February 2005

Die qualifizierte elektronische Signatur - Vertrauensbonus vom Gesetzgeber, Schaffung von Vertrauen bei den Bürgern durch das deutsche Signaturbündnis?

Susanne Schreiber
Technische Universität Dresden

In: Ferstl, Otto K, u.a. (Hg) 2005. *Wirtschaftsinformatik 2005: eEconomy, eGovernment, eSociety*; 7. Internationale Tagung Wirtschaftsinformatik 2005. Heidelberg: Physica-Verlag

ISBN: 3-7908-1574-8

Die qualifizierte elektronische Signatur

- Vertrauensbonus vom Gesetzgeber, Schaffung von Vertrauen bei den Bürgern durch das deutsche Signaturbündnis?

Susanne Schreiber
Technische Universität Dresden

Zusammenfassung: In Deutschland sind die rechtlichen Rahmenbedingungen für den Einsatz der qualifizierten elektronischen Signatur günstig. So wurde etwa nach der Gleichstellung der elektronischen Form mit der Schriftform im Privatrecht auch im Verwaltungsverfahrensrecht die rechtsverbindliche elektronische Kommunikation eingeführt. Dennoch konnte sich die qualifizierte elektronische Signatur noch nicht im erforderlichen Maße durchsetzen. Im Folgenden wird untersucht, ob das deutsche Signaturbündnis als eine geeignete Lösung zur Vertrauensschaffung und damit zur Gewinnung der notwendigen kritischen Masse anzusehen ist. Anhand der Analyse ausgewählter wichtiger Problembereiche wird deutlich, dass die Realisierung dieser Ziele nicht leicht sein wird. Außerdem werden zusätzliche Maßnahmen zur Vertrauensschaffung nötig sein.

Schlüsselworte: Signaturbündnis, qualifizierte elektronische Signatur, Signaturgesetz, Gültigkeitsmodell, Pseudonym-Zertifikate, Präsentationsproblem, Warnfunktion der Unterschrift, Vertrauensschaffung

1 Einleitung

Obwohl Deutschland im Hinblick auf die Rahmenbedingungen für den Einsatz qualifizierter elektronischer Signaturen „weltweit eine Spitzenstellung“ [Roßn03a, S. 1] einnimmt, konnte sich die qualifizierte elektronische Signatur bislang noch nicht in der für einen elektronischen Geschäfts- und Rechtsverkehr notwendigen Breite durchsetzen. Dabei könnten qualifizierte elektronische Signaturen in den unterschiedlichsten Lebensbereichen eingesetzt werden. Nicht nur beispielsweise im eCommerce, sondern etwa auch im eGovernment könnten so allen Beteiligten Vorteile verschafft werden. Vor allem um die erforderliche kritische Masse von Nutzern zu gewinnen, wurde im April 2003 das deutsche Signaturbündnis gegründet.

Im Folgenden wird zunächst kurz beleuchtet, inwiefern die qualifizierte elektronische Signatur im geltenden deutschen Recht der eigenhändigen Unterschrift gleichgestellt ist; es geht dabei also um den Vertrauensbonus des Gesetzgebers für die qualifizierte elektronische Signatur. Daran anschließend wird untersucht, ob das Signaturbündnis als eine geeignete Lösung zur Vertrauensschaffung anzusehen ist. Denn Vertrauen ist eine grundlegende Voraussetzung für die Anwendung qualifizierter elektronischer Signaturen. Analysiert werden hierbei ausgewählte Problembereiche, und zwar sowohl technische Problemfelder – wie etwa das Gültigkeitsmodell oder auch die generellen Grenzen sicherheitstechnischer Lösungen – als auch die Kostenfrage sowie Problembereiche, die sich aus der geplanten kleinen Novelle des Signaturgesetzes (SigG) ergeben. Eingegangen wird außerdem auf nötige flankierende Maßnahmen zur Vertrauensschaffung.

2 Weitgehende Gleichstellung der qualifizierten elektronischen Signatur mit der eigenhändigen Unterschrift im geltenden Recht

2.1 Ausgangspunkt: Die EU-Signaturrichtlinie

Vor allem aufgrund der Ende der neunziger Jahre feststellbaren zunehmenden normativen Diversifizierung wurde eine europäische Initiative zur digitalen Signatur veranlasst [Schm02, S. 509]. So wurde im Dezember 1999 die Richtlinie 1999/93/EG – die so genannte EG-Signaturrichtlinie – verabschiedet. Diese war von den Mitgliedstaaten bis zum 19.7.2001 in nationales Recht umzusetzen. In erster Linie bestand das Ziel der Richtlinie in der Harmonisierung und Sicherstellung der grenzüberschreitenden rechtlichen Anerkennung elektronischer Signaturen. Denn divergierende Regelungen im Hinblick auf die rechtliche Anerkennung können sich als eine spürbare Behinderung des elektronischen Handels und der Entwicklung eines gemeinsamen Marktes erweisen [Dum+04, S. 143; LaUl02, S. 85]. Unter anderem regelte die EU-Signaturrichtlinie auch die Voraussetzungen, unter denen die Mitgliedstaaten elektronische Signaturen mit der eigenhändigen Unterschrift gleichzustellen haben und außerdem das Gebot, elektronische Signaturen in gerichtlichen Verfahren als Beweismittel zuzulassen.

In Deutschland führten die Vorgaben der EU-Signaturrichtlinie zum einen zu einer Novellierung des Signaturgesetzes durch das Gesetz über Rahmenbedingungen für elektronische Signaturen. Zum anderen wurden die Folgeänderungen im Privatrecht durch das „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr“ (GAFP) bewirkt.

2.2 Anpassung des geltenden Rechts: Wichtige ausgewählte Gesetzesänderungen

Durch das GAFP ergaben sich einige Änderungen im Bürgerlichen Gesetzbuch (BGB) sowie in der Zivilprozessordnung (ZPO). So wurde etwa im Bürgerlichen Gesetzbuch die Vorschrift des § 126 Abs. 3 BGB eingefügt. Diese bestimmt, dass die schriftliche Form grundsätzlich durch die elektronische Form ersetzt werden kann. In § 126a BGB werden die Voraussetzungen angeführt, die die elektronische Form erfüllen muss, um die durch Gesetz vorgeschriebene Schriftform zu ersetzen. Dafür ist gemäß § 126a BGB eine qualifizierte elektronische Signatur (nach dem Signaturgesetz) erforderlich; außerdem muss der Aussteller der Erklärung dieser seinen Namen hinzusetzen. Im Unterschied zu fortgeschrittenen elektronischen Signaturen sind qualifizierte elektronische Signaturen dadurch charakterisiert, dass sie auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit – also einer Smartcard – erzeugt werden.[1]

Ebenfalls durch das GAFP wurde in die Zivilprozessordnung eine neue Vorschrift aufgenommen, nämlich § 292a ZPO. Danach kann der Anschein der Echtheit einer in elektronischer Form (§ 126a BGB) vorliegenden Willenserklärung lediglich durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist. Somit ergibt sich als Rechtsfolge des § 292a ZPO der Anschein der Echtheit der Willenserklärung, deren Abgabe und auch der willentlichen Entäußerung durch den Sigaturschlüssel-Inhaber [Jung02, S. 136; Jung03, S. 71; Fis+02, S. 710]. Daraus wird erkennbar, dass diese Vorschrift zu einer „beweisrechtlichen Privilegierung“ [Schm02, S. 514] von qualifizierten elektronischen Signaturen führt. Insofern haben qualifizierte elektronische Signaturen durch die Regelung gemäß § 292a ZPO vom Gesetzgeber einen klaren „Vertrauensbonus“ [Jung03, S. 72] erhalten. Zu unterstreichen ist jedoch, dass die Einführung einer derartigen Beweisregelung nicht vom europäischen Recht vorgeschrieben wurde, sondern eine Schlussfolgerung der Bundesregierung aus der Diskussion um die Beweisfragen elektronisch signierter Dokumente darstellt [Roßn01, S. 1819; Geis02, S. 60].

