WEKA

www.datenschuetzer.de

Datenschutz PRAXIS

Datenschutz – rechtssicher, vollständig, dauerhaft.

Ausgabe Januar 2007 | 9 € zzgl. MwSt.

Die digitale Signatur

Digital statt eigenhändig

Die digitale Unterschrift wird sich zukünftig immer mehr durchsetzen. E-Government als die „Killerapplikation" der Behörden oder sichere und schnellere Abwicklungen in den Verfahren läuten den Siegeszug der elektronischen Unterschrift ein. Auch in Ihrem Betrieb? Prüfen Sie vorab, ob Ihr Unternehmen datenschutzkonforme Rahmenbedingungen für den Einsatz der Signaturkarte schafft.

Die elektronische Signatur gewährleistet die Unveränderheit (Integrität) der Daten und die Identität des Versenders (Authentizität). Kryptografische Verfahren bei der elektronischen Signatur machen jede Manipulation oder Verfälschung an den Originaldaten sofort erkennbar. Zweifelsfrei lässt sich der Urheber einer Nachricht identifizieren (Nichtabstreitbarkeit).

Zusätzliche Verschlüsselung der Daten verhindert unbefugten Einblick

Elektronische Signaturen schützen jedoch nicht davor, dass Unbefugte Einblick in die Daten erhalten.

Bei vertraulichen Inhalten ist deshalb zusätzlich zur elektronischen Signatur eine Verschlüsselung erforderlich.

Die gesetzliche Basis, auf die Sie sich berufen können, ist zum einen das BDSG

Als Grundlage zur Einbeziehung des Datenschutzbeauftragten bei der Implementierung eines Verfahrens mit digitaler Signaturkarte dienen folgende gesetzliche Regelungen:

- § 35 BDSG Berichtigung, Löschung und Sperrung von Daten (1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

Wird beispielsweise festgestellt, dass personenbezogene Daten unrichtig sind, oder wird ihre Richtigkeit von

Fortsetzung auf Seite 8

ISSN-Nr. 1614-6867

Fortsetzung von Seite 1

dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten.

- § 9 BDSG Technische und organisatorische Maßnahmen und deren Anlagen
  Absatz 5 verlangt zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).

Eine digitale Signaturkarte fällt also eindeutig in den Aufgabenbereich eines Datenschutzbeauftragten, da sie einer bestimmbaren Person zugeordnet werden kann.

Zum anderen ist das Signaturgesetz relevant

Mit Inkrafttreten des „Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“, kurz Signaturgesetz oder SigG, vom Mai 2001 wurden die rechtlichen Rahmenbedingungen geschaffen. Basis ist ein einheitlicher europäischer Sicherheitsstandard nach 1999/93/EG.

Signatur ist nicht gleich Signatur

§ 2 SigG zählt drei Signaturstandards auf. Die wesentlichen Unterscheidungskriterien sind die Rechtskräftigkeit, die Art des Zertifikats und der Erzeugungsort der Signatur.

- § 2 Nr. 1 SigG „einfache elektronische Signatur“
  ohne besondere Sicherheitsanforderungen, daher kaum beweiskräftig (z.B. eingescannte Unterschrift)
- § 2 Nr. 2 SigG „fortgeschrittene elektronische Signatur“
  gewisses Maß an Sicherheits-Checks (z.B. PGP-(Pretty Good Privacy)-Verfahren mit Web oder Trust)
- § 2 Nr. 3 SigG „qualifizierte elektronische Signatur“
  eigenhändiger Unterschrift gleichgestellt – hohe Sicherheitsanforderungen durch Zertifizierungsdiensteanbieter (ZDA) entsprechend der Signaturverordnung (SignV)

Begriffsbestimmungen zur Signatur nach § 2 SigG

Im Sinne dieses Gesetzes sind

1. „elektronische Signaturen“ Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.
2. „fortgeschrittene elektronische Signaturen“ elektronische Signaturen nach Nummer 1, die
   a. ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
   b. die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
   c. mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
   d. mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann
3. „qualifizierte elektronische Signaturen“ elektronische Signaturen nach Nummer 2, die
   a. auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
   b. mit einer sicheren Signaturerstellungseinheit erzeugt werden

Die einfache Signatur ist rechtlich nicht anerkannt, da sie zu unsicher ist

Eine einfache elektronische Signatur lässt schon sich mit Hausmitteln erstellen, z.B. als Bitmap-Datei mit der eingescannten Unterschrift im elektronischen Dokument.

Signaturen mit einer einfachen elektronischen Signatur nach § 2 Nr. 1 SigG sind jedoch nicht rechtlich anerkannt. Wesentlich ist, dass die einfache Signatur keine gesicherten und überprüfbaren Rückschlüsse auf die Identität des Verfassers und auf die Integrität des Dokuments zulässt.

Die fortgeschrittene Signatur bietet eine Authentizitätsprüfung

Die fortgeschrittene elektronische Signatur erlaubt eine Identifizierung des Signaturschlüssel-Inhabers. Dies ist die Authentizitätsprüfung. Dabei handelt es sich um eine kryptografisch-technisch erzeugte elektronische Signatur. Die Identität des Schlüsselinhabers wird durch einen Dritten, z.B. durch ein Trust-Center, in einem Zertifikat bescheinigt.

