DuD
Datenschutz und Datensicherheit

Eine kritische Würdigung des SigG

Dirk Fox

Mit der Verabschiedung des Signaturgesetzes (SigG) und der Signaturverordnung (SigV) haben Bundestag und Bundesregierung Mitte 1997 Neuland beschritten: Vor allen anderen europäischen Ländern und als zweites Land weltweit (nach dem US-Bundesstaat Utah) bekam Deutschland eine gesetzliche Regelung zu digitalen Signaturen. Der nun vorgelegte Evaluierungsbericht der Bundesregierung zum IuKDG, der den vom Bundestag beschlossenen zweijährigen Evaluierungszeitraum abschließt, sieht keinen Grund für Änderungen am Gesetz.[1] Der vorliegende Beitrag unterzieht das SigG einer kritischen Würdigung – und kommt zu einem anderen Ergebnis.

Dipl.-Inform.
Dirk Fox

Security Consultant und Geschäftsführer der Secorvo Security Consulting GmbH.
Arbeitsschwerpunkt: Public Key Infrastrukturen, Digitale Signaturen, Sicherheit in Netzen.
E-Mail: fox@secorvo.de

Einleitung

Mit der Verabschiedung des zum 1. August 1997 als Art. 3 des Informations- und Kommunikationsdienste-Gesetzes in Kraft getretenen deutschen Signaturgesetzes (SigG) [SigG_97] wurde vom Bundesgesetzgeber aufgrund der zum damaligen Zeitpunkt vergleichsweise geringen Erfahrungen mit digitalen Signaturen im praktischen Einsatz festgelegt, das Gesetz in Zweijahresfrist einer Evaluierung zu unterziehen,[2] um zu prüfen, ob Korrekturen oder Änderungen erforderlich sind. Am 16. Juni 1999 wurde der Evaluierungsbericht der Bundesregierung vorgelegt. Kernaussage: „Nach den bisherigen Erfahrungen mit dem Signaturgesetz und der Signaturverordnung besteht keine Veranlassung zu grundlegenden Änderungen von Gesetz und Verordnung.“[3] Dieser Beitrag kommt zu einem anderen Ergebnis.

1 Konzeption des Signaturgesetzes

Abweichend von den Ansätzen anderer Staaten einschließlich dem aktuellen Regulierungsvorschlag der EU-Kommission [EU_99] und entgegen anderslautenden Forderungen wurde im deutschen Signaturgesetz die Rechtswirksamkeit digitaler Signaturen nicht gesetzlich festgeschrieben. Dies geschah unter anderem aufgrund der Einsicht, daß sich auch der Beweiswert von eigenhändigen Unterschriften erst in vielen Jahren Rechtsgeschichte schrittweise entwickelt hat.

Statt dessen legt das Signaturgesetz Sicherheitsanforderungen an eine Infrastruktur für Schlüsselerzeugung, -zertifizierung, -verteilung und -anwendung fest, die für eine hohe Vertrauenswürdigkeit digitaler Signaturen nach Signaturgesetz sorgen sollen. Dazu zählen insbesondere die folgenden:

- Für alle nach dem Signaturgesetz *anerkannten Zertifizierungsstellen* sind ein Sicherheitskonzept sowie regelmäßige Prüfungen Voraussetzung für die Betriebsgenehmigung.
- Die eingesetzten *technischen Komponenten* müssen hohen Sicherheits-Standards genügen (vorgeschrieben ist eine Sicherheitszertifizierung nach ITSEC, E2/E4 hoch).
- Die geforderten *Mindestschlüssellängen* für die *kryptographischen Verfahren* sind so gewählt, daß eine Kompromittierung der Schlüssel unter realistischen Annahmen wenigstens in den nächsten zehn Jahren nicht zu erwarten ist.
- Die *geheimen Schlüssel* werden gleich nach der Erzeugung in einem physisch geschützten „Sicherheits-Token“ (einer Smartcard) unauslesbar gespeichert, den sie zu keinem Zeitpunkt verlassen. Die Nutzung der Schlüssel ist nicht nur an den Besitz der Smartcard („Haben“), sondern an zusätzliche Parameter wie eine PIN („Wissen“) oder ein biometrisches Merkmal („Sein“) gebunden.
- Die *Wurzel-Instanz* der Schlüsselinfrastruktur nach Signaturgesetz ist bei der Regulierungsbehörde für Post und Telekommunikation (RegTP) angesiedelt, die auch die Kontrolle über die Zertifizierungsstellen innehat.

