Digitale Signatur

1 Einleitung

Die offenen Netze des Internet erleichtern die weltweite interaktive Kommunikation zwischen Parteien, die vorher in keiner Beziehung zueinander standen. Um einen sicheren Dokumententransfer zu ermöglichen bedarf es der elektronischen Authentizität.

Es gibt verschiedene Methoden zur elektronischen Unterzeichnung von Dokumenten, angefangen von einfachen Methoden (z.B. eingescannte Unterschriften) bis hin zu sehr fortschrittlichen Methoden (z.B. digitale Signaturen auf der Basis kryptographischer Systeme). Da in den nächsten Jahren ein explosionsartiges Wachstum an virtuellen Kaufhäusern, Banken, Bibliotheken und Dienstleistungsunternehmen erwartet wird, werden immer mehr Kunden ihre geschäftlichen Beziehungen per Internet abwickeln. Sowohl Vertragsabschlüsse als auch Geldzahlungen sind auf elektronischem Wege möglich. Doch muss dieser Datenaustausch sicher und rechtsverbindlich sein. Dazu muss der Absender eines elektronischen Dokuments eindeutig zuzuordnen sein (Authentizitätsgebot) und es muss gewährleistet sein, dass der vermittelte Inhalt eines Dokuments nicht von außenstehenden Dritten verändert wurde (Integritätsgebot). Die digitale Signatur dient nicht nur der Beweiserleichterung, sondern auch dem sicheren Austausch elektronischer Willenserklärungen. Durch sie soll die Sicherheit des Rechtsverkehrs gewährleistet werden.

Das Verfahren der digitalen Signatur ist nicht zu verwechseln mit der Verschlüsselung eines Dokuments (z.B. durch Pretty Good Privacy; PGP). Auch ist die elektronisch versandte Nachricht durch das Verfahren der digitalen Signatur nicht geschützt. Um den Inhalt für unbefugte Dritte uneinsehbar zu mache, ist die Nachricht unabhängig von der Verwendung der digitalen Signatur zu verschlüsseln. Das Verschlüsselungsverfahren erfolgt ebenfalls durch ein asymmetrisches Verfahren, d.h. öffentliches und privates Schlüsselpaar. Die digitale Signatur zielt insbesondere auf die Rechtsverbindlichkeit im elektronischen Geschäftsverkehr ab.

Autor Dr. Uwe Altenschmidt
Datei Digitale Signatur.doc

LITTLE softwarehouse GmbH
Zentnerstr. 19, D-80789 München
www.littlesoft.com

Eine digitale Signatur im Sinne des Signaturgesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Signaturschlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt (§ 2 Abs. 1 SigG).Die digitale Signatur ist in Deutschland seit dem Inkrafttreten des Multimediagesetzes (IuKDG, Art. 3) am 1. August 1997 gesetzlich geregelt. Weltweit ist das deutsche Signaturgesetz das erste nationale Gesetz dieser Art. Nur in den Vereinigten Staaten von Amerika gab es vorher schon vereinzelte bundesstaatliche Signaturgesetze. Die ersten Angebote an gesetzeskonformen Dienstleistungen in Deutschland werden für das Jahr 1999 erwartet .

Zur Verdeutlichung sei erläutert, welche Arten von Bedrohungen es im Internet gibt.

1.) Die abgeschickte Nachricht wird auf dem Weg vom Absender zum Empfänger verändert.
2.) Die Nachricht wird auf dem weg vom Absender zum Empfänger abgehört.
3.) Der Absender verleugnet das Absenden der Nachricht. Hier gibt es zwei Varianten:
    a. Es wird behauptet, jemand hätte in seinem Namen eine Nachricht verschickt.
    b. Es wird bestritten, dass die Nachricht jemals von ihm abgeschickt wurde.

    Dann muss der Empfänger nachweisen, dass er wirklich eine Nachricht erhalten hat.
4.) Der Empfänger streitet ab, jemals die Nachricht erhalten zu haben.

Vertrauen in die Kommunikation und Sicherheit bei der Übertragung sind die Grundelemente für die Akzeptanz des electronic commerce. Die Technik der digitalen Signatur ist in der Lage, die notwendige Sicherheit zu garantieren.