Bedeutsam ist im Übrigen in diesem Zusammenhang, dass nach der grundsätzlichen Gleichstellung der elektronischen Form mit der Schriftform im Privatrecht[2] in Deutschland auch die rechtsverbindliche elektronische Kommunikation in der öffentlichen Verwaltung eingeführt worden ist. Auch das neue Verwaltungsverfahrensrecht entscheidet sich hierbei generell für eine qualifizierte elektronische Signatur (§ 3a VwVfG). Damit wird die qualifizierte elektronische Signatur

---

1 Vgl. § 2 Nr. 3 SigG.

2 Zum Ausschluss bestimmter Anwendungen von dieser Regel durch den Gesetzgeber vgl. 3.4.4.

„gleichrangiges Äquivalent der herkömmlichen Schriftform und gesetzliches Leitbild rechtsverbindlichen elektronischen Verwaltungshandelns“ [Wohl02, S. 235].

3 Das Signaturbündnis – geeignete Lösung zur Vertrauensschaffung?

3.1 Ausgangssituation

Obgleich die rechtlichen Rahmenbedingungen für die qualifizierte elektronische Signatur in Deutschland somit günstig sind, konnte sie sich bisher noch nicht in der für einen elektronischen Geschäfts- und Rechtsverkehr notwendigen Breite durchsetzen [Roßn03a, S. 1; Büg+04, S. 133ff]. Zum einen hängt dies damit zusammen, dass viele potentielle Nutzer nicht das erforderliche Vertrauen in die Sicherheit des eCommerce und des eGovernment haben. So führen etwa Betrügereien bei Online-Händlern zu Verlusten und bewirken bei etlichen potentiellen Kunden, dass sie – aufgrund von Angst vor späterem Ärger – die Möglichkeit des Online-Shoppings gar nicht erst nutzen.

Zum anderen ist der Nutzen von qualifizierten elektronischen Signaturen in der Praxis eher gering, wenn sich nicht viele Kommunikationspartner an diesem System beteiligen [Fox04, S. 130; Büg+04, S. 135]. Denn der Nutzen einer solchen Infrastruktur steigt mit der Anzahl der Teilnehmer. Wird das System lediglich von wenigen Teilnehmern genutzt, erweist sich die Bereitschaft von Unternehmen als gering, Applikationen dafür zu schaffen. Gibt es jedoch nur wenige Applikationen, schätzen viele potentielle Nutzer eine etwaige Teilnahme als nicht lohnend ein.

Die damit zusammenhängende Hürde ist umso größer, je höher die anfänglichen Kosten für potentielle Nutzer sind. Außerdem wird die momentan geringe Nutzerzahl weiterhin niedrig bleiben, sofern für fast jeden Anwendungsbereich – etwa Online-Banking, Steuererklärung, virtuelles Rathaus, Bundesverwaltung – ein eigenes Signaturverfahren verwendet wird, das sich von den Signaturverfahren der anderen Bereiche unterscheidet und daher in diesen anderen Bereichen nicht verwendet werden kann. Daraus ergibt sich, dass keine dieser Teillösungen zu der nötigen wirtschaftlichen Rentabilität und der gesellschaftlichen Akzeptanz führen wird.

Mittlerweile wurde erkannt, dass ein gemeinsames Vorgehen aller Beteiligten erforderlich ist, um den Nutzen für alle zu erhöhen – für die Kunden beispielsweise Zeitersparnis durch eGovernment, für den Handel geringeres Risiko bei elektronischen Geschäften, für den Staat Kostenersparnis und für die Kreditwirtschaft die Durchführung von Finanzdienstleistungen ohne Medienbruch [Büg+04, S. 134] –

und zugleich die Kosten zu senken. Um die Verbreitung der elektronischen Signatur in Deutschland gemeinsam zu fördern, haben sich – initiiert von der Bundesregierung – staatliche Stellen, Kreditwirtschaft und Industrie zusammengetan und im April 2003 das „Bündnis für elektronische Signaturen“ – das so genannte Signaturbündnis – gegründet. Inzwischen sind diesem Bündnis weit mehr als 30 Partner beigetreten.

3.2 Zielsetzung des Signaturbündnisses

Wie im Rahmen der Vorgaben und Konvergenzziele für das Signaturbündnis unterstrichen wird, liegt der Zweck des Signaturbündnisses in erster Linie darin, die Anwendung, Verbreitung und Einführung chipkartenbasierter elektronischer Signaturen und anderer PKI-Anwendungen zu fördern [SigBüVK03, S. 3]. Dazu verpflichten sich die Bündnispartner, eine stabile Grundlage für interoperable Infrastrukturen auf Basis gemeinsam akzeptierter Standards zu schaffen.

So hat das Bündnis die folgende Vision: „ Der Bürger kann mit

- jeder beliebigen Chipkarte
- jedem Kartenleser
- eine Vielzahl – idealerweise alle –
- der verfügbaren Applikationen aus
- eCommerce und eGovernment nutzen“ [SigBü03, S. 1].

Als Ausgangspunkte des Signaturbündnisses lassen sich die Schwierigkeiten auffassen, wie das Problem der kritischen Masse überwunden werden kann und wie eine für sämtliche potentielle Nutzer zugängliche Sicherheitsinfrastruktur geschaffen werden kann. Um die Ziele des Signaturbündnisses erreichen zu können, sollen bereits vorhandene Infrastrukturen – wie etwa die Bankkarten der Kreditinstitute – genutzt werden. Da die zugrunde liegende Infrastruktur eine große Verbreitung besitzen muss, bieten sich die von der Kreditwirtschaft ausgegebenen Karten geradezu an, da fast alle volljährigen Bundesbürger Zugriff auf ein Bankkonto haben. Überdies muss aufgrund gesetzlicher Regelungen die Identifizierung von Kunden bei der Eröffnung von Konten sehr genau vorgenommen werden, wobei die Vorlage eines Ausweispapiers zwingend vorgeschrieben ist [Büg+04, S. 135].

So sollen die Bankkarten zukünftig mit einem Chip ausgestattet werden, der – in Verbindung mit einem Kartenleser – die Authentisierung im Netz sowie die rechtsverbindliche elektronische Unterschrift ermöglicht. Dabei besteht das Ziel darin, mit lediglich einer Karte als Zugang zu unterschiedlichen Anwendungen auszukommen; in diesem Zusammenhang spricht man daher von einer multifunktionellen Chipkarte [SigBüVK03, S. 5]. Neben der multifunktionellen Chip-

karte gehören auch die Einhaltung einheitlicher Sicherheitsniveaus sowie die Ermöglichung des Einsatzes qualifizierter Signaturen zu den Konvergenzzielen des Signaturbündnisses [SigBüVK03, S. 5]. Das Signaturgesetz unterscheidet nämlich zwischen einfachen, fortgeschrittenen[3] und qualifizierten Signaturen.[4] Da lediglich die qualifizierten elektronischen Signaturen – wie bereits hervorgehoben – in ihrer Rechtsfolge der handschriftlichen Unterschrift weitgehend gleichgestellt sind, sind qualifizierte elektronische Signaturen in diesem Zusammenhang besonders bedeutsam.

Sowohl das Signaturgesetz als auch die Signaturverordnung (SigV) geben einige Voraussetzungen vor, denen ein Anbieter entsprechen muss, der qualifizierte Signaturen herausgibt. So ist für qualifizierte elektronische Signaturen stets eine sichere Signaturerstellungseinheit – das heißt eine Smartcard – notwendig. Daneben werden hohe Anforderungen an die Identifizierung der Karteninhaber gestellt. Indessen war es – als Signaturgesetz und Signaturverordnung abgefasst wurden – nicht vorauszusehen, dass die Kundenkarten der Banken das Trägermedium darstellen würden. Nicht zuletzt um eine Anpassung des rechtlichen Rahmens an die üblichen Prozesse in der Kreditwirtschaft zu ermöglichen [Schu04, S. 32], wurde im April 2004 der Entwurf eines Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigÄndG) veröffentlicht.

