Digitale Signaturen - Teil 3

Praxis des Signaturgesetzes

von Dipl.-Inf. Robert Gehring

In den vorangegangenen zwei Folgen dieser Reihe wurden digitale Signaturen eingeführt. Es wurde dargestellt, woher sie kommen - aus der Kryptologie - und wie sie erzeugt werden - durch das Verschlüsseln von Hashwerten. Daß sie in Deutschland Gegenstand eines eigenen Gesetzes geworden sind, blieb auch nicht unerwähnt. Damit sollte alles zum Thema gesagt sein, könnte man meinen. Oder ist da noch was? Richtig, fast hätten wir sie übersehen - die Praxis. Wie es dort mit der Umsetzung der schönen Theorien aussieht, soll in dieser letzten Folge diskutiert werden.

Wieso, weshalb, warum?

Eine digitale Signatur ist eine digitale Signatur. Soviel steht fest und daran wollen wir uns erinnern, wenn es im folgenden manchmal nebulös werden sollte. Und was ist nun eine digitale Signatur, außerdem? Irgendwie war es ja so gedacht, daß im Zeitalter von *ftp* und *EMail* ein Pendant zur Unterschrift auf dem Papier her sollte. Technisch wurde diese Aufgabe bekanntlich gelöst. Nur die Frage, wie es damit weitergehen sollte, ist noch weitgehend unbeantwortet. Wie wird aus einer digitalen Signatur eine Unterschrift?

Um noch einmal auf das Problem hinzuweisen: Eine digitale Signatur ist eine Bytefolge, die einer Menge von anderen Bytes, z.B. einer EMail, eine Art von Identität verleiht. In dieser Identität stecken Informationen über die Herkunft der Information und ihre Integrität. Da solche digitalen Signaturen bei korrekter Handhabung fälschungssicher sind, könnte man sie bei elektronischem Datenaustausch einer Unterschrift gleichsetzen. Könnte man. Könnte wer? Und wie? Und weshalb überhaupt?

Die Unterschrift ist eine elementarer Bestandteil unserer Rechtskultur. Als ihr gleichwertig, kennt das bürgerliche Recht nur noch *„notariell beglaubigte Handzeichen „*. Drei Kreuze, von einem Notar beglaubigt, würden ausreichen, um einen Kaufvertrag wasserdicht zu machen. Um eine digitale Signatur als weiteres Äquivalent zu etablieren, müßte diese kompatibel zu den bestehenden rechtlichen Bestimmungen gemacht werden. Das Signaturgesetz stellt den deutschen Versuch dazu dar - fast. So ganz scheinen sich die Experten ihrer Sache nicht sicher gewesen sein, sonst wären die Formulierungen wohl anders ausgefallen. Aber, bevor wir näher darauf eingehen, was mit dem „fast" gemeint ist, sollen noch einige grundsätzliche Überlegungen zur Einführung von digitalen Unterschriften angestellt werden.Die Aufgabe ist klar: Es sollen aus digitalen Signaturen digitale Unterschriften werden. Welche Lösungen sind denkbar? Zwei unterschiedliche Ansätze markieren die Grenzen. Auf der einen Seite lassen sich digitale Signaturen als der Unterschrift gleichwertiges Instrument zusätzlich ins Recht einführen. Es wird jedem klar sein, daß damit eine Menge neuer Regeln fällig werden. Man könnte die Bezeichnung „instrumenteller Ansatz" dafür verwenden.

Als Beispiel könnte der „Utah Digital Signature Act" (UDSA) [1] dienen, die weltweit erste gesetzliche Regelung zu digitalen Signaturen überhaupt. Darin finden sich genaue Definitionen über Ziel und Wirkungsbereich, sowie die eingesetzten Mittel und Methoden. Besonders beachtenswert ist die Tatsache, daß sich der dortige Gesetzgeber Gedanken über die möglichen Folgen des Einsatzes digitaler Signaturen gemacht hat. In deren Bewertung hat man sich entschlossen, Haftungsregelungen ins Gesetz mit aufzunehmen, um eine Benachteiligung bestimmter Parteien zu vermeiden.

Viele Wege führen nach Rom

Auf der anderen Seite kann man digitale Signaturen zu Unterschriften im Sinne der bestehenden Regelungen erklären, wenn sie als solche gemeint sind. Dieser Ansatz ist vielleicht der konsequentere. Jedenfalls kommt er mit dem geringsten Aufwand zur „Implementierung" aus. Allerdings kann man sich vorstellen, daß die Bewertung einer Signatur im Streitfall schwierig werden könnte. Dieser Weg soll als „funktionaler Ansatz" bezeichnet werden. Um den „funktionalen Ansatz" zu illustrieren, ein Zitat aus dem „Massachusetts Electronic Records and Signatures Act":

„If a rule of law requires a signa-

lure, or provides consequences in die absence of a signature, an electronic signature satisfies that rule. " [2]

Aufmerksame Leser werden vielleicht bei *electronic signature* etwas gestutzt haben. Warum ist hier nicht von *digital signature* die Rede? Im Sinne eines „funktionalen Ansatzes" ist die Formulierung *electronic signature* passender, da sie weniger einschränkend ist und auf eine *digital signature* allemal zutrifft. Es kommt darauf an, die Funktion einer Unterschrift auf elektronischem Wege zu erfüllen, nicht darauf, es auf eine definierte Art und Weise zu tun. So läßt sich annehmen, daß PGP-Signaturen in Massachusetts als vollwertige Unterschriften gelten können. Neuere Entwicklungen können jederzeit zum Einsatz kommen.

Der deutsche Weg

Zwischen den beiden genannten Ansätzen ist noch viel Platz. Mangels Erfahrungen über längere Zeiträume, fällt es schwer, einen als den besseren und den anderen als den schlechteren Ansatz zu bezeichnen. Da hilft nur Abwarten. Die letzte Bundesregierung mit ihrem „Zukunftsminister" J. Rüttgers wartete jedoch nicht ab, sondern ging voran. So konnte sie Ende 1996 ein Signaturgesetz präsentieren, das zum 1. August 1997 in Kraft trat. Damit hatte Deutschland das erste nationale Signaturgesetz weltweit.

Nun, über anderthalb Jahre später, läßt sich feststellen, daß der Ansatz zum großen Sprung nur ein Stolpern hervorgebracht hat. Die oberste Zertifizierungsstelle hat im Herbst 1998, d.h. mehr als ein Jahr nach Inkrafttreten des Gesetzes, die ersten Schlüssel signiert [3]. Damit könnten die ersten privaten Zertifizierungsstellen ihre Arbeit aufnehmen. Nur kurze Zeit später verkündet ein internationales Konsortium aus acht Großbanken (unter anderem Deutsche Bank und Citibank), daß sie eine eigene Zertifizierungsinfrastruktur, die nicht zum deutschen Signaturgesetz kompatibel sein wird, aufbauen wollen [4]. Da kann doch etwas nicht in Ordnung sein!

Um es auf den Punkt zu bringen: Im Signaturgesetz ist der Wurm drin. Und nicht nur dort. Der ganze Versuch der Multimediagesetzgebung, in die das Signaturgesetz als Artikel 3 des Informations- und Kommunikationsdienstegesetzes (IuKDG) integriert ist, ist in seiner jetzigen Form zum Scheitern verurteilt. Das krasseste Beispiel dafür ist das Urteil gegen den ehemaligen CompuServe-Manager Felix Somm, der bekanntlich als Internetprovider für fremde Inhalte haftbar gemacht wurde. Während die einen Regelungen von den Staatsanwälten in ihr Gegenteil verkehrt werden *(„Entgegen aller konventionellen Lesarten erklärte sie [Bundesanwaltschaft - Anm.d.A.], daß die strafrechtliche Verantwortlichkeit der Provider zwar im IuKDG geregelt worden sei, doch im Wortlaut der nunmehr Gesetz gewordenen Vorschrift keine Stütze gefunden habe. Ergo: Auch künftig werde die Bundesanwaltschaft Provider für Internet-Inhalte im Ausland verantwortlich machen. " [5]),* finden andere mangels Umsetzbarkeit de facto keine Anwendung (z.B. das Signaturgesetz).

Nun lassen sich in diesem Rahmen unmöglich alle Schwachstellen der Multimediagesetzgebung herausarbeiten. Wir wollen uns deshalb auf das Signaturgesetz beschränken. Den größten Fehler des Gesetzes stellt die Halbherzigkeit dar, mit der es gemacht wurde. Diese resultiert zum einen aus dem zwiespältigen Verhältnis des Staates zu den Freiheiten der Staatsbürger und seinem Kontrollbedürfnis, sprich: Verschlüsselungsfreiheit, zum anderen aus der Eile, mit der man die eigene Modernität zeigen wollte. Hinzu kommt das Bedürfnis vieler deutscher Bürokraten, alles in Vorschriften geregelt sehen zu wollen. Gleichzeitig wollten sich die Autoren des Gesetzes vor den unkalkulierbaren Folgen ihrer Arbeit drücken und haben versucht das wirtschaftliche Risiko auf die Anwender abzuwälzen. Das sind harte Worte, die begründet sein wollen.

Fehlertoleranz

Da wäre zum einen das hierarchische, zentralistische Modell für eine Zertifizierungsinfrastruktur. Es scheint doch mehr als zweifelhaft, ob damit auf die sich immer stärker vernetzenden Strukturen der realen Welt angemessen reagiert werden kann. Hierarchien zeichnen sich gemeinhin durch eine gewisse Trägheit, nicht durch Innovationsfreude aus.

Die Zentralisierung der Aktivitäten von Zertifizierungsstellen führt scheinbar zu einer besseren Kontrollierbarkeit. Wenn die Sicherheit nur an wenigen Stellen kontrolliert werden muß, sollte der Aufwand geringer ausfallen. Demgegenüber sinkt jedoch die Fehlertoleranz des Gesamtsystems. Ein einziger schwerer Fehler in einer der wenigen Zertifizierungsstellen kann das gesamte System der Zertifizierung in Gefahr bringen. Die Kompromittierung des Schlüssels einer Zertifizierungsstelle entwertet auf einen Schlag sämtliche Zertifikate. Je weniger Zertifizierungsstellen es gibt, desto mehr Zertifikate muß aber jede einzelne von ihnen verwalten. Die mögliche Größe des Schadens nimmt dadurch zu. Auch

bieten große, zentrale Zertifizierungsstellen mehr Angriffsfläche, als viele kleine, verteilte Zertifizierungsstellen.

Kosten, Kosten, Kosten

Daß es zu einer Zentralisierung kommt, dafür hat der Gesetzgeber gesorgt. Die Kriterien aus dem Maßnahmenkatalog zum Signaturgesetz bzw. zur Signaturverordnung lassen sich nur mit Millionenaufwand erfüllen. Seriöse Schätzungen von Fachleuten aus der Wirtschaft gehen von Kosten in Millionenhöhe je Trustcenter (Zertifizierungsstelle) aus. Und das bei unsicheren Hoffnungen auf Amortisierung. Es werden sich wohl nur ein, zwei Dutzend Interessenten finden, die sich darauf einlassen - Banken, Versicherungen, Telekommunikationsunternehmen. Im März 1998 waren es 20 Unternehmen, die eine Lizenz beantragt hatten [6].

Hinzu kommen auf der Anwenderseite Investitionen in sichere Hardware. Gewöhnliche PC's werden die Sicherheitsanforderungen aus dem Maßnahmenkatalog nicht erfüllen können. Jeder, der digitale Signaturen gesetzeskonform einsetzen will, wird sich ein zertifiziertes Chipkartenlesegerät zulegen müssen. Die Kosten dafür können - je nach Verbreitung - zwischen 50 und 200 DM liegen [6]. Und wie sieht es mit der Unterstützung bei den Betriebssystemen aus? Werden diese Geräte nur von Windows aus zu bedienen sein? Vielleicht noch vom Mac? Und was ist mit Linux, OS/2 oder TOS? Wird man sich gar einen neuen Computer kaufen müssen? Fragen, die sich ein Anwender stellen wird.

Nun wollen wir einmal annehmen, die Zertifizierungsstellen arbeiten, und man hat sich ein passendes Chipkartenlesegerät (Signierkomponente) zugelegt. Wie geht es dann weiter? Zuerst benötigt man ein Paar asymmetrischer Schlüssel. Wer da denkt, er/sie könne seine/ihre PGP-Schlüssel benutzen, irrt sich. Schlüssel dürfen ebenfalls nur mit auf ihre Sicherheit geprüften Geräten erzeugt werden. Der PC zu Hause genügt diesen Anforderungen nicht.

Die Alternative besteht im Erwerb von Schlüsseln beim Trustcenter. Dort muß man ohnehin persönlich vorstellig werden, um sich zu identifizieren. Erst im Anschluß daran wird ein Zertifikat erstellt. Für diese Prozedur, d.h. Schlüsselerwerb und Zertifikatserstellung, werden etwa Kosten von 60 bis 150 DM veranschlagt [6].

Wer alle diese Zahlen zusammenrechnet und gegen den möglichen Nutzen abwägt, wird ins Grübeln kommen. Im Mittelwert sind vielleicht 200 DM auf der Anwenderseite zu investieren, bevor man die erste gesetzmäßige Signatur erzeugen kann. Was kann man mit dieser Signatur anfangen? Man könnte Bestellungen im Internet signieren und Überweisungen beim Homebanking. Wie lange wird es dauern, bis man damit 200 DM - gegenüber der bisherigen Vorgehensweise - hat einsparen können? Weiterhin fallen einige Pfennige je Signaturprüfung an. Lohnt sich das? Mit den kostenlosen Programmen PGP oder GPG [7] würde es doch auch gehen, oder? Neben der Kostenfrage stellt sich die nach der Sicherheit.

Sicherheit?

Besonders zwei Teile einer Zertifizierungsinfrastruktur verdienen Aufmerksamkeit, wenn es um Sicherheit geht: die Schlüsselverwaltung und die Zertifikatsverwaltung. Die einzige konkrete Vor-

schrift, die sich im Signaturgesetz diesbezüglich befindet, ist §2 (1), worin asymmetrische Schlüssel verlangt werden. Ein wenig verklausuliert heißt es dort:

„Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde nach §3 versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt. " [8]

Daß es *„Signaturschlüssel"* statt Schlüssel, wie in der Fachliteratur üblich, heißt, ist der oben erwähnten Haltung zur Verschlüsselung zu verdanken. Obwohl sich der Gesetzgeber bewußt ist, daß von Kryptographie die Rede ist, sagt er es nicht. So hält man sich die Möglichkeit eines Kryptoverbotes trotz Signaturgesetz offen. Das scheint nicht nur schizophren, es ist schizophren. Aber weiter mit den harten Fakten.

Klar ist jedenfalls, daß symmetrische Schlüssel (symmetrische Verfahren) nicht in Frage kommen. Der öffentliche Schlüssel aus dem Paar asymmetrischer Schlüssel wird von der Zertifizierungsstelle im Zertifikat eingetragen, nach §5(1) SigG. So weit, so gut. Es stellt sich die Frage, wo die Schlüssel herkommen. Im Gesetz wird dazu nichts gesagt. Der Blick in die nachgeschaltete Signaturverordnung zeigt, daß Schlüssel vom Inhaber *oder* von der Zertifizierungsstelle erzeugt werden können (§5 SigV). Jedoch wird im ersten Falle verlangt, daß sich die Zertifizierungsstelle von der Eignung der dafür verwendeten technischen Komponenten überzeugt. Gleiches gilt für die Komponenten, auf denen der *„private Signaturschlüssel"* gespeichert wird. Wie soll man sich das vorstellen? Der Begriff *„geeignete technische Komponenten"* hat es in sich. In der amtlichen Lesart muß es sich um Komponenten handeln, deren Eignung erwiesen und bestätigt ist. Die notwendigen Prüfungen der Eignung der Geräte kann nur eine anerkannt qualifizierte Stelle durchführen und anschließend zertifizieren. Zu prüfen sind die Geräte gemäß den ITSEC-Kriterien (Information Technology Security Evaluation Criteria), wie sich aus dem „Maßnahmenkatalog für digitale Signaturen" ergibt:

„In der Begründung zur § 17(1) SigV wird für die Evaluierungstiefe technischer Komponenten zur Schlüsselerzeugung einschließlich Ladevorgang eindeutig 'E4 hoch' gefordert. " [9]

Die Prüfstellen müssen ihrerseits hohe Qualifikation nachgewiesen haben und entsprechend zertifiziert sein. Für solche Aufgaben kommt eigentlich nur das BSI (Bundesamt für Sicherheit in der Informationstechnik) in Frage. Natürlich kosten diese Zertifizierungen - die der Prüfstellen und die der Komponenten - auch Geld. Die Beträge dafür wird ein privater Anwender nicht aufbringen können und es wahrscheinlich auch nicht wollen. Die theoretische Möglichkeit, die von der Verordnung zur privaten Schlüsselerzeugung, von der Verordnung eingeräumt, wird sich also in der Praxis - zumindest für Privatleute - nicht realisieren lassen.

Was bleibt, ist der Gang zur Zertifizierungsstelle, um sich dort Schlüssel generieren und aushändigen zu lassen. Einen Vorteil hat die Sache, daß man sich gleich ein Zertifikat erstellen lassen kann. Nun hängt der Wert einer digitalen Signatur von der Qualität des Schlüsselpaares und der absoluten Geheimhaltung des geheimen (privaten) Schlüssels aus dem Bund ab. Jemand, der sich seine Schlüssel selbst erzeugt hat, wird berechtigt davon ausgehen können, daß nur er über ein Exemplar dieses geheimen Schlüssels verfügt. Wieviel Vertrauen man kann jedoch der Beteuerung eines Angestellten der Zertifizierungsstelle schenken, daß niemand in der Lage ist, von den dort erzeugten Schlüsseln Kopien anzufertigen?

Diese Frage ist schwer zu beantworten und kann bei detaillierter Erörterung zu einem fast theologischen Problem werden: Wann kann man Glauben schenken? Wem? Eine adäquate Antwort verlangt diese Frage schon deshalb, weil die Konsequenzen aus einem Fehlurteil verheerend sein könnten. Wer auch immer an die Kopie eines geheimen Schlüssels gelangt, könnte damit Erklärungen jeglicher Art im Namen des legalen Eigentümers abgeben. Der rechtmäßige Eigentümer könnte um seinen Besitz und seinen Ruf gebracht, ja seine Existenz könnte gefährdet werden. Man stelle sich vor, der Besitzer der illegalen Schlüsselkopie richtet eine Webseite mit - da ist sie wieder - Kinderpornographie ein. Oder wie wäre es mit illegal kopierter Software, oder mit Verleumdungen von Regierungsmitgliedern? Diese Seite wird dann mit der Signatur des eigentlichen Schlüsseleigentümers versehen, die mit der illegalen Schlüsselkopie erzeugt würde. Anschließend genügte eine Anzeige bei den Strafverfolgungsbehörden, um einen unbescholtenen Bürger ins Gefängnis zu befördern. Mit einiger Phantasie kann man sich die unterschiedlichsten Szenarien ausmalen.

Obenstehende Beispiele dürften genügen, die Bedeutung der Geheimhaltung von privaten

Schlüsseln zu illustrieren. Inwiefern werden Signatur-Gesetz, -Verordnung und der Maßnahmenkatalog dem gerecht? Erforderlich wären sichere, d.h. auf ihre Sicherheit geprüfte Verfahren und Geräte auf der Seite der Zertifizierungsstelle. Im Detail würde das bedeuten, daß sichere Algorithmen korrekt implementiert werden, in Geräten, die nicht manipuliert werden können. Der Einsatz dieser Geräte müßte in einem Prozeß erfolgen, der seinerseits Manipulationen ausschließt. Der Prozeß müßte vor allen anderen Dingen so gestaltet sein, daß Duplikate von privaten Schlüsseln unmöglich erzeugt werden können. Nur wenn sichergestellt ist, daß ein privater Schlüssel nur einmal existieren kann, läßt er sich für zuverlässige Signaturen einsetzen. Jede noch so geringe Wahrscheinlichkeit für ein Duplizieren des privaten Schlüssels stellt ein inakzeptables Risiko dar.

Warum diese strenge Wertung? An daheim erzeugte PGP-Schlüssel würde man solche Forderungen sicher nicht stellen. Um von diesen ein Duplikat zu erzeugen, würde es genügen, Zugriff auf den Rechner und die Festplatte, auf denen der Schlüssel gespeichert ist, zu erlangen. Sinn machte diese Aktion nur, wenn sie unbemerkt erfolgen würde, da der Besitzer des Schlüsselpaares die Schlüssel sonst widerrufen würde, was sie praktisch wertlos machen würde. Selbst, wenn der Diebstahl unbemerkt bliebe, wäre nur eine Person davon betroffen. Jeder weitere Schlüssel müßte mit vergleichbar hohem Aufwand beschafft werden, immer unter dem Risiko der Entdeckung.

Innerhalb einer Zertifizierungsstelle könnte jedoch kein Schlüsseleigentümer feststellen, ob sein Schlüssel kopiert wurde. Nicht die Eigentümer der Schlüssel, sondern das Personal der Zertifizierungsstelle würde über die Schlüssel verfügen. Daß eine solche Institution das geballte Interesse vieler Mitlieder der „intelligence society" in Staatsapparaten und konkurrierenden Unternehmen hervorrufen dürfte, ist unschwer vorzustellen. Eine sorgfältige Auswahl des Personals mag eine gewisse Barriere darstellen. Aber wie wirkungsvoll mag diese gegen Methoden *der „Kryptanalyse mit Gewalt"* oder mit Geld sein, wie sie der Experte Bruce Schneier beschreibt:

„Der Kryptanalytiker bedroht, erpreßt oder quält jemanden solange, bis er ihm den Schlüssel verrät. Bestechung wird gelegentlich `Angriff mit gekauftem Schlüssel' genannt. All diese Angriffsmethoden sind äußerst wirkungsvoll und oft der beste Weg, ... " [10]

In diesem Sinne kann es nicht darum gehen, die Möglichkeiten zum Duplizieren geheimer Schlüssel einzuschränken. Vielmehr muß es praktisch unmöglich sein, einen geheimen Schlüssel zu kopieren. Eine solche praktische Unmöglichkeit ist gegeben, wenn der notwendige Aufwand größer als der mögliche Erfolg ist. Nach heutigem Kenntnisstand eignen sich dazu nur sehr teure Smartcards, die gegen Manipulationen gut geschützt sind, sogenannte „tamper proof smartcards". Verschiedene Meldungen in der Fachpresse haben zwar gezeigt, daß auch solche Karten ausgelesen werden können. Aber wer verfügt schon über Kapazitäten, wie die Sandia National Labs in Albuquerque?

Inwieweit reflektiert die Signaturgesetzgebung derartige Bedenken? Kaum, muß man feststellen. Während das Gesetz und die Verordnung noch relativ eindeutig fordern, daß geheime Schlüssel bei der Zertifizierungsstelle nicht gespeichert werden dürfen -

„Sie [die Zertifizierungsstelle - Anm.d.A.] *hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der privaten Signaturschlüssel zu gewährleisten. Eine Speicherung privater Signaturschlüssel bei der Zertifizierungsstelle ist unzulässig. " [11]*

bzw.

„Die Geheimhaltung des privaten Schlüssels muß gewährleistet sein und er darf nicht dupliziert werden können. " [12]

- gehen die Autoren des Maßnahmenkataloges sehr wohl von einer zumindest temporären Speicherung aus, wenn sie schreiben:

„Während der Schlüsselerzeugung und Zertifikatserstellung verwendete Speicherbereiche werden automatisch nach erfolgter Verarbeitung im System so gelöscht (z.B. durch Überschreiben der Speicherinhalte mit einem zufälligen Bitmuster), daß keine Rückschlüsse auf ihren früheren Inhalt möglich sind." [13]

oder auch:

„Signaturschlüssel- oder Personalisierungsdaten auf Datenträgern der Schlüsselerzeugungs- und Zertifikatserstellungsumgebung werden durch geeignete Verschlüsselung vor unberechtigter Kenntnisnahme geschützt. " [13]

Da ist schon deutlich von einer Speicherung der Schlüssel auf Datenträgern die Rede. Im letzten Satz bereitet die Phrase von der *„unberechtigten Kenntnisnahme"* besondere Kopfschmerzen. Wenn es eine *„unberechtigte Kenntnisnahme"* gibt, müßte es doch auch eine „berechtigte Kenntnisnahme" geben, oder warum heißt es sonst nicht einfach „Kenntnisnahme"? Wenn dem so ist, wer gehört zum Kreis der zur Kenntnisnahme berechtigten Personen? Da, scheint es, liegt einiges im Argen, zumal es weitere Passagen mit ähnlich

fragwürdigen Formulierungen, wie *z.B. „Auch das Bedienpersonal der Personalisierungsumgebung darf keine Kenntnis der privaten Schlüssel erhalten."* gibt. Wäre man an einem wirklichen Ausschlußkriterium interessiert, hätte man da nicht Worte, wie „Niemand, auch nicht das Bedienpersonal der Personalisierungsumgebung darf eine Kenntnis der privaten Schlüssel erhalten." finden können, ja müssen?

Nun ist der Maßnahmenkatalog rechtlich nicht bindend. Jede interessierte Firma kann die Vorgaben aus Gesetz und Verordnung so umsetzen, wie sie es für richtig hält. Der Maßnahmenkatalog dient dabei nur zur Orientierung. Eine Zulassung als Zertifizierungsstelle erhält sie jedoch nur nach Prüfung durch eine von der obersten Zertifizierungsstelle bei der Regulierungsbehörde für Telekommunikation und Post. Die führt solche Prüfungen natürlich nicht selbst durch, sondern beauftragt eine andere Institution damit. Jene hat dann die Prüfung nach den *„Angaben des Bundesamtes für Sicherheit in der Informationstechnik unter Berücksichtigung internationaler Standards" [14]* durchzuführen. Und eben jenes BSI hat den Maßnahmenkatalog erarbeitet. Der Maßnahmenkatalog dürfte mithin bei der Evaluierung eine große Rolle spielen.