Banken sind schon lange Vorreiter für die elektronische Kommunikation und, da es oft um viel Geld geht, auch der Sicherheitseinrichtungen. Um die Daten vor Manipulation zu schützen, müssen sie vor allem integritätsgesichert sein. Die betrifft insbesondere den Datenverkehr in den Beziehungen Kunde-Bank oder der Geldinstitute untereinander. Mit dem vom deutschen Kreditgewerbe verabschiedeten neuen Standard „Homebanking Computer Interface HBCI“ wird den Bankkunden

ein komfortables und sicheres Homebanking über offene Netze, insbesondere dem Internet, angeboten. Das HBCI benutzt als Sicherheitsfunktion die digitale Unterschrift, so dass das umständliche Hantieren mit der Transaktionsnummer TAN bald der Vergangenheit angehören kann.

Die digitale Signatur wird in den elektronischen Alltag einziehen und zur Selbstverständlichkeit werden, denn für eine sichere elektronische Kommunikation ist ein sicheres Unterschriftenverfahren unentbehrlich.

2 Wie funktioniert die digitale Signatur ?

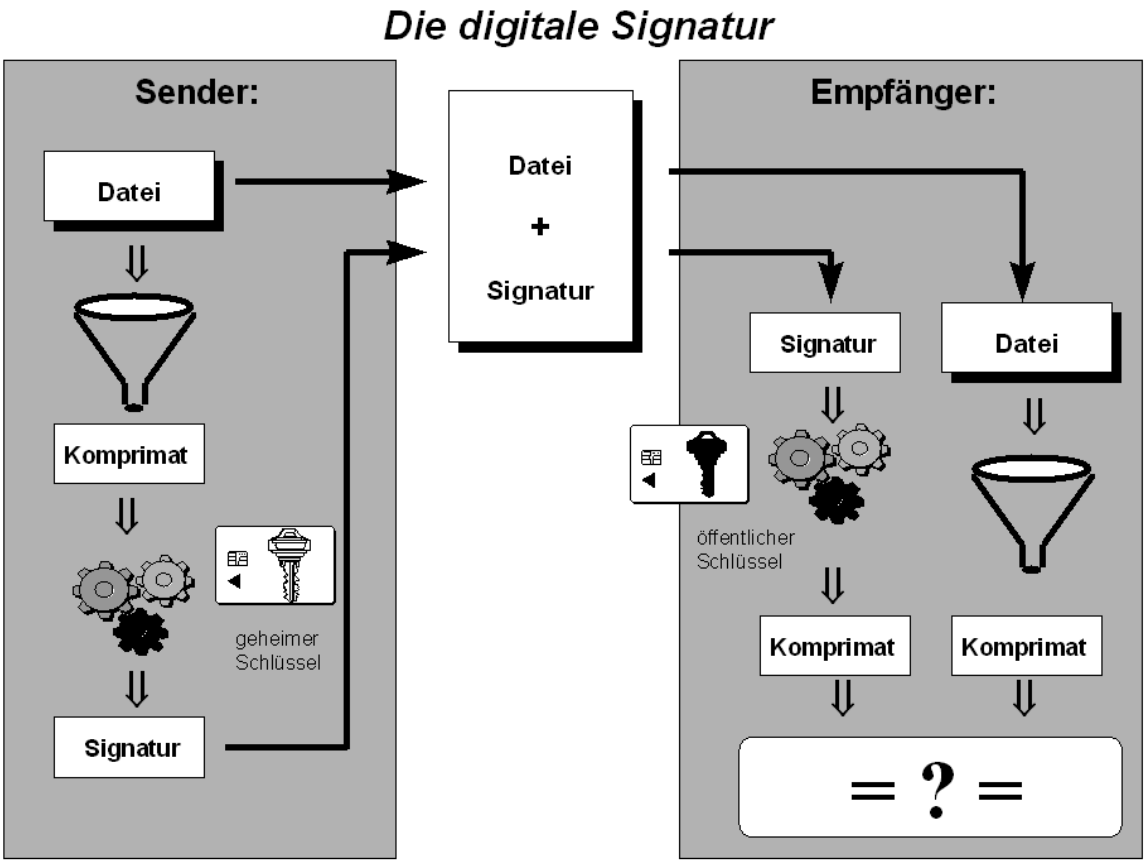

Abbildung 1 Prinzip der digitalen Signatur

Voraussetzung für die gesetzlich digitale Signatur wird ein asymmetrisches Verschlüsselungsverfahren mit bekannt gegebenen öffentlichem Schlüssel und einem dazugehörigen privaten Schlüssel. Ein Schlüssel kann beispielsweise aus 1024 Bit bestehen, was einer 300-stelligen Dezimalzahl entspricht. Die

Rücktransformation einer verschlüsselten Information ohne Kenntnis des Schlüssels ist daher sehr unwahrscheinlich.

