DuD
Datenschutz und Datensicherheit

Rechtliche Rahmenbedingungen des Einsatzes digitaler Signaturen

Andreas Bertsch, Sophie-D. Fleisch, Markus Michels

Nach langer Diskussion wurden im vergangenen Jahr das SigG an die EG-Signaturrichtlinie vom 13.12.1999 angepasst sowie die Formvorschriften des Privatrechts geändert, um den Einsatz elektronischer Signaturen zu ermöglichen. Der Beitrag diskutiert die gesetzlichen Bestimmungen in Hinblick auf den Grad der Harmonisierung und ihre Auswirkungen auf tatsächliche Anwendungen.[1]

Dr. Andreas Bertsch

SIZ – Informatikzentrum der Sparkassenorganisation GmbH
Arbeitsschwerpunkt: Trust und Authentication Services
E-Mail: andreas.bertsch@siz.de

Sophie-D. Fleisch
Assessorin

Secorvo Security Consulting GmbH
Leiterin Marketing und Vertrieb
E-Mail: fleisch@secorvo.de

Dr. Markus Michels

Security Consultant, Secorvo Security Consulting GmbH
Arbeitsschwerpunkt: PKI, Signaturgesetz
E-Mail: michels@secorvo.de

[1] Der Beitrag basiert auf den Ergebnissen einer für das Informatikzentrum der Sparkassenorganisation (SIZ) durchgeführten Studie.

1 Einleitung

Mit der Verabschiedung des „Gesetzes über Rahmenbedingungen für elektronische Signaturen sowie zur Änderung weiterer Vorschriften“ vom 16.05.2001 (BGBl. 2001, Teil 1 Nr. 22 vom 21.05.2001) hat die Bundesregierung das Signaturgesetz (SigG) vom 22.07.1997 an die Bestimmungen der EG-Richtlinie 1999/93 vom 13.12.1999 „Über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“ (SigRL) angepasst. Inzwischen wurde auch die zugehörige, am 01.11.1997 in Kraft getretene Signaturverordnung (SigV) mit Beschluss des Bundeskabinetts vom 24.10.2001 durch eine neue „Verordnung zur elektronischen Signatur“ ersetzt.

Neben SigG und SigV hat die Bundesregierung verschiedene Gesetzesinitiativen und Verordnungen in die Wege geleitet, um durch die Einführung digitaler Signaturen dem elektronischen Geschäftsverkehr zum Durchbruch zu verhelfen. Zu diesen zählen insbesondere

- das „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr“ (FormAnpG) vom 13.07.2001, veröffentlicht im Bundesgesetzblatt am 17.07.2001, das rechtsverbindliches Handeln mit Hilfe einer gesetzlichen elektronischen Signatur ermöglicht,
- der „Entwurf eines Dritten Gesetzes zur Änderung verwaltungsverfahrensrechtlicher Vorschriften“ (3. VwVfÄndG) vom 16.07.2001, der für eine rechtsverbindliche Kommunikation zwischen Bürgern und Verwaltung sorgen soll, und
- die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU), BMF-Schreiben vom 16.07.2001.

Insbesondere die Regelungen der GDPdU, die seit dem 01.01.2002 anzuwenden sind, werden erhebliche Auswirkungen haben. Denn sie regeln nicht nur den Datenzugriff, sondern auch die Prüfbarkeit sowie die Archivierung digitaler Unterlagen. Dort werden qualifizierte digitale Signaturen mit Anbieter-Akkreditierung gemäß Signaturgesetz für die steuerliche Abzugsfähigkeit elektronischer Abrechnungen gefordert. Diese gesetzlichen Bestimmungen sollen nun in Hinblick auf

- den Grad der Harmonisierung der EU Signaturrichtlinie und ihre Umsetzung in SigG/SigV sowie
- die Auswirkungen einiger Regelungen in SigG/SigV auf reale Anwendungen

untersucht werden. Dabei werden jeweils die folgenden Aspekte betrachtet: *Anwendungsbereich*, *Genehmigung und Aufsicht*, *Typen von Signaturen*, *Rechtsfolgen*, *Haftung* sowie *technische Umsetzungen*. Anschließend werden zusammenfassend die Vor- und Nachteile des freiwilligen Einsatzes qualifizierter Signaturen diskutiert.

2 Harmonisierung

Anwendungsbereich

Das Ziel des SigRL ist, „*rechtliche Rahmenbedingungen für elektronische Signaturen und für bestimmte Zertifizierungsdienste fest[zulegen], damit das reibungslose Funktionieren des Binnenmarktes gewährleistet ist*“ und insofern divergierende Regeln in den Mitgliedsstaaten zu verhindern. Jedoch wird dieses Ziel in zwei wesentlichen Punkten eingeschränkt:

- Sie regelt keine elektronischen Signaturen, die ausschließlich in Systemen verwendet werden, die auf freiwilligen privatrechtlichen Vereinbarungen zwischen einer bestimmten Anzahl von Teilnehmern beruhen („geschlossene Systeme“, Erwägungsgrund 16).
- Die Mitgliedstaaten können den Einsatz elektronischer Signaturen im öffentlichen Bereich möglichen zusätzlichen Anforderungen unterwerfen. Diese Anforderungen müssen objektiv, transpa-

rent, verhältnismäßig und nicht-diskriminierend sein. Sie dürfen sich nur auf die spezifischen Merkmale der betreffenden Anwendung beziehen (SigRL § 3.7).

Damit wird die Harmonisierung jedoch stark beschränkt, da damit zu rechnen ist, dass die überwiegende Mehrzahl der auf elektronischen Signaturen beruhenden Anwendungen zu einem dieser beiden Fälle zählt.

Damit beschränken sich die regulierten und harmonisierten Anwendungen in Deutschland im Wesentlichen auf solche, in denen Willenserklärungen, für die die gesetzliche Schriftform vorgeschrieben ist, nur durch die elektronische Form (inklusive qualifizierter Signatur) ersetzt werden können. Dies sind aber nur wenige, denn grundsätzlich gilt in Deutschland für die Abgabe von Willenserklärungen die Formfreiheit; selbst Willenserklärungen , die der gewillkürten Schriftform genügen müssen, können durch nicht-qualifizierte Signaturen nach FormAnpG formgerecht unterschrieben werden .

