Digitale Signaturen

Schriftliche Belegarbeit im Fach
Informatik und Gesellschaft

vorgelegt von

Tino Hempel

Studiengang „Lehramt Informatik“ an der
Ernst-Moritz-Arndt-Universität Greifswald

Greifswald, den 12.01.2001

Inhaltsverzeichnis

1 Einführung

„Als Kinder haben wir von dem tragischen Ereignis gehört, das die Brüder Grimm unter dem Titel ‚Der Wolf und die sieben jungen Geißlein' aufgezeichnet haben ... die Handlung erreicht ihren Höhepunkt, als der Wolf mit durch Kreide verfeinerter Stimme und mit frischen Teig bestrichener Pfote an die Haustür klopft und ruft: "Liebe Kinder, lasst mich ein, ich bin eure Mutter, jedes von euch soll etwas geschenkt kriegen." Die sieben Geiserchen wollten erst die Pfote sehen, und wie sie sahen, dass sie schneeweiß war, und weil sie den Wolf so fein sprechen hörten, glaubten sie, es wäre ihre Mutter, und machten die Thüre auf, und der Wolf kam herein.'

Wir wissen alle, wie die Geschichte weitergeht ... Am besten wäre es gewesen, die Geiß und ihre Geißlein hätten lesen und schreiben können. Dann hätte die Mutter etwa gesagt: ‚Wenn ich zurückkomme, schiebe ich durch den Türschlitz einen Zettel mit meiner Unterschrift, dann könnt ihr erkennen, ob es eure Mutter ist oder nicht.' Auf den Zettel hätten die Geißlein schon eher vertrauen können, so wie wir uns und selbst Gerichte sich auf handschriftlich signierte Dokumente verlassen, gegebenenfalls erst, wenn Gutachter die Echtheit einer Unterschrift nach Vergleich mit anderen Schriftproben verbürgen." [2]

Die Unterschrift – im täglichen Leben garantiert sie dafür, dass ein Dokument von einer ganz bestimmten Person stammt. Wie aber lassen sich elektronische Dokumente signieren?

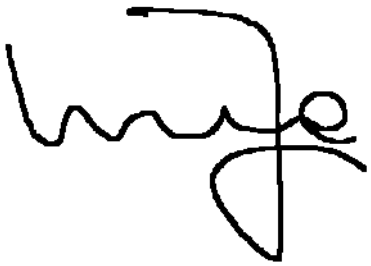

Abb. 1: Eine Unterschrift (aus [VII])

2 Die Unterschrift

2.1 Zweck einer Unterschrift

Eine Unterschrift soll einen Text, einen Vertrag oder ebene eine schriftlich fixierte Aussage bestätigen. Damit wird das geschriebene Wort an eine bestimmte (natürliche) Person gebunden. Diese Person garantiert über die Unterschrift das, was auf demselben Stück Papier oder im selben, zusammengehörenden Dokumentteil (zusammengeheftete Papiere) steht. Das Papier trägt die Informationen und bindet somit die Unterschrift an den Text.
Nach Unterzeichnung sind Änderungen nicht mehr zulässig. Auch hier hilft das Papier, weil auf diesem Medium eine Änderung meistens Spuren hinterlässt und rasch auffällt (siehe auch [VII]).

2.2 Eigenschaften einer Unterschrift

Herkömmliche Unterschriften von Hand besitzen einige Eigenschaften, auf die insbesondere das Rechtswesen zurück greift. Eine Unterschrift

- ist **persönlich**, d.h., sie wird an eine bestimmte Person gebunden,
- ist **eindeutig**, da jede Person eine eigene Unterschrift hat,
- ist **verifizierbar** (überprüfbar), da über einen Vergleich festgestellt werden kann, ob die Unterschrift von einer ganz bestimmten Person stammt.
- sollte möglichst **nicht fälschbar** sein, i.d.R. sind Fälschungen durch Experten schnell nachweisbar.
- **identifiziert** eine bestimmte Person.

3 Rechtliche Grundlagen

3.1 Die eigenhändige Unterschrift

Zum allgemeinen Verständnis ist es notwendig, zunächst die Unterscheidung der Schriftform zu erläutern. Das deutsche Recht unterscheidet zwischen gewillkürter und gesetzlicher Schriftform. Erste wird für nicht gesetzlich vorgeschriebene Schriftstücke, (Bestellungen, Reklamationen, Rechnungen, u.a.) eingesetzt. Die gesetzliche Schriftform wird explizit in Gesetzen als Dokumentation eines Rechtsgeschäfts in Form einer Urkunde festgelegt. Diese Urkunde ist dann manuell zu unterzeichnen. Das BGB drückt dies so aus:

> **§ 126** (Gesetzliche Schriftform)
> (1) Ist durch ein Gesetz schriftliche Form vorgeschrieben, so muss die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichen unterzeichnet werden.

Nach [12] gibt es ca. 3800 Stellen im deutschen Recht, an denen die gesetzliche Schriftform zwingend vorgeschrieben ist (§ 127 BGB).
Das BGB fasst den Zweck einer Unterschrift und ihre Eigenschaften in vier Funktionen der Unterschrift zusammen:

(1) **Abschlussfunktion**
(2) **Identitätsfunktion,** Erkennbarkeit des Ausstellers,
(3) **Echtheitsfunktion,** d.h. erkennbare Urheberschaft des Unterzeichners,
(4) **Warnfunktion**.

Diese Funktionen muss auch eine digitale Unterschrift erfüllen und einige darüber hinausgehende.

3.2 Anforderungen an eine digitale Unterschrift

Eine herkömmliche Unterschrift wird ganz einfach zum betreffenden Dokument hinzugefügt. Wie oben beschrieben sorgt das Papier dafür, dass die Unterschrift mit dem Text in Verbindung gebracht wird. Nichts mehr und nichts weniger als der unterzeichnete Text!
Bei digitalen Dokumenten ist das nicht so einfach. Es genügt nicht, die Unterschrift dem Text mitzugeben. Auf diese Weise besteht keinerlei Beziehung zwischen dem Text und der Unterschrift. Digitale Dokumente können problemlos und vor allem spurlos verändert werden. Neue Textstellen können hinzugefügt und alte Stellen entfernt werden. Bei digitalen Dokumenten muss also die Echtheit des Dokumentes in doppelter Hinsicht garantiert werden.
Erstens der Schutz vor Manipulation durch Dritte (Nachrichtenauthentizität genannt). Der Empfänger B einer Nachricht muss sich sicher sein, das diese auch wirklich vom Absender A stammt und nicht durch den unbekannten Mr. X verfälscht wurde. Um dies zu gewährleisten gibt es verschiedene Verschlüsselungsverfahren.
Zweitens der Schutz voreinander selbst, denn folgende Szenarien sind denkbar (aus [4]):

- Teilnehmer B könnte die von A empfangene Nachricht abändern.
- Teilnehmer A könnte abstreiten, eine Nachricht abgeschickt zu haben und behaupten, B habe die Nachricht gefälscht.

