



Digitale Signatur

Autor: Jürgen Schüler

Letzte Änderung: 18.05.2012

Die digitale Signatur wird in Zukunft eine dominierende Rolle bei den elektronischen Geschäftsprozessen innerhalb des Handwerks, der Industrie und den Ämtern, Kammer und Verbänden einnehmen. Spätestens mit der Ausgabe des neuen Personalausweises, der für eine qualifizierte digitale Signatur vorbereitet ist, wird der Durchbruch erfolgen. In Verbindung mit den One- Stop-Shops erlangt die Signatur auch Bedeutung für die Handwerkskammern und alle anderen öffentlichen Einrichtungen.

Inhaltsverzeichnis

Bedeutung der Technologie / Marktentwicklung für das Handwerk

- Problem der E- Mails
- Rechtsverbindliche Kommunikation
- Was ist eine elektronische Signatur?
- Der Weg zur Qualifizierten Digitalen Signatur
- Kosten
- Funktionsweise
- Schutz eines Dokuments

Marktpotential

Betroffene Handwerksberufe

Demonstrations- / Weiterbildungs- oder Qualifizierungsmöglichkeiten

Weiterführende Informationen

Hersteller und Anbieter

Seminare / Informationsveranstaltungen

Fachberatung

Quellen

Gesetze

Standardfragen - FAQ

Bedeutung der Technologie / Marktentwicklung für das Handwerk



Quelle: Autor

Aufgrund der weiten Verbreitung des Internets und der sich daraus ergebenden Kommunikationsmöglichkeiten - beispielsweise dem Versand elektronischer Dokumente per E- Mail - können im unternehmerischen Alltag Geschäftsprozesse vereinfacht, beschleunigt und effizienter organisiert werden. Dadurch können nicht nur Kosten reduziert, sondern viele Vorgänge, die das Unternehmensumfeld betreffen, effektiver gestaltet werden. Handgeschriebene oder gedruckte Briefe sind nicht nur teuer, sie schaffen vor allem Medienbrüche. Aus diesem Grund verwenden immer mehr öffentliche Verwaltungen und Unternehmen elektronische Dokumente, um Medienbrüche zu vermeiden.

Problem der E- Mails

Durch E- Mail - über das unsichere Internet - übermittelte elektronische Dokumente bringen gleich mehrere Nachteile mit sich und verlieren dadurch ihre Rechtsverbindlichkeit.

So ist die Identität des Absenders nicht eindeutig feststellbar, denn eine Absenderadresse kann mit einfachen Mitteln gefälscht werden. Auf dem Weg zum Empfänger können die übertragenen Dokumente manipuliert (z. B. Textpassagen gestrichen oder Zusammenhänge verändert) werden, ohne dass der Empfänger dies erkennen kann. Da alle Informationen, die über eine E- Mail versendet werden, im Klartext vorliegen, können diese von Dritten mitgelesen und reproduziert werden. Um elektronische Dokumente wie Rechnungen, Verträge, Mahnungen etc. rechtsverbindlich übermitteln zu können bzw. diese der Schriftform gleichzusetzen, bedarf es eines besonderen Umgangs mit solchen. Die Lösung dieser Probleme bietet die qualifizierte digitale Signatur.

Rechtsverbindliche Kommunikation

Neben dem digitalen Unterzeichnen kann die Signaturkarte auch für einen sicheren und vertraulichen Online- Datenversand mit Geschäftspartnern weltweit und zum Verschlüsseln von Nachrichten verwendet werden. Dazu wird das Dokument auf der Senderseite mit dem öffentlichen Schlüssel des Empfängers und dem privaten Schlüssel des Senders verschlüsselt. Nur der Empfänger kann mit seinem privaten Schlüssel die Nachricht entschlüsseln. Dadurch können wichtige Dokumente wie Lebensläufe, Patente o. ä. vor dem Zugriff Unbefugter geschützt werden.

