verfahren der qualifizierten elektronischen Signatur der Zertifizierungsstelle eine zentrale Funktion zu. Im Wesentlichen hat sie zwei Aufgaben zu erfüllen. Zum einen werden die benötigten Schlüssel von ihr generiert und auf einem sicheren Datenträger gespeichert. Dabei handelt es sich um eine technisch komplexe Aufgabe, da die Fälschungssicherheit der Schlüssel gewährleistet werden muss. Zum anderen bestätigt sie die Zuordnung eines Schlüssels zu einer bestimmten natürlichen Person.

Angesichts der herausragenden Bedeutung qualifizierter elektronischer Signaturen für den Rechtsverkehr hätte es in der Tradition der Daseinsvorsorge[21] eigentlich nahe gelegen, ihre Erteilung in die Hand einer staatlichen Behörde zu legen, um maximale Zuverlässigkeit zu gewährleisten. Der Gesetzgeber hat sich jedoch – nicht zuletzt aufgrund der gemeinschaftsrechtlichen Vorgaben durch die Signaturrichtlinie[22] – für ein Modell der Erbringung öffentlicher Leistungen durch Private unter der Aufsicht einer unabhängigen Regulierungsbehörde entschieden, wie es sich im anglo-amerikanischen Raum seit Ende des 19. Jahrhunderts entwickelt hat und derzeit auch in Europa im Vordringen befindet.[23] Ein Großteil möglicher Mängel elektronischer Signaturen hat seine Gründe denn auch in der komplizierten Regelung des Zertifizierungsverfahrens.[24]

III. Normzweck und Regelungsgehalt von § 39 a BeurkG

Ausgangspunkt für die Prüfung der Auswirkungen von Verstößen gegen das Signaturgesetz auf die Wirksamkeit der elektronischen notariellen Urkunde ist § 39 a BeurkG. Die Vorschrift erfüllt verschiedene Funktionen. Zunächst ermöglicht sie überhaupt erst die Erstellung elektronischer notarieller Vermerkurkunden. Solche wären ohne § 39 a BeurkG nicht denkbar. Des Weiteren macht sie Vorgaben zum Inhalt des elektronischen Vermerks und zum anwendbaren technischen Verfahren, indem sie auf das Signaturgesetz Bezug nimmt und in den Sätzen 2 und 4 das Vorliegen einer qualifizierten elektronischen Signatur und eine Bestätigung der Notareigenschaft als Muss-Voraussetzungen benennt. Schließlich stellt § 39 a BeurkG klar, dass sämtliche in § 39 BeurkG genannten einfachen Zeugnisse auch Gegenstand einer elektronischen Vermerkurkunde sein können.[25] Beide Vorschriften sind somit hinsichtlich der Frage des möglichen Inhaltes des Urkundsvermerks deckungsgleich. Unterschiede bestehen zwischen beiden Rege-

18 Bettendorf, RNotZ 2005, 277, 280 f.; Gassen, Digitale Signaturen in der Praxis – Grundlagen, Sicherheitsfragen und normativer Rahmen, 2003, 1. Teil III. 5.

19 BT-Drs. 14/4662, 21.

20 BGBl I 2006, 3416, 3417.

21 Grundlegend zur Daseinsvorsorge Forsthoff, Die Verwaltung als Leistungsträger, 1938; siehe ferner Huber, in: FS Ernst Forsthoff, 1974, 139 ff.

22 Aufgrund der Entstaatlichungsvorgaben des sekundären Gemeinschaftsrechts ist sogar ein öffentliches Zulassungsverfahren für Zertifizierungsstellen mit präventiver Qualitätskontrolle verboten (vgl. Art. 3 Abs. 1 Richtlinie 99/93/EG vom 13. 12. 1999, ABl. [2000] Nr. L 13, 12).

23 Bullinger, DVBl. 2003, 1355 ff.; Masing, AöR 128 (2003), 558 ff.; zur historischen Entwicklung in den USA Lepsius, Verwaltungsrecht unter dem Common Law, 1997, 68 ff. Zum Übergang vom „Leistungsstaat" zum „Gewährleistungsstaat" Voßkuhle, VVDStRL 62 (2002), 266, 275–326 m. w. N.; kritisch Broß, JZ 2003, 874 ff.

24 Näher unten Abschnitt VI.

25 BT-Drs. 15/4067, 54; Meyer-Wehage, in: Scherf/Schmieszek/Viefhues, Elektronischer Rechtsverkehr – Kommentar und Handbuch, 2006, Teil C.VI. Rn. 10 f.

lungen nur hinsichtlich der Verkörperungsform des Vermerks (papiergebunden bzw. elektronisch).

Größere praktische Relevanz wird die elektronische Vermerkurkunde zunächst nur im elektronischen Handelsregisterverfahren erlangen.[26] Hier geht es um die Fertigung elektronischer beglaubigter Abschriften von Papierurkunden: Fordert das Gesetz wie in § 12 Abs. 1 HGB eine *Unterschrifts*beglaubigung und sollen elektronische Dokumente eingereicht werden, so ist auf der Grundlage der gegenwärtigen Fassung des § 129 BGB[27] wie folgt zu verfahren: Die in Papierform vorliegende Handelsregisteranmeldung ist vom Antragsteller eigenhändig zu unterzeichnen. Der Notar hat über die Leistung bzw. Anerkennung der Unterschrift sodann – wie bisher – einen Beglaubigungsvermerk in Papierform zu errichten. Als zusätzlicher Arbeitsschritt ist danach die unterzeichnete Handelsregisteranmeldung einschließlich des Beglaubigungsvermerks über die Leistung bzw. das Anerkenntnis der Unterschrift einzuscannen. Schließlich hat der Notar die Übereinstimmung der Scan-Datei mit der Papierurkunde im Wege einer *Abschrifts*beglaubigung nach § 39 a BeurkG zu bestätigen. Durch eine Kombination von *Unterschrifts*beglaubigung in Papierform und *Abschrifts*beglaubigung in elektronischer Form wird die Einreichung elektronischer öffentlicher Dokumente beim Handelsregister ermöglicht, die den Formanforderungen des § 12 HGB entsprechen.[28]

