Zur Archivfähigkeit digitaler Signaturen in elektronischen Registern

Von Frank M. Bischoff

Am 22. Juli 1997 hat der Bundestag das *Informations- und Kommunikationsdienste-Gesetz* verabschiedet.[1] Das Gesetz besteht aus 11 Artikeln, die sich mit der Nutzung von Telediensten sowie dem Datenschutz bei Telediensten befassen und eine Reihe von Änderungen in bestehenden Gesetzen vornehmen. Artikel 3 umfaßt das *Gesetz zur digitalen Signatur* (Signaturgesetz – SigG).[2] In Analogie zur besiegelten Urkunde wird die digitale Signatur als eine Art von Siegel zu digitalen Daten bezeichnet. Ähnlich wie das Siegel sagt sie nichts über die Richtigkeit des Inhalts eines elektronischen Dokumentes aus und liefert auch keinerlei Interpretationshilfe zum Verständnis eines elektronischen Textes.[3] Sie kann lediglich zweierlei garantieren, nämlich

1. daß ein elektronisches Dokument von einer ganz bestimmten Person signiert wurde (Authentizität) und
2. daß der Inhalt dieses Dokumentes nach der Signierung nicht verändert wurde (Integrität).

Hintergrund des Signaturgesetzes ist die Einsicht, daß elektronische Dokumente einfach und spurenfrei gefälscht und verfälscht werden können und daß der Nachweis über Urheber und Ursprung eines Dokuments mit herkömmlichen Mitteln, an erster Stelle der forensischen Schriftanalyse, nicht zu erbringen ist. „Hacker" sind heute durchaus dazu in der Lage, elektronische Post abzufangen, zu verändern und in den Datennetzen wieder zu versenden. Wenn es sich bei diesen Nachrichten zufällig um eine Bankanweisung handelt, dann kann ein „Angreifer", so die

---

[1] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG). In: Bundesgesetzblatt 1997. Teil I. S. 1870–1880.

[2] Vgl. zur Entstehung Alexander *Roßnagel*: Das Gesetz und die Verordnung zur digitalen Signatur – Entstehung und Regelungsgehalt. In: Recht der Datenverarbeitung 14 (1998) S. 5–15. – Einen Überblick geben Peter *Rott*: Die Auswirkungen des Signaturgesetzes auf die rechtliche Behandlung von elektronischem Datenmanagement und Datenaustausch – eine Prognose. In: Neue Juristische Wochenschrift – Computerreport 1998. S. 420–429, und J. *Gulbins* und R. *Schuster*: Digitale IDs – Funktion, Anwendungen und rechtliche Situation. In: Klaus-Peter *Boden* und Michael *Barabas* (Hg.): Internet – von der Technologie zum Wirtschaftsfaktor. Deutscher Internet Kongress '97 Düsseldorf. Heidelberg 1997. S. 197–218.

[3] Vgl. dazu Dirk *Fox*: Zu einem prinzipiellen Problem digitaler Signaturen: In: Datenschutz und Datensicherheit 22 (1998) S. 386–388.

Bezeichnung im Fachjargon der Informatiker, die Identifikationsdaten abfangen und eine Anweisung zu seinen Gunsten tätigen.[4]

Da der Bedarf nach einem sicher abzuwickelnden elektronischen Rechtsverkehr in den letzten Jahren enorm gestiegen ist und erhebliche wirtschaftliche Interessen verschiedenster Gruppen tangiert, war eine gesetzliche Regelung überfällig. Der Gesetzgeber hat mit dem Signaturgesetz Rahmenregelungen vorgegeben, die eine Überprüfbarkeit gewährleisten sollen. Erst wenn die obengenannten Bedingungen, nämlich die Identität des Urhebers und Integrität der Daten, nachweislich erfüllt sind, kann auch der Inhalt eines elektronischen Dokuments als glaubhaft gelten.[5] Die Bedeutung der digitalen Signatur für den elektronischen Rechts- und Geschäftsverkehr liegt damit auf der Hand.[6] Bleibt zu fragen, wo ihre Bedeutung für die Archive liegt.[7]

Die digitale Signatur kann für die Archive in Zukunft aus zwei Gründen eine Rolle spielen. Zum einen sind Archive daran interessiert, die Authentizität und die

---

[4] Vgl. zu den möglichen Gefahren der Datenmanipulation und des Datendiebstahls Wendelin *Bieser* und Heinrich *Kersten*: Chipkarte statt Füllfederhalter. Daten beweissicher „elektronisch unterschreiben" und zuverlässig schützen. Heidelberg 1998. S. 3–16.

[5] In der Praxis muß die digitale Signatur noch eine Reihe weiterer Bedingungen erfüllen, die mit den Schriftformerfordernissen zusammenhängen. Dazu zählen vor allem die Abschlußfunktion (die Signatur schließt den Text ab bzw. umfaßt den Text als Ganzes.), die Warnfunktion (es muß dem Signierer bewußt sein, daß er mit der Signatur einen rechtserheblichen Vorgang vollzieht.) und die Nicht-Abstreitbarkeit (der Signierer darf nicht glaubhaft abstreiten können, daß er die Signatur geleistet hat, es sei denn, er habe im Umgang mit seiner Chip-Karte und der dazugehörigen persönlichen Identifikationsnummer (PIN) seine Sorgfaltspflicht verletzt, was ihn nicht von einer Haftung entbindet.). – Vgl. dazu Siegfried *Herda*: Zurechenbarkeit – Verbindlichkeit – Nichtabstreitbarkeit. In: Albert *Glade*, Helmut *Reimer* und Bruno *Struif* (Hg.): Digitale Signatur und sicherheitssensitive Anwendungen (DUD-Fachbeiträge). Braunschweig und Wiesbaden 1995. S. 96–114; Sigrun *Erber-Faller*: Die „elektronische Unterschrift" im Rechtsverkehr. In: Albert *Glade*, Helmut *Reimer* und Bruno *Struif* (Hg.): Digitale Signatur und sicherheitssensitive Anwendungen (DUD-Fachbeiträge). Braunschweig und Wiesbaden 1995. S. 115–132, bes. S. 116–124; Karl *Rihaczek*: Schriftform – Elektronische Form. In: Albert *Glade*, Helmut *Reimer* und Bruno *Struif* (Hg.): Digitale Signatur und sicherheitssensitive Anwendungen (DUD-Fachbeiträge). Braunschweig und Wiesbaden 1995. S. 133–152, bes. S. 135–146.

[6] Inzwischen hat auch die Europäische Kommission den Entwurf einer EG-Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen – Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates. In: KOM (1998) 297/2, vorgelegt. Die deutsche Fassung ist wiedergegeben unter URL: http://www.dud.de. – Vgl. dazu auch Rüdiger *Grimm* und Dirk *Fox*: Entwurf einer EU-Richtlinie zu Rahmenbedingungen „elektronischer Signaturen". In: Datenschutz und Datensicherheit 22 (1998). S. 407f.

[7] Vgl. dazu auch Michael *Wettengel*: Digitale Signaturen und Pilotprojekte zur IT-gestützten Vorgangsbearbeitung in der Bundesverwaltung. In: Frank M. *Bischoff* (Hg.): Archivierung von Unterlagen aus digitalen Systemen. Beiträge zur Tagung im Staatsarchiv Münster. 3.–4. März 1997 (Veröffentlichungen der staatlichen Archive des Landes Nordrhein-Westfalen E 4). Münster 1997. S. 9–20.

