Udo Schäfer,
Authentizität: Elektronische Signaturen oder Ius Archivi?

aus:

Digitales Verwalten – Digitales Archivieren

Veröffentlichungen aus dem Staatsarchiv der Freien und Hansestadt Hamburg, Band 19

Herausgegeben von Rainer Hering und
Udo Schäfer

S. 13-31

Impressum für die Gesamtausgabe

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Diese Publikation ist außerdem auf der Website des Verlags Hamburg University Press *open access* verfügbar unter http://hup.rrz.uni-hamburg.de.

Die Deutsche Bibliothek hat die Netzpublikation archiviert. Diese ist dauerhaft auf dem Archivserver Der Deutschen Bibliothek verfügbar unter http://deposit.ddb.de.
ISBN 3-937816-09-7 (Printausgabe)
ISSN 0436-6638 (Printausgabe)

Inhalt

Dokumentenmanagementsysteme (DMS) zwischen Verwaltung und Archiv

Authentizität:
Elektronische Signaturen oder Ius Archivi?

Udo Schäfer

1 Authentizität

> „As a society, we want our leaders and the people who act in our name to be accountable for their actions, and records play a role in rendering that account. So it is in our interest to establish standards for reliable and authentic records, and archivists have a role to play in achieving that objective.“[1]

Mit diesem Satz begründet Heather MacNeil, School of Library, Archival and Information Studies der University of British Columbia, weshalb sich Archivarinnen und Archivare mit der Frage befassen müssen, wie die Authentizität digitaler Aufzeichnungen zu gewährleisten ist. Auch in Deutschland ist die Frage von den öffentlichen Archiven sowie der Archivwissenschaft aufgegriffen worden. So haben Michael Wettengel,[2] Frank M. Bischoff[3] und der Verfasser[4] in den Jahren 1997 bis 1999 Aufsätze zur digita-

---

[1] Heather MacNeil: Trusting Records in a Postmodern World. In: Archivaria 51 (2001) S. 46.

[2] Michael Wettengel: Digitale Unterschriften. In: Der Archivar 50 (1997) Sp. 89–94. – Ders.: Digitale Signaturen und Pilotprojekte zur IT-gestützten Vorgangsbearbeitung in der Bundesverwaltung. In: Archivierung von Unterlagen aus digitalen Systemen. Beiträge zur Tagung im Staatsarchiv Münster, 3.–4. März 1997. Hg. von Frank M. Bischoff (Veröffentlichungen der staatlichen Archive des Landes Nordrhein-Westfalen E 4). Münster 1997. S. 11–13.

[3] Frank M. Bischoff: Authentizitätssicherung elektronischer Dokumente – Zur Bedeutung digitaler Signaturen für die Archivierung. In: Archivkurier 12 (1998) S. 8–13. – Ders.: Zur

len Signatur veröffentlicht. Eine Aufzeichnung ist authentisch, wenn sie das ist, was sie vorgibt zu sein, und wenn sie frei von Verfälschung oder unerlaubter Veränderung ist.[5] Eine Möglichkeit, den Nachweis der Authentizität digitaler Aufzeichnungen zu führen, ist die Verwendung digitaler Signaturen.

Zur digitalen Signierung eines elektronischen Dokuments bedarf es eines Algorithmus zur Erzeugung eines Komprimats und zweier Algorithmen zur Erzeugung eines asymmetrischen Schlüsselpaares.[6] Die Signatur wird

---

Archivfähigkeit digitaler Signaturen in elektronischen Registern. In: Archivierung elektronischer Unterlagen. Hg. von Udo Schäfer und Nicole Bickhoff (Werkhefte der Staatlichen Archivverwaltung Baden-Württemberg A 13). Stuttgart 1999. S. 183–198.

[4] Udo Schäfer: Authentizität. Vom Siegel zur digitalen Signatur. In: Archivierung elektronischer Unterlagen. Hg. von dems. und Nicole Bickhoff (Werkhefte der Staatlichen Archivverwaltung Baden-Württemberg A 13). Stuttgart 1999. S. 165–181.

[5] Authenticity Task Force Report. S. 2. In: The Long-term Preservation of Authentic Electronic Records: Findings of the InterPares Project. September 2002 (www.interpares.org. Abruf: 5.8.2003). – Luciana Duranti: Draft Conceptual Requirements for Authenticity. In: Preserving Authentic Electronic Records: Preliminary Research Findings. Proceedings from an International Symposium, February 17, 2001, University of British Columbia. Hg. von Luigi Sarno. Vancouver 2001 (www.interpares.org. Abruf: 19.8.2003). S. 42. – Heather MacNeil: Providing Grounds for Trust: Developing Conceptual Requirements for the Long-Term Preservation of Authentic Electronic Records. In: Archivaria 50 (2000) S. 53. – Dies.: Conceptualizing an Authentic Electronic Record. Presentation on the Society of American Archivists' Annual Meeting, Denver, Colorado, August 31, 2000 (www.interpares.org. Abruf: 17.10.2002). S. 1. – Dies.: Providing Grounds for Trust II: The Findings of the Authenticity Task Force of InterPARES. In: Archivaria 54 (2002) S. 26. – Dies.: Grounds for Trust: The Findings of the Authenticity Task Force of InterPARES 1. Presentation on the Society of American Archivists' Annual Meeting, Birmingham, Alabama, June 22, 2002, S. 1.

