STEFANIE FISCHER-DIESKAU / ALEXANDER ROßNAGEL / ROLAND STEIDLE

Beweisführung am seidenen Bit-String? – Die Langzeitaufbewahrung elektronischer Signaturen auf dem Prüfstand

Seit über zehn Jahren wird in der rechtswissenschaftlichen Literatur der Beweiswert elektronischer Signaturen diskutiert. Alle bisherigen Abhandlungen sind jedoch rein theoretischer Natur. Auch beschäftigen sie sich nur mit einem Teil der Problematik, indem sie lediglich einen relativ kurzen Zeitpunkt nach der Signaturerzeugung betrachten. Praktische Erfahrungen mit der Beweisführung mittels elektronisch signierter Dokumente fehlen vollständig. Im Forschungsprojekt „ArchiSig" konnten nun erstmals praktische Erfahrungen gewonnen werden, die zur Schließung beider Lücken beitragen können. Der vorliegende Aufsatz stellt die aus einer Simulationsstudie gewonnenen Erkenntnisse tatsächlicher Beweiserhebungen mit elektronisch signierten Dokumenten dar und zeigt Konsequenzen für die sichere Langzeitaufbewahrung auf.

I. Simulationsstudie als Methode der praktischen Erfahrungsgewinnung

Elektronische Signaturen sind ein geeignetes Mittel für eine rechtssichere und beweiskräftige elektronische Kommunikation.[1] Daher hat der Gesetzgeber mit dem SigG erforderliche Rahmenbedingungen für das Angebot elektronischer Signaturen, mit dem Formanpassungsgesetz, dem Dritten Verwaltungsverfahrensänderungsgesetz und anderen Gesetzen Regeln für die Verwendung elektronischer Signaturen und mit § 292a ZPO eine Regelung für die Beweisführung mit elektronisch signierten Dokumenten festgelegt. Für die Langzeitsicherung elektronischer Signaturen hat der Verordnungsgeber darüber hinaus in § 17 SigV ein bestimmtes Verfahren normiert. Bisher stehen noch alle auf elektronischen Signaturen basierenden Verwendungskonzepte, insbesondere aber solche zur Langzeitaufbewahrung elektronisch signierter Dokumente vor dem Problem, dass sie die Geeignetheit ihrer Konzepte zur Beweissicherung behaupten, aber bisher keinen praktischen Nachweis führen konnten. Vor allem für langfristig aufbewahrte elektronisch signierte Dokumente wird dies erst nach Jahren und Jahrzehnten möglich sein. Gelingt der Nachweis dann jedoch nicht, sind die Investitionen vertan und die Schäden nicht mehr rückgängig zu machen.

Um in einer solchen Situation dennoch praktische Erfahrungen zu gewinnen und die erforderliche Bewertungssicherheit zu erlangen, bietet sich die Durchführung von Simulationsstudien an.[2] Hierbei werden unter Einbeziehung von Experten zukünftige Fallgestaltungen unter möglichst realen Bedingungen „durchgespielt".[3] Die Simulationsstudie „ArchiSig" verfolgte das Ziel, den prozessualen Beweiswert langfristig aufbewahrter elektronisch signierter Dokumente zu bestimmen. Dementsprechend wurden die vom Projekt entwickelten Konzepte zur Langzeitarchivierung in zwölf Prozessen mit simulierten Fallgestaltungen von Richtern, Anwälten und Gutachtern praktisch überprüft. Unter Zugrundelegung eines Zeitraffers, wonach Jahre durch Tage abgebildet wurden, waren in allen Prozessen elektronisch signierte Dokumente streitentscheidend.[4] In diesen ersten (simulierten) Prozessen mit Beweisaufnahmen über elektronisch signierte Dokumente konnten Erfahrungen hinsichtlich folgender Fragen gewonnen werden: Eignung signierter Dokumente zur Beweisführung, Anwendbarkeit des § 292a ZPO, Auswirkungen des § 17 SigV auf den Beweiswert, erforderliche Verifikationsdaten zum Nachweis der Authentizität nach langer Zeit. Bereits bekannte Probleme elektronischer Signaturen, insbesondere die Autorisierung mittels Besitz und Wissen[5] und die Präsentationsproblematik[6] waren nicht Thema der Studie und wurden daher nicht weiter erörtert.