Integrität von Archivgut zu erhalten.[8] Im Zusammenhang mit digitalen Unterlagen, die in den nächsten Jahren auf die Archive zukommen, muß deshalb geprüft werden, ob die elektronische Unterschrift ein geeignetes Instrument darstellt, um dieses Ziel zu erreichen. Zum anderen werden die Archive auch Unterlagen übernehmen müssen, die bereits signiert sind. Hier gilt es Konzepte zu entwickeln, wie mit diesen Signaturen im Archiv verfahren werden muß.

Als Beispiel seien hier die elektronischen Register herangezogen. In Nordrhein-Westfalen werden unter anderem das Grundbuch[9] und das Handelsregister[10] auf eine elektronische Basis umgestellt und mit digitalen Signaturen versehen. Die Voraussetzungen dafür wurden durch das Registerverfahrenbeschleunigungsgesetz von 1993 geschaffen, das die erforderlichen Änderungen der Grundbuchordnung, des Handelsgesetzbuches und des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit brachte.[11] Die Umstellung soll bis zum Jahr 2000 an den wichtigsten Produktionsstandorten erfolgen. Das digitale Grundbuch mit der in Nordrhein-Westfalen geplanten Systemumgebung wird auch oder ist bereits in den Länder Bayern, Sachsen, Sachsen-Anhalt, Hamburg, Berlin, Bremen, Thüringen, Brandenburg, Hessen und Saarland eingeführt.

Obwohl es noch einige Zeit dauern wird, bis die ersten geschlossenen elektronischen Register in die Archive gelangen, besteht bereits jetzt die Notwendigkeit, sich nach dem Prinzip des Interventionismus[12] mit den damit verbundenen Problemen auseinanderzusetzen. Denn einerseits muß frühzeitig sichergestellt werden, daß in den elektronischen Systemen der Verwaltungen und Gerichte überhaupt archivfähige[13] Unterlagen erzeugt werden, die auch unabhängig von ihrer

---

[8] Vgl. zum Beispiel Michael *Wettengel*. In: Einfluß von Informationstechnologien auf Archivierungsverfahren. Hg. v. der Arbeitsgemeinschaft für Wirtschaftliche Verwaltung e. V. (AWV-Schrift 06 571). Eschborn 1997. S. 26.

[9] Vgl. hier und im folgenden Frank M. *Bischoff*: Einführung des elektronischen Grundbuchs in Nordrhein-Westfalen – Möglichkeiten der Überlieferungssicherung aus archivischer Perspektive. In diesem Band.

[10] Vgl. dazu den Überblick bei Hermann *Lindhorst*: Automation des Handelsregisters – ein Dauerthema ?. In: Computer und Recht 14 (1998) S. 590–598.

[11] Gesetz zur Vereinfachung und Beschleunigung registerrechtlicher und anderer Verfahren (Registerverfahrenbeschleunigungsgesetz – RegVBG). In: Bundesgesetzblatt 1993. Teil I. S. 2182–2235. Darin: Abschnitt 1 zur Beschleunigung der Registerführung beim Grundbuch (Unterabschnitt 1), beim Handels- und Genossenschaftsregister (Unterabschnitt 2), beim Schiffsregister (Unterabschnitt 3) und beim Vereinsregister (Unterabschnitt 4).

[12] Vgl. Udo *Schäfer*: Büroautomation in der Landesverwaltung Baden-Württemberg. Strategisches und operatives archivarisches Handeln am Beispiel der Justiz. In: Frank M. *Bischoff* (Hg.): Archivierung von Unterlagen aus digitalen Systemen. Beiträge zur Tagung im Staatsarchiv Münster. 3.–4. März 1997 (Veröffentlichungen der staatlichen Archive des Landes Nordrhein-Westfalen E 4). Münster 1997. S. 44 f.

[13] Unter *Archivfähigkeit* verstehe ich in Anlehnung an Angelika Menne-Haritz die materielle, funktionelle und strukturelle Qualität, die Aufzeichnungen für eine unbefristete Archivierung geeignet machen. Normalerweise sollte sie aus der Registraturfähigkeit resultieren, was aber vor dem Hintergrund der zur Zeit zum Teil hektisch durchgeführten Umstellung auf elektronische Unterlagen keinesfalls als gesichert gelten darf. Im besonderen Fall der digitalen Signatur kann es durchaus sein, daß diese in den Zeitdimensionen behördlichen Handelns durchaus für eine Aufbewahrung geeignet erscheinen, in der

originären Systemplattform und der darauf aufsetzenden Softwareumgebung vollständig und unverfälscht gelesen werden können. Andererseits spielen im speziellen Fall der Register Massenfragen für die Archive eine Rolle. Das derzeit noch bestehende Loseblatt-Grundbuch soll in Nordrhein-Westfalen wie auch in anderen Bundesländern eingescannt werden. Nach Abschluß der Übertragung wird das papiergestützte Grundbuch geschlossen und den Staatsarchiven früher oder später zur Übernahme angeboten. Bei den 5,1 Millionen „lebenden" Loseblatt-Grundbüchern in Nordrhein-Westfalen handelt es sich um ca. 32 Regalkilometer im Format DIN A 4, die dann gegebenenfalls in die Magazine aufgenommen werden müssen.

Im Zusammenhang mit der Einführung des elektronischen Grundbuchs ist es daher allein schon im Interesse einer ökonomisch tragfähigen Archivierung geboten, auszuloten, ob die Notwendigkeit zur Archivierung des papiergestützten Grundbuchs besteht, oder ob es sich unter Berücksichtigung der elektronischen Fassung des Grundbuchs nicht vielmehr um eine Doppelüberlieferung handelt, die vermieden werden muß. Hier sind allerdings nicht allein technische, sondern auch juristische Fragen berührt, auf die an dieser Stelle nicht weiter einzugehen ist.

Authentizität und Beweiskraft digitaler Unterlagen

Grundbuchverfügung (GBV)[14] und Handelsregisterverfügung (HRV)[15] bestimmen, daß Eintragungen in das jeweilige maschinell geführte Register nur möglich sein sollen, wenn der zuständige Urkundsbeamte der Eintragung seinen Namen hinzusetzt und beides elektronisch unterschreibt. Dabei soll die elektronische Unterschrift in einem allgemein als sicher anerkannten automatisierten kryptographischen Verfahren textabhängig und unterzeichnerabhängig hergestellt werden.

Hier klingt bereits der Aspekt der Rechtssicherheit an, den das Signaturgesetz, regeln will. Allerdings schreiben weder die Grundbuchverfügung noch die Handelsregisterverfügung vor, daß die Handhabung der digitalen Signaturen in Anlehnung an das Signaturgesetz zu erfolgen habe. Insbesondere werden keine Regelungen bezüglich einer Erneuerung der Signaturen erlassen. Da aber die digitale Signatur den notwendigen Sicherheitsanforderungen nur genügt, wenn sie in enger Übereinstimmung mit Signaturgesetz und Signaturverordnung (SigV) gehandhabt wird, ist davon auszugehen, daß sich die Verfahren im Bereich der Register im wesentlichen an Gesetz und Verordnung zur digitalen Signatur orientieren.

In der Begründung des Regierungsentwurfs zum Signaturgesetz wird auf die Manipulierbarkeit elektronischer Daten abgehoben und gefolgert: *Nur die nachweisliche Sicherheit gesetzlicher digitaler Signaturen wird es bei verschiedenen*

Langzeitperspektive der Archive allerdings ihren Wert verliert. – Vgl. auch den deutschen Entwurf der Projektgruppe zur Terminologie des Internationalen Archivrats, s.v. Archivfähigkeit (URL: http://staff-www.uni-marburg.de/~mennehar/germanterms.htm).