[6] Vgl. zur Kryptographie Markus Sanner: Die digitale Signatur. Regensburg 2001. S. 5–14. – Sebastian Jungermann: Der Beweiswert elektronischer Signaturen. Eine Studie zur Verläßlichkeit elektronischer Signaturen und zu den Voraussetzungen und Rechtsfolgen des § 292a ZPO (Schriften zum Handels- und Wirtschaftsrecht 9). Frankfurt am Main u. a. 2002. S. 5–25, 45–60. – Christiane Rapp: Rechtliche Rahmenbedingungen und Formqualität elektronischer Signaturen (Information und Recht 37). München 2002. S. 5–22.

erstellt, indem der Aussteller aus dem Text des Dokuments ein Komprimat mit einer bestimmten Länge berechnet und dieses Komprimat mit seinem privaten Schlüssel verschlüsselt. Der Text des Dokuments wird dem Empfänger zusammen mit der Signatur übermittelt. Der Empfänger kann die Signatur verifizieren,[7] indem er

1. aus dem Text des Dokuments mit demselben Algorithmus ein zweites Komprimat bildet, das erste Komprimat mit dem beim jeweiligen Zertifizierungsdiensteanbieter abgerufenen öffentlichen Schlüssel entschlüsselt und das zweite mit dem ersten Komprimat vergleicht,
2. über das beim jeweiligen Zertifizierungsdiensteanbieter abgerufene Zertifikat prüft,
   a. ob der als Aussteller des Dokuments Angegebene mit dem Inhaber des öffentlichen Schlüssels identisch ist und
   b. das Zertifikat zum Zeitpunkt der Signierung noch gültig war und
3. über den Bundesanzeiger prüft, ob die zur Signierung und zur Verifikation verwendeten Algorithmen zum Zeitpunkt der Verifikation noch als geeignet anzusehen sind.

Ist die digitale Signatur mit Erfolg verifiziert worden, so darf das elektronische Dokument als authentisch betrachtet werden.

Elektronische Unterlagen, die bleibenden Wert besitzen, sind vor der Übergabe an das zuständige Archiv in das Format zu konvertieren, das vom Archiv verwendet wird, um Archivgut in digitaler Form zu verwahren. Durch die Konversion wird sich die binäre Darstellung verändern. Sofern die elektronischen Unterlagen digital signierte Dokumente enthalten, wird das mit dem privaten Schlüssel verschlüsselte erste Komprimat nach der Konversion bereits nicht mit dem öffentlichen Schlüssel entschlüsselt werden können oder mit dem zweiten Komprimat nicht übereinstimmen. Jedenfalls können die digitalen Signaturen nach der Konversion nicht mehr verifiziert werden.[8] Deshalb hat der Verfasser in seinem Aufsatz aus dem

---

[7] Vgl. zur Verifikation Stephan Spitz: Verifikation von digitalen Signaturen. Modellierung einer vollständigen Signaturprüfung. In: Datenschutz und Datensicherheit 25 (2001) S. 459–463.

[8] Jos Dumortier und Sofie Van den Eynde: Electronic signatures and trusted archival services. In: Proceedings of the DLM-Forum 2002. @ccess and preservation of electronic in-

Jahre 1999 vorgeschlagen, das Institut des *ius archivi* im passiven Sinne aus dem römisch-kanonischen *ius commune* und dem *ius publicum* des Alten Reiches in das geltende Recht zu übernehmen.[9] Von Seiten der Rechtswissenschaft hat sich mit diesem Vorschlag bisher lediglich Dieter Strauch, Professor emeritus an der Juristischen Fakultät der Universität Köln, beschäftigt.[10] Nach einer Einführung in das Recht der elektronischen Signaturen und in das Projekt „International Research on Permanent Authentic Records in Electronic Systems 1" wird der Verfasser seinen Vorschlag noch einmal darlegen. Der Begriff der digitalen Signatur ist nicht mit dem der elektronischen Signatur identisch. Vielmehr wird Letzterer als Oberbegriff verwendet.

2 Das Recht der elektronischen Signaturen

2.1 Das internationale Recht

In den Jahren 1966 und 1967 haben die Vereinten Nationen die United Nations Commission on International Trade Law (UNCITRAL) errichtet, um die Harmonisierung des Handels- und Wirtschaftsrechts zu fördern.[11] Die Kommission hat im Jahre 1996 das „UNCITRAL Model Law on Electronic Commerce"[12] und im Jahre 2001 das „UNCITRAL Model Law on

formation: Best practices and solutions. Barcelona, 6–8 May 2002 (INSAR. Supplement 7). Luxemburg 2002. S. 521. – Alexander Roßnagel, Stefanie Fischer-Dieskau, Ulrich Pordesch und Ralf Brandner: Erneuerung elektronischer Signaturen. Grundfragen der Archivierung elektronischer Dokumente. In: Computer und Recht 19 (2003) S. 305.

[9] Schäfer, wie Anm. 4, S. 178–181.

[10] Dieter Strauch: Rechtliche und archivische Probleme der digitalen Signatur. In: Gedächtnisschrift für Alexander Lüderitz. München 2000. S. 751–787.

[11] Herbert Kronke: Ziele – Methoden, Kosten – Nutzen: Perspektive der Privatrechtsharmonisierung nach 75 Jahren UNIDROIT. In: Juristenzeitung 56 (2001) S. 1149–1157.

[12] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 (www.uncitral.org. Abruf: 16.9.2003). – Vgl. Sanner, wie Anm. 6, S. 212–218.

Electronic Signatures“[13] vorgelegt. Das „UNCITRAL Model Law on Electronic Commerce“ verwendet in Art. 7 Abs. 1 einen weiten Begriff der Signatur:

> „Where the law requires a signature of a person, that requirement is met in relation to a data message if:
> (a) method is used to identify that person and to indicate that person’s approval of the information contained in the data message; and
> (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.“

In Art. 2 lit. a und Art. 6 Abs. 1 hat das „UNCITRAL Model Law on Electronic Signatures“ diesen weiten Begriff übernommen. Es beschreibt in Art. 6 Abs. 3 die Anforderungen an eine zuverlässige elektronische Signatur:

> „An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:
> (a) The signature creation data are, within in the context in which they are used, linked to the signatory and to no other person;
> (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
> (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
> (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.“

---

[13] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001. New York 2002 (www.uncitral.org. Abruf: 10.7.2002). – Vgl. zum Entwurf (Stand: September 1999) Felix Blum: Das UNCITRAL-Modellgesetz zu elektronischen Signaturen. In: Kommunikation & Recht 3 (2000) S. 63–71. – Sanner, wie Anm. 6, S. 219–253, und zum Entwurf (Stand: September 2000) Rapp, wie Anm. 6, S. 127–131.