Zudem ist durch einen Hash-Wert, der bei der Erstellung eines Dokuments erzeugt wird, eine Manipulation oder Veränderung am signierten Originaldokument erkennbar.

Um eine angemessene Vertraulichkeit zu gewährleisten, sollte ein Verfahren verwendet werden, das ausreichend lange Schlüssel unterstützt. Derzeit wird die Verwendung von Schlüsseln mit einer Länge von mindestens 1.024 Bit empfohlen.

Auch die fortgeschrittene Signatur ist nicht als rechtssicher anerkannt

Selbst Signaturen nach dem § 2 Nr. 2 SigG gelten nicht als rechtssicher – obwohl nach diesem Verfahren Manipulationen der Daten erkennbar sind und sich Dokumente eindeutig einer natürlichen Person mittels elektronischen Zertifikats zuordnen lassen.

Die Sicherheit schwankt je nach Umgebung und Sorgfalt des Anwenders

Die tatsächliche Sicherheit dieser fortgeschrittenen Signatur hängt stark von der verwendeten Hard- und Software ab und nicht zuletzt auch von der Sorg-

Achtung: Nicht jede digitale Signatur ist auch rechtsgültig.

falt bei der Signaturerstellung durch den Anwender. Im Zweifel muss der Schlüsselinhaber beweisen, dass die Signatur tatsächlich in diesem Sinne sicher erzeugt wurde.

Nur die qualifizierte Signatur genügt wirklich den höchsten Sicherheitsanforderungen

Mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 SigG können Sie Dateien und Dokumente rechtssicher signieren. Nur diese Form der elektronischen Signatur erfüllt die höchsten Sicherheitsanforderungen des deutschen Signaturgesetzes und ist der eigenhändigen Unterschrift gleichgestellt.

Sie ist auch im elektronischen Rechtsverkehr zugelassen

Die verschlüsselten und mit qualifizierter elektronischer Signatur erstellten Dokumente sind eindeutig dem tatsächlichen Urheber zuzuordnen. Jede nachträgliche Veränderung der Daten wird erkannt. Die Vertraulichkeit und Echtheit der Dokumente im elektronischen Rechts- und Geschäftsverkehr sind gewährleistet.

Vertrauenswürdiger Zertifizierungsdiensteanbieter nach SignV

Basis ist das qualifizierte Zertifikat eines nach der Signaturverordnung vom November 2001 (SignV) geprüften Trust-Centers. Das Zertifikat belegt die Zusammengehörigkeit zwischen einem öffentlich bekannten Signaturprüfschlüssels und der Identität des Signaturschlüsselinhabers.

Führen Sie eine Vorabkontrolle durch!

Als Datenschutzbeauftragter haben Sie mit der betrieblichen Umsetzung zur Einführung einer elektronischen Signatur vermutlich weniger zu tun. Prüfen Sie aber im Rahmen der Vorabkontrolle folgende Punkte:

- ✔ **Rechtliches Umfeld prüfen:** Welche Verfahren und Dokumente erlauben digitale Unterschrift?
- ✔ **Akzeptanz des elektronischen Datenverkehrs prüfen:** Sind Ihre Kunden z.B. mit E-Faktura einverstanden?
- ✔ **Verfahren definieren – geeignetes Umfeld schaffen:**
  - gemeinsamen Standard bzw. Interoperabilität der Signaturkarte prüfen
  - Arbeitsplatzgestaltung (unbeobachtete PIN-Eingabe ermöglichen)
  - Vertretungsregelungen (mit eigener Signaturkarte)
  - Zeichnungsberechtigungen überprüfen
- ✔ **Aufklärung/Schulung/Betreuung prüfen:**
  - beteiligte Nutzer aufklären (rechtliche Konsequenzen/ Nichtabstreitbarkeit)
  - Abfolge erklären – Protokolldateien erläutern (für normale Nutzer nicht mehr durchschaubares Gebiet)
  - Support für die laufende Betreuung bereitstellen

Eliminieren Sie Schwachstellen

Um mögliche Schwachstellen bei der Umsetzung zu vermeiden, veranlassen Sie zudem entsprechende Organisationsanweisungen (siehe Kasten).

Hermann Keck

Hermann Keck ist externer Datenschutzbeauftragter (*http://www.keck-dsb.de*).

Wichtige Punkte für Organisationsanweisungen

Verhinderung von möglichen Schwachstellen in der praktischen Umsetzung:

- ✔ Signaturkarte sicher aufbewahren, um unbefugten Zugriff zu vermeiden
- ✔ Karte bei Verlassen des Arbeitsplatzes aus dem Kartenleser entnehmen
- ✔ PIN-Nummer nicht auf der Chipkarte notieren!
- ✔ Weitergabe verbieten (auch im Urlaubs- oder Vertretungsfall)
- ✔ Verantwortlichkeit bei unsachgemäßer Verwendung nicht abstreiten
- ✔ Unregelmäßigkeiten sofort melden:
  - plötzliche Änderung des Verfahrensablaufs
  - Verdacht auf Missbrauch durch Dritte
  - Verlust der Signaturkarte
  - vermuteter unautorisierter Einsatz
  - Verdacht, dass die Signaturkarte korrumpiert sein könnte
- ✔ Verfahren bei Ausscheiden eines Schlüsselinhabers festlegen
- ✔ privaten Einsatz der Signaturkarte regeln