II. Beweisführung mit elektronisch signierten Dokumenten

Ausgangspunkt für die Beweisführung mit elektronisch signierten Dokumenten ist zunächst § 292a ZPO. Dieser bietet eine Beweiserleichterung durch einen Anscheinsbeweis für die Echtheit (Authentizität und Integrität) mindes-

1) *Roßnagel/Pfitzmann*, NJW 2003, 1209; *Mankowski*, CR 2003, 44.
2) Zur Simulationsstudie als Methode s. z.B. *Roßnagel*, Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin, 1993, S. 185; *ders.*, Simulationsstudien als Methode der Technikgestaltung, in: Müller/Stapf (Hrsg.), Mehrseitige Sicherheit, Bd. 2, 1988, S. 323 ff.; *Hammer*, Simulationsstudie im Prozess der Technikgestaltung, in: *BSI*, Computersimulation: (K)ein Spiegel der Wirklichkeit, 1994, S. 126 ff.; *Kumbruck*, Angemessenheit für situierte Kooperation – Ein Kriterium arbeitswissenschaftlicher Technikforschung und -gestaltung, 1999; *Pordesch*, Die elektronische Form und das Präsentationsproblem, 2002, S. 276 ff.
3) Simulationsstudien wurden erfolgreich eingesetzt im Bereich der Rechtspflege – s. *provet/GMD*, Die Simulationsstudie Rechtspflege – Eine neue Methode zur Technikgestaltung für Telekooperation, 1994; im Bereich der Vorgangsbearbeitung – s. *provet/GMD*, Rechtsverbindliche Telekooperation in der elektronischen Vorgangsbearbeitung, GMD-Studien Nr. 235, 1995; im Bereich des Gesundheitswesens – s. *Roßnagel/Haux/Herzog* (Hrsg.), Mobile und sichere Kommunikation im Gesundheitswesen, 1998; und im Bereich des E-Commerce – s. *Roßnagel* (Hrsg.), Datenschutz beim Online-Einkauf, 2002.
4) Die Simulationsstudie wurde von der *Projektgruppe verfassungsverträgliche Technikgestaltung* (*provet*) der Universität Kassel und dem FhG-Institut für sichere Telekooperationstechnik (*SIT*) durchgeführt.
5) S. z.B. *Albrecht*, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, 2003.
6) S. z.B. *Pordesch* (o. Fußn. 2).

■ Prof. Dr. Alexander Roßnagel ist Universitätsprofessor für öffentliches Recht an der Universität Kassel, dort Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet), und wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR), Saarbrücken. Stefanie Fischer-Dieskau und Roland Steidle sind wissenschaftliche Mitarbeiter in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet).
Dieser Beitrag entstand i.R.v. Forschungsarbeiten des Projekts „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente", das vom *Bundesministerium für Wirtschaft und Arbeit* i.R.d. Wettbewerbs „VERNET" unter dem Förderkennzeichen „01MS121" gefördert wurde.

tens entsprechend § 126a BGB qualifiziert signierter Dokumente, wenn sich die Echtheit auf Grund einer Prüfung nach dem SigG ergibt. Dies bedeutet, dass der Anscheinsbeweis überhaupt erst dann zum Tragen kommt, wenn eine Prüfung der signaturrechtlichen Vorschriften ergibt, dass eine ordnungsgemäße qualifizierte Signatur vorliegt. Erst dann sieht das Gesetz vor, dass dieser Anschein nur noch durch Tatsachen erschüttert werden kann, die ernstliche Zweifel an der willentlichen Abgabe der Erklärung durch den Signaturschlüsselinhaber begründen.[7] Solche können sich z.B. aus der Autorisierungs- oder Präsentationsproblematik ergeben.

Das Vorliegen einer akkreditierten oder qualifizierten elektronischen Signatur begründet somit aus sich heraus nicht automatisch das Vorliegen der Voraussetzungen des Anscheinsbeweises. Vielmehr müssen sich diese erst aus der Prüfung der Signatur nach dem SigG ergeben. Ist ihr Vorliegen vor Gericht zwischen den Parteien unstreitig, hat das Gericht dies als Tatsache in seine Beweiswürdigung und Entscheidung einzubeziehen.[8] Ist die Signaturstufe jedoch strittig, so muss der Beweisführer ihr Vorliegen zur Überzeugung des Gerichts nachweisen.[9] Hierbei kommen ihm Vorteile, die sich aus der Akkreditierung eines Zertifizierungsdiensteanbieters ergeben, zugute. Die Aufbewahrungsfristen hinsichtlich Verzeichnisdienst und Dokumentation von 30 Jahren wie auch das Zertifikat der *Reg TP* als Wurzelinstanz erleichtern eine dauerhafte Nachweisführung der Echtheit des Zertifikats.[10] Insbesondere erleichtert jedoch die Sicherheitsvermutung nach § 15 Abs. 1 Satz 4 SigG dem Beweispflichtigen die Nachweisführung beim Vorliegen akkreditierter Signaturen.[11] Mit ihrer Hilfe kann er die technisch-organisatorische Sicherheit des Zertifizierungsdiensteanbieters nachweisen, die er für das Vorliegen eines qualifizierten Zertifikats gem. § 2 Nr. 3a) und Nr. 7 SigG darlegen muss. Zwar kann auch diese Vermutung widerlegt werden, doch sind hieran entsprechend den Grundsätzen des Anscheinsbeweises hohe Anforderungen zu stellen.