Abhilfe schafft eine digitale Unterschrift, wenn sie folgende Anforderungen erfüllt:

(1) **Authentizität**
Nur der Urheber des Dokumentes kann die Unterschrift erzeugen.

(2) **Nichtübertragbarkeit**
Die Unterschrift gilt nur im Zusammenhang mit dem Dokument, d.h. sie kann nicht auf ein anderes Dokument übertragen werden.

(3) **Verbindlichkeit**
Der Absender kann die Urheberschaft nicht abstreiten.

(4) **Verifizierbarkeit**
Der Empfänger des Dokumentes kann die Unterschrift zweifelsfrei prüfen, d.h. verifizieren oder falsifizieren.

Es ist also **nicht** die Aufgabe digitaler Signaturen dafür zu sorgen, dass Dritte den Inhalt einer Nachricht nicht lesen können.
Die Anforderungen an eine digitale Signatur gehen weit über die Eigenschaften einer „normalen“ Unterschrift hinaus, d.h. es muss ein rechtlicher Rahmen geschaffen werden.

3.3 Die digitale Unterschrift

Seit 1. August 1997 ist in Deutschland das Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG) in Kraft. Der dritte Artikel des Gesetzes ist das Signaturgesetz (SigG).

> **§ 1 Abs. 1 SigG**
> Zweck des Gesetzes ist es, Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können.

Es stellt somit den für den Einsatz digitaler Unterschriften erforderlichen Rahmen zur Verfügung und enthält deshalb auch folgerichtig keine Aussagen zur rechtlichen Verbindlichkeit digitaler Signaturen.
Das Gesetz zur digitalen Signatur definiert eine digitale Unterschrift wie folgt:

> **§ 2 Abs. 1 SigG**
> 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.

Gemäß der Definition einer digitalen Signatur bedarf es also einem mathematisch-kryptologischen Verfahrens, welches für die Herstellung des notwendigen Schlüsselpaares notwendig ist. Die Schlüssel besteht aus einem ”privaten" und einem dazugehörigen

”öffentlichen" Signaturschlüssel. Der ”private" Schlüssel darf nur dem Besitzer bekannt sein, der ”öffentliche" Schlüssel muss dagegen für jedermann zugänglich sein.
Darüber hinaus sind auch sog. staatliche Zertifizierungsstellen notwendig. Diese sollen gewährleisten, dass jede digitale Signatur nur einem Teilnehmer zugeteilt wird und Echtheit und Urheberschaft der Signatur jederzeit überprüfbar und die Unverfälschtheit der Daten feststellbar ist. Aus diesem Grund ist es dringend erforderlich, dass diese Instanzen absolut zuverlässig arbeiten und die notwendigen Sicherheitsanforderungen erfüllen.
Das Signaturgesetz wird durch die Verordnung zur Digitalen Signatur ergänzt.

3.4 Rechtliche Probleme

Die aktuellen Gesetze und Verordnungen beinhalten einige rechtliche Problemen, die hier nur andiskutieret werden sollen.

(1) Im Dezember 1999 erließ die EU eine Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. Diese Richtlinie ist regelt Digitale Signaturen nicht so stark, wie das deutsche Signaturgesetz. Die wichtigsten Punkte der Richtlinie sind:

- Anforderungen an die digitale Signatur
  - Sie muss den Unterzeichner eindeutig **identifizieren**.
  - Der Benutzer muss die **alleinige Kontrolle** über das Zertifikat haben.
  - Signatur und Dokument müssen so miteinander verknüpft sein, dass eine Veränderung zum Dokument offenkundig wird.
- Zertifizierungsstellen bedürfen **nicht** der Genehmigung des Staates.
- Im Gerichtsverfahren gelten digitale Signaturen **gleichermaßen als Beweismittel** wie handschriftliche Unterschriften.
- **Trustcenter haften** für die Richtigkeit der Zertifikate.
- Bis zum 31.12.2000 müssen die EU-Mitgliedstaaten die erforderlichen Rechts- und Verwaltungsvorschriften erlassen, um der Richtlinie nachzukommen.

(2) Trotz Signaturgesetz (SigG von 1997) dürfen für Urkunden in gesetzlicher Schriftform keine elektronischen Dokumente verwendet werden und damit auch keine elektronischen Unterschriften. Da das Signaturgesetz wie oben beschrieben an Europarecht angepasst werden muss, soll im Jahr 2001 die digitale Unterschrift der handschriftlichen gleichgestellt werden. Dazu ist es aber notwendig, die Gesetze und Rechtsvorschriften entsprechend anzupassen [12], wie es z.B. bereits mit der Rechtsvorschrift „Allgemeine Verwaltungsvorschrift über Rechnungswesen in der Sozialversicherung“ § 41 geschehen ist.

§ 41
Soweit nach dieser Verwaltungsvorschrift eine Unterschrift verlangt

wird, kann diese durch eine digitale Signatur nach dem Signaturgesetz geleistet werden.

4 Umsetzung der digitalen Signatur

4.1 Kryptographische Ideen

Bis in die 70er Jahre des 20. Jahrhunderts war man der festen Überzeugung, dass es nicht möglich ist, eine geheime Nachricht zu übermitteln, ohne sich vorher über den Codierungsschlüssel ausgetauscht zu haben. 1976 stellten Whitefield Diffie und Martin Hellmann in einer wissenschaftlichen Publikation mit dem provokanten Titel „New Directions in Cryptography“ die Frage, ob es eine Verschlüsselung ohne Schlüsselaustausch überhaupt geben kann. Mit anderen Worten: Ist es möglich, dass ich einer mir völlig unbekannten „wildfremden“ Personen, eine verschlüsselte Nachricht zuschicken und nur diese die Information daraus entschlüsseln kann, ohne vorher mit ihr irgendwie kommuniziert zu haben?
Zwar konnten die Autoren die Frage nicht beantworten, sie formulieren sie aber mathematisch. Dabei taucht der Begriff der Einwegfunktion auf. Eine solche Funktion arbeitet wie eine Einbahnstraße. In die eine Richtung kann man problemlos Werte berechnen, aber in die andere Richtung (eigentlich) nicht. „Eigentlich“ deshalb, weil es für die Anwendung solcher Funktionen in der Kryptologie eine „trapdoor“, also einen Geheimgang geben muss, mit der man die Einwegfunktion doch rückgängig machen kann.
Im übertragenen Sinne stellt für einen Schüler der Jahrgangsstufe 6 das Quadrieren vom echt gebrochenen Zahlen eine solche Funktion dar. Für ihn ist es (hoffentlich) leicht die Gleichung $y = 1{,}32^2$ zu lösen, (fast) unmöglich ist jedoch die Lösung der Gleichung $1{,}724 = x^2$. Allerdings liegt es hier nicht an der Schwierigkeit der darin verborgenden Mathematik, sondern am mangelnden Know-how.
Diffie und Hellmann bewiesen nun, dass aus der Existenz von trapdoor Einwegfunktionen auch die Möglichkeit der Verschlüsselung ohne vorherigen Schlüsselaustausch folgt. Allerdings konnten sie eine solche trapdoor Einwegfunktion nicht angeben. Erst den Forschern Ronald Rivest, Adi Shamir und Len Adlemann gelang dies. Interessanterweise beim Versuch, die Existenz von trapdoor Einwegfunktionen zu verneinen! Mit der gefundnen Funktion entwickelten die drei Erfinder 1977 den berühmtesten Public-Key-Algorithmus RSA, entsprechend der Erfinder-Initialen (siehe auch [1]).