Sinn und Zweck des Art. 6 ist es, die elektronische Signatur der eigenhändigen Unterschrift gleichzustellen.[14]

2.2 Das Recht der Europäischen Union

Die Mitgliedstaaten der Europäischen Union hatten die Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt[15] und die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen[16] in nationales Recht umzusetzen.[17] Die Richtlinie 1999/93/EG unterscheidet zwischen

1. der elektronischen Signatur gemäß Art. 2 Nr. 1,
2. der fortgeschrittenen elektronischen Signatur gemäß Art. 2 Nr. 2 und

---

[14] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, wie Anm. 13, S. 52.

[15] Amtsblatt der Europäischen Gemeinschaften 2000. L 178. S. 1–16.

[16] Amtsblatt der Europäischen Gemeinschaften 2000. L 13. S. 12–20.

[17] Vgl. Wendelin Bieser: Signaturgesetz: Die digitale Signatur im europäischen und internationalen Kontext. In: Recht der Datenverarbeitung 16 (2000) S. 197–202, 264–268. – Helmut Redeker: EU-Signaturrichtlinie und Umsetzungsbedarf im deutschen Recht. In: Computer und Recht 16 (2000) S. 455–461. – Alexander Roßnagel: Der europäische Standard: Die elektronische Signatur der europäischen Richtlinie. In: Die digitale Signatur – eine Sicherheitstechnik für die Informationsgesellschaft. Ein Leitfaden für Anwender und Entscheider. Hg. von Ivo Geis. Eschborn 2000. S. 195–230. – Ders.: Digitale Signaturen im europäischen elektronischen Rechtsverkehr. In: Kommunikation & Recht 3 (2000) S. 313–323. – Alexander Tettenborn: Die Evaluierung des Signaturgesetzes und Umsetzung der EG-Signaturrichtlinie. In: Die digitale Signatur – eine Sicherheitstechnik für die Informationsgesellschaft. Ein Leitfaden für Anwender und Entscheider. Hg. von Ivo Geis. Eschborn 2000. S. 231–252. – Uwe Blaurock und Jürgen Adam: Elektronische Signatur und europäisches Privatrecht. In: Zeitschrift für Europäisches Privatrecht 9 (2001) S. 93–115. – Rapp, wie Anm. 6, S. 36–50.

3. der fortgeschrittenen elektronischen Signatur im Sinne des Art. 5 Abs. 1, die auf einem qualifizierten Zertifikat gemäß Art. 2 Nr. 10 beruht und von einer sicheren Signaturerstellungseinheit gemäß Art. 2 Nr. 6 erstellt wird.

Während Art. 2 Nr. 13 den Mitgliedstaaten die Befugnis gewährt, Systeme zur freiwilligen Akkreditierung von Zertifizierungsdiensteanbietern einzuführen, bietet Art. 3 Abs. 7 den Mitgliedstaaten die Möglichkeit, an den Einsatz elektronischer Signaturen im öffentlichen Sektor zusätzliche Anforderungen zu stellen. Für den privaten Sektor verlangt Art. 9 Abs. 1 der Richtlinie 2000/31/EG die Gleichsetzung einer elektronischen Willenserklärung mit einer Urkunde. Für den privaten und den öffentlichen Sektor fordert Art. 5 Abs. 1 lit. a der Richtlinie 1999/93/EG die Gleichstellung der fortgeschrittenen elektronischen Signatur, die auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erstellt wird, mit der eigenhändigen Unterschrift.[18]

2.3 Das Recht der Bundesrepublik Deutschland

2.3.1 Technik- und Gewerberecht

In Umsetzung der Richtlinie 1999/93/EG sind das Gesetz zur digitalen Signatur (Signaturgesetz – SigG) vom 22. Juli 1997[19] zum 22. Mai 2001 durch das Gesetz über Rahmenbedingungen für elektronische Signaturen

---

[18] Alexander Roßnagel: Digitale Signaturen im europäischen elektronischen Rechtsverkehr. In: Kommunikation & Recht 3 (2000) S. 320–323.

[19] Bundesgesetzblatt 1997. Teil I. S. 1872–1876. – Vgl. Alexander Roßnagel: Die Sicherheitsvermutung des Signaturgesetzes. In: Neue Juristische Wochenschrift 51 (1998) S. 3312–3320. – Ders.: Das Signaturgesetz nach zwei Jahren. Hinweise zur Gesetzesevaluierung. In: Neue Juristische Wochenschrift 52 (1999) S. 1591–1596. – Michael Baum: Gültigkeitsmodell des SigG. Die Gültigkeit der Signatur als Voraussetzung für die Sicherheitsvermutung nach § 1 I SigG. In: Datenschutz und Datensicherheit 23 (1999) S. 199–205. – Rapp, wie Anm. 6, S. 34–36.