Die tatbestandlichen Voraussetzungen des § 292a ZPO müssen somit immer, unabhängig von der verwendeten Signaturstufe, vom Beweisführer nachgewiesen werden. Je höher die Stufe, umso leichter mag ihm dieser Beweis gelingen, umso größer ist somit die damit verbundene Rechtssicherheit. Ein Automatismus zur Anwendung des § 292a ZPO besteht jedoch bei keiner Signaturstufe.

III. Beweisführung nach vielen Jahren

Nach § 6 Abs. 1 Satz 2 SigG ist der Nutzer eines Signaturschlüssels bereits bei der Antragstellung für ein qualifiziertes Zertifikat darauf hinzuweisen, dass elektronische Signaturen ihren Sicherheitswert durch Zeitablauf verlieren können und bei Bedarf eine Neusignierung vorzunehmen ist. Wie diese zu erfolgen hat, ergibt sich aus § 17 SigV. Danach ist eine Neusignierung vorzunehmen, wenn die Signaturen für längere Zeit benötigt werden, „als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind". In diesem Fall sind „die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten Signatur zu versehen", die mit „geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen" muss.

1. Das Zusammenspiel von § 17 SigV mit § 292a ZPO

Der Anschein der Echtheit einer qualifiziert signierten Erklärung nach § 292a ZPO setzt voraus, dass er sich aus einer „Prüfung nach dem Signaturgesetz" ergibt. Fraglich ist, ob eine Neusignierung Gegenstand dieser Prüfung und somit Voraussetzung zur Anwendbarkeit des § 292a ZPO ist und wie § 17 SigV zu verstehen ist.

a) Praxisgerechte Auslegung von § 17 SigV

Der Auslegung von § 17 SigV kommt in den von „ArchiSig" entwickelten Konzepten[12] eine entscheidende Rolle zu. Sie ist in einem Gerichtsprozess, dessen Ausgang von einem neu signierten Dokument abhängt, entscheidend. Grundlage der prototyptechnischen Umsetzung und Gegenstand der Evaluierung waren die von „ArchiSig" entwickelten Konzepte, die auf einer praxisgerechten Auslegung dieser Vorschrift beruhen.

Vor allem zwei Aspekte der Auslegung des § 17 SigV wurden in der Simulationsstudie überprüft. Zum einen war zu klären, was genau nach § 17 Satz 2 SigV unter den „Daten" zu verstehen ist, die nach Ablauf der Sicherheitseignung der Algorithmen oder Parameter neu zu signieren sind. Zum anderen war zu prüfen, ob – wie der Wortlaut des § 17 SigV allein nahe legt – eine neue qualifizierte Signatur „und" ein qualifizierter Zeitstempel zur Neusignierung erforderlich sind, selbst wenn der verwendete qualifizierte Zeitstempel bereits eine qualifizierte Signatur beinhaltet.

Unter der Voraussetzung, dass der Sicherheitswert elektronischer Signaturen technisch erhalten bleiben muss, kann angenommen werden, dass unter den „Daten" nicht nur die ursprünglichen Originaldateien gemeint sind, sondern dass an deren Stelle auch ein eindeutiger Repräsentant wie der Hash-Wert der Originaldatei neu signiert werden kann, solange die Eindeutigkeit durch die Sicherheitseignung der Hash-Algorithmen gewährleistet bleibt.[13] Für die Neusignierung genügt ein qualifizierter Zeitstempel, wenn dieser zugleich eine qualifizierte Signatur beinhaltet. Eine zu einem solchen Zeitstempel zusätzliche Signatur würde kein Mehr an Sicherheit erreichen, sondern lediglich den Vorgang der Neusignierung unnötig verkomplizieren.[14] Beide Auslegungen fanden die Zustimmung sowohl der technischen Sachverständigen als auch der Richter und Rechtsanwälte.

b) Einhaltung des § 17 SigV als Voraussetzung für § 292a ZPO

In allen entschiedenen Fällen wurde die Erfüllung der Voraussetzungen des § 17 SigV als notwendige Voraussetzung und Bestandteil der Prüfung nach dem SigG i.R.v. § 292a ZPO angesehen. War § 17 SigV tatbestandsmäßig nicht erfüllt, wurde gefolgert, dass eine nach § 292a ZPO

---

7) *Fischer-Dieskau/Gitter/Paul/Steidle*, MMR 2002, 709; *Roßnagel*, MMR 2002, 215; *Jungermann*, DuD 2003, 69; *Borges*, Verträge im elektronischen geschäftsverkehr, 2003, S. 505 ff.

8) S. allg. zur Beweisbedürftigkeit *Thomas/Putzo*, 24. Aufl., 2002, Vor § 284, Rdnr. 1.

9) *Fischer-Dieskau/Gitter/Paul/Steidle*, MMR 2002, 709.

10) *Roßnagel*, MMR 2002, 215.

11) BT-Drs. 14/4662, S. 28; *Roßnagel*, NJW 2001, 1817.