4.2 Der RSA-Algorithmus

In der klassischen Kryptographie gibt es einen Klartext, der mit Hilfe eines geheimen Schlüssels in einen Geheimtext umgewandelt wird. Der Empfänger muss nun zum Entschlüsseln wieder mit dem geheimen Schlüssel arbeiten, d.h. beiden muss der geheime Schlüssel bekannt sein!

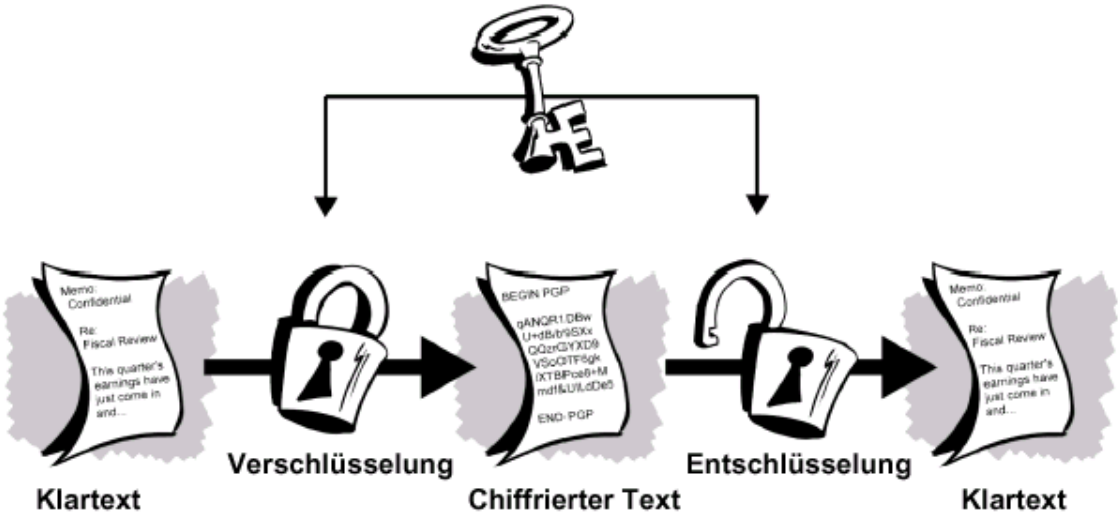

Abb. 2: Verschlüsselung mit konventionellem Schlüssel (aus [6])

Das Problem: der geheime Schlüssel muss ja auch irgendwie übermittelt werden. Deshalb wäre es günstiger, wenn es keine zu übertragende Geheimnisse (Schlüssel, Codebücher, o.ä.) gäbe. Die Lösung: Nutzung der trapdoor Einwegfunktionen. Im Falle der RSA-Verschlüsselung sind dies Primzahlfaktorisierungen, denn die Schlüssel werden über eine Zahl n gebildet, die das Produkt zweier Primzahlen p und q sind. p und q müssen so groß gewählt werden, dass niemand in der Lage ist, n in das Produkt seiner beiden Primzahlen zu zerlegen. Nach längerem Rechnen (durch Zusammenschaltung mehrerer Rechner) gelang es 1996 dem amerikanischen Mathematikprofessor Arjen K. Lenstra die 130-stellige RSA-Zahl (Darstellung ca. 500 Bit) in zwei Primfaktoren zu zerlegen. Man empfiehlt heute übrigens eine 1024 Bit-Zahl zu verwenden. Neben der Zahl n, die ein öffentlicher Schlüssel ist, benötigt man noch zwei weitere Zahlen d und e. Außerdem bestimme man zwei natürliche Zahlen e und d, gemäß der hier angegebenen Formel $e \cdot d \bmod (p-1)(q-1) = 1$, wobei „mod“ die Restfunktion ist, d.h. $e \cdot d$ ist zu $(p-1)(q-1)$ teilerfremd. Die Zahl e wird mit zum öffentlichen Schlüssel, d.h. sie ist mit n allen zugänglich (zu machen). Der geheime Schlüssel d wird dem Teilnehmer zugeordnet. Nun kann ver- und entschlüsselt werden. Dazu geht man so vor:

	Verschlüsseln eines Textes durch einen beliebigen Teilnehmer	Entschlüsseln des Geheimtextes c durch den Empfänger
1.	Umwandlung des Klartexts in eine Zahl m mit m < n z.B. Zeichenfolge durch den ASCII-Code ersetzt.	Berechnung von m' = c^d mod n mittels des privaten Schlüssels des Empfängers
2.	Berechnung von c = m^e mod n aus den öffentlichen Schlüsseln des Empfängers	Umwandlung der Zahl m' in den Klartexts
3.	Übermittlung des Geheimtexts c	

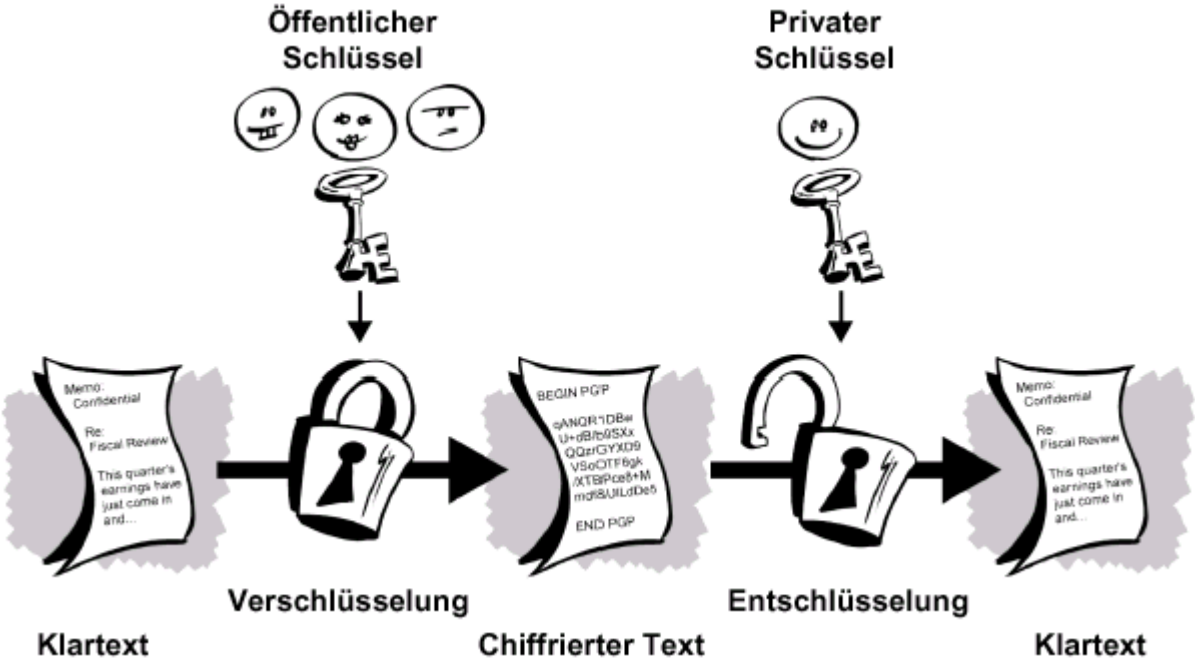

Abb. 3: Verschlüsselung mit öffentlichen Schlüsseln (aus [6])

