Digitale Signatur – Ihr Personalausweis für das Internet

Einsatzmöglichkeiten der digitalen Signatur im Handwerksbetrieb

Seit Anfang der neunziger Jahre vollzieht sich ein rasanter Wandel in der betrieblichen Kommunikation. Das Internet wird immer häufiger für Geschäftsprozesse genutzt. Der klassische hand unterschriebene Brief wird künftig wohl nur noch im Privatbereich üblich sein. Die elektronische Kommunikation zwischen Unternehmen untereinander und zu Privatpersonen und Behörden ist schnell, effizient und stets aktuell. Längst werden nicht nur allgemeine Informationen über das Internet weitergegeben, sondern auch Rechnungen, Verträge und Steuererklärungen.

Rechtsverbindliche Unterschriften auf elektronischen Dokumenten – mit der digitalen Signatur sind sie möglich

Gerade für diese Vorgänge hat das Internet einen Nachteil gegenüber dem handschriftlich signierten Brief. Schriftstücke können nicht handschriftlich rechtsverbindlich unterschrieben werden! Das Einscannen einer Unterschrift und die Einbindung in das Dokument garantiert genauso wenig Rechtsverbindlichkeit, als wenn das Schriftstück ohne Unterschrift versendet wird. Doch hier gibt es eine Lösung für dieses Problem, die geeignet ist, elektronische Dokumente rechtsverbindlich mit einer fälschungssicheren Unterschrift zu unterzeichnen: die digitale Signatur.

Die elektronische Signatur gewährleistet die Unversehrtheit von elektronischen Schriftstücken. Das heißt eine unbemerkte Manipulation der Daten ist nicht mehr möglich, da sie die eindeutige Identifikation des Unterzeichners durch eine Instanz, dem so genannten Trustcenter, erlaubt.

Grundlagen - Erste Schritte auf dem Weg zur rechtsverbindlichen Unterschrift

Der erste Schritt zu einer rechtsverbindlichen digitalen Signatur ist die Beantragung einer persönlichen Chipkarte. Genau genommen beantragen Sie dabei Ihr persönliches Zertifikat, eine digitale Bestätigung Ihrer Zertifizierungsstelle, dass Sie als Person zuverlässig identifiziert wurden und Ihnen ein eindeutiger Signaturschlüssel zugeordnet wurde. Diese Chipkarte müssen Sie sich dabei wie einen Personalausweis in der digitalen Welt vorstellen. Alle Angaben aus Ihrem Personalausweis müssen in dem Antragsformular angegeben werden. Die von Ihnen gemachten Angaben werden persönlich von Mitarbeitern der Zertifizierungsstelle überprüft, nachdem Sie den Antrag, zusammen mit einer Kopie Ihres Ausweises, bei der zuständigen Stelle abgeben haben. Dieses auf dem ersten Blick sehr formalistische Vorgehen dient der zweifelsfreien Zuordnung des Zertifikates zu Ihrer Person. Anschließend erhalten Sie innerhalb weniger Tage Ihre persönliche Chipkarte. Den Empfang der Karte müssen Sie lediglich gegenüber der Zertifizierungsstelle bestätigen, damit Ihre Signaturkarte frei geschaltet werden kann. Jetzt kann es mit Ihrer rechtsverbindlichen Kommunikation über das Internet losgehen. Sie benötigen neben Ihrer Signaturkarte lediglich eine Signiersoftware sowie einen Kartenleser. Beides erhalten Sie ebenfalls, häufig in einem Paket, von Ihrem Anbieter der digitalen Signatur.

Wie funktioniert das Unterschreiben?

Ihre Signiersoftware haben Sie installiert, der Kartenleser ist angeschlossen, und nun wollen Sie Ihrem Geschäftspartner einen digital signierten Vertrag per E-Mail zuschicken. Zunächst wählen Sie die zu signierende Datei aus, anschließend weisen Sie dieser Datei mit Hilfe der Signiersoftware Ihre Signatur zu. Dabei wird Ihr privater Schlüssel für den Signiervorgang verwendet. Sie müssen diesen Vorgang lediglich mit Ihrem Passwort freigeben. Schon haben Sie Ihre erste digitale Signatur nach dem deutschen Signaturgesetz geleistet. Die so unterschriebene Datei können Sie, ebenso wie Ihren öffentlichen Schlüssel einfach an eine E-Mail anhängen und Ihrem Vertragspartner zusenden. Soll die Datei zusätzlich noch verschlüsselt werden, benötigen Sie den öffentlichen Schlüssel des Empfängers. Durch dieses Verfahren ist gewährleistet, dass nur derjenige, der zu dem öffentlichen Schlüssel den entsprechenden privaten Schlüssel besitzt, die Datei öffnen und lesen kann.

