



Die elektronische Signatur

Mit dem fortschreitenden „Siegeszug“ des Internets wachsen auch die Möglichkeiten des „electronic commerce“ täglich. Die technischen Voraussetzungen für derartige „online“-Geschäfte bestehen schon lange. Trotzdem gibt es noch immer viele Vorbehalte gegen die Geschäfte im Internet. Schließlich gehören E-Mails zu der unsichersten Form der elektronischen Kommunikation. Sie müssen auf ihrem Weg durch das weltweite Internet viele Stationen passieren, an denen man sie abfangen, mitleesen oder auch verändern kann. Außerdem lassen sie sich auch in Bezug auf den angezeigten Absender leicht manipulieren. Verständlich, dass diese Risiken einen verlässlichen Geschäftsverkehr verhindern und auch Behörden und andere öffentliche Einrichtungen bislang überwiegend auf elektronisch übermittelte Formulare verzichtet haben.

Es gibt aber Möglichkeiten, wie man sich mit einfachen Mitteln vor solchen Risiken schützen kann. Um E-Mails vertraulich zu machen, gibt es den Weg der Verschlüsselung. Und mit Hilfe der Digitalen Signatur können Sie sicherstellen, dass der Empfänger die Person des Absenders und die Unverfälschtheit des Inhalts einer E-Mail nachprüfen kann. Experten sind sich einig, dass die elektronische Unterschrift sicherer ist, als die eigenhändige Unterschrift auf einem Schriftstück.

Was ist eine „elektronische Signatur“ und wie funktioniert sie?

Eine „elektronische Signatur“ im Sinne des Gesetzes (§ 2 Abs. 1 Signaturgesetz) ist ein digitales Siegel, beziehungsweise eine willkürlich anmutende Zahlen- und Buchstabenkette, und wird einem elektronischen Dokument, entsprechend einer handschriftlichen Unterschrift, angehängt. Hergestellt wird dieses Siegel unter Einsatz mathematischer Verfahren mit Hilfe eines sogenannten (privaten) „Signaturprüfschlüssels“. Dieser errechnet aus dem Text und dem Format der zu unterschreibenden Nachricht die genannte Zahlen- und Buchstabenkette, den sogenannten Hash-Wert. Der Empfänger der elektronisch übermittelten Daten kann nun seinerseits mittels eines dazugehörigen (öffentlichen) „Signaturprüfschlüssels“ und eines entsprechenden „Zertifikates“ die Echtheit und den Urheber der Signatur jederzeit überprüfen und die Unverfälschtheit der Daten feststellen. Mit Hilfe des „Signaturprüfschlüssels“ wird erneut der Hash-Wert der Nachricht ermittelt. Stimmt er mit der Signatur überein, ist die Unverfälschtheit der Nachricht nachgewiesen.

Zertifizierungsdiensteanbieter gewährleisten, dass jede elektronische Signatur nur einem Teilnehmer zugeteilt wird. Das private Siegel kann also nur von einer einzelnen Person verwendet werden (vergleichbar einer EC-Karte mit der dazugehörigen PIN). So wird die Überprüfbarkeit des Absenders gewährleistet.

Verschlüsselt, also unlesbar gemacht, wird die E-Mail durch das Signaturverfahren nicht! Hierzu bedürfte es eines gesonderten Verschlüsselungsverfahrens.

Welcher Voraussetzungen bedarf das elektronische Signaturverfahren?

„Schlüssel“, „Zertifikate“

Um ein Dokument elektronisch unterschreiben zu können, benötigt der Anwender zunächst ein persönliches Schlüsselpaar, also zwei aufeinander abgestimmte Algorithmen. Dieses Schlüsselpaar besteht aus dem (privaten) Signaturschlüssel, der nur dem Besitzer zugänglich ist, und einem dazugehörigen (öffentlichen) Signaturprüfschlüssel. Beide Schlüssel erhält der Anwender auf Antrag und gegen Vorlage seines Personalausweises oder Reisepasses nach Abschluss eines entsprechenden Servicevertrages von einem Zertifizierungsdiensteanbieter in Form einer Chipkarte. Auf dieser befinden

den sich neben den genannten Schlüsseln und der Personenidentitätsnummer (PIN) des Anwenders auch das sogenannte „Zertifikat“. Hierbei handelt es sich gem. § 2 Nr. 6 Signaturgesetz um eine (elektronische) Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person. Juristischen Personen werden hingegen keine Chipkarten erteilt. Vielmehr müssen sich diese durch natürliche Personen vertreten lassen. Die Vertretungsmacht kann dann entweder im Signaturschlüssel-Zertifikat selbst oder in einem sogenannte „Attribut-Zertifikat“ (vergleiche § 5 Abs. 2 Signaturgesetz) ausgewiesen werden.