4.3 Digitale Unterschrift – Version I

Mittels RSA-Verfahren lassen sich nun die digitale Signaturen bilden. Zur Erinnerung: die Signatur muss den Unterzeichner eindeutig identifizieren und Signatur und Dokument müssen so miteinander verknüpft sein, dass eine Veränderung zum Dokument offenkundig wird.
Also darf nur der Versender der Nachricht die Signatur verfassen können und dies mit einer geheimen, nur ihm zugänglichen Information, denn sonst könnte es ja jeder unterschreiben. Damit ergibt sich zwangsläufig die folgende Prozedur zum digitalen Signieren:

1.	Umwandlung der Nachricht in eine Zahl m kleiner als n,
2.	Berechnung von s = m^d mod n mit Hilfe des privaten Schlüssels des Senders s ist dann die digitale Signatur der Nachricht m
3.	Versenden des unterschriebenen Dokumentes bestehend aus der Nachricht m und der Signatur s

Das Dokument kann nun von jedem verifiziert werden.

1. Berechnung von m' = s^e mod n mit Hilfe des öffentlichen Schlüssels des Senders
2. Überprüfung, ob m = m' ist. Falls dies gilt, ist das Dokument echt und stammt vom Sender.

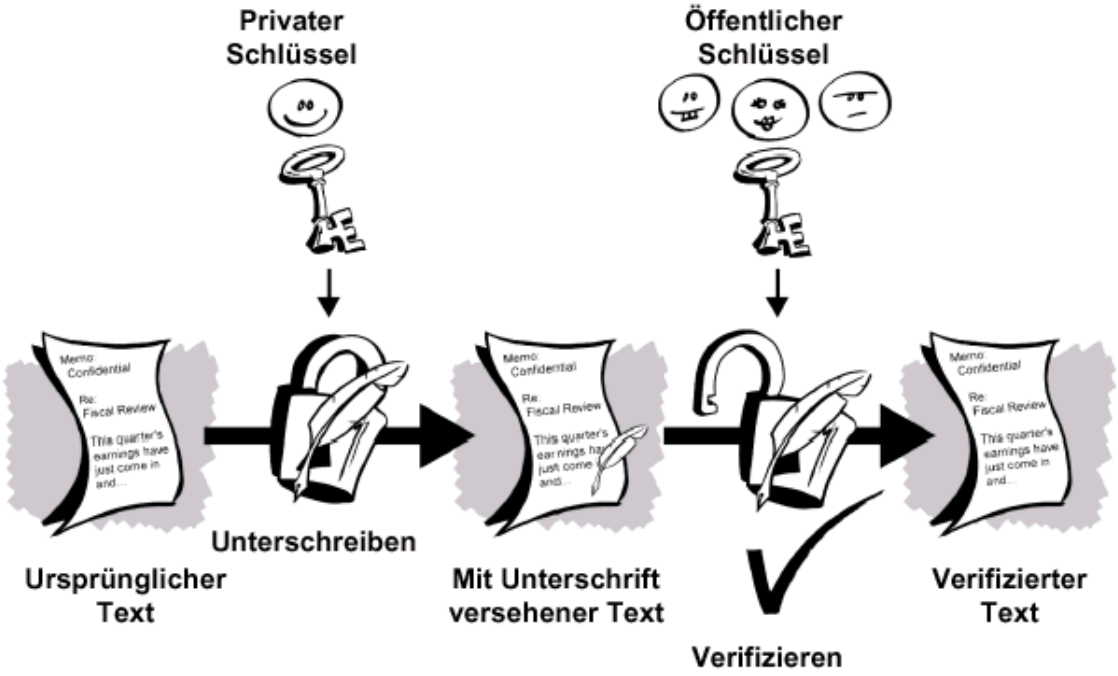

Abb. 4: Einfache digitale Unterschrift (aus [6])

Im folgenden soll anhand eines einfachen Beispieles der Vorgang des Signierens gezeigt werden. Die angegebenen Berechnungen wurden mit dem Programm DERIVE durchgeführt. (Zahlenmaterial aus [16])

1. Bestimmung der geheimen und öffentlichen Schlüssel

(i.d.R. durch das Trust-Center oder ein geeignetes Verschlüsselungsprogramm, wie etwa PGP)

- Wahl zweier großer Primzahlen p und q:
  p = 37419669101 q = 11110693267
- Bestimmen des Produkts n = p · q
  n = 415758465533848642967
  n lässt sich übrigens relativ schnell (DERIVE auf Pentium 120: ca. 20 Sekunden) wieder faktorisieren und genügt somit nicht den Sicherheitsanforderungen. p und q sollten ja auch mehr als 160 Dezimalstellen haben!
- Bestimmung x = (p-1)·(q-1)
  x = (p-1)·(q-1) = 41575846548531828060O
- Suchen einer Zahl e, die zu x teilerfremd ist, also ggT(e,x) = 1
  e = 2^{16} + 1 = 65537

- Bestimmung der Zahl d mit e·d mod x = 1 unter Nutzung des Erweiterten Euklidischen Algorithmus (siehe auch [16])
  d = 16481384459631305873
- Veröffentlichung von n und e als öffentlicher Schlüssel, Geheimhaltung von d als privater Schlüssel

2. Bilden der Unterschrift

- Umwandeln des Textes in eine Zahlenfolge m < n (hier durch Stelle des Buchstaben im Alphabet)
  Text: MUSTERMANN → m = 13211920051813011414
- Signieren von m zu s mit $s = m^d \bmod n$
  $s = 13211920051813011414^{16481384459631305873} \bmod 415758465533848642967$
  s = 25673749040340126743
- Übermittlung des Textes und der Unterschrift s

3. Prüfen der Unterschrift

- Berechnen von m' mit $m' = s^e \bmod n$
  $m' = 25673749040340126743^{65537} \bmod 415758465533848642967$
  m' = 13211920051813011414
- Umwandeln der Zahlenfolge in einen Textes ebenfalls durch die Stelle des Buchstaben im Alphabet
  m' = 13211920051813011414 → Text: MUSTERMANN
- Prüfung auf Gleichheit der Texte

Beispiel mit Manipulation an der Unterschrift

- Sei s nun manipuliert zu s' = 25673749040340126740
- Berechnen von m'' mit $m'' = s^e \bmod n$
  $m'' = 25673749040340126740^{65537} \bmod 415758465533848642967$
  m'' = 324175484298523535472
- Umwandeln der Zahlenfolge in einen scheitert bereits am Zahlenanfang, da es nur 26 Buchstaben gibt und somit zu 32 kein „Gegenstück"

4.4 Digitale Unterschrift – Version II

Das oben beschriebene Verfahren hat einige Nachteile:

- Die digitale Signatur ist genauso lang wie die eigentliche Nachricht, d.h. es muss die doppelte Datenmenge übertragen und gespeichert werden.
- Das Signaturverfahren ist sehr langsam. Das liegt insbesondere in der Berechnung der großen Potenzzahlen. Außerdem produziert eine gewaltige Datenmenge, mindestens das Doppelte der ursprünglichen Daten.

