

Digitale Signaturen

Unterschreiben Sie noch oder signieren Sie schon?

Längste Zeit waren nur Papierdokumente mit eigenhändiger Unterschrift und Stempel rechtsverbindlich. Durch die digitale Signatur ist aber auch bei elektronischen Dokumenten ein rechtssicheres Agieren möglich geworden. Was die digitale Signatur konkret ist und wie man sie einsetzen kann, erfuhr Das Büro von den Signaturexperten soft Xpansion und TC TrustCenter.

In Deutschland müssen seit dem 1. Juli 2004 per E-Mail versendete Rechnungen laut Signaturgesetz (SigG) und der Signaturverordnung (SigV) mit einer so genannten qualifizierten Signatur digital unterschrieben werden, um als Äquivalent einer Papierrechnung akzeptiert zu werden. Denn nur so kann auch auf dem elektronischen Wege die Identität des Absenders und die Integrität des versendeten Inhalts gewährleistet werden.

Was sind digitale Signaturen?

Digitale Signaturen basieren auf der Verwendung von zwei elektronischen Schlüsseln, die als ein Schlüsselpaar zusammengehören. Mit einem so genannten privaten oder geheimen Schlüssel, der nur dem Versender bekannt sein darf, werden Inhalte unterzeichnet bzw. verschlüsselt. Das mit dem privaten Schlüssel verbundene Zertifikat bescheinigt die

Digitale vs. elektronische Signatur

Oftmals werden die Begriffe „digitale Signatur“ und „elektronische Signatur“ synonym verwendet, was nicht ganz korrekt ist. Der Begriff „digitale Signatur“ bezeichnet eine Klasse von kryptografischen (d. h. mathematischen) Verfahren, während „elektronische Signatur“ ein rein rechtlicher Begriff ist und neben digitalen Signaturen auch andere, nicht auf kryptografischen Methoden basierende Verfahren umfasst.

Identität des Verfassers. Meist wird der private Signaturschlüssel in einer speziellen Hardware, der Signaturerstellungseinheit, gespeichert und angewendet, wie z. B. bei Chipkarten mit integriertem Mikroprozessor (Smart Cards) oder USB-Token. Mit seinem Gegenstück, dem öffentlichen Schlüssel, der allgemein bekannt sein darf, werden die Identität des Verfassers und die Integrität der versendeten Nachrichten im Rahmen der Entschlüsselung überprüft. Die beiden Schlüssel sind durch das mathematische asymmetrische (kryptografische) Verfahren ihrer Erstellung miteinander ver-

knüpft. Bei Daten, die mit einem privaten Schlüssel signiert bzw. verschlüsselt wurden, können die Signaturen nur mit dem korrespondierenden öffentlichen Schlüssel entschlüsselt und verifiziert werden.

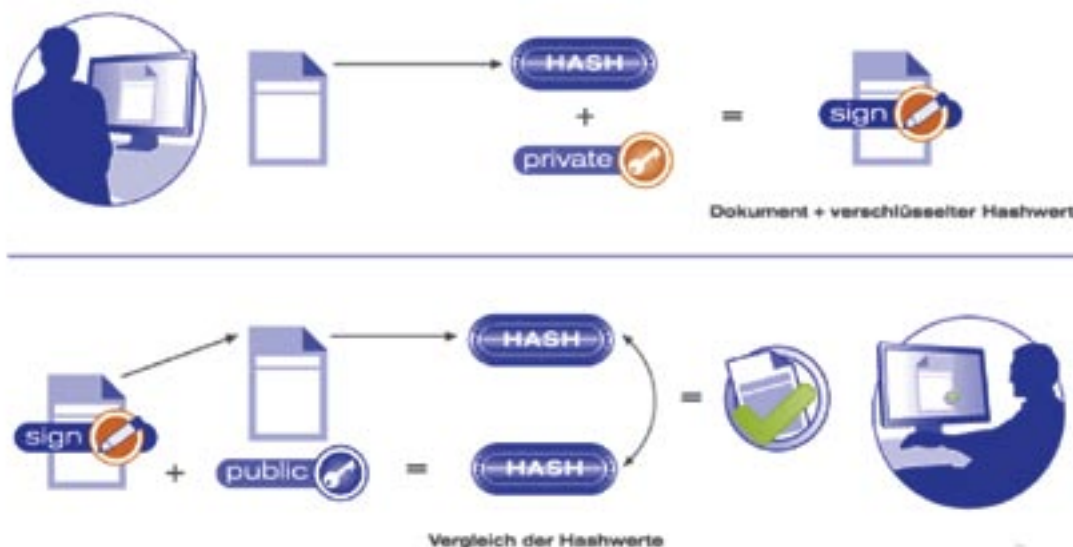
Aufgaben der digitalen Signatur

Eine digitale Signatur erfüllt vor diesem Hintergrund folgende Zwecke:

1. Authentifizierung

Die eindeutige Identifizierung des Verfassers wird dadurch erreicht, dass einer Person ein so genannter geheimer Schlüssel

Wie funktioniert die digitale Signatur eines Dokuments?