IV. Muss- und Soll-Anforderungen in § 39 a BeurkG

1. Qualifizierte elektronische Signatur und Notarattribut als Ersatz von Notarunterschrift und Amtssiegel

Der Wortlaut von § 39 a BeurkG unterscheidet zwischen Muss- und Soll-Anforderungen. Nach den allgemeinen Grundsätzen des Beurkundungsverfahrensrechts führen nur Verstöße gegen Muss-Vorschriften zur Unwirksamkeit der Urkunde, während die Nichtbeachtung von Soll-Vorschriften ihre Wirksamkeit unberührt lässt.[29] Soll-Vorschriften begründen grundsätzlich lediglich Amtspflichten des Notars, deren Verletzung dienstrechtliche Konsequenzen nach sich ziehen kann. Diese Grundsätze und die geringe Anzahl an Muss-Vorschriften dienen der Rechtssicherheit. Gemeinsames Merkmal eines Verstoßes gegen eine Muss-Vorschrift des BeurkG ist, dass dieser aus der Urkunde leicht erkennbar ist.[30] Es soll auf den ersten Blick klar sein, ob eine notarielle Urkunde formell wirksam ist.

Demnach führt das gänzliche Fehlen einer qualifizierten elektronischen Signatur (§ 39 a Satz 2 BeurkG) oder eines Nachweises der Notareigenschaft (§ 39 a Satz 4 BeurkG) zu einer Unwirksamkeit der elektronischen Urkunde. Hingegen ist es für die Wirksamkeit der Urkunde unschädlich, wenn die Signatur nicht auf einem Zertifikat beruht, das auf Dauer prüfbar ist (§ 39 a Satz 3 BeurkG), oder wenn das Zeugnis nicht Ort und Tag der Ausstellung angibt (§ 39 a Satz 4 BeurkG).

Dies entspricht der Systematik des § 39 BeurkG für die papiergebundene Urkunde. Unabdingbare Voraussetzungen für die Wirksamkeit eines einfachen notariellen Zeugnisses sind danach sowohl die Unterschrift des Notars als auch sein Siegel. Die qualifizierte elektronische Signatur ist Äquivalent der eigenhändigen Unterschrift des Notars, wie sich aus § 126 Abs. 3 BGB i. V. m. § 126 a BGB und § 6 Abs. 2 SigG ergibt.[31] Der Nachweis der Notareigenschaft wird gewöhnlich über das im Zertifizierungsverfahren nach § 5 Abs. 2 Satz 2 SigG erteilte Notarattribut geführt.[32] Das Notarattribut erfüllt vergleichbare Funktionen wie das Amtssiegel bei der papiergebundenen Urkunde. Erst hierdurch wird aus dem elektronischen Dokument eine elektronische öffentliche Urkunde. Wie das Siegel dient das Notarattribut als Nachweis, dass die Urkunde von einem Notar in Ausübung seiner Hoheitsgewalt errichtet worden ist. Vollständig vergleichbar zum Amtssiegel ist es dennoch nicht. Denn das visuell wahrnehmbare Amtssiegel ist ein klar erkennbares äußeres Zeichen der staatlichen Beleihung und der hoheitlichen Amtsausübung durch den Notar.[33] Das Notarattribut ist als Konsequenz des elektronischen Rechtsverkehrs hingegen rein virtuell und weist signaturrechtlich keine besondere hervorgehobene Stellung im Vergleich zu anderen Berufsattributen auf.

2. § 39 a Satz 3 BeurkG

Nach § 39 a Satz 3 BeurkG ist für die Wirksamkeit der elektronischen Vermerkurkunde die Dauer der Nachprüfbarkeit des Zertifikats durch Vorhalten des öffentlichen Schlüssels (*public key*) beim Zertifizierungsdiensteanbieter unbeachtlich. Denn es handelt sich lediglich um eine Soll-Vorschrift. Welche genauen Anforderungen an das Tatbestandsmerkmal „auf Dauer prüfbar" zu stellen sind, um einen Verstoß gegen diese Soll-Vorschrift zu vermeiden, ist noch nicht in allen Ein-

26 Vgl. zu weiteren möglichen Anwendungsfällen Malzer, DNotZ 2006, 9, 13 ff.

27 Der Wortlaut des § 129 BGB fordert eine „Unterschrift". Anders als für die Schriftform (§§ 126, 126 a BGB) ist eine Gleichstellung der qualifizierten elektronischen Signatur in § 129 BGB gerade nicht erfolgt. Ebenso Malzer, DNotZ 2006, 9, 22 f.

