Stefanie Fischer-Dieskau,

Elektronisch signierte Dokumente

Anforderungen und Maßnahmen für ihren dauerhaften Erhalt

aus:

Digitales Verwalten – Digitales Archivieren

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

Herausgegeben von Rainer Hering und Udo Schäfer

S. 33-50

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

Elektronisch signierte Dokumente

Anforderungen und Maßnahmen für ihren dauerhaften Erhalt[1]

Stefanie Fischer-Dieskau

1 Einleitung zum Thema

Elektronische Signaturen gelten als Schlüsseltechnologie für die Sicherung der Integrität und Authentizität elektronischer Dokumente. Mit ihrer gesetzlichen Verankerung durch das Signaturgesetz (SigG),[2] der Einführung der elektronischen Form in das Zivil-[3] und Verwaltungsrecht[4] wie auch der beweisrechtlichen Privilegierung elektronisch signierter Dokumente nach § 292a ZPO sind grundlegende rechtliche Voraussetzungen für einen rechtssicheren elektronischen Rechts- und Geschäftsverkehr geschaffen worden.

Den Blickwinkel auf die Aufbewahrung von Dokumenten gerichtet, ist der Einsatz elektronischer Signaturen jedoch nur dann ein probates Sicherungsmittel, wenn ihr Einsatz eine dauerhaft nachweisbare Bestimmung der

---

[1] Der Beitrag stellt Ergebnisse des ArchiSig-Projektes vor. Das Projekt „ArchiSig – beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“ wurde vom Bundesministerium für Wirtschaft und Arbeit gefördert. Siehe mit weiteren Literaturverweisen www.archisig.de.

[2] Signaturgesetz vom 16. Mai 2001. In: Bundesgesetzblatt 2001. Teil I. S. 876.

[3] Formvorschriftenanpassungsgesetz vom 13. Juli 2001. In: Bundesgesetzblatt 2001. Teil I. S. 1542.

[4] Drittes Verwaltungsverfahrensänderungsgesetz vom 27. August 2002. In: Bundesgesetzblatt 2002. Teil I. S. 3322.

Integrität und Authentizität des elektronisch signierten Dokuments erlaubt. Darüber hinaus darf ihr Einsatz nicht zu Einschränkungen der Lesbarkeit der Dokumente führen.[5]

2 Risiken bei der Verwendung elektronischer Signaturen

Der Faktor Zeit hat sowohl auf den Nachweis der Integrität wie auch der Authentizität elektronisch signierter Dokumente Auswirkungen. Im Laufe der Zeit kann die Sicherheitseignung der der Signatur zugrunde liegenden Algorithmen und zugehörigen Parameter nachlassen und die zur Bestimmung der Integrität und Authentizität erforderliche Signaturprüfung kann unmöglich werden. Schließlich ergeben sich mittelbar aus der Verwendung elektronischer Signaturen Gefahren für die Lesbarkeit der elektronisch signierten Dokumente.

2.1 Sicherheitseignung von Algorithmen

Elektronische Signaturen basieren auf der Verwendung unterschiedlicher mathematischer Verfahren zur Schlüsselerzeugung, Hashwertbildung und Signierung.[6] Die Sicherheit der Verfahren ergibt sich zum einen aus der bisher angenommenen, aber nicht nachgewiesenen, mathematischen Sicherheit, zum anderen aus den gewählten Längen der eingesetzten Verfahren. Steigende Rechnerkapazitäten ermöglichen zwar nicht den Bruch der angenommenen Sicherheit der verwendeten Algorithmen, schaffen jedoch

---

[5] Auf diese Schwierigkeiten wies unter anderem bereits hin: 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. 183–198.

[6] Siehe zur Funktionsweise elektronischer Signaturen Bruce Schneier: Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C. Bonn 1996. S. 185 ff. – Zur Sicherheit von Hashverfahren: Hans Dobbertin: Digitale Fingerabdrücke. In: Datenschutz und Datensicherheit 21 (1997) S. 82–87, hier S. 83. – Alexander Roßnagel und Volker Hammer. In: Recht der Multimedia-Dienste. Hg. von Alexander Roßnagel, § 14 SigG, Rdnr. 98.

die notwendige Voraussetzung, um durch systematisches Ausprobieren die Einzigartigkeit der Werte zu durchbrechen.[7] Der Verlust an Sicherheitseignung kann zur Folge haben, dass sowohl die Integrität als auch die Authentizität der signierten Dokumente nicht mehr nachgewiesen werden kann.[8]

Eine dauerhafte Sicherheitseignung kann für die mathematischen Verfahren nicht endgültig bestimmt, ihre Eignung in die Zukunft nur für einen Mindestzeitraum festgelegt werden. Zuständig für die Beurteilung der Sicherheitseignung ist nach Anlage 1 I Nr. 2 zur Signaturverordnung (SigV) die Regulierungsbehörde für Telekommunikation und Post (RegTP).[9] Unter Hinzuziehung eines Fachkreises aus Wissenschaft und Wirtschaft bestimmt sie jährlich sowie nach Bedarf die Eignung der Algorithmen und ihrer Längen für die jeweils nächsten sechs Jahre und veröffentlicht diese im Bundesanzeiger.[10] Für den dauerhaften Schutz, den eine elektronische Signatur bieten soll, ist es daher erforderlich, die Sicherheitseignung der verwendeten Verfahren zu überprüfen und im Bedarfsfall geeignete Vorkehrungen zu treffen, die dem drohenden Verlust der Nachweisbarkeit der Integrität und Authentizität der signierten Dokumente entgegenwirkt.

2.2 Prüfbarkeit von Signaturen

Die Bestimmung der Authentizität kann erst dann festgestellt werden, wenn die umfangreiche Verifikationsprüfung der Signatur zu einem positiven Ergebnis geführt hat. Dies kann nur durch die Überprüfung des der Signatur zugrunde liegenden Nutzerzertifikats und der weiteren zur Gültigkeitsprüfung dieses Zertifikats erforderlichen Informationen erfolgen. Hierzu gehören insbesondere die Zertifikatsketten bis zum Wurzelzertifikat, Gül-

---

[7] Amtliche Begründung zu § 18 SigV 1997. Zu den Angriffen durch systematisches Ausprobieren (Brute-Force-Angriffe): Dominik Gassen: Digitale Signaturen in der Praxis. Grundlagen, Sicherheitsfragen und normativer Rahmen. Köln 2003. S. 72.

[8] Alexander Roßnagel, Stefanie Fischer-Dieskau, Ulrich Pordesch und Ralf Brandner: Erneuerung elektronischer Signaturen. In: Computer und Recht 19 (2003) S. 301–306, hier S. 301.

[9] Die Zuständigkeit der RegTP folgt aus § 3 SigG in Verbindung mit § 66 TKG.

[10] Abrufbar unter www.regtp.de und weiter: elektronische Signatur/Veröffentlichungen.

tigkeitsabfragen bei Zertifizierungsdiensteanbietern und angebrachte Zeitstempel zur Ermittlung des spätesten Signaturerstellungszeitpunkts.

Die Verfügbarkeit dieser Verifikationsdaten ist jedoch nicht dauerhaft gewährleistet. Anbieter von fortgeschrittenen Signaturen sind nicht verpflichtet, Verzeichnis- und Sperrdienste oder eine Dokumentation ihrer Tätigkeit zu führen.[11] Bei ihnen kann sich eine dauerhafte Verfügbarkeit lediglich aus einer Vereinbarung mit ihren Vertragspartnern oder einer Selbstverpflichtung ergeben. Demgegenüber sind qualifizierte und akkreditierte Zertifizierungsdiensteanbieter gesetzlich verpflichtet, einen Verzeichnisdienst für Zertifikate, aus dem auch die frühzeitige Sperrung eines Zertifikats entnommen werden kann, nach § 5 Abs. 1 SigG zu führen. Darüber hinaus müssen sie eine Dokumentation über ihr Sicherheitskonzept und die Ausstellung und Sperrung von Zertifikaten entsprechend den Vorgaben nach § 10 SigG und § 8 SigV erstellen.

Nach §§ 4 Abs. 1, 5 Abs. 2 SigV sind qualifizierte Zertifizierungsdiensteanbieter verpflichtet, die von ihnen ausgestellten Zertifikate für eine Dauer von mindestens fünf Jahren nach Ablauf des Jahres ihrer Gültigkeit im Verzeichnis nachprüfbar zu halten. Auch die Dokumentation ist gemäß §§ 8 Abs. 3, 4 Abs. 1 SigV für denselben Zeitraum vom Zertifizierungsdiensteanbieter aufzubewahren. Für akkreditierte Zertifizierungsdiensteanbieter gilt für die Dokumentation ein Aufbewahrungszeitraum von mindestens 30 Jahren (§§ 8 Abs. 3, 4 Abs. 2 SigV). Zertifikate sind mindestens 30 Jahre nach Ablauf des Jahres der Gültigkeit eines Zertifikats im Verzeichnisdienst nachprüfbar zu halten (§§ 8 Abs. 3, 4 Abs. 2 SigV).

Eine Sicherheit, dass diese Daten für den vorgesehenen Zeitraum auch tatsächlich zur Verfügung stehen, besteht bei der Verwendung qualifizierter Signaturen jedoch nicht.[12] Im Konkursfall oder im Fall ihrer Geschäftsaufgabe haben die Zertifizierungsdiensteanbieter zwar dafür Sorge zu tragen, dass die bei Einstellung der Tätigkeit gültigen qualifizierten Zertifikate nach § 13 Abs. 1 SigG von einem anderen Zertifizierungsdiensteanbieter

---

[11] Hierzu und allgemein zur fortgeschrittenen Signatur Alexander Roßnagel: Die fortgeschrittene elektronische Signatur. In: MultiMedia und Recht 6 (2003) S. 164–170, hier S. 164.

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

übernommen werden, allerdings besteht für keine Instanz eine Verpflichtung, die Daten und Verzeichnisdienste zu übernehmen und vorzuhalten. Übernimmt sie keiner, hat der Zertifizierungsdiensteanbieter die Zertifikate zu sperren und die RegTP hat nach § 10 Abs. 2 Satz 2 SigG die Dokumentation zu übernehmen. Nur bei Vorlage eines berechtigten Interesses erteilt die RegTP Auskunft zur Dokumentation, wenn ihr dies technisch ohne unverhältnismäßig großen Aufwand möglich ist. Ein Fortführen des Verzeichnisdienstes erfolgt in diesen Fällen nicht. Dies ist lediglich bei akkreditierten Zertifizierungsdiensteanbietern sichergestellt. Hier übernimmt die RegTP, wenn sich kein anderer akkreditierter Zertifizierungsdiensteanbieter findet, nach §§ 15 Abs. 6, 10 Abs. 1 SigG das Führen und Vorhalten der Verzeichnisdienste und die Aufbewahrung der Dokumentation für den noch verbleibenden Zeitraum bis zur Erfüllung der 30 Jahre.

2.3 Lesbarkeit der elektronisch signierten Dokumente

Ermöglicht der Einsatz elektronischer Signaturen bei Erfüllung geeigneter Maßnahmen zwar einen dauerhaften Integritäts- und Authentizitätsschutz der Dokumente, so stellt die rasche technologische Entwicklung der Systeme und ihrer dazugehörigen Komponenten wie aber auch der Datenformate die Gestaltung an eine elektronische Aufbewahrung vor eine weitere Herausforderung. Solche Hard- und Softwarewechsel können dazu führen, dass die Lesbarkeit der elektronischen Dokumente nicht mehr sichergestellt ist. Dieses Problem kann auch nur bedingt dadurch gelöst werden, dass von vornherein stabile und standardisierte Formate sowohl für die Dokumenten- wie auch Signaturerstellung verwendet werden.

Dieses nicht im unmittelbaren Zusammenhang mit der Verwendung elektronischer Signaturen stehende Problem erlangt dadurch seine Relevanz, dass eine Migration der Daten in ein aktuelleres Format ohne weitergehende Maßnahmen nicht möglich ist. Im Falle der Migration verliert die Signa-

tur nämlich ihre Funktion als Sicherungsmittel,[13] Integrität und Authentizität des ursprünglichen Dokuments lassen sich nicht mehr feststellen.

3 Lösungskonzepte

Elektronische Signaturen sind daher nur dann als geeignetes Sicherungsmittel für elektronische Dokumente anzusehen, wenn den aufgeführten Risiken Lösungen entgegengesetzt werden können, die ihre Verwirklichung verhindern.

3.1 Sicherstellung der Integrität

3.1.1 Neusignierung nach § 17 SigV

Als geeignete Vorkehrung, dem Verlust der Sicherheitseignung der eingesetzten Algorithmen und zugehörigen Parametern – und dadurch der damit erzeugten elektronischen Signaturen – infolge neuer wissenschaftlicher Erkenntnisse oder des technischen Fortschritts entgegenzuwirken,[14] sieht das Signaturrecht in § 17 SigV ein gesetzlich normiertes Verfahren zur erneuten Signatur vor. Nach § 17 Satz 2 SigV sind in diesem Falle die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen und der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Satz 3 verlangt darüber hinaus, dass diese erneute Signatur mit geeigneten neuen Algorithmen und zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen muss.

---

[13] Bundestags-Drucksache 14/9000. S. 32, spricht insoweit sehr plastisch von der Zerstörung der Signatur, was allerdings der Sache nicht ganz gerecht wird, da die Signatur als solche erhalten bleibt.

[14] Amtliche Begründung zu § 17 SigV.

3.1.1.1 Rechtliche Qualifizierung der Neusignierung

Die erneute Signatur zur langfristigen Datensicherung, die keine entsprechende Grundlage in der europäischen Richtlinie zur elektronischen Signatur[15] findet, soll als Sicherungsmittel dazu dienen, die rein technisch bedingten Sicherheitsverluste der ursprünglich verwendeten Algorithmen und zugehörigen Parameter aufzufangen und den bestehenden Sicherungsschutz und somit auch den ursprünglichen Beweiswert des elektronisch signierten Dokumentes erhalten. Sie stellt somit keine Willens- oder Wissenserklärung dar,[16] die eine vorherige Überprüfung der erneut zu signierenden Signatur erfordert. Es ist daher unbeachtlich, wer die erneute Signatur vornimmt. Sie kann zum Beispiel durch einen Archivar erfolgen[17] und auch im automatisierten Verfahren[18] erstellt werden.

3.1.1.2 Gestaltung und Umfang der Neusignierung

Die erneute Signatur ist rechtzeitig vor Ablauf der Sicherheitseignung der ursprünglich verwendeten Algorithmen und zugehörigen Parameter vorzunehmen.[19] Damit die Neusignierung nachweislich vor Ablauf der Sicherheitseignung der verwendeten Algorithmen und zugehörigen Parameter

---

[15] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vom 13. Dezember 1999. In: Amtsblatt der Europäischen Gemeinschaften 2000. L 13. S. 12.

[16] Roßnagel/Fischer-Dieskau/Pordesch/Brandner, wie Anm. 8, S. 301.

[17] Amtliche Begründung zu § 18 SigV 1997.

[18] Zur Zulässigkeit der automatisiert erstellten Signatur Alexander Roßnagel und Stefanie Fischer-Dieskau: Automatisiert erzeugte elektronische Signaturen. In: MultiMedia und Recht 7 (2004) S. 133–139, hier S. 133.

[19] In diesem Zusammenhang bringt das Fehlen einer verbindlichen elektronischen Fassung der Bestimmung geeigneter Algorithmen neben dem entstehenden Aufwand der regelmäßigen Durchsicht des Bundesanzeigers den Nachteil mit sich, dass eine Neusignierung nur bedingt rein automatisiert angestoßen werden kann. Siehe dazu Christian Frye und Ulrich Pordesch: Sicherheitseignung von Algorithmen von qualifizierten Signaturen. In: Datenschutz und Datensicherheit 27 (2003) S. 73–78, hier S. 73.

erfolgt, verlangt das Gesetz die Verwendung eines qualifizierten Zeitstempels. Dieser ist entsprechend der Legaldefinition in § 2 Nr. 14 SigG eine elektronische Bescheinigung eines qualifizierten Zertifizierungsdiensteanbieters darüber, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben, so dass dadurch eine Missbrauchsmöglichkeit durch Rückdatierung der erneuten Signatur auf einen Zeitpunkt, zu dem der Sicherheitswert der früheren digitalen Signatur möglicherweise bereits so gering geworden ist, dass Fälschungen möglich sind, ausgeschlossen wird.[20]

Dem Gesetzeswortlaut folgend sind die Daten erneut zu signieren und mit einem Zeitstempel zu versehen, ohne danach zu differenzieren, welcher Algorithmus seine Sicherheitseignung zu verlieren droht. Ein Zugriff auf die ursprünglich signierten Dokumente ist jedoch aus sicherheitstechnischer Sicht nur dann sinnvoll und erforderlich, wenn der verwendete Hash-Algorithmus unsicher wird und somit der Hashwert nicht mehr als kollisionsresistent bewertet werden kann. Ist demgegenüber lediglich der verwendete Verschlüsselungsalgorithmus, mit dem der Hashwert signiert worden ist, in seiner Sicherheit bedroht, so repräsentiert der Hashwert weiterhin die zu signierenden Daten.[21] Ein erneutes Hashen der Daten würde den gleichen Hashwert ergeben und ist somit überflüssig, da es in Bezug auf das verfolgte Sicherheitsziel keinen Mehrwert bringt. In diesem Fall ist es daher aus sicherheitstechnischen Überlegungen heraus ausreichend, die Signaturen beziehungsweise erneuten Signaturen des elektronischen Dokumentes zu signieren, um das Ziel der Regelung, nämlich die dauerhafte Datensicherung, zu erreichen.[22] Solange der drohende Sicherheitsverlust nur auf den Verschlüsselungsverfahren basiert, ist das vom Wortlaut des Gesetzestextes verlangte Signieren der Daten zu weit gefasst und insoweit auf den ihm nach dem Regelungszweck des Gesetzes zukommenden Anwendungsbe-

---

[20] Amtliche Begründung zu § 17 SigV.

[21] Ralf Brandner, Ulrich Pordesch, Alexander Roßnagel und Joachim Schachermayer: Langzeitsicherung qualifizierter elektronischer Signaturen. In: Datenschutz und Datensicherheit 26 (2002) S. 97–103.

[22] Roßnagel/Fischer-Dieskau/Pordesch/Brandner, wie Anm. 8, S. 301.

reich zu reduzieren.[23] Der Wortlaut des § 17 SigV ist dementsprechend im Wege der teleologischen Reduktion auszulegen und ein erneuter Zugriff auf die elektronischen Dokumente nur dann erforderlich, wenn ihre Hashwerte unsicher werden.

Eine weitere teleologische Reduktion des Gesetzeswortlauts ist in den Fällen vorzunehmen, in denen Zeitstempel verwendet werden, die eine mindestens qualifizierte elektronische Signatur beinhalten.[24] Vom Wortlaut her verlangt § 17 SigV zwar, dass die Daten mit einer neuen qualifizierten elektronischen Signatur zu versehen sind und diese erneute Signatur einen qualifizierten Zeitstempel tragen muss. Würde nunmehr jedoch verlangt, dass die mit einem, eine qualifizierte Signatur enthaltenden, qualifizierten Zeitstempel versehenen Daten zusätzlich mit einer qualifizierten Signatur abgesichert werden sollen, so würde diese zweite Signatur keinen zusätzlichen Sicherheitswert erbringen, sondern lediglich ein gerade neu abgesichertes Ergebnis noch einmal mit demselben Sicherungsmittel sichern.[25] Für eine erneute qualifizierte elektronische Signatur im Sinne des § 17 S. 3 SigV genügt es daher, wenn die elektronisch signierten Dokumente mit einem qualifizierten Zeitstempel versehen werden, der eine qualifizierte Signatur enthält.

Erneut signiert werden müssen die Daten, und die früheren Signaturen sind mit einzuschließen. Es muss sich nicht um die Daten eines Dokumentes beziehungsweise um jede einzelne Signatur handeln. Schon der ver-

---

[23] Karl Larenz und Claus-Wilhelm Canaris: Methodenlehre der Rechtswissenschaft. Studienausgabe. Berlin [3]1995. S. 210 ff.

[24] A. A. Ralf Schneider: Neusignatur – Anforderungen und Praxis. In: Datenschutz und Datensicherheit 27 (2003) S. 91–94, hier S. 91, 93, und Jan Skrobotz. In: Telekommunikations- und Multimediarecht. Hg. von Gerrit Manssen, § 17 SigV, Rdnr. 23, die eine solche teleologische Reduktion unter Verweis auf den Wortlaut für nicht zulässig halten.

[25] So auch Ralf Schneider: Erhalt der Beweiskraft elektronischer Signaturen durch Neusignatur. In: D. A. CH Security. Bestandsaufnahme. Konzepte. Anwendungen. Perspektiven. Hg. von Patrick Horster (IT Security & IT-Management). 2003. S. 285–292, hier S. 285, 289, der allerdings verkennt, dass ein Zeitstempel nicht gesetzlich zwingend eine qualifizierte Signatur beinhalten muss.

wendete Plural spricht dafür, beliebig viele signierte Dokumente und Signaturen in eine erneute Signatur einbeziehen zu können. Auch die Begründung zu § 18 SigV 1997 erläutert, dass „für eine beliebige Anzahl signierter Daten eine (übergreifende) neue digitale Signatur […] angebracht werden kann“.[26] Die Verpflichtung zur Einbeziehung aller früheren Signaturen bezieht etwaige Parallelsignaturen zu einem Dokument mit ein.[27] Als reines Sicherungsmittel kann die erneute Signatur ihre Wirkung unabhängig von der Anzahl der zu erneuernden Signaturen entfalten, solange alle früheren Signaturen mit eingeschlossen und damit „konserviert“ werden.[28] Die Prüfung erfolgt dann entsprechend geschachtelt.[29] Zu beachten ist in diesem Zusammenhang, dass die erneute Signatur mindestens die gleiche Qualitätsstufe haben muss wie die Signaturen, die es abzusichern gilt.

3.1.2 Konsequenzen für die praktische Umsetzung

§ 17 SigV bietet ausreichend Interpretations- und Gestaltungsspielraum, um eine signaturgesetzkonforme Neusignierung verhältnismäßig kostengünstig und effizient einzusetzen. Ein Zugriff auf die Dokumente ist nur in den Fällen erforderlich, in denen der Hash-Algorithmus seine Sicherheitseignung zu verlieren droht und die Dokumente neu gehasht werden müssen. Dies wiederum ermöglicht eine getrennte Aufbewahrung der Signaturen vom signierten Dokument selbst und schafft die Möglichkeit, die Neusignierung zu zentralisieren und sogar an Dritte auszulagern. Durch die Mög-

---

[26] So auch Martin Eifert, Jan-Ole Püschel und Claudia Stapel-Schulz. In: Rechtskonformes E-Government. Antworten auf Kernfragen beim Bau eines virtuellen Rathauses. Hg. von Bundesministerium für Wirtschaft und Arbeit und Hans-Bredow-Institut. Stand: Februar 2003. S. 83.

[27] Dieses Vorgehen führt zu einer Beweiswerterhöhung des ursprünglich signierten Dokumentes. Sobald eine erneute, übergreifende Signatur erstellt worden ist, kann eine einzelne Signatur nicht mehr unerkennbar gelöscht und somit die Vollständigkeit des elektronisch signierten Dokumentes sichergestellt werden.

[28] Amtliche Begründung zu § 17 SigV.

[29] Siehe Alexander Roßnagel/Volker Hammer in: Recht der Multimedia-Dienste, wie Anm. 6, § 18 SigV, Rdnr. 34.

lichkeit, viele Signaturen gemeinsam erneut zu signieren, kann die Zahl der erforderlichen Zeitstempel und somit auch die Höhe der Kosten reduziert werden. Eine durchgängige Signaturprüfung jeder einzelnen Signatur wird in diesen Fällen durch die Bildung von Hashwertbäumen gewährleistet,[30] selbst wenn einzelne Dokumente und Signaturen gelöscht oder gesperrt werden. Das nur begrenzte Erfordernis des Zugriffs auf die Dokumente und somit auf personenbezogene Daten wird den Anforderungen des Daten- und Geheimnisschutzes besonders gerecht.

3.2 Sicherstellung der Authentizität

Dient die Neusignierung der rein mathematischen Sicherheit der elektronisch signierten Dokumente, so lässt sich daraus nicht seine Authentizität feststellen. Darauf kann erst dann geschlossen werden, wenn die umfangreiche Signaturprüfung der (gegebenenfalls unter Einschluss der erneuten) Signaturen zu einem positiven Ergebnis geführt hat. Aufgrund der nicht dauerhaft bestehenden Möglichkeit, auf Zertifikatsverzeichnisse und Dokumentationen des Zertifizierungsdiensteanbieters zugreifen zu können, bedarf es eines Konzepts zur rechtzeitigen Sicherung der erforderlichen Verifikationsdaten zur Prüfung einer Signatur. Vor ihrem Verlust müssen sie beschafft und der Signatur beigefügt werden.

3.2.1 Rechtliche Grundlagen der Authentizitätssicherung

Vorgaben zur Authentizitätssicherung sind gesetzlich nur teilweise geregelt. Neben der Neusignierung nach § 17 SigV ergeben sich lediglich Anhaltspunkte aus Anforderungen an die Signaturprüfung. Da die Sicherstellung der Signaturprüfung als Teil der allgemeinen Beweissicherungspflichten, -obliegenheiten oder -interessen zu verstehen ist, können die Vorgaben zur Authentizitätssicherung entsprechend den Anforderungen an die Bestimmung der Beweiskraft elektronisch signierter Dokumente entwickelt werden. Ausgangspunkt für die Bestimmung des Umfangs ist daher die für

[30] Ralf Brandner und Ulrich Pordesch: Konzept zur signaturgesetzkonformen Erneuerung qualifizierter Signaturen. In: Datenschutz und Datensicherheit 27 (2003) S. 354–359, hier S. 354.

den Anscheinsbeweis bei qualifizierten elektronischen Signaturen erforderliche Signaturprüfung.

3.2.2 Die Signaturprüfung nach § 292a ZPO

Die Geltendmachung des Anscheinsbeweises setzt voraus, dass eine Erklärung in elektronischer Form entsprechend § 126a BGB vorliegt, dass mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 2 und 3 SigG signiert wurde.[31] Gemäß § 2 Nr. 2a SigG muss die Signatur ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sein. Daneben muss sie entsprechend § 2 Nr. 2 b-d SigG eine Identifizierung des Signaturschlüssel-Inhabers ermöglichen, mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und mit den Daten, auf die sie sich beziehen, so verknüpft sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Darüber hinaus muss sie auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen (§ 2 Nr. 3a SigG) und mit einer sicheren Signaturerstellungseinheit erzeugt worden sein (§ 2 Nr. 3b SigG).

Für die Prüfung sind dabei entsprechend den Voraussetzungen einer qualifizierten elektronischen Signatur folgende Verifikationsdaten erforderlich:

- das qualifizierte Zertifikat des Signaturschlüssel-Inhabers und die dazugehörige Zertifikatskette bis zur Wurzelinstanz;[32] die Zertifikatskette bis zum Wurzelzertifikat ist für die Ermittlung der Vertrauenswürdigkeit des Zertifikats erforderlich;
- ein Nachweis über die Gültigkeit des Zertifikats des Signaturschlüssel-Inhabers zum Zeitpunkt der Signaturerstellung, zum Beispiel eine

---

[31] Siehe hierzu Stefanie Fischer-Dieskau, Rotraud Gitter, Sandra Paul und Roland Steidle: Elektronisch signierte Dokumente als Beweismittel im Zivilprozess. In: MultiMedia und Recht 5 (2002) S. 709–713, hier S. 709.

[32] Entsprechend § 7 Abs. 1 SigG muss das Zertifikat des Signaturschlüssel-Inhabers eine qualifizierte Signatur des Zertifizierungsdiensteanbieters tragen; mangels Vorliegen einer solchen bei qualifizierten Zertifizierungsdiensteanbietern genügt bei diesen eine fortgeschrittene Signatur; siehe zu dieser Problematik: Johann Bizer: Das Wurzelzertifikat des Zertifizierungsdiensteanbieters. In: Datenschutz und Datensicherheit 26 (2002) S. 107.

OCSP-Response, und die dazugehörige Zertifikatskette bis zur Wurzelinstanz;

– ein Nachweis der Verwendung geeigneter Algorithmen;

– ein Nachweis, dass der das Zertifikat ausstellende Zertifizierungsdiensteanbieter mindestens qualifizierte Zertifikate ausstellen darf, da er die technisch-organisatorischen Anforderungen des SigG erfüllt.

Hinsichtlich des Nachweises, dass es sich um ein qualifiziertes Zertifikat handelt, kommt dem Beweisführer bei einer akkreditierten Signatur die Sicherheitsvermutung nach § 15 Abs. 1 S. 4 SigG für Zertifizierungsdiensteanbieter mit Anbieter-Akkreditierung zu Gute. Darüber hinaus kann der Beweisführer die Vertrauenswürdigkeit des Zertifizierungsdiensteanbieters durch das Zertifikat der RegTP als Wurzelzertifikat akkreditierter Signaturen nachweisen. Die Gültigkeit und Echtheit dieses Zertifikats lässt sich dauerhaft nachweisen, da die RegTP als öffentliche Behörde eine Verpflichtung hat, diese auf unbegrenzte Dauer aufzubewahren.[33]

Bedarf es bei der Neusignierung eines qualifizierten Zeitstempels, um eindeutig nachweisen zu können, dass diese vor Ablauf der Sicherheitseignung der verwendeten Algorithmen und zugehörigen Parameter erfolgt ist, so erfordert die Überprüfung einer Signatur einen ebenso vertrauenswürdigen Referenzzeitpunkt, zu dem die Signatur auf ihre Gültigkeit hin verifiziert werden kann. Maßgeblich ist dabei der Signaturerstellungszeitpunkt, der sich zwar grundsätzlich aus der Signatur selbst ergibt. Da Änderungen an der Systemzeit des Rechners möglich sind, sollte ein vertrauenswürdiger Referenzzeitpunkt geschafft und daher ein qualifizierter Zeitstempel eingeholt werden. Als weiteres Verifikationsdatum erforderlich ist daher

– ein mindestens qualifizierter Zeitstempel für die Signatur und die dazugehörige Zertifikatskette bis zur Wurzelinstanz.

Diese Verifikationsdaten betreffen die Authentizitätsprüfung der Signatur des Signaturschlüssel-Inhabers. Auch die Zertifikate der Zertifizierungs-

[33] Eine Verpflichtung zur Veröffentlichung im Bundesanzeiger, wie in § 8 Abs. 2 SigV 1997 vorgesehen, besteht nicht mehr. Aus allgemeinem Interesse wird die RegTP dieses jedoch weiterhin vornehmen.

diensteanbieter könnten wiederum auf ihre Gültigkeit hin überprüft werden. Es wird allerdings vermutet, dass die oben genannten Daten zumindest für die Echtheits- und Gültigkeitsprüfung akkreditierter Signaturen ausreichend sind.

3.2.3 Konsequenz für die praktische Umsetzung

Die vorstehenden Ausführungen zeigen, dass die dauerhafte Überprüfbarkeit elektronischer Signaturen und damit der Nachweis der Authentizität bei der Verwendung qualifizierter Signaturen Schwierigkeiten bereiten können. Diese resultieren zum einen aus der nur bedingten Vertrauenswürdigkeit qualifizierter Zertifizierungsdiensteanbieter, die zumindest so lange besteht, wie sich die behauptete Vertrauenswürdigkeit nicht tatsächlich bestätigt hat; zum anderen begründen die nur verhältnismäßig kurze Aufbewahrungsdauer der Zertifikate und Dokumentationen sowie ihre fehlende Konkurs- und Geschäftsaufgaberesistenz die Schwäche qualifizierter Signaturen. Grundsätzlich ist daher aus Sicht einer dauerhaft gesicherten Aufbewahrung der Einsatz akkreditierter Signaturen zu empfehlen. Darüber hinaus sollten frühzeitig alle zur Verfügung stehenden Verifikationsdaten eingeholt und der Signatur beigefügt oder gesondert aufbewahrt werden.