[14] § 75 GBV.

[15] § 57 HRV.

Rechtsvorschriften erlauben, neben der papiergebundenen Schriftform auch die digitale Form zuzulassen.[16] In Anlehnung daran wird der Zweck des Gesetzes in § 1 mit einer Sicherheitsvermutung verknüpft: Das Signaturgesetz soll Rahmenbedingungen für digitale Signaturen schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können.

Obwohl der Gesetzgeber damit ein Regelwerk geschaffen hat, das eine Überprüfbarkeit von Datenintegrität und Ursprungsauthentizität gewährleistet, räumt er einem digital signierten elektronischen Dokument nicht den Rang einer Urkunde ein. Vor Gericht können sie zunächst nur als Augenscheinsobjekte behandelt werden und unterliegen damit der freien richterlichen Beweiswürdigung.[17] Allerdings wird in der juristischen Diskussion davon ausgegangen, daß die faktische Sicherheit der digitalen Signatur im Rahmen der freien Beweiswürdigung von den Gerichten honoriert werde – so schon die Erwartung des Gesetzgebers in der amtlichen Begründung zum Signaturgesetz[18] – und daß sich daneben in naher Zukunft Regeln eines Anscheinsbeweises entwickeln, die dann eine ausreichende Beweissicherheit bieten.[19] In einem Entschließungsantrag der Fraktionen CDU/CSU und FDP hat der Bundestag die Bundesregierung denn auch aufgefordert, innerhalb von zwei Jahren nach Inkrafttreten des Signaturgesetzes zu überprüfen, welche Anpassungen im Zivilrecht, Zivilprozeßrecht und Verwaltungsrecht vorzunehmen seien.[20]

---

[16] Bundestagsdrucksache 13/7385. In: Horst E. *Theis*: Die Multimedia-Gesetze. Erläuterungen, Gesetzestexte, amtliche Begründungen. Neuwied, Kriftel und Berlin 1997. S. 182.

[17] Im Prinzip gilt das auch für digitale Signaturen in den elektronischen Registern. Allerdings genießt das Grundbuch nach § 892 BGB öffentlichen Glauben.

[18] *Die Beweisfunktion signierter digitaler Daten soll über die faktische Sicherheit gesetzlicher digitaler Signaturen erreicht werden, da davon ausgegangen werden kann, daß die Gerichte diese im Rahmen der freien Beweiswürdigung honorieren werden. In einem weiteren (gesonderten) Schritt wird geprüft, ob Änderungen im Beweisrecht geboten sind* (Bundestagsdrucksache 13/7385. In: Horst E. *Theis*, wie Anm. 16, S. 182).

[19] Ulrich *Seidel*: Das Recht des elektronischen Geschäftsverkehrs. Rahmenbedingungen, technische Infrastruktur und Signaturgesetzgebung, (DUD-Fachbeiträge). Wiesbaden 1997. S. 33 ff. – Alexander *Roßnagel*, wie Anm. 2, S. 15. – Peter *Rott*, wie Anm. 2, S. 425, 427 ff., hält es angesichts der Unvorhersehbarkeit der technischen Weiterentwicklung für unwahrscheinlich, daß das Beweisrecht angepaßt wird; denkbar seien aber offene Formulierungen in der Zivilprozeßordnung, die auf dem Weg der Rechtsverordnung konkretisiert werden könnten.

[20] Bundestagsdrucksache 13/7935, S. 2 f. – Bereits in ihrer Gegenäußerung zur Stellungnahme des Bundesrates zum Entwurf des IuKDG hatte die Bundesregierung eine Prüfung der Frage angekündigt, *ob im Hinblick auf die Nutzung digitaler Signaturen Änderungen bzw. Ergänzungen im bürgerlichen Recht und im Zivilprozeßrecht notwendig sind. Im Kern geht es darum, ob die strenge gesetzliche Schriftform des BGB noch modernem Rechtsgeschäftsverkehr genügt und zweitens für papierlosen, elektronischen Rechtsgeschäftsverkehr besondere Regelungen notwendig sind* (Bundestagsdrucksache 13/7385. S. 72).

Organisatorisches Konzept und Funktionsweise digitaler Signaturen am Beispiel der Registerpflege

Eine digitale Signatur ist weniger ein Siegel, wie im Signaturgesetz definiert,[21] sondern ein Kryptogramm. Ihre Nutzung setzt ein assymetrisches Schlüsselpaar[22] voraus, nämlich einen privaten Schlüssel, der ähnlich wie eine Scheckkarte[23] an eine natürliche Person ausgegeben wird, und einen öffentlichen, der allen Interessenten zugänglich gemacht werden kann. Daten, die mit dem privaten Schlüssel verschlüsselt werden, können nur mit dem öffentlichen Schlüssel wieder entschlüsselt werden. Die Länge des zur Signierung von Grundbuch- und Handelsregistereinträgen vorgesehenen Schlüssels beträgt 1024 Bit, was etwa einer 300stelligen Zahl entspricht. Zur Zeit wird davon ausgegangen, daß es praktisch nicht möglich ist, einen solchen Schlüssel zu „knacken".[24]

Bei der Nutzung der digitalen Signatur gibt es im Prinzip fünf Akteure mit unterschiedlichen Rollen: Den Signierenden, den Nutzer, der die Signatur prüfen möchte, das für die Vergabe der Signaturschlüsselzertifikate[25] zuständige Trust-Center und eine für die Zertifizierung der Zertifizierungstellen zuständige Kontrollbehörde, die eine Reihe von Sicherheitsüberprüfungen auf andere Stellen übertragen kann (Abbildung 1).

Das Trust-Center nimmt die Rolle des vertrauenswürdigen Dritten ein, der die Sicherheit der Signaturschlüssel, die Identität des Schlüsselbesitzers und der eingesetzten Verfahren garantiert. Es bestätigt, daß es sich bei einem angegebenen Schlüssel um den öffentlichen Schlüssel einer bestimmten Person handelt und benennt Beginn und Ende der Gültigkeit. Dieses in ein öffentlich zugängliches Verzeichnis eingestellte Zertifikat wird mit dem privaten Schlüssel des Trust-Centers signiert und kann mit dem dazugehörigen öffentlichen Schlüssel überprüft werden.

---

[21] § 2 Abs. 1 SigG.

[22] Als derzeit sicherstes Verfahren gilt das RSA-Verfahren, benannt nach seinen Erfindern Ronald Rivest, Adi Shamir und Leonard Adleman.

[23] Vgl. zu den Sicherheitsvorgaben für Chipkarten Klaus-Werner *Schröder*: Zertifizierte Sicherheit für Chipkarten. In: Albert *Glade*, Helmut *Reimer* und Bruno *Struif* (Hg.): Digitale Signatur und sicherheitssensitive Anwendungen (DUD-Fachbeiträge). Braunschweig und Wiesbaden 1995. S. 242–249.

[24] Wendelin *Bieser* und Heinrich *Kersten*, wie Anm. 4, S. 29. – Allerdings ist man sich der Tatsache bewußt, daß die Sicherheit mit der Zeit abnimmt. So werden bereits jetzt für Hochsicherheits-Anforderungen Schlüssellängen von 2048 Bit empfohlen. Vgl. Steffen *Raßmann*: Elektronische Unterschriften im Zahlungsverkehr. In: Computer und Recht 14 (1998) S. 36–41, hier S. 38.