Die Probleme lassen sich durch den Einsatz einer sog. Einweg-Hash-Funktion h(x) (auch Fingerprint genannt) lösen. Diese hat folgende Eigenschaften:

- Nachrichten beliebiger Länge x werden auf Nachrichten einer festen kurzen Länge h(x) abgebildet (typischer Wert: 160 Bit),
- h(x) lässt sich effizient aus x berechnen, aber es gibt keinen effizienten Algorithmus, um x aus h(x) zu ermitteln
- Es ist praktisch unmöglich, zwei verschiedene Nachrichten x und y mit gleichem Hashwert h(x) =h(y) zu finden.

Mit Hilfe der **nicht geheimen** Hash-Funktion lassen sich nun (verbesserte) digitale Signaturen bilden und zwar wie folgt:

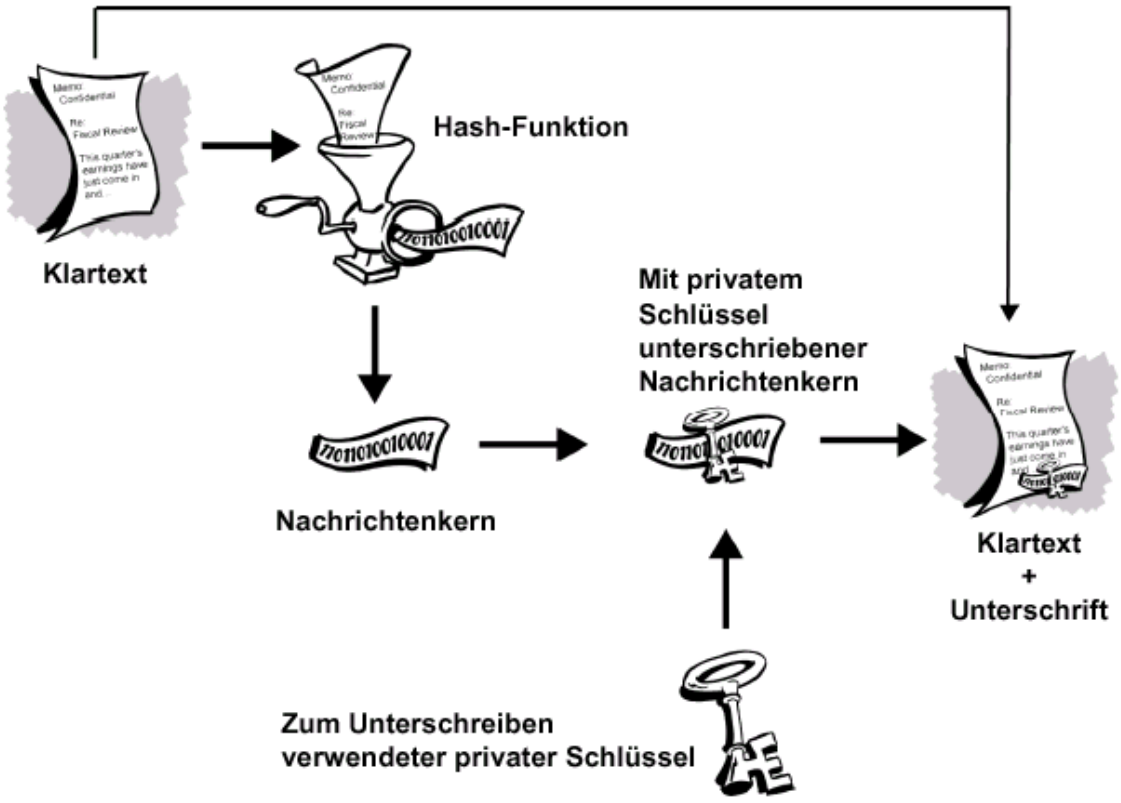

Abb. 5: Sichere digitale Unterschrift (aus [6])

1.	Umwandlung der Nachricht in eine Zahl M,
2.	Berechnung des Hash-Wertes m = h(M); dies geht sehr schnell, da ein effizienter Algorithmus vorliegt
3.	Signierung der „Zwischennachricht“ m über $s = m^d \bmod n$ mit Hilfe des privaten Schlüssels des Senders s ist dann die digitale Signatur der Nachricht M
4.	Versenden des unterschriebenen Dokumentes bestehend aus der Originalnachricht M und der Signatur s

Das Dokument kann nun von jedem verifiziert werden.

1. Berechnung von h(M) über die öffentlich bekannt Hash-Funktion,
2. Berechnung von m' = s^e mod n mit Hilfe des öffentlichen Schlüssels des Senders
3. Überprüfung, ob h(M) = m' ist. Falls dies gilt, ist das Dokument echt und stammt vom Sender.

Da mit der Hash-Funktion eine Bitfolge fester Länge erzeugt wird, entstehen auch nur kleine Signaturen, deren Berechnung schnell geht. Durch die Einweg-Eigenschaft der Hash-Funktion kann auch keine „Scheinnachricht" generiert werden, die vom Absender stammen soll. Auch der Austausch der Signaturen fällt sofort auf, da die Hash-Funktion kollisionsfrei sein muss.

4.5 Sicherheitsaspekte der digitalen Signatur

Die oben beschriebene Verfahren haben Schwachstellen:

(1) Ein Teilnehmer A, der eine Nachricht versandt hat, kann dies bestreiten, indem er behauptet, sein privater Schlüssel sei verloren oder gestohlen wurden und jemand anderes hat die Signatur damit gefälscht.

(2) Einem Teilnehmer A kann der private Schlüssel tatsächlich gestohlen wurden sein; der Dieb kann nun Nachrichten senden, die anscheinend vom Teilnehmer A stammen.

(3) Ein Angreifer könnte anstelle des öffentlichen Schlüssels des Teilnehmers A seinen öffentlichen Schlüssel in das Verzeichnis aller öffentlichen Schlüssel schreiben.

Diese Schwachstellen können beseitigt bzw. entschärft werden, durch die Verwendung der im Signaturgesetz vorgesehenen Zertifizierungsstellen.

§ 2 Abs. 2 bis 4 SigG

(2) Eine **Zertifizierungsstelle** im Sinne dieses Gesetzes ist eine natürliche oder juristische Person, die die Zuordnung von öffentlichen Signaturschlüsseln zu natürlichen Personen bescheinigt und dafür eine Genehmigung gemäß § 4 besitzt.

(3) Ein **Zertifikat** im Sinne dieses Gesetzes ist eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person (Signaturschlüssel-Zertifikat) oder eine gesonderte digitale Bescheinigung, die unter eindeutiger Bezugnahme auf ein Signaturschlüssel-Zertifikat weitere Angaben enthält (Attribut-Zertifikat).

> (4) Ein **Zeitstempel** im Sinne dieses Gesetzes ist eine mit einer digitalen Signatur versehene digitale Bescheinigung einer Zertifizierungsstelle, dass ihr bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben.

Durch Zertifikate soll sichergestellt werden, dass ein öffentlicher Schlüssel wirklich dem angegebene Eigentümer gehört und keine Fälschung ist. Dabei ist ein Zertifikat eine Bescheinigung, ähnlich eines Ausweises. Es enthält zusätzlich zum öffentlichen Schlüssel Daten, mit denen festgesellt werden kann, ob der Schlüssel gültig ist. Das Zertifikat enthält

- einen öffentlichen Schlüssel,
- Zertifikatsdaten, also die Daten zur „Identität“ eines Benutzers (Name, Benutzer-ID, usw.),
- einer oder mehreren digitalen Unterschriften.

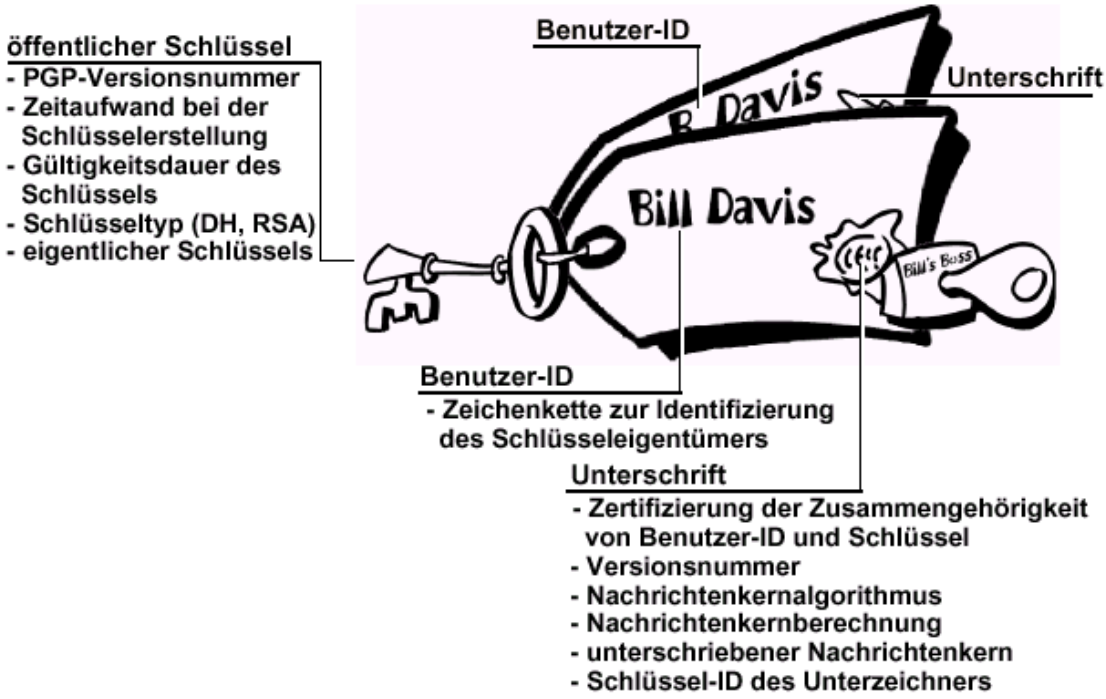

Abb. 6: Bestandteile eines PGP-Zertfikates (aus [6])

Mit der digitalen Unterschrift auf dem Zertifikat werden die Zertifikatsdaten durch eine dritte Person oder Behörde beglaubigt. Es wird somit ausgesagt, dass die unterschriebenen Daten zum öffentlichen Schlüssel gehören oder an diesen gebunden sind.

Der Austausch der Zertifikate kann in kleine Gruppen manuell über Disketten oder E-Mails mit den jeweiligen öffentlichen Schlüsseln der Eigentümer erfolgen. Dieses Verfahren ist aber im großen Rahmen unpraktisch. Deshalb gibt es sog. Certificate Servers mit hohem Sicherheitsstandard. Diese Server bestehen aus einer Datenbank und dienen ausschließlich der Speicherung und des Austauschs von öffentlichen Schlüsseln. Mit zusätzlichen Schlüsselverwaltungsfunktionen versehen sind sog. „Public Key Infra-Struktur“ (PKIs). Diese haben neben den Funktionen eines Certificate Servers auch die Möglichkeit Zertifikate

auszustellen, zurückzunehmen, zu speichern, abzurufen und diese zu vertrauen. Zu jeder PKI gehört eine Zertifizierungsstelle, d.h. eines von der Bundesrepublik Deutschland genehmigtes Unternehmen, welches zur Zertifikatsausstellung ermächtigt wurde.
Gemäß der Forderungen des gültigen SigG läuft die Schlüsselvergabe und Zertifizierung wie folgt ab:
„Die staatlich zugelassenen Zertifizierungsstellen (auch Trust-Center genannt) erzeugen für Antragsteller ein Paar aus öffentlichem und privatem Schlüssel. Im Zusammenhang damit weist die Zertifizierungsstelle jedem Schlüsselpaar eine individuelle und registrierte Benutzeridentität zu, die vorab durch Vorlage eines Personalausweises oder Rücksprache mit den Meldebehörden beglaubigt wurde. Die Verknüpfung von Benutzeridentität und Schlüsselpaar wird mittels eines geheimen Schlüssels der Zertifizierungsstelle dauerhaft und manipulationssicher auf einer Chipkarte ... versiegelt. Damit sind die Zertifizierungsstellen quasi die Einwohnermeldeämter des Internets, bei denen sich jeder über die Gültigkeit einer fremden Signatur erkundigen kann.“ [5]
Damit ist das Problem (3) einigermaßen gelöst. „Risiken birgt des weiteren der gleichzeitige Verlust von Chipkarte und PIN-Nummer. Insoweit gilt es, die gleichen Verhaltensregeln wie für Scheck- bzw. Kreditkarten zu beachten. Geht dem Anwender die Karte dennoch verloren, so muss er, um jeglichen Missbrauch sicher ausschließen zu können, seinen (privaten) Signaturschlüssel bei der Zertifizierungsstelle sperren lassen ...“ [XI]