Der Beweiswert einer digitalen Signatur ist damit nicht präjudiziert, sondern muß sich erst vor Gericht erweisen. Bei Nutzung einer Zertifizierungsinfrastruktur nach Signaturgesetz sollte jedoch eine sehr hohe Wahrscheinlichkeit für die Anerkennung digitaler Signaturen als Beweismittel vor Gericht im Rahmen der freien Beweiswürdigung durch den Richter bestehen.[4]

Es ist sicherlich zu erwarten, daß der Beweiswert digitaler Signaturen sich auf der Grundlage der Einschätzungen von

[1] Evaluierungsbericht der Bundesregierung, BT Drs. 14/1191 vom 16.06.1999.

[2] Beschluß des Bundestages, BT-Drs. 13/7935, vom 11.06.1997.

[3] Evaluierungsbericht der Bundesregierung zum IuKDG, BT Drs. 14/1191 vom 16.06.1999.

[4] Roßnagel spricht in diesem Zusammenhang von der „Sicherheitsvermutung“ des Signaturgesetzes, von der er eine Entlastung des Beweisführers erwartet [Roßn_98].

gerichtlich bestellten Gutachtern in den nächsten Jahren etablieren wird. Sollte es dazu kommen, so erscheint es sinnvoll, mit zunehmender Erfahrung im Umgang mit digitalen Signaturen über eine gesetzliche Verankerung der Rechtswirkung nachzudenken, wie sie heute bereits im Vorschlag für eine EU-Richtlinie zu digitalen Signaturen gefordert wird [EU_99]. Der jüngste Vorschlag des Justizministeriums zur Einführung einer „elektronischen Form“ geht in Richtung.

2 Würdigung

Zweifellos kann man schon jetzt eine Reihe sehr positiver, durch das Signaturgesetz verursachter Entwicklungen feststellen:

- **Marktentwicklung**: Allein die Verabschiedung des Signaturgesetzes hat eine erhebliche Förderung der Entwicklung und Nachfrage von Sicherheitsprodukten in Deutschland bewirkt. Denn Signaturgesetz und Signaturverordnung geben Orientierung und Investitionsschutz: Sowohl Hersteller als auch Unternehmen, die den Aufbau einer Public Key Infrastruktr (PKI) planen, gewinnen Gewißheit, daß ihre Investitionen in PKI-Produkte und organisatorische Abläufe nicht durch zukünftige Gesetzgebung (Verbot, gesetzliche Auflagen) Makulatur werden.
- **Sicherheitsbewußtsein**: Das Signaturgesetz legt die „Latte“ der Sicherheitsanforderungen sehr hoch und betont damit die Bedeutung hoher Sicherheitsstandards in Sicherheitsinfrastrukturen. Auch die im Gesetz vorgesehene Kontroll-Infrastruktur, die durch eine Bindung der Betriebsgenehmigung für Zertifizierungsstellen an regelmäßige unabhängige Prüfungen und Abnahmen für die Erhaltung eines hohen Sicherheitslevels sorgen soll, ist nicht nur für SigG-konforme Zertifizierungsstellen eine wichtige Einrichtung.
- **Anerkennung digitaler Signaturen**: Nicht zuletzt macht das Signaturgesetz die zukünftige Anerkennung digitaler Signaturen als Beweismittel vor Gericht sehr wahrscheinlich, möglicherweise auch die nicht Signaturgesetz-konformer digitaler Signaturen.
- **Infrastrukturförderung**: Für kleine und mittelständische Unternehmen sowie für Privatpersonen, die sich den Aufbau und Betrieb einer eigenen Sicherheitsinfrastruktur nicht leisten können, wird die Möglichkeit zur Nutzung von öffentlichen Zertifizierungsdiensten, wie sie das Signaturgesetz explizit fordert, in Zukunft von Bedeutung sein.