[25] Unter einem Zertifikat wird ein elektronisch unterschriebenes elektronisches Dokument einer zugelassenen Zertifizierungsstelle verstanden, in dem diese die Zuordnung eines öffentlichen Schlüssels zu einem Teilnehmer bescheinigt. – Vgl. Thorsten *Brandt*: Auswirkungen der elektronischen Unterschrift auf Archivierungssysteme am Beispiel des Zahlungsverkehrs: In: info21 1998. Heft 3. S. 51–54. – Vgl. zur Terminologie auch Siegfried *Herda*, wie Anm. 5, S. 109–114.

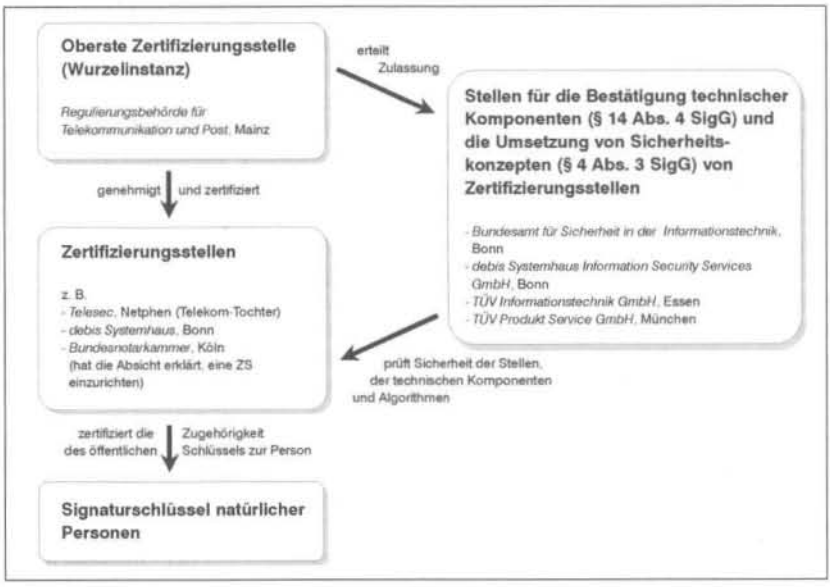

Abb. 1: Zuständigkeiten von Zertifizierungsstellen.

Das Signaturgesetz sieht vor, daß die Zertifizierungsstellen durch eine „Wurzelinstanz" genehmigt und kontrolliert werden. Diese Aufgabe übernimmt die *Regulierungsbehörde für Telekommunikation und Post* als oberste nationale Zertifizierungsstelle. Sie genehmigt Zertifizierungsstellen und erteilt anderen geeigneten Institutionen die Zulassung zur Prüfung der Sicherheit von Zertifizierungsstellen und technischen Komponenten. Mit dieser Aufgabe ist das Bundesamt für Sicherheit in der Informationstechnik (BSI)[26] betraut, das inzwischen Maßnahmenkataloge zu den §§ 12 Abs. 2 und 16 Abs. 6 SigV vorgelegt hat.[27] Das BSI hat zum gegenwärtigen Zeitpunkt Abkommen mit drei privaten IT-Sicherheitszertifizie-

[26] Marit *Blattner-Zimmermann*: Warum (BSI-)Zertifikate?. In: Datenschutz und Datensicherheit 22 (1998) S. 222.

[27] Die Kataloge sind einsehbar auf der Website der Regulierungsbehörde für Telekommunikation und Post (URL: http://www.regtp.de/fachinfo/digitalsign/start.htm). Auf dieser findet sich auch die im Bundesanzeiger Nr. 31 vom 14. 2. 1998 veröffentlichte Bekanntmachung zur digitalen Signatur nach Signaturgesetz und Signaturverordnung mit den Listen der anerkannten Stellen für die Bestätigung von technischen Komponenten gemäß § 14 Abs. 4 SigG, der anerkannten Stellen für die Prüfung und Bestätigung der Umsetzung von Sicherheitskonzepten gemäß § 4 Abs. 3 SigG und der Stellen, die nach Kenntnis der Regulierungsbehörde in der Lage sind, die Prüfung der Sicherheit von technischen Komponenten nach § 14 Abs. 3 SigG in Verbindung mit § 17 Abs. 1 SigV durchzuführen.

rungsstellen[28] abgeschlossen, die dadurch ebenfalls von der Regulierungsbehörde anerkannt werden.

Die Regulierungsbehörde verfügt ihrerseits über ein Schlüsselpaar. Bei der Ausstellung eines Zertifikats für eine Zertifizierungsstelle signiert sie den öffentlichen Schlüssel der Zertifizierungsstelle nach dem bereits beschriebenen Verfahren und gewährleistet damit die Verifikation der Zertifikate des Trust-Centers. Der öffentliche Schlüssel der Regulierungsbehörde, für den diese sich selbst ein „Wurzelzertifikat" ausstellt, wird unter anderem im Bundesanzeiger veröffentlicht.

Zum besseren Verständnis sei das Verfahren der Signierung elektronischer Unterlagen durch einen Schlüsselinhaber am Beispiel des elektronischen Grundbuchs nach dem derzeit erkennbaren Stand der Planungen in Nordrhein-Westfalen erläutert.[29] Die Verfahrensabläufe beim Handelsregister sind weitgehend analog aufgebaut, mit dem Unterschied, daß die nordrhein-westfälische Justiz auf eine Konzentration der Produktionsstandorte für das Handelsregister zielt,[30] während die Produktion des elektronischen Grundbuchs nach wie vor an allen Amtsgerichten erfolgen soll.[31] In beiden Fällen wird aber die Datenhaltung zentralisert. Die Justiz spricht in diesem Zusammenhang von einem zentralen „Grundbucharchiv" bzw. „Handelsregisterarchiv", von dem aus auch der Postverkehr und die Beauskunftung erfolgen soll.

Bei einem Landesrechenzentrum wird ein Zentralserver mit der Grundbuchproduktion aus den Amtsgerichten gespeist. Die Grundbuchdaten können von dazu autorisierten Personen und Institutionen über einen Auskunftsserver abgerufen werden. Zur Illustration des Drucks, unter dem die Justiz agiert, sei hier nur angemerkt, daß im Rahmen von Einsichtnahmen und Auskunftserteilungen aus dem Grundbuch jährlich annähernd 3,5 Millionen Zugriffe erfolgen, die zu rund 75 %

---

[28] Vgl. zu den Sicherheitszertifizierungstellen Josef *Heiler*: Unbürokratische Zertifizierung?. In: Datenschutz und Datensicherheit 22 (1998) S. 224; Ernst-Hermann *Gruschwitz*: TÜViT – der Informatik-TÜV. In: Datenschutz und Datensicherheit 22 (1998) S. 225; Heinrich *Kersten*: debisZERT. In: Datenschutz und Datensicherheit 22 (1998) S. 223. – Vgl. zu einigen grundsätzlichen Probleme mit dem durch das Signaturgesetz vorgegebenen Zertifizierungssystem Kai *Rannenberg*: Sicherheitszertifizierung. Probleme, Trends und Chancen. In: Datenschutz und Datensicherheit 22 (1998) S. 190–192.

[29] Vgl. hier und im folgenden C. *Köhrer* und Dietrich *Kruse*: Anwendungen der digitalen Signatur – elektronischer Rechtsverkehr bei den Grundbuchämtern, In: Albert *Glade*, Helmut *Reimer* und Bruno *Struif* (Hg.): Digitale Signatur & Sicherheitssensitive Anwendungen (DUD-Fachbeiträge). Braunschweig und Wiesbaden 1995. S. 48–54; Franz *Göttlinger*: Elektronisches Grundbuch bei den sächsischen Grundbuchämtern. In: Kulturelle Beherrschbarkeit digitaler Signaturen. Interdisziplinärer Diskurs zu querschnittlichen Fragen der IT-Sicherheit. Hg. vom Bundesamt für Sicherheit in der Informationstechnik. Ingelheim 1997. S. 88–93.