5 Aktuelle Entwicklungen

5.1 Rechtsentwicklung

Die alte SigG bespricht nur die von behördlich zugelassenen Zertifizierungsstellen ausgegebene digitale Signatur, für die es keine rechtlichen Schranken gibt. Fällt die in der Zertifizierungsstelle erworbene Chip-Karte mit der digitalen Signatur in falsche Hände, so ist es möglich, den Bestohlenen maximal zu schädigen, denn dem Besitzer obliegt die Beweislast und auch die Haftung.
Um diese Mankos zu beseitigen geben die TrustCenter sogenannte Attribut-Zertifkate aus. Diese Attribute können beliebige Beschränkungen für Transaktionswerte (z.B. 400 DM) und Gebrauchsarten (z.B. „nur für betriebliche Zwecke“) beinhalten. Berücksichtigt dies ein Anbieter nicht, so kann der Eigentümer der Signaturkarte für eventuell eintretenden Schaden nicht haftbar gemacht werden. Außerdem gehen die Trust-Center dazu über, zusätzliche Versicherungen anzubieten.
Das Bundeskabinett beschloss am 16. August 2000 den „Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“. Diese Gesetz soll das derzeit gültige Signaturgesetz von 1997 ablösen. Die Neufassung des Signaturgesetzes wurde ja aufgrund der EU-Richtlinie notwendig. Nach dem Zeitplan der

Regierung soll das neue Gesetz am 01. Januar 2001 in Kraft treten, dieser Zeitpunkt ist aber nicht mehr einzuhalten.

Einige wichtige Änderungen (gemäß der Anpassung) sind:

- Drei Arten von digitalen Signaturen:
  - **elektronische Signaturen** – Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen *(z.B. Abscannen des Augenhintergrundes)*
  - **fortgeschrittene elektronische Signaturen** – wie oben, die jedoch
    a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
    b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
    c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
    d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,
    (*also Verfahren, die die Integrität und Authentizität der Daten sicherstellen, aber keinen Anforderungen an die technische Infrastruktur unterliegen (z.B. PGP)).*
  - **qualifizierte elektronische Signaturen** – fortgeschrittene elektronische Signaturen, die jedoch
    a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
    b) mit einer sicheren Signaturerstellungseinheit erzeugt werden,
    (*entspricht weites gehend der bisherigen Regelung)*
- **Haftung seitens der Anbieter**
- Statt eines Genehmigungsverfahrens der Trust-Center soll es ein **freiwilliges Akkreditierungsverfahren** geben, dennoch bleiben die Institute unter der Kontrolle der Regulierungsbehörde.

Mit den neuen Regelungen wird das bisherige strenge Gesetz aufgeweicht und entfernt sich damit vom bisherigen hierarchischen Verwaltungsansatz und macht auch anarchische Varianten (wie etwa PGP) möglich.

In den USA sieht das Signaturgesetz übrigens keinerlei staatliche Aktivität für Normierung vor. Nach Angaben der Amerikaner wird sich der Markt selbst regulieren.

5.2 Entwicklung von Einsatzmöglichkeiten

In der Praxis werden digitale Signaturen stark diskutiert. Die wohl (für den Privatanwender) wichtigsten Anwendung dürften im elektronischen Zahlungsverkehr liegen. Hier einige Beispiele, die das Trust-Center „SecCommerce“ sieht:

- **Online-Anmeldung neuer Kunden** inkl. Schlüsseldiskettenerstellung, Verwendung von Signaturkarten (SmartCard, JavaCard) und ggf. Konto/Depoteröffnung.

- **Online-Banking:** Ausführen von Überweisungen, Einrichten von Daueraufträgen, Kontostandabfrage etc.
- **Online-HBCI-Banking**: Ausführen von HBCI-Banking-Vorgängen, Anbindung von HBCI-Kartenlesegeräten
- **Online-Fonds-Banking:** Depoteröffnung, Einrichtung eines Ansparplans oder eines Entnahmeplans etc.
- **Online-Brokerage:** Depotverwaltung, Kauf/Verkauf-Aufträge etc.
- **Online-Insurance:** Berechnung und Abschluss von Versicherungen etc.

Die IT-Branche diskutiert digitale Signaturen sehr stark. Einerseits ist die Einführung und Benutzung extrem wünschenswert, andererseits hindert das SigG die digitalen Signaturen. Als Beispiele seien hier nur einige Schlagzeilen aus der ComputerZeitung des Jahres 2000 aufgeführt:

Nr. 16 vom 20.04.2000	Zertifikationseinsatz lohnt sich kaum ... Bei Kosten im fünf- bis sechsstelligen Bereich eignen sich Public-Key-Infrastrukturen nur für große Unternehmen ...
Nr. 16 vom 20.04.2000	Verschlüsselungsverfahren sollen Sicherheit im Netz gewährleisten ... Digitale Unterschriften kommen in Mode ... Die Public-Key-Infrastruktur (PKI) erfreut sich heute zunehmender Beliebtheit ...
Nr. 22 vom 02.06.2000	Digitale Signatur sorgt für Streit ... Der Empfänger einer E-Mail soll künftig die Beweislast für die Korrektheit einer Signatur zu tragen haben ...
Nr. 37 vom 14.09.2000	Digitale Signatur soll nicht immer gelten Noch in diesem Jahr wird das deutsche Signaturgesetz an Europarecht angepasst ... Jörg Tauss, Medienbeauftragter der SPD-Bundestagsfraktion, hofft, dass die digitale Unterschrift noch im nächsten Jahr der handschriftlichen gleichgestellt wird.
Nr. 37 vom 14.09.2000	Digitale Signatur kommt gut an ... 70 Prozent der Internet-Benutzer befürworten die Gleichstellung der digitalen Signatur mit ihrem handschriftlichen Pedant ... Rund die Hälfte der Befragten hat jedoch Sorgen bezüglich der Sicherheit ...
Nr. 40 vom 05.10.2000	Digitale Signaturen sind lange noch nicht unterschriftsreif ... Digitale Signaturen drohen zum Rohrkrepierer zu werden. Komplexe Installationen sowie rechtliche und

	technische Probleme verschrecken die Nutzer einer Public-Key-Infrastruktur (PKI) ...
Nr. 41 vom 12.10.2000	Digitale Signatur bekommt Beine ... Der Mobilfunk soll digitalen Signaturen den erhofften Durchbruch bringen ...
Nr. 41 vom 12.10.2000	Digitale Signatur bekommt Beine „Das deutsche Gesetz hat digitale Signaturen gebremst“
Nr. 43 vom 26.10.2000	Viele Gremien werkeln an mobilen Signaturen

6 Zusammenfassung

Digitale Signaturen sind eine „feine Sache“. Allerdings haben sie sich noch nicht durchsetzen können. Als Gründe hierfür sind die strengen rechtlichen Regelungen zu nennen und die für die Unternehmen und den Endanwender auftretenden Kosten (z.B. für das Chipkartenlesegerät). Erst die Liberalisierung des Signaturgesetztes aufgrund der Anpassung an die EU-Richtlinie könnte den Durchbruch der digitalen Signatur auf allen Gebieten bringen. Insbesondere durch die Anerkennung der Unterschrift (fortgeschrittene elektronische Signatur) durch das weltweit am häufigsten genutzte Programm PGP ist auch der Privatanwender in der Lage, von der Entwicklung zu profitieren (zur Anwendung von PGP siehe auch [IX]). Allerdings hat der Gesetzgeber bisher versäumt festzulegen, für welche Zwecke die drei Arten der elektronischen Unterschrift einzusetzen sind. Bleibt zu hoffen, dass es hier keine zu starke Beschränkungen gibt.