(Signaturgesetz – SigG) vom 16. Mai 2001[20] und die Verordnung zur digitalen Signatur (Signaturverordnung – SigV) vom 22. Oktober 1997[21] zum 22. November 2001 durch die Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001[22] abgelöst worden. Dabei fand die folgende Differenzierung[23] Eingang in das Technik- und Gewerberecht:

1. Elektronische Signaturen sind gemäß § 2 Nr. 1 SigG Daten in elektronischer Form, die mit anderen elektronischen Daten verbunden sind und die zur Authentifizierung dienen.
2. Fortgeschrittene elektronische Signaturen[24] sind gemäß § 2 Nr. 2 SigG elektronische Signaturen, die
   a. ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
   b. die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
   c. mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
   d. mit den Daten, auf die sie sich beziehen, so verbunden sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

---

[20] Bundesgesetzblatt 2001. Teil I. S. 876–883. – Vgl. zum Entwurf Alexander Tettenborn: Die Novelle des Signaturgesetzes. In: Computer und Recht 16 (2000) S. 683–691, und zum Gesetz Alexander Roßnagel: Das neue Recht elektronischer Signaturen. Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO. In: Neue Juristische Wochenschrift 54 (2001) S. 1818, 1819–1825. – Rapp, wie Anm. 6, S. 52–66. – Michael Schmidl: Die elektronische Signatur. Funktionsweise, rechtliche Implikationen, Auswirkungen der EG-Richtlinie. In: Computer und Recht 18 (2002) S. 508–517.

[21] Bundesgesetzblatt 1997. Teil I. S. 2498–2502.

[22] Bundesgesetzblatt 2001. Teil I. S. 3074–3084. – Vgl. Ivo Geis: Die neue Signaturverordnung: Das Sicherheitssystem für die elektronische Kommunikation. In: Kommunikation & Recht 5 (2002) S. 59–61.

[23] Vgl. Alexander Roßnagel: Rechtliche Unterschiede von Signaturverfahren. In: MultiMedia und Recht 5 (2002) S. 215–222.

[24] Vgl. Alexander Roßnagel: Die fortgeschrittene elektronische Signatur. In: MultiMedia und Recht 6 (2003) S. 164–170.

3. Qualifizierte elektronische Signaturen sind gemäß § 2 Nr. 3 SigG fortgeschrittene elektronische Signaturen, die
   a. auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat nach § 2 Nr. 7 SigG beruhen und
   b. mit einer sicheren Signaturerstellungseinheit nach § 2 Nr. 10 SigG erzeugt werden.

Daten, die mit einer qualifizierten elektronischen Signatur versehen worden sind, müssen gemäß § 17 SigV mit einer weiteren qualifizierten oder einer akkreditierten elektronischen Signatur sowie einem qualifizierten Zeitstempel nach § 2 Nr. 14 SigG versehen werden, bevor die Eignung der zur Erzeugung und Prüfung eingesetzten Algorithmen sowie der zugehörigen Parameter abläuft, sofern die Daten über diesen Zeitpunkt hinaus in signierter Form benötigt werden. Nach Veröffentlichung der Algorithmen und zugehörigen Parameter im Bundesanzeiger soll die Dauer der Eignung mindestens sechs Jahre betragen.[25] Die erneute Signierung muss frühere Signaturen einschließen.[26] Die qualifizierten Zertifikate sind gemäß § 4 Abs. 1 SigV nach Ablauf des Jahres, in dem deren Gültigkeit endet, vom Zertifizierungsdiensteanbieter lediglich fünf Jahre lang aufzubewahren. Nach § 14 Abs. 3 Satz 1 SigV darf die Gültigkeitsdauer eines qualifizierten Zertifikates höchstens fünf Jahre betragen und den Zeitraum der Eignung der Algorithmen und zugehörigen Parameter nicht überschreiten.

4. Akkreditierte elektronische Signaturen[27] sind gemäß § 15 Abs. 1 Satz 4 SigG qualifizierte elektronische Signaturen, deren qualifiziertes Zertifikat von einem akkreditierten Zertifizierungsdiensteanbieter im Sinne des § 15 Abs. 1 Sätze 1 und 2 SigG ausgestellt worden ist. Nach § 4 Abs. 2 SigV müssen akkreditierte Zertifizierungsdiensteanbieter die qualifizierten Zertifikate nach Ablauf des Jahres, in dem deren Gültigkeit endet, 30 Jahre lang aufbewahren.

---

[25] SigV. Anlage 1. Nr. 2.

[26] Vgl. Ralf Schneider: Neusignatur – Anforderungen und Praxis. In: Datenschutz und Datensicherheit 27 (2003) S. 91–94.

[27] Vgl. zum Begriff Roßnagel, wie Anm. 20, S. 1822. – Ders., wie Anm. 23, S. 215, Anm. 2.

Digitale Signaturen, die auf asymmetrischer Kryptographie beruhen, stellen lediglich die qualifizierte und die akkreditierte elektronische Signatur dar.[28] Nur der Einsatz der akkreditierten elektronischen Signatur ist gemäß § 15 Abs. 1 Satz 4 SigG mit einer technisch-organisatorischen Sicherheitsvermutung verbunden.[29]

2.3.2 Zivilrecht und Zivilprozessrecht

Die Richtlinien 2000/31/EG und 1999/93/EG bewirkten die Aufnahme von Regelungen über elektronisch signierte Dokumente in das Zivilrecht und das Zivilprozessrecht. Als Alternative zur schriftlichen Form im Sinne des § 126 Abs. 1 und 2 BGB darf gemäß § 126 Abs. 3 BGB die elektronische Form im Sinne des § 126a BGB verwendet werden. Der Aussteller muss dem elektronischen Dokument seinen Namen hinzufügen und es mit einer qualifizierten elektronischen Signatur im Sinne des § 2 Nr. 3 SigG versehen.[30] Ein elektronisches Dokument darf gemäß § 130a Abs. 1 Satz 1 und Abs. 2 ZPO bei einem Zivilgericht als Schriftsatz eingereicht werden, sofern eine Rechtsverordnung diese Möglichkeit eröffnet. Das elektronische Dokument soll gemäß § 130a Abs. 1 Satz 2 ZPO mit einer qualifizierten elektronischen Signatur im Sinne des § 2 Nr. 3 SigG versehen werden. § 299a ZPO erlaubt die retrospektive Digitalisierung analoger Prozessakten.