[30] Arbeitsgruppe *Elektronische Grundbuch- und Registerführung* des Justizministeriums des Landes Nordrhein-Westfalen beim Oberlandesgericht Hamm: Schlußbericht zur Voruntersuchung betreffend die Frage der Einführung eines elektronischen Handelsregisters im Lande Nordrhein-Westfalen. Bd. 1. April 1997. S. 208–239.

[31] Arbeitsgruppe *Elektronische Grundbuch- und Registerführung* des Justizministeriums des Landes Nordrhein-Westfalen beim Oberlandesgericht Hamm: Bericht zur Voruntersuchung betreffend die Frage der Einführung eines elektronischen Grundbuchs im Lande Nordrhein-Westfalen. Bd. 1. September 1997. S. 137–146.

auf Notare, Banken, Behörden und Justizgeschäftsstellen entfallen,[32] Kunden also, die in ein Online-Auskunftsprogramm einbezogen werden sollen.

Die Signierung der Grundbucheinträge erfolgt im jeweiligen Amtsgericht durch den zuständigen Rechtspfleger, der den Signiervorgang explizit anstossen muß (Abbildung 2). Aus einem beliebig langen Grundbucheintrag wird mittels eines Verdichtungsalgorithmus (Hash-Funktion) ein signifikanter Block fester Größe (Komprimat) errechnet. Die Länge des Komprimats ist also unabhängig vom Umfang des Eintrags immer gleich. Hash-Funktionen sind Einwegfunktionen, d. h., daß sich aus dem Komprimat der ursprüngliche Text nicht wieder errechnen läßt. Genau genommen sind Komprimate nicht derart einzigartig, daß ein Komprimat nur aus einem Text resultieren könnte. Das würde bei einer gegebenen Länge des Komprimats von 128 Bit eine endliche Zahl von Texten voraussetzen. Es wird aber davon ausgegangen, daß es rechnerisch schwierig ist, zwei bedeutungstragende Texte mit demselben Hash-Wert zu finden.[33]

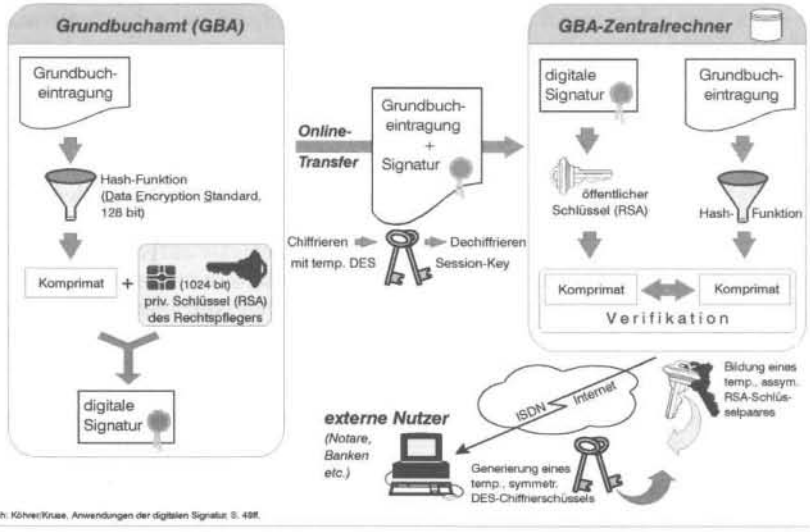

Abb. 2: Einsatz digitaler Signaturen in Grundbuchämtern nach dem Konzept von *Solum-Star.*

Das weitere Verfahren baut auf der assymetrischen Verschlüsselung auf. Der Rechtspfleger verfügt über einen privaten, nur ihm bekannten bzw. in seiner Chipkarte enthaltenen Schlüssel, mit dem er das Komprimat verschlüsseln und damit signieren kann.

---

[32] Arbeitsgruppe *Elektronische Grundbuch- und Registerführung* des Justizministeriums des Landes Nordrhein-Westfalen beim Oberlandesgericht Hamm, wie Anm. 31, S. 56 f.

[33] Es handelt sich um eine kollisionsresistente Hash-Funktion nach der Definition von Siegfried *Herda*, wie Anm. 5, S. 111.

Nachdem die Signierung eines Eintrags vorgenommen und ein Zeitstempel[34] eingeholt wurde, erfolgt die chiffrierte Übertragung des Grundbucheintrags und der Signatur vom Server des Grundbuchamtes zum Grundbuch-Zentralrechner. Dort wird zunächst dechiffriert und dann mit dem öffentlichen Schlüssel des Rechtspflegers die Signatur entschlüsselt, so daß das Komprimat vorliegt. Parallel dazu wird die übermittelte Grundbucheintragung mit der Hash-Funktion komprimiert. Sind beide Komprimate identisch, gilt die Eintragung als authentisch und die Identität des verantwortlichen Rechtspflegers als gesichert. Die elektronische Signatur wird zusammen mit dem Grundbucheintrag abgespeichert, so daß der Prüfvorgang zu jeder Zeit wiederholt werden kann.

Sofern durch Veränderungen in einer Abteilung des Grundbuchs oder wegen Ablauf der Gültigkeit der Signatur eine Nachsignierung erforderlich ist, werden die bereits vorhandenen Signaturen in die Berechnung des Hash-Wertes miteinbezogen.[35] Damit bleibt die Überprüfbarkeit der Integrität und der Verantwortlichkeiten im gesamten Verlauf des Produktionsprozesses gewährleistet.

Der Online-Kontakt zu Notaren und Banken soll in ähnlicher Weise organisiert werden. Hier gelangen ein assymmetrisches Schlüsselpaar und ein symmetrischer Chiffrierschlüssel zum Einsatz.[36]

Archivfähigkeit digitaler Signaturen

Die Sicherheit, die mit der digitalen Signatur erreicht wird, ist auf den ersten Blick bestechend und erfüllt wesentliche Anforderungen, die in der Diskussion um elektronische Unterlagen auch von Seiten der Archivare aufgestellt wurden.[37] Sie gewährleistet die Feststellbarkeit von Verantwortlichkeiten und ermöglicht die Überprüfung der Unverfälschtheit von Aufzeichnungen. Verzichtet man auf eine

---

[34] Der Zeitstempel wird von einem Zeitstempeldienst eingeholt. Er zertifiziert, daß eine bestimmte Information – hier die digitale Signatur – zu einem bestimmten Zeitpunkt vorgelegen hat. – Vgl. die Erläuterungen des Bundesamtes für Sicherheit in der Informationstechnik bei Roger *Gatti* und Fritz *Bauspieß* (Bearb.): Schnittstellenspezifikation für die Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV. Abschnitt A 4: Zeitstempel. Version 1. Stand: 17. August 1998 (URL: http://www.bsi.bund.de).

[35] § 18 SigV: *Werden Daten über längere Zeit in signierter Form benötigt, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter nach § 17 Abs. 2 als geeignet beurteilt sind, so sind die Daten vor Ablauf des Zeitpunktes der Eignung der Algorithmen und zugehörigen Parameter mit einer neuen digitalen Signatur zu versehen. Diese muß mit neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere digitale Signaturen einschließen und einen Zeitstempel tragen.*

[36] Das Verfahren wird beschrieben von C. *Köhrer* und Dietrich *Kruse*, wie Anm. 29, S. 52 f.