12) S. zu den technischen Konzepten *Brandner/Pordesch*, DuD 2003, 354, und *Frye/Pordesch*, DuD 2003, 73.

13) *Roßnagel/Fischer-Dieskau/Pordesch/Brandner*, CR 2003, 301; *Brandner/Pordesch*, DuD 2003, 354; *Roßnagel/Pordesch*, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, § 17 SigV Rdnr. 49.

14) S. zu dieser teleologischen Reduktion *Brandner/Pordesch/Roßnagel/Schachermayer*, DuD 2002, 97; *Roßnagel/Pordesch* (o. Fußn. 13), § 17 SigV Rdnr. 54.

notwendige Voraussetzung des Anscheins, „der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt", nicht vorlag. § 17 SigV wurde einhellig nicht nur als ein mögliches Verfahren zur Datensicherung, sondern vielmehr als Bestandteil des gesamten Signaturrechts, das Einfluss auf die Beweisführung hat, angesehen. Dies hat zur Folge, dass eine andere, nicht den Voraussetzungen des § 17 SigV entsprechende Neusignierung die Anwendung des Anscheinsbeweises im Prozess verhindert.[15]

2. Erforderliche Verifikationsdaten und § 292a ZPO

Vor der Bestimmung der erforderlichen Verifikationsdaten für die dauerhafte Nachweisführung der Authentizität eines elektronisch signierten Dokuments steht die Frage, welche Verifikationsdaten überhaupt für den Authentizitätsnachweis erforderlich sind. Diese hat in der rechtswissenschaftlichen Diskussion bisher sehr wenig Beachtung gefunden. In den simulierten Rechtsstreitigkeiten musste daher auch überprüft werden, welche Verifikationsdaten zum Nachweis der Authentizität erforderlich sind. Da diese Frage nicht unmittelbar geregelt ist, musste eine Antwort mittelbar aus dem Zweck der Verifikationsdaten und den für sie bestehenden Regelungen gewonnen werden. Auf diesem Weg wurden Konzepte entwickelt, welche Verifikationsdaten notwendig sind und daher im Fall ihres Fehlens vor dem Einbringen des elektronischen Dokuments in ein Archiv noch eingeholt werden müssen. Diese Konzepte müssen berücksichtigen, dass mit Blick auf die dauerhaft mögliche Nachweisführung je nach Signaturstufe Jahre nach der Signaturerstellung nicht mehr gewährleistet ist, dass der Zertifizierungsdiensteanbieter seine vollständigen Dokumentationen noch vorrätig hat, Zertifikate noch nachprüfbar oder überhaupt noch existent sind.[16]

a) Die Konzeption für die langfristige Aufbewahrung

Auf Grund des nahezu unüberschaubaren Umfangs möglicher Verifikationsdaten[17] ist eine Risikoabwägung[18] vorzunehmen, welche Verifikationsdaten mit den Signaturen aufbewahrt und neu signiert werden sollen. Im Regelfall dürfte es zumindest für Zertifikate akkreditierter Zertifizierungsdiensteanbieter zum Nachweis der Authentizität ausreichen, lediglich die Zertifikatsketten zum Nutzerzertifikat und der OCSP-Response[19] zum Nutzerzertifikat einzuholen. Bedenkt man den hohen Sicherheitsstandard akkreditierter Zertifizierungsdiensteanbieter, so erscheint es im Regelfall vertretbar, die Gültigkeit der Zertifikate der Diensteanbieter auf die OCSP-Response nicht zu überprüfen und aufzubewahren. Unregelmäßigkeiten bei einem akkreditierten Zertifizierungsdiensteanbieter werden ein öffentliches Aufsehen hervorrufen, das auch nach Jahren noch festgestellt werden kann.

Darüber hinaus wird für den Empfänger das zeitnahe Einholen eines Zeitstempels zur Signaturerstellung empfohlen, um auf einen gesicherten Referenzzeitpunkt für die spätere Überprüfung der Signatur zurückgreifen zu können. Fehlt ein solch zeitnaher Zeitstempel, so kann bei einer zwischenzeitlich eingetretenen Ungültigkeit des Zertifikats gegebenenfalls nicht mehr nachgewiesen werden, dass das Zertifikat bei Signaturerstellung noch gültig war.

b) Erfahrungen und Schlussfolgerungen

Die Simulationsstudie hat folgende Erkenntnisse gebracht: Die an sich sehr komplexe individuelle Risikoabwägung, die auf Grund des Fehlens klarer Vorgaben erforderlich ist, wird durch zwei Aspekte entschärft. Zum einen ermöglichen die für die Zertifizierungsdiensteanbieter geltenden langen Aufbewahrungsfristen ein nachträgliches Einholen und Prüfen der Verifikationsdaten. Zum anderen wurde dem Wurzelzertifikat der *Reg TP* mit dem im Bundesanzeiger veröffentlichten und daher nachprüfbaren öffentlichen Schlüssel von allen Beteiligten großes Vertrauen entgegengebracht.[20] Grundsätzlich kann daher in Langzeitarchiven nach dem vorgestellten Konzept verfahren werden. Auf Grund vielfältiger spezifischer Risikosituationen sollten Verifikationsroutinen, aber auch Archivierungssysteme in jedem Fall so gestaltet sein, dass sie entsprechend der jeweiligen Risikoabwägung eine individuelle Skalierbarkeit ermöglichen.