3.3 Geplante „kleine“ Novelle des Signaturgesetzes

In der Begründung zum Entwurf des 1. SigÄndG wird unterstrichen, dass durch die geplante „kleine“ Novelle des Signaturgesetzes die Voraussetzungen für eine schnelle Beantragung und Ausgabe von Signaturkarten mit qualifizierten elektronischen Signaturen im elektronischen Verfahren geschaffen werden sollen [BSigÄndG04, S. 2]. Wie der Begründung außerdem zu entnehmen ist, sollen die Verfahrensprozesse beispielsweise bei der Registrierung und Ausgabe von EC- oder Bankkundenkarten, die im Wirtschaftsleben bereits seit langem eingeführt und bewährt sind, auch für die Ausgabe von Signaturkarten mit qualifizierten elektronischen Zertifikaten genutzt werden, und zwar mit den entsprechenden Synergieeffekten, etwa Kostenreduzierung bzw. Verwaltungsvereinfachung [BSigÄndG04, S. 2].

Bei den Änderungen gemäß dem Gesetzentwurf handelt es sich im Wesentlichen um Folgendes [ESigÄndG04, Artikel 1]: So soll § 5 SigG, der die Vergabe von qualifizierten Zertifikaten regelt, dahingehend geändert werden, dass die Verpflichtung zur Erteilung eines Pseudonyms vertraglich ausgeschlossen werden

---

3 Zu Details im Hinblick auf die fortgeschrittene elektronische Signatur und den damit verbundenen Problembereichen – insbesondere Sicherheitsniveau bzw. Manipulationsmöglichkeiten – vgl. [Roßn03b, S. 166ff].

4 Vgl. § 2 SigG.

kann. Außerdem soll für die Unterrichtung gemäß § 6 SigG in Zukunft die Textform ausreichen. Bisher hat der Zertifizierungsdiensteanbieter nach § 6 Abs. 3 SigG dem Antragsteller eine schriftliche Belehrung über die Maßnahmen auszuhändigen, die notwendig sind, um zur Sicherheit von qualifizierten elektronischen Signaturen und deren zuverlässiger Prüfung beizutragen; überdies muss der Antragsteller darüber unterrichtet werden, dass einer qualifizierten elektronischen Signatur im Rechtsverkehr weitgehend die gleiche Wirkung zukommt wie einer eigenhändigen Unterschrift. § 6 Abs. 3 SigG fordert zudem, dass der Antragsteller die Kenntnisnahme dieser Belehrung durch eine gesonderte Unterschrift zu bestätigen hat. Nach dem Entwurf des 1. SigÄndG soll das Erfordernis dieser handschriftlichen Bestätigung der Kenntnisnahme der Belehrung in Zukunft wegfallen.

Klar gestellt werden soll darüber hinaus, dass der Katalog der in § 8 SigG angeführten Gründe für die Sperrung von qualifizierten Zertifikaten vertraglich erweitert werden kann. Neu eingeführt werden soll nach dem Entwurf des 1. SigÄndG auch, dass Zertifizierungsdiensteanbieter unentgeltlich auf Ersuchen die Daten über die Identität eines Signaturschlüssel-Inhabers an die zuständigen Stellen übermitteln müssen, sofern dies zum Beispiel für die Verfolgung von Straftaten oder Ordnungswidrigkeiten oder zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung erforderlich ist.

Im Folgenden geht es darum, ausgewählte Problemfelder im Zusammenhang mit der qualifizierten elektronischen Signatur zu beleuchten und näher zu analysieren. Dabei werden sowohl generelle Problembereiche im Hinblick auf die qualifizierte elektronische Signatur als auch Problemfelder betrachtet, die sich aus der geplanten Änderung des Signaturgesetzes ergeben. Wichtig ist diese Analyse insbesondere vor folgendem Hintergrund, der auch in der Begründung zum Entwurf des 1. SigÄndG genannt wird: „Sicherheit und Vertrauen sind von zentraler Bedeutung im elektronischen Geschäftsverkehr und in der elektronischen Verwaltung. Kernstück zur Förderung dieses Vertrauens ist die qualifizierte elektronische Signatur“ [BSigÄndG04, S. 1]. Die Schaffung von Vertrauen ist generell vor allem deswegen so wichtig, weil Vertrauen als „komplexitätsreduzierender Mechanismus“ [LaUl02, S.51] dient [Voge01, S. 168].

3.4 Analyse ausgewählter Problembereiche

3.4.1 Gültigkeitsmodell

Während handschriftliche Unterschriften auch noch nach vielen Jahren ohne Schwierigkeiten überprüft werden können, ist dies bei qualifizierten elektronischen Signaturen bisweilen problematischer. Dies hängt damit zusammen, dass das nötige Signaturschlüsselpaar – das heißt einerseits der private Schlüssel zum Signieren, der auf der Karte gespeichert ist, und andererseits der öffentliche Schlüssel zum Verifizieren – lediglich so lange zum Erstellen der Signatur einge-

setzt wird, wie das betreffende Zertifikat gültig ist. Wenn der Anwender später die Folgekarte erhält, bekommt er damit ein neues Schlüsselpaar sowie ein zugehöriges Zertifikat.

Diese Beschränkung der Gültigkeit von Zertifikaten ist erforderlich, um ein dauerhaft hohes Sicherheitsniveau zu garantieren. Dadurch ist es möglich, die verwendeten Verfahren und auch die Schlüssellängen etwa an die Entwicklungen der Rechnerleistungen anzupassen [Büg+04, S. 137]. Der maximale Zeitraum für Anwenderzertifikate beträgt nach dem Signaturgesetz fünf Jahre.

Allerdings ergibt sich aus dieser zeitlichen Begrenzung, dass im Rahmen der Prüfung einer qualifizierten elektronischen Signatur zu untersuchen ist, ob die Zertifikate gültig waren. Diese Frage der Gültigkeit bezieht sich generell auf den Zeitpunkt der Erstellung der Signatur. Durch die digitale Unterschrift des Zertifizierungsdiensteanbieters im Anwenderzertifikat wird dessen Überprüfung ermöglicht. So kann die Gültigkeit dieses so genannten Certification Authorithy (CA)-Zertifikats geprüft werden [Büg+04, S. 137]. Dieses CA-Zertifikat kann dann wiederum auf andere CA-Zertifikate verweisen. Auf diese Weise kommt eine Kette von Zertifikaten zustande, wobei das letzte Zertifikat – das Wurzelzertifikat – grundsätzlich einen Vertrauensanker darstellt. Alle diese Zertifikate haben dabei jeweils einen bestimmten Gültigkeitszeitraum.

Indessen weichen diese Zeiträume prinzipiell voneinander ab. In Abhängigkeit von den Gültigkeitszeiträumen der Zertifikate in dieser Kette bestimmt das Gültigkeitsmodell, wann eine digitale Signatur als gültig aufzufassen ist [Ber+02, S.73]. Zur Zeit sind zwei verschiedene Gültigkeitsmodelle in Deutschland markt- und anwendungsrelevant: das Schalenmodell und das Kettenmodell. Jedoch unterstützen Anwendungen im Allgemeinen lediglich eines der beiden Modelle [SigBüVK03, S. 15].

Gemäß dem Schalenmodell gilt eine Signatur als gültig, wenn zu dem Zeitpunkt ihrer Erstellung sowohl das Anwenderzertifikat als auch sämtliche zugrunde liegenden Zertifikate gültig waren. Die Überprüfung erfolgt in „Schalen“. Dabei bildet das Anwenderzertifikat den innersten Kern, und die zugrunde liegenden Zertifikate bilden die höheren Schichten [Büg+04, S. 138]. Bedeutsam ist in diesem Zusammenhang, dass das Schalenmodell das einzige Gültigkeitsmodell ist, welches flächendeckend in Standardsoftware implementiert wurde. Es hat sich auch inzwischen zu einem internationalen Standard entwickelt.