[37] Vgl. die Übersicht über den Stand der Diskussion von Alf *Erlandsson*: Electronic records management. A literature review (ICA Studies 10). Paris 1997. S. 29–42. – Vgl. auch Luciana *Duranti*: Die Sicherung der Integrität von Datensätzen. In: Vorträge und Ergebnisse des DLM-Forums über elektronische Aufzeichnungen. Brüssel, 18.–20. Dezember 1996 (INSAR. Beilage II). Luxemburg 1997. S. 60–65; Michael *Wettengel*. In: Einfluß von Informationstechnologien auf Archivierungsverfahren, wie Anm. 8, S. 25–29; Leitlinien für den Umgang mit elektronischen Informationen. Maschinenlesbare Daten und elektronische Dokumente (INSAR. Beilage III). Luxemburg 1998. S. 30.

Aufbewahrung der digitalen Signaturen, begibt man sich zugleich auch der damit faktisch gewonnenen Rechtssicherheit. Legt man das Kriterium der technischen Nachprüfbarkeit zugrunde, so haben Archive dem nichts Vergleichbares entgegenzusetzen.

Aus archivischer Perspektive muß daher geprüft werden, welche Anforderungen eine Archivierung elektronischer Unterschriften stellt und ob es Gründe gibt, die einer sinnvollen Archivierung elektronischer Unterschriften entgegenstehen könnten.

Zunächst ist festzuhalten, daß die Aufbewahrung der digitalen Signatur kein sonderliches Problem darstellt, zumindest wenn man sich auf die grundsätzlich mit einer Archivierung digitaler Unterlagen verbundenen Probleme einläßt, wozu die Archive in Zukunft gezwungen sein werden, wenn sie Herr ihrer Aufgaben bleiben wollen. Ein 1024 Bit langer String stellt keine höheren Anforderungen, als eine beliebige Textdatei. Nimmt man das Konzept der elektronischen Unterschrift ernst, dann sind mit der digitalen Signatur allerdings Folgelasten verbunden.

Nachsignierung

Grundbuchverfügung[38] und Handelsregisterverfügung[39] bestimmen, daß die elektronische Unterschrift in einem allgemein als sicher anerkannten kryptographischen Verfahren erstellt werden soll. Ein Problem der digitalen Signatur besteht darin, daß ihre Sicherheit allein durch Zeitablauf geringer wird, weil die eingesetzten Verfahren *infolge neuer wissenschaftlicher Erkenntnisse oder des technischen Fortschritts (z. B. schnellere Rechner) an Sicherheitswert verlieren.*[40] Deshalb bestimmt das Signaturgesetz, daß die Zertifizierungsstelle die Antragsteller darauf hinzuweisen hat, daß Daten mit digitaler Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.[41] Die Signaturverordnung legt die maximale Gültigkeitsdauer von Zertifikaten auf fünf Jahre fest.[42] Daten, die über längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Verfahren als geeignet beurteilt sind, müssen vor Ablauf des Eignungszeitraums mit einer neuen digitalen Signatur versehen werden. Nach § 18 SigV muß die Neusignierung mit neuen Verfahren erfolgen, frühere digitale Signaturen einschließen und einen Zeitstempel tragen.[43]

Im Rahmen einer Langzeitsicherung von Dokumenten mittels digitaler Signaturen werden aus diesen Vorschriften ganze Serien von Signaturschlüsseln resultieren, die nachgehalten werden müssen, um eine Verifizierung zu gewährleisten.

---

[38] § 75 Satz 2 GBV.

[39] § 57 Satz 2 HRV verweist auf § 75 GBV.

[40] Begründung zur Verordnung zur digitalen Signatur in der Fassung des Beschlusses der Bundesregierung vom 8. Oktober 1997 (URL: http://www.iid.de/rahmen/sigv_begr.html) zu § 18.

[41] § 6 SigG.

[42] § 7 SigV.

[43] Vgl. Anm. 35.

Der Verlust nur eines einzigen Gliedes in dieser Signaturkette würde eine Verifizierung der früheren Glieder bereits unmöglich machen. Selbstverständlich besteht das Sicherungsproblem nach einer Abgabe der Unterlagen an die Archive bei der gegenwärtigen Gesetzeslage in demselben Maße wie vorher. Das hätte zur Konsequenz, daß die Archive nach der Übernahme signierter Unterlagen den Signierprozeß selbst fortsetzen müßten, um ihre Authentizität zu gewährleisten.

Selbst wenn sich die Verfahren als stabil erweisen und nicht in fünfjährigen Intervallen ihren Sicherheitswert verlieren würden, wäre eine Nachsignierung vermutlich schon im Zusammenhang mit konservatorischen Maßnahmen erforderlich. Eine Rückfrage bei zwei Zertifizierungsstellen, der Telekom-Tochter *Telesec* und dem *debis Systemhaus* der Daimler-Benz-Gruppe, brachte die Empfehlung, bei einem Wechsel des Speichermediums eine Nachsignierung vorzunehmen. Für welche Speichermedien sich Archive im Rahmen einer Langzeitaufbewahrung von digitalen Unterlagen auch entscheiden – ein Wechsel des Mediums wird in jedem Falle nach 5–10 Jahren notwendig sein.

Zur Aufrechterhaltung des Sicherheitswertes digitaler Signaturen würde es mithin zur Standardaufgabe von Archiven gehören, sich bei einem Trust-Center in periodischen Intervallen neue Zertifizierungsschlüssel ausgeben zu lassen, um Archivgut nachzusignieren. Ob eine so weitreichende Pflicht stillschweigend und ohne entsprechende Rahmenregelungen übernommen werden kann, muß bezweifelt werden.

Konvertierungsprobleme und Wechsel des Kodierungssystems

Selbst wenn Archive bereit wären, diese Aufgaben zu übernehmen, ist damit die Frage der langfristigen Validität digitaler Signaturen nicht gelöst. Wie bereits ausgeführt ergibt sich die digitale Signatur aus dem Komprimat eines Dokuments. Der Hash-Wert wiederum errechnet sich aus der Summe der Bits, die das Dokument umfaßt. Jede Veränderung, sei es auch nur das Hinzufügen oder die Löschung eines Leerzeichens führt somit automatisch zu einem anderen Hash-Wert. Das bedeutet, daß die Funktion der digitalen Signatur nur gewährleistet bleibt, wenn die digitalen Unterlagen selbst nicht verändert werden. Die Erfahrungen der letzten 20 Jahre zeigen aber, daß im Rahmen einer Langzeitaufbewahrung von elektronischen Daten eine Veränderung der physikalischen Speichertechniken zu erwarten ist, d. h. eine Konvertierung auf neue Standards notwendig wird.

An einem aktuellen Beipiel seien die Konsequenzen verdeutlicht. Zumeist wird heute noch mit 8-Bit-Zeichensätzen gearbeitet. D.h., daß ein Zeichen intern durch eine achtstellige Folge von Nullen und Einsen dargestellt wird. Daraus ergeben sich die 2^8, also 256 Zeichen, die – abzüglich der reservierten Steuerzeichen – auf einem Rechner zur Verfügung stehen. Die Beschränkung auf 256 Zeichen beinhaltet gewisse Nachteile. Die Schriftzeichen anderer Sprachen, z. B. des Griechischen, stehen nicht bzw. in Textverarbeitungssystemen nur durch die Wahl eines anderen Fonts zur Verfügung.[44] Deshalb findet zur Zeit die Umstellung auf ei-

[44] Bereits hier besteht ein Problem der digitalen Signatur: Wird die Information über den verwendeten Font und das verwendete System nicht mitgespeichert und -signiert bzw. ist der verwendete Font oder das verwendete System bei einer späteren Überprüfung

nen neuen 16-Bit-Standard statt (*Unicode*). Aus der 16stelligen Folge von Nullen und Einsen ergeben sich 65 536 mögliche Zeichen.