Nach § 371 Abs. 1 Satz 2 ZPO unterliegen elektronische Dokumente dem Beweis durch Augenschein.[31] Erfolgte die Ausstellung des Dokuments aber in der elektronischen Form des § 126a BGB, so ordnet § 292a ZPO den Anschein der Echtheit des Dokuments an. An die Stelle eines Erfah-

---

[28] Vgl. zur Differenzierung zwischen den Begriffen der elektronischen und der digitalen Signatur: UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, wie Anm. 13, S. 20–31.

[29] Roßnagel, wie Anm. 20, S. 1822. – Ders., wie Anm. 23, S. 217 f.

[30] Vgl. Walter Boente und Thomas Riehm: Das BGB im Zeitalter digitaler Kommunikation – Neue Formvorschriften. In: Juristische Ausbildung 23 (2001) S. 795–798.

[31] Vgl. Stefanie Fischer-Dieskau, Rotraud Gitter, Sandra Paul und Roland Steidle: Elektronisch signierte Dokumente als Beweismittel im Zivilprozess. In: MultiMedia und Recht 5 (2002) S. 709 f.

rungssatzes tritt eine gesetzliche Vorgabe. Der Gegenbeweis setzt nicht das Maß eines Beweises des Gegenteils einer gesetzlichen Vermutung im Sinne des § 292 Satz 1 ZPO voraus. § 292a ZPO ist keine das Gericht bindende Beweisregel im Sinne des § 286 Abs. 2 ZPO. Vielmehr ist mit § 292a ZPO lediglich eine in der Wirkung reduzierte Beweislastumkehr verbunden.[32] Die technisch-organisatorische Sicherheitsvermutung des § 15 Abs. 1 Satz 4 SigG erleichtert die Widerlegung des Gegenbeweises.[33]

2.3.3 Verwaltungsrecht und Verwaltungsprozessrecht

Die Richtlinie 1999/93/EG förderte auch die Aufnahme von Regelungen über elektronisch signierte Dokumente in das Verwaltungsrecht[34] und das Verwaltungsprozessrecht. An Stelle der Schriftform darf gemäß § 3a Abs. 2 Satz 1 Allgemeines Verwaltungsverfahrensgesetz (VwVfG) Bund die elektronische Form verwendet werden. Das elektronische Dokument ist gemäß § 3a Abs. 2 Satz 2 VwVfG Bund mit einer qualifizierten elektronischen Signatur im Sinne des § 2 Nr. 3 SigG zu versehen. Für den Erlass eines Verwaltungsaktes in elektronischer Form nach § 37 Abs. 3 VwVfG Bund kann gemäß § 37 Abs. 4 VwVfG Bund durch Rechtsvorschrift[35] die Verwendung einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur vorgeschrieben werden. Die Feststellung der dauerhaften Überprüfbarkeit erfolgt nach dem Stand der Technik. Aktuell wird die akkreditierte elektronische Signatur im Sinne des § 15 Abs. 1 Satz 4 SigG als dauerhaft

---

[32] Jungermann, wie Anm. 6, S. 87–133. – Ders.: Der Beweiswert elektronischer Signaturen. Zu den Voraussetzungen und Rechtsfolgen des § 292a ZPO. In: Datenschutz und Datensicherheit 27 (2003) S. 69–72.

[33] Vgl. aber Roßnagel, wie Anm. 20, S. 1826. – Ders., wie Anm. 23, S. 217 f. – Fischer-Dieskau/Gitter/Paul/Steidle, wie Anm. 31, S. 710–713.

[34] Vgl. Walter Ganßer: Organisatorische Aspekte der Einführung der elektronischen Signatur. In: Verwaltung und Management 9 (2003) S. 89–95.

[35] Vgl. zum Beispiel § 69 Abs. 2 Satz 2 VwVfG Bund.

überprüfbar im Sinne des § 37 Abs. 4 VwVfG Bund betrachtet.[36] Nach § 86a Abs. 1 Satz 1 und Abs. 2 Verwaltungsgerichtsordnung (VwGO) darf ein elektronisches Dokument bei einem Verwaltungsgericht als Schriftsatz eingereicht werden, sofern eine Rechtsverordnung diese Möglichkeit eröffnet. Das elektronische Dokument soll gemäß § 86a Abs. 1 Satz 2 VwGO mit einer qualifizierten elektronischen Signatur im Sinne des § 2 Nr. 3 SigG versehen werden. Nach § 173 Satz 1 VwGO gilt § 299a ZPO entsprechend.

Da sich die binäre Darstellung eines elektronischen Dokuments, das mit qualifizierten elektronischen Signaturen versehen worden ist, mit der Konversion in ein anderes Format ändert, sind die qualifizierten elektronischen Signaturen nach der Konversion nicht mehr verifizierbar. Deshalb ermächtigt § 33 Abs. 1, Abs. 4 Nr. 4b VwVfG Bund die Behörden im Sinne des § 1 Abs. 4 VwVfG Bund, elektronische Dokumente nach der Konversion zu beglaubigen. Nach § 33 Abs. 5 Satz 2, Satz 1 Nr. 2 und 1 VwVfG Bund muss der Beglaubigungsvermerk die Ergebnisse der vor der Konversion erfolgten Verifikation enthalten und mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur im Sinne des § 37 Abs. 4 VwVfG Bund versehen werden.[37] Vor dem Verwaltungsgericht gelten § 371 Abs. 1 Satz 2 ZPO gemäß § 98 VwGO[38] und § 292a ZPO gemäß § 173 Satz 1 VwGO entsprechend.

