Testat FKOM

Name: Ndricim Ramadani

Wie sicher ist die digitale Unterschrift?

###### Wie sicher ist die digitale Unterschrift?

**Das Märchen von "What You See Is What You Sign"**

Ein Computer ist ein hochkomplexes Gerät, das aus vielen verschiedenen Komponenten besteht. Trotz seiner Komplexität kann es dank seiner grafischen Oberfläche ohne grosse Kenntnisse zur Erledigung vieler Aufgaben genutzt werden und damit den Alltag erleichtern. Aufgrund dieser Eigenschaften und den Darstellungsmöglichkeiten ist die Hauptaufgabe eines Computers die Abstraktion.

Um 100 prozentige Gewissheit zu haben, ist die Abstraktion bei der digitalen Unterschrift nicht immer wünschenswert. Andererseits wäre es ohne diese nicht möglich, die Dokumente zu entschlüsseln. Der Computer zeigt ja nicht seinen Speicherinhalt und, auch wenn dieser es tun würde, könnte der Mensch nichts mit diesem Inhalt anfangen. Was also tatsächlich innerhalb eines PCs geschieht, bleibt dem Menschen verborgen und das ist auch gut so, denn diese Vorgänge nehmen viel Arbeit ab. Allerdings stellt sich eine ganz zentrale Frage beim Umgang mit digitalen Unterschriften: Woher weiss der Nutzer, ob er das unterschreibt, was er sieht? Bei digitalen Unterschriften ist es sehr wichtig, dass der Mensch, der unterschreiben möchte, genau weiss, was er unterschreibt. Er muss sich also sicher sein, dass die Ansicht des auf dem Bildschirm abgebildeten Dokuments dem entspricht, was er am Ende unterschreibt. Diesbezüglich gibt es verschiedene Sicherheitsstufen.

**Verschiedene Sicherheits- und Rechtsstufen**

Dank digitaler Signaturen lassen sich Dokumente schnell, praktisch und kostengünstig unterzeichnen. Jede digitale Signatur basiert auf der sogenannten asymmetrischen Verschlüsselung. Sie wird auch als Public-Key-Verfahren bezeichnet und nutzt einen öffentlichen und einen privaten (geheimen) Schlüssel. Mit dem privaten Schlüssel wird die digitale Signatur erzeugt, während mit dem öffentlichen Schlüssel die Authentizität der Unterschrift überprüft wird. Digitale Signaturen können genau wie die handschriftliche Unterschrift auf Papier Rechtsgültigkeit haben. Das ist aber nicht immer der Fall, da das Bundesgesetz zwischen mehreren Typen unterscheidet.

**Einfache elektronische Signaturen** sind Daten, «die anderen elektronischen Daten beigefügt oder die logisch mit ihnen verknüpft sind und zu deren Authentifizierung dienen». Dazu gehören Signaturen, die man etwa in Adobe Acrobat Reader aufs Dokument zeichnet. Das Zertifikat, das dabei im Hintergrund erstellt wird, stellt bloss die Echtheit des Dokuments sicher. Es zeigt im besten Fall an, das dieses Dokument zwischen dem Zeitpunkt des Signierens und Öffnens nichts geändert wurde. Sie dient nicht zur Identifizierung von Personen und bietet kaum Rechtssicherheit.

**Fortgeschrittene elektronische Signaturen** dienen der Personenidentifikation. Das bei der Signatur ausgestellte Zertifikat ordnet die Unterschrift der Inhaberin oder dem Inhaber zu. Somit haben diese die alleinige Befugnis, eine solche Signatur zu erstellen. Das kann – wie bei der Suisse ID der Post – eine SIM- oder Chipkarte sein; sie enthält ein Zertifikat zur Nutzeridentifikation und eines für die digitale Signatur und wird in einen Kartenleser oder USB-Stick eingesetzt. Die Methoden müssen auch nachträgliche Veränderungen der Daten sichtbar machen.

**Die qualifizierte elektronische Signatur** besitzt im Grundsatz dieselben Eigenschaften wie die fortgeschrittene; jedoch beruht sie auf einem qualifizierten Zertifikat, das von einem anerkannten Anbieter ausgestellt wird. In der Schweiz überprüft die KPMG, ob die Zertifikate der Signaturanbieter nicht nur die Anforderungen für fortgeschrittene, sondern auch für qualifizierte elektronische Signaturen erfüllen. Ein qualifiziertes Zertifikat muss als solches gekennzeichnet sein. Auch wird es – im Gegensatz zum Zertifikat einer fortgeschrittenen Signatur – nur auf eine natürliche Person ausgestellt und darf ausschliesslich für die elektronische Signatur eingesetzt werden. Nur die qualifizierte Signatur ist im Schweizer Gesetz festgehalten. So ist nur die qualifizierte elektronische Signatur der handschriftlichen Signatur rechtlich gleichgestellt.

**Quellen**

informatik-aktuell.de/betrieb/sicherheit/sicherheit-digitaler-unterschriften

swisscom.ch/de/magazin/datensicherheit-infrastruktur/digitale-signatur-fortgeschritten-qualifiziert/

# Beurteilungsraster für den Blogbeitrag

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Informationsgehalt, Relevanz, Aktualität | 5 |  |  |  |  |  | * Interessanter Inhalt |
| Strukturierung, Titel, Lead |  |  | 3 |  |  |  | * Aufbau nicht nach Pyramidenprinzip |
| Vernetzung, intern / extern | 5 |  |  |  |  |  |  |
| Stilistik,  Zielgruppe |  |  | 3 |  |  |  | * WIR-Form nicht zulässig * Siehe oben |
| Korrektheit, Quellenangabe | 5 |  |  |  |  |  | * Apa; aber das konnten Sie damals nicht wissen. |
| Punkte TOTAL | 21 | | | | | | Maximum: 25 Punkte |

Testat bestanden; korrekte Arbeit