

Signaturgesetz mit Tücken

Biometrie & Digitale Signatur

mag. iur. Maria Winkler
Advokatur SURY BRUN HOOL

Agenda

- Stand der Gesetzgebung
- Gleichstellung der digitalen Signatur mit der eigenhändigen Unterschrift?
- Haftung wofür?
- Digitale Signatur in der Praxis

Stand der Gesetzgebung

- EU- Richtