Was ist eine elektronische Signatur?

Mit der zunehmenden Verbreitung und Akzeptanz des Internets ist es notwendig geworden, ein elektronisches Äquivalent zur manuellen Unterschrift zu schaffen.

Immer häufiger fällt in diesem Zusammenhang der Begriff "elektronische Signatur".

Als elektronische Signatur wird die Verknüpfung von elektronischen Daten mit einem privaten (personifizierten) Schlüssel bezeichnet. Dadurch wird die Identität des Signierenden und die Integrität der signierten Daten gewährleistet. Die Gewährleistung dieser Eigenschaften beruht auf einem komplexen mathematischen Verfahren, das im Abschnitt "Funktionsweise" erläutert wird.

Wofür braucht man elektronische Signaturen?

Beim Datenaustausch über anonyme Netzwerke (wie z.B. das Internet) kann die Situation entstehen, dass sich die an einer elektronischen Transaktion beteiligten Kommunikationspartner nicht kennen. In diesem Fall können diese sich nicht sicher sein, dass der jeweilige Partner auch tatsächlich die Person ist, für die er sich ausgibt.

Ebenfalls ist nicht sichergestellt, dass die zwischen den Kommunikationspartnern übertragenen Daten beim Empfänger in der Form ankommen, in der sie vom Sender verschickt worden sind. Solange die Kommunikationspartner kein Vertrauen zueinander haben, ist eine rechtsverbindliche Kommunikation auf elektronischem Wege nicht oder nur sehr eingeschränkt möglich.

Hier hilft Ihnen die elektronische Signatur weiter. Sie ist das elektronische Äquivalent einer eigenhändigen Unterschrift und garantiert die Identität eines jeden Anwenders. Sie ermöglicht darüber hinaus die sichere Authentifizierung aller an einer elektronischen Transaktion beteiligten Kommunikationspartner.

Zusätzlich kann mit Hilfe der elektronischen Signatur auch die Integrität der übertragenen Daten garantiert werden, da etwaige Datenmanipulationen für die Kommunikationspartner ersichtlich werden.

Wie funktioniert die elektronische Signatur?

Auch wenn die Funktionsweise der elektronischen Signatur recht komplex wirkt, bekommen Sie von den nachfolgend beschriebenen mathematischen Verfahren im täglichen, operativen Umgang mit der elektronischen Signatur nicht viel mit. Die komplexen Prozesse werden vollständig durch spezielle Softwarekomponenten abgedeckt.

Das technische Verfahren der elektronischen Signatur basiert auf der Verwendung zweier unterschiedlicher elektronischer Schlüssel (Public Key-Konzept). Jedes Schlüsselpaar besteht dabei aus einem privaten Schlüssel (Private Key) und einem korrespondierenden öffentlichen Schlüssel (Public Key). Beide Schlüssel sind zwar voneinander abhängig, können jedoch getrennt voneinander genutzt werden.

Jedes einzelne Schlüsselpaar identifiziert eindeutig einen Eigentümer. Ein Eigentümer kann beispielsweise eine natürliche Person, aber auch eine technische Komponente (z.B. Server) oder eine E-Mail-Adresse sein. Der bei der Erstellung des Schlüsselpaares verwendete mathematische Algorithmus von Rivest, Shamir und Adleman (RSA-Algorithmus) stellt sicher, dass der private Schlüssel auch dann nicht berechnet werden kann, wenn der korrespondierende öffentliche Schlüssel bekannt ist.

Mit dem privaten Schlüssel können elektronische Inhalte (z.B. eine E-Mail oder ein Bestellvorgang) elektronisch unterschrieben (signiert) werden. Dazu wird von dem zu signierenden elektronischen Dokument mittels einer speziellen mathematischen Funktion (Hashfunktion) ein individueller "Fingerabdruck" ermittelt. Bei unverändertem Inhalt des Dokumentes führt die Hashwert-Berechnung immer zum selben Ergebnis.