Diese Daten, die selbst alle elektronisch signiert sind, sind als erforderlicher Bestandteil zur Nachweisführung der Gültigkeitsüberprüfung einer Signatur genauso dauerhaft zu pflegen wie die elektronische Signatur selbst. Werden diese Maßnahmen nicht getroffen, so besteht die Gefahr, die Integrität und Authentizität der Dokumente nicht nachweisen zu können.

3.3 Sicherstellung der Lesbarkeit

Zur Lösung der Risiken, die aus dem drohenden Verlust der Lesbarkeit elektronisch signierter Dokumente folgen, stehen unterschiedliche Konzepte zur Diskussion.[34] Die Einrichtung eines Technikmuseums, in dem die an sich veraltete, für die Sicherstellung der Lesbarkeit der Daten jedoch erfor-

[34] Frank M. Bischoff: Archivierung digitaler Unterlagen – Neue Anforderungen an die Archive. In: Archiv und Wirtschaft 34 (2001) S. 13–25, hier S. 13. – Christian Keitel: Die Archivierung elektronischer Unterlagen in der baden-württembergischen Archivverwaltung. Eine Konzeption, 12.6.2002 (www.lad-bw.de/lad/konzeption.pdf).

derliche Hard- und Software vorgehalten wird, kann ausschließlich für kurz- oder mittelfristige Aufbewahrungsvorhaben als Lösung herangezogen werden. Ein weiterer Ansatz wird in der Emulation gesehen.[35] Dabei wird auf zukünftigen Systemen das Verhalten alter Betriebssysteme imitiert mit dem Ergebnis, dass sich eine gegenwärtig dem Stand der Technik entsprechende Systemumgebung so verhält wie die ursprünglich verwendete. Der große Vorteil dieser Lösung besteht, wie auch bei dem Vorhalten eines Hard- und Softwaremuseums, darin, dass die Daten in ihrem *Originalzustand* gelesen werden können. Die Emulation ist bisher jedoch lediglich ein theoretisches Konzept, dass sich noch nicht in der Praxis bewährt hat.[36]

Momentan wird die Lösung des Problems der Gewährleistung der Lesbarkeit in der Migration der Daten in ein anderes Format gesehen. Wird unter Migration grundsätzlich die Übertragung eines in einem bestimmten Format vorhandenen Dokuments in ein neues Standardformat verstanden, so unterscheidet sich die vorliegende Problematik dadurch, dass das Ziel- oder das Quelldokument (oder beide Dokumente) mit einer elektronischen Signatur versehen sind. Zur Differenzierung wird daher im Folgenden von Transformation gesprochen.

3.3.1 Transformation

Der Gesetzgeber hat durch die Erweiterung der Regelungen zur Beglaubigung nach § 33 Abs. 4 und 5 VwVfG einen Weg aufgezeigt, um dem drohenden Verlust der Lesbarkeit durch eine Transformation entgegenzuwirken und den rechtlichen Wert des signierten Dokuments zu erhalten.[37] § 33 Abs. 5 Nr. 2 S. 2 VwVfG sieht im Falle der Transformation eines qualifiziert signierten elektronischen Dokumentes in ein neues Format vor, dass

---

[35] Frank M. Bischoff: Emulation – das Archivierungskonzept der Zukunft? In: Digitale Herausforderungen für Archive. 3. Tagung des Arbeitskreises Archivierung von Unterlagen aus digitalen Systemen am 22. und 23. März 1999 im Bundesarchiv in Koblenz. Hg. von Michael Wettengel (Materialien aus dem Bundesarchiv 7). Koblenz 1999. S. 15–23, hier S. 15.

[36] Bischoff, wie Anm. 34, S. 13, 20.

[37] Bundestags-Drucksache 14/9000. S. 32.

ein Beglaubigungsvermerk zu erstellen ist, der die Feststellungen enthalten muss,

a. wen die Signaturprüfung als Inhaber der Signatur ausweist,

b. welchen Zeitpunkt die Signaturprüfung für die Anbringung der Signatur nennt und

c. welche Zertifikate mit welchen Daten dieser Signatur zugrunde lagen.[38]

Dieser Beglaubigungsvermerk muss den Namen des zuständigen Bediensteten und der vornehmenden Behörde benennen und mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur versehen werden. Begründet werden diese Anforderungen damit, dass anhand dieser Angaben die Geltung des Signaturschlüssels überprüft werden könne.[39]

Der vom Gesetzgeber verfolgte Ansatz zur Transformation lässt jedoch noch eine Reihe von Fragen offen. Zum einen baut die Beglaubigung in ihrer derzeitigen Form auf einem von einem Menschen ausgestellten Beglaubigungsvermerk auf, der die Feststellung der Übereinstimmung der beiden Dokumente trifft. Eine automatisierte Bestätigung, die jedoch aufgrund der großen Anzahl der zu transformierenden Dokumente erforderlich wäre, ist nach derzeitiger Gesetzeslage unzulässig. Ungeklärt bleibt auch, inwieweit bei der Feststellung der Übereinstimmung der Dokumente die sich aus der Präsentationsproblematik ergebenden Schwierigkeiten der Bestimmung des eindeutigen Inhalts Berücksichtigung finden müssen.[40]

---

[38] Der nunmehr als Referentenentwurf vorliegende Entwurf eines Gesetzes über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG) sieht zwar auch Regelungen zur Transformation vor, beschränkt sich dabei jedoch auf die Beglaubigung aufgrund eines Medienwechsels (Ausdruck eines elektronischen Dokumentes beziehungsweise Scannen eines Schriftstücks). In beiden Fällen ist das Dokument in seiner ursprünglichen Fassung bis zum rechtskräftigen Abschluss des Verfahrens aufzubewahren. Eine Transformation aufgrund eines erforderlichen Formatwechsels ist derzeit nicht vorgesehen.