Rechtsfolgen

Eine weitere Ebene des Verzichtes auf Harmonisierungen betrifft die Rechtsfolgen. Nach Erwägungsgrund 17 der SigRL zielt die Richtlinie „*nicht darauf ab, nationales Vertragsrecht, insbesondere betreffend den Abschluss und die Erfüllung von Verträgen, oder andere, außervertragliche Formvorschriften bezüglich der Unterschriften zu harmonisieren.*“

Dies bedeutet, dass in den Mitgliedsstaaten Willenserklärungen für jeweils verschiedene spezifische Anwendungen, die Formvorschriften genügen müssen, nicht durch elektronische Willenserklärungen gleich welcher Art ersetzt werden können, da diese formnichtig sein würden. In Deutschland kann für etliche Anwendungen die gesetzliche Schriftform nicht durch die elektronische Form ersetzt werden. Es ist damit zu rechnen, dass in anderen Ländern die elektronische Signatur für weitere Anwendungen nicht rechtswirksam eingesetzt werden kann (siehe etwa [MeSc99] für Österreich) – eine Einschränkung, die die Umsetzung betroffener grenzüberschreitender Anwendungen verunmöglichen würde.

Akkreditierungssysteme

Eine weitere Einschränkung der Harmonisierung verursachen die Akkreditierungssysteme. Zwar ist die Richtlinie nicht den Vorstellungen einiger Mitgliedsstaaten gefolgt, Akkreditierungen (bzw. Genehmigungen) von Zertifizierungsdiensteanbietern (ZDA) vorzuschreiben, jedoch steht es jedem Mitgliedsland frei, freiwillige Akkreditierungssysteme anzubieten (Erwägungsgrund 11 SigRL).

Es ist zu erwarten, dass Mitgliedsländer durch zusätzliche Anforderungen für den öffentlichen Bereich die Akkreditierung für spezifische Anwendungen implizit verbindlich vorschreiben. Da die Akkreditierungssysteme hinsichtlich der Anforderungen und des Sicherheitsniveaus nicht harmonisiert sind und der öffentlich-rechtliche Bereich im Markt für qualifizierte Signaturen sicher zukünftig eine wichtige Rolle spielen wird, steigt damit die Markteintrittsschwelle für ausländische ZDA, denn sie müssen sich in jedem Land nach unterschiedlichen Anforderungen akkreditieren lassen, wollen sie ihre Produkte europaweit anbieten. Eine gegenseitige Anerkennung der unterschiedlichen Akkreditierungssysteme wird nur der Fall sein, wenn die bei der ZDA eingesetzten Systeme „gleichwertige Sicherheit“ aufweisen und dies auch praktisch nachgewiesen werden kann (SigG § 23). In Deutschland ist die Markteintrittschwelle für ausländische ZDA besonders hoch, wie sich aus den Vorschriften für die technischen Umsetzungen ergibt (s.u.).

Haftung

Die SigRL legt für die Haftung Mindestanforderungen fest, die recht schwach sind. Insbesondere kann aus der SigRL keine Haftung der ZDA aus Produktversagen oder ungeeigneten technischen Sicherheitsumgebungen abgeleitet werden, wie in der Begründung zum Entwurf des Signaturgesetzes [BSigG01] zu Recht kritisiert wird. Aus diesem Grund hat der deutsche Gesetzgeber die Haftung verschärft und zusätzlich durch die Forderung nach einer Deckungsvorsorge sichergestellt, dass die ZDA auch de facto Schadenersatz leisten können. Werden die Haftungsregelungen in anderen EU-Mitgliedsstaaten gegenüber dem SigRL nicht verschärft, so könnte sich – zumindest für nicht akkreditierte Anbieter – eine Wettbewerbsverzerrung ergeben. Auch für akkreditierte ausländische Anbieter, die nachweislich „gleichwertige Sicherheit“ aufweisen können, scheint es keine zusätzlichen Anforderungen zu geben, die die deutschen Haftungsbedingungen als Mindestkriterium festschreiben.

Technische Umsetzung

Die EU Kommission hat frühzeitig erkannt, dass die technischen Umsetzungen der nationalen Gesetze die Harmonierungsbemühungen zunichte machen können. Daher können für zentrale Komponenten nach SigRL § 3.6 durch das so genannte „Artikel-9-Komitee“ (nach SigRL § 9) Referenznummern für allgemein anerkannte Normen für Produkte für elektronische Signaturen festgelegt werden. Die Mitgliedstaaten gehen davon aus, dass Produkte, die diese Normen erfüllen

- den Anforderungen nach vertrauenswürdigen Produkten seitens der Zertifizierungsdiensteanbieter (Anhang II.f) und
- den Anforderungen hinsichtlich der sicheren Signaturerstellungseinheit (nach Anhang III) genügen.

Für die technische Umsetzung der EU-Signaturrichtlinie wurde 1999 die *European Electronic Signature Standardisation Initiative* (EESSI) ins Leben gerufen. Ihre Aufgabe war zunächst, die Themengebiete für den notwendigen Standardisierungsbedarf zu identifizieren und den Standardisierungsgremien CEN-ISSS ESIGN und ETSI-SEC ESI entsprechende Arbeitspakete vorzuschlagen. Für die Standardisierung der kryptographischen Algorithmen wurde eine eigene Gruppe ins Leben gerufen.

Inzwischen wurden Standards zu oben genannten und weiteren Komponenten ausgearbeitet. Zu erwähnen ist darunter insbesondere der Standard für sichere Signaturerstellungseinheiten: Dort sollte ein Sicherheitsprofil z.B. für Chipkarten nach Common Criteria erarbeitet werden. Aufgrund fehlenden Konsenses zwischen den Teilnehmern wurden schließlich in *einem* Standard *zwei* Profile verabschiedet: eines mit der Prüftiefe EAL4 und eines mit der Prüftiefe EAL4+.[2]

Weitere relevante Standards (CWA – Common Working Agreement) betreffen vertrauenswürdige Produkte – so werden etwa nach FIPS 140-1 evaluierte HSM für ZDA zugelassen – und Richtlinien für ZDA, Anforderungen an Signaturerstellungsumgebung und -prüfung sowie Interoperabilitätsstandards für qualifizierte Zertifikate und Zeitstempelprotokolle.[3] Zur Zeit werden die fertiggestellten Standards auf Eignung überprüft. Eine Erklärung zur Norm würde diese Standards für ZDA in Europa relevant werden lassen. In Deutschland sind solche Normen allerdings *nur relevant für nicht-akkreditierte ZDA* (SigV Anhang I,

[2] CEN/ISSS CWA 14167-1 und -2, siehe http://www.ni.din.de/sixcms/detail.php3?id=389

[3] siehe www.ni.din.de/sixcms/detail.php3?id=389 und http://portal.etsi.org/sec/el-sign.asp.