28 Diese elektronischen beglaubigten Abschriften müssen nach § 8 Abs. 1 DONot nicht in die Urkundenrolle eingetragen werden. Hier kann für elektronische Urkunden nichts anderes gelten als für Papierurkunden, da nach der Regelungssystematik des § 8 Abs. 1 DONot allein der Inhalt der Vermerkurkunde über die Eintragungsbedürftigkeit in der Urkundenrolle entscheidet, nicht jedoch das Medium der Urkunde (Bettendorf, in: Beck'sches Notar-Handbuch, 4. Aufl. 2006, Kap. M Rn. 16). Anders, jedoch unter Verkennung der Regelungssystematik des § 8 Abs. 1 DONot Weingärtner/Ehrlich, DONot, 10. Aufl. 2006, Rn. 148, die einen „Vermerk über die Erstellung des elektronischen Beglaubigungsvermerks" für eintragungspflichtig halten.

29 BT-Drs. 5/3282, 24; BayObLGZ 1983, 101, 106; Armbrüster/Renner, in: Huhn/von Schuckmann, BeurkG, 4. Aufl. 2004, Einl. Rn. 40 f.; Eylmann, in: Eylmann/Vaasen, BeurkG, 2. Aufl. 2004, Einl. Rn. 6; Kanzleiter, DNotZ 1993, 434, 436 f.; Winkler, BeurkG, 15. Aufl. 2003, Einl. Rn. 13.

30 Mecke, DNotZ 1968, 584, 601; Winkler, BeurkG, 15. Aufl. 2003, Einl. Rn. 11.

31 Vgl. bereits Abschnitt II.1.

32 Vgl. Abschnitt II.3. Der Nachweis der Notareigenschaft über ein Attribut nach § 7 Abs. 1 Nr. 9 SigG, welches Bestandteil des qualifizierten Zertifikats ist, oder über ein gesondertes Attributs-Zertifikat nach § 7 Abs. 2 SigG ist nicht zwingend. So wird er bei der elektronischen notariellen Urkunde des Notarvertreters gewöhnlich über eine elektronische beglaubigte Abschrift der Vertreterbestellungsurkunde geführt (Rundschreiben 25/2006 der Bundesnotarkammer; BNotK-Intern 6/2006, 5 f.).

33 Blaeschke, in: Eylmann/Vaasen, DONot, 2. Aufl. 2004, § 2 Rn. 6; Weingärtner/Ehrlich, DONot, 10. Aufl. 2006, Rn. 27.

zelheiten geklärt.[34] Der Gesetzgeber legt dem Begriff ein funktionales Verständnis zu Grunde.[35] Die Dauer der Prüfbarkeit des Zertifikats hängt damit von der möglichen Verwendbarkeit des öffentlichen elektronischen Dokuments ab. Generell sollte aber bei der Auswahl des Zertifizierungsdiensteanbieters darauf geachtet werden, dass es sich um einen akkreditierten Anbieter handelt. Denn dieser gewährleistet ein Vorhalten des öffentlichen Schlüssels erheblich länger als die grundsätzlich erforderlichen 5 Jahre (§ 4 Abs. 1 SigV). Gemäß § 4 Abs. 2 SigG muss ein akkreditierter Zertifizierungsdiensteanbieter die Überprüfbarkeit des Zertifikats über einen Zeitraum von 30 Jahren ab Beendigung der Gültigkeit eines Zertifikats sicherstellen. Derartige Akkreditierungen werden von der Bundesnetzagentur als Aufsichtsbehörde erteilt. Nach § 16 Abs. 2 SigG besteht eine Verpflichtung der Bundesnetzagentur, Namen, Anschriften und Kommunikationsverbindungen von akkreditierten Zertifizierungsdiensteanbietern und den Widerruf oder die Rücknahme einer Akkreditierung jederzeit für jeden über öffentlich zugängliche Kommunikationsverbindungen nachprüfbar und abrufbar zu halten. Dies geschieht auf den Internetseiten der Bundesnetzagentur.[36] Die Bundesnotarkammer ist eine derartige Zertifizierungsstelle mit Anbieter-Akkreditierung.

V. Regelungen zur Beschaffenheit von papiergebundenen notariellen Urkunden

Neben den Fällen eines gänzlichen Fehlens der qualifizierten elektronischen Signatur und eines Nachweises der Notareigenschaft[37] sind zahlreiche andere Fehler bei der Erzeugung einer qualifizierten elektronischen Signatur durch den Notar oder bei der Erteilung des qualifizierten elektronischen Zertifikats durch den Zertifizierungsdiensteanbieter denkbar. Bevor diese denkbaren Mängel der elektronischen Urkunde im Einzelnen behandelt werden (Abschnitt VI.), ist zunächst ein Vergleich zur Rechtslage bei papiergebundenen notariellen Urkunden zu ziehen. Denn eine äquivalente Behandlung von elektronischen Vermerkurkunden ist häufig sachgerecht, da diese lediglich ein anderes Medium notariellen Handelns darstellen. Aufgrund der parallelen Struktur der Vorschriften des § 39 BeurkG und des § 39 a BeurkG ist es eine Regelungsvorgabe des Gesetzgebers, die elektronische notarielle Urkunde nach dem Vorbild der papiergebundenen Urkunde auszugestalten. Auf der anderen Seite muss aber stets geprüft werden, ob sich aus dem Einsatz von Elektronik und damit aus dem anders gearteten Medium Besonderheiten und die Notwendigkeit einer anderen Behandlung ergeben.