Beim Signieren werden die Daten über die Hashfunktion digital zusammengefasst. Daraus wird ein Hashwert (eine kryptografische Prüfsumme) ermittelt, der als eindeutiges und individuelles digitales Identifizierungsmerkmal gilt.

zugeordnet ist, der zusammen mit der Signatur in das digital unterzeichnete Dokument eingefügt wird.

2. Unleugbarkeit

Die digitale Signatur verhindert, dass der Versender einer Nachricht zu einem späteren Zeitpunkt abstreitet, die Nachricht versendet zu haben.

3. Integrität von Inhalten

Die digitale Signatur weist nach, dass ein Dokument nach der Unterzeichnung nicht verändert wurde.

4. Verwendung von Zeitstempeln

Wenn die digitale Unterschrift mit einem qualifizierten Zeitstempel (§2 Nr. 14 SigG) versehen ist, kann zuverlässig nachvollzogen werden, wann ein Dokument erstellt, unterzeichnet und gegebenenfalls modifiziert wurde. Nachträgliche Vor- oder Rückdatierungen von Nachrichten und Daten können so ausgeschlossen werden.



Bei signotec erfolgt die digitale Signatur über das Unterschriften-Pad.

Digitale Signatur in der Praxis

1. E-Mail-Kommunikation

Hier wird nicht nur die Authentizität und Integrität einer E-Mail sichergestellt, sondern auch die Vertraulichkeit dieser Kommunikation.

2. Signatur von Rechnungen

Seit Anfang 2004 ist es rechtlich geregelt, dass nur noch elektronische Rechnungen vorsteuerabzugsfähig sind, die mit einer qualifizierten digitalen Signatur versehen wurden.

3. Elektronische Archivierung

Durch den Einsatz qualifizierter Zeitstempel wird der rechtssichere Medienübergang von Papierdokumenten zu deren Digitalisierung ermöglicht. Ein Zeitstempel ist eine elektronische Bescheinigung eines Zertifizierungsdiensteanbieters, der nachweist, dass die Daten nach einem definierten Zeitpunkt – dem Zeitstempel – nicht mehr verändert wurden.

4. Signatur von PDF-Dateien

PDFs benötigen wenig Speicher und eignen sich vor allem für ausfüllbare Formulare. Durch einen einzigen Mausklick wird dem Empfänger in einem separaten Fenster die Signaturgültigkeit und damit die Urheberschaft des Dokumenten-Absenders bestätigt.

Die herausgebenden Anbieter von Zertifikaten, elektronischen Schlüsseln und Zeitstempeln (ZDA) müssen sich vor Ausstellung bei der Bundesnetzagentur akkredi-

tieren. Aktuelle Anbieter sind z. B. TC TrustCenter, T-Systems mit T-Telesec, DATEV mit e:secure, D-TRUST, Deutsche Post mit Signtrust und die Bundesnotarkammer.

Signatur-Tipps von TC TrustCenter

Grundsätzlich ist beim Einsatz der digitalen Signatur zwischen der fortgeschrittenen und der qualifizierten Signatur zu unterscheiden. In der Geschäftskommunikation, insbesondere bei internen Prozessen, ist die fortgeschrittene Signatur bereits ausreichend. Die gleiche rechtsverbindliche Wirkung wie die eigenhändige Unterschrift hat allerdings nur die qualifizierte elektronische Signatur.

Checkliste „Digitale Signatur“

- **Schritt 1:** Identifizieren Sie relevante Geschäftsprozesse zum Einsatz der Signatur.
- **Schritt 2:** Wählen Sie die hierfür passende Sicherheitsstufe (fortgeschritten, qualifiziert) aus und identifizieren Sie die Stellen, an denen Signaturen zu leisten sind.
- **Schritt 3:** Wählen Sie geeignete Software oder Dienste für Ihre digitalen Geschäftsprozesse aus.

- **Schritt 4:** Statten Sie betreffende Mitarbeiter mit Signatur-Zertifikaten eines anerkannten Trustcenters aus.

Typische Anwendungen der qualifizierten elektronischen Signatur

- Elektronische Steuererklärung (Elster Online)
- Elektronische Rechnungsstellung (E-Billing/E-Invoicing)
- Elektronisches Abfallnachweisverfahren (eANV)
- Vergabeplattformen (e-Vergabe)
- Deutsches Patent- und Markenamt
- ITeBAU – Das digitale Bauantragsverfahren
- weitere Anwendungen unter www.signaturauskunft.de

Mehr Informationen unter www.soft-xpansion.de und www.trustcenter.de.