II): Nur sie haben die Freiheit, Produkte einzusetzen, die sich an die durch das Artikel-9-Komitee zur Norm erklärten Standards orientieren.

Für akkreditierte ZDA trifft dies nur dann zu, wenn die Normen mit den in SigV Annex I ausgeführten Anforderungen übereinstimmen. Dies ist jedoch in verschiedenen Punkten nicht der Fall:

- Für die Komponente der sicheren Signaturerstellungseinheiten schreibt SigV Annex I die höhere Prüftiefe EAL 4+ vor.[4]
- Auch die Zulassung eines FIPS 140-1 evaluierten HSMs beim ZDA wird als nicht ausreichend nach Annex I SigV erachtet, denn ein ZDA muss zur Erstellung eines qualifizierten Zertifikats eine qualifizierte Signatur verwenden, die wiederum durch eine sichere Signaturerstellungseinheit erzeugt wird. Für letztere ist aber in SigV die Evaluierung nach ITSEC oder Common Criteria mit Prüftiefe EAL4 / E3 vorgeschrieben.

Voraussichtlich werden sich die meisten ZDA akkreditieren lassen oder haben dies bereits getan, um ihre Produkte und Dienstleistungen auch im behördlichen Umfeld anbieten zu können. Selbst ein ZDA, der sich zunächst nicht akkreditieren lassen will, tut gut daran, die in SigV Annex I und II explizit ausgeführten Anforderungen zu erfüllen, um sich nicht eine spätere Akkreditierung zu verbauen.

Eine weitere Ebene der Harmonisierung ist die technische Interoperabilität. Zwar ist damit zu rechnen, dass einige Interoperabilitätsstandards (etwa der zur Profilierung des qualifizierten Zertifikates) verwendet werden, jedoch führen schon spezifische deutsche Regelungen (s.u.) dazu, dass diese Spezifikationen entweder erneut profiliert oder sogar erweitert werden müssen, um den Regelungen zu genügen.

Spezifische Probleme, wie etwa die technische Umsetzung einer allfälligen Anerkennung (bzw. späteren Aberkennung) ausländischer Anbieter wurden auf technischer Ebene bislang nicht näher ausgeführt. Zu beantworten wäre etwa, wie das Wurzelzertifikat der ausländischen CAs (bzw. das Wurzelzertifikat der zuständigen Behörde) in die Client-Produkte integriert wird.

[4] Es ist nicht Aufgabe des Artikel-9 Komitees eigene Standards herzustellen, es soll vielmehr aus existierenden Standards die geeigneten heraussuchen. Daher wird CWA 14167 voraussichtlich entweder komplett oder gar nicht zur Norm erklärt werden(siehe auch [Geng01]).

Summa summarum kann gesagt werden, dass die in EESSI ausgearbeiteten Standards nicht den Grad der Harmonisierung auf technischer Umsetzungsebene erreichen werden, der wohl ursprünglich beabsichtigt war oder erhofft wurde.

3 Analyse von Einzelaspekten

Anwendungsbereich

Nach SigG § 2.7 sind qualifizierte Zertifikate elektronische Bescheinigungen für natürliche Personen und nicht für juristische Personen auszustellen. Dies ist eine enorme Einschränkung, die z.B. für Anwendungen nicht akzeptabel ist, in denen die Signaturerstellung von mehreren Personen mit bestimmten Rollen gemeinsam kontrolliert werden soll; die Personen innerhalb einer Rolle jedoch wechseln dürfen oder sogar müssen.

Auch innerhalb der durch das SigG implizierten Infrastruktur gibt es das Problem, wie die zuständige Behörde den untergeordneten ZDA, die juristische Personen sind, ein Zertifikat auf deren öffentlichen Schlüssel ausstellen kann. Dies wird heute technisch dadurch gelöst, dass ein Zertifikat zu einem Pseudonym ausgestellt wird, das wiederum auf eine natürliche Person verweist. Bei Bedarf, etwa Austritt der Person aus der ZDA, übernimmt eine andere Person das Pseudonym. Pseudonyme sind allerdings für einen gänzlich anderen Zweck gedacht, nämlich für den Schutz der persönlichen Daten einer Person. Diese zweckentfremdende Verwendung von Pseudonymen in ZDA-Zertifikaten führt insbesondere die Idee der Ausstellung von Zertifikaten für natürliche Personen ad absurdum: Von einer eindeutigen Zuordnung eines öffentlichen Schlüssels zu einer natürlichen Person kann bei dieser Lösung keine Rede mehr sein. Auch bleiben die Konsequenzen einer Übertragung auf andere Personen (etwa in haftungsrechtlicher Hinsicht) vollständig offen. Anderseits lassen sich durch diese „Pseudonym"-Lösung l möglicherweise auch Anwendungen realisieren, die ansonsten nur mit nichtqualifizierten Signaturen umgesetzt werden könnten.

Es ist davon auszugehen, dass qualifizierte Signaturen in betrieblichen Abläufen häufig automatisch erstellt werden – erst dann ermöglichen elektronische Abläufe die gewünschten Effizienzgewinne. Es ist jedoch eine offene Frage, ob Massensignaturen überhaupt erlaubt sind: Nach der Begründung zu SigV § 15.2 [BSigV] sind sie grundsätzlich möglich, sofern Signaturen nur zu dem voreingestellten Zweck (z.B. Signaturen zu Zahlungsanweisungen bei Großanwendern) und durch eine zuvor geprüfte und abgenommene Anwendung vorgenommen werden. Auch hier wird aber das zugehörige Zertifikat nicht für den Betrieb, sondern für eine einzelne natürliche Person ausgestellt werden müssen (sofern nicht auf die „Pseudonym"-Lösung ausgewichen wird – mit der erwähnten Haftungsproblematik).

Genehmigung und Aufsicht

Ein interessanter Aspekt sind die Auswirkungen der Aberkennung der Akkreditierung eines Anbieters bzw. die Untersagung des Betriebs eines Anbieters.