Technisch wird während dieses Vorganges eine mathematische Prüfsumme, der so genannte Hash-Wert, gebildet und mit Ihrer Signatur mit der Datei verbunden. Das Besondere an dieser Funktion ist, dass dieser Wert für jedes Dokument einzigartig ist. Eine noch so geringfügige Änderung in der Datei führt zu einer anderen Prüfsumme und somit zum Verlust der Rechtsverbindlichkeit!

Verifikation einer signierten Datei

Ihr Geschäftspartner hat nun per E-Mail von Ihnen den verschlüsselten und digital unterschriebenen Vertrag erhalten. Zunächst muss er die Datei entschlüsseln. Da Sie die Datei mit dem öffentlichen Schlüssel des Empfängers codiert haben, kann nur Ihr Geschäftspartner mit seinem privaten Schlüssel die Datei entschlüsseln. Erst dann ist das Dokument für ihn lesbar. Um die digitale Signatur des Absenders zu prüfen, benötigt der Empfänger Ihren öffentlichen Schlüssel. Mit Hilfe dieses Schlüssels wird eine neue Prüfsumme aus der Datei ermittelt. Sind beide Prüfsummen identisch, so wurde das elektronisch unterschriebene Dokument unverfälscht übermittelt. Zudem ist dies der Beweis dafür, dass wirklich der Absender die Nachricht versandt hat. Mit dem Abschluss der Zertifikatsprüfung ist auch auf Empfängerseite alles getan, was notwendig ist. Ihr Geschäftspartner hält nun einen rechtwirksamen Vertrag in den Händen. Der Vorgang der Verifikation ist zwar etwas komplizierter als der des Signierens aber trotzdem leicht erlernbar.

Anwendungen für die digitale Signatur

Die Zahl der Anwendungen für die digitale Signatur wächst stetig. Dies hängt zum einen mit der Erkenntnis der Anbieter von Anwendungen zusammen, dass digital unterschriebene Dokumente medienbruchfrei weiter verarbeitet und archiviert werden können und somit dazu beitragen, Kosten zu senken. Zum anderen werden Anwendungen künftig gesetzlich verpflichtend nur noch über elektronische Medien angenommen. Zurzeit hat der Nutzer zwei Möglichkeiten ein Formular einzureichen: entweder in Papierform oder digital signiert. Überlegungen des Gesetzgebers gehen allerdings in die Richtung, Einreichungen in Papierform nicht mehr anzuerkennen oder diese mit einer höheren Gebühr auszustatten als die Online-Variante.

Allerdings lohnt es sich bereits heute über den Einsatz der digitalen Signatur, auch ohne gesetzliche Pflicht, nachzudenken. Eine Reihe von interessanten Anwendungen für die digitale Signatur, mit denen Handwerksbetriebe nicht nur Zeit, sondern auch Kosten sparen können sind bereits erfolgreich im Einsatz. Nachfolgend stellen wir Ihnen einige handwerksrelevante Anwendungen kurz vor.

Mahnanträge: Unter www.online-mahnantrag.de können Sie Mahnbescheide online beantragen. Sie sparen dabei nicht nur die Formular- und Portokosten für den Mahnantrag. Der beantragte Mahnbescheid verlässt das Mahngericht in der Regel noch am selben Tag. So kommen Sie bis zu vier Wochen schneller an Ihr Geld.

Ausschreibungen: Unter www.subreport-elvis.de (Subreport Verlag) oder www.dvn.net (Deutsche Vergabenetz GmbH) können Sie nicht nur online nach Ausschreibungen suchen. Sie können mit Ihrer digitalen Signatur auch sämtliche Unterlagen zur Ausschreibung herunterlanden, diese am eigenen PC bearbeiten, digital signieren und direkt wieder an die Vergabeplattform zurücksenden.

Patente: Das Deutsche Patentamt akzeptiert digital signierte Anmeldungen – zu ermäßigten Gebühren. Außerdem erfahren Sie online frühzeitig, ob Ihre Unterlagen vollständig eingereicht sind.

Rechtsverbindliche Rechnungen und Verträge: Mit der Adobe Destiller Vollversion 7.0 können Sie Ihre Rechnungen mit einem Unterschriftenfeld versehen, digital unterzeichen und per E-Mail versenden. Der Einsatz der digitalen Signatur ist wichtig, damit der Empfänger zum Vorsteuerabzug berechtigt ist.

Weitere bereits nutzbare und zukünftige Anwendungen können Sie in der ibi-Signaturdatenbank der Universität Regensburg unter www.sigdb.ibi.de recherchieren.