Trotz der anerkennungswürdigen Wirkungen des Signaturgesetzes ist festzuhalten, daß es bislang nicht den erhofften Durchbruch erzielt hat: Bis heute existiert die angestrebte Zertifizierungsinfrastruktur erst in Ansätzen.

3 Praktische Schwierigkeiten

Im Januar 1999, ganze 18 Monate nach Inkrafttreten des Signaturgesetzes, hat die erste (und bislang einzige) Zertifizierungsstelle ihren Betrieb aufgenommen.[5] Die Nachfrage nach deren Zertifizierungsdienst ist bisher minimal: Bis März lagen noch keine 100 Zertifizierungsanträge vor.

Daß es trotz über 30 weiteren Antragstellern bislang keine weitere produktive Zertifizierungsstelle gibt, hat Gründe: Der Betreiber einer öffentlichen Zertifizierungsstelle nach Signaturgesetz muß bei Konzeption und Aufbau eine Vielzahl von Anforderungen berücksichtigen:

- **Betriebsgenehmigung**: Signaturgesetzkonforme Zertifizierungsstellen müssen den hohen Sicherheitsanforderungen des Signaturgesetzes entsprechen. Der Prozeß der Anerkennung einer Zertifizierungsstelle durch die Regulierungsbehörde ist zeit- und kostenintensiv.
- **Kundennähe**: Den größten Teil der Kosten bei der Ausstellung eines Zertifikats verursacht die Registrierung eines Schlüsselinhabers – sowohl für den Schlüsselinhaber selbst (Wegezeiten) als auch für den Anbieter (Identifizierung, Einweisung, Dokumentation). Für den Anbieter rechnet sich die Dienstleistung nur dann, wenn er bei der Registrierung ein existierendes eigenes oder externes Filialnetz mit Kundennähe nutzen kann.
- **Konkurrenzproblematik**: Ein Anbieter, der in anderen Geschäftsbereichen seines Unternehmens mit potentiellen Kunden konkurriert, kann ein Akzeptanzproblem haben, insbesondere dann, wenn er die Schlüssel in seiner Zertifizierungsstelle generiert.

Neben diesen Schwierigkeiten gibt es eine Anzahl grundsätzlicher Bedenken, die Unternehmen daran hindern können, als Betreiber einer Zertifizierungsstelle nach Signaturgesetz aufzutreten:

- **Interoperabilität**: Zertifikate nach Signaturgesetz müssen keinen internationalen Standards entsprechen; es ist nicht einmal sichergestellt, daß Zertifikate der einen mit denen einer anderen Zertifizierungsstelle kompatibel sind.[6] Das beschränkt den Nutzen eines solchen Zertifikats erheblich.
- **Einsatzgebiet**: Proprietäre Zertifikate (wie sie nach SigG bis zu einem gewissen Grad unvermeidlich sind) werden nur in speziell dafür vorbereiteten oder angepaßten Anwendungen eingesetzt werden können. Solche Anwendungen sind erst in sehr kleiner Zahl und von nur wenigen Herstellern verfügbar und nicht verbreitet. Sie erfordern zudem den Besitz eines SmartCard-Lesers (der sich z. T. nur für diese Anwendung nutzen läßt) und sind vergleichsweise teuer.
- **Business Case**: Die Investitionen in eine Zertifizierungsstelle nach Signaturgesetz müssen sich in einem überschaubaren Zeitraum amortisieren. Der Markt für Zertifikate nach Signaturgesetz ist allerdings begrenzt: Es wird sicherlich mindestens noch zehn Jahre dauern, bis sich das Konzept einer „Signaturschlüssel-Smartcard“ bundesweit durchgesetzt hat. Außerdem wirken die Lebensdauer von fünf Jahren, die Tatsache, daß Zertifikate nur für natürliche Pesonen ausgestellt werden, und die Beschränkung auf den deutschen Markt begrenzend. Schließlich werden sich mehrere Anbieter den Markt teilen müssen. Dazu kommen fixe Kosten (für Smartcards, Mitarbeiter in Registrierungsstellen, Dokumentation), die je Zertifikat anfallen. Dadurch wird ein realistischer Preis eines Zertifikats kaum unter 50 DM liegen – wiederum ein marktbegrenzender Faktor.
- **Synergien**: Signaturen nach Signaturgesetz sind nur eine spezielle Anwendung von PKI-basierten digitalen Signaturen. In der Praxis sind bereits heute PKIs im Einsatz, meist im Zusammenhang mit Anwendungen, in denen die Frage einer gerichtlichen Würdigung der erzeugten digitalen Signaturen irrelevant ist. Oft genügen hier deutlich geringere Sicherheitsanforderungen als die in SigG/SigV