Das zweite Modell wird als Kettenmodell bezeichnet. Dieses Modell geht auf den Inhalt von § 19 Abs. 5 SigG zurück. Dort wird nämlich verlangt, dass die „Gültigkeit der von einem Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikate … von … der Einstellung der Tätigkeit … unberührt“ bleiben muss. Auf den ersten Blick scheint dies nicht mit dem Schalenmodell konform zu gehen. Denn eine Sperrung eines CA-Zertifikates bewirkt hierbei, dass danach mit keinem unter diesem CA-Zertifikat ausgegebenen Anwenderzertifikat die Erstellung einer gültigen Signatur erreicht werden kann [Ber+02, S. 73; Büg+04, S. 138].

Aufgelöst wird dieser Gegensatz zum bestehenden deutschen Signaturgesetz jedoch, wenn man im Gültigkeitsmodell nur fordert, dass das CA-Zertifikat im Zeitpunkt der Ausgabe des Anwenderzertifikats gültig gewesen sein muss. Zu bedenken ist hierbei auch, dass Signaturgesetz und Signaturverordnung nicht explizit ein bestimmtes Gültigkeitsmodell festlegen. Auch das zuständige Bundesministerium für Wirtschaft und Arbeit hat mittlerweile klargestellt, dass der Inhalt von § 19 Abs. 5 SigG keinesfalls das Schalenmodell in der soeben erläuterten Form ausschließt, wenn dies vertraglich bei der Signaturkartenausgabe vereinbart wird [Büg+04, S. 138].

Im Rahmen der Vorgaben und Konvergenzziele haben sich die Teilnehmer des Signaturbündnisses auf eine Anwendung des Schalenmodells geeinigt [SigBüVK03, S. 15]. Weil dieses Gültigkeitsmodell den internationalen Standard darstellt und bereits in der Standardsoftware implementiert ist, erscheint dies als sinnvoll. Zudem ist das Schalenmodell in der dargelegten Form mit dem Signaturgesetz vereinbar.

3.4.2 Pseudonym-Zertifikate

Vor allem aus Sicht der Banken ein kritischer Punkt am bestehenden Signaturgesetz ist der Inhalt des § 5 Abs. 3 SigG, der dem Anwender die Möglichkeit eröffnet, ein Pseudonym-Zertifikat zu erhalten. So möchten die Kreditinstitute generell nicht verpflichtet werden, Bankkarten an Pseudonyme auszugeben [Büg+04, S. 136].

Im Zuge der geplanten „kleinen“ Novelle des Signaturgesetzes soll daher – wie bereits erwähnt – § 5 Abs. 3 SigG dahingehend geändert werden, dass in Zukunft vertraglich die Verpflichtung zur Erteilung eines Pseudonym-Zertifikats ausgeschlossen werden kann. Folglich soll es sich damit zukünftig bei der Erteilung eines Pseudonyms nicht um eine Pflichtdienstleistung, sondern lediglich um eine Wahldienstleistung des Zertifizierungsdiensteanbieters handeln. Insofern sollen die Vorgaben des Signaturgesetzes auf europäisches Niveau abgesenkt werden. Denn nach dem Inhalt der EU-Signaturrichtlinie zählt die Möglichkeit der Aufnahme eines Pseudonyms nicht zu den zwingenden Anforderungen an ein qualifiziertes Zertifikat [BESigÄndG04, S. 6].

Allerdings enthält die momentan gültige Fassung des § 5 Abs. 3 SigG für die Anwender sozusagen einen Schutz-Mechanismus. So können sich Anwender durch den Gebrauch von Pseudonymen gegen das Erstellen von Persönlichkeitsprofilen schützen („Selbst-Datenschutz“) [BESigÄndG04, S. 5]. Prinzipiell erhöht die Verwendung elektronischer Signaturen das Risiko, dass Datenspuren entstehen, die zu einem Persönlichkeitsbild zusammengefügt werden könnten [Horn04, S. 6]. Durch den Gebrauch von Pseudonymen wird verhindert, „dass der Nutzer im elektronischen Geschäftsverkehr aufgrund der zahlreichen Datenspuren ausgeforscht werden kann“ [HoGr02, S. 83]. Vor allem kann so „das Vertrauen des Nutzers in den elektronischen Geschäftsverkehr gestärkt werden“ [HoGr02, S.

83]. Aus diesem Grunde muss anonymes bzw. pseudonymes Handeln weiterhin diskriminierungsfrei möglich sein [Dum+04, S. 146]. Durch pseudonymes Handeln können außerdem die in den modernen Datenschutzgesetzen verankerten Prinzipien der Datenvermeidung und der Datensparsamkeit erfüllt werden [HoGr02, S. 83; LaUl02, S. 20]. Das Recht auf informationelle Selbstbestimmung, das als eine notwendige Voraussetzung für eine funktionierende Demokratie anzusehen ist [Klew03, S. 159; FeHa03, S. 262], erscheint „heute wichtiger denn je" [Bäum03, S. 160].

Durch die Verwendung von Pseudonymen wird verantwortliches Handeln ermöglicht, ohne dass die Identität des Handelnden offen gelegt werden muss, solange die Transaktionen störungsfrei ablaufen. Die Bedingungen hierfür müssen „jedermann zu bequemen Bedingungen offen stehen" [LaUl02, S. 20]. Ob dies auch nach der geplanten Gesetzesänderung weiterhin der Fall sein wird, bleibt abzuwarten. Sollte die Gesetzesänderung jedoch bewirken, dass es für Anwender sehr schwierig wird, Pseudonym-Zertifikate zu erhalten, könnte dies dazu führen, dass das Vertrauen vieler Anwender erheblich sinken wird. Dies würde allerdings der Zielsetzung des Signaturbündnisses zuwiderlaufen. Generell ist der „Aufbau von Strukturen für die breite Nutzung elektronischer Signaturen … nur zu verantworten, wenn die Inanspruchnahme von Pseudonymen … zu angemessenen Kosten und ohne Diskriminierung gewährleistet ist" [LaUl02, S. 20]. Denn es ist zu beachten, dass die „umfassende Gewährleistung von Datenschutz und Datensicherheit … der entscheidende Akzeptanzfaktor für eine wirklich breite Nutzung von internetbasierten eGovernment-Anwendungen in Deutschland" [Nedd03, S. 128] ist.

3.4.3 Geplante Änderungen im Hinblick auf die Unterrichtungspflicht

Ebenfalls aus Sicht der Kreditinstitute nachteilig am bestehenden Signaturgesetz ist der Inhalt von § 6 Abs. 3 SigG, der bestimmt, dass die vorgeschriebene schriftliche Belehrung dem Antragsteller auszuhändigen ist und dieser deren Kenntnisnahme durch eine gesonderte Unterschrift zu bestätigen hat; dies impliziert eine „persönliche Anwesenheit des Antragstellers beim Zertifizierungsdiensteanbieter oder einem von ihm eingesetzten Dritten" [Skro04, S. 412]. So wird argumentiert, dies stehe nicht im Einklang mit der üblichen Praxis der Banken, bei der die Karten an die Kunden versendet werden. Zudem seien Bankkunden nicht daran gewöhnt, am Bankschalter obligatorisch belehrt zu werden [Büg+04, S. 136]. Gemäß dem Entwurf des 1. SigÄndG soll – wie schon betont – für die Unterrichtung gemäß § 6 SigG in Zukunft die Textform genügen. Außerdem soll das Erfordernis der Bestätigung der Kenntnisnahme der Belehrung zukünftig wegfallen. Auch insofern soll das deutsche Signaturgesetz an die Signaturgesetze anderer EU-Mitgliedstaaten angepasst werden. Das Erfordernis einer handschriftlichen Bestätigung der Kenntnisnahme findet sich auch nicht in der EU-Signaturrichtlinie.

Insgesamt wird erkennbar, dass der Entwurf des 1. SigÄndG die Hürden „auf dem Weg zur „berührungslosen“ Beantragung … von Signaturkarten“ [Skro04, S. 412] beseitigt. Somit sollen künftig Signaturkarten für qualifizierte elektronische Signaturen beantragt werden können, ohne dass es zu einer persönlichen Überprüfung des Antragstellers kommt. Diese doch eher geringe Sicherheit in Bezug auf die Identifizierung des Antragstellers erscheint problematisch, nicht zuletzt angesichts der weitreichenden Rechtsfolgen der Verwendung qualifizierter elektronischer Signaturen, insbesondere in Anbetracht der „Beweisprivilegierung durch den Anscheinsbeweis in § 292a ZPO“ [Bize04, S. 388].

