Mit dem Computer unterschreiben

Das Signaturgesetz stellt hohe Sicherheitsanforderungen an die elektronische Signatur in Deutschland. Elektronisch unterschriebene Dokumente haben nun gleiche Rechtskraft wie eine Urkunde auf Papier.

von Jürgen Brenn

Die Spielregeln sind festgelegt. Die technischen Mittel stehen bereit. Theoretisch ist Deutschland seit Mitte vergangenen Jahres im Zeitalter der „virtuellen Urkunde“ angekommen. Am 22. Mai 2001 trat des „Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“, kurz Signaturgesetz, in Kraft. Die „Verordnung zur elektronischen Signatur“ sowie das dazugehörige „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr“ flankieren das neue Regelwerk.

Rechtsverbindliche Unterschrift

Die Grundlage für das deutsche Signaturgesetz bildet eine EG-Richtlinie von Anfang 2000. Bundeswirtschaftminister Dr. Werner Müller sagte nach der Verabschiedung der Signaturverordnung Ende Oktober 2001: „Mit der neuen Verordnung, dem Signaturgesetz und den Formanpassungsvorschriften bekommen wir in Deutschland einen verlässlichen Rechtsrahmen für eine breite Anwendung elektronischer Signaturen in Wirtschaft, Verwaltung und für die Verbraucherinnen und Verbraucher im täglichen Rechts- und Geschäftsverkehr.“

Mit Hilfe der digitalen Signatur können Daten mit einer rechtsverbindlichen Unterschrift via Internet versandt werden. Gleichzeitig sind die meisten Systeme mit Verschlüsselungsprogrammen ausgerüstet, die besonders hohen sicherheitstechnischen Anforderungen bei der Übermittlung von zum Beispiel Patientendaten genügen sollen.

Das Signaturgesetz hebt die digitale Signatur auf die gleiche rechtliche Stufe wie die handschriftliche Unterschrift unter einem Dokument. Mit einer Unterschrift erlangt ein Stück Papier Beweiskraft und wird zur Urkunde. Damit können in der „analogen“ Welt rechtsgültige Verträge geschlossen werden. Dies geht nun auch in der „virtuellen“ Welt, wobei hier sowohl die verwendeten Begriffe als auch die technischen Verfahren für erhebliche Verunsicherung unter den Verbrauchern und Internetnutzern sorgen.

Drei Arten der Signatur

Das Signaturgesetz unterscheidet zwischen drei Arten der elektronischen Signatur, die verschiedenen Sicherheitsanforderungen genügen:

1. einfache elektronische Signatur,
2. fortgeschrittene elektronische Signatur und
3. qualifizierte elektronische Signatur.

Die beiden ersten Formen werden vom Signaturgesetz nicht berührt und sind weiterhin unreguliert. Unter der „einfachen elektronischen Signatur“ versteht der Gesetzgeber Authentifizierungsverfahren, wie sie im Internet weit verbreitet sind, zum Beispiel das „Pretty Good Privacy-Verfahren“ (PGP). Aber auch die eigenhändige, gescannte und in ein Schriftstück hineinkopierte Unterschrift ist eine einfache elektronische Signatur. Zu dem Bereich gehören auch biometrische Verfahren, wie etwa Iris- oder Gesichtserkennungs-Verfahren, wenn nicht überprüfbar ist, wem die Daten zugeordnet sind.

Eine „fortgeschrittene elektronische Signatur“ wird mit Authentifizierungs-Verfahren erzeugt, die dem Signaturschlüssel-Inhaber eindeutig zugeordnet werden können und seine Identifizierung ermöglichen. Ebenfalls muss der Schlüssel unter der alleinigen Kontrolle des Inhabers sein. Daneben müssen die Verfahren eine nachträgliche Veränderung des Dokumenteninhalts anzeigen, so dass der Empfänger der Daten erkennen kann, von wem diese signiert wurden und ob diese nach der „Unterschrift“ quasi unterwegs verändert worden sind.