2.3.4 Registerrecht

Der öffentliche Glaube des elektronischen Grundbuchs und anderer elektronischer Register der Freiwilligen Gerichtsbarkeit beruht auch auf der

---

[36] Deutscher Bundestag. Drucksache 14/9000. S. 33. – Heribert Schmitz und Arne Schlatmann: Digitale Verwaltung? Das Dritte Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften. In: Neue Zeitschrift für Verwaltungsrecht 21 (2002) S. 1286 f. – Alexander Roßnagel: Das elektronische Verwaltungsverfahren. Das Dritte Verwaltungsverfahrensänderungsgesetz. In: Neue Juristische Wochenschrift 56 (2003) S. 473.

[37] Roßnagel, wie Anm. 36, S. 474.

[38] Schmitz/Schlatmann, wie Anm. 36, S. 1288 f., 1287 f.

digitalen Signierung[39] der Eintragungen. Die Verwahrung geschlossener elektronischer Registerblätter als Archivgut ohne Pflege der digitalen Signaturen oder sogar ohne Übernahme der bisherigen digitalen Signaturen bedarf deshalb der gesetzlichen Regelung.[40]

3 Das Projekt InterPARES 1

Auf der Grundlage der insbesondere von Luciana Duranti, Professorin an der School of Library, Archival and Information Studies der University of British Columbia, entwickelten Richtung *contemporary archival diplomatics*[41] und den Ergebnissen des Projekts „The Preservation of the Integrity of Electronic Records" der University of British Columbia aus den Jahren 1994 bis 1997[42] führte eine internationale und multidisziplinäre Gruppe unter Leitung von Luciana Duranti in den Jahren 1999 bis 2001 das Projekt „International Research on Permanent Authentic Records in Electronic Systems 1" (InterPARES 1) durch.[43] In dem Projekt sind zwei Gruppen von

---

[39] § 75 GBV. – §§ 57 HRV, 75 GBV. – §§ 1 Abs. 1 PRV, 57 HRV, 75 GBV. – §§ 28 VRV, 75 GBV. – § 62 SchRegDV. – §§ 13 Abs. 5 LuftRegV, 62 SchRegDV.

[40] Schäfer, wie Anm. 4, S. 177 f., 180. – Frank M. Bischoff: Zur Archivfähigkeit digitaler Signaturen in elektronischen Registern. In: Archivierung elektronischer Unterlagen. Hg. von Udo Schäfer und Nicole Bickhoff (Werkhefte der Staatlichen Archivverwaltung Baden-Württemberg A 13). Stuttgart 1999. S. 197 f. – Vgl. aber Strauch, wie Anm. 10, S. 776–781.

[41] Luciana Duranti: Diplomatics. New Uses for an Old Science. Lanham 1998. – Heather MacNeil: Trusting Records. Legal, Historical and Diplomatic Perspectives (The Archivists Library 1). Dordrecht, Boston und London 2000. – Vgl. Schäfer, wie Anm. 4, S. 171 f. – Vgl. aber die Kritik von Angelika Menne-Haritz: Die Archivwissenschaft, die Diplomatik und die elektronischen Verwaltungsaufzeichnungen. In: Archiv für Diplomatik 44 (1998) S. 337–376.

[42] Luciana Duranti, Terence M. Eastwood und Heather MacNeil: Preservation of the Integrity of Electronic Records. Dordrecht 2002. – Vgl. Schäfer, wie Anm. 4, S. 172–174.

[43] Anne J. Gilliland-Swetland: Testing Our Truths: Delineating the Parameters of the Authentic Archival Electronic Record. In: The American Archivist 65, 2 (2002) S. 200 f.

Anforderungen, deren Erfüllung die Authentizität elektronischer Unterlagen vermuten lassen, entwickelt worden:

1. Die erste Gruppe bilden die *benchmark requirements*. Sie richten sich an die abgebende Stelle. Die Vermutung der Authentizität beruht auf der Anzahl der Anforderungen, die erfüllt werden, und dem Grad, bis zu dem den erfüllten Anforderungen entsprochen wird. Die Integration von Verfahren, die den Verlust oder die unerlaubte Veränderung von Aufzeichnungen verhindern, entdecken oder berichtigen, in das elektronische System stellt eine der Anforderungen dar.
2. Die zweite Gruppe bilden die *baseline requirements*. Sie richten sich an das übernehmende Archiv. Die Vermutung der Authentizität setzt die Erfüllung aller Anforderungen voraus. Als eine der Anforderungen ist die *unbroken custody* zu gewährleisten. Die Anforderungen ergeben sich aus der Rolle des Archivs als *trusted custodian*.[44]

4 Ius Archivi

Die Rolle des Archivs als *trusted custodian* lag bereits dem Institut des *ius archivi* im passiven Sinne, dessen Kenntnis die Rechtsgeschichte[45] vermittelt,

---

[44] Appendix 2. Requirements for Assessing and Maintaining the Authenticity of Electronic Records. In: The Long-term Preservation of Authentic Electronic Records: Findings of the InterPares Project, wie Anm. 5. – Gilliland-Swetland, wie Anm. 43, S. 211 f. – MacNeil: Providing Grounds for Trust II, wie Anm. 5, S. 38–40. – Dies.: Grounds for Trust: The Findings of the Authenticity Task Force of InterPARES 1. Presentation on the Society of American Archivists' Annual Meeting, Birmingham, Alabama, June 22, 2002. S. 7–10.

[45] Friedrich Merzbacher: Ius Archivi. Zum geschichtlichen Archivrecht. In: Archivalische Zeitschrift 75 (1979) S. 135–174. – Schäfer, wie Anm. 4, S. 165–171. – Vgl. Ernst Pitz: Beiträge zur Geschichte des Ius Archivi. In: Der Archivar 16 (1963) Sp. 279–286. – Heinz Lieberich. In: Handwörterbuch zur deutschen Rechtsgeschichte 1. Berlin 1971, Archive, Sp. 213–215. – J. Friedrich Battenberg: Der Funktionswandel der Archive vom 18. Jahrhundert bis zum Beginn des 20. Jahrhunderts. In: 50 Jahre Verein deutscher Archivare. Bilanz und Perspektiven des Archivwesens in Deutschland. Referate des 67. Deutschen Archivtags und

zugrunde. Die Idee, das durch historische Rechtsvergleichung ermittelte Institut des *ius archivi* im passiven Sinne in das geltende Recht zu übernehmen,[46] entspricht der insbesondere von Reinhard Zimmermann, Direktor am Max-Planck-Institut für ausländisches und internationales Privatrecht in Hamburg, verfolgten Konzeption der Rechtsgeschichte als angewandter Rechtswissenschaft.[47] Auf dieser Konzeption beruht auch das Projekt eines historisch-kritischen Kommentars zum BGB, dessen erster Band[48] im Jahre 2003 erschienen ist.