Zu bedenken ist in diesem Zusammenhang auch, dass sich der deutsche Gesetzgeber bereits ursprünglich bei der Schaffung des Signaturgesetzes der Tatsache bewusst war, dass ein nur auf einem Bildschirm vorhandener Text unter Umständen leichter oder aber sogar leichtfertig unterzeichnet wird, während dies bei einem verkörperten Dokument im Allgemeinen nicht getan wird [Schm02, S. 515]. Diesem Umstand soll in erster Linie dadurch Rechnung getragen werden, dass der Zertifizierungsdiensteanbieter denjenigen, der ein qualifiziertes Zertifikat beantragt, gemäß § 6 Abs. 2 SigG schriftlich darüber belehren muss, dass im Rechtsverkehr eine qualifizierte elektronische Signatur prinzipiell die gleiche Wirkung hat wie eine eigenhändige Unterschrift; diese schriftliche Belehrung darüber hat der Antragsteller nach § 6 Abs. 3 SigG schriftlich zu bestätigen.

Ob eine Belehrung, die dem Antragsteller lediglich in Textform übermittelt wird und deren Kenntnisnahme er nicht durch eine gesonderte Unterschrift bestätigen muss, genügt, um bei allen Signierenden ein ausreichendes rechtsgeschäftliches Handlungsbewusstsein zu erzeugen, mag sehr bezweifelt werden. Auch die Inhalte der geplanten neuen Anfügungen in § 5 SigG – das heißt die geplanten neuen Absätze 7 und 8 – dürften daran wenig ändern.

3.4.4 Warnfunktion der Unterschrift

Eng damit hängt Folgendes zusammen: Wie schon erläutert, kann die gesetzliche Schriftform durch die elektronische Form – mit einer qualifizierten elektronischen Signatur – generell ersetzt werden. Allerdings sind vom Gesetzgeber bestimmte Anwendungen von dieser Regel ausgeschlossen worden. Dies hat folgenden Hintergrund: Die Unterschrift in Schriftform erfüllt verschiedene Funktionen: die Abschlussfunktion, die Perpetuierungsfunktion, die Identitätsfunktion, die Echtheitsfunktion, die Verifikationsfunktion, die Beweisfunktion und die Warnfunktion. Dabei bedeutet Warnfunktion, dass der Unterschreibende durch den bewussten Akt der Unterzeichnung auf die erhöhte rechtliche Verbindlichkeit aufmerksam gemacht wird. In erster Linie soll dies dazu dienen, ihn vor übereilten Rechtsgeschäften zu schützen [Uhlm03, S. 177; Ber+02, S. 72].

So hat der Gesetzgeber etwa für Bürgschaftserklärungen (§ 766 BGB), Schuldversprechen (§ 780 BGB), sowie Anerkenntnis (§ 781 BGB) jeweils die elektronische Form ausgeschlossen. Dies lässt sich mit der Warnfunktion der Unter-

schrift erklären. Denn der Schuldner soll vor einer übereilten Erklärung geschützt werden [Schm02, S. 514]. Zwar entfalten auch die einzelnen Schritte im Rahmen der qualifizierten elektronischen Signatur durchaus eine deutliche Warnfunktion. Zumindest aus subjektiven Gründen hat die Warnfunktion der Unterschrift bei der elektronischen Form gegenüber der Schriftform noch Nachteile [Ber+02, S. 72]. Nach Ansicht des Gesetzgebers gewährt die Schriftform aufgrund der herkömmlichen Assoziation von Schriftlichkeit mit Verbindlichkeit zumindest mittelfristig noch einen besseren Übereilungsschutz. Dies ist ausschlaggebend, wenn die Rechtsfolgen derart wesentlich sind. Zu Recht hat aber der Gesetzgeber deutlich gemacht, dass sich dies ändern könnte, wenn sich die elektronische Form (mit der qualifizierten elektronischen Signatur) in ähnlicher Weise wie die Schriftform etabliert hat.

3.4.5 Keine Anbieterakkreditierung?

Aus den Reihen der Vertreter der Kreditinstitute im Rahmen des Signaturbündnisses sind Stimmen zu hören, die sich gegen eine Anbieterakkreditierung aussprechen. So würde eine Anbieterakkreditierung für die Anbieter vor allem hohe Kosten nach sich ziehen, die letztendlich die Nutzer zu tragen hätten. Überdies stünden diese zusätzlichen Kosten in keinem Verhältnis zu dem erwarteten Nutzen für den Gebrauch im normalen Geschäftsleben [Büg+04, S. 139].

Dabei ist indessen Mehreres zu bedenken: Angesichts einer behördlichen Vorabkontrolle bei der Akkreditierung „wird ein behauptetes Sicherheitsniveau auf Seiten des Anbieters schwerer zu erschüttern sein als bei nicht akkreditierten Verfahren“ [Jung03, S. 72]. Insofern unterscheidet sich der Beweiswert beider Verfahren. Allerdings wird hiervon lediglich der Bereich des Zertifizierungsdiensteanbieters betroffen, nicht dagegen der kritische Bereich des Signaturkarten-Inhabers. Somit spiegelt sich die Sicherheit akkreditierter Verfahren zum Beispiel bei dem Einsatz sicherer technischer Komponenten wie Verzeichnis-, Sperr- und auch Zeitstempeldiensten wider.

Außerdem sollen sich die von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten Zertifikate gegenüber den anderen qualifizierten Zertifikaten unter anderem insbesondere dadurch auszeichnen, dass sie langfristig prüfbar sind. So muss sichergestellt sein, dass alle Zertifikate von akkreditierten Zertifizierungsdiensteanbietern mindestens 30 Jahre lang online überprüft werden können.

Im Unterschied dazu müssen bei qualifizierten Signaturverfahren ohne Anbieterakkreditierung Zertifikate lediglich für eine vergleichsweise kurze Zeit aufbewahrt sowie prüfbar oder abrufbar gehalten werden, und zwar für die Dauer ihrer Gültigkeit zuzüglich fünf Jahre ab Jahresende [Roßn02, S. 218]. Folglich bieten qualifizierte Signaturen ohne Anbieterakkreditierung keine Gewähr für eine langfristige Prüfbarkeit [Stor02, S. 579]. Allerdings sind für rechtlich verbindliche elektronische Willenserklärungen, welche „notfalls auch als Beweismittel vor Gericht dienen sollen, … für viele Anwendungen das Sicherheitsniveau und die Nachweis-

sicherheit akkreditierter Signaturverfahren … erforderlich“ [Roßn02, S. 221], ebenfalls auch „in allen Anwendungen, in denen nicht auszuschließen ist, dass die signierten Daten nach fünf Jahren noch benötigt werden“ [Roßn02, S. 221].

Insgesamt ist zu unterstreichen, dass qualifizierte elektronische Signaturen mit Anbieterakkreditierung das positive Image haben, „über die beste Qualität und das höchste Sicherheitsniveau zu verfügen und damit allen Anforderungen gewachsen zu sein“ [Roßn02, S. 222]. Bei der Akkreditierung handelt es sich somit um eine Art Gütesiegel [Geis02, S. 61; Ber+02, S. 75]. Damit dürften allein qualifizierte elektronische Signaturen mit Anbieterakkreditierung dem grundlegenden Ziel des Signaturbündnisses – der Schaffung von Vertrauen bei den Bürgern – dienlich sein.

Will man das Vertrauen der Bürger in die qualifizierte elektronische Signatur erhöhen, bedarf es dazu glaubwürdiger Signale. Aus der Informationsökonomie weiß man, „dass nur teure Signale glaubwürdig sein können. Andernfalls wären sie leicht zu imitieren“ [Ball04, S. I] und würden Besseres von Schlechterem „nicht zu unterscheiden erlauben“ [Ball04, S. I]. Auch wenn Anbieterakkreditierungen teuer sind, sollte man daher nicht auf sie verzichten.