Verschiedene Verfahren möglich

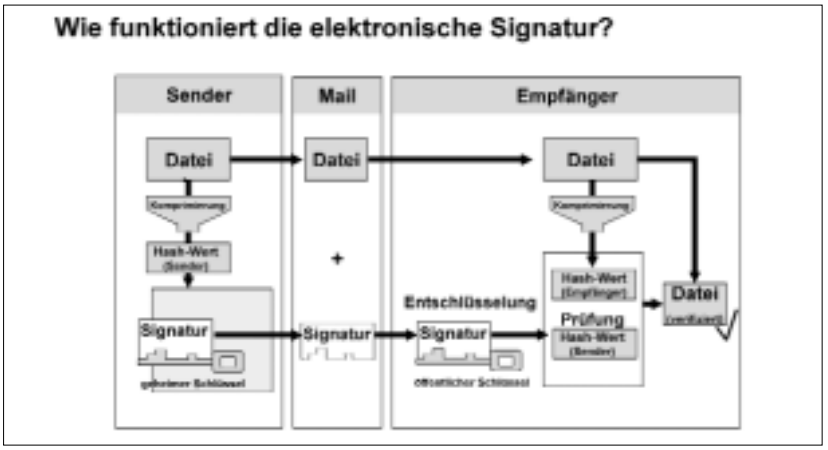
Um eine fortgeschrittene elektronische Signatur zu erstellen, können ebenfalls biometrische Verfahren eingesetzt werden, wobei auch die Identität des Absenders überprüfbar und erkennbar sein muss. Hier können auch Passwort-Verfahren mit entsprechenden Zusatzfunktionen oder Signatur- bzw. Chipkarten zum Einsatz kommen. Die fortgeschrittene elektronische Signatur hat zwar vor Gericht Beweiskraft, allerdings muss der Beweiswert im Einzelfall per Gutachten ermittelt werden, gibt die aufsichtführende Behörde, die Bonner „Regulierungsbehörde für Telekommunikation und Post“ (RegTP) zu bedenken.

Die höchste Sicherheitsstufe hat die „qualifizierte elektronische Signatur“, auf die sich das Signaturgesetz vornehmlich konzentriert. Die qualifizierte Signatur muss die Voraussetzungen der fortgeschrittenen elektronischen Signatur erfüllen, darüber hinaus auf einem zum Zeitpunkt der Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt werden.

Bei diesem Verfahren kommen normalerweise Chipkarten zum Einsatz, die von sogenannten Trust-

centern ausgegeben werden. Der Inhaber der Karte muss sich bei dem Trustcenter registrieren lassen und bei Erhalt der Karte durch seinen Personalausweis oder Reisepass ausweisen. Die Trustcenter stellen das Zertifikat auch aus.

Das deutsche Signaturgesetz hat bei der qualifizierten elektronischen Signatur eine weitere Abstufung eingebaut, die sich auf die Trustcenter bezieht. So ist der Betrieb eines Zertifizierungsdienstes im Rahmen der Gesetze genehmigungsfrei. Der Betrieb muss lediglich bei der RegTP angezeigt werden. Die Trustcenter können Karten für die qualifizierte elektronische Signatur ausgeben. Daneben können sich die Trustcenter oder Zertifizierungsdienste auch bei der RegTP akkreditieren lassen. Das heißt, der Dienstanbieter weist der zuständigen Behörde seine technische und administrative Sicherheit nach, erhält im Gegenzug ein offizielles Gütesiegel und kann sich „akkreditierter Zertifizierungsdiensteanbieter“ nennen. Solche Trustcenter (zum Beispiel Datev, Telekom oder Post) vergeben die Signaturkomponenten für die „akkreditierte qualifizierte Signatur“. Nach Einschätzung der RegTP wird sich diese Form der qualifizierten Signatur in Deutschland durchsetzen.



Schematische Darstellung der qualifizierten elektronischen Signatur. Quelle: Deutsche Post World Net.

Einfache Handhabung

Für den Benutzer ist die Handhabung einfach. Um ein Dokument zu signieren, drückt der Anwender in der Software den entsprechenden Knopf und schiebt seine Signaturkarte in das externe Lesegerät, das mit dem Computer verbunden ist. Gegebenenfalls muss der Anwender seine persönliche Signaturkarte aktivieren, indem er eine Geheimnummer (PIN) eingibt oder sich über biometrische Merkmale als Karteninhaber ausweist. Den Rest übernimmt der Computer.

Der Empfänger eines signierten Dokumentes überlässt alles seinem Rechner, der die Entschlüsselung und Überprüfung des verwendeten Schlüssels und Zertifikats und damit die Überprüfung der Identität des Absenders übernimmt. Nur wenn das Dokument nach der Signatur nicht verändert worden ist, wird es auf dem Bildschirm angezeigt.

Technisch steckt hinter dem Vorgang eine komplexe Mischung aus Kryptografie und Verrechungsverfahren, die in mehrere Stufen eingeteilt werden kann *(siehe Schaubild)*. Die elektronische Signatur beruht auf dem Prinzip des asymmetrischen Verschlüsselungsverfahren, bei dem zwei Schlüssel eingesetzt werden, (private key/public key).

