Signaturgesetzkonformität des Standardisierungsvorschlags „Long-Term Conservation of Electronic Signatures“ für die ISIS-MTT Spezifikation vom 30.6.2004

Rechtsgutachten

für die Fraunhofer-Gesellschaft
Institut für Sichere Telekooperation

von

Prof. Dr. Alexander Roßnagel, Kassel

Kassel, den 20. Juli 2004

1. Sachverhalt

Die Fraunhofer-Gesellschaft betreibt im Zusammenhang mit dem Forschungsprojekt „Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente (Archi-Sig)“ mit Unterstützung durch das Bundesministerium für Wirtschaft und Arbeit eine Standardisierungsinitiative. In dieser soll ein Vorschlag für einen Anhang zur ISIS-MTT Spezifikation entwickelt werden, der ein Konzept zur Langzeitsicherung qualifizierter elektronischer Signaturen spezifiziert, das dem Signaturgesetz und der Signaturverordnung entspricht.

Der Entwurf einer solchen Spezifikation wurde zum 30.6.2004 vorgelegt. Das vorliegende Gutachten betrifft die Frage, ob dieser Entwurf den Vorgaben des deutschen Rechts insbesondere dem Signaturgesetz und der Signaturverordnung, aber auch dem Datenschutzrecht entspricht.

Hierfür werden im folgenden Kapitel die Vorgaben des deutschen Rechts erläutert, danach werden die wenigen – nur formalen – Vorgaben des europäischen Rechts dargestellt und sodann die Einhaltung dieser Vorgaben durch den Entwurf des genannten Standards überprüft. Abschließend werden die gefundenen Ergebnisse kurz zusammengefasst.

2. Vorgaben des deutschen Rechts

Das deutsche Recht enthält zum einen Vorgaben für das „Ob“ einer langfristigen Aufbewahrung signierter Dokumente und zum anderen Vorgaben für das „Wie“ der Aufbewahrung. Während die Vorgaben für das „Ob“ der Aufbewahrung überwiegend verpflichtend sind, gelten die Vorgaben für das „Wie“ optional. Allerdings hat auch die Befolgung und die Nichtbefolgung dieser optionalen Vorgaben Rechtsfolgen, die für die Wahl des Verfahrens der Aufbewahrung bedacht werden müssen. Insbesondere kann der besondere Beweiswert qualifiziert signierter Dokumente nur gesichert und damit die vielfach erforderliche Beweissicherheit im Electronic Commerce und Electronic Government nur erreicht werden, wenn die Vorgaben des Signaturgesetzes und der Signaturverordnung an das „Wie“ der Aufbewahrung eingehalten werden.

2.1 Rechtliche Erfordernisse langfristiger Aufbewahrung

Das Recht schreibt eine längerfristige Aufbewahrung von Dokumenten im Wesentlichen aus vier Gründen vor.[1] Dokumente sollen aufbewahrt werden, weil sie sicher stellen sollen, dass

- später wieder auf die in ihnen enthaltenen Informationen zugegriffen werden kann (z. B. Arzt- oder Verwaltungsdokumentation oder anderen Formen der Dokumentation arbeitsteiliger Sachbearbeitung),

[1] S. hierzu auch *Fischer-Dieskau/Roßnagel/Steidle/Pordesch*, in: Roßnagel/Schmücker, 2004, i.E.

- ein Rechtszustand nachgewiesen werden kann (z.B. durch die vorsorgende Gerichtsbarkeit – z.B. Grundbuch – und die streitentscheidende Gerichtsbarkeit – z.B. Straf-, Zivil-, Verwaltungs-, Sozial- oder Arbeitsprozess),
- Kontrollen durchgeführt werden können (Arbeitgeber, Wirtschaftsprüfer, Aktionäre, Finanzverwaltung, Rechnungshof, Parlament, Gerichte, Datenschutzbeauftragte, Antragsteller, die Akteneinsicht oder Informationszugang begehren, Datenschutzbetroffene),
- die Inhalte im allgemeinen öffentlichen Interesse dauerhaft aufbewahrt werden können (Archivierung).

Die Aufbewahrung von Dokumenten kann ihren jeweiligen Zweck nur dann erfüllen, wenn die Dokumente bereits in einer dem Zweck entsprechenden Weise erstellt werden. Daher richten sich die einschlägigen Rechtsvorschriften in der Regel an die Dokumentation im Ganzen und nicht nur an die Aufbewahrung von einzelnen Dokumenten. Um diese Ziele der Dokumentation auch nach längerer Zeit noch erfüllen zu können, muss die Aufbewahrung den im Folgenden erörterten Anforderungen entsprechen.

Die gesetzlich vorgegebenen oder aus dem Gesetzeszweck abzuleitenden Aufbewahrungsfristen sind sehr unterschiedlich und reichen von fünf Jahren (z.B. §§ 4 und 8 SigV), sechs Jahren (z.B. § 257 Abs. 4 HGB), zehn Jahren (§ 10 Abs. 3 Musterberufsordnung für Ärzte), 30 Jahren (z.B. § 42 Strahlenschutzverordnung, § 28 Abs. 3 Röntgenverordnung) und mehr. Dies kann für das gesamte Leben des Betroffenen gelten. Bei längeren Dauerschuldverhältnissen etwa müssen die Dokumente, die dieses begründen, für die Dauer der Vertragsgeltung, der Nachsorgepflichten und der Verjährung aufbewahrt werden. Nach § 42 Strahlenschutzverordnung beispielsweise müssen Aufzeichnungen bis zum 75. Lebensjahr des Überwachten aufbewahrt werden. Im Rahmen der Bau-, Gewerbe oder Umweltverwaltung zum Beispiel müssen die Unterlagen über Genehmigungen von Bauwerken, Gewerbe- oder Industrieanlagen solange aufbewahrt werden, wie das Gebäude oder die Anlage steht – und wegen potentieller Altlasten sogar noch länger.

Für diese Dokumente ist vielfach Schriftform vorgeschrieben. Auch ohne gesetzlichen Zwang wird die Schriftform oftmals aufgrund ihrer hohen Beweissicherheit gewählt.[2] Unter Schriftform versteht das Recht (z.B. § 126 Abs. 1 BGB) in der Regel ein eigenhändig unterschriebenes Papierdokument. Der Gesetzgeber hat jedoch inzwischen in nahezu allen Bereichen (z.B. § 126 Abs. 3 BGB, § 3a VwVfG) ermöglicht, dass die Schriftform durch die elektronische Form ersetzt werden kann. Da auf diese Weise die Schriftform durch ein elektronisches Verfahren ersetzt werden kann, ist damit auch die Möglichkeit eröffnet worden, die gesetzlichen Aufbewahrungspflichten durch die Aufbewahrung elektronischer Dokumente zu erfüllen.

Um beim Ersatz der Schriftform durch die elektronische Form die erforderliche Sicherheit der Integrität und Authentizität der Daten ausreichend gewährleisten zu können, verlangt der Gesetzgeber hierfür den Einsatz qualifizierter elektronischer Signaturen nach dem Signaturgesetz als Ersatz der Unterschrift (z.B. § 126 Abs. 3 BGB, § 3a

---

[2] *Bizer*, in: Kröger./Gimmy (Hrsg.), Handbuch zum Internetrecht, 41.

VwVfG). Vielfach werden elektronische Dokumente aber auch ohne gesetzlichen Zwang nur aus Gründen der Beweissicherung mit qualifizierten elektronischen Signaturen versehen, um für diese einen papiernen Urkunden vergleichbaren Beweiswert zu schaffen.

Eine fehlende, oder fehlerhafte Aufbewahrung kann zu negativen Rechtsfolgen führen. Diese unterscheiden sich je nach dem, ob die betroffene Stelle zur Aufbewahrung verpflichtet war oder nicht. Bestand eine Rechtspflicht zur Aufbewahrung, so muss die Stelle zum einen mit einer Schadensersatzforderung aus Vertrags- oder aus Amtspflichtverletzung rechnen. In der Regel kann dann eine Partei ihre Rechtsforderungen nicht mehr belegen oder ist einer ungerechtfertigten Forderung ohne Abwehrmöglichkeiten ausgeliefert. Der dadurch entstehende Schaden trifft dann die aufbewahrungspflichtige Stelle. Ist die Stelle selbst Prozesspartei, trifft sie zum anderen eine Beweislast für ihr ordnungsgemäßes Handeln, selbst wenn eigentlich die andere Partei beweispflichtig wäre.

Handelt es sich bei der Aufbewahrung nicht um eine Rechtspflicht, sondern nur um eine Obliegenheit (eine Obliegenheit ist verletzt, wenn die Partei in zurechenbarer Weise gegen ihr eigenes Interesse handelt – z.B. Nichtaufbewahrung eines Kaufvertrages, um den Kauf nachweisen zu können), so kann dies zum Verlust eines Rechtsstreits führen. Ist die Partei beweispflichtig, so kann sie mangels geeigneter Beweismittel einen Anspruch nicht gerichtlich geltend machen oder abwehren.

2.2 Beweisführung mit signierten Dokumenten

Die Beweisführung mit elektronischen Dokumenten nach den allgemeinen Regeln der Beweislast und der freien Beweiswürdigung ist im Fall des Bestreitens der Integrität und Authentizität für den Beweispflichtigen sehr schwierig und oft unmöglich.[3] Dies gilt bei einem qualifizierten Bestreiten auch beim Vorliegen von elektronischen Signaturen.[4] Hier kann sich das zusätzliche Beweisproblem ergeben, dass die Einhaltung der elektronischen Form nachzuweisen ist. Dies erfordert, eine bestimmte Qualität elektronischer Signaturen, nämlich das Vorliegen qualifizierter elektronischer Signaturen nach § 2 Nr. 3 SigG, auch noch nach längerer Zeit zu belegen zu können.[5]

Um diesen Beweisnachteil auszugleichen, hat der Gesetzgeber in § 292a ZPO eine Beweiserleichterung für die Beweisführung mit qualifizierten elektronisch signierten Dokumenten geschaffen. Erst und nur diese bietet für elektronisch signierte Dokumente eine vergleichbare Rechts- und Beweissicherheit, wie sie Papierdokumente bieten. § 292a ZPO gilt nicht nur für den Zivilprozess, sondern aufgrund der Verweisungen auf die ZPO in anderen Prozessordnungen[6] auch für alle Prozessverfahren auf Basis deutschen Prozessrechts.

---

3 S. z.B. *Roßnagel/Pfitzmann*, NJW 2003, 1209 ff.

4 S. *Roßnagel*, Einleitung ins SigG, in: ders. (Hrsg.), Recht der Multimediadienste, Rn. 224 ff.

5 Zu den Möglichkeiten und Schwierigkeiten einer Beweisführung im Rahmen der freien Beweiswürdigung s. näher *Fischer-Dieskau/Roßnagel/Steidle*, MMR 2004, 451 ff.

6 S. §§ 173 VwGO, 202 SGG, 155 FGO, die auf die ZPO verweisen.

Voraussetzung für die Inanspruchnahme der Beweiserleichterung des § 292a ZPO ist eine in elektronischer Form (§ 126a BGB) vorliegende Willenserklärung, deren Anschein der Echtheit sich auf Grund einer Prüfung nach dem Signaturgesetz ergibt. Die elektronische Form nach § 126a BGB setzt den Einsatz einer gültigen qualifizierten elektronischen Signatur voraus. Wird im Zivilprozess die elektronische Form nicht bestritten, so geht das Gericht von ihrem Vorliegen aus. Bestreitet dagegen der Beklagte ihr Vorliegen mit qualifizierten Argumenten, so muss im Regelfall der Kläger ihr Vorliegen nachweisen. Er muss somit alle Voraussetzungen einer qualifizierten elektronischen Signatur nach § 2 Nr. 2 und 3 SigG belegen. Hiermit dürfte er meist überfordert sein, weil er keinen Einblick in die technisch-organisatorischen Maßnahmen des Zertifizierungsdiensteanbieters hat. Weist das Dokument dagegen akkreditierte Signaturen auf, kommt der beweispflichtigen Partei die Sicherheitsvermutung des § 15 Abs. 1 Satz 4 SigG zu Hilfe. Mit ihrer Unterstützung kann der Beweisführer die Voraussetzung der technisch-organisatorischen Sicherheit des Zertifizierungsdiensteanbieters nachweisen. Diese Erleichterung besteht beim Einsatz qualifizierter elektronischer Signaturen nicht.[7]

Kann die beweispflichtige Partei in einem Rechtsstreit den Richter nicht vom Wahrheitsgehalt ihrer Behauptung, hier von der Authentizität und Integrität einer elektronischen Signatur oder ihrer signaturrechtlichen Qualität, überzeugen, verliert sie den Prozess. War eine der Parteien zur Aufbewahrung des elektronischen Dokuments verpflichtet und kann sie das Dokument nicht (mehr) im Rechtsstreit vorlegen, so kann dies zu einer Beweislastumkehr führen. In diesem Fall ist die an sich nicht beweispflichtige, aber aufbewahrungspflichtige Partei verpflichtet, ihr ordnungsgemäßes Handeln nachzuweisen, und trägt somit das Risiko der überzeugenden Beweisführung. Ohne das aufzubewahrende Dokument oder ohne Nachweismöglichkeit seiner Integrität, Authentizität oder Formerfüllung wird sie den Prozess verlieren.

2.3 Integritätssicherung nach § 17 SigV

Werden signierte Daten für längere Zeit aufbewahrt, stellt sich das Problem, dass die Signaturen ihre Fälschungssicherheit verlieren können. Durch Fortschritte in der Kryptanalyse und der Rechnerleistung nimmt die Eignung der eingesetzten öffentlichen Schlüsselverfahren und Hashverfahren mit der Zeit ab – und mit ihnen die Sicherheit der elektronischen Signaturen und damit verbunden auch ihr Beweiswert.

Vom Verlust der Sicherheitseignung bedroht ist nicht nur der verschlüsselte Hashwert der signierten Nutzdaten, also des Dokuments. Ebenso bedroht sind andere für die Verifikation der Signatur zusätzlich erforderliche Daten, wie Zertifikate oder Verzeichnisauskünfte,[8] weil auch diese durch Signaturen abgesichert werden. Falls zur Beweiswertsicherung erneute Signaturen verwendet werden, so sind schließlich auch die darin verwendeten Algorithmen und Parameter zu beachten. Auch der Beweiswert all dieser zur Prüfung von Nutzersignaturen notwendigen Daten ist daher zu erhalten.

---

7 S. hierzu ausführlich *Fischer-Dieskau/Gitter/Paul/Steidle*, MMR 2002, 709; *Roßnagel*, NJW 2001, 1825; *Borges*, Verträge im elektronischen Geschäftsverkehr, 2003, 506.

8 S. näher *Roßnagel/Pordesch*, in: Roßnagel (Hrsg.), Recht der Multimediadienste, § 17 SigV, Rn. 62 ff.

Aus der Zielsetzung der Aufbewahrung, für eine bestimmte Dauer die Rechtmäßigkeit vorgenommener Handlungen oder Unterlassungen nachzuweisen und ihre Nachvollziehbarkeit und Kontinuität zu gewährleisten, ergibt sich jedoch die Anforderung, für die erforderliche Dauer die Vollständigkeit und Fälschungssicherheit sicher zu stellen. Haben einzelne Handlungen einem bestimmten Formerfordernis unterlegen, so muss auch deren Einhaltung dauerhaft nachweisbar sein.

Wird festgestellt, dass die Algorithmen oder ihre Parameter keine ausreichende Sicherheit für den vorgeschriebenen oder gewünschten Aufbewahrungszeitraum bieten, benötigen sie daher einen neuen Integritätsschutz. Es ist nachweisbar zu machen, dass bestimmte Daten existiert haben, bevor die Algorithmen und Parameter unsicher und Fälschungen möglich wurden. Wurde ein Hashalgorithmus unsicher, so muss wenigstens nachgewiesen werden können, dass die gehashten Daten zu einem Zeitpunkt vorlagen, bevor der Algorithmus unsicher wurde. Wurde ein Verschlüsselungsalgorithmus unsicher, so muss wenigstens nachgewiesen werden können, dass der Signaturwert, das heißt, der verschlüsselte Hashwert, der Signaturprüfschlüssel und das Verschlüsselungsverfahren vorlagen, bevor der Algorithmus unsicher wurde.[9]

Um für den Rechtsverkehr zu dieser Frage eine verlässliche Auskunft zu geben, verpflichtet die Signaturverordnung in Anlage 1 Nr. I. 2. die Regulierungsbehörde für Telekommunikation und Post, eine Übersicht über die geeigneten Algorithmen und zugehörigen Parameter sowie den Zeitpunkt, bis zu dem die Sicherheitseignung gilt, zu veröffentlichen.[10] Der Zeitpunkt soll mindestens sechs Jahre nach dem Zeitpunkt der Bewertung und ihrer Veröffentlichung liegen. Die Eignung ist jährlich sowie bei Bedarf neu zu bestimmen.

Werden die signierten Daten für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter nach dieser Veröffentlichung der Regulierungsbehörde als geeignet beurteilt sind, sollen sie entsprechend § 6 Abs. 1 Satz 2 SigG und § 17 Satz 1 SigV neu signiert werden. Spätestens wenn in einer solchen Veröffentlichung angegeben wird, dass ein Algorithmus oder Parameter demnächst nicht mehr als sicherheitsgeeignet anzusehen ist, müssen also alte Signaturen neu signiert werden. Nicht notwendig ist hingegen ein regelmäßiges erneutes Signieren.[11]

Wie die Neusignierung erfolgen soll, bestimmt § 17 SigV in seinen Sätzen 2 und 3. Danach sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere

---

9 S. hierzu *Roßnagel/Pordesch*, in: Roßnagel (Hrsg.), Recht der Multimediadienste, § 17 SigV, Rn. 46.

10 S. zur letzten Bekanntmachung der Regulierungsbehörde vom 13.2.2004 Bundesanzeiger Nr. 31, 1787; Bekanntmachungen der Regulierungsbehörde zu geeigneten Kryptoalgorithmen nach § 17 Abs. 2 SigV sind über www.regtp.de erhältlich.

11 So allerdings noch die Amtl. Begründung zum SigG 1997, BR-Drs. 966/96, 29.

Signaturen einschließen und einen qualifizierten Zeitstempel tragen. Diese Vorschrift ist missverständlich und bedarf der praxisgerechten Auslegung.[12]

§ 17 Satz 2 SigV fordert, dass die „Daten ... neu zu signieren“ sind. Diese Anforderung ist nicht so zu verstehen, dass immer der jeweilige Datensatz neu gehasht und signiert werden muss. Vielmehr muss diese Anforderung von der Sicherheitsfunktion der Neusignierung, die durch die Anforderung realisiert werden soll, dahingehend verstanden werden, dass die neu zu signierenden Daten entsprechend der fehlenden Eignung des Sicherungsmittels neu signiert werden müssen. Werden sowohl die verwendeten Signaturverfahren als auch die eingesetzten Hashverfahren unsicher, so sind die gesamten Daten neu zu hashen und zu signieren. Gelten hingegen nur die Signaturverfahren oder deren Parameter als nicht mehr geeignet, so reichen erneute elektronische Signaturen über die Signaturwerte (in Verbindung mit der Angabe des Signaturprüfschlüssels und Signaturalgorithmus) aus, um den Zweck der Vorschrift zu erfüllen, die Daten langfristig zu sichern. Die Daten werden in diesem Fall durch einen noch sicheren Hashwert repräsentiert.

Die gleiche Anforderung ist auch nicht so zu verstehen, dass immer die Daten des jeweiligen Dokuments neu signiert werden müssen. Nicht für jedes elektronisch signierte Dokument muss jeweils eine einzelne erneute Signatur erzeugt werden. Vielmehr können die Daten vieler Dokumente gleichzeitig neu signiert werden.[13]

Müssen elektronisch signierte Dokumente für sehr lange Zeiträume aufbewahrt werden, kann es für einen hohen Nachweiswert der elektronischen Signatur erforderlich sein, mehrfach nach jeweils einigen Jahren eine neue elektronische Signatur anzubringen. Jede neue Signatur bildet eine neue „Integritätshülle“ für die vorhergehenden Signaturen. Die Prüfung der elektronischen Signaturen erfolgt dann entsprechend logisch „geschachtelt“.[14]

Nach dem Wortlaut des § 17 Satz 3 SigV muss die erneute Signatur eine qualifizierte Signatur und einen qualifizierten Zeitstempel tragen. Doch auch diese Anforderung ist mit Blick auf ihren Sicherungszweck interpretationsbedürftig. Zwar fordert ein qualifizierter Zeitstempel keine Signatur. Er wird vielmehr von § 2 Nr. 14 SigG lediglich definiert als „elektronische Bescheinigung eines Zertifizierungsdiensteanbieters ... darüber, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben“. Gegenwärtig gibt es aber nur eine anerkannte technische Spezifikation für Zeitstempel, nach der die Daten und die authentische Zeitangabe durch die elektronische Signatur des Zeitstempeldienstes miteinander verbunden werden, sowie zugehörige zertifizierte technische Produkte und akkreditierte Dienstleister.[15] Um für den – derzeit üblichen – Fall, dass ein Zeitstempel mit Hilfe einer qualifizierten Signatur erstellt wird, das unsinnige Ergebnis zu vermeiden, dass zur Erstellung einer erneuten Signatur zwei

---

12 S. zum Folgenden ausführlich *Roßnagel/Fischer-Dieskau/Brandner/Pordesch*, CR 2003, 301

13 So hatte bereits die amtliche Begründung für die Vorgängervorschrift des § 18 SigV 1997 festgestellt, dass „für eine beliebige Anzahl signierter Daten eine (übergreifende) neue digitale Signatur“ genügt.

14 S. *Roßnagel/Fischer-Dieskau/Pordesch/Brandner*, CR 2003, 301 ff.

15 RFC 3161 - Time Stamp Protocol, Network Working Group, 2001.

qualifizierte elektronische Signaturen angebracht werden müssen, ist eine an der sicherheitstechnischen Zielsetzung der Vorschrift orientierte teleologische Reduktion vorzunehmen: Werden elektronisch signierte Dokumente mit einem qualifizierten Zeitstempel versehen, der eine qualifizierte Signatur enthält, so genügt dies für eine erneute Signatur im Sinn des § 17 Satz 3 SigV.[16] Dieser Zeitstempel kann mit einem Zertifikat, das auf ein Pseudonym lautet, automatisiert erstellt werden.[17]

Interpretationsbedürftig ist schließlich auch die Forderung des § 17 Satz 3 SigV, dass die erneute Signatur „frühere Signaturen einschließen" muss. Diese Anforderung ist einmal so zu verstehen, dass „frühere Signaturen" alle Signaturen meint, die bereits Teil des Ursprungsdokuments waren, aber auch diejenigen, die bereits vor der Neusignierung zum Zweck der Beweiswerterhaltung angebracht worden sind und nun selbst neu signiert werden müssen, weil ihre Algorithmen und Parameter unsicher werden. Bei mehreren in zeitlichem Abstand angebrachten erneuten Signaturen muss jede weitere Neusignierung somit alle zuvor angebrachten erneuten Signaturen umfassen, um die Konsistenz aller Signatur- und Dokumentfassungen sicher zu stellen. Diese Anforderung ist zum anderen so zu verstehen, dass bei Mehrfachsignaturen zum ursprünglichen elektronischen Dokument auch deren Zusammengehörigkeit für die Aufbewahrung durch eine gemeinsame neue Signatur gesichert werden soll. Dadurch soll die Vollständigkeit aller Signaturen zu einem Dokument sichergestellt und eine unerkannte Löschung einer Signatur verhindert werden.[18]

§ 17 Satz 3 SigV unterscheidet nicht zwischen der Erneuerung akkreditierter und qualifizierter elektronischer Signaturen. Allerdings ist erforderlich, dass dort, wo das Gesetz eine langfristige Prüfbarkeit fordert und damit indirekt akkreditierte elektronische Signaturen verlangt, auch ein Zeitstempel eines akkreditierten Zertifizierungsdiensteanbieters angebracht wird. Das Ziel, den ursprünglich bestehenden Grad an Sicherheit zu erhalten, kann nur durch ein Sicherungsmittel gewährleistet werden, das mindestens den ursprünglichen Sicherheitsanforderungen entspricht. Grundsätzlich muss somit die erneute Signatur mindestens die gleiche Qualitätsstufe haben wie die ihre Sicherheit verlierende Ausgangssignatur, wenn deren Qualität – etwa zur Erfüllung der Form oder des Beweiswerts – erhalten bleiben soll.[19]

§ 17 SigV beschreibt keine obligatorische Verpflichtung für denjenigen, der elektronisch signierte Dokumente aufbewahrt. Andere Methoden, die Unversehrtheit der elektronisch signierten Dokumente sicher zu stellen, werden damit nicht ausgeschlossen. Allerdings bleibt die Sicherheit qualifizierter elektronischer Signaturen bei einer langfristigen Aufbewahrung nur dann gewahrt, wenn sie nach dieser Vorschrift erfolgt. „Unterbleibt bei einer vorhandenen qualifizierten elektronischen Signatur mit Ablauf der Eignung der Algorithmen und zugehörigen Parameter eine erneute Signatur, so verliert

---

16 Nach der amtlichen Begründung zur dieser Vorschrift reicht es aus, „dem Zeitstempeldienst den Hashwert des zeitzustempelnden Dokuments zu schicken, wobei das Hashverfahren von dem Zeitstempeldienst vorgegeben ist".

17 S. *Roßnagel*/*Fischer-Dieskau*, MMR 2004, 133.

18 S. *Fischer-Dieskau/Roßnagel/Steidle*, MMR 2004, 451 ff.

19 S. z.B. *Roßnagel/Pordesch*, in: Roßnagel (Hrsg.), Recht der Multimediadienste, § 17 SigV, Rn. 59.

sie damit die vorgegebene Sicherheit."[20] Zwar behält die elektronische Signatur auch nach dem formalen Verlust der Eignung des mathematischen Verfahrens in der Regel noch über mehrere Jahre eine hohe Sicherheit,[21] da bei der Feststellung der Eignung immer eine erhebliche Sicherheitsreserve einbezogen werden soll.[22] Da das Verfahren aber nicht mehr als sicher vermutet werden kann, könnte im Streitfall die Beweiseinrede vorgebracht werden, die das elektronisch signierte Dokument vorlegende Partei oder ein Dritter habe die Signatur gefälscht.[23] Zumindest kann für ein solches Dokument nicht mehr die Beweiserleichterung des § 292a ZPO für einen Anschein seiner Unversehrtheit und Urheberschaft geltend gemacht werden.[24] Nicht nach § 17 SigV rechtzeitig neusignierte elektronische Signaturen verlieren damit ihre Beweissicherheit hinsichtlich ihrer Integrität.

2.4 Authentizitätssicherung durch Verifikationsdaten

Neben der Integrität des elektronischen Dokuments soll eine elektronische Signatur auch die Authentizität, die Zurechenbarkeit zu einer bestimmten Person, sicherstellen. Der Urheber des Dokuments sowie aller daran vorgenommenen Veränderungen (Verbesserungen, Ergänzungen) soll eindeutig erkennbar sein.

Diese Zuordnung erfolgt über qualifizierte Zertifikate nach § 7 SigG. Diese Zertifikate sind dann geeignet, die Zuordnung des Signaturschlüssels zum Signaturschlüssel-Inhaber zu bestätigen, wenn der Signaturschlüssel-Inhaber sich gegenüber dem Zertifizierungsdiensteanbieter identifiziert hat und dieser ihm die sichere Signaturerstellungseinheit mit seinem Signaturschlüssel und seinen Identifizierungsdaten korrekt übergeben hat. Der Zertifizierungsdiensteanbieter darf daher nach § 5 Abs. 2 SigV das Zertifikat erst dann in das Zertifikatverzeichnis einstellen, wenn der Signaturschlüssel-Inhaber schriftlich bestätigt hat, dass ihm die sichere Signaturerstellungseinheit korrekt übergeben worden ist. Entsteht nachträglich ein Sperrgrund, hat er das Zertifikat im Verzeichnisdienst zu sperren.

Hieran knüpft die Beweiserleichterung des § 292a ZPO an. Sie gewährt für qualifizierte elektronische Signaturen nur dann den schwer widerlegbaren Anschein der Authentizität, wenn eine Prüfung nach Signaturgesetz erfolgreich ist. Dies meint neben der Prüfung der Integrität auch eine Prüfung der Authentizität entsprechend § 7 Abs. 1 Nr. 5 und § 5 Abs. 1 Satz 2 SigG: Nach § 7 Abs. 1 Nr. 5 SigG ist im Zertifikat selbst das Ende seiner Gültigkeit eingetragen. Nach § 5 Abs. 1 Satz 2 SigG wird die Gültigkeit eines Zertifikats hinsichtlich seiner Ausstellung und einer vorzeitigen Sperrung durch automatisierte Abfragen bei dem jeweiligen Zertifizierungsdiensteanbieter überprüft, der das

---

20 Amtliche Begründung zur Vorschrift.

21 Amtliche Begründung zur Vorschrift; s. auch *Bieser/Kersten* 1999, 68; zur Beweisführung mit nicht neu signierten elektronisch signierten Dokumenten s. *Fischer-Dieskau/Roßnagel/Steidle*, MMR 2004, 451.

22 S. *Roßnagel/Hammer*, in: Roßnagel (Hrsg.), Recht der Multimediadienste, § 18 SigV 1997, Rn. 62 ff .

23 S. z.B. *provet/GMD* 1994, 227 ff.; *Bizer/Hammer/Pordesch* 1995, 99.

24 S. *Fischer-Dieskau/Roßnagel/Steidle*, MMR 2004, 451.

Zertifikat ausgestellt hat.[25] Sofern das Zertifikat abrufbar gehalten wird, kann der Prüfende es selbst prüfen oder sich sogar herunter laden. Wird es vom Zertifizierungsdiensteanbieter nur nachprüfbar gehalten, bestätigt dieser entweder die Gültigkeit des Zertifikats, verneint diese oder erklärt das Zertifikat für unbekannt. Nur bei einer Bestätigung der Gültigkeit des Zertifikats ist eine positive Prüfung der Signatur nach dem Signaturgesetz im Sinn des § 292a ZPO erfolgt.

Von Bedeutung ist nun, bei welchem Status ihrer Zertifikate eine Signatur vom Prüfprogramm für gültig erklärt wird. Hier gibt es unterschiedliche Gültigkeitsmodelle, die sich durch den Zeitpunkt, für den jeweils die Gültigkeit geprüft wird, und die Berücksichtigung der Gültigkeit der Zertifikate in der Zertifikatkette unterscheiden. Das Schalenmodell[26] stellt auf den Prüfzeitpunkt ab und erkennt eine Signatur dann als gültig an, wenn zu diesem Zeitpunkt alle zugehörigen Zertifikate in der Kette gültig sind. Der Zertifizierungsdiensteanbieter wird nach dem Schalenmodell in seiner Verzeichnisdienstauskunft ein Zertifikat nur dann für gültig erklären, wenn dieses selbst und das Zertifikat des Zertifizierungsdiensteanbieters sowie weitere notwendige Zertifikate aktuell gültig sind. Dagegen stellt das Kettenmodell für die Prüfung auf den Zeitpunkt der Signaturerzeugung ab und erkennt eine Signatur dann als gültig an, wenn zu diesem Zeitpunkt das zugehörige Zertifikat gültig war. Da für dieses Zertifikat das gleiche gilt, kann das zweite oder dritte Zertifikat in der Kette bei der Erzeugung der Signatur des Signaturschlüssel-Inhabers bereits ungültig gewesen sein, ohne dass dies die Gültigkeit der Signatur betrifft, wenn sie jeweils gültig waren, als das darunter liegende Zertifikat erzeugt wurde.[27] Die Verzeichnisdienstauskunft gibt daher immer dann die Auskunft „gültig", wenn jeweils das zu der zu prüfenden Signatur (des Signaturschlüssel-Inhabers oder des Zertifizierungsdiensteanbieters) zugehörige Zertifikat zum Zeitpunkt der Signaturerzeugung gültig war.

Nach § 19 Abs. 5 SigG bleibt die „Gültigkeit der ... qualifizierten Zertifikate ... von der Untersagung des Betriebes und der Einstellung der Tätigkeit sowie der Rücknahme und dem Widerruf einer Akkreditierung unberührt". Da der qualifizierte Zertifizierungsdiensteanbieter seine eigenen Zertifikate bei einer Untersagung oder Einstellung des Betriebs sperrt oder die Regulierungsbehörde bei einem akkreditierten Zertifizierungsdiensteanbieter die Sperrung nach § 16 Abs. 1 durchführt, ohne dass das die Gültigkeit des Zertifikats des Signaturschlüssel-Inhaber berühren darf, kann geschlossen werden, dass das Signaturgesetz für das Gültigkeitsmodell fordert, dass dieses auf den Zeitpunkt der Signaturerzeugung abstellt und dass allein eine fehlende Gültigkeit eines zugehörigen Zertifikats zum Prüfzeitpunkt die Gültigkeit der Signatur nicht berühren darf. Für das Signaturgesetz ist nicht entscheidend, nach welchem Modell geprüft wird, sondern dass diese Anforderungen erfüllt werden. Dies ist jedenfalls beim Kettenmodell der Fall. Ob sie derzeit auch durch ein modifiziertes Schalenmodell erfüllt werden können,[28] kann hier dahin stehen. Nach dem Entwurf des 1. SigÄndG vom 30.4.2004,[29] wird § 8 SigG dahingehend geändert, dass weitere Sperrgründe vertraglich vereinbart

---

25 Derzeit nach dem Standard „Online Certificate Status Protocol (OCSP)".

26 S. z.B. *ITU-T*, X 509; *Hously/Polk/Ford/Solo*, RFC 3280.

27 S. hierzu *Regulierungsbehörde für Telekommunikation und Post* 2004.

28 So *Büger/Esslinger/Koy*, DuD 2004, 138.

29 BT-Drs. 15/3417.

werden können. Dadurch soll auch ermöglicht werden, Sperrungen durchzuführen, die sich aus einem modifizierten Schalenmodell ergeben. Jedenfalls müssen die Zertifikate nach dem Modell überprüft werden, das ihrer Erzeugung zugrunde lag. Daher muss dieses im Zertifikat signalisiert werden, damit bei einer automatisierten Prüfung nach dem richtigen Modell geprüft wird.

Bei einer langfristigen Aufbewahrung von elektronisch signierten Dokumenten ergibt sich für den Authentizitätsnachweis ebenfalls ein mit der Zeit zunehmendes Beweisproblem. Die Daten für die Verifikation der Authentizität, die Zertifikate und Zertifikatketten, sind nur eine begrenzte Zeit verfügbar. Die Zertifizierungsdiensteanbieter sind nur verpflichtet, diese Verifikationsdaten für eine begrenzte Zeit vorzuhalten und löschen sie in der Regel nach Ablauf dieser Frist. Diese Frist beträgt gemäß § 4 Abs. 2 SigV nach Ablauf des Jahres der Gültigkeit des Zertifikats bei akkreditierten Zertifizierungsdiensteanbietern mindestens 30 Jahre, bei Anbietern qualifizierter Zertifikate nur fünf Jahre. Eine konkursresistente Aufbewahrung ist nur bei akkreditierten Zertifizierungsdiensteanbietern gewährleistet.[30] Für die zum Zertifikat gehörige Dokumentation gelten nach § 8 Abs. 1 Satz 1 SigV durch den Verweis auf § 4 Abs. 2 SigV die gleichen Fristen.

Die dauerhafte Überprüfung der Gültigkeit eines Zertifikats ist somit bei einer Abhängigkeit vom Zertifizierungsdiensteanbieter nicht sichergestellt. Für den langfristigen Authentizitätsnachweis muss daher der Aufbewahrungspflichtige alle erforderlichen Verifikationsdaten selbst einholen, aufbewahren und sichern.[31] Eine dauerhafte Erhaltung des Beweiswerts ist somit allein durch die von § 17 SigV geregelte Neusignierung noch nicht gewährleistet. Hierfür bedarf es neben dem dort geregelten Verfahren weiterer Maßnahmen, um den Authentizitätsnachweis durch Einbeziehung von Verifikationsdaten zu sichern. Auch wenn dies in § 17 SigV nicht geregelt ist, sind diese Maßnahmen eine unverzichtbare Voraussetzung, um das Ziel dieser Vorschrift zu erreichen. Um die Beweiskraft elektronisch signierter Dokumente über die gesetzlich vorgeschriebenen Aufbewahrungsfristen von 30 und mehr Jahren zu gewährleisten, müssen qualifizierte elektronische Signaturen rechtzeitig um langfristig benötigte Verifikationsdaten ergänzt werden.

Notwendige Verifikationsdaten, die für eine längere Aufbewahrung zu beschaffen, zu archivieren und zu sichern sind, betreffen nicht nur die Zertifikate und die sie betreffenden Gültigkeitsbestätigungen der Ursprungssignatur, sondern auch alle Verifikationsdaten der neu angebrachten Signaturen.

Werden die erforderlichen Verifikationsdaten nicht aufbewahrt und nach § 17 SigV gesichert und sind sie auch nicht mehr durch Online-Abfragen bei den Zertifizierungsdiensteanbietern nachprüfbar, ist eine Prüfung nach dem Signaturgesetz nicht möglich und die Beweiserleichterung des § 292a ZPO kann nicht zur Anwendung kommen. In diesem Fall ist auch eine Beweisführung allein nach den Regeln der freien Beweiswürdigung höchst unwahrscheinlich, da die beweispflichtige Partei keine Möglichkeiten

---

30 S. hierzu *Roßnagel*, MMR 2002, 219f.

31 S. *Roßnagel/Fischer-Dieskau/Pordesch/Brandner*, CR 2003, 301 ff.; *Fischer-Dieskau/Roßnagel/Steidle*, MMR 2004, 451 ff.

hat, einer qualifizierten Beweiseinrede fehlender Urheberschaft durch Beweismittel entgegenzutreten. Ohne prüfbare Verifikationsdaten verlieren elektronische Signaturen ihre Beweissicherheit hinsichtlich ihrer Authentizität.

2.5 Daten- und Geheimnisschutz

Jede Art der Aufbewahrung von Dokumenten unterliegt, sobald in diesen personenbezogene Daten enthalten sind, dem Datengeheimnis und weiteren datenschutzrechtlichen Anforderungen. Da in Zertifikaten personenbezogene Daten enthalten sind, ist der Datenschutz im Regelfall bei allen signierten elektronischen Dokumenten betroffen. Neben dem Datenschutz können durch die aufzubewahrenden Dokumente auch Berufs-, Geschäfts-, Amts- und sonstige rechtlich geschützte Geheimnisse berührt sein. Daher ergeben sich aus der Sicherstellung des Daten- und Geheimnisschutzes weitere Anforderungen an die Aufbewahrung, zu deren Erfüllung besondere Schutzmaßnahmen getroffen werden müssen.

Das Datenschutzrecht dient der Gewährleistung der informationellen Selbstbestimmung des Betroffenen. Hier sind vor allem zwei Aspekte von besonderem Interesse. Erstens unterliegen die Daten einer Zweckbindung. Ist der Zweck des Gesetzes oder des Vertrags erreicht, liegt kein Grund für eine weitere Aufbewahrung vor, und die Unterlagen können und müssen vernichtet werden.[32] Das Datenschutzrecht bestimmt also eine Höchstaufbewahrungsdauer. Diese ist für die einzelnen Dokumente unterschiedlich. Die Aufbewahrung muss also so erfolgen, dass einzelne Dokumente gelöscht werden können, ohne den Beweiswert anderer Dokumente zu gefährden. Zweitens gewährt das Datenschutzrecht dem Betroffenen spezifische Rechte, die auch Ansprüche auf Berichtigung, Löschung, Sperrung und gegebenenfalls Gegendarstellung umfassen.[33] Damit der Betroffene diese Rechte auch tatsächlich geltend machen kann, muss die Aufbewahrung und ihre Sicherung durch Neusignierung in einer Weise erfolgen, die es ermöglicht, Dokumente zu ändern, zu ergänzen oder teilweise zu löschen, ohne den Beweiswert anderer Dokumente zu gefährden. Dokumente müssen einzeln langfristig verifizierbar sein. Aus diesem Grund sollte die Neusignierung – soweit möglich – unabhängig vom elektronischen Dokument erfolgen können.

Der Schutz von Geheimnissen zielt darauf, Nichtberechtigte von der Kenntnisnahme des Geheimnisses und der Verfügung über dieses auszuschließen. Soweit Dokumente aufzubewahren sind, die Geheimnisse betreffen, ist sicherzustellen, dass Nichtberechtigte keinen Zugang zu und keinen Zugriff auf diese Dokumente haben können. Das Datenschutzrecht fordert von den verantwortlichen Stellen, technisch-organisatorische Schutzvorkehrungen zu treffen, um die Rechte der Betroffenen zu wahren. Hierzu gehören ebenfalls Maßnahmen, die den Schutz vor dem Zugang und dem Zugriff Unbefugter sicherstellen.[34] Schließlich sollen durch die Einrichtung und Beteiligung von unabhängigen Kontrollinstanzen die Kontrollrechte der Betroffenen verbessert und gewahrt werden. Neben Maßnahmen des Zugangs- und Zugriffsschutzes ist die Verschlüsselung

---

32 Eine Ausnahme besteht dann, wenn sie nach den Archivgesetzen als archivwürdig auf Dauer in ein öffentliches Archiv übernommen werden

33 S. hierzu näher *Wedde*, in: *Roßnagel*, Handbuch Datenschutzrecht, Kap. 4.4.

34 S. hierzu näher *Heibey*, in: *Roßnagel*, Handbuch Datenschutzrecht, Kap. 4.5

der Daten eine wichtige Maßnahme des gesetzlich gebotenen Schutzes der aufzubewahrenden Dokumente. Die Erneuerung qualifizierter elektronischer Signaturen sollte daher auch bei verschlüsselten Dokumenten möglich sein.

Künftig wird die Auslagerung der Aufbewahrung von Dokumenten an spezialisierte Archivdienstleister immer mehr an Bedeutung gewinnen. Zu deren Aufgaben wird auch die langfristige Beweiswerterhaltung elektronisch signierter Dokumente gehören. Die Verfahren zur Neusignierung sollten daher so gestaltet sein, dass sie eine Auslagerung dieser Aufgabe ermöglichen. Eine solche externe Langzeitspeicherung ist jedoch in vielen Bereichen nur zulässig, wenn „sich die Archivierung beschränkt auf während der Verwahrung bestimmungsgemäß verschlossen zu haltende, anonymisierte Behältnisse (Taschen, Mappen, Umschläge), welche äußerlich den Namen des Patienten nicht erkennen lassen."[35] Dies setzt jedoch voraus, dass die Daten verschlüsselt werden können. Die Verschlüsselung ist nicht nur zum Schutz von Amts-, Mandanten-, Patienten-, Betriebs- und Geschäftsgeheimnissen erforderlich, sondern auch bei der Auslagerung personenbezogener Daten geboten. Die Neusignierung sollte bei verschlüsselten Daten jedoch möglich sein, ohne dass die Daten zuvor jedes Mal durch den Dokumenteigentümer entschlüsselt werden müssen. Notwendige Voraussetzung für die Anwendung der Verschlüsselung im Zusammenhang mit der Neusignierung ist, dass zweifelsfrei nachweisbar ist, dass die verschlüsselten Daten, die erneut signiert wurden, das signierte Dokument repräsentieren. Dies ist an Bedingungen geknüpft, die unter anderem dadurch erfüllbar sind, dass der Verschlüsselungsschlüssel wie auch das angewendete Verschlüsselungsverfahren durch die erneute Signatur umfasst und dadurch nachweisbar sind.[36]

3. Vorgaben des europäischen Rechts

Die europäische Richtlinie für elektronische Signaturen hat die Frage der langfristigen Aufbewahrung elektronisch signierter Dokumente nicht explizit geregelt.

Sie hat in Art. 9 lediglich geregelt, dass die Europäische Kommission von einem „Ausschuss für elektronische Signaturen" unterstützt wird. Der Ausschuss soll nach Art. 10 RLeS die in den Anhängen der Richtlinie festgelegten Anforderungen präzisieren.

Diese Präzisierungen des Ausschusses hat die Signaturverordnung in § 15 Abs. 6 in der Weise berücksichtigt, dass an die Stelle der materiellen Anforderungen und der Prüfanforderungen für Produkte für qualifizierte Signaturverfahren die europäischen Normen treten können, die der Ausschuss für elektronische Signaturen allgemein anerkannt hat und die im EG-Amtsblatt veröffentlicht worden sind. Diese gehen dann aufgrund des dynamischen Verweises des § 15 Abs. 6 SigV den Anforderungen in der Signaturverordnung vor, ohne dass diese geändert werden müssen.[37]

Bisher hat dieser Ausschuss jedoch keine Regelung zur langfristigen Sicherung elektronischer Signaturen getroffen. Es ist auch nicht zu erwarten, dass er in absehbarer Zeit

---

35 OLG Düsseldorf, CR 1997, 536, für die externe Aufbewahrung von Patientendaten..

36 S. hierzu *Fischlin/Pordesch*, DuD 2004, 163 ff.

37 S. hierzu die amtliche Begründung 26 und 31.

solche Regelungen trifft. Daher gelten die nationalen Regelungen uneingeschränkt. Diese Abstinenz des europäischen Richtliniengebers macht es schwierig, geeignete Standards und Produkte zur Neusignierung für den europäischen Markt zu entwickeln. Daher ist es notwendig, im Rahmen der Standardisierung die erforderlichen einheitlichen Vorgaben zur Sicherheitseignung von Algorithmen und Parametern, zur Gültigkeit und Sperrung von Zertifikaten und zur Durchführung der Neusignierung zu erlassen.

Mit den Regelungen in der Signaturverordnung zur langfristigen Sicherung elektronischer Signaturen hat der deutsche Verordnungsgeber den Freiraum genutzt, den ihm die sehr weiten Rahmenregelungen der Richtlinie für elektronische Signaturen lassen. Da § 17 SigV ein technologieneutrales Verfahren mit objektiven Vorgaben beschreibt, keine anderen Verfahren ausschließt und den Binnenmarkt für elektronische Signaturverfahren nicht behindert, bestehen keine Bedenken gegen ihre Konformität mit europarechtlichen Vorgaben.[38]

4. Erfüllung der rechtlichen Anforderungen

Nachdem die zu berücksichtigenden rechtlichen Anforderungen an eine Spezifikation der Langzeitaufbewahrung qualifizierter elektronischer Signaturen dargestellt worden sind, kann geprüft werden, ob diese Anforderungen in dem Entwurf der ISIS/MTT-Spezifikation „Long Term Conservation of Electronic Signatures“ vom 30.6.2004 ausreichend berücksichtigt worden sind. Dabei wird entsprechend der drei großen Anforderungsbereiche untersucht, ob die Anforderungen zu Erhaltung der Integrität und Authentizität und zur Wahrung des Daten- und Geheimnisschutzes erfüllt worden sind.

Die Zielsetzung des Entwurfs in Kap. 1 entsprechen den Zielsetzungen des Signaturrechts, insbesondere § 6 SigG und § 17 SigV, den Beweiswert langfristig aufbewahrter qualifiziert signierter Dokumente zu erhalten. Die beiden hierfür spezifizierten Maßnahmen, die Integration der Verifikationsdaten in die zugehörigen Signaturen und die Neusignierung ihre Eignung verlierender Signaturen, entsprechen dieser Zielsetzung. Die SigG-Profilierung in Kap. 6 entspricht dem deutschen Signaturrecht.

4.1 Integritätssicherung

Der Entwurf basiert auf der richtigen Erkenntnis, dass zur Sicherung der Integrität der aufzubewahrenden Signaturen, von Zeit zu Zeit neue Signaturen erzeugt werden müssen. Hierfür hat die vorhergehende rechtliche Analyse ergeben, dass die folgenden Anforderungen erfüllt werden müssen.

1. Rechtzeitig Neusignierung

Werden Algorithmen und zugehörige Parameter in der jährlichen Veröffentlichung der Regulierungsbehörde für Telekommunikation und Post als nur noch für einen bestimmten Zeitraum als geeignet angesehen, muss eine Neusignierung mit geeigneten Algorithmen und zugehörige Parametern vor Ablauf dieser Frist erfolgen. Die Anforderun-

[38] S. *Roßnagel/Pordesch*, in: Roßnagel (Hrsg.), Recht der Multimediadienste, § 17 SigV, Rn. 27.

gen, um die Notwendigkeit einer Neusignierung zu erkennen und diese anzustoßen, werden in Kap. 5 und 6.1 zutreffend spezifiziert.

In Kap. 4.3 ist eine Verfahrensvariante vorgesehen, nach der entsprechend ETSI TS 101 733 Archiv-Zeitstempel angebracht werden können, es aber immer möglich sein muss, solche angebrachten Zeitstempel zu prüfen. Für diese Variante ist nicht festgelegt, wann der Zeitstempel jeweils anzubringen ist. SigG-konform ist sie nur dann, wenn der Zeitpunkt den genannten Anforderungen entspricht.

2. Neusignatur nach Sicherheitsbedarf

Kap. 4.4 sieht vor, dass Hashwerte und Signaturen unabhängig voneinander jeweils dann neu gehasht oder neu signiert werden, wenn die Eignung ihrer Algorithmen und zugehörigen Parameter schwächer wird. Diese am Sicherheitsbedarf orientierte Neusicherung der signierten Dokumente ist mit § 17 SigV vereinbar. Kap. 6.1 fordert für die Neusignatur jeweils geeignete Algorithmen und Parameter. Dies entspricht § 17 SigV.

In der Verfahrensvariante in Kap. 4.3 wird keine Unterscheidung nach dem Sicherheitsbedarf getroffen. Es werden stets die alte Signatur und die vorangehenden erneuten Signaturen (=ETSI-Archivzeitstempel) erneut signiert. Dies ist mit dem SigG konform.

3. Zusammenfassung mehrerer Dokumente

Der Entwurf sieht in Kap. 4.4 aus Gründen der Kostenersparnis und der Performance die Neusignatur vieler elektronisch signierter Dokumente durch einen Archivzeitstempel vor. Dies ist signaturrechtlich zulässig. § 17 SigV fordert nicht für jedes elektronisch signierte Dokument jeweils eine einzelne erneute Signatur. Vielmehr können die Daten vieler Dokumente gleichzeitig neu signiert werden.

Nach deutschem Signaturrecht ist es daher nicht notwendig – wie die Spezifikation ETSI TS 101 733 fordert –, für jede Signatur zur Erneuerung einen Zeitstempel vorzusehen. Diese in Kap. 4.3 vorgesehene Variante widerspricht aber auch nicht dem SigG.

4. Archivzeitstempel

Werden elektronisch signierte Dokumente mit einem qualifizierten Zeitstempel versehen, der eine qualifizierte Signatur enthält, so genügt dies für eine erneute Signatur im Sinn des § 17 Satz 3 SigV. Diese Anforderung wird durch Kap. 4.4 erfüllt. Kap. 6.1 gibt die Rechtslage korrekt wieder.

Die in Kap. 4.3 beschriebene Verfahrensvariante entspricht ebenfalls dieser Anforderung.

5. Einschluss aller alten und früheren neuen Signaturen

Die Forderung des § 17 Satz 3 SigV, dass die erneute Signatur „frühere Signaturen einschließen“ muss, gilt sowohl für die Signaturen des Ursprungsdokuments als auch für die Signaturen, die bereits vor der Neusignierung zum Zweck der Beweiswerterhaltung angebracht worden sind und nun bei nachlassender Eignung ihrer Algorithmen und Pa-

rameter selbst neu signiert werden müssen. Diese Anforderung wird durch Kap. 4.4 erfüllt und durch Kap. 6.1 bestätigt.

Insoweit ist auch die Verfahrensvariante in Kap. 4.3 mit dem Signaturgesetz vereinbar.

6. Einschluss von Mehrfachsignaturen

Die Forderung des § 17 Satz 3 SigV, dass die erneute Signatur „frühere Signaturen einschließen“ muss, gilt auch für Mehrfachsignaturen. Diese sollen nicht einzeln für sich, sondern gemeinsam neu signiert werden, damit deren Zusammengehörigkeit für die Aufbewahrung gesichert wird. Diese Anforderung wird durch Kap. 4.4 erfüllt und durch Kap. 6.1 bestätigt.

Dieser Anforderung des deutschen Signaturrechts wird die Verfahrensvariante in Kap. 4.3, die auf die Spezifikation ETSI TS 101 733 verweist, nicht gerecht, weil nach ihr nur einzelne elektronische Signaturen neu signiert werden, nicht aber alle Signaturen eines mehrfach signierten Dokumentes zusammen. Daher hat der Entwurf in seinem SigG-Profil diese Spezifikation zu Recht ausgeschlossen.

7. Schalenförmige Neusignierung

Hinsichtlich der Art und Weise der Neusignierung fordert § 17 SigV, dass jede neue Signatur eine neue „Integritätshülle“ für die vorhergehenden (alten und früheren neuen) Signaturen bildet. Die Prüfung der elektronischen Signaturen erfolgt entsprechend logisch nach den verschiedenen Schalen von außen nach innen. Diese Anforderung wird durch Kap. 4.4 erfüllt.

In der in Kap. 4.3 beschriebenen Verfahrensvariante wird stets die alte Signatur und die vorangehenden erneuten Signaturen (=ETSI-Archivzeitstempel) erneut signiert. Dies entspricht ebenfalls der Anforderung.

8. Einschluss der Verifikationsdaten

Die Forderung des § 17 Satz 3 SigV, dass die erneute Signatur „frühere Signaturen einschließen“ muss, betrifft auch die Signaturen der Verifikationsdaten. Nur wenn diese bei nachlassender Eignung ihrer Algorithmen und Parameter ebenfalls in ihrer Integrität geschützt werden, können sie die Authentizität des Ursprungsdokuments beweisen. Dies betrifft sowohl die Zertifikatkette sowie alle Gültigkeitsauskünfte. Jedenfalls ist nur dann bezogen auf die Verifikationsdaten die Beweiserleichterung des § 292a ZPO anwendbar. Diese Forderung wird in beiden Varianten der Signaturerneuerung in Kap. 4.3 und 4.4 erfüllt und durch Kap. 6.1 bestätigt.

9. Erhaltung der Formqualität

Haben einzelne signierte Dokumente einem bestimmten Formerfordernis unterlegen, so muss auch deren Einhaltung dauerhaft nachweisbar sein. Dies wird durch den Entwurf gewährleistet, weil zu jeder Zeit geprüft werden kann, dass qualifizierte Signaturen mit qualifizierten Zertifikaten vorliegen.

Dieser Nachweis kann auch mit der in Kap. 4.3 beschriebenen Verfahrensvariante gelingen. Jedoch bestehen für diese Variante größere Risiken, weil einzelne Signaturen – mit ihren Neusignaturen – unbemerkt gelöscht werden können.

10. Erhaltung der Signaturstufe

Grundsätzlich muss die erneute Signatur mindestens die gleiche Qualitätsstufe haben wie die ihre Sicherheit verlierende Ursprungssignatur, wenn deren Qualität – etwa zur Erfüllung der Form oder des Beweiswerts – erhalten bleiben soll. Diese Anforderung wird durch die SigG-Profilierung in Kap. 6.1 und 6.3 erfüllt, da dort diese Forderung erhoben und dahingehend präzisiert wird, dass Prozesse zur Neusignierung entweder akkreditierte Zeitstempel verwenden müssen oder die Möglichkeit eröffnen müssen, diesen Zeitstempeltyp zu wählen.

Die Erfüllung dieser Anforderung ist in der in Kap. 4.3 beschriebenen Verfahrensvariante nicht festgelegt, aber möglich.

4.2 Authentizitätssicherung

Der Entwurf berücksichtigt, dass die erforderlichen Verifikationsdaten zu dem Zeitpunkt, zu dem das qualifiziert signierte Dokument benötigt wird, nicht mehr verfügbar sein können. Daher spezifiziert er ein Verfahren, die Signaturen bei der Aufnahme ins Archiv zu prüfen, die erforderlichen Verifikationsdaten zu erheben, als unsignierte Attribute der Signatur hinzuzufügen und dann später mit einer ersten erneuten Signatur zu sichern. Hierfür hat die vorhergehende rechtliche Analyse ergeben, dass die folgenden Anforderungen erfüllt werden müssen.

1. Gültigkeitsabfragen

Für die Prüfung der Signatur sind geeignete automatisierte Gültigkeitsabfrage nach § 5 Abs. 1 Satz 2 SigG durchzuführen. Dies wird in Kap. 3.3.2 berücksichtigt, indem OCSP-Responses abgespeichert werden können und im SigG-Profil in Kapitel 6.2., indem ein OCSP gefordert und eine Sperrliste CRL ausgeschlossen wird.

2. SigG-konformes Gültigkeitsmodell

Für die Prüfung der Signatur ist ein mit § 19 Abs. 5 SigG zu vereinbarendes Gültigkeitsmodell anzuwenden. Dies berücksichtigt der Entwurf insofern, als er in Kap. 3.3.1 auf den Zeitpunkt der Signaturerzeugung oder einen anderen beweisrelevanten Zeitpunkt in der Vergangenheit abstellt. Zu den verschiedenen Gültigkeitsmodellen äußert er sicht nicht explizit. In Kap. 3.3.2 lässt er diese Frage offen. Kap. 6.1 fordert er ein mit dem Signaturgesetz vereinbares Gültigkeitsmodell.

3. Prüfung nach dem gleichen Gültigkeitsmodell

Zertifikate, die nach dem einen Gültigkeitsmodell gültig sind, können nach einem anderen Gültigkeitsmodell ungültig sein. Wenn etwa ein Nutzer-Zertifikat ausgestellt wurde, für das zwar das Zertifikat des Zertifizierungsdiensteanbieters noch gültig ist, nicht aber mehr dessen Zertifikat, dann ist das Nutzerzertifikat nur nach dem Kettenmodell, nicht aber nach dem Schalenmodell gültig. Das Gleiche kann für die Gültigkeitsprüfung bei

der Erhebung der Verifikationsdaten vor der Archivierung gelten. Signaturen, die nach dem Kettenmodell gültig sind, können nach dem Schalenmodell ungültig sein. Daher muss eine spätere Prüfung immer nach dem gleichen Gültigkeitsmodell wie die früheren Prüfungen erfolgen können. Diese Forderung ist in Kap. 6.1 aufgenommen. Die Verwendung eines bestimmten Gültigkeitsmodells ist nicht vorgeschrieben.

4. Speicherung der erforderlichen Verifikationsdaten

Die erforderlichen Verifikationsdaten sind zu gewinnen, zu speichern und zu sichern, bevor sie nicht mehr verfügbar sind. Diese Forderung wird in Kap. 6.1 wiederholt.

In Kap. 3.4 ist vorgesehen, dass alle Zertifikate der Zertifikatkette einschließlich des Wurzelzertifikats aufbewahrt werden. Für die Gültigkeitsabfragen bezüglich der Zertifikate des Zertifizierungsdiensteanbieters und die verfügbaren Sperrlisten wird nur gefordert, dass sie gespeichert werden „sollen“. Die Gültigkeitsabfragen der Zertifikate bezüglich der OCSP-Antworten sind nicht aufgenommen.

In der SigG-Profilierung in Kap. 6.2 werden die erforderlichen Verifikationsdaten dahingehend spezifiziert, dass

- das Zertifikat des Signaturschlüssel-Inhabers und darauf bezogene Attributzertifikate,
- das Zertifikat des Zertifizierungsdiensteanbieters und
- die OCSP-Abfragen zu dem Zertifikat des Signaturschlüssel-Inhabers und darauf bezogenen Attributzertifikate

in den Signaturen aufbewahrt werden müssen. In Zeitstempeln müssen ebenfalls die Signaturschlüssel-Zertifikate integriert werden. Root-Zertifikate sollten aufbewahrt werden. Weitere Verifikationsdaten, wie die OCSP-Abfragen zu Zertifikaten des Zertifizierungsdiensteanbieters und der Root, werden nicht gefordert.

Die Beschränkung auf diese Verifikationsdaten ist verhältnismäßig und vertretbar. Die Zertifikate der qualifizierten und akkreditierten Zertifizierungsdiensteanbieter und erst Recht die Zertifikate der Root werden jeweils für eine längere Zeit von vielen Signaturschlüssel-Inhabern in unzähligen Signaturen verwendet und immer wieder geprüft. Sie sind daher auch noch nach vielen Jahren an vielen Stellen verfügbar. Die vorzeitige Sperrung eines solchen Zertifikats wegen Schlüsselmissbrauch oder -kompromittierung würde europaweit bekannt gemacht. Daher erscheint es übertrieben und unverhältnismäßig, diese Verifikationsdaten für jede einzelne Signatur zu erheben und aufzubewahren. Insoweit ist es vertretbar, diese Forderung nicht für ISIS-MTT-konforme Produkte zu erheben. Archivbetreibern sollte empfohlen werden, diese Verifikationsdaten für ihr gesamtes Archiv einmalig zu sammeln, so dass in einem Streitfall auf diese Sammlung zurückgegriffen werden kann. Diese Empfehlung betrifft jedoch nicht die in dem Entwurf zu spezifizierenden Produkte.

4.3 Daten- und Geheimnisschutz

Der Entwurf berücksichtigt Datenschutzanforderungen nicht explizit, spezifiziert aber den Standard so, dass die identifizierten Anforderungen – soweit möglich – erfüllt werden.

1. Löschen einzelner Dokumente

Bei Zweckerreichung und auf Anforderung eines Betroffenen muss es möglich sein, einzelne Dokumente aus dem Archiv zu löschen, ohne dass dadurch die Prüfung der ursprünglichen Signaturen anderer Dokumente beeinträchtigt wird. Indem der Entwurf in Kap. 4.4 die Verwendung oder Erzeugung von Hashwerten, deren Verbindung zu Hashbäumen und deren Neusignierung durch Archivzeitstempel vorsieht, erfolgt in dem Fall, dass Signaturverfahren ihre Eignung verlieren, die Neusignierung unabhängig von den einzelnen Dokumenten. Obwohl der Hashbaum auch das gelöschte Dokument beinhaltet, kann ein Dokument gelöscht werden, ohne die Prüfbarkeit der verbliebenen Signaturen zu beeinträchtigen.[39]

Werden die Algorithmen und zugehörigen Parameter von Hashverfahren ungeeignet, sind nach Kap. 4.4 alle betroffenen Dokumente neu zu hashen und die Hashbäume neu aufzubauen und zu signieren. In diesem Fall wird der neue Hausbaum ohne den Hashwert des gelöschten Dokuments aufgebaut, so dass dessen Löschung die Prüfbarkeit der anderen signierten Dokumente nicht behindern kann.

Die vom Bundesamt für die Sicherheit in der Informatik entworfene Signaturinteroperabilitätsspezifikationen (SigI) entspricht in ihrem Konzept für eine erneute elektronische Signatur[40] nicht diesen Anforderungen. Sie führt bei wiederholter Neusignierung mehrerer Dokumente zu einer Datenstruktur, die verhindert, dass das Löschen einzelner Dokumente ohne Verlust des Beweiswertes aller mitsignierten Dokumente möglich ist.

Für die in Kap. 4.3 beschriebene Verfahrensvariante ist eine gemeinsame Neusignierung mehrerer Dokumente nicht möglich. Insofern ist für diese Variante das Löschen eines Dokuments für die anderen Dokumente irrelevant.

2. Veränderungen in einem Dokument

Auf Anforderung eines Betroffenen muss es möglich sein, in einem Dokument Teile zu berichtigen, zu ergänzen, zu löschen oder zu sperren, ohne die Prüfung der anderen signierten Dokumente zu beeinträchtigen. Dies ist aufgrund der unter 1. beschriebenen Verfahren möglich.

3. Zugangs- und Zugriffsschutz

Maßnahmen des Zugangs- und Zugriffsschutzes werden in dem Entwurf nicht spezifiziert. Diese nach deutschem Datenschutzrecht notwendigen Maßnahmen müssen nicht durch Produkte zur Langzeitaufbewahrung von qualifizierten Signaturen gewährleistet

---

39 S. hierzu näher *Brandner/Pordesch*, DuD 2003, 354.

40 *BSI*, Signaturinteroperabilitätsspezifikationen, Abschnitt B5.

werden, sondern sind sinnvoller Weise im Rahmen des Archivierungssystems zu realisieren.

4. Verschlüsselung der Dokumente

Da die elektronisch signierten Dokumente personenbezogene Daten enthalten, für die Aufbewahrung von Dokumenten, die Berufs-, Amts-, Geschäfts- und andere rechtlich geschützte Geheimnisse enthalten, geeignet sein sollen und auch die Auslagerung der Aufbewahrung zu Dritten (Dienstleistern) ermöglichen sollen, muss es möglich sein, sie zu verschlüsseln, ohne dadurch die Neusignierung und die Prüfung der Signaturen zu beeinträchtigen. Notwendige Voraussetzung für die Anwendung der Verschlüsselung im Zusammenhang mit der Neusignierung ist, dass zweifelsfrei nachweisbar ist, dass die verschlüsselten Daten, die erneut signiert wurden, das signierte Dokument repräsentieren. Es muss also sowohl der Verschlüsselungsschlüssel als auch das angewendete Verschlüsselungsverfahren nachweisbar sein. Diese Anforderungen werden durch das in Kap. 4.4 beschriebene Verfahren für den Fall erfüllt, dass Signaturen neu signiert werden müssen.[41]

Werden die Algorithmen und zugehörigen Parameter von Hashverfahren ungeeignet, sind allerdings nach Kap. 4.4 alle betroffenen Dokumente neu zu hashen und die Hashbäume neu aufzubauen und zu signieren. In diesem Fall ist es unvermeidlich, die betroffenen Dokumente zu entschlüsseln, neu zu hashen und danach neu zu verschlüsseln. In diesem Fall sind spezifische zusätzliche Sicherungsmaßnahmen notwendig, um die Geheimnisse zu schützen.

5. Ergebnis

Der Entwurf entspricht deutschem und europäischem Signaturrecht und erfüllt die Anforderungen an den Schutz der informationellen Selbstbestimmung und rechtlich geschützter Geheimnissen in dem möglichen Umfang, wenn das SigG-Profil gewählt wird.

(Prof. Dr. Alexander Roßnagel)

41 S. näher *Fischlin./Pordesch*, DuD 2004, 163.

Verwendete Literatur

Bieser, W./Kersten, H., Elektronisch unterschreiben. Die digitale Signatur in der Praxis, 2. Aufl., Heidelberg 1999.

Bizer, J.: Elektronische Signaturen im Rechtsverkehr, in: Kröger, D./Gimmy, M. (Hrsg.), Handbuch zum Internetrecht, Berlin u.a., 2. Auflage, 2002, 41.

Bizer, J./Hammer, V./Pordesch U.: Gestaltungsvorschläge zur Verbesserung des Beweiswerts digital signierter Dokumente, in: *Pohl, H./Weck, G.* (Hrsg.), Beiträge zur Informationssicherheit, München 1995, 99.

Borges, G.: Verträge im elektronischen Geschäftsverkehr, München 2003.

Brandner R./Pordesch U.: Konzept zur signaturgesetzkonformen Erneuerung qualifizierter Signaturen, DuD 2003, 354.

Brandner, R./Pordesch, U./Roßnagel, A./Schachermayer, J.: Langzeitsicherheit qualifizierter elektronischer Signaturen, DuD 2002, 97.

Büger, M./Esslinger, B./Koy, H.: Das deutsche Signaturbündnis, DuD 2004, 133.

Bundesamt für die Sicherheit in der Informationstechnik (BSI), Signaturinteroperabilitätsspezifikationen, Abschnitt B5 Mehrfachsignaturen / Erneute Signatur, Version 1.2, 30.8.1999.

Fischer-Dieskau, S./Gitter, R./Paul, S./Steidle, R.: Elektronisch signierte Dokumente als Beweismittel im Zivilprozess, MMR 2002, 709.

Fischer-Dieskau, S./Roßnagel, A./Steidle, R.: Beweisführung am seidenen Bit-String? – Die Langzeitaufbewahrung elektronischer Signaturen auf dem Prüfstand, MMR 2004, 451.

Fischer-Dieskau, S./Roßnagel, A./Steidle, R./Pordesch, U.: Rechtliche Rahmenbedingungen und Anforderungen, in: Roßnagel, A./Schmücker, P. (Hrsg.), Langzeitarchivierung elektronisch signierter Dokumente, 2004, i.E.

Fischlin, M./Pordesch, U.: Nichtabstreitbarkeit trotz Verschlüsselung, DuD 2004, 163.

Frye, C./Pordesch, U.: Berücksichtigung der Sicherheitseignung von Algorithmen qualifizierter elektronischer Signaturen, DuD 2003, 73

Heibey, W.: Datensicherung, in: Roßnagel, A. (Hrsg.), Handbuch Datenschutzrecht, München 2003, Kap. 4.5.

Hously, R./Polk, W./Ford, W./Solo, D.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280, April 2002.

International Telecommunication Union - Telecommunication Sector (ITU-T): ITU-T Recommendation X.509 - Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 06/1997 (= ISO/IEC 9594-8), Entwurf 1997.

provet/GMD: Die Simulationsstudie Rechtspflege, Eine neue Methode zur Technikgestaltung für Telekooperation, Berlin 1994.

Regulierungsbehörde für Telekommunikation und Post: Frequently Asked Questions (FAQ), Antwort Nr. 14: Das „deutsche Verfahren" nach der Signaturgesetz unterscheidet sich angeblich im „Gültigkeitsmodell" von den bisher eingesetzten, was bedeutet das?, www.regtp.de (Stand 29.7.2004).

Roßnagel, A.: Einleitung ins Signaturgesetz, in: ders. (Hrsg.), Recht der Multimediadienste, München 1999 ff. (Loseblatt).

Ders., Das neue Recht elektronischer Signaturen. Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO, NJW 2001, 1817.

Ders., Die neue Signaturverordnung, BB 2002, 261.

Ders., Rechtliche Unterschiede von Signaturverfahren, MMR 2002, 218.

Roßnagel, A./Fischer-Dieskau, S.: Automatisiert erzeugte elektronische Signaturen, MMR 2004, 133.

Roßnagel, A./Fischer-Dieskau, S./Brandner, R./Pordesch, U., Die Erneuerung elektronischer Signaturen, CR 2003, 301.

Roßnagel, A./Pfitzmann, A., Der Beweiswert von E-Mail, NJW 2003, 1209.

Roßnagel, A./Pordesch, U.: Kommentierung von § 17 SigV, in: Roßnagel, A. (Hrsg.), Recht der Multimediadienste, München 2004.

Wedde, P.: Rechte der Betroffenen, in: Roßnagel, A. (Hrsg.), Handbuch Datenschutzrecht, München 2003, Kap. 4.4.