Nach SigG § 13 hat ein Anbieter die Einstellung seiner Tätigkeit anzuzeigen und muss entweder selbst dafür sorgen, dass die gültigen qualifizierten Zertifikate von einer anderen ZDA übernommen werden, oder er muss diese Zertifikate sperren. Für akkreditierte ZDA sorgt die Behörde für die Übernahme durch einen anderen akkreditieren ZDA. In beiden Fällen übernimmt die Behörde die Dokumentation, wenn keine ZDA für die Übernahme gefunden wird. In SigV § 10 wird gefordert, dass eine Unterrichtung der zuständigen Behörde und der Signaturschlüssel-Inhaber zwei Monate vor der Einstellung der Tätigkeit erfolgt.

Wichtig in diesem Zusammenhang ist, dass nach SigG § 15 (6) *„im Falle des Widerrufs [...] eines akkreditierten Zertifizierungsdiensteanbieter ... die zuständige Behörde eine Übernahme der Tätigkeit durch einen anderen akkreditierten Zertifizierungsdiensteanbieter oder die Abwicklung der Verträge mit den Signaturschlüssel-Inhabern sicherzustellen*" hat. Damit ist die Weiterführung des Betriebes als nichtakkreditierter ZDA, zumindest mit den bisherigen Kunden und ohne neue Verträge, nicht möglich.

Unklar ist allerdings, warum nur die gültigen Zertifikate übernommen werden müssen (SigG § 13.1). Wird dies in technischer Hinsicht interpretiert (wie in [Blum01]), so würde dies bedeuten, dass gesperrte Zertifikate nicht übernommen werden und damit online nicht mehr verfügbar sein müssen. Damit gehen wichtige Informationen wie beispielsweise der Sperrzeitpunkt eines Zertifikats verloren, die für die langfristige Prüfbarkeit einer

Signatur relevant sein können. Selbst wenn die Übernahme nur haftungsrechtlich interpretiert wird, würde dies bedeuten, dass der übernehmende ZDA nicht für gesperrte Zertifikate einstehen muss. Jedoch können auch gesperrte Zertifikate noch zu positiven Signaturprüfergebnissen führen, wenn der Signaturzeitpunkt vor dem Sperrzeitpunkt lag, und damit auch haftungsrechtlich von Bedeutung sein. In jedem Fall betrifft eine Einstellung bzw. die Aberkennung der Akkreditierung den Anwender:

- Bei einer geordneten Übergabe an einen anderen ZDA und technischen Weiterführung des Systems entstehen u.U. zusätzliche Kosten.
- Schwieriger wird es, wenn der Betrieb durch einen bestehenden anderen ZDA weitergeführt wird und dieser ZDA die übernommenen Benutzer rasch auf seine technische Infrastruktur migrieren möchte. In diesem Falle müsste gewährleistet sein, dass zumindest die Nachprüfbarkeit auch der „alten" Signaturen möglich ist. Bei einer Übernahme durch einen ausländischen ZDA wäre zu prüfen, ob und inwiefern sich Änderungen etwa bei der Haftung ergeben.
- Wird der Betrieb einer ZDA eingestellt und übernimmt kein anderer ZDA die Tätigkeit, ist die Regulierungsbehörde für Telekommunikation und Post (RegTP) nur verpflichtet, die Dokumentation zu übernehmen, nicht aber den Betrieb aufrechtzuerhalten. Die zuständige Behörde muss in diesem Fall bei nicht akkreditierten Anbietern (§ 13.2) nur dann bei Vorliegen eines berechtigten Interesses Auskunft zur Dokumentation (aus der die notwendige Information gewonnen werden könnte) erteilen, soweit dies technisch ohne unverhältnismäßig großen Aufwand möglich ist. Nach der zugehörigen Begründung [Druc] kann die Behörde bei Übernahme der Dokumentation nicht akkreditierter ZDA aus technischen Gründen (unterschiedliche Schlüssellängen, Software etc.) keine jederzeitige Nachprüfbarkeit garantieren.

  Im Gegensatz dazu kann nach SigG § 15 (6) und [Druc] die zuständige Behörde im Rahmen des Verfahrens der freiwilligen Akkreditierung auch die technischen Voraussetzungen der Nachprüfbarkeit im Falle der Übernahme sicherstellen. Die Begründung für die unterschiedliche Behandlung der akkreditierten und nicht akkreditierten Anbieter überzeugt nicht, denn auch akkreditierte Anbieter haben unterschiedliche Software mit z.T. proprietären Formaten und nicht akkreditierte ZDA können nicht beliebige Schlüssellängen wählen. Schließlich bleibt zu prüfen, ob die Aufrechterhaltung der Nachprüfbarkeit ausreichend ist, denn dies schließt nicht die Abrufbarkeit ein. Dies bedeutet, dass die Zertifikate in jedem Fall auch auf andere Weise zum Prüfer gelangen können müssen, am einfachsten dadurch, dass sie Teil der Signatur sind bzw. der Signatur beigefügt werden.[5]

Zusammenfassend kann gesagt werden, dass bei nicht akkreditierten ZDA die generelle Aufrechterhaltung des elementaren Dienstes der Nachprüfbarkeit nicht gewährleistet ist und daher für Anwendungen, in denen die langfristige Überprüfbarkeit der Signatur gefordert ist, nur akkreditierte ZDA geeignet sind.

Rechtsfolgen

Wie ausgeführt, kann die gesetzliche Schriftform durch die elektronische Form (mit qualifizierter Signatur) zwar grundsätzlich ersetzt werden, es sind jedoch zahlreiche Anwendungen von dieser Regel ausgeschlossen. Aus der Begründung zum Entwurf des Formvorschriftenanpassungsgesetzes geht hervor, dass der Gesetzgeber im wesentlichen zwei Beweggründe hatte:

- Häufig kann (noch) nicht davon ausgegangen werden, dass technische Einrichtung für die elektronischen Willenserklärungen vorhanden sind (etwa bei Zeugnissen in Klein- und Mittelbetrieben). In dem Falle hätte die elektronische Form keinen Nutzen, sondern wäre eher hinderlich.
- Die Warnfunktion der Unterschrift[6] hat zumindest aus subjektiven Gründen bei der elektronischen Form gegenüber der Schriftform noch Nachteile. Dies ist entscheidend, wenn die Rechtsfolgen wesentlich sind, wie etwa bei der Kündigung des Arbeitsplatzes oder Bürgschaftserklärungen. Der Gesetzgeber macht aber auch deutlich, dass sich dies ändern könnte, wenn sich die elektronische Form etabliert hat.