Bei der Signaturbildung wird ein anderer Schlüssel verwendet als bei der Signaturüberprüfung. Der Absender verwendet zum Signieren seinen privaten, nur ihm allein zugänglichen Schlüssel, der sich auf der Signaturkarte befindet. Der Empfänger entschlüsselt mit dem öffentlich zugänglichen Schlüssel, dem public key (Prüfschlüssel, Verifizierschlüssel) die Nachricht und überprüft beim Trustcenter, ob der gebrauchte private key und der Benutzer registriert sind und ob ein gültiges Zertifikat vorliegt.

Gegebenenfalls werden weitere Attribute wie zum Beispiel „Arzt“ angezeigt, wenn sich der Absender diese hat zertifizieren lassen. Bei der Erzeugung der Schlüssel werden Algorithmen verwendet, die „sicher“, das heißt, nach dem Stand der Technik nicht zu brechen sind. Bei dem RSA-Verfahren werden Schlüssel mit einer Länge von zur Zeit 1024 Bit erzeugt. Das entspricht etwa einer 300-stelligen Zahl. So entstehen jeweils einmalige Schlüsselpaare. Der Trustcenter muss zusätzlich überprüfen, ob in seinem Verzeichnis jeder Schlüssel nur einmal vorkommt.

Digitaler Fingerabdruck

Bei der eigentlichen Erstellung der Signatur kommt ein weiterer kryptografischer Mechanismus zum Einsatz, die sogenannte Hash-Funktion (zu deutsch: „Zerhacktes“). Vor dem Signieren wird das Dokument auf den Hash-Wert reduziert. Das Dokument bekommt einen digitalen Fingerabdruck. Allein der Hash-Wert wird signiert, das heißt, mit Hilfe des Algorithmus des private key codiert. Die elektronische Signatur ist fertig und wird an das Originaldokument angehängt. Dadurch kann Rechen-, Übertragungszeit und Speicherplatz gespart werden. Die Hash-Funktion muss dabei zwei Eigenschaften aufweisen: Erstens sollte es unmöglich sein, zwei Dokumente zu finden, die dasselbe Hash-Ergebnis haben. Zweitens sollte unmöglich sein, aus einem Hash-Ergebnis das ursprünglich Dokument wieder herzustellen (Einwegfunktion).

Der Empfänger eines elektronisch signierten Dokumentes benutzt den public key, um den Hash-Wert zu decodieren. Um festzustellen, ob das signierte Dokument nachträglich verändert wurde, errechnet der Empfangscomputer aus dem Originaldokument wiederum den Hash-Wert und vergleicht die-

sen mit dem nun decodierten Wert. Sind diese identisch, ist die elektronische Signatur authentisch und das Dokument nicht verändert worden. Denn bereits ein hinzugefügtes Leerzeichen würde einen anderen Hash-Wert ergeben.

Nun muss noch überprüft werden, ob der mitgesandte öffentliche Schlüssel tatsächlich dem Absender zuzuordnen ist. Dazu erfolgt eine Abfrage bei dem Trustcenter, der dem Absender den privaten Schlüssel zur Verfügung gestellt und das Signaturschlüssel-Zertifikat ausgestellt hat. Die Zertifikate sind elektronische Bescheinigungen, mit denen Signaturprüfschlüssel (public key) einer Person zugeordnet werden und die Identität dieser Person bestätigen. Die Zertifizierungsstelle übernimmt also eine Garantiefunktion für authentische Signaturschlüssel-Zertifikate und deren Integrität.

Signatur schützt nicht vor Zugriff Dritter

Grundsätzlich muss sich der Anwender einer digitalen Signatur darüber im Klaren sein, dass diese das elektronisch „unterschriebene" Dokument „nicht vor unbefugter oder unerwünschter Kenntnisnahme Dritter" schützt, wie die RegTP in einer Broschüre zum Thema feststellt. Die digitale Signatur schützt also nicht die Vertraulichkeit des Inhalts, genauso wenig wie dies eine eigenhändige Unterschrift vermag. Allerdings sieht zum Beispiel die angebotene Anwendung der Post Signtrust GmbH die Möglichkeit vor, vertrauliche Dokumente zusätzlich zu verschlüsseln, erklärte Post-Sprecherin Ina Quilling dem *Rheinischen Ärzteblatt*.