Der so errechnete Hashwert wird mit Hilfe des privaten Schlüssels des Absenders verschlüsselt und dann zusammen mit dem Zertifikat des Absenders und dem Ursprungsdokument verbunden. Diese Komponenten bilden gemeinsam das elektronisch unterschriebene Dokument. Das Zertifikat des Absenders enthält u. a. Angaben zur Person (Name, Adresse etc.) und seinen öffentlichen Schlüssel.

Will der Empfänger die Signatur eines elektronisch signierten Dokumentes prüfen, benötigt er den mitgelieferten öffentlichen Schlüssel des Absenders. Mit diesem wird die verschlüsselte Prüfsumme entschlüsselt. Aus dem elektronischen Ursprungsdokument wird unabhängig davon noch einmal ein Hashwert ermittelt. Nun werden beide Hashwerte miteinander verglichen. Stimmen sie nicht überein, ist das vorliegende Dokument (z. B. durch Manipulation Dritter während des Transportes) definitiv verändert worden.

Das RSA-Verfahren ist nach heutigem Stand sicher. Es gibt bislang nur eine theoretische Möglichkeit, einen privaten Schlüssel aus einem öffentlichen Schlüssel zu errechnen und damit das Verfahren zu unterlaufen. Selbst bei der Bündelung der Rechenleistung aller weltweit verfügbaren Computersysteme würde die Errechnung eines einzelnen privaten Schlüssels jedoch mehrere Jahre dauern.

Um auch zukünftig maximalen Schutz bieten zu können, kann die Schlüssellänge variabel erhöht werden. In der Regel erfolgt dies durch ihre Verdoppelung. Derzeit gebräuchlich und sicher sind 1024 Bit, im Zuge der nächsten Anpassung werden Schlüssel mit einer Länge von 2048 Bit zum Einsatz kommen.

Welche Vorteile bietet Ihnen die elektronische Signatur?

Elektronische Signaturen haben zwei wichtige Eigenschaften: Zum einen sichern sie die Identität des Signierenden und zum anderen die Integrität der zwischen Sender und Empfänger übertragenen elektronischen Daten.

Sie können sich beim Empfang von elektronisch signierten Daten also sicher sein, dass Ihr Kommunikationspartner auch tatsächlich die Person ist, für die er sich ausgibt und dass die zwischen Ihnen und Ihrem Kommunikationspartner übertragenen Daten auf dem Weg durch das Internet nicht verändert worden sind. Jede auch noch so kleine Änderung wird durch das zugrunde liegende technische Verfahren aufgedeckt und für den Empfänger sofort sichtbar gemacht.

Aufgrund dieser Eigenschaften stellen elektronische Signaturen die technische Grundlage für eine sichere und rechtsverbindliche Durchführung von elektronischen Transaktionen dar. Die qualifizierte elektronische Signatur hat daher im Rechtsgeschäft die gleiche rechtsverbindliche Wirkung wie Ihre eigenhändige Unterschrift. Dabei ist die elektronische Signatur noch viel genauer und fälschungssicherer als eine manuelle Unterschrift.

Wofür braucht man eine elektronische Verschlüsselung?

Die elektronische Verschlüsselung gewährleistet die Vertraulichkeit der übertragenen Daten. Sie stellt sicher, dass die übertragenen Daten auch tatsächlich nur von den dafür vorgesehenen Kommunikationspartnern eingesehen werden können.

Um die sehr eingeschränkte Sicherheit einer unverschlüsselten E-Mail-Übertragung zu veranschaulichen, wird nachfolgend ein Vergleich mit einer normalen Postbeförderung dargestellt. In diesem Fall hätte eine E-Mail in etwa dieselben Sicherheitseigenschaften wie eine mit Bleistift beschriebene Postkarte: Diese ist auf dem Weg vom Absender zum Empfänger von jedermann lesbar und manipulierbar.

Dabei können sich Manipulationen sowohl auf Änderungen des Absendernamens, als auch auf Veränderungen des eigentlichen E-Mail-Inhaltes oder auch eventuell angefügter Anlagen (Word-Dokumente, Präsentationen etc.) beziehen. Die eigentliche Gefahr besteht darin, dass weder der Sender, noch der Empfänger der E-Mail etwaige Manipulationen überhaupt bemerken. Außerdem sind solche Manipulationen aufgrund ihres digitalen Charakters nicht nachzuweisen und die Gefahr, als Verursacher entdeckt zu werden, ist ausgesprochen gering.