Es muss möglicherweise mit weiteren Ausschlüssen gerechnet werden, wenn diese Gründe für einen Anwendungsfall zutreffen Bei der derzeit geringen Verbreitung qualifizierter Signaturen und der zugehörigen technischen Einrichtungen trifft der erste Grund im Prinzip auf fast alle Anwendungen zu, so dass Voraussagen schwierig sind

Ein weiterer näher zu beleuchtender Aspekt sind die Rechtsfolgen bei einem freiwilligen Einsatz qualifizierter Signaturen. Generelles Ziel des Formvorschriftenanpassungsgesetzes ist die Ergänzung des gesetzlichen Schriftformerfordernisses um eine elektronische Form, damit dieser in Verbindung mit einer qualifizierten Signatur der Anscheinsbeweis zukommt. Bei einem freiwilligen Einsatz der qualifizierten Signatur gilt dieser Anscheinsbeweis aber in derselben Weise. Es existieren jedoch zweifellos auch Anwendungen, für die diese Regelung gerade nicht gewünscht ist – sei es, dass Personen diese Regelung nicht wünschen oder ein Anbieter einer Dienstleistung, die auf elektronischen Signaturen beruht, seinen Kunden diese Regelung nicht zumuten möchte. In gewisser Hinsicht kann diese Bindung gemäß SigG § 7.7 zwar auf bestimmte Anwendungen nach Art und Umfang beschränkt werden, jedoch anscheinend für die zulässigen Anwendungen nicht abbedungen werden.

Schließlich muss beachtet werden, dass eine Willenserklärung zu ihrer Wirksamkeit noch des Zugangs beim Empfänger bedarf. Da das Formvorschriftenanpassungsgesetz selber den Zugang nicht regelt, bieten nach [Niss01] „*§ 130 BGB und die dazu entwickelten Grundsätze auch für elektronische Willenserklärungen ein geeignetes und ausreichendes Instrumentarium*". Danach ist eine Erklärung wirksam, wenn sie derart in den Machtbereich des Empfängers gelangt ist, dass bei Annahme gewöhnlicher Umstände der Empfänger die Möglichkeit ihrer Kenntnisnahme hat. Eine Erklärung ist dann im Machtbereich oder in der Verfügungsgewalt, wenn eine Speicherung (Konservierung) durch Briefablage, elektronische Speicherung o.ä. möglich ist.

[5] Dies stellt grundsätzlich kein Problem dar (international übliche Standards wie S/MIME sehen dies ohnehin als Möglichkeit vor; die Beifügung ist jedoch nicht obligatorisch), stellt in gewisser Weise aber den Dienst der Abrufbarkeit in Frage, denn er wird danach grundsätzlich nicht benötigt.

[6] Die Unterschrift in Schriftform erfüllt unterschiedliche Funktionen: die Abschlussfunktion, die Perpetuierungsfunktion, die Identitätsfunktion, die Echtheitsfunktion, die Verifikationsfunktion, die Beweisfunktion sowie die Warnfunktion. Die Warnfunktion bedeutet, dass der Erklärende durch den bewussten Akt der Unterzeichnung auf die erhöhte rechtliche Verbindlichkeit hingewiesen wird. Dadurch soll er vor übereilten Rechtsgeschäften geschützt werden.

Haftung

Haftungsregeln des ZDA sind ein zentrales Thema des Regelungsmodells. Generell bieten die Spezialregelungen des Signaturgesetzes eine Besserstellung bestimmter Dritter (z.B. von bestimmten Parteien, die qualifizierte Signaturen erhalten) hinsichtlich der Haftung seitens des ZDA als auch hinsichtlich der Nicht-Abstreitbarkeit der Abgabe der Willenserklärung seitens des Erklärenden.

Der ZDA haftet u.a. für die Auskünfte nach SigG § 5.1 (2), d.h. für die Nachprüfbarkeit und Abrufbarkeit der Zertifikate. In diesem Zusammenhang ist zu fragen, wie aktuell die Nachprüfbarkeit sein muss und ob und gegebenenfalls welche Verzögerungen zwischen aktueller Sperrung und dem Eintrag in das Verzeichnis (so dass die Auskunft den aktuellen Stand der Sperrung wiedergibt) erlaubt sind [Bert01]. Zudem ist die Sperrung (also etwa der Anruf des Signaturschlüssel-Inhabers an die Sperrhotline) ein Prozess, der eine gewisse Zeit dauert, so dass die Haftung in den Zeiträumen zwischen Sperrantrag und Sperreintrag in das Verzeichnis nicht klar geregelt zu sein scheint [BePo99]. Ferner beschränkt sich die Haftung nach SigG § 11 auf jede Person „*die vernünftiger Weise auf das Zertifikat vertraut*“. Damit sind etwa Schäden, die ein Signaturschlüssel-Inhaber oder ein Dritter erleiden, weil ein Sperrantrag nicht rechtzeitig umgesetzt wurde, nicht durch SigG § 11 abgedeckt. Die Haftung für diese Schäden müssten durch vertragliche Absicherung zwischen dem ZDA und dem Signaturschlüssel-Inhaber geregelt werden. Eine Deckungsvorsorgepflicht auch für vertragliche Haftung (wie von [Blum01] vorgeschlagen) wurde aber nicht umgesetzt; auch Beweisprobleme für den Signaturschlüssel-Inhaber sind vorprogrammiert, falls die Sperrung etwa nur fernmündlich erfolgt.

Es sollte zudem darauf hingewiesen werden, dass neben § 11 gegebenenfalls weitere Haftungstatbestände treten [Blum01], etwa § 826 BGB (vorsätzliche sittenwidrige Schädigung) und § 823 Abs. 2 BGB (Verletzung eines Schutzgesetzes), die auch Vermögenswerte erfassen, sowie § 823 Abs. 1 BGB, wenn andere Rechtsgüter verletzt werden [Blum01].