Auf einer Chipkarte befinden sich neben dem vor Auslesen geschützten privaten Schlüssel zugleich die PIN und die gesamte manipulationsgeschützte Signatur-Software. Es wird ein PC mit einer Signaturkomponente und einem Chipkartenlesegerät benötigt. Nach Eingabe der Karte muss das zu signierende Dokument aufgerufen und mit einem Mausklick der Befehl „Signieren“ eingegeben werden. Soll ein Dokument signiert werden, wird durch die Signatur-Software ein Wert generiert, der das zu unterschreibende Dokument eindeutig repräsentiert. Dieser mathematische Algorithmus führt immer zu dem gleichen Ergebnis, solange der Inhalt des Dokuments nicht verändert wird. Diese Berechnung findet in der Chipkarte statt. Das bedeutet, der private Schlüssel verlässt niemals die Karte, ist also nicht über das Internet ermittelbar.

3 Vorteile der digitalen Signatur

- einfach zu leisten
- Text ist in die Signatur einbezogen
- Echtheit (Authentizität) des Absenders ist nachweisbar.
- Die Unterschriftenprüfung erfolgt rationell.
- Bei jedem neuen Text ergibt sich ein anderes Binärmuster der digitalen Signatur.
- Mit der digitalen Signatur können auch geistiges Eigentum und Urheberrechte signiert werden, z.B. digitalisierte Bilder, Töne, Software.

4 Prüfung der digitalen Signatur

Will der Empfänger einer Nachricht prüfen, ob die Nachricht unverändert bei ihm angekommen ist, so kann er dies tun, indem er die angekommene Signatur durch seinen PC prüfen lässt. Durch ein technisches Verfahren wird das abgeschickte Dokument mit dem angekommenen verglichen. Ist die Prüfsumme gleich, so kann der Empfänger sicher sein, dass die Daten nicht verändert wurden.

Weiterhin kann der Empfänger einer Nachricht die Gültigkeit der digitalen Signatur überprüfen. Dies geschieht, in dem er online in das Verzeichnis der noch gültigen Zertifikate hineingeht. Ist die digitale Signatur noch gültig, so wird ihm eine Bestätigung erteilt, ist die digitale Signatur ungültig, ist sie in die Sperrliste überführt worden. Gründe für eine Sperrung können z.B. sein: Diebstahl, Verlust der Karte, austritt aus der Firma oder Ende der Gültigkeit.

5 Was braucht der Anwender zur Nutzung des digitalen Schlüssels ?

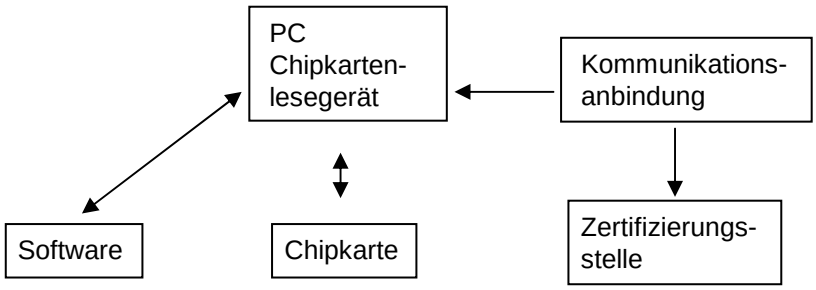

Abbildung 2 Infrastruktur des Anwenders

Damit ein Anwender die Signatur nutzen kann, benötigt er nach der deutschen Sichtweise:

a. einen PC mit Chipkartenleser
b. eine Chipkarte mit einem Signaturschlüssel
c. Sicherheitsmodule für den PC
d. Geeignete Software mit Signaturfunktion

Die Software muss in der Lage sein, zu gewährleisten, dass keine Signaturen ohne den Willen des Anwenders erzeugt werden.

Bevor ein Dokument signiert wird, muss der Anwender seine PIN-Nummer eingeben und somit aktiv die Signatur erzeugen.