Was ist eine elektronische Signatur?

Elektronische Signaturen sind an Personen gebundene und von diesen elektronisch erstellte Willenserklärungen oder Bestätigungen. Sie werden als Datenstruktur entweder in digitale Dokumente eingefügt oder solchen Dokumenten angehängt und lassen auf den Urheber des Dokumentes schließen.

Die rechtsverbindliche "Digitale Unterschrift" wird über ein asymmetrisches kryptographisches Schlüsselverfahren generiert. Bei diesem Verfahren kommen zwei verschiedene Schlüssel zum Einsatz: ein privater Schlüssel, der vom Unterzeichner stets geheim gehalten werden muss und zusätzlich durch ein Passwort geschützt ist sowie ein dazu passender öffentlicher Schlüssel, der jedem zugänglich ist und mit dessen Hilfe die Echtheit der Signatur und Identität des Urhebers überprüft werden kann.



Quelle:
Autor

Es gibt eine Reihe von Signaturarten, die sich durch verschiedene Rechtswirkungen unterscheiden:

- Einfache Signatur
- Fortgeschrittene Signatur
- Qualifizierte Digitale Signatur
- Qualifizierte Digitale Signatur mit Anbieterakkreditierung

Die **einfache Signatur** lässt keine gesicherten und überprüfbaren Rückschlüsse auf die Identität des Verfassers und auf die Integrität der Nachricht zu. Man kann also weder feststellen, ob sich die Nachricht noch im Ursprungszustand befindet, noch wer sie ursprünglich verfasst hat.

Beispiele für eine einfache Signatur:

- Gescannte Unterschrift
- Kontaktinformationen am Ende einer E- Mail mit Angaben zur Person, Firma etc.
- RSA- Signatur (für den Fernzugriff auf Rechner) ohne Zertifikat

In vielen Fällen der elektronischen Kommunikation mit Behörden und Unternehmen reicht diese Form der Signatur bereits aus.

Bei der **fortgeschrittenen elektronischen Signatur** handelt es sich um eine mit kryptographischen Mitteln erzeugte elektronische Signatur. Die Nachricht wird mit einer Art persönlichem Siegel - welches ausschließlich dem Unterzeichner zugeordnet ist - versehen.

Die Identität des Signaturschlüssel- Inhabers oder einer E- Mail- Adresse wird selbst oder durch einen Dritten in einem Zertifikat bescheinigt. Dieses ermöglicht eine Identifizierung des Unterzeichners bzw. einer E- Mail- Adresse. Veränderungen am signierten Dokument sind erkennbar, Manipulationen machen die Signatur ungültig.

Häufig wird diese Signatur durch einen privaten Schlüssel lokal im Rechner erzeugt. Der private Schlüssel wird zusammen mit dem öffentlichen Schlüssel auf der Festplatte oder einem anderen auslesbaren Medium, z.B. einem USB- Stick oder einer Signaturkarte gespeichert.

Beispiele für eine fortgeschrittene elektronische Signatur:

- Signatur, erzeugt auf Basis eines softwarebasierten Schlüsselpaares mit Zertifikat z.B. mit
der verbreiteten Signatur- Software PGP (Pretty Good Privacy).
- Signatur auf Basis biometrischer Merkmale (Fingerabdruck, Unterschrift etc.)

Elektronische Dokumente mit "einfachen" und "fortgeschrittenen" Signaturen gelten als Objekte des Augenscheins (§371 ZPO). Die fortgeschrittene elektronische Signatur ersetzt nicht die Schriftform gem. § 126 BGB und hat geringe Beweiskraft vor Gericht (§371a ZPO).

Gescannte Unterschriften, Faxe und Kopien, also rein 2- dimensionale Images können nicht als beweiskräftiges Signaturverfahren eingesetzt werden. Erst durch die qualifizierte digitale Signatur kann die Schriftform ersetzt werden.