[39] Bundestags-Drucksache 14/9000. S. 33.

[40] Umfassend zur Präsentationsproblematik Ulrich Pordesch: Die elektronische Form und das Präsentationsproblem. Baden-Baden 2002.

Schließlich sind auch die im Beglaubigungsvermerk aufzunehmenden Angaben nicht ausreichend, um die Geltung des Signaturschlüssels überprüfen zu können.[41]

Es fehlen Angaben zu den verwendeten Algorithmen und zugehörigen Parametern, so dass nicht nachvollzogen werden kann, ob die ursprüngliche Signatur ihren Integritätsschutz zum Zeitpunkt der Transformation noch gewährleisten konnte. Die Angabe, *welche Zertifikate mit welchen Angaben* der Signatur zugrunde lagen, ist zu unbestimmt. Es bleibt unklar, inwieweit die Zertifikate bis zu ihrem Wurzelzertifikat geprüft worden sind und inwieweit diese zum Zeitpunkt ihrer Signaturerstellung gültig waren. Darüber hinaus fehlen Angaben, ob es sich bei dem Signaturerstellungszeitpunkt um eine verlässliche Zeitangabe aufgrund der Verwendung eines Zeitstempels oder um die angegebene Systemzeit handelt. Allein aus dem Zeitpunkt der Signaturerstellung und den Angaben zum zugrunde liegenden Zertifikat als Bestandteil des Beglaubigungsvermerks lässt sich nicht die Gültigkeit einer Signatur bestimmen, da das Zertifikat bereits gesperrt gewesen sein könnte.

Schließlich schlägt sich bei der Bestimmung der erforderlichen Prüfdaten für den Beglaubigungsvermerk ein ganz generelles Problem bei der Bestimmung der Gültigkeit von Signaturen nieder. Die Einbeziehung des Zertifikats, das der Signatur zugrunde liegt, muss nicht von Gesetzes wegen in die Signatur einbezogen werden. Dieses Fehlen ermöglicht den unerkannten Austausch von Zertifikaten, die auf den gleichen öffentlichen Schlüssel ausgestellt sind.[42] Solange die Einbeziehung nicht zwingend für die Wirksamkeit einer Signatur ist, sollte die beglaubigende Stelle zumin-

---

[41] Siehe Stefanie Fischer-Dieskau: Der Referentenentwurf zum Justizkommunikationsgesetz aus Sicht des Signaturrechts. In: MultiMedia und Recht 6 (2003) S. 701–705.

[42] Gesellschaft für Informatik: Stellungnahme zum Gesetzentwurf „Formvorschriften des Privatrechts“. In: Datenschutz und Datensicherheit 25 (2001) S. 38–40, hier S. 38. – Alexander Roßnagel: Das neue Recht elektronischer Signaturen. Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO. In: Neue Juristische Wochenschrift 54 (2001) S. 1817–1826, hier S. 1825. – Stefanie Fischer-Dieskau, Rotraud Gitter und Gerrit Hornung: Die Beschränkung des qualifizierten Zertifikats. In: MultiMedia und Recht 6 (2003) S. 384–389, hier S. 384.

dest in den Beglaubigungsvermerk aufnehmen, ob das Zertifikat integraler Bestandteil der Signatur war oder nicht.

3.3.2 Konsequenz

Die Gewährleistung der dauerhaften Lesbarkeit stellt derzeit sicherlich die größte Herausforderung bei den Fragen der elektronischen Aufbewahrung dar, da das eigentliche Sicherungsmittel bei Umsetzung der Transformationslösung seine Funktion verliert. Da die Beglaubigung momentan an die Person des Beglaubigers gebunden ist, kann sie nicht in einem rein automatisierten Prozess erfolgen. Dies zu ermöglichen muss jedoch das Ziel sein, wenn die Transformation von elektronisch signierten Dokumenten ein geeigneter Weg zur Sicherstellung ihrer Lesbarkeit sein soll. Hierzu besteht jedoch noch weiterer Forschungsbedarf.

4 Fazit

Die Aufbewahrung elektronisch signierter Dokumente stellt eine komplexe Aufgabe dar. Die Probleme, die sich bei der Aufbewahrung elektronisch signierter Dokumente stellen, sind mittlerweile bekannt und teilweise auch bereits konzeptionell und prototypisch gelöst.[43] Die Neusignierung wie auch die Verifikationsdatenbeschaffung zur Sicherstellung der Überprüfung elektronischer Signaturen lassen sich in automatisierten Prozessen durchführen und bilden – sobald als marktreifes Produkt entwickelt – ein weiteres Modul beziehungsweise weitere Komponenten für Aufbewahrungssysteme.[44] Zur Ermöglichung der Transformation von elektronisch signierten Dokumenten befindet sich die Wissenschaft noch in den Anfängen. Es ist zu hoffen, dass auch dieses Problem in den nächsten Jahren zu einer Lösung geführt wird.

---

[43] Insoweit sei insbesondere auf die Ergebnisse des Forschungsprojektes ArchiSig – beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente verwiesen (www.archisig.de).

[44] Michael Wettengel: Digitale Unterschriften. In: Der Archivar 50 (1997) Sp. 89–94, hier Sp. 89 (92), spricht hierbei von einem erforderlichen Signaturmanagement. Durch Einsatz automatisierter Prozesse relativiert sich jedoch der Aufwand.