6 Wo bekommt der Anwender die Chipkarte ?

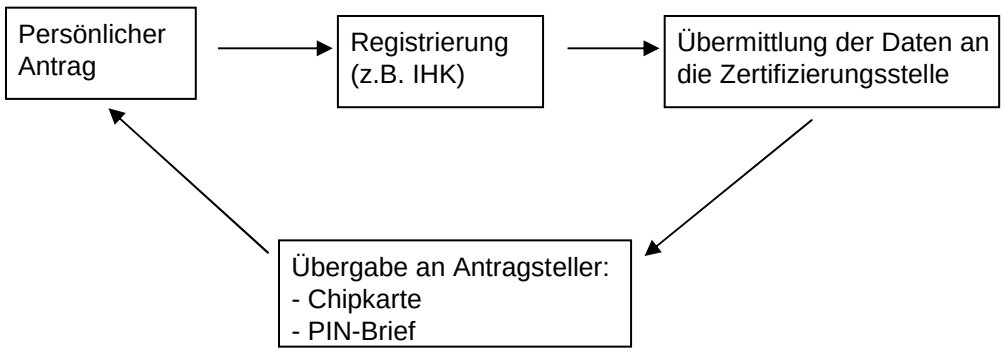

Abbildung 3 Zertifikatserstellung

Die Chipkarte mit dem geheimen Signaturschlüssel erhält der Anwender bei einer Zertifizierungsstelle für digitale Signaturen. Die Zertifizierungsstellen bestehen aus einer technischen Einheit (trust center) und einer Registrierungsstelle. Bei den Registrierungsstellen können die digitalen Signaturzertifikate beantragt werden.

Praktisch sieht das Verfahren folgendermaßen aus:

a.) Antragsteller erscheint persönlich bei der Registrierungsstelle.

b.) Antragsteller wird informiert.
c.) Erfassen der persönlichen Daten des Antragstellers.
d.) Antrag auf digitale Signatur wird „händisch“ unterschrieben.
e.) Übermittlung der Daten an die Zertifizierungsstelle und Erzeugen eines Signaturschlüssels, der auf einer Chipkarte geladen wird.
f.) Chipkarte und PIN-Brief werden dem Antragsteller zugestellt.

7 Behördlich genehmigte Zertifizierungsstellen

Die Zertifizierungsstellen verwalten die Daten einer Person, die auf einer Chipkarte gespeichert sind und bestätigen durch Zertifikate, dass die Daten zu einer bestimmten Person gehören.

Um eine Lizenz als Zertifizierungsstelle zu erhalten, muss der Antragsteller der Regulierungsbehörde gegenüber nachweisen, dass sowohl der Antragsteller als auch sein Personal die notwendige Zuverlässigkeit besitzen. Die Rechtsgrundlage ist das Signaturgesetz (Artikel 3, IuKDG, 1.8.1997).

Die Zertifizierungsstelle hat den Antragsteller über erforderliche Maßnahmen zur Gewährleistung der Sicherheit der digitalen Signatur zu unterrichten.

Sicherheitskonzept:

- Sicherheitsmaßnahmen
- Übersicht der technischen Komponenten
- Darstellung der Ablauforganisation der Zertifizierungstätigkeit.

Die Regulierungsbehörde führt einen Katalog von geeigneten Sicherheitsmaßnahmen, den sie im Bundesanzeiger veröffentlicht. Dieser Katalog ist bei der Erstellung des Sicherheitskonzepts zu berücksichtigen.

Der Inhaber eines Zertifikats muss den geheimen Schlüssel mit angemessener Sorgfallspflicht aufbewahren und geheim halten. In der Praxis werden geheime Schlüssel meist auf Chipkarten gespeichert.

Eine Zertifizierungsstelle „bürgt“ mit ihrem Namen für die richtige Verwaltung und Pflege aller Daten.

8 Aufgaben der Zertifizierungsstelle

Neben der Schlüsselerzeugung und -verwaltung hat die Zertifizierungsstelle noch weitere Aufgaben.

a.) Öffentliches Zertifikatsverzeichnis: Hierbei handelt es sich um eine Art „gelber Seiten“, in denen alle von einer

Zertifizierungsstelle ausgestellten Zertifikate aufgeführt sind. Dabei ist zu unterscheiden zwischen Verzeichnissen, bei denen nur eine Gültigkeitsabfrage möglich ist und Verzeichnissen, bei denen die Zertifikate abrufbar sind.

b.) Sperrlisten-Management: Geht eine Chipkarte verloren, so muss der Inhaber des Zertifikats dies unverzüglich der Zertifizierungsstelle mitteilen. Es wird daraufhin eine Sperrung vorgenommen.

c.) Zeitstempeldienste: Ein Zeitstempel ist eine elektronische Bescheinigung mit digitaler Signatur einer Zertifizierungsstelle darüber, dass ihr bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Durch einen Zeitstempel kann der Zeitpunkt des Versands des Dokuments nicht vor- oder rückdatiert werden.