3.4.6 Generelle Grenzen sicherheitstechnischer Lösungen

Allerdings vermag all dies nicht darüber hinwegzutäuschen, dass es im Zusammenhang mit digitalen Signaturen generelle Probleme gibt, die zwar bekannt, aber noch immer ungelöst sind. Hierzu zählt beispielsweise das Präsentationsproblem [Pord00, S. 89ff; Schm00, S. 154ff; BoEi02, S. 78].

Darunter versteht man das Problem, dass zwei oder gar mehrere verschiedene Präsentationen derselben signierten Datei derart divergieren, dass der Inhalt der Erklärung unterschiedlich interpretiert werden kann. Dies hängt damit zusammen, dass nicht Dokumente, sondern Bitfolgen unterschrieben werden, sodass „zur Interpretation dieser Bitfolgen häufig parametergesteuerte Präsentationen benötigt werden“ [Ber+02, S. 74]. So können zu bestimmten Rohdaten (zum Beispiel Bitfolgen) verschiedene Präsentationen erzeugt werden, etwa weil Text und Grafikprogramm auf unterschiedliche Fonts zugreifen oder weil auf der Ebene des Betriebssystems etwa Standardeinstellungen für Textfarben und Hintergrund unterschiedlich gewählt werden können. Ohne Veränderung des signierten Bitstrings kann es dadurch dazu kommen, dass verschiedene Erklärungen – und im Extremfall verschiedene sinnvolle Erklärungen – erfolgen [Fox98, S. 386ff].

Ein anderes Problem besteht darin, dass die Sicherheit des Systems generell untergraben werden kann, sofern es einem Angreifer gelingt, einen Trojaner (oder andere Spähprogramme) in die Signaturerstellungsumgebung zu integrieren. So wurde bereits praktisch demonstriert, dass dadurch in Systemen akkreditierter Anbieter Dateien vor dem Signieren verändert und auch die PIN ausgelesen werden konnten [Ber+02, S. 74].

Als Gegenmaßnahme gegen derartige Angriffe bietet sich etwa der Einsatz von Kartenlesern mit eigenem Keypad an, damit das Auslesen der PIN dadurch vermieden wird [Schi02, S. 488]. Zusätzlich kann man auch eine Überprüfung auf biometrische Merkmale integrieren.

Indessen ist ein umfassender Schutz nicht vorstellbar. Eine absolute Sicherheit kann es nicht geben. Auch der Einsatz biometrischer Erkennungsmerkmale zur Freischaltung der Signaturkarte dürfte keine völlige Fälschungssicherheit bewirken, weil sämtliche Daten, auch die biometrischen Referenzdaten, obwohl sie stark verschlüsselt sind, dennoch lediglich in digitaler Form vorhanden sind und deswegen „theoretisch entschlüsselt, kopiert und manipuliert werden könnten“ [Jung03, S. 70].

Wie bei der Kryptologie kann auch bei dem Einsatz biometrischer Erkennungssysteme infolge technischer Grenzen lediglich ein Sicherheitsniveau nach dem jeweiligen aktuellen Stand der Technik eingehalten werden. Zwar dürfte eine völlige Fälschungssicherheit insofern nie zu erreichen sein. Jedoch ist demgegenüber zu unterstreichen, dass der Fälschungsaufwand im Vergleich zu dem bei einer eigenhändigen Unterschrift um ein Vielfaches größer ist [Jung03, S. 70]. Dies gilt es stets zu bedenken.

Im Hinblick auf das Signaturbündnis wäre es sicherlich sinnvoll, im Rahmen einer breit angelegten Informations- und Werbekampagne für die qualifizierte elektronische Signatur auch in gewisser Weise die erwähnten Problembereiche offenzulegen. Auch dies kann dazu beitragen, das Vertrauen zu fördern, denn „Ehrlichkeit ist eine hochgeschätzte, äußerst positiv besetzte Tugend. Deshalb ist das Informieren der Nutzer über eventuelle Risiken zur Vertrauensbildung im Zweifel höher einzuschätzen als die Hoffnung, durch Verschweigen Schäden vermeiden zu können“ [LaUl02, S. 26].

Das Ziel einer solchen Offenlegung besteht darin, aktuelle und potentielle Nutzer objektiv zu informieren. Dabei sollte natürlich insbesondere auch betont werden, dass der Fälschungsaufwand bei qualifizierten elektronischen Signaturen gegenüber dem bei einer handschriftlichen Unterschrift sehr viel höher ist. Dies dürfte auch dazu dienlich sein, das Vertrauen in qualifizierte elektronische Signaturen zu stärken.

3.4.7 Kostenfrage

Einer der Hauptgründe, welche bisher einer schnellen Verbreitung der qualifizierten elektronischen Signatur entgegenstehen, ist die (noch ungeklärte) Kostenfrage. Denn diejenigen, die in Signaturprodukte und in Zertifizierungsdienste investieren sollen, haben oft selbst davon lediglich in begrenztem Maße einen Nutzen.

Aus diesem Grunde sind sie lediglich bedingt (oder aber gar nicht) zur Erbringung von Vorleistungen bereit [Roßn03a, S. 2]. So sind bei einigen Unternehmen die

Befürchtungen groß, dass sich Mitbewerber später – ohne dass diese dann selbst Kosten zu tragen hätten – „einfach auf die bestehende Struktur aufsetzen könnten“ [LüAd02, S. 12].

Daher dürfte eine der Bedingungen für den Erfolg des Signaturbündnisses darin liegen, „dass es zu einem fairen Interessenausgleich zwischen den Nutzern und Anbietern der neuen Infrastruktur kommt“ [Büg+04, S. 139]. Würden etwa die Kreditinstitute ohne Verrechnung ihre Karten mit der Signaturfunktion ausstatten oder aber sich die dafür notwendigen Kosten lediglich mit ihren Kunden teilen, erhielten beispielsweise Behörden sowie eCommerce-Anbieter (Online-Shops) beträchtliche Vorteile durch Effizienzgewinne und bei der rechtlichen Durchsetzung ihrer Forderungen, ohne überhaupt Kosten für die neue Infrastruktur zu übernehmen.

Bei einem fairen Geschäftsmodell müssen deshalb alle Gruppen, die durch die neue Infrastruktur Vorteile erhalten, in angemessener Weise an den Kosten dieser Infrastruktur beteiligt werden. Falls dies nicht gelingt, werden sich diejenigen, denen der Nutzen zu gering erscheint – Kreditinstitute, Kunden oder Applikationsanbieter – lediglich halbherzig bzw. nicht in ausreichendem Maße an der neuen Infrastruktur beteiligen [Büg+, S. 139]. Dadurch könnte das Ziel des Signaturbündnisses kaum erreicht werden.

Dabei ist darüber hinaus zu bedenken, dass im privaten Bereich – das heißt im Bereich der Privatkunden – generell keine Bereitschaft für eine mit erheblichen Kosten verbundene Lösung gegeben sein dürfte. Indessen dürften (nahezu) kostenneutrale Lösungen für den privaten Bereich nur schwer realisierbar sein, „möglicherweise entscheiden sie aber über Erfolg oder Misserfolg der elektronischen Signatur im nicht-institutionellen Sektor“ [LaUl02, S. 128].

3.5 Notwendige flankierende zusätzliche Maßnahmen zur Vertrauensschaffung

Vor dem Hintergrund der bereits aufgezeigten Problemfelder wird deutlich, dass zusätzliche flankierende Maßnahmen notwendig sein werden, um bei den Bürgern die erforderliche breite Vertrauensbasis in die qualifizierte elektronische Signatur zu schaffen. Hinzu kommt nämlich außerdem, dass einige Bürger die Tatsache, dass man sich für eine qualifizierte elektronische Signatur „die „in Tinte getauchte Feder“ nicht mehr leihen kann“ [LaUl02, S. 17], als einen technischen Rückschritt empfinden. Deswegen erscheinen weitere Maßnahmen zur Vertrauensschaffung nötig.