1. Einschlägige Vorschriften

Bei herkömmlichen papiergebundenen notariellen Urkunden sind die Anforderungen an die körperliche Ausgestaltung in §§ 44 BeurkG, 28 ff. DONot geregelt. In § 29 DONot sind insbesondere die Qualität, die Farbe und das Format des Papiers sowie die Beschaffenheit des Schreibmittels (Tinte, Farbbänder, Kugelschreiber, Drucker oder Kopiergeräte) normiert. § 31 Satz 2, 3 DONot legen die näheren Anforderungen an das Siegel (Farbdrucksiegel, Prägesiegel in Lack oder unter Verwendung einer Mehloblate) fest. §§ 44 BeurkG, 30, 31 Satz 1 DONot regeln die Verbindung des Siegels mit dem Papier.

2. Folge bei Verstößen

Es besteht Einigkeit darüber, dass Verstöße gegen die §§ 44 BeurkG, 29, 30 f. DONot die Wirksamkeit der Urkunde nicht beeinträchtigen.[38] § 44 BeurkG ist eine Soll-Vorschrift, deren Verletzung die Wirksamkeit der Urkunde unberührt lässt und allenfalls deren Beweiswert beeinträchtigt.[39] Verstöße gegen die Vorschriften der DONot als Festlegung interner Amtspflichten des Notars beeinträchtigen die Wirksamkeit der Urkunde ebenfalls von vornherein nicht, weil sie für den Rechtsverkehr im Regelfall nicht erkennbar sind.[40] Dies gilt sogar unabhängig davon, ob es sich um eine Muss- oder Soll-Vorschrift der DONot handelt. Hier ist der in Abschnitt IV. 1. dargestellte Grundsatz maßgeblich, wonach nur der Verstoß gegen eine Muss-Vorschrift des Beurkundungsgesetzes die Unwirksamkeit der Urkunde nach sich zieht.

VI. Regelungsäquivalent bei einfachen elektronischen Zeugnissen

1. Keine eigenständige Regelung im notariellen Verfahrensrecht

Im notariellen Verfahrensrecht gibt es kein Gegenstück zu den §§ 44 BeurkG, 29, 30 f. DONot für die Erstellung elektronischer Urkunden. Die Anforderungen an eine qualifizierte elektronische Signatur sind vielmehr nur allgemein in § 2 Nr. 3 i. V. m. § 2 Nr. 2 SigG definiert. Diese Bestimmung gilt unabhängig davon, ob das qualifizierte elektronische Zertifikat durch Privatpersonen verwendet wird oder ob mit ihm eine notarielle Urkunde erzeugt werden soll. § 39 a Satz 2 BeurkG schafft jedoch eine Verbindung zwischen dem Signaturgesetz und dem Beurkundungsverfahren, indem die qualifizierte elektronische Signatur als Äquivalent der eigenhändigen Unterschrift des Notars definiert wird. Aufgrund dieser Verknüpfung stellt sich die Frage, ob die Einhaltung sämtlicher Anforderungen des Signaturgesetzes zur Wirksamkeitsvoraussetzung für die notarielle Urkunde gemacht wird.

---

34 Gassen/Wegerhoff, Elektronischer Rechtsverkehr mit „SigNotar“ und „StrADa“, ZNotP 2005, 414, 416; Malzer, DNotZ 2006, 9, 25.

35 BT-Drs. 15/4067, 25.

36 www.bundesnetzagentur.de/enid/2.html.

37 Vgl. Abschnitt IV.1.

38 BGHZ 136, 357, 366; Limmer, in: Eylmann/Vaasen, BeurkG, 2. Aufl. 2004, § 44 Rn. 1; von Schuckmann/Preuß, in: Huhn/von Schuckmann, BeurkG, 4. Aufl. 2004, § 44 Rn. 6; Weingärtner/Ehrlich, DONot, 10. Aufl. 2006, Rn. 462; Winkler, BeurkG, 15. Aufl. 2003, § 44 Rn. 11.

39 OLG Schleswig, DNotZ 1972, 556; Limmer, in: Eylmann/Vaasen, BeurkG, 2. Aufl. 2004, § 44 Rn. 1; von Schuckmann/Preuß, in: Huhn/von Schuckmann, BeurkG, 4. Aufl. 2004, § 44 Rn. 6; Weingärtner/Ehrlich, DONot, 10. Aufl. 2006, Rn. 462; Winkler, BeurkG, 15. Aufl. 2003, § 44 Rn. 11.

40 Blaeschke, in: Eylmann/Vaasen, DONot, 2. Aufl. 2004, § 29 Rn. 2; Weingärtner/Ehrlich, DONot, 10. Aufl. 2006, Rn. 7, 454, 462.

2. Mögliche Verstöße gegen das Signaturgesetz

Es sind vielfältige Verstöße gegen das Signaturgesetz denkbar. Zunächst sind Mängel auf Seiten des Zertifizierungsdiensteanbieters vorstellbar. Dieser kann u. U. nicht über die notwendigen persönlichen, sachlichen und technischen Voraussetzungen nach § 4 Abs. 2 SigG für den Betrieb einer Zertifizierungsstelle verfügen. Ihm können Fehler bei der Erteilung eines qualifizierten Zertifikats unterlaufen, weil er beispielsweise ein Zertifikat ohne zuverlässigen Identifizierungsnachweis nach § 5 Abs. 1 SigG ausgibt. Ebenso sind auf Seiten des Anwenders zahlreiche Fehler denkbar. Beispielsweise kann er die Signaturkarte und Geheimzahl (PIN) zur Erzeugung der Signatur an einen Dritten weitergeben oder nicht signaturgesetzkonforme Software oder Kartenlesegeräte zur Erzeugung der Signatur („Signaturanwendungskomponenten" nach § 2 Nr. 11 SigG) verwenden.