Identifikation

Die Anforderungen an die Identifikation (bzw. die erneute Identifikation, etwa bei Verlust der Chipkarte und des Passworts) sind hoch, um die Sicherheit des Systems zu gewährleisten. Nach SigV § 3.1 muss die Identifizierung eines Antragsstellers durch Vorlage des Personalausweis oder des Reisepasses eines EU Mitgliedlandes oder elektronisch mittels einer qualifizierten Signatur erfolgen. Dies kann jedoch zu Verzögerungen beim Prozess der Identifikation (etwa bei der Ausgabe einer Chipkarte) führen, die nicht für Anwendungen akzeptabel sind, in denen ein Mitarbeiter auch bei Verlust der Chipkarte in kürzester Zeit wieder „signierfähig“ sein muss. Auch Anwendungen, in denen die Daten der Benutzer vorhanden sind und auf einen aufwendigen Identifikationsprozess verzichtet werden soll, um die Akezeptanz neuer Dienste zu ermöglichen (etwa bei einer Kundensignierkarte), könnten sich durch die Anforderungen an die Identifikation als nicht realisierbar erweisen.

Ein weiterer interessanter Aspekt ist die Verbindung zwischen Zertifikat und zugehöriger Person: Zwar wird gefordert, dass gegebenenfalls der Name des Antragstellers um einen Zusatz erweitert werden muss, um Verwechslungen zu vermeiden (SigG § 7.1), jedoch darf mit Recht daran gezweifelt werden, ob dies ausreicht, daraus auf die reale Person zu schließen [Baum99]. Zudem ist der Zusatz nicht näher festgelegt und es bleibt offen, wie ZDA die Eindeutigkeit des Namens außerhalb ihrer Domäne sicherstellen wollen. Lösbar wäre das Problem wohl nur durch eine digitale Identität, die jedoch wieder datenschutzrechtlich bedenklich wäre [Bert01].

Technische Umsetzungen

Limitierungen

Die im Signaturgesetz gestellten Anforderungen implizieren eine Begrenzung für die Möglichkeiten technischer Umsetzungen:

- Die generelle Architektur ist eine 2-stufige Hierarchie: Die zuständige Behörde (RegTP) stellt dabei die Wurzel (Root) dar, die ein Zertifikat an die akkreditierten ZDA ausstellt und dieses bei Widerruf der Akkreditierung oder Einstellung des Betriebs des ZDA wieder sperrt. Weitere Hierarchiestufen sind für manche Anwendungen wünschenswert.
- Die Auskunft für die Nachprüfbarkeit muss neben der Sperrinformation auch enthalten, ob das Zertifikat von dem ZDA überhaupt erstellt wurde (sogenannte Positivauskunft). Dies hängt mit dem durch das Signaturgesetz implizierten Gültigkeitsmodell zusammen (s.u.).
- Aus der Diskussion der möglichen Einstellung des Betriebes eines ZDA ergab sich, dass der Zertifikatspfad der Signatur beigefügt sein sollte.
- Die Anforderungen hinsichtlich Drittevaluierungen an die zu verwendenden Komponenten sind hoch, insbesondere für akkreditierte ZDA.

Die oben erwähnten Anforderungen führen – neben den Auflagen für die Sicherheit der Produkte – dazu, dass ZDA auf spezifischen technischen Lösungen aufbauen müssen. Dies treibt die Kosten in die Höhe. Auch auf der Anwenderseite können Sicherheitsinfrastrukturen, die gegebenenfalls schon in Organisationen vorhanden sind, nicht verwendet werden.

Gültigkeitsmodell

Das Gültigkeitsmodell schreibt fest, unter welchen Umständen eine elektronische Signatur in bezug auf bestimmte Daten in technischer Hinsicht gültig ist oder nicht. Die Nicht-Gültigkeit umfasst den Fall der technischen Ungültigkeit wie auch der zeitweisen technischen Nicht-Prüfbarkeit (wenn bspw. der Auskunftsdienst vorübergehend ausgefallen ist).

Im Signaturgesetz werden Rahmenbedingungen für das Gültigkeitsmodell festgelegt, insbesondere heißt es in § 19 (5), dass „*die Gültigkeit der von einem Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikate ... von der Untersagung des Betriebes und der Einstellung der Tätigkeit sowie der Rücknahme und dem Widerruf einer Akkreditierung unberührt*“ bleibt. Durch diese Bestimmung wird für zeitbezogene Statusprüfungen das sogenannte Kettenmodell impliziert, in dem geprüft wird, ob das Benutzerzertifikat zum Signaturprüfzeitpunkt (entspricht i.A. dem Signaturerstellungszeitpunkt) gültig und nicht gesperrt war, das ZDA-Zertifikat zum Zeitpunkt der Erstellung des Benutzerzertifikats gültig und nicht gesperrt war und schließlich das RegTP-Zertifikat zum Zeitpunkt der Erstellung des Zertifikats für den ZDA gültig und nicht gesperrt war. Dies weicht vom international üblichen Schalenmodell (etwa im PKIX-Standard) ab, in dem alle Zertifikate zum Signaturprüfzeitpunkt nicht gesperrt sein dürfen [Hamm00]. Eine Konsequenz ist, dass dieser technische Sonderweg spezifische technische Lösungen bedingt und „commercial of-the-shelf“ (COTS) Produkte nicht eingesetzt werden können.

Ein weiteres Problem ist, dass durch die generelle Unverbindlichkeit des Gültigkeitsmodells die technische Gültigkeit einer Signatur grundsätzlich nur innerhalb eines

ZDA wohldefiniert ist (oder zumindest sein muss). Im allgemeinen kann die Signatur, die mit der Signaturkarte des einen ZDA erstellt wurde, nicht mit der (Client-) Software eines anderen ZDA verlässlich überprüft werden. Erst wenn sich alle ZDA freiwillig an das gleiche Gültigkeitsmodell halten würden (ein solches wird etwa in ISIS-MTT ausgearbeitet), könnte das Grundproblem – von Interoperabilitätsproblemen abgesehen – überwunden werden.

Interoperabilität

Durch SigG/SigV wird keine Interoperabilität zwischen den ZDA garantiert; die Interoperabilitätsspezifikationen (SigI, ISIS, ISIS/MTT) haben nur empfehlenden Charakter. Dabei wird ISIS-MTT von den deutschen ZDA vorangetrieben und es ist damit zu rechnen, dass mittelfristig zumindest einige ZDA diesen Standard umsetzen werden. Heute ist dies (noch) nicht der Fall; einzelne ZDA (wie auch die RegTP) setzen sogar definitiv proprietäre Formate ein.

Zusätzliche Probleme könnte es bei der Harmonisierung konkreter Anwendung geben, in denen das Format durch die Beteiligten (etwa durch Behörden bei der Kommunikation zwischen Bürgern und Verwaltungen) vorgegeben wird. Dies könnte dazu führen, dass nur die Produkte bestimmter Anbieter Verwendung finden können.