Eine **qualifizierte elektronische Signatur** ist eine fortgeschrittene elektronische Signatur, die auf einem gültigen qualifizierten Zertifikat beruht und mit einem Kartenleser erzeugt wurde.



Quelle: Autor

Die qualifizierte digitale Signatur ist gleichbedeutend mit einer handschriftlichen Unterschrift.

Über eine vertrauenswürdige Instanz, dem sog. Trust Center wird dem Anwender einmalig ein persönliches Zertifikat ausgehändigt. Er muss sich persönlich bei einem Registrierungspunkt des Zertifizierungsdienste- Anbieters (ZDA) melden, oder wird über das Post- Ident- Verfahren der DBP AG vor Ausgabe des Zertifikats identifiziert. Der ZDA haftet dafür, dass die Informationen im Zertifikat richtig sind. Somit kann bei der Überprüfung eines Zertifikates eindeutig die Identität der Person festgestellt werden.

Bei der **Qualifizierten Digitalen Signatur** mit Anbieterakkreditierung garantiert ein Trust Center die höchsten technischen und organisatorischen Sicherheitsanforderungen seines Rechenzentrums.

Eine Qualifizierte Digitale Signatur ist genauso gültig wie eine handschriftliche Unterschrift und vor Gericht als Beweismittel zulässig.

Um Dokumente mit der qualifizierten digitalen Signatur unterzeichnen zu können, benötigt der Anwender folgende zertifizierte Komponenten:



Quelle: Autor

- Kartenlesegerät
- Signatursoftware zum Unterzeichnen und ggf. Verschlüsseln der Nachrichten
- Signaturkarte.

Zur Verifizierung von Signaturen benötigt der Anwender Zugriff auf den Verzeichnisdienst des Trust Centers.

Bei der Bundesnetzagentur sind akkreditiert:

für das Ausstellen sowohl qualifizierter Zertifikate als auch qualifizierter Zeitstempel:

- Produktzentrum TeleSec der Deutschen Telekom AG
- Bundesnotarkammer
- DATEV eG Zertifizierungsstelle
- D- Trust GmbH
- Deutsche Post Com GmbH Geschäftsfeld Signtrust
- TC TrustCenter GmbH

für das Ausstellen qualifizierter Zertifikate:

- Deutscher Sparkassen Verlag GmbH
- DGN Deutsches Gesundheitsnetz Service GmbH

für das Ausstellen qualifizierter Zeitstempel:

- AuthentiDate International AG

Ihren Betrieb als Zertifizierungsdienste- Anbieter nur angezeigt haben:

- Deutsche Rentenversicherung Bund

Der Weg zur Qualifizierten Digitalen Signatur

Zunächst muss bei einem Registrierungspunkt einer Zertifizierungsstelle - unter Vorlage des Personalausweises - ein persönliches Zertifikat beantragt werden. Je nach Zertifizierungsdienste- Anbieter wird die Qualifizierte Digitale Signatur in Form einer Chipkarte direkt ausgehändigt oder auf dem Postweg übersandt.

Kosten



Quelle: Autor

Bei der Qualifizierten Digitalen Signatur fallen einmalige Kosten für Signaturkarte, Kartenleser, Lizenz für Signatursoftware in Höhe von ca. 100 € und laufende Kosten für die Signatur in Höhe von ca. 20 € pro Jahr an.

Funktionsweise

Soll ein Dokument per E- Mail verschickt werden, wird über eine mathematische Funktion eine Art Fingerabdruck von dem Dokument erstellt. Danach wird mit dem privaten Schlüssel, der sich auf der Chipkarte im Kartenlesegerät befindet und dem ermittelten Fingerabdruck des Dokumentes ein digitales Zertifikat erzeugt, das dem Dokument angehängt wird. Auf Wunsch kann das Dokument noch mit einem Zeitstempel versehen werden. Die Nachricht, bestehend aus Dokument, Zertifikat und ggf. Zeitstempel, kann jetzt per E- Mail an den Empfänger gesendet werden.