Hardware, Software

Neben den genannten Schlüsseln und Zertifikaten benötigt der Anwender einen PC mit einer geeigneten Benutzeroberfläche, ein Chipkartenlesegerät sowie die entsprechende Software. Diese kann er entweder bei einem Soft-/ Hardwarehersteller oder evtl. direkt „im Paket“ bei der Zertifizierungsstelle erhalten. Die Kosten für das Lesegerät und die entsprechende Software sind mit ca. 100,00 bis 200,00 Euro zu veranschlagen. Wirksam einsetzen kann der Anwender die elektronische Signatur allerdings nur dann, wenn auch der Empfänger des digitalen Dokumentes über die entsprechende Hard- und Software verfügt (siehe unten).

Wie läuft ein Geschäftsabschluss im „Signaturverfahren“ ab?

Soweit die genannten Voraussetzungen erfüllt sind, vollzieht sich der Abschluss eines „online“-Geschäftes im Signaturverfahren im Prinzip sehr einfach. Nach Erstellung des zu unterschreibenden Dokumentes gibt der Anwender die Chipkarte in das Lesegerät ein und klickt mit der Maus den Befehl „Signieren“ an (den Befehl bietet die erforderliche Software). Danach sendet er das signierte Dokument an den bestimmungsgemäßen Empfänger. Dieser kann dann an Hand des mitübertragenen Signaturprüfchlüssels in Verbindung mit dem ebenfalls mitgesandten Signaturschlüssel-Zertifikat oder an Hand eines öffentlichen Zertifikat-Verzeichnisses das Dokument auf Echtheit und Unverfälschtheit hin überprüfen.

Welchen Formerfordernissen genügt die elektronische Signatur?

Auf Grund der Entwicklungen im Informations- und Kommunikationstechnologiebereich hat der Gesetzgeber in einem neuen § 126 Abs. 3 Bundesgesetzbuch die elektronische Form neben der Textform als Option zur Schriftform eingeführt, wobei mit der elektronischen Form die elektronischen Signaturen gemäß § 126a Bundesgesetzbuch und dem Signaturgesetz gemeint sind. Auch neben der freiwillig vereinbarten Schriftform wird die elektronische Form in Zukunft ihre Anwendung finden können.

Sicherheit?

Nach Einschätzung von Experten ist es mit der zurzeit verfügbaren Technik praktisch unmöglich, die Verschlüsselung zu knacken. Inwieweit ein solcher Missbrauch durch Dritte auch für die Zukunft ausgeschlossen werden kann, ist auf Grund der Rasanzen technologischer Entwicklungen jedoch fraglich. Risiken birgt des Weiteren der gleichzeitige Verlust von Chipkarte und PIN-Nummer. Insoweit gilt es, die gleichen Verhaltensregeln wie für Scheck- beziehungsweise 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. Darüber hinaus sollte der Anwender sich vor jedem Signiervorgang vergewissern, ob das auf dem Bildschirm dargestellte Dokument identisch ist mit dem Datensatz, den er tatsächlich signieren will. Da nicht alle herkömmlichen PCs die hierfür erforderliche Gewährleistung bieten, sollte sich der Anwender hierüber

bei seinem Hardwarehersteller vorab informieren und gegebenenfalls zusätzliche Sicherheitsmodule in den Computer einbauen lassen.

Wer kann von der „elektronischen Signatur“ profitieren?

Diese Frage ist schnell zu beantworten: Im Prinzip jeder. Das heißt, nicht nur die sogenannten „global players“, sondern auch kleine und mittelständische Unternehmen, Privatleute, staatliche Einrichtungen, Verwaltungen und so weiter. Der wesentliche Vorteil liegt hierbei darin, dass einem elektronisch signierten Dokument ein vor Gericht verwertbarer Beweiswert zukommt. Während der bisher mögliche electronic commerce auf Grund der bestehenden Manipulationsmöglichkeiten stets ein Vabanquespiel war und daher nur ein Schattendasein führte, bietet das Signaturverfahren die Möglichkeit, Rechtsgeschäfte in einer verbindlichen Form und ohne Angst vor Manipulation, sei es durch den Geschäftspartner, sei es durch Dritte, via Internet abzuwickeln. Sollte es zwischen den Vertragspartnern dann doch zu Meinungsverschiedenheiten über den Inhalt des Geschäftsabschlusses kommen, stellen die digital signierten Dokumente verwertbare und aussagekräftige Beweismittel vor Gericht dar.

Hinweis: Dieses Merkblatt soll - als Service Ihrer IHK Köln - nur erste Hinweise geben und erhebt keinen Anspruch auf Vollständigkeit. Obwohl es mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.

Stand: Juli 2010

Mitgliedsunternehmen der IHK Köln und solche Personen, die in der Region Köln die Gründung eines Unternehmens planen, erhalten weitere Informationen bei:

Ihr Ansprechpartner

Horst Hohn
Tel. 0221 1640-131
Fax 0221 1640-139
E-Mail: Horst.Hohn@koeln.ihk.de

Industrie- und Handelskammer zu Köln
Unter Sachsenhausen 10–26
50667 Köln
www.ihk-koeln.de