Die Anwendung der digitalen Unterschrift löst aber nur eine Klasse von oben beschriebenen Problemen. Es sollte nicht vergessen werden, dass die Nachricht nach wie vor als Klartext übermittelt wird und damit für einen böswilligen Angreifer lesbar ist. Abhilfe schafft hier nur die Benutzung eines Signiersystems, d.h. die Nachricht wird zunächst nach Methode II unterschrieben und anschließend chiffriert (siehe auch [5]).

Das Thema „Digitale Signaturen“, welches im Bereich Informatik und Gesellschaft angesiedelt ist, sollte auch im Schulunterricht des Fachs Informatik eine Rolle spielen. Umsetzungsmöglichkeiten dazu findet man insbesondere in [4] und [5]. Als Online-Quelle sei der fertig ausgearbeitete Unterrichtsbaustein der ETH Zürich [VII] zu nennen.

7 Erklärung

Ich versichere, dass ich die Arbeit selbständig angefertigt, nur die angegebenen Hilfsmittel benutzt und alle Stellen, die dem Wortlaut oder dem Sinn nach anderen Werken entnommen sind, durch Quellen als Entlehnung kenntlich gemacht habe.

Greifswald, den 12.01.2001 Tino Hempel

8 Anhang

8.1 Online-Quellen

[I] Sicherheit im Internet: Internet-Seiten der Bundesministerien für Wirtschaft und Technologie sowie des Inneren und des Bundesamtes für Sicherheit in der Informationstechnik.
URL: http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=38

[II] BSI-Projektbüro „Digitale Signatur": Internet-Seiten des Bundesamtes für Sicherheit in der Informationstechnik.
URL: http://www.bsi.de/aufgaben/projekte/pbdigsig/index.htm

[III] Die Digitale Signatur: Private Internet-Seite.
URL: http://www.digital-law.net/knupfer/

[IV] E-Commerce mit der digitalen Signatur: Private Internet-Seite.
URL: http://home.t-online.de/home/Jens.Uhl/digitalesignatur.htm

[V] Digitale Signatur: Private Internet-Seite.
URL: http://home.t-online.de/home/ifkom-da/digsig.htm

[VI] SecCommerce GmbH: Digitale Signatur für sicheres E-Commerce:
URL: http://www.seccommerce.de/

[VII] EducETH – Informatik – ETH-Lernaufgabe: Digitale Unterschrift.
URL: http://www.educeth.ch/informatik/lernaufg/digsign/

[VIII] Online-Gesetzestexte:
URL: http://www.iid.de/

[IX] E-Mails.....aber sicher! Leitfaden der Landesbeauftragten für den Datenschutz für sichere elektronische Post.
URL: http://www.lfd.nrw.de/fachbereich/fach_7_3_2_zusammensetzen.html

[X] Telekom T-TeleSec TrustCenter:
URL: http://www.telekom.de/dtag/t-telesec/start

[XI] IHK Köln: Merkblatt zur „Digitalen Signatur“
URL: http://www.ihk-koeln.de

8.2 Print-Quellen

[1] Beutelsbacher, A.: Geheimsprachen: Geschichte und Techniken. München: Beck, 1997. (Beck'sche Reihe: 2071), S. 66ff.

[2] Kippenhahn, R.: Verschlüsselte Botschaften: Geheimschrift, Enigma und Chipkarte. Reinbek bei Hamburg: Rowohlt Verlag, 1997, S. 268ff.

[3] Bauer, F.L.: Entzifferte Geheimnissee – Methoden und Maximen der Kryptologie. Berlin u.a.: Springer, 1995.

[4] Baumann, R.: Digitale Unterschrift – Sichere Rechtsgeschäfte im Internet (Teil 1). In: LOG IN, 19 (1999), H.2, S. 46-49.

[5] Baumann, R.: Digitale Unterschrift – Sichere Rechtsgeschäfte im Internet (Teil 2). In: LOG IN, 19 (1999), H.3/4, S. 82-89.

[6] Network Associates Inc. (Hrsg.): Handbuch "Einführung in die Kryptographie", Bestandteil des Softwarepaketes PGP Ver. 6.5.1. deutsch, Datei „IntroToCrypto.pdf".

[7] Network Associates Inc. (Hrsg.): Handbuch "PGP Benutzerhandbuch", Bestandteil des Softwarepaketes PGP Ver. 6.5.1. deutsch, Datei: „PGPWinUsersGuide.pdf".

[8] „Digitale Signaturen sind ...": Computerzeitung vom 05.10.2000, Nr. 40, S. 1.

[9] „Zertifikationseinsatz ...": Computerzeitung vom 20.04.2000, Nr. 16, S. 1.

[10] „Verschlüsselungsverfahren sollen...": Computerzeitung vom 20.04.2000, Nr. 16, S. 49.

[11] „Digitale Signatur sorgt für Streit": Computerzeitung, vom 02.06.2000, Nr. 22, S. 1.

[12] „Digitale Signatur soll nicht immer gelten": Computerzeitung vom 14.09.2000, Nr. 37, S. 1, S.7 und S. 30.

[13] „Digitale Signatur bekommt Beine": Computerzeitung vom 12.10.2000, Nr. 41, S. 1.

[14] „Digitale Signatur bekommt Beine": Computerzeitung vom 12.10.2000, Nr. 41, S. 16.

[15] „Viele Gremien werkeln ...": Computerzeitung vom 26.10.2000, Nr. 43, S. 4.

[16] Becker, K.; Beutelsbacher, A.: Hinter Schloß und Riegel. In: mc Heft 05/1995, S. 88ff.

[17] Vorlesungsmitschrift: „Kryptologie", Prof. Böttcher, TU Chemnitz, 1995.

[18] Vorlesungsmitschrift „Informatik und Gesellschaft", Prof. Völkel, Prof. Bär, Dr. Breier, Universität Greifswald, 2000.

8.3 Gesetzestexte

Alle hier aufgeführten Gesetze befinden sich auf dem zugehörigem Datenträger als PDF-Dateien.

- Informations- und Kommunikationsgesetz mit Signaturgesetz (SigG von 1997)
- Signaturverordnung (SigV von 1997)
- EU-Direktive zur digitalen Signatur (1999)
- Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (SigG 2000)