Es steht zu vermuten, daß auf kurz oder lang alle Texte in den 16-Bit-Standard konvertiert werden. Damit verlieren Signaturen, die auf der Basis von Texten im 8-Bit-Standard erstellt wurden, ihre Funktion. Obwohl die Darstellung eines Textes auf dem Bildschirm oder in der Druckausgabe beim 8-Bit- und beim 16-Bit-Standard jeweils bis hin zur Zahl der Leerzeichen identisch sein kann, wird sich der Hash-Wert je nach verwendetem Standard anders darstellen. Daraus folgt, daß auch die auf der Basis des 8-Bit-Textes erstellte elektronische Signatur nicht mehr zum Nachweis der Unverfälschtheit des inzwischen in den 16-Bit-Standard konvertierten Textes dienen kann. Man kann auch in diesem Fall nicht einfach die alten Signaturen löschen und neue anbringen. Damit wäre die Kette wieder durchbrochen und ein Nachweis der Urheberschaft von Dokumenten oder Datenbankeinträgen nicht mehr möglich.

Der Gesetzgeber hat zwar im Signaturgesetz den Wandel der Algorithmen bedacht und deshalb besondere Sicherungsklauseln eingebaut. Ein Wechsel des Zeichenstandards ist allerdings nicht vorgesehen. Soweit es noch benötigte Texte, etwa lebende Grundbuch- und Handelsregistereinträge angeht, darf man vielleicht darauf vertrauen, daß die Informatik in Zusammenarbeit mit der Justiz hier einen Ausweg findet. Bei Archivgut, dessen Aufbewahrung und Nutzbarkeit langfristig zu gewährleisten ist, wird man jedoch mit einer Reihe von Konvertierungen rechnen müssen.[45] Angesichts der Entwicklungsgeschwindigkeit des EDV-Sektors und der derzeitigen Gesetzeslage ist es daher unwahrscheinlich, daß digitale Signaturen im Archiv dauerhaft ihren Wert behalten können.

Verifikationsmöglichkeiten und Aufbewahrungsdauer der Zertifikate

Eine Aufbewahrung digitaler Signaturen kann letztlich nur dem Zweck dienen, die beschriebene Verifikation des signierten Dokuments zu gestatten, d. h. die Prüfung der Unverfälschheit des Textes und den Nachweis des Urhebers zu ermöglichen. Dazu bedarf es wenigstens zweier Programme oder Programmbausteine, nämlich des Programms zur Berechnung des Komprimats des abgespeicherten Dokuments und des Programms zur Entschlüsselung der Signatur, also des öffentlichen Schlüssels. Erst dadurch wird eine Verifikation gewährleistet.

Wie alle Programme laufen auch diese in bestimmten Systemumgebungen. Eingangs wurde bereits angedeutet, daß es von Archiven zurecht abgelehnt wird,

---

nicht greifbar, dann läßt sich zwar immer noch die Integrität der Bitfolge belegen. Die richtige Darstellung des Textes in der Zeichenfolge, in der er von dem Signierenden zum Zeitpunkt der Signierung gesehen wurde, ist aber infrage gestellt. Grundsätzlich dazu Dirk *Fox*, wie Anm. 3, S. 387 f., der unter anderem darauf hinweist, daß Textdarstellungen in *WinWord* und in *Word für Macintosh* sich empfindlich unterscheiden können. Die von Dirk Fox vorgeschlagenen Lösungen helfen allerdings nicht, die im Zusammenhang mit einer Langzeitarchivierung auftretenden Probleme zu überwinden.

[45] Erinnert sei daran, daß im Laufe der letzten 20 Jahre verschiedene Zeichensätze in Gebrauch waren, vor allem ASCII 7-Bit, ASCII 8-Bit, EBCDIC, derzeit ANSI und demnächst Unicode.

Hardware- und Softwareumgebungen aufzubewahren oder spezialisierte Programme für Benutzer bereitzustellen.[46] Sofern man gegen diesen Grundsatz nicht verstoßen will, scheidet die Möglichkeit aus, den Prozeß der Verifikation durch das Archiv vornehmen zu lassen.

Im Signaturgesetz wird bestimmt, daß die Zertifizierungsstelle für digitale Unterschriften unter anderem die Pflicht hat, den Namen des Signaturschlüssel-Inhabers, den öffentlichen Signaturschlüssel und die Bezeichnung der Algorithmen, mit denen der öffentliche Schlüssel des Signaturschlüssel-Inhabers benutzt werden kann, nachprüfbar und unter bestimmten Bedingungen abrufbar zu halten.[47] Es liegt also nahe, für eine Verifikation archivierter Signaturen auf die Zertifizierungsstelle zu verweisen. Diese könnte die Verifikation selbst vornehmen oder einer anderen, damit beauftragten Stelle die notwendigen Informationen übermitteln.

Allerdings hat der Gesetzgeber eine solche Möglichkeit zeitlich begrenzt. Das Signaturgesetz führt aus, daß die Sicherheitsmaßnahmen und die ausgestellten Zertifikate so zu dokumentieren sind, daß die Daten und ihre Unverfälschheit jederzeit nachprüfbar sind, überläßt aber nähere Regelungen einer Rechtsverordnung.[48] Laut Signaturverordnung besteht eine Pflicht zur Aufbewahrung und Verfügbarhaltung der Zertifikatsdokumentation mindestens 35 Jahre ab dem Zeitpunkt der Ausstellung des Signaturschlüssel-Zertifikats.[49] Eine Abgabe der Zertifikatsdokumentation an Archive ist nicht vorgesehen.[50] Wenn digitale Grundbücher oder Handelsregistereinträge den Archiven zur Übernahme angeboten werden, ist die 35jährige Aufbewahrungsfrist im Zweifelsfall bereits abgelaufen. Abgesehen von den bereits genannten Problemen scheitert eine Verifizierung archivierter Signaturen unter Umständen schon daran, daß der vertrauenswürdige Dritte, die Zertifizierungsstelle, seine im Gesamtkonzept der elektronischen Unterschrift notwendige Funktion nicht mehr wahrnehmen kann, da er nicht mehr über die Zertifikatsdokumentation verfügt. Ob über vertragliche Sonderregelungen mit Zertifizierungsstellen eine dauerhafte Verfügbarkeit der Dokumentation und der für jede Signaturschicht erforderlichen Hard- und Softwareumgebung zu ökonomisch tragfähigen Bedingungen gewährleistet werden kann, bleibt abzuwarten.[51]

---

[46] International Council on Archives. Committee on Electronic Records: Guide for managing electronic records from an archival perspective (ICA Studies 8). Paris 1997. S. 47f.

[47] Vgl. zur Zuordnung von Zertifikaten § 5 Abs. 1 Satz 2 SigG und zum Inhalt von Zertifikaten § 7 Abs. 1 SigG.

[48] § 10 SigG.

[49] § 13 Abs. 2 SigV.

[50] Lediglich für den Fall, daß eine Zertifizierungsstelle ihre Tätigkeit einstellt und ihre Zertifikatsdokumentation nicht von einer anderen Zertifizierungsstelle in der Nachfolge übernommen wird, soll die Dokumentation an die zuständige Behörde abgegeben werden (§ 11 Abs. 2 SigG und § 14 Abs. 4 SigV). Nur auf diesem Weg wäre eine Übernahme der Dokumentation in ein öffentliches Archiv möglich, was aber – den Erfolg des Signaturgesetzes vorausgesetzt – wohl nur für den geringeren Teil der Zertifikatsdokumentation der Fall sein dürfte.