Man kann festhalten, daß es zumindest Widersprüche im Komplex der Signaturgesetzgebung gibt, was den Umgang mit geheimen Schlüsseln angeht. Das Ziel des Signaturgesetzes, *„Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten" [15],* kann wegen der genannten Unwägbarkeiten im Umgang mit den Schlüsseln kaum erreicht werden.

Haftung?

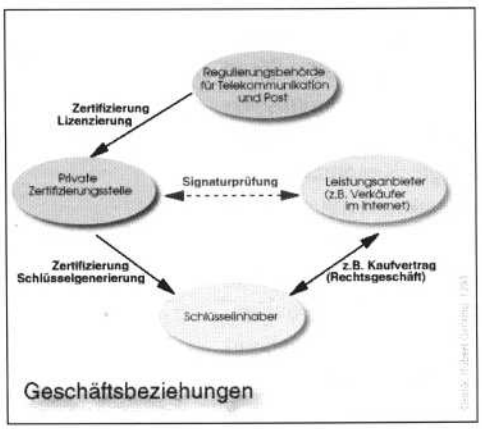
Digitale Signaturen sind ja nun nicht Selbstzweck, Kryptologen einmal ausgenommen. Mit dem Einsatz verbindet die Industrie die Hoffnung auf erleichterte und sichere Geschäftsabwicklung über elektronische Medien. E-Kommerz lautet das Stichwort. Sicherheit bedeutet aber auch, zu wissen, was im Falle der Störung der Geschäftsbeziehung geschehen wird. Im großen und ganzen faßt man diese Problematik unter dem Begriff der Haftung zusammen: Wenn durch mein Verhalten Schaden entsteht, bin ich verpflichtet, diesen zu ersetzen. Im Normalfalle geht es nicht unbedingt um einen Schaden, sondern um die einfache Erfüllung eines Geschäftes. Versandhausware muß bezahlt werden, meint zumindest der Versender und erwartet vom Gesetzgeber Rechtsicherheit, d.h. Instrumente zur Durchsetzung seiner Forderung.

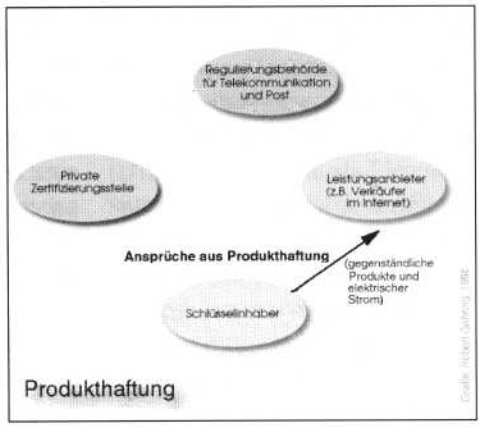
Im klassischen Geschäftsleben gibt es dazu Kaufvertrag und Unterschrift, die als Beleg dienen. Im E-Kommerz gibt es den elektronischen Kaufvertrag mit der elektronischen Unterschrift. Leider ist die Aussage des letzten Satzes nicht wahr. Es gibt keine elektronische Unterschrift, sondern eine digitale Signatur, was nicht dasselbe ist. Das Signaturgesetz stellt digital signierte, elektronische Dokumente papiernen Verträgen mit eigenhändiger Unterschrift nicht gleich. Die Folge davon kann die „Nichtigkeit" sein: *„Ein Rechtsgeschäft, welches durch der durch Gesetz vorgeschriebenen Form ermangelt, ist nichtig. " [16]* Und der Forderung nach der Schriftform -

„Ist durch Gesetz schriftliche Form vorgeschrieben, so muß die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden." [17]

- kann mit einer digitalen Signatur solange nicht nachgekommen werden, wie diese nicht expressis verbis dafür zugelassen wird. Genau das hat der Gesetzgeber unterlassen.

Nun ist nicht unbedingt ein Stück Papier nötig, um ein *Rechtsgeschäft* wirksam werden zu lassen. Die meisten Verträge sind auch ohne Schriftform gültig. (Diejenigen, die über's Internet heiraten wollen, muß ich jedoch enttäuschen. Der Ehevertrag benötigt die Unterschrift der Heiratswilligen und ihrer Trauzeugen, zumindest auf der weltlichen Seite.) Schwierig sieht es nur mit dem Nachweis darüber aus, daß der Vertrag geschlossen wurde. Will man die Erfüllung der Verpflichtungen aus einem Vertrag einfordern, sollte





man besser ein Stück Papier in der Hand haben.

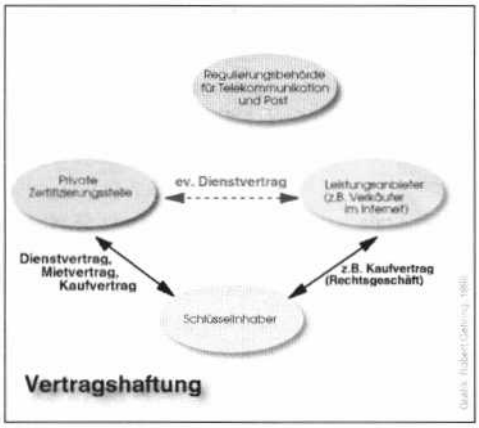
Was aber, wenn das fehlt? Was, wenn man eine E-Mail mit digitaler Signatur in der Hand hält und der mutmaßliche Signatar abstreitet, deren Urheber zu sein. Oder wie sieht es aus, wenn auf Grund eines Fehlers in der Zertifizierungsstelle ein Zertifikat für einen Schlüssel nicht rechtzeitig widerrufen wurde? Jetzt kommt die wirklich schlechte Nachricht: Düster sieht es aus. In der ersten Grafik sind die Beziehungen zwischen den vier betroffenen „Mitspielern" (Regulierungsbehörde als Lizenzgeber, Zertifizierungsstelle als Lizenznehmer, Schlüsselinhaber und Leistungsanbieter) dargestellt. Die anderen Grafiken zeigen die Haftungsansprüche zwischen den einzelnen Beteiligten.