Schließlich führen die oben erwähnten technischen Sonderwege inklusive Gültigkeitsmodell dazu, dass die Interoperabilität mit nicht-deutschen Anbietern erschwert wird. Die Umsetzung dieser Sonderwege findet sich daher auch zwangsläufig in der Interoperabilitätsspezifikation ISIS/MTT v1.0.1[7] wieder. Darüber hinaus gibt es in ISIS/MTT einige Modifikationen der zugrunde liegenden internationalen Standards, die Interoperabilitätsprobleme (mit nicht deutschen Anbietern oder nicht qualifizierten Signaturen, etwa von internen PKI Lösungen) verursachen können. Zum Beispiel gibt es verbindliche Anforderungen an symmetrische und asymmetrische Algorithmen, die sich von denen in S/MIME v3 geforderten Verfahren unterscheiden, obwohl das in der Spezifikation definierte Nachrichtenformat auf S/MIME v3 basiert

Grenzen sicherheitstechnischer Lösungen

Im Kontrast zu den hohen technischen Sicherheitsanforderungen an die zentralen Komponenten bei der ZDA und besonders der (dezentralen) sicheren Signaturerstellungseinheiten stehen die generellen Probleme der weiteren dezentralen Komponenten. Diese ergeben sich auch aus der Notwendigkeit, marktgängige Client Systeme (Betriebssysteme, Browser) zu unterstützen, um auf dem Markt bestehen zu können. Dazu zählen:

- *Präsentation*: Es werden nicht Dokumente sondern Bitfolgen unterschrieben, so dass die zur Interpretation dieser Bitfolgen häufig parametergesteuerte Präsentationen benötigt werden. Dies kann dazu führen, dass es zu bestimmten Rohdaten (z.B. Bitfolgen) unterschiedliche Präsentationen erzeugt werden können, z.B. weil etwa Text und Grafikprogramme auf verschiedene Fonts zugreifen oder gar auf der Betriebssystemebene Standardeinstellungen für Hintergrund und Textfarben verschieden gewählt werden können. Im Extremfall kann dies dazu führen, dass es für bestimmte Rohdaten unterschiedliche *sinnvolle* Präsentationen gibt, so dass Verfälschungen, insbesondere in fremdkontrollierten Systemumgebungen, möglich sind [Pord00, Fox98].
- *Schutz der zu signierenden Daten*: Daten müssen von der Signaturerstellungsumgebung (etwa: Windows-PC) zur Signaturerstellungseinheit (z.B. Chipkarte) transportiert werden. Soll dies auf sichere Weise geschehen, müssen hier geeignete Sicherheitsmechanismen wie symmetrische und/oder asymmetrische Sicherheitsmechanismen verwendet werden. Dazu ist jedoch entweder ein komplexes Schlüsselmanagement nötig, oder die Architektur ist nicht flexibel (etwa: bestimmte Chipkarten können nur mit einer bestimmten Software verwendet werden).
- *Trojaner*: Gelingt es einem Angreifer einen Trojaner in die Signaturerstellungsumgebung zu integrieren, so kann die Sicherheit des Systems i.A. leicht untergraben werden. Dies wurde auch praktisch demonstriert [Kies01]: In Systemen akkreditierter Anbieter konnten Dateien vor dem Signieren verändert und die PIN ausgelesen werden. Zwar gibt es Gegenmaßnahmen gegen solche Angriffe (etwa den Einsatz von Kartenlesern mit eigenem Keypad, um das Auslesen der PIN zu vermeiden), ein umfassender Schutz ist jedoch nicht vorstellbar.

Aus den geschilderten Beispielen ist zu entnehmen, dass Sicherheit nicht allein technisch realisiert werden kann, sondern nur im Verbund mit organisatorischen Maßnahmen auch auf Anwenderseite (etwa dem Hinweis, dass die Sicherheitsumgebung frei von Trojanern sein muss). Daher muss die Frage erlaubt sein, ob nicht die an anderer Stelle erhobenen sehr hohen technischen Anforderungen (etwa an die sicherere Signaturerstellungseinheit) wirklich die Gesamtsicherheit des System in einer Weise erhöhen, die den damit verbundenen Aufwand und die Kosten rechtfertigen.

Aus Sicht der Anwendung kann umgekehrt gefragt werden, ob (allein) die vermutete höhere technische Sicherheit der qualifizierten Signatur den Ausschlag für einen freiwilligen Einsatz qualifizierter Signaturen geben kann.

Praxis in Deutschland

Zur Zeit (Stand Dezember 2001) gibt es 15 zertifizierte bzw. akkreditierte Zertifizierungsdiensteanbieter. Eine aktuelle Liste kann bei der RegTP abgerufen werden.[8] Viele davon bieten branchenspezifische Dienste (so sind unter den Anbietern drei Rechtsanwaltskammern und sechs Steuerberaterkammern) oder Speziallösungen an.

Allgemeine Lösungen bieten insbesondere die TeleSec und SignTrust an. Allerdings sind die Lösungen nicht interoperabel. TeleSec und auch die RegTP als Root CA verwenden die sogenannten TeleSec-Messages (auch TTP-Messages genannt) zur Kommunikation zwischen Client- und Server-Komponenten; SignTrust verwendet den ISIS-Standard, den Vorläufer von ISIS-MTT. Es ist damit zu rechnen, dass die Anbieter mittelfristig auf den ISIS-MTT Standard migrieren; allerdings wäre das Gesamtsystem ohne Migration der RegTP auch dann proprietär.

Zudem sind zur Zeit alle vier gemäß RegTP evaluierten Signaturprüfprodukte laut den Prüfberichten unvollständig: Sie können die Formate der RegTP nicht interpretieren und auch nur zur Systemzeit prüfen. Letzteres impliziert, dass alle Signaturen nach Sperrung eines Zertifikats als ungültig gewertet werden, womit die Nicht-Abstreitbarkeit der geleisteten Signatur offensichtlich nicht gewährleistet ist.

[7] http://www.t7-isis.de/ISIS-MTT/isis-mtt.html

[8] http://www.regtp.de/tech_reg_tele/start/in_06-02-04-00-00_m/index.html#akkreditiert

4 Einsatz qualifizierter Signaturen

Es lassen sich die beiden folgenden Fälle für den Einsatz qualifizierter Signaturen unterscheiden:

- Qualifizierte Signaturen *müssen* eingesetzt werden, wenn in der konkreten geschäftlichen Anwendung das gesetzliche Schriftformgebot vorgeschrieben ist oder – im Verkehr mit Behörden – die Verwendung qualifizierter Signaturen (eventuell mit zusätzlichen Anforderungen) verlangt wird.
- In allen anderen Fällen *können* qualifizierte Signaturen verwendet werden, jedoch auch andere Signaturen.