---

des Internationalen Kolloquiums zum Thema: Die Rolle der archivarischen Fachverbände in der Entwicklung des Berufsstandes, 17.–20. September 1996 in Darmstadt (Der Archivar. Beiband 2). Siegburg 1997. S. 108 f.

[46] Schäfer, wie Anm. 4, S. 178–181.

[47] Reinhard Zimmermann: Heutiges Recht, Römisches Recht und heutiges Römisches Recht. Die Geschichte einer Emanzipation durch „Auseinanderdenken". In: Rechtsgeschichte und Privatrechtsdogmatik. Hg. von Reinhard Zimmermann. Heidelberg 2000. S. 1–39. – Ders.: Roman Law, Contemporary Law, European Law. The Civilian Tradition Today. New York 2001. – Ders.: Gemeines Recht heute: Das Kreuz des Südens. In: Der praktische Nutzen der Rechtsgeschichte. Hans Hattenhauer zum 8. September 2001. Hg. von Jörn Eckert. Heidelberg 2002. S. 601–627. – Ders.: Europa und das römische Recht. In: Archiv für die civilistische Praxis 202 (2002) S. 243–316. – Vgl. Rolf Knütel: Rechtseinheit in Europa und römisches Recht. In: Zeitschrift für Europäisches Privatrecht 2 (1994) S. 244–276. – Vgl. auch Christoph Krampe: Europa und das römische Recht. In: Europa. Die Gegenwärtigkeit der antiken Überlieferung. Hg. von Justus Cobet, Carl Friedrich Gethmann und Dieter Lau (Essener Beiträge zur Kulturgeschichte 2). Aachen 2000. S. 383–402. – Vgl. aber die Kritik von Klaus Luig: The History of Roman Private Law and the Unification of European Law. In: Zeitschrift für Europäisches Privatrecht 5 (1997) S. 405–427. – Ders.: Geschichte und Dogmatik bei Knütel, Kötz und Zimmermann. In: Norm und Tradition. Welche Geschichtlichkeit für die Rechtsgeschichte? – Fra norma e tradizione. Quale storicità per la storia giuridica? Hg. von Pio Caroni und Gerhard Dilcher. Köln, Weimar und Wien 1998. S. 169–182.

[48] Historisch-kritischer Kommentar zum BGB. Hg. von Mathias Schmoeckel, Joachim Rückert und Reinhard Zimmermann. Bd. 1. Allgemeiner Teil. §§ 1–240. Redaktion: Mathias Schmoeckel. Tübingen 2003.

In der Reichspublizistik des 17. Jahrhunderts erfuhr das *ius archivi* mit dem *Tractatus de jure archivi et cancellariae* des Ahasver Fritsch[49] und der *Dissertatio de jure archivorum* des Georg Engelbrecht[50] eine monographische Behandlung.[51] Die beweisrechtliche Wirkung des *ius archivi* im passiven Sinne beschrieb Ahasver Fritsch mit den folgenden Sätzen:

„1. Scripturae ex archivo publico prolatae etiamsi non sint publicae, regulariter integram fidem faciunt […].“[52]

„2. Vis archivi etiam extra territorium se extendit; seu, scriptura ex archivo producta pro producente non solum contra subditos, sed etiam contra tertios probat […].“[53]

„3. Scripturae ex archivo prolatae nullam aliam extrinsecum probationem, vel sigilli recognitionem requirunt […].“[54]

(„1. Die Schriftstücke, die aus einem öffentlichen Archiv vorgelegt worden sind, verdienen auch dann, wenn sie nicht öffentlich sind, regelmäßig unbeschädigte Glaubwürdigkeit […].“

„2. Die Wirkung des Archivs erstreckt sich auch auf Gebiete außerhalb des Territoriums; ein Schriftstück, das aus einem Archiv vorgelegt worden ist, entfaltet seine beweisrechtliche Wirkung zugunsten des Vorlegenden nicht nur gegen Untertanen, sondern auch gegen Dritte […].“

„3. Die Schriftstücke, die aus einem Archiv vorgelegt worden sind, bedürfen keines anderen extrinsischen Beweises oder einer Anerkennung des Siegels […].“)

---

[49] Ahasver Fritsch: Tractatus de jure archivi et cancellariae. Jena 1664.

[50] Georg Engelbrecht: Dissertatio de jure archivorum. Helmstedt 1688.

[51] Lieberich, wie Anm. 45, Sp. 214.

[52] Fritsch, wie Anm. 49, S. 47.

[53] Fritsch, wie Anm. 49, S. 61.

[54] Fritsch, wie Anm. 49, S. 62.