Der Empfänger des Dokumentes kann mit dem öffentlichen Schlüssel des Senders die Identität bei dessen Trust Center überprüfen. Außerdem kann anhand des öffentlichen Schlüssels überprüft werden, ob das Dokument auf dem Weg von unbefugten Dritten verändert wurde.

Schutz eines Dokuments

Neben der Integritätsprüfung eines Dokumentes kann die qualifizierte digitale Signatur

auch zur verschlüsselten Übertragung von Nachrichten verwendet werden. Dazu wird das Dokument auf der Senderseite mit dem öffentlichen Schlüssel des Empfängers und dem privaten Schlüssel des Senders verschlüsselt. Nur der Empfänger kann mit seinem privaten Schlüssel die Nachricht entschlüsseln. Dadurch können wichtige Dokumente wie Lebensläufe, Patente o.ä. vor dem Zugriff Unbefugter geschützt werden.



Entwicklungstendenzen

Die digitale Signatur wird in Zukunft eine dominierende Rolle bei den elektronischen Geschäftsprozessen innerhalb des Handwerks, der Industrie und den Ämtern, Kammer und Verbänden einnehmen. Spätestens mit der Ausgabe des neuen Personalausweises, der für eine qualifizierte digitale Signatur vorbereitet ist, wird der Durchbruch erfolgen. In Verbindung mit den One- Stop- Shops erlangt die Signatur auch Bedeutung für die Handwerkskammern und alle anderen öffentlichen Einrichtungen.

Technische Voraussetzungen für den Einsatz der qualifizierten elektronischen Signatur sind:

- Chipkarte von akkreditierten Dienstleistungsanbietern
- Chipkartenleser mit Zahlentastatur für Eingabe der PIN mit Zulassung des ZKA

Marktpotential

Nur die qualifizierte elektronische Signatur hat entsprechend Signaturgesetz Rechtskraft.

Einsatzmöglichkeiten werden sein:

- elektronische Rechnungen
- elektronische Verträge
- Prozesse im Rahmen e- Gouvernement mit Ämtern, Kommunen und Kammern



Quelle: Autor

- Teilnahme an elektronischen Ausschreibungen
- Archivierung
- Verschlüsselung von Dokumenten
- Elektronische Steuererklärung (ELSTER- Plus)

- Seit 01.01.2005 müssen Lohn- und Umsatzsteuervoranmeldungen grundsätzlich elektronisch erfolgen



Quelle: Autor

- Vergabe öffentlicher Aufträge
- Gem. §15 VgV können Angebote für öffentliche Aufträge elektronisch abgegeben werden.
- Online- Rechnungen
- Der Rechnungsempfänger ist nur dann vorsteuerabzugsberechtigt, wenn diese mit einer Qualifizierten Digitalen Signatur versehen war.



Quelle: Autor

- Online- Mahnbescheid
- Anträge auf Erlass von Mahn- und Vollstreckungsbescheiden können elektronisch abgegeben werden.
- Patent- und Markenmeldungen
- Das Deutsche Patent- und Markenamt (DPMA) nimmt Anträge zur Patent- und Markenmeldung elektronisch entgegen.

Betroffene Handwerksberufe

Betroffen sind alle Gewerke, bei E- Ausschreibungen und E- Vergabe vorrangig die Bau- und Dienstleistungsgewerke.

Demonstrations- / Weiterbildungs- oder Qualifizierungsmöglichkeiten

Den Umgang mit der Qualifizierten Digitalen Signatur kann man sich im Kompetenzzentrum IT- Sicherheit und Qualifizierte Digitale Signatur der Handwerkskammer Rheinhessen demonstrieren lassen. Dieses Zentrum bietet auch Weiterbildungsmöglichkeiten an.