[5] Die Root-CA der RegTP ist seit dem 23. September 1998 betriebsbereit.

[6] Aus diesem Grund wurde vom BSI die Erstellung einer Interoperabilitätsspezifikation beauftragt; siehe [Berg_99]. Diese Spezifikation hat allerdings nur Empfehlungscharakter und ist bislang nicht abgeschlossen.

geforderten. PKI-Dienstleistungen nach SigG/SigV müssen allerdings aus Sicherheitsgründen streng von nicht Signaturgesetz-konformen getrennt werden: Dies erfordert Investitionen in zwei technisch unabhängige, teure Infrastrukturen.

4 Korrekturbedarf

Daß der Start einer öffentlichen Zertifizierungsinfrastruktur derzeit in den Startlöchern hängenbleibt, hat konkrete Gründe, die sich in einzelnen Bestimmungen des Signaturgesetzes finden lassen. Sie verhindern, daß das Geschäftsmodell einer potentiellen Zertifizierungsstelle aufgeht, und können die erheblichen Investitionen in eine Zertifizierungsstelle nach Signaturgesetz für den Betreiber zu einem Verlustgeschäft werden lassen.

Aus praktischer Erfahrung und technischer Sicht gibt es daher zu mehreren wichtigen Bestimmungen des Signaturgesetzes Nacharbeits- und Korrekturbedarf:

- **Hierarchie**: Das Signaturgesetz arbeitet mit einer nur zweistufigen Hierarchie (Zertifizierungsstellen und Root-CA bei der Regulierungsbehörde). Obwohl eine solche flache Hierarchie die Konzeption vereinfacht und auch sicherheitstechnisch einfacher zu beherrschen ist, ist dies für praktische Anwendungsfälle eine erhebliche Einschränkung.
- **Zertifikate für juristische Personen**: Das Signaturgesetz erlaubt die Ausstellung von Schlüsselzertifikaten nur für natürliche Personen. Das gilt auch für die Schlüssel von Zertifizierungsstellen, die zur Ausstellung von Schlüsselzertifikaten, Rückruflisten, Verzeichnisdiensten oder Zeitstempeln verwendet werden. Um bei Kündigung eines Mitarbeiters den Schlüssel der Zertifizierungsstelle nicht zurückrufen zu müssen, behilft man sich heute mit der Verwendung eines eigentlich aus Datenschutzgründen im Signaturgesetz vorgesehenen Mechanismus: einem Pseudonym. Der dem Pseudonym zugeordnete Mitarbeiter kann wechseln, der Schlüssel bleibt erhalten – ein dem Prinzip des Gesetzes widersprechender Vorgang, denn hier wechselt die Identität des Schlüsselinhabers. Grundsätzlich ist es jedoch in vielen praktischen Fällen sinnvoll, wie bei Unterschriftsberechtigungen und Prokura in Unternehmen, Schlüsselzertifikate für juristische Personen auszustellen.
- **Gültigkeitsprüfung**: Das derzeit dem Signaturgesetz zugrundeliegende Verständnis der Gültigkeit einer digitalen Signatur nimmt an, daß der Empfänger einer digitalen Signatur immer prüfen kann, ob ein Signaturschlüsselzertifikat gültig und nicht gesperrt ist (und damit der zugehörige Schlüssel akzeptiert werden kann). Technisch erfordert diese Annahme die Bereitstellung eines absolut zuverlässigen und hochverfügbaren Online-Dienstes, bei dem zu jeder Zeit die Gültigkeit eines Zertifikats geprüft werden kann. Offline-Benutzer sind damit von einer Gültigkeitsprüfung ausgeschlossen. Zudem entsteht in der Praxis ein erheblicher Kommunikationsaufwand. Auch eine rückwirkende Sperrung von Zertifikaten bei Bekanntwerden einer Schlüsselkompromittierung, der in bestimmten Fällen in der Praxis sinnvoll sein kann, ist nicht signaturgesetzkonform. Schließlich erfordert das dem Signaturgesetz zugrundegelegte Gültigkeitsmodell [Baum_99], daß mit jeder Signatur die gesamte Zertifikatskette in die Signatur eingeschlossen wird – dies kollidiert mit allen existierenden Standards.
- **Diensterbringung durch Dritte**: Nach Signaturgesetz werden alle Dienste, von der Registrierung über die Zertifizierung bis hin zu Verzeichnis- und Zeitstempeldienst, von einer Zertifizierungsstelle erbracht. Das kollidiert mit dem praktischen Erfordernis, insbesondere die Registrierung geographisch in Kundennähe zu plazieren, um Wegekosten zu reduzieren.