9 Internationale Entwicklungen

Am 13.5.1998 hat die Europäische Kommission einen Entwurf für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen herausgegeben.

Die gegenseitige Anerkennung der digitalen Signaturen in den einzelnen europäischen Nationen ist der Dreh- und Angelpunkt im internationalen Kontext. Ziel muss es sein, ein ausländisches Zertifikat so anzuerkennen als ob es in Deutschland hergestellt wäre. Grundlage ist die Einheitlichkeit von Sicherheitstechniken.

10 Wann werden die ersten digitalen Signaturen in Deutschland erhältlich sein ?

Der Aufbau nach dem Signaturgesetz ist in Deutschland sehr kostspielig und die technischen Anforderungen nicht leicht umzusetzen. Nur wenige Unternehmen haben in Deutschland die dafür notwendigen Investitionen vorgenommen. Daraus leitet sich ein Trend ab: Es wird wenige Zertifizierungsstellen geben aber eine ausreichende Zahl von Registrierungsstellen, die sich der Technik der Zertifizierungsstellen bedienen.

Ab 1999 soll es die ersten digitalen Signaturen nach dem Signaturgesetz geben.

11 Rechtswirkung der digitalen Signatur bei Verträgen

Da die digitale Signatur nicht mit der eigenhändigen Unterschrift gleichzusetzen ist, stellt sich das Problem des Schriftformerfordernisses bei Verträgen.

Bei Kaufverträgen über Waren und Dienstleistungen ist Schriftform nicht gesetzlich gefordert. Grundsätzlich gilt für alle rechtsgeschäftlichen Verträge Formfreiheit. Ausnahmen sind Grundstückskaufverträge oder Bürgschaften.

Wenn das Gesetz Schriftform voraussetzt (§ 126 BGB), bedarf es für die Gültigkeit des Rechtsgeschäfts einer Urkunde, die vom Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigtem Handzeichen zu unterzeichnen ist.

Die eigenhändige Unterschrift ist bei der Nutzung elektronischer Kommunikationswege nicht möglich. Auch die eingescannte Unterschrift erfüllt nicht die gesetzlichen Voraussetzungen einer eigenhändigen Unterschrift.

12 Beweiskraft elektronischer Dokumente

Es stellt sich die Frage, ob eine elektronisch abgegebene Willenserklärung, die mit einer digitalen Signatur versehen ist, als Urkunde zu qualifizieren und somit als besonderes

Beweismittel vor Gericht anzusehen ist (§416 ZPO). Die Zivilprozessordnung setzt dafür die eigenhändige Unterschrift voraus.

Da eine eigenhändige Unterschrift bei der Nutzung der elektronischen Kommunikationswege nicht möglich ist, erhält die digitale Signatur keine Urkundenqualität. Damit erlangt eine elektronisch abgegebene Erklärung nicht diese Beweiskraft. Das führt zu dem großen Problem für einen Verkäufer, der im streitigen Fall die Beweiskraft für das Zustandekommen und damit Vorliegen eines Vertrags trägt.

Davon unabhängig ist allerdings die „Rechtsgültigkeit“ elektronisch abgegebener Willenserklärungen. Denn nach deutschem Recht ist jede Willenserklärung – unabhängig davon, in welcher Form sie abgegeben wurde – grundsätzlich „rechtsgültig“.

Damit erfährt ein elektronisch abgegebenes Dokument nicht die Beweiskraft von schriftlichen Urkunden, ist aber rechtsgültig.

13 Beweiskraft digitaler Signaturen

Eine wichtige Regelung im Signaturgesetz ist die Vermutung der Fälschungssicherheit digitaler Signaturen und signierter Daten (§

1 Abs. 1 SigG). Somit kann der Empfänger einer mit einer digitalen Signatur versehenen elektronisch abgegebenen Erklärung nachweisen, dass eine bestimmte Nachricht von einem bestimmten Absender stammt. Zusätzlich kann belegt werden, dass der Inhalt nicht verändert wurde.

Dennoch hat ein nach dem Signaturgesetz signiertes Dokument keine Beweiskraft im Sinne einer Urkunde, bekommt aber durch die gesetzliche Annahme, sie sei sicher, einen hohen Beweiswert.

Zur Zeit wird durch die Bundesregierung geprüft, ob das Schriftformerfordernis des § 126 BGB ergänzt oder geändert werden soll.

Quellen:

1. Digitale Signatur, DIHT, 1998
2. Digitale Signatur, www.TeleTrusT.de
3. K. Fuhrberg: Internet-Sicherheit, Hanser, 1998