Mit Hilfe der elektronischen Verschlüsselung kann auch dieser Mangel behoben werden. Die elektronische Signatur zur Sicherung der Identität der Kommunikationspartner und Integrität der übertragenen Daten stellt die Grundlage für die elektronische Kommunikation dar. In Kombination mit elektronischer Verschlüsselung zur Sicherung der Vertraulichkeit der übertragenen Daten wird darüber hinaus eine hochsichere elektronische Kommunikation ermöglicht.

Wo können Sie die elektronische Verschlüsselung einsetzen?

Die Einsatzmöglichkeiten der elektronischen Verschlüsselung sind vielfältig und richten sich nach den persönlichen Sicherheitsanforderungen eines jeden Einzelnen.

Ein wichtiges Einsatzszenario ist z.B. die Absicherung der elektronischen Kommunikation via E-Mail. Im privaten und insbesondere im beruflichen Umfeld werden hin und wieder inhaltlich brisante E-Mails versendet, deren Informationen nicht in die Hände von Unbefugten gelangen sollten. Hier schafft die elektronische Verschlüsselung Abhilfe, da sichergestellt wird, dass die Inhalte der E-Mail auch tatsächlich nur für diejenigen sichtbar werden, für die diese Informationen bestimmt sind.

Eine weitere Einsatzmöglichkeit besteht darin, bestimmte Dateien oder auch ganze Verzeichnisse der Festplatte zu verschlüsseln, um zu verhindern, dass vertrauliche Informationen in fremde Hände fallen.

Wie funktioniert die elektronische Verschlüsselung?

Ähnlich wie der elektronischen Signatur liegt auch der elektronischen Verschlüsselung ein komplexes mathematisches Verfahren zu Grunde. Es handelt sich hierbei um ein hybrides Verfahren, d.h. um die Kopplung eines asymmetrischen mit einem symmetrischen Verschlüsselungsverfahren.

Das hybride Verfahren kombiniert die Geschwindigkeitsvorteile von symmetrischen Verfahren mit der Flexibilität der asymmetrischen Verfahren. Der Vorgang einer Verschlüsselung erfolgt mehrstufig. Im ersten Schritt wird ein "Session Key" erzeugt. Wie der Name vermuten lässt, handelt es sich hierbei um einen einmaligen Schlüssel, der genau für einen Verschlüsselungsvorgang verwendet wird. Die elektronischen Daten werden nun mit dem Session Key verschlüsselt.

Um den Session Key zusammen mit dem verschlüsselten Daten sicher zu übertragen, wird dieser im nächsten Schritt mit dem öffentlichen Schlüssel des Empfängers nach asymmetrischem Verfahren verschlüsselt. Anschließend können die so verschlüsselten Daten elektronisch übertragen werden.

Der Empfänger einer verschlüsselten Nachricht entschlüsselt zuerst den Session Key mit seinem privaten Schlüssel. Mit dem entschlüsselten Session Key können dann auch die Daten entschlüsselt werden.

Auch hier gilt: Von den Details einer Ver- und Entschlüsselung bekommen Sie im operativen Umgang nicht viel mit. Die komplexen Prozesse werden vollständig durch spezielle Softwarekomponenten abgedeckt.

Welche Vorteile bietet Ihnen die elektronische Verschlüsselung?

Die Elektronische Verschlüsselung bietet Ihnen die Möglichkeit, vertrauliche Informationen auf elektronischem Weg zu übertragen und dabei sicher sein zu können, dass diese Informationen nicht von unberechtigten Dritten eingesehen werden.

In Kombination mit der elektronischen Signatur bietet die elektronische Verschlüsselung maximalen Schutz und Sicherheit bei der Übertragung von elektronischen Daten und bei der elektronischen Kommunikation.