[51] In der Begründung zur Verordnung zur digitalen Signatur in der Fassung des Beschlusses der Bundesregierung vom 8. Oktober 1997, wie Anm. 40, heißt es zu § 13 Abs. 2: *So-*

Fazit

Das Konzept der digitalen Signatur und die diesbezüglichen Regelungen des Gesetzgebers mögen kurz- und mittelfristige Rechtssicherheit gewährleisten. Daß im Rahmen der behördlichen Aufbewahrungs- und Aussonderungsvorschriften Unterlagen – auch digital signierte Unterlagen – nach Ablauf bestimmter Fristen ordnungsgemäß ausgesondert und den Archiven zur Übernahme angeboten werden müssen, ist in die Überlegungen des Gesetzgebers allerdings nicht eingeflossen. Eine dauernde Aufbewahrung elektronischer Unterschriften ist in den bestehenden Gesetzen und Verordnungen *de facto* nicht eingeplant.

Es ist in diesem Zusammenhang bemerkenswert, daß am 11. Juni 1997 ein Entschließungsantrag in den Bundestag eingebracht wurde, der unter anderem vorsieht, elektronisch abgewickelte Rechtsgeschäfte wieder auf Papier zu sichern: *Eine zentrale, hoheitliche Dokumentationsstelle sollte es den Teilnehmern am digitalen Signiersystem auf freiwilliger Basis erlauben, die signierten Dokumente sicher und dauerhaft in materialisierter Form zu hinterlegen, um für den Fall eines Versagens der technischen und organisatorischen Systeme Konfliktfälle lösen zu können.*[52] Kann darin auch nicht ernsthaft die Lösung für den elektronischen Rechtsverkehr gesehen werden,[53] so zeigt der Entschließungsantrag doch die Unsicherheiten in Verbindung mit der digitalen Signatur.

Vor diesem Hintergrund können auch Archive nicht das Unlösbare lösen, sondern sollten dort, wo es möglich ist, auf eine Übernahme digitaler Signaturen verzichten. Die meisten Archivbenutzer dürfte das kaum stören. Man nimmt damit in Kauf, daß auch ursprünglich signierte Dokumente keinen Anscheinsbeweis beanspruchen können, sondern der freien richterlichen Beweiswürdigung unterliegen. Diese, durch die aktuelle Rechtslage herbeigeführte Situation kann aber – sofern daran überhaupt ein gesellschaftliches Interesse besteht – nur vom Gesetzgeber korrigiert werden. Eine Alternative bestünde womöglich darin, öffentliche Archive als vertrauenswürdige Instanzen aufzufassen, so daß – ähnlich dem früheren *ius archivi* – dort aufbewahrtes, ursprünglich digital signiertes Schriftgut öf-

---

weit in bestimmten Bereichen (z. B. Medizin) längere Aufbewahrungsfristen erforderlich sind, muß dies über eigene Zertifizierungsstellen oder vertragliche Vereinbarungen sichergestellt werden. Soweit die Dokumentation in digitaler Form erfolgt (z. B. bei den Zertifikaten), schließt „verfügbar" (Satz 1) die Überprüfbarkeit ein, das heißt, es muß dafür geeignete Hard-/Software zur Verfügung stehen. Vergleichbar lange Fristen bestehen z. B. für „digitale Dokumente" beim Flugzeugbau (50 Jahre) oder beim elektronischen Grundbuch, das auf Dauer geführt wird.

[52] Bundestagsdrucksache 13/7936. S. 7.

[53] Klaus-Werner *Schröder*: Digitale Signaturen – wer beherrscht wen?. In: Kulturelle Beherrschbarkeit digitaler Signaturen. Interdisziplinärer Diskurs zu querschnittlichen Fragen der IT-Sicherheit. Hg. vom Bundesamt für Sicherheit in der Informationstechnik. Ingelheim 1997. S. 68–78, geht im Zusammenhang mit der Alterungsproblematik digitaler Signaturen davon aus, *daß die beweiskräftige Archivierung als besondere Dienstleistung einer neutralen Stelle an Signierende oder Verfizierende angeboten wird* (S. 77), macht aber keine Angaben über die mögliche Dauer einer solchen „Archivierung" und räumt ein, daß die maßgeblichen Anforderungen an eine solche Stelle erst noch definiert werden müssen.

fentlicher Behörden *per se* Authentizität beansprüchen dürfte.[54] Man darf aber nicht verkennen, daß gerade mangelndes Vertrauen in die Integrität elektronischer Dokumente den Hintergrund der Signaturgesetzgebung bildet, so daß es sicherlich erheblicher Bemühungen und Verfahrensregelungen bedarf, um dieses Ziel zu realisieren.

Daneben sind weitere Gespräche mit Vertretern der Behörden und Gerichte, in denen elektronische Signaturen zum Einsatz gelangen sollen, notwendig. Die für die elektronischen Register zuständigen Vertreter der nordrhein-westfälischen Justiz haben die Probleme um die digitale Signatur erkannt und in der logischen Konsequenz vorgeschlagen, auf eine Archivierung elektronischer Unterschriften zu verzichten. Die Durchführbarkeit dieses Vorschlags wird allerdings durch die Gesetzeslage verwehrt. Grundbuchverfügung und Handelsregisterverfügung bestimmen nämlich, daß die vom Rechtspfleger unterschriebene Eintragung *und* die elektronische Unterschrift Bestandteil des maschinell geführten Grundbuchs bzw. Handelsregisters werden.[55] Da eine dauernde Aufbewahrung geschlossener Grundbücher und Handelregister vorgeschrieben ist,[56] muß folglich die Summe ihrer Bestandteile dauerhaft aufbewahrt werden. Die Übernahme elektronischer Unterschriften ist somit bei einer Archivierung der digitalen Register erforderlich, obwohl – oder vielleicht besser weil – eine Archivierung signierter Unterlagen vom Gesetzgeber nicht bedacht wurde. Bleiben die rechtlichen Rahmenbedingungen unverändert, dann geraten Archive in die mißliche Lage, in Zukunft auch unbrauchbare Daten aufbewahren und pflegen zu müssen.

---

[54] Dieses Ziel wurde bereits von Michael *Wettengel*: Digitale Unterschriften. In: Der Archivar 50 (1997) Sp. 90–94, hier Sp. 94, angedeutet. – Vgl. ausführlich Udo *Schäfer*: Authentizität. Vom Siegel zur digitalen Signatur. In diesem Band.

[55] § 75 Satz 3 GBV und § 57 Satz 2 HRV.

[56] § 72 Abs. 2 GBV bestimmt, daß der Inhalt geschlossener, maschinell geführter Grundbuchblätter weiterhin wiedergabefähig oder lesbar bleiben soll. Nach § 60 Abs. 2 HRV sollen geschlossene, maschinell geführte Registerblätter weiterhin, auch in der Form von Ausdrucken, wiedergabefähig oder lesbar bleiben. Die Datenträger für geschlossene Registerblätter können auch bei der für die Archivierung von Handelsregisterblättern zuständigen Stelle verfügbar gehalten werden. – Vgl. § 10 a Abs. 1 Satz 1, Abs. 2 Satz 2 GBO. – Vgl. im übrigen die Aufbewahrungsbestimmungen. Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden. Beschluß der Konferenz der Justizverwaltungen des Bundes und der Länder vom 23. und 24. November 1971 in Düsseldorf. Stand: 1996. Nr. 71, 73.