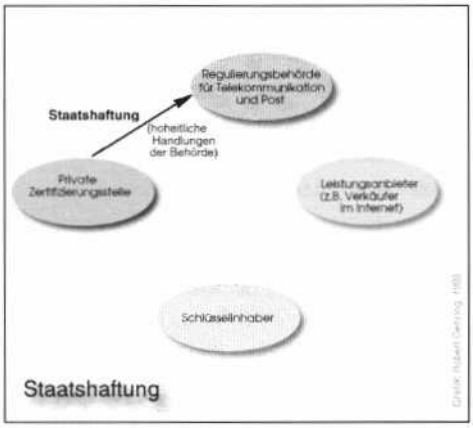
Als Haftungsgrundlagen kommen im Schadensfalle nach deutschem Recht

- Produkthaftung (ProdHaftG)
- Vertragshaftung (§§459, 634 BGB)
  Produzentenhaftung (§823 BGB)
  Staatshaftung (Art. 34 GG)

in Frage. Die Produkthaftung gilt nur für gegenständliche Produkte und elektrischen Strom. Explodierende Smartcards oder selbstentzündliche Lesegeräte würden darunter fallen. Die gespeicherten Schlüssel oder gelesene Daten aus Zertifikaten leider nicht.

Wie sieht es mit der Vertragshaftung aus? Wer schließt mit wem einen Vertrag, und worüber? Ohne Zweifel gibt es den Vertrag zwischen Schlüsselinhaber und Zertifizierungsstelle darüber, die Zertifikate und andere vereinbarte Dienstleistungen zu erbringen. Eventuell bieten die Zertifizierungsstellen selbst auch Lesegeräte für SmartCards zum Kauf oder zur Miete an. Daraus entstehen dann wechselseite Ansprüche zwischen Zertifizierungsstelle und Schlüsselinhaber.





Der Leistungsanbieter hat mit der Zertifizierungsstelle in der Regel keinen Vertrag über die Zertifizierungsleistungen. Da im Gesetz vorgeschrieben ist, daß die Zertifikate jederzeit und von jedermann abrufbar sein müssen, auch ohne Vertrag, gibt es dafür keine Notwendigkeit. Darin besteht ja auch der Vorteil solcher Zertifikate. Sollte der Leistungsanbieter jedoch von sich aus einen Vertrag mit der Zertifizierungsstelle schließen wollen, z.B. von Taiwan aus, dürfte das schwierig werden. Streitet die Zertifizierungsstelle den Vertragsschluß ab, gerät er in dieselbe Beweisnot, wie gegenüber einem unwilligen Kunden. Ein langwieriger Schriftwechsel könnte dem vorbeugen, würde dem Wesen des E-Kommerz jedoch diametral gegenüberstehen. So verbleibt dem Leistungsanbieter nur die Hoffnung auf gutwillige Kunden und sorgfältig arbeitende Zertifizierungsstellen.

Da weder Schlüsselinhaber, noch Leistungsanbieter in einem Vertragsverhältnis mit der Regulierungsbehörde stehen, gibt es auch da keine Vertragshaftung. Ja überhaupt gibt es eigentlich kein Verhältnis zu jener, wodurch auch die Staatshaftung entfällt, die für hoheitsrechtliche Handlungen von Behörden gelten. Inwieweit die Behörde gegenüber den Zertifizierungsstellen haftet, falls sie jener unzulängliche Verfahrensweisen vorschreibt, bleibt weitgehend offen.

Dann gibt es noch die Produzentenhaftung. Die wäre unter Umständen für den Schlüsselinhaber gegenüber der Zertifizierungsstelle anwendbar, erstreckt sich jedoch nicht auf Vermögensschäden. Und die körperliche Unversehrtheit wird durch eine gefälschte digitale Signatur nur in theoretischen Fällen gefährdet sein. Was sagt denn der Gesetzgeber zum Haftungsproblem?

„Hinsichtlich der Haftung der Zertifizierungsstellen gegenüber Dritten kann sich im Einzelfall eine Haftungslücke ergeben." [181

Man ist sich des Problems zumindest teilweise bewußt. Unternommen wurde - bis jetzt - nichts dagegen. Das größte Risiko liegt somit auf der Seite des Leistungsanbieters. Unter solchen Vorzeichen sind die optimistischen Prognosen zum Wachstum des Internethandels mit Vorsicht zu genießen.

Und sonst?