Auf ein weiteres Sicherheitsmanko macht Dr. nat. Adrian Spalka vom Institut für Informatik III der Universität Bonn aufmerksam. Trojanische Pferde, eine besondere Art von Computer-Viren, können bereits vor dem Signieren das Dokument verändern. Der Benutzer versendet dann ein bereits auf seinem Rechner verfälschtes Dokument, ohne dies zu bemerken. Das Problem sei von den Produkteanbietern erkannt worden und an Lösungen werde gearbeitet, sagt Spalka.

Ein weiteres Unsicherheitspotential ist die Eingabe der PIN über die Computertastatur, mit der sich der „Unterzeichner" gegenüber seiner Signaturkarte identifiziert. Viren auf dem Computer könnten die PIN mitlesen und damit Unbefugten bekannt werden. Um dieses Problem zu umgehen, werden Kartenlesegeräte zunehmend mit Eingabefeldern ausgerüstet, sodass die Identifikation außerhalb des Computers geschieht.

Die RegTP hat zu den Schwierigkeiten einen Sicherheitshinweis veröffentlicht. Die Behörde empfiehlt, dass „Anwenderkomponenten, welche zum Beispiel zur Erzeugung bzw. Verifikation qualifizierter elektronischer Signaturen eingesetzt werden, nur auf vertrauenswürdigen IT-Systemen betrieben werden sollten".

Mit dem „Beschluss zur Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung" legte das Bundeskabinett Anfang des Jahres den Grundstein für den rechtsverbindlichen elektronischen Austausch von Daten innerhalb der Bundesverwaltung und auch mit den Bürgern.

Praktische Anwendung

Für die Ärzteschaft beschäftigt sich seit 1996 der gemeinsame Lenkungsausschuss „Elektronischer Arztausweis" der Bundesärztekammer und Kassenärztlichen Bundesvereinigung mit dem Thema. Der Elektronische Arztausweis soll die Funktion des Sichtausweises haben, als Codierschlüssel für vertrauliche Dokumente und als elektronische Signaturkarte dienen. Nach einem Beschluss des Vorstandes der Bundesärztekammer soll der Elektronische Arztausweis den Anforderungen des Signaturgesetzes entsprechen, damit eine notwendige rechtliche Sicherheit in der Anwendung der elektronischen Unterschrift mit Hilfe des Elektronischen Arztausweises gewährleistet ist.

Die 1999 vorgestellten Spezifikationen für die „Health Professional Card" (HPC) sollen an das neue Signaturgesetz angepasst werden, sagte Jörg-Erich Speth, der die Geschäfte des Ausschusses leitet und Hauptgeschäftsführer der Ärztekammer Westfalen-Lippe ist, dem *Rheinischen Ärzteblatt*. Die HPC soll sich in Punkto Sicherheit an die Anforderungen anlehnen, die die Bundesbehörden bei ihren Projekten vorgeben. Zahlreiche Entwicklungen in der Telematik beziehen die HPC in ihre Konzepte mit ein. Auf dem Kongress „eHealth 2002 – Telematik im Gesundheitswesen" diskutierten kürzlich in Bonn die Teilnehmer entsprechende Pläne.

Ausblick

Bisher sind zwar die rechtlichen Grundlagen geschaffen worden und auch die Hardware-Produkte stehen bereit, allerdings fehlen noch die konkreten Anwendungen für die elektronische Signatur. Die Trustcenter arbeiten derzeit an Software-Anwendungen, die den Einsatz der elektronischen Signatur implementieren. So erstellt der Post Signtrust Softwarelösungen für die Bereiche E-Commerce und E-Goverment und ist eine Partnerschaft mit Microsoft eingegangen, um hier die elektronische Signatur zu implementieren.

Da sich in Deutschland alle größeren Trustcenter auf einen gemeinsamen Standard geeinigt haben, werden die elektronischen Signaturen zukünftig untereinander kompatibel sein, so Ina Quilling von Post Signtrust. Auch werde europaweit sowie global versucht, Kompatibilität herzustellen. Bis sich allerdings spezielle Anwendungen und sich damit auch die elektronische Signatur durchsetzen, werden voraussichtlich noch einige Jahre vergehen. „Wir gehen davon aus, dass der Durchbruch zwischen 2003 und spätestens 2005 kommt", sagt Quilling. Dann wird die Benutzung der elektronischen Signatur so selbstverständlich sein, wie heute bereits die E-Mail.

Internetadresse zum Thema

www.bsi.bund.de/esig/index.htm
www.regtp.de
www.teletrust.de
www.signtrust.de/
www.telekom.de/dtag/t-telesec/index