Die formelle Wirksamkeit einer notariellen Urkunde kann nicht von all diesen signaturrechtlichen Unwägbarkeiten und Anforderungen abhängig sein. Die Gründe für dieses aus praktischer Sicht gebotene Ergebnis liegen teilweise im Signaturrecht selbst (3.), teilweise aber auch im Beurkundungsrecht (4.).

3. Qualifizierte elektronische Signatur und Signaturgesetz

a) Allgemeines

Bereits aus signaturrechtlicher Sicht führt nicht jeder Verstoß gegen eine Anforderung des Signaturgesetzes zum Fehlen einer qualifizierten elektronischen Signatur. Besitzt etwa der Zertifizierungsdiensteanbieter nicht die erforderliche Zuverlässigkeit und Fachkunde nach § 4 Abs. 2 SigG, kann die Bundesnetzagentur als Aufsichtsbehörde den Betrieb untersagen (§ 19 Abs. 3 SigG). Gemäß § 19 Abs. 5 SigG bleibt hiervon jedoch die Wirksamkeit von ausgestellten Zertifikaten unberührt. Sind qualifizierte Zertifikate nicht hinreichend fälschungssicher, kann eine Sperrung angeordnet werden (§ 19 Abs. 4 SigG). Eine Unwirksamkeitssanktion enthält die Vorschrift hingegen nicht.

Auf der anderen Seite muss gemäß § 7 SigG ein qualifiziertes Zertifikat bestimmte Mindestangaben enthalten und selbst eine qualifizierte elektronische Signatur tragen. Denn Signaturen mit einem geringeren Sicherheitswert können nicht nur leicht eine Fälschung der qualifizierten Zertifikate ermöglichen, sondern in der Folge auch eine Fälschung der darauf beruhenden qualifizierten elektronischen Signaturen.[41] Jeglicher Verstoß gegen die Mindestanforderungen des § 7 SigG hat damit ein Fehlen der Form einer qualifizierten elektronischen Signatur zur Folge.

b) Sichere Signaturerstellungseinheit

Gemäß § 2 Nr. 3 SigG ist Tatbestandsmerkmal einer qualifizierten elektronischen Signatur, dass diese mit einer „sicheren Signaturerstellungseinheit" (§ 2 Nr. 10 SigG), also mit einer sicheren Signaturkarte und ihrer zugehörigen PIN, erzeugt worden ist. Die Anforderungen an eine „sichere Signaturerstellungseinheit" sind in § 17 Abs. 1, 3 SigG näher definiert. Sie zielen auf die Fälschungssicherheit von Signaturen und signierten Daten ab. Demgemäß sind Adressaten dieser Vorschriften die Zertifizierungsdiensteanbieter. Das Signaturgesetz macht in § 17 Abs. 4 Satz 1 das Vorliegen einer „sicheren Signaturerstellungseinheit" davon abhängig, dass eine nach § 18 SigG von der Bundesnetzagentur anerkannte Bestätigungsstelle[42] die Übereinstimmung der Karte mit den Anforderungen der § 17 Abs. 1 und Abs. 3 Nr. 1 SigG bestätigt hat. Ein derartiger Bestätigungsvermerk wird regelmäßig erst nach einer aufwendigen Sicherheitsüberprüfung der vom Zertifizierungsdiensteanbieter angewendeten Verfahren und Techniken erteilt.[43]

Die Folgen eines Verstoßes gegen die in § 17 Abs. 1 und Abs. 3 Nr. 1 SigG normierten Anforderungen an eine „sichere Signaturerstellungseinheit" sind zwar im Signaturgesetz nicht ausdrücklich festgelegt, ergeben sich aber mittelbar aus § 19 Abs. 4 SigG. Danach ist ein solcher Verstoß für die Existenz einer qualifizierten elektronischen Signatur im Ergebnis ohne Relevanz. Zwar kann es zu Sicherheitsmängeln des Zertifikats führen, wenn §§ 17 Abs. 1, 3 Nr. 1 SigG verletzt wird. Bei Bestehen von Sicherheitsmängeln sieht § 19 Abs. 4 SigG aber lediglich die Sperrung des Zertifikats vor, nicht dessen Unwirksamkeit. Des Weiteren ist zu beachten, dass im Wege einer vorbeugenden Kontrolle die sicherheitstechnische Unbedenklichkeit der „sicheren Signaturerstellungseinheit" durch die von der Bundesnetzagentur anerkannte Bestätigungsstelle umfassend geprüft und in einem Bestätigungsvermerk festgestellt sein muss. Diese Bestätigungsvermerke über die Sicherheit der Signaturerstellungseinheit werden von der Bundesnetzagentur auf ihren Internetseiten veröffentlicht. Auf ihre Zuverlässigkeit muss sich der Rechtsverkehr verlassen können.

c) Die Festlegung von Einsatzbedingungen in den Bestätigungsvermerken nach § 17 Abs. 4 Satz 1 SigG

Die Bestätigungsstellen legen in ihren Bestätigungsvermerken nach § 17 Abs. 4 Satz 1 SigG in aller Regel als Einsatzbedingung fest, dass die Signaturkarte verantwortungsvoll verwahrt und eingesetzt werden muss, wobei für den verantwortungsvollen Einsatz vorausgesetzt wird, dass sich der Benutzer über die Signaturgesetzkonformität der Einsatzumgebung vergewissert hat.[44] In neueren Bestätigungsvermerken sind die zuständigen Stellen sogar dazu übergegangen, einen Einsatz nur „in Verbindung mit hinreichend geprüften Signaturanwendungskomponenten" zuzulassen.[45] Damit wird insbesondere auf § 17 Abs. 2 Satz 3 SigG Bezug genommen. Danach hat der Signaturschlüssel-Inhaber geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer

41 Geis, in: Spindler/Schmitz/Geis, SigG, 2004, § 7 Rn. 1.

42 Hierbei handelt es sich um Unternehmen, die die nachgewiesene erforderliche technische Kompetenz für die Prüftätigkeit aufweisen. Die Namen der Prüf- und Bestätigungsstellen werden auch auf den Internetseiten der Bundesnetzagentur veröffentlicht (www.bundesnetzagentur.de/enid/2.html).

43 Fischer-Dieskau, Das elektronisch signierte Dokument als Mittel zur Beweissicherung, 2006, 1. Teil 2.2.2.4.3.; Gassen, Digitale Signaturen in der Praxis – Grundlagen, Sicherheitsfragen und normativer Rahmen, 2003, 3. Teil III. 3.

44 Vgl. Signaturkarte „Signtrust Signaturkarte SEA-Card, Version 2.0", www.bundesnetzagentur.de/media/archive/1555.pdf.

45 Vgl. Signaturkarte „D-TRUST Card, Version 1.0", www.bundesnetzagentur.de/media/archive/1558.pdf.

Signaturen zu treffen. Denn auch der Benutzer muss bei der verwendeten Hard- und Software[46] zur Erzeugung der qualifizierten elektronischen Signatur sicherstellen, dass ein Ausspähen der Signaturdaten nicht über Sicherheitsmängel bei der Einsatzumgebung erfolgen kann.

Die Betonung des engen Zusammenhangs zwischen der „sicheren Signaturerstellungseinheit" und der ebenfalls zur Erzeugung der qualifizierten elektronischen Signatur erforderlichen „Signaturanwendungskomponenten" (§ 2 Nr. 11 SigG) ist angesichts des Ziels der Gewährleistung eines bestimmten Sicherheitsniveaus zwar sachlich richtig. Eine Missachtung dieser in den Bestätigungsvermerken enthaltenen Vorgaben zur Einsatzumgebung ändert signaturrechtlich jedoch nichts an der Existenz und Wirksamkeit einer qualifizierten elektronischen Signatur. Denn Tatbestandsmerkmal des § 2 Nr. 3 SigG ist nur das Vorliegen einer „sicheren Signaturerstellungseinheit". Anforderungen an die Beschaffenheit der „Signaturanwendungskomponenten", also insbesondere an die zur Erzeugung der Signatur notwendige Software (wie beispielsweise SigNotar) oder an die zu verwendenden Kartelesegeräte, werden nicht gestellt. Aufgrund der besonderen Bedeutung der „sicheren Signaturerstellungseinheit" für das wirksame Erzeugen einer qualifizierten elektronischen Signatur sieht § 17 Abs. 4 Satz 1 SigG auch nur für diese eine Bestätigung durch von der Bundesnetzagentur anerkannte Stellen vor, während für „Signaturanwendungskomponenten" eine Herstellererklärung über die Sicherheit und die Erfüllung der Anforderungen des Signaturgesetzes genügt (§ 17 Abs. 4 Satz 2 SigG). Eine Zertifizierung der „Anwendungskomponenten" durch von der Bundesnetzagentur anerkannte Stellen fordert das Gesetz gerade nicht. Entsprechendes kann daher in den Bestätigungsvermerken auch nicht verlangt werden.

Allerdings müssen qualifizierte elektronische Signaturen nach § 2 Nr. 3 SigG i. V. m. § 2 Nr. 2 lit. c) SigG „mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann".[47] Hieraus ergeben sich für „Signaturanwendungskomponenten" jedoch keine besonderen Anforderungen. Denn § 17 SigG regelt detailliert die Anforderungen an Produkte für qualifizierte elektronische Signaturen, also sowohl an „sichere Signaturerstellungseinheiten" als auch an „Signaturanwendungskomponenten".[48] Die Vorschrift geht der allgemeinen Definition in § 2 Nr. 3 SigG i. V. m. § 2 Nr. 2 lit. c) SigG als lex specialis vor. Der Gesetzgeber hatte bei § 2 Nr. 2 lit. c) SigG „Signaturanwendungskomponenten" überhaupt nicht im Sinn. Ihm ging es ausweislich der Begründung des Regierungsentwurfs allein darum, dass der Signaturschlüssel-Inhaber seine „Signaturerstellungseinheit" vor unbefugter Nutzung schützen kann.[49] Der Zertifizierungsdiensteanbieter hat deshalb nach § 2 Nr. 3 SigG i. V. m. § 2 Nr. 2 lit. c) SigG bereits bei der Produktgestaltung darauf zu achten, dass der Signaturschlüssel-Inhaber in die Lage versetzt wird, eine elektronische Signatur ohne Mitwirkung Dritter zu erzeugen.[50] Zudem hat er den Signaturschlüssel-Inhaber über die Notwendigkeit des Ausschlusses Dritter vom Zugriff auf Signaturkarte und PIN zu unterrichten.[51] Im Ergebnis bezieht sich § 2 Nr. 2 lit. c) SigG daher allein auf die „sichere Signaturerstellungseinheit". Für die „Signaturanwendungskomponenten", also für die Signatursoftware und das Kartenlesegerät, ist die Vorschrift dagegen ohne Belang.