So wäre es zum Beispiel – wie bereits angedeutet – zweckmäßig, die Öffentlichkeit im Rahmen einer breit angelegten Werbekampagne für die qualifizierte elektronische Signatur aufzuklären und dafür zu sensibilisieren. Dies kann sinnvollerweise unter Zuhilfenahme der neuen medialen Möglichkeiten durch eine In-

tegration von „Education and Entertainment“ (Edutainment) geschehen [LaUl02, S. 18].

Dabei sollten natürlich auch in erster Linie die Vorteile von qualifizierten elektronischen Signaturen herausgestellt werden. Um jedoch wirkliches Vertrauen zu schaffen, empfiehlt es sich – wie schon erläutert – ebenfalls, gewisse Informationen zu den Risiken zu gewähren. Der Zweck dieser Marketing- und Aufklärungskampagne besteht hauptsächlich darin, objektive Informationen über qualifizierte elektronische Signaturen bereit zu stellen und eine Förderung des Vertrauens in diese neue Technik zu erreichen. Dies soll auch dazu beitragen, dass es durch den vermehrten Einsatz von qualifizierten elektronischen Signaturen nicht zu einer weiteren Vertiefung der digitalen Teilung der Gesellschaft kommt.

Darüber hinaus wäre es eventuell zu erwägen, eine unabhängige Stelle zu schaffen, die dem Gemeinwohl verpflichtet ist und die Aufgabe hat, die Hardware und die Software für qualifizierte elektronische Signaturen zu testen [LaUl02, S. 21]. Zur Zeit ist es für die meisten Verbraucher nämlich „kaum möglich, sich über die Sicherheitseigenschaften von IT-Produkten zu informieren“ [LaUl02, S. 21]. Aus Sicht der Öffentlichkeit wären transparente Produkttests durch eine Stelle ähnlich wie die Stiftung Warentest notwendig, die das breite Vertrauen der Nutzer hat.

Denn Vertrauen in qualifizierte elektronische Signaturen kann nur dann geschaffen werden, wenn die Nutzer die digitale Welt als verlässlich und transparent empfinden. Indessen können Transparenz und Verlässlichkeit durch einen durchschnittlichen Nutzer nicht allein erfahren werden. Deswegen stellt die Schaffung einer solchen unabhängigen und vertrauenswürdigen Institution, die dies stellvertretend für die Bürger übernimmt, eine zweckmäßige Begleitmaßnahme zur Förderung des Vertrauens in die qualifizierte elektronische Signatur dar.

4 Zusammenfassung und Ausblick

Angesichts der weitgehenden Gleichstellung der elektronischen Form mit der Schriftform im Privatrecht und der Einführung der rechtsverbindlichen Kommunikation in der öffentlichen Verwaltung wird deutlich, dass der Gesetzgeber der qualifizierten elektronischen Signatur einen Vertrauensbonus eingeräumt hat. Dennoch konnte sich die qualifizierte elektronische Signatur noch nicht im erforderlichen Maße durchsetzen. Vor allem auch um dies zu ändern, wurde im April 2003 das deutsche Signaturbündnis gegründet.

Insgesamt betrachtet, erscheinen die Ziele des Signaturbündnisses – die Förderung der Anwendung und Verbreitung chipkartenbasierter elektronischer Signaturen und die Schaffung der dafür erforderlichen Infrastruktur – als überaus sinnvoll. In Anbetracht der analysierten Problembereiche wird jedoch deutlich, dass die Realisierung dieser Ziele alles andere als ein einfaches Unterfangen darstellt.

Wünschenswert wäre es jedoch, dass es durch das Signaturbündnis erreicht werden könnte, die notwendige kritische Masse für die neue Infrastruktur sowie eine breite Vertrauensbasis der Bürger in die qualifizierte elektronische Signatur zu schaffen. Sollte dies – nicht zuletzt auch mit Hilfe flankierender Informations- und Werbekampagnen – gelingen, könnten alle von den Vorteilen der qualifizierten elektronischen Signatur profitieren, beispielsweise die Bürger allgemein durch Zeitersparnis infolge von eGovernment, der Handel durch ein niedrigeres Risiko bei elektronischen Geschäften, die Kreditwirtschaft durch die Durchführung von Finanzdienstleistungen ohne Medienbruch und auch der Staat durch Kostenersparnis infolge von eGovernment. Es bleibt daher zu hoffen, dass es – mit Unterstützung durch notwendige begleitende Maßnahmen zur Vertrauensschaffung – gelingen kann, die Ziele des Signaturbündnisses zu verwirklichen.

Einen „entscheidenden Impuls“ [HoRo04, S. 269] für die Verbreitung von qualifizierten elektronischen Signaturen könnte dabei auch die geplante Einführung der JobCard darstellen. Ähnlich positiv in diese Richtung könnte sich auch die geplante Einführung der elektronischen Gesundheitskarte und des digitalen Personalausweises auswirken. So soll etwa die elektronische Gesundheitskarte als Weiterentwicklung der Versichertenkarte der gesetzlichen Krankenversicherung ab 2006 jedem Patienten zur Verfügung stehen, allerdings zunächst lediglich als Speicher für elektronische Rezepte [Schu04, S. 32]. Als Hauptmotivation für die Einführung der elektronischen Gesundheitskarte wird generell das Einsparen von Kosten angeführt. Durch das elektronische Rezept (E-Rezept) soll es gelingen, bei der Rezepterstellung, -einlösung und –abrechnung Medienbrüche zu vermeiden; in Anbetracht von jährlich rund 700 Millionen Rezepten in Deutschland wird hierin ein beträchtliches Einsparpotential gesehen [Weic04, S. 396; Schu04, S. 32]. Überdies soll die elektronische Gesundheitskarte auf freiwilliger Basis die Bereitstellung und die Nutzung medizinischer Daten unterstützen wie etwa Informationen für eine Notfallversorgung, den elektronischen Arztbrief sowie eine elektronische Patientenakte [Schu04, S. 32, Weic04, S. 394]. Zwar soll die elektronische Gesundheitskarte zunächst keine qualifizierte elektronische Signatur enthalten, sie soll jedoch entsprechend erweitert werden können [Weic04, S. 395].

Als ein „Schlüsselprojekt“ [Schu04, S. 33] für eine breite Einführung von Chipkarten, die zur Erstellung qualifizierter elektronischer Signaturen in der Lage sind, wird das geplante System der JobCard angesehen. An diesem Verfahren kann jeder Arbeitnehmer nur dann teilnehmen, wenn er über eine Signaturkarte mit einer qualifizierten elektronischen Signatur verfügt [Erne04, S. 405]. Ermöglichen soll die JobCard den Zugriff auf die Daten des jeweiligen Arbeitnehmers zu den Beschäftigungszeiten, zu der Höhe von Entgeltzahlungen und zu einer Auflösung des Beschäftigungsverhältnisses. Dadurch soll die JobCard dazu beitragen, die Verwaltungsabläufe der Arbeitsämter bzw. Jobcenter zu beschleunigen, damit die Bearbeitung und die Genehmigung von Lohnersatzleistungen zügiger ablaufen kann [Schu04, S. 33]. Durch eine gesetzliche Einführung der JobCard erhält jeder Antragsteller in der Arbeitslosenversicherung eine rechtliche Verpflichtung, eine

Signaturkarte zu besitzen [HoRo04, S. 265]. Obgleich mit der Einführung der JobCard einige datenschutzrechtliche Probleme verbunden sind [Bize04, S. 388], beispielsweise „eindeutige Identifizierung der Arbeitnehmer, Vorratsspeicherung der Entgeltdatensätze über Jahre und Risiken bei dem Betrieb des Verfahrens“ [Erne04, S. 409], gilt es auch die Vorteile der geplanten Einführung der JobCard zu unterstreichen: So ist damit zu rechnen, dass dadurch „der Preis für Signaturkarten und Anwendungen erheblich fallen wird und damit weitere Anwendungen erschlossen werden könnten“ [Erne04, S. 409]. Dies wiederum dürfte dazu beitragen, dass viele Bürger, die nicht am System der JobCard beteiligt sind, sich eine Signaturkarte mit einer qualifizierten elektronischen Signatur beschaffen, um in den Genuss der neuen Möglichkeiten zu kommen.