Kosten für die digitale Signatur?

Die digitale Signatur gibt es natürlich nicht umsonst. Es sind einmalige Anschaffungskosten sowie laufende Kosten für die Signaturkarte zu berücksichtigen: Einmalige Kosten entstehen für den Kauf eines Starter Signaturpaketes (enthält den Kartenleser und die Signiersoftware). Diese liegen je nach Anbieter zwischen 130 und 180 Euro. Für die qualifizierte digitale Signatur kommen jährliche Kosten in Höhe von ca. 30 Euro hinzu. Stellen Sie diese Kosten den potenziellen Einsparungen gegenüber, kann sich diese Investition bei entsprechender Nutzung bereits nach einem Jahr amortisieren!

Glossar zu Begriffen rund um die digitale Signatur

Akkreditierung: Trustcenter, die durch die Bundesnetzagentur geprüft wurden, sind berechtigt, die rechtsverbindliche qualifizierte digitale Signatur herauszugeben. Diese Herausgeber sind somit akkreditiert.

Authentizität: Unter Authentizität einer Information versteht man die eindeutige Zuordnung eines digitalen Dokuments zum Verfasser, Ersteller und/oder Absender sowie den Nachweis, dass die Informationen nachträglich nicht mehr verändert worden sind.
Hash-Wert: Bezeichnet einen mathematischen Wert (Prüfsumme), der von einer elektronischen Datei erzeugt wird. Ein Hash-Wert bildet eine eindeutige Verknüpfung zum ursprünglichen Original ab. Die der Prüfsumme zugrunde liegende Datei kann von unbefugten Personen nicht wieder rekonstruiert werden.

Integrität: Auf dem Gebiet der Datensicherheit versteht man unter Integrität den Nachweis, dass elektronische Daten vollständig und unverändert sind.

Schlüssel: Zu unterscheiden ist zwischen dem privaten (geheimen) Schlüssel, der sich auf der Karte befindet und einem öffentlichen Schlüssel. Zur Signaturerzeugung wird der private Schlüssel verwendet, der Empfänger kann mit Hilfe des öffentlichen Schlüssels die Gültigkeit der Signatur des Absenders sowie die Unverfälschtheit der übermittelten Daten feststellen.

Signaturgesetz (SigG) und Signaturverordnung (SigV): Regeln die Rahmenbedingungen für die Erzeugung elektronischer Signaturen sowie für Anbieter von Signaturen, damit diese als sicher und rechtskonform gelten.

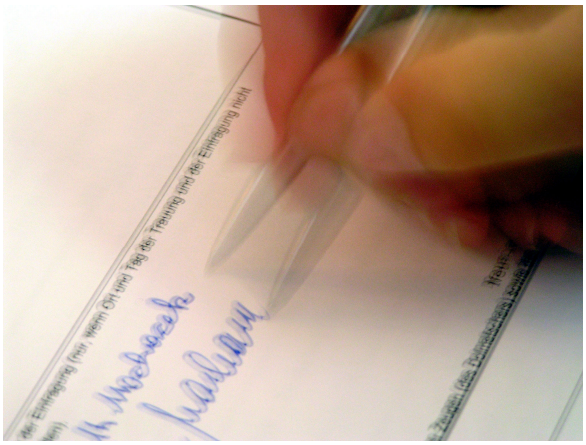
Trustcenter: Der Begriff Trustcenter bezeichnet eine vertrauenswürdige Instanz, die gemäß den strengen Auflagen des Signaturgesetzes Dienste, wie z.B. Ausstellung von Zertifikaten, Ausstellung von Zeitstempeln oder Auskünfte über ausgegebene Zertifikate anbietet.

Verifikation: Unter Verifikation im Zusammenhang mit der digitalen Signatur versteht man die Prüfung, ob eine signierte Datei unversehrt ist und ob das Zertifikat des Unterzeichners gültig ist.

Verschlüsselung: Technisches Verfahren unter Verwendung von öffentlichen und privaten Schlüsseln zum Schutz von elektronischen Daten. Die Daten werden durch die Verschlüsselung vor unbefugter Einsicht und dem Zugriff Dritter geschützt.

Zertifikat: Ein Zertifikat ist eine digitale Bestätigung der Registrierungsstelle, dass der Nutzer der digitalen Signatur eindeutig identifiziert wurde und ihm ein eindeutiger Signaturschlüssel zugeordnet wurde.

Kontakt:
Dipl.-Ing. Dieter Mester, Beauftragter für Innovation und Technologie bei der Handwerkskammer Oldenburg
Tel. 0441/232-214
E-Mail: mester@hwk-Oldenburg.de



Bildmaterial www.photocase.com