Mit Fehlertoleranz, Schlüsselsicherheit, Kosten und Haftung wur-

INFOS

[1] Utah Digital Signature Act; http://www.commerce.state.ut.us/web/commerce/digsig/act.htm

[2] Massachusetts Electronic Records and Signatures Act; http://www.state.ma.us/itd/legal/mersa.htm

[3] „Im Herbst gehen die ersten Zertifizierungsstellen für die digitale Signatur an den Start. Das Trustcenter setzt den Schlußstein auf das virtuelle Dienstleistungsgebäude", Computer Zeitung Nr. 36/3. September 1998

[4] „Konsortium ignoriert deutsches Gesetz. Banken vergeben digitale Signaturen", Computer Zeitung Nr. 44/29. Oktober 1998

[5] „Scheitert das Multimediagesetz?", Christiane Schulzki-Haddouti, 8.5.1998 in Telepolis, http://www.heise.de/tp/deutsch/inhalt/te/1465/1.html

[6] „Mit der digitalen Signatur läßt sich viel Geld machen", Computer Zeitung Nr. 12/19. März 1998

[7] Tools nur für AI Capone?, Marco Budde, Linux-Magazin 12/98, 5.64 ff

[8] Signaturgesetz, §2 (1); http://www.iid.de/rahmen/iukdgbt.html#a3

[9] Maßnahmenkatalog für digitale Signaturen, Version 1.0 vom 18.11.1997, S. 98, 99, http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/main/spezi.htm#Kataloge

[10] „Angewandte Kryptographie", Bruce Schneier, Addison Wesley-Verlag, 1996, S. 7

[11] Signaturgesetz, §5 (4); http://www.iid.de/rahmen/iukdgbt.html#a3

[12] Signaturverordnung, § 16 (1); http://www.iid.de/rahmen/sigv.html

[13] Maßnahmenkatalog für digitale Signaturen, Version 1.0 vom 18.11.1997, M-SZ 1.2, 5.108, http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/main/spezi.htm#Kataloge

[14] Signaturverordnung, § 17 (2); http://www.iid.de/rahmen/sigv.html

[15] Signaturgesetz, §1 (1); http://www.iid.de/rahmen/iukdgbt.html#a3

[16] BGB §125 S.1

[17] BGB §126 (1)

[18] Amtliche Begründung zum Signaturgesetz; http://telematik.iig.uni-freiburg.de/dbskolleg/public/dbs.kb 1.inhalt.html

[19] BSI-Errichtungsgesetz §3 Abs. 1 Nr.6; http://www.bsi.bund.de/aufgaben/index.htm

den vier der vielen drängenden Fragen diskutiert, die durch die Signaturgesetzgebung aufgeworfen worden sind. Neben diesen, existieren noch andere Kritikpunkte, die erwähnt werden sollten. Da ist das Datenschutzproblem. Eine Zertifizierungsstelle erhält wichtige persönliche Daten. Wer kontrolliert einen verantwortungsvollen Umgang damit? Welche Möglichkeiten für den Zugriff darauf gibt es für Strafverfolgungsbehörden und Nachrichtendienste? Es ist kein Geheimnis, daß das BSI eine ehemalige Zweigstelle des BND ist. Bei seiner Gründung bekam es unter anderem den Auftrag, die *„Dienste der Inneren Sicherheit (Polizei, Staatsanwaltschaften und Verfassungsschutzämter) zu unterstützen" [19]*

Vertrauenerweckend?

Auch mit der internationalen Kompatibilität sieht es nicht so besonders gut aus. Internationale Standards befinden sich zum Großteil noch in der Entwicklung und es ist anzunehmen, daß in vielen Staaten eine derartig unflexible Zertifizierungsstruktur, wie sie das Signaturgesetz vorschreibt, abgelehnt wird. Muß man künftig für jedes Land einen anderen Schlüssel haben? Und was geschieht mit Zertifikaten, die aus dem Ausland abgerufen werden?

Dann wäre da noch die Diskussion über ein Verschlüsselungsverbot. Wenn ein solches wider die Meinung der Experten durchgesetzt werden sollte, was kann man dann von der Sicherheit der für die Signaturen eingesetzten Verschlüsselungsverfahren halten?

Fazit

Wer sich auf das Signaturgesetz verläßt, sollte zumindest mit großer Vorsicht zuwege gehen. Sonst kann es ihm passieren, daß ihn/sie die guten Geister verlassen. Rechtssicherheit zur Position von digitalen Signaturen bietet das Gesetz jedenfalls nicht. Damit ist nicht gesagt, daß gesetzeskonforme Signaturen nicht sicher seien. Vielmehr verbessern sie die Position desjenigen, der sich darauf beruft, nicht entscheidend. Mit PGP oder GPG erzeugte Signaturen können durchaus ebenbürtige Chancen einer Anerkennung vor Gericht haben. Zuverlässige Zeugen für die Authentizität des geheimen Schlüssels werden dabei vorausgesetzt. So spart man sich die Kosten für Zertifizierung und Zusatzhardware. Und gerade in großen Unternehmen kommen dafür schnell erhebliche Summen zusammen.

Ein Gutes hat das Gesetz allerdings - ein „Verfallsdatum". Zwei Jahre nach seinem Inkrafttreten muß es vom Gesetzgeber hinsichtlich seiner Umsetzung überprüft und gegebenenfalls überarbeitet werden. Dieses „Verfallsdatum" ist ein Novum in der deutschen Rechtsgeschichte. Auch eine Art von Fortschritt ;-)

DER AUTOR

Robert Gehring hat Informatik und Philosophie an der TU Berlin studiert. Seit der Linux-Version 0.9.12 ist er mit dabei, entwickelte diverse Software und setzte dieses Betriebssystem auch ausgiebig für seine Sudien/Diplomarbeit ein. Zu erreichen ist er unter *rag@zblmath.FIZ-Karlsruhe.DE*.