5 Prinzipielle Probleme

Schließlich stellen sich zwei grunsätzliche Probleme, für die bis heute eine überzeugende technische Lösung aussteht:

- **Ansichtskomponente**: Die (zweifellos sinnvolle) Anforderung an Signier- und Prüfkomponenten, dem Signierer resp. Prüfer zu garantieren, daß er sieht, was er digital signiert bzw. was digital signiert wurde, stößt auf ein prinzipielles Problem: Eine digitale Signatur bezieht sich immer nur auf Bits (also die Syntax), nicht aber auf den Inhalt eines Dokuments (seine Semantik) – selbst die Kodierung der Dokumenteninhalte ist nicht festgelegt. Verbreitete Office-Produkte bieten jedoch eine Vielzahl von Möglichkeiten, nicht-eindeutig darstellbare Dokumente zu erzeugen (versteckter Text, Notizen, Anmerkungen, Ausnutzung von Inkompatibilitäten zwischen Produktversionen etc.; näher dazu [Fox_98]). Bisher gibt es kein geeignetes und verfügbares Produkt, das dieses Problem einer eindeutigen Ansichtskomponente zufriedenstellend löst. Eine strengen Sicherheitsanforderungen genügende Lösung wird zudem sowohl teuer als auch in der Funktionalität stark eingeschränkt sein.[7]
- **Unsichere Betriebsumgebung**: Jede in der Praxis sinnvoll einsetzbare Lösung muß, wenn sie eine Chance auf hohe Akzeptanz haben soll, auf heute verbreiteten Arbeitsplatzrechnern eingesetzt werden können – also unter anerkannt unsicheren Betriebssystemen, die die Gefahr Trojanischer Pferde bergen. Die Entwicklung spezieller, sicherer Signier-Geräte mit geprüftem Betriebssystem würde das Problem lösen – allerdings die Kosten erheblich in die Höhe treiben.

Literatur

[Baum_99] Baum, Michael: *Gültigkeitsmodell des SigG*. DuD 4/1999, S. 1999-205.

[Berg_99] Berger, Andreas: *Signatur-Interoperabilitätsspezifikation*. DuD 4/1999, S. 206-212.

[EU_99] EU-Kommission: *Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen*. COM(1999) 195 endg. vom 29. April 1999.

[Fox_98] Fox, Dirk: *Zu einem prinzipiellen Problem Digitaler Signaturen*. DuD 7/1998, S. 386-388.

[Roßn_98] Roßnagel, Alexander: *Die Sicherheitsvermutung des Signaturgesetzes*. Neue Juristische Wochenschrift (NJW), 45/98, S. 3312-3320.

[SigG_97] *Gesetz zur digitalen Signatur (Signaturgesetz – SigG)*. Beschluß des Bundestages vom 13. Juni 1997 (BT-Drs. 13/7935).

[7] Die Interoperabilitätsspezifikation nach Signaturgesetz beschränkt sich auf Betreiben des BSI auf die Forderung, daß der Dateiname korrekt ist – eine Kapitulation vor dem Problem.