IV. Beweiswürdigung nach § 286 ZPO

Die Nichtanwendbarkeit des § 292a ZPO führte in keinem Fall dazu, dass ein elektronisch signiertes Dokument von den Teilnehmern im Prozess als beweisrechtlich unerhebliches „Nullum" behandelt wurde. Vielmehr zeigte sich, dass ein „fehlerhaft"[21] aufbewahrtes Dokument dann allein i.R.d. freien richterlichen Beweiswürdigung nach § 286 ZPO zu beurteilen ist. Dabei war es allerdings je nach Fallkonstellation vom Vorliegen weiterer unterstützender Tatsachen abhängig, ob der Beweis mit dem Dokument erbracht werden konnte oder auch nicht. Der Ausgang eines Prozesses war daher mit Unsicherheiten verbunden. Das Fehlen einer Neusignierung nach § 17 SigV führte zu einem deutlich erhöhten Prozessrisiko.

Sofern Richter, Rechtsanwälte und Sachverständige elektronisch signierte Dokumente zu beurteilen hatten, kamen dabei – neben dem Fehlen erforderlicher Verifikationsdaten – vor allem Fälle der gar nicht durchgeführten Neusignierung sowie der zu spät erfolgten Neusignierung zur Entscheidung.

Bei der Beurteilung beweiserheblicher elektronisch signierter Dokumente, die nach Ablauf der Sicherheitseignung der Algorithmen gar nicht neu signiert wurden, standen die beteiligten Richter vor den größten Problemen. War die Signatur bereits so lange nicht neu signiert worden, dass die ursprünglich bei der Signaturerstellung verwendeten Algorithmen eine stark verminderte Sicherheitseignung aufwiesen und auch von Laien mit verhältnismäßig geringem Aufwand gebrochen werden konnten, so gelang es regelmäßig nicht mehr, die Authentizität und Integrität des Dokuments aus sich heraus nachzuweisen. Allerdings zeigte sich auch, dass die Richter trotzdem weite-

---

15) S. näher *Roßnagel/Schmücker* (Hrsg.), Beweiskräftige und sichere Langzeitaufbewahrung elektronisch signierter Dokumente, i.E.

16) Zertifizierungsdiensteanbieter mit Anbieterakkreditierung müssen ihre Dokumentation und die Zertifikate gem. § 8 Abs. 3 i.V.m § 4 Abs. 2 SigV mindestens 30 Jahre nach Ablauf des Jahres, in dem die Gültigkeit des Zertifikats endet, aufbewahren. Für qualifizierte Zertifizierungsdiensteanbieter gilt eine Aufbewahrungspflicht von mindestens fünf Jahren nach § 4 Abs. 1 SigV. Für Letztere ist bei Geschäftsaufgabe oder Insolvenz nicht einmal diese Aufbewahrungsdauer sichergestellt; s. *Roßnagel*, MMR 2002, 215.

17) Hierzu gehören insb. die Zertifikate bis zur Wurzelinstanz, Cross-Zertifikate, Gültigkeitsabfragen zu all diesen Zertifikaten, Zertifikate auf die Antworten zur Gültigkeitsabfrage (diese Prüfung ließe sich theoretisch unendlich fortsetzen) und Zeitstempel.

18) Die Risikoabwägung soll einen Ausgleich zwischen Kosten und Aufwand auf der einen Seite und der Bedeutung des archivierten Dokuments und der realistischen Durchsetzbarkeit möglicher Einwände gegen die Authentizität wegen eines fehlenden Verifikationsdatums auf der anderen Seite schaffen.

19) Online Certificate Status Protocol.

20) S. näher *Roßnagel/Schmücker* (o. Fußn. 15).

21) Fehlerhaft meint hier, dass gar keine, eine verspätete oder eine nicht § 17 SigV-konforme Neusignierung vorlag.

re Indizien zur Urteilsfindung heranzogen. Der technischen Prüfung folgte immer auch eine rechtliche Plausibilitätsprüfung. In einem Fall gar nicht erfolgter Neusignierung war beispielsweise der Streitwert gering und die schon ältere Klägerin hatte keinerlei Kenntnisse der Informatik. Daraus schloss das Gericht, dass die Klägerin die elektronische Signatur nicht gefälscht haben konnte. In der Regel konnte jedoch mit einem gar nicht neu signierten Dokument nicht mehr erfolgreich Beweis geführt werden.