Im folgenden sollen nun die Vor- und Nachteile des *freiwilligen* Einsatzes qualifizierter Signaturen diskutiert werden.

Vorteile

- *Anscheinsbeweis:* Der qualifizierten Signatur wird ein Anscheinsbeweis zuerkannt, während andere Signaturen lediglich der freien Beweiswürdigung vor Gericht unterliegen.
- *Haftung:* Externe ZDA, die einen Dienst im Sinne des SigG anbieten, haften über das übliche Haftungsrecht hinaus für gewisse Schäden gegenüber speziellen Dritten.
- *Sicherheit:* Die Sicherheit der vom ZDA verwendeten Produkte und des Sicherheitskonzept ist von einer unabhängigen Instanz (Bestätigungsstelle) geprüft worden und bietet Gewähr für die Qualität der Lösung. Dies gilt im besonderen Maße für akkreditierte ZDA; die Akkreditierung stellt damit eine Art Gütesiegel dar.
- *Nachprüfbarkeit:* Bei akkreditierten ZDA wird selbst bei Betriebseinstellung die Nachprüfbarkeit der Zertifikate garantiert, so dass „alte“ Signaturen in jedem Falle (bis 30 Jahre nach Ablauf der Gültigkeit) prüfbar sind.

Nachteile

- *Inflexibilität des Systems*: Das gesamte System hängt von den Bestimmungen des Gesetzgebers ab, was die Flexibilität der Lösungen einschränkt. Beispiele für technische Limitierungen ist die zweistufige Hierarchie der Architektur, das Gültigkeitsmodell sowie die Bestimmungen für die (Re-) Identifikation eines Endbenutzers.
- *Auslagerung*: Die zumindest teilweise Auslagerung der Lösung an einen externen ZDA ist de facto unvermeidlich (was u.U. nicht erwünscht ist), denn der Aufbau einer ZDA ist mit hohen Kosten verbunden und rechtfertigt daher den Aufbau einer eigenen Infrastruktur i.d.R. nicht.
- *Hohe Kosten*: Durch die vom Gesetzgeber geforderten Auflagen und Bestimmungen an den ZDA entstehen sehr hohe Kosten, die früher oder später an den Kunden weitergegeben werden müssen.
- *Marktakzeptanz*: Qualifizierte Signaturen sind bislang nicht sehr verbreitet.
- *Marktlösungen*: Die bisherigen Lösungen sind wie oben ausgeführt i.A. nicht interoperabel und nicht immer benutzerfreundlich. Teils werden definitiv proprietäre Formate verwendet.
- *Produktauswahl*: In jedem Fall ist die Auswahl der Lösungen auf die ZDA beschränkt. Internationale Produktanbieter erfüllen die zahlreichen Anforderungen des Gesetzes nicht.
- *Grenzüberschreitende Anerkennung*: Die grenzüberschreitende Anerkennung von qualifizierten Signaturen innerhalb der EU Mitgliedsländer ist grundsätzlich durch entsprechenden Vorschriften in der SigRL und der entsprechenden Umsetzung im SigG gegeben, dennoch können unterschiedliche Detailanforderungen dieses Ziel de facto erschweren. Zwischen EU-Ländern und Drittstaaten gibt es bislang nur generelle Regeln zur Anerkennung. Zudem gibt es wie oben ausgeführt zahlreiche Einschränkungen der Harmonisierung der elektronische Signatur zwischen den Mitgliedsländern.
- *Rechtlicher Rahmen:* Bei qualifizierten Signaturen ist den Beteiligten ein rechtlicher Rahmen vorgegeben, der nicht beliebig verändert werden kann. Durch zivilrechtliche Regelungen kann dies u.U. freier geschehen.

Dank

An den Ergebnissen dieses Beitrags haben neben den Autoren insbesondere Dirk Fox und Jörg Völker mit gewirkt.

Literatur

[Baum99] M.Baum, *Die elektronische Identität?*, DuD 9/1999, S. 511-513.

[BePo99] A.Bertsch, U.Pordesch, *Zur Problematik von Prozeßlaufzeiten bei Sperrung von Zertifikaten*, DuD 9/1999, S. 514-519.

[Bert01] A.Bertsch, *Digitale Signaturen*, Springer Verlag, 2001, 264 Seiten.

[Blum01] F.Blum, *Entwurf eines neuen Signaturgesetzes*, DuD 2/2001, S. 71-78.

[BSigV] *Begründung zur Verordnung zur elektronischen Signatur und zur Umstellung der Gebühren auf Euro*, 37 Seiten.

[Druc] *Beschlussempfehlung und Bericht des Auschusses für Wirtschaft und Technologie zu dem Gesetzentwurf der Bundesregierung*, Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, Drs. 140/5324, 14.02.2001.

[Fox 98] D.Fox, *Zu einem prinzipiellen Problem digitaler Signaturen*, DuD 7/1998, S. 386-388

[Geng01] R.Genghini, *Global Relevanz of the European Electronic Signatures co-regulation process*, DuD 9/2001, S. 511-514.

[Hamm00] V.Hammer, *Signaturprüfungen nach SigI*, DuD 2/2000, S. 96-103.

[Kies01] R.Kiesler, *Wie sicher sind digitale Signaturen?*, PC Professionell 12/2001, S. 168-169.

[MeSc99] T.Menzel, E.Schweighofer, *Das österreichische Signaturgesetz*, DuD 9/1999, S. 503-507.

[Niss01] R.Nissel, *Neue Formvorschriften bei Rechtsgeschäften*, Bundesanzeiger, Jhrg. 53, Nr. 198a, 23.10.2001, 254 Seiten.

[Pord00] U.Pordesch, *Der fehlende Nachweis der Präsentation signierter Daten*, DuD 2/2000, S. 89-95

[SigG01] *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften*, BGBl. 2001, Teil 1 Nr. 22 vom 21.05.2001

[SigRL00] *Richtlinie 1999/93/EG des europäischen Parlaments und des Rates vom 13.Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*

[SigV01] *Verordnung zur elektronischen Signatur*, 2001.