Weiterführende Informationen

Kompetenzzentrum für IT- Sicherheit und
 Qualifizierte Digitale Signatur
 der Handwerkskammer Rheinhessen
 Jürgen Schüler
 - Projektleiter-
 Dagobertstraße 2
 55116 Mainz
 Tel. +49 (6131) 9992-61
 Fax +49 (6131) 9992-52

Hersteller und Anbieter

Zur Verifizierung von Signaturen benötigt der Anwender Zugriff auf den Verzeichnisdienst des Trust Centers. Bei der Bundesnetzagentur sind akkreditiert:

für das Ausstellen sowohl qualifizierter Zertifikate als auch qualifizierter Zeitstempel:

- Produktzentrum TeleSec der Deutschen Telekom AG
- Bundesnotarkammer
- DATEV eG Zertifizierungsstelle
- D- Trust GmbH
- Deutsche Post Com GmbH Geschäftsfeld Signtrust
- TC TrustCenter GmbH

für das Ausstellen qualifizierter Zertifikate:

- DGN Deutsches Gesundheitsnetz Service GmbH

für das Ausstellen qualifizierter Zeitstempel:

- AuthentiDate International AG

Ihren Betrieb als Zertifizierungsdienste- Anbieter nur angezeigt haben:

- Deutscher Sparkassen Verlag GmbH
- Deutsche Rentenversicherung Bund

Seminare / Informationsveranstaltungen

Seminar NT 1.17 E- Mail- Sicherheit und Signatur

Heinz- Piest- Institut für Handwerkstechnik an der Universität Hannover
[Rahmenlehrplan]

Seminar: E- Mail- Sicherheit +Digitale Signatur

Kompetenzzentrum IT- Sicherheit und Qualifizierte Digitale Signatur der
Handwerkskammer Rheinhessen, Ansprechpartner: Herr Jürgen Schüler, Telefon
06131-999261, E- Mail j.schueler@hwk.de

Fachberatung

- Kompetenzzentrum IT- Sicherheit und
Qualifizierte Digitale Signatur
der Handwerkskammer Rheinhessen
Ansprechpartner: Herr Jürgen Schüler,
Telefon (06131) 9992-61, E- Mail j.schueler@hwk.de

- Technologieberater der Handwerkskammern

Quellen

-www.komzet-hwk.de ([http:// www.komzet- hwk.de](http://www.komzet-hwk.de))

- Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der

Bundesverwaltung www.kbst.bund.de (<http:// www.kbst.bund.de>)

Gesetze

Signaturgesetz (2001)

www.gesetze-im-internet.de/sigg_2001/index.html ([http:// www.gesetze-im-internet.de/ sigg_2001/ index.html](http://www.gesetze-im-internet.de/sigg_2001/index.html))

Signaturverordnung (2001)

www.gesetze-im-internet.de/sigv_2001/index.html ([\[www.signaturcenter.de\]\(http://www.signaturcenter.de\) \(<http:// www.signaturcenter.de>\)](http:// www.gesetze-im-internet.de/ sigv_2001/ index.html)</p></div><div data-bbox=)

Standardfragen - FAQ

finden Sie auf der unten verlinkten Seite des Komzets unter Themenkatalog/ Digitale Signatur/ FAQ

[www.komzet-hwk.de/ index.php? id=314](http://www.komzet-hwk.de/index.php?id=314) (<http:// www.komzet-hwk.de/ index.php?id=314>)

Weiterführende Fachinformationen zu "Digitale Signatur"

- Einsatzfelder für die Qualifizierte Elektronische Signatur

([http:// fachinfo.bistech.de/ artikel/616/ Einsatzfelder +f %C3%BCr +die +Qualifizierte +Elektronische +Signatur](http://fachinfo.bistech.de/artikel/616/Einsatzfelder+f%C3%BCr+die+Qualifizierte+Elektronische+Signatur))

Diesen Artikel finden Sie als **BISTECH** Fachinformation für Handwerksunternehmen unter www.fachinfo.bistech.de.