Im Gegensatz dazu gelang dies wesentlich häufiger, wenn elektronische Signaturen „nur" zu spät neu signiert worden waren. In diesen Fällen war zunächst zu berücksichtigen, dass die Sicherheitseignung regelmäßig noch nicht derart gering war, dass eine Signatur ohne weiteres hätte gefälscht werden können. Der Ablauf der Sicherheitseignung ist nicht gleichbedeutend damit, dass nun schlagartig eine Signatur gebrochen werden kann.[22] Es zeigte sich bei der Beweiswürdigung auch, dass ein initialer Archivzeitstempel[23] nach Ablauf der Sicherheitseignung die Beweissituation verbessern konnte. So konnte ein initialer Archivzeitstempel zwar nicht die in der Vergangenheit unterlassene Neusignierung ausgleichen, jedoch konnte das Vorliegen des Dokuments zu einem bestimmten Zeitpunkt in der Vergangenheit nachgewiesen werden. Damit konnte der Zeitraum einer möglichen Fälschung – ab Ablauf der Sicherheitseignung bis zum initialen Archivzeitstempel – eingegrenzt werden. Eine Fälschung hätte dann nur in diesem Zeitraum stattfinden können. In diesem lag aber in den verhandelten Fällen meist noch gar kein Fälschungsinteresse oder gar ein anhängiger Prozess vor. Die beweisbelastete Partei hätte daher vielfach geradezu hellseherische Fähigkeiten besitzen müssen, um vorsorglich einzelne, im Archiv aufbewahrte Signaturen zu fälschen. Konnte dann noch festgestellt werden, dass die Sicherheitseignung bis zum Anbringen des Zeitstempels nur gering nachgelassen hatte und eine Manipulation nur äußerst schwierig möglich gewesen wäre, konnte i.R.d. freien Beweiswürdigung der Indizienschluss leichter oder eindeutiger gezogen werden.

Bei der Beweiswürdigung von fehlerhaft neu signierten Dokumenten spielte in den meisten Fällen das Verhältnis von Streitwert und Aufwand für eine Fälschung eine große Rolle. War die Sicherheitseignung von Algorithmen einer elektronischen Signatur nur kurze Zeit abgelaufen, so war es mit realistisch zu vertretendem Aufwand und Kosten noch gar nicht möglich, eine Signatur zu fälschen.[24] Sollte dies dennoch gelingen, so würde der enorme Aufwand zumindest in Fachkreisen bekannt werden und daher mit großer Wahrscheinlichkeit an die Öffentlichkeit kommen. Weiterhin war für die Beweiseinrede der Fälschung ein Fälschungsinteresse von entscheidender Bedeutung. Zu dessen Feststellung wurde einerseits auf die Bedeutung des Rechtsstreits für eine Partei und zum anderen auf ein Fälschungsmotiv und die subjektiven Fälschungsmöglichkeiten geachtet. War ein solches Fälschungsinteresse nicht plausibel, schlossen alle Richter eine Fälschung der Signatur aus. Letztlich entscheidend für den Ausgang des Prozesses waren somit die nachweisbaren Umstände des Einzelfalls, nicht allein die Qualität des aufbewahrten elektronisch signierten Dokuments.

Allein die Behauptung eines sicher geführten Archivs reichte nicht aus, eine fehlende Neusignierung „auszugleichen". In diesen Fällen forderte das Gericht den Nachweis der Sicherheit des Archivs wie auch die sichere Übermittlung des elektronischen Dokuments vom Archiv zum Gericht. Diese lückenlose Sicherheit und damit die Abwesenheit einer Fälschungsmöglichkeit kann eigentlich gar nicht nachgewiesen werden. Wer dies dennoch versucht, lädt sich die Last eines sehr hohen jahrelangen Dokumentations- und Protokollierungsaufwands auf.

Zusammenfassend kann festgehalten werden: Ein nicht oder fehlerhaft neu signiertes Dokument scheidet nicht von vornherein als Beweismittel aus. Ob der Beweis mit ihm gelingt, hängt jedoch von den nachweisbaren Umständen des jeweiligen Einzelfalls ab. Eine Rechtssicherheit lässt sich daher nicht in dem Umfang erreichen, wie dies mit dem Einsatz geeigneter Prozesse zur Neusignierung möglich ist.