Literatur

[Ball04] Ballwieser, W.: Entwurf zur Modernisierung der EU-Abschlussprüferrichtlinie: neue Transparenzvorschriften für Abschlussprüfer und Geprüfte. Betriebs-Berater 59, Heft 17, 2004: S. I.

[Bäum03] Bäumler, H.: Gibt es ein Recht auf Anonymität? Macht Anonymität heute noch Sinn?. Datenschutz und Datensicherheit 27, 2003: S. 160.

[Ber+02] Bertsch, A.; Fleisch, S.-D.; Michels, M.: Rechtliche Rahmenbedingungen des Einsatzes digitaler Signaturen. Datenschutz und Datensicherheit 26, 2002: S. 69-74.

[BESigÄndG04] Begründung zum Entwurf eines Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigÄndG). http://www.iid.de/iukdg/04-04-01-ge%E4nderte-SigG-Begr%FCndung-BMVELt.pdf, 2004, letzter Abruf am 2004-06-22.

[Bize04] Bizer, J.: Flächendeckende Identifizierungsstruktur. Datenschutz und Datensicherheit 28, 2004: S. 388.

[BoEi02] Bovenschulte, A.; Eifert, M.: Rechtsfragen der Anwendung technischer Produkte nach dem Signaturgesetz. Datenschutz und Datensicherheit 26, 2002: S. 76-78.

[Büg+04] Büger, M.; Esslinger, B.; Koy, H.: Das deutsche Signaturbündnis: Ein pragmatischer Weg zum Aufbau einer interoperablen Sicherheitsinfrastruktur und Applikationslandschaft. Datenschutz und Datensicherheit 28, 2004: S. 133-140.

[Dum+04] Dumortier, J.; Kelm, S.; Nilsson, H; Skouma, G.; van Eecke, P.: The legal and market aspects of electronic signatures. Datenschutz und Datensicherheit 28, 2004: S. 141-146.

[Erne04] Ernestus, W.: JobCard – Schlüssel zur elektronischen Kommunikation?. Datenschutz und Datensicherheit 28, 2004: S. 404-409.

[ESigÄndG04] Entwurf eines Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigÄndG). http://www.iid.de/iukdg/04-04-01-ge%E4nderter-SigG-Entwurf-BMVEL.pdf, 2004, letzter Abruf am 2004-06-22.

[FeHa03] Federrath, H.; Hansen, M.: Wer bin ich?. Datenschutz und Datensicherheit 27, 2003: S. 262.

[Fis+02] Fischer-Dieskau, S.; Gitter, R.; Paul, S.; Steidle, R.: Elektronisch signierte Dokumente als Beweismittel im Zivilprozess. MultiMedia und Recht 5, 2002: S. 709-713.

[Fox98] Fox, D.: Zu einem prinzipiellen Problem digitaler Signaturen. Datenschutz und Datensicherheit 22, 1998: S. 386-388.

[Fox04] Fox, D.: Wiedergeburt. Die zweite. Datenschutz und Datensicherheit 28, 2004: S. 130.

[Geis02] Geis, I.: Die neue Signaturverordnung: Das Sicherheitssystem für die elektronische Kommunikation. Kommunikation & Recht 5, 2002: S. 59-61.

[HoGr02] Hopp, C.; Grünvogel, A.: Pseudonyme nach dem deutschen und österreichischen Signaturgesetz. Datenschutz und Datensicherheit 26, 2002: S. 79-83.

[Horn04] Hornung, G.: Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW. MultiMedia und Recht 7, 2004: S. 3-8.

[HoRo04] Hornung, G.; Roßnagel, A.: Die JobCard – „Killer-Applikation“ für die elektronische Signatur?. Kommunikation & Recht 7, 2004: S. 263-269.

[Jung02] Jungermann, S.: Der Beweiswert elektronischer Signaturen. Eine Studie zur Verläßlichkeit elektronischer Signaturen und zu den Voraussetzungen und Rechtsfolgen des § 292a ZPO. Peter Lang-Verlag: Frankfurt am Main et al., 2002.

[Jung03] Jungermann, S.: Der Beweiswert elektronischer Signaturen. Zu den Voraussetzungen und Rechtsfolgen des § 292a ZPO. Datenschutz und Datensicherheit 27, 2003: S. 69-72.

[Klew03] Klewitz-Hommelsen, S.: Recht auf Anonymität? Oder Anspruch auf Transparenz? Datenschutz und Datensicherheit 27, 2003: S. 159.

[LaUl02] Langenbach, C. J.; Ulrich, O.: Elektronische Signaturen. Springer: Berlin et al., 2002.

[LüAd02] Lüdemann, V.; Adams, N.: Die elektronische Signatur in der Rechtspraxis. Kommunikation & Recht 5, 2002: S. 8-12.

[Nedd03] Nedden, B.: Handlungsempfehlungen für „Datenschutzgerechtes eGovernment“. Datenschutz und Datensicherheit 27, 2003: S. 128.

[Pord00] Pordesch, U.: Der fehlende Nachweis der Präsentation signierter Daten. Datenschutz und Datensicherheit 24, 2000: S. 89-95.

[Roßn01] Roßnagel, A.: Das neue Recht elektronischer Signaturen. Neue Juristische Wochenschrift 54, 2001: S. 1817-1826.

[Roßn02] Roßnagel, A.: Rechtliche Unterschiede von Signaturverfahren. MultiMedia und Recht 5, 2002: S. 215-222.

[Roßn03a] Roßnagel, A.: Editorial: Eine konzertierte Aktion für die elektronische Signatur. MultiMedia und Recht 6, 2003: S. 1-2.

[Roßn03b] Roßnagel, A.: Die fortgeschrittene elektronische Signatur. MultiMedia und Recht 6, 2003: S. 164-170.

[Schi02] Schindler, W.: Sichere digitale Kommunikation – Motivation, Anforderungen, mathematisch-technische Realisierung und rechtliche Aspekte. Kommunikation und Recht 5, 2002: S. 481-490.

[Schm00] Schmidt, A. U.: Signiertes XML und das Präsentationsproblem. Datenschutz und Datensicherheit 24, 2000: S. 153-158.

[Schm02] Schmidl, M.: Die elektronische Signatur. Funktionsweise, rechtliche Implikationen, Auswirkungen der EG-Richtlinie. Computer und Recht 18, 2002: S. 508-517.

[Schu04] Schulzki-Haddouti, C.: Signaturbündnis macht Dampf. c't, Heft 10, 2004: S. 32-33.

[SigBü03] Signaturbündnis. http://www.signaturbuendnis.de, letzter Abruf am 2004-06-22.

[SigBüVK03] Signaturbündnis: Vorgaben und Konvergenzziele für das Signaturbündnis. http://www.iid.de/iukdg/sigbue_vorg_konverg.pdf, 2003, letzter Abruf am 2004-06-22.

[Skro04] Skrobotz, J.: „Lex Deutsche Bank": Das 1. SigÄndG. Datenschutz und Datensicherheit 28, 2004: S. 410-413.

[Stor02] Storr, S.: Elektronische Kommunikation in der öffentlichen Verwaltung. Die Einführung des elektronischen Verwaltungsakts. MultiMedia und Recht 5, 2002: S. 579-584.

[Uhlm03] Uhlmann, A. M.: Elektronische Verträge aus deutscher, europäischer und US-amerikanischer Sicht. Peter Lang-Verlag: Frankfurt am Main et al., 2003.

[Voge01] Vogel, H.-H.: Das Internet und der Schutz der persönlichen Integrität aus verwaltungsrechtlicher Sicht. In: Hohloch, G. (Hrsg.) Recht und Internet. Nomos: Baden-Baden 2001, S. 159-169.

[Weic04] Weichert, T.: Die elektronische Gesundheitskarte. Datenschutz und Datensicherheit 28, 2004: S. 391-403.

[Wohl02] Wohlfahrth, J.: Elektronische Verwaltung – Vorgaben und Werkzeuge für datenschutzgerechte Anwendungen. Recht der Datenverarbeitung 18, 2002: S. 231-236.