Nicht anders beurteilte Georg Engelbrecht die beweisrechtliche Wirkung des *ius archivi* im passiven Sinne.[55]

Im Jahre 2003 hat das Bundesministerium der Justiz den Referentenentwurf eines Artikelgesetzes über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG)[56] vorgelegt. Ziel des Entwurfs ist die Führung elektronischer Prozessakten. Nach § 298a Abs. 1 ZPO-E darf ein Zivilgericht elektronische Prozessakten führen, sofern eine Rechtsverordnung diese Möglichkeit eröffnet. Außerdem bezieht § 371a ZPO-E elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen worden sind, in die Begriffe der privaten und der öffentlichen Urkunde ein.[57] Als Senatsamt hat das Staatsarchiv Hamburg mit Schreiben vom 14. August 2003 gegenüber der Justizbehörde Hamburg als Fachbehörde eine Stellungnahme zu dem Referentenentwurf, insbesondere zu § 371a ZPO-E, abgegeben. Dabei hat das Staatsarchiv vorgeschlagen, dem § 371a ZPO den folgenden Wortlaut zu geben:

> „(1) Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich aufgrund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.
> (2) Auf private elektronische Dokumente, die bis zur Konvertierung in ein anderes technisches Format und zur Übermittlung

---

[55] Engelbrecht, wie Anm. 50, Kap. 29 und 30.

[56] www.bmj.bund.de. Abruf: 14.4.2004. – Vgl. Stefanie Fischer-Dieskau: Der Referentenentwurf zum Justizkommunikationsgesetz aus Sicht des Signaturrechts. In: MultiMedia und Recht 6 (2003) S. 701–705. – Wolfram Viefhues: Referentenentwurf des Justizkommunikationsgesetzes (JKomG). Auf dem Wege zur elektronischen Gerichtsakte. In: Computer und Recht 19 (2003) S. 541–548.

[57] Vgl. bereits Schäfer, wie Anm. 4, S. 178.

an ein öffentliches Archiv mit einer qualifizierten elektronischen Signatur versehen waren, finden die Vorschriften über die Beweiskraft privater Urkunden dann entsprechende Anwendung, wenn

1. unmittelbar vor der Konvertierung und der Übermittlung eine Prüfung nach dem Signaturgesetz erfolgt ist,
2. die Ergebnisse der Prüfung und die Dokumentation der Konvertierung durch einen Beglaubigungsvermerk beglaubigt worden sind und
3. das öffentliche Archiv für die Übermittlung und die Speicherung Verfahren gewählt hat, die als geeignet anzusehen sind, um elektronische Dokumente vor Verfälschung zu bewahren.

Der Anschein der Echtheit eines elektronischen Dokuments, der sich aus der Erfüllung der in Satz 1 genannten Voraussetzungen ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass das Dokument von der als Aussteller angegebenen Person verantwortet wird.

(3) Auf elektronische Dokumente, die von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind (öffentliche elektronische Dokumente), finden die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Ist das Dokument mit einer qualifizierten elektronischen Signatur versehen, gilt § 437 entsprechend.

(4) Auf öffentliche elektronische Dokumente, die bis zur Konvertierung in ein anderes technisches Format und zur Übermittlung an ein öffentliches Archiv mit einer qualifizierten elektronischen Signatur versehen waren, finden die Vorschriften über die Beweiskraft öffentlicher Urkunden dann entsprechende Anwendung, wenn

1. unmittelbar vor der Konvertierung und der Übermittlung eine Prüfung nach dem Signaturgesetz erfolgt ist,
2. die Ergebnisse der Prüfung und die Dokumentation der Konvertierung durch einen Beglaubigungsvermerk beglaubigt worden sind und

> 3. das öffentliche Archiv für die Übermittlung und die Speicherung Verfahren gewählt hat, die als geeignet anzusehen sind, um elektronische Dokumente vor Verfälschung zu bewahren.
> Sind die in Satz 1 genannten Voraussetzungen erfüllt, gilt § 437 entsprechend."

Die Absätze 1 und 3 des Vorschlags entsprechen den Absätzen 1 und 2 des § 371a ZPO-E. Nach dem Referentenentwurf wird der bisherige § 292a ZPO aufgehoben. An dessen Stelle tritt § 371a Abs. 1 Satz 2 ZPO-E. Mit den Absätzen 2 und 4 des Vorschlags wird das *ius archivi* im passiven Sinne in die Zivilprozessordnung übernommen.

Für die Verwaltungsgerichte bietet § 55b VwGO-E eine dem § 298a ZPO-E entsprechende Regelung. Nach § 98 VwGO wäre § 371a ZPO-E vor den Verwaltungsgerichten entsprechend anzuwenden.

Nach dem Vorschlag des Staatsarchivs treten mit der Übergabe an das öffentliche Archiv Verfahren für die Übermittlung und die Speicherung, die als geeignet anzusehen sind, um elektronische Dokumente vor Verfälschung zu bewahren, an die Stelle qualifizierter elektronischer Signaturen. Für die Speicherung sei auf den im Jahre 2003 veröffentlichten Vorschlag von Frank M. Bischoff[58] verwiesen. Ob die Ergebnisse des Projekts „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente"[59] den öffentlichen Archiven andere Alternativen bieten, wird sich zeigen.

---

[58] Frank M. Bischoff: Empfehlungen für die elektronische Archivierung. Ein Normentwurf der Association Française de Normalisation. In: Virtuelle Welten im Magazin. Aussonderung, Aufbewahrung, Sicherung und Nutzung. Vorträge der 5. Tagung des Arbeitskreises Archivierung von Unterlagen aus digitalen Systemen in München, 5. und 6. März 2001. Hg. von Karl-Ernst Lupprian (Sonderveröffentlichungen der Staatlichen Archive Bayerns 2). München 2003. S. 97 f.

[59] Vgl. Ralf Brandner, Ulrich Pordesch, Alexander Roßnagel und Joachim Schachermayer: Langzeitsicherung qualifizierter elektronischer Signaturen. In: Datenschutz und Datensicherheit 26 (2002) S. 97–103. – Roßnagel/Fischer-Dieskau/Pordesch/Brandner, wie Anm. 8, S. 301–306. – Ralf Brandner und Ulrich Pordesch: Konzept zur signaturgesetzkonformen Erneuerung qualifizierter Signaturen. In: Datenschutz und Datensicherheit 27 (2003) S. 354–359.