V. Hinzuziehung Sachverständiger

Bei den in der Simulationsstudie verhandelten Fällen war es oftmals erforderlich, die technische Sicherheit elektronischer Signaturen durch Sachverständige beurteilen zu lassen. Dies war immer dann der Fall, wenn die – als zertifiziert angenommene – Prüfsoftware eine fehlerhafte Signatur oder Unregelmäßigkeiten anzeigte. Es stellte sich heraus, dass trotz konkreter Hinweise auf den Mangel der Signatur oder Neusignierung die Richter mangels Vertrauensanker (belastbares Prüfsoftwareergebnis) schnell das Einschalten eines Sachverständigen als notwendig ansahen. Dabei zeigte sich deutlich, dass selbst für mit Signaturfragen vertraute Richter die möglichen Fehlerquellen einer Neusignierung so komplex waren, dass eine eigene Bewertung der technischen Zusammenhänge nur noch schwer möglich und die technischen Sachverständigen spätestens bei Fragen hinsichtlich der Fälschungsmöglichkeit einer zu spät oder gar nicht neu signierten Signatur unverzichtbar waren. Bei der Einbeziehung der Sachverständigen war vor allem der Gesichtspunkt der Fälschungsmöglichkeit einer nicht ordnungsgemäß neu signierten Signatur von zentraler Bedeutung.

1. Schwierigkeiten bei der Beauftragung der Sachverständigen

Mit zunehmender Komplexität der technischen Sachverhalte wurde die Formulierung des Beweisthemas immer ungenauer. Mehrfach ließ das Gericht die Signatur generell hinsichtlich aller denkbaren Fälschungsmöglichkeiten durch den Sachverständigen untersuchen. Für diesen Zweck wurde ihnen umfangreiches Aktenmaterial zur Verfügung gestellt.[25] Ursächlich hierfür war vor allem die Unsicherheit des Gerichts, den Beweiswert eines elektronisch signierten Dokuments zu beurteilen. Auch ungenaue Fragestellungen aller Beteiligten in der mündlichen Verhandlung spiegelten bei fehlender Prüfunterstützung die Unsicherheit bei der Beurteilung der komplexen Technik wider.

Wie in anderen Prozessarten, z.B. dem Arzthaftungs- oder dem Baurecht, bei denen Rechtsstreite teilweise nur unter Hinzuziehung von Sachverständigen geführt werden können, war das Finden einer gemeinsamen Sprachenfür das

22) S. *Roßnagel/Pordesch* (o. Fußn. 13), § 17 SigV Rdnr. 47.

23) Bei Eingang eines Dokuments in ein Archiv wird vor der Archivierung ein erster (initialer) Archivzeitstempel angebracht. Dieser beinhaltet eine qualifizierte Signatur und erfüllt daher die Voraussetzungen einer Neusignierung nach § 17 SigV – s. *Brandner/Pordesch*, DuD 2003, 354.

24) Nach Ausführung der Sachverständigen bedingt eine Fälschung je nach Zeitablauf der Sicherheitseignung den Zusammenschluss mehrerer hundert oder tausend Rechner.

25) S. näher *Roßnagel/Schmücker* (o. Fußn. 15).

Verständnis aller Beteiligten untereinander schwierig. Auf der einen Seite hatten die Richter und Rechtsanwälte Schwierigkeiten, Beweisthemen gegenüber den Sachverständigen präzise zu formulieren. Auf der anderen Seite taten sich die Sachverständigen schwer, in einer für Juristen verständlichen Sprache ihre Gutachten zu formulieren und diese begrenzt auf die Fragestellung zu erläutern, ohne dabei eigene Wertungen zu treffen, die dem Urteil vorgreifen.

2. Abhängigkeit der Richter vom Urteil der Sachverständigen?

Im Anfangsstadium eines Prozesses bestand bei der Sachverhaltsermittlung oftmals ein starkes Abhängigkeitsverhältnis der Gerichte von den Sachverständigen. Dieses war umso stärker, je weniger sichere Anhaltspunkte für eine eigene Beurteilung der elektronischen Signatur bestanden. Sofern nicht wie bei akkreditierten Signaturen ein Vertrauensanker in Form eines Wurzelzertifikats der *Reg TP* vorlag, war die Einschaltung von Sachverständigen unumgänglich. Zwar nahmen alle Gerichte nach der Begutachtung durch Sachverständige eine eigene juristische Plausibilitätsprüfung anhand weiterer Indizien außerhalb der technischen Fragestellungen vor.[26] Die Materie ist daher grundsätzlich justiziabel. Jedoch besteht die Gefahr, dass stets ein Sachverständiger vorab eingeschaltet werden muss.

Daher kann das Prozessrisiko bei einem geringen Streitwert und hohen Kosten für einen Sachverständigen untragbar werden. Im Gegensatz zu Prozessen etwa im Baurecht oder im Arzthaftungsrecht, bei dem es regelmäßig um hohe Gegenstandswerte geht, ist dies bei Prozessen mit elektronisch signierten Dokumenten nicht ohne weiteres der Fall. Wirtschaftlich schwächere Parteien können sich ohne Prozesskostenhilfe einen Rechtsstreit, bei dem mit größter Wahrscheinlichkeit von vornherein absehbar ist, dass ein Sachverständiger hinzugezogen werden wird, nicht mehr leisten. Bei geringen Streitwerten steht daher zu befürchten, dass die grundgesetzlich zwar garantierte Möglichkeit, vor ein staatliches Gericht zu gehen, wegen wirtschaftlicher Erwägungen faktisch ausgehebelt wird. Die Verwendung elektronisch signierter Dokumente als Beweismittel kann somit ohne einfach überprüfbare Sicherheit elektronischer Signaturen zu einem faktischen Ausschluss der Rechtsweggarantie des Art. 19 Abs. 4 GG führen.[27]