4. Beurkundungsverfahrensrechtliche Grundsätze

Die Erkenntnis, dass eine Verletzung signaturrechtlicher Vorschriften mit Ausnahme der Mindestanforderungen nach § 7 SigG für die Wirksamkeit einer qualifizierten elektronischen Signatur und damit für die Wirksamkeit der elektronischen öffentlichen Urkunde grundsätzlich unschädlich ist, wird durch beurkundungsverfahrensrechtliche Überlegungen gestützt.

a) Mängel beim Zertifizierungsdiensteanbieter und fehlerhafter Einsatz der Signaturkarte

Mängel beim Zertifizierungsdiensteanbieter (wie z. B. das Fehlen der Voraussetzungen zum Betrieb einer Zertifizierungsstelle) oder Mängel beim Anwender (etwa aufgrund des fehlerhaften Einsatzes der Signaturkarte) sind für den Rechtsverkehr regelmäßig nicht erkennbar. Häufig kann selbst der Notar, der die Signaturkarte benutzt, derartige Mängel nicht erkennen, weil er keinen Einblick in die interne Organisation des Zertifizierungsdiensteanbieters hat oder weil ihm Mängel in der Einsatzumgebung (wie z. B. eine unzureichende Firewall oder ein unzureichender Virenschutz) nicht bewusst sind. Ebenso wenig wie die Wirksamkeit einer in Papierform erstellten beglaubigten Abschrift nach § 42 Abs. 1 BeurkG davon abhängt, ob der Notar für seine Unterschrift eine den Anforderungen des § 29 DONot entsprechende dokumentenechte Tinte verwendet hat oder ob ein den Anforderungen des § 31 Satz 2 und 3 DONot entsprechendes Farbdruck- bzw. Prägesiegel zum Einsatz gekommen ist, kann die Wirksamkeit eines elektronischen Beglaubigungsvermerks nach § 39 a BeurkG davon abhängen, ob der Notar die in der Bestätigung nach § 17 Abs. 4 Satz 1 SigG für den Einsatz der Signaturkarte festgelegten Bedingungen eingehalten hat oder ob der Zertifizierungsdiensteanbieter sämtliche Voraussetzungen erfüllt, die nach § 4 Abs. 2 SigG an seine Zuverlässigkeit und Sachkunde gestellt werden. Allenfalls kommt – analog zu den bei einem Verstoß gegen die DONot geltenden Grundsätzen – eine Beeinträchtigung des Beweiswertes der Urkunde in Betracht.[52] Letztlich ist auch in diesem Zusammenhang der oben in Abschnitt IV. 1.

---

46 „Signaturanwendungskomponenten" nach § 2 Nr. 11 SigG sind – wie bereits unter Abschnitt VI.2. erwähnt – z. B. das Kartenlesegerät oder die neben der Signaturkarte zur Erzeugung von qualifizierten elektronischen Signaturen erforderliche Software wie z. B. das von der Notarnet GmbH entwickelte Produkt „SigNotar". Zum Begriff der Signaturanwendungskomponente vgl. Demmel, in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, Kommentar, 5. Erglfg. 2001, § 2 SigG Rn. 6.

47 Diese in § 2 Nr. 2 lit. c) SigG normierte Voraussetzung gilt zunächst für „fortgeschrittene elektronische Signaturen". Deren Anforderungen müssen nach § 2 Nr. 3 SigG qua Definition auch bei qualifizierten elektronischen Signaturen beachtet werden (vgl. § 2 Nr. 3 SigG).

48 Vgl. die Legaldefintion in § 2 Nr. 12 SigG.

49 BT-Drs. 14/4662, 18.

50 Demmel, in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, Kommentar, 5. Erglfg. 2001, § 2 SigG Rn. 6.

51 Demmel, in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, Kommentar, 5. Erglfg. 2001, § 2 SigG Rn. 6.

52 Vgl. bereits Abschnitt V.2.

herausgearbeitete Gedanke maßgeblich, dass im Interesse der Rechtssicherheit nur ein Verstoß gegen die wenigen Muss-Vorschriften des BeurkG zur Unwirksamkeit der Urkunde führt und die Verletzung des Verfahrensrechts dabei regelmäßig aus der Urkunde selbst hervorgehen muss.[53]

b) Vorliegen einer qualifizierten elektronischen Signatur mit Nachweis der Notareigenschaft

Wie oben bereits erwähnt,[54] muss eine qualifizierte elektronische Signatur gemäß § 7 SigG allerdings bestimmte Mindestvoraussetzungen erfüllen. Beim Signieren zeigt die Signatursoftware dem Notar regelmäßig an, ob der Signiervorgang erfolgreich war oder ob dabei ein Fehler aufgetreten ist. Arbeitet die Signatursoftware hier nicht richtig, ist jedoch der Fall denkbar, dass ein erfolgreicher Signiervorgang angezeigt wird, obwohl eine qualifizierte elektronische Signatur tatsächlich nicht erzeugt worden ist. Dies hat zur Konsequenz, dass die elektronische Vermerkurkunde nicht wirksam entstanden ist. Beurkundungsverfahrensrechtliche Grundsätze können an diesem Ergebnis nichts ändern, da das Vorliegen einer qualifizierten elektronischen Signatur (§ 39 a Satz 2 BeurkG) und der Nachweis der Notareigenschaft (§ 39 a Satz 4 BeurkG) Muss-Voraussetzungen sind. Für den Notar hat dies die unangenehme Folge, dass er anders als bei der Papierurkunde die Erfüllung aller beurkundungsrechtlichen Voraussetzungen aus eigener Anschauung nicht mit letzter Sicherheit überprüfen kann, sondern auf das fehlerfreie Funktionieren der Signatursoftware angewiesen ist. Letztlich ist diese Folge jedoch vertretbar, weil der Notar über eine auf dem neuesten Stand gehaltene Firewall und einen entsprechenden Virenschutz derartige Fallkonstellationen praktisch ausschließen kann. Im Übrigen muss man sich stets vor Augen führen, dass der Signiervorgang die eigenhändige Unterschrift des Notars ersetzt und aufgrund dieser großen Bedeutung bestimmte Mindestvoraussetzungen eingehalten werden müssen.

c) Weitergabe von Signaturkarte und PIN

Es ist eine Selbstverständlichkeit des Beurkundungsrechts, dass der Notar seine Unterschrift eigenhändig zu leisten hat und ohne formale Bestellung eines Notarvertreters eine Stellvertretung unzulässig ist. Ein Handeln in verdeckter Stellvertretung ohne formale Vertreterbestellung führt zur Unwirksamkeit der Urkunde, denn gemäß § 39 BeurkG *muss* die Urkunde die Unterschrift des Notars selbst tragen. Wenn der Notar den Signiervorgang nicht selbst vornimmt, sondern unter Verstoß gegen das Beurkundungsgesetz und die Richtlinien nach Weitergabe von Signaturkarte und PIN durch einen Dritten ausführen lässt, ist die elektronische Vermerkurkunde unwirksam. Denn elektronisches Äquivalent der *eigenhändigen* Unterschrift des Notars ist die *eigenhändige* Erzeugung einer qualifizierten elektronischen Signatur unter Verwendung von Signaturkarte und PIN.[55]

---

53 Mecke, DNotZ 1968, 584, 601; Winkler, BeurkG, 15. Aufl. 2003, Einl. Rn. 11.

54 Vgl. Abschnitt VI.3.a).

55 Ausführlich zum Verbot der Weitergabe von Signaturkarte und PIN auch Bettendorf, in: Beck'sches Notar-Handbuch, 4. Aufl. 2006, Kap. M Rn. 154. Vgl. zudem bereits Abschnitt II.1.

Ehegattenverfügungen bei behinderten, sozialhilfebedürftigen oder verschuldeten Kindern: Einsetzung des „Problemkindes" als Nacherbe?

(von Notar Dr. Michael Kleensang, M.A., Pulheim)

1. Einleitung

Wie Behindertentestamente sollen auch Verfügungen von Todes wegen zugunsten Verschuldeter oder Sozialhilfeempfänger in der Regel zwei Ziele erreichen: Der Begünstigte soll an der Erbschaft partizipieren, diese aber gleichzeitig dem Zugriff seiner Gläubiger, des Sozialhilfeträgers oder, im Restschuldbefreiungsverfahren nach §§ 295 ff. InsO, des Treuhänders entzogen werden. Verfügungen zugunsten Verschuldeter stehen sowohl vor dem Hintergrund des 1999 eingeführten Verbraucherinsolvenzverfahrens als auch aufgrund der 2005 in Kraft getretenen „Hartz IV"-Reformen vor teilweise neuen Gestaltungaufgaben und einem insgesamt ausgeweiteten Anwendungsfeld: So hat das Restschuldbefreiungsverfahren nach §§ 295 ff. InsO neue Fragen aufgeworfen, insbesondere die, ob der Treuhänder die Restschuldbefreiung versagen darf, wenn der Betroffene die Geltendmachung eines Pflichtteilsanspruches unterlässt.[1] Damit stellt sich auch im Bereich des Verschuldetentestaments die Aufgabe, das Entstehen eines Pflichtteilsanspruches möglichst zu vermeiden, während außerhalb eines Restschuldbefreiungsverfahrens ein „gewöhnlicher" Gläubiger den Pflichtteilsanspruch – entgegen dem Wortlaut des § 852 Abs. 1 ZPO – zwar pfänden, aber nicht verwerten kann.[2] Gleiches gilt für das am 1. 1. 2005 in Kraft getretene Vierte Gesetz für moderne Dienstleistungen am Arbeitsmarkt[3], kurz „Hartz IV": Sobald der Betroffene kein Arbeitslosengeld I mehr erhält, sondern Bezieher von Arbeitslosengeld II wird, mutiert er faktisch zum Sozialhilfeempfänger.[4] Wie bei dem sozialhilfebedürftigen Behinderten nach § 93 SGB XII könnte der Leistungsträger einen dem Leistungsbezieher zustehenden Pflichtteilsanspruch auf sich überleiten und geltendmachen (§ 33 SGB II).

---

1 Vgl. Ivo, ZErb 2003, 250, 255 f.: zumindest in Höhe der Hälfte des Pflichtteilsanspruches müsse eine Geltendmachung erfolgen; anderenfalls sei ein Obliegenheitsverstoß anzunehmen, der nach § 296 InsO zur Versagung der Restschuldbefreiuung führen könne.

2 BGHZ 123, 183.

3 BGBl I 2003, 2954.

4 Vgl. näher J. Mayer, in: Mayer/Bonefeld/Wälzholz/Weidlich, Testamentsvollstreckung, 2. Aufl. 2005, Rn. 610 ff.