3. Vermutungsregelungen und Zertifizierungen

Um die Abhängigkeit der Gerichte von Sachverständigen zu reduzieren, müssen den Gerichten zunächst belastbare Vermutungsregelungen wie § 15 Abs. 1 Satz 4 SigG zur Hand gegeben werden, mit denen sie selbst auch die Authentizität und Integrität eines elektronisch signierten Dokuments beurteilen können. Solche Vermutungsregelungen müssen sachlich begründet sein und setzen daher einen gewissen Sicherheitsstandard der verwendeten Signaturverfahren voraus, wie er in Deutschland derzeit für akkreditierte Signaturen gegeben ist.[28] Damit Vermutungsregelungen aber nicht eine Sicherheit suggerieren, die tatsächlich nicht besteht, muss im Auge behalten werden, dass diese nicht zu Gunsten jeglicher Signaturstufe angewendet werden. Denn in diesem Fall ist damit zu rechnen, dass die Vermutung mittels eines Sachverständigen leicht zu entkräften ist. Die Konsequenz wäre wiederum, dass in der Mehrzahl signaturrechtlicher Verfahren Sachverständige eingeschaltet werden müssen, mit der beschriebenen Beeinträchtigung der Rechtswegsgarantie.

Darüber hinaus sollten auch entsprechend § 17 SigG geprüfte und bestätigte Signaturerzeugungs- und Prüfkomponenten verwendet werden. Nur so können sich allgemein gültige Erfahrungswerte herausbilden, die Gerichte auch ohne Sachverständige ihren Entscheidungen zu Grunde legen können.

VI. Fazit

Die in „ArchiSig" erstmals durchgeführte praktische Überprüfung neu signierter elektronischer Dokumente hat gezeigt, dass mit den entwickelten Konzepten erfolgreich Beweis vor Gericht geführt werden konnte. Elektronisch signierte Dokumente mit fehlenden Verifikationsdaten oder mit fehlender, nicht rechtzeitig oder nicht § 17 SigV-konformer Neusignierung sind beweisrechtlich nicht wertlos. Für sie kann jedoch der Anscheinsbeweis nach § 292a ZPO nicht angewendet werden, sodass eine Beurteilung nur i.R.d. freien Beweiswürdigung unter Hinzuziehung zusätzlicher Beweismittel wie Anfragen beim Zertifizierungsdiensteanbieter oder Indizien außerhalb der Signatur vorgenommen werden kann. Dies führt zu Unsicherheiten für den Ausgang eines Verfahrens. Den Entwicklern und Anwendern von Archivierungssystemen ist daher zu empfehlen, Komponenten zur automatisierten Beschaffung von Verifikationsdaten und zur automatisierten Neusignierung der signierten elektronischen Dokumente nach den Konzepten von „ArchiSig" vorzusehen, wenn sie den Beweiswert der elektronisch signierten Dokumente erhalten wollen.

Nicht spezialisierte Richter und Rechtsanwälte werden mit Signaturprüfungen und ihrer Bewertung häufig überfordert sein, sodass die Hinzuziehung von Sachverständigen regelmäßig zu erwarten ist. Dagegen könnten belastbare Vermutungsregelungen sowie standardisierte und zertifizierte Anwendungskomponenten helfen, dem Gericht eine eigene Bewertung der Authentizität und Integrität eines elektronisch signierten Dokuments zu ermöglichen. Die Sorge, Gerichte würden sich zu stark von den Beurteilungen der Sachverständigen leiten lassen und keine juristische Plausibilitätsprüfung vornehmen, hat sich nicht bewahrheitet. Vielmehr ließen alle Richter eine große Ausgewogenheit und Umsicht, aber auch Aufgeschlossenheit erkennen.

Die Simulationsstudie als Methode, um bereits heute praktische Erfahrungen im Umgang mit Technik und Rechtsfragen der Zukunft zu gewinnen, hat sich zum wiederholten Mal bewährt. Sie sollte öfter genutzt werden, um Technikgestaltungen und Rechtsregeln zu überprüfen, solange noch Korrekturmöglichkeiten bestehen und bevor Fehlentwicklungen zu großen Schäden führen.

---

26) S. unter IV.

27) S. hierzu schon *Roßnagel*, Digitale Unterschriften und Verfassungsverträglichkeit, in: Reimer/Struif (Hrsg.), Kommunikation und Sicherheit, 1992, S. 40 ff.

28) *Roßnagel*, MMR 2000, 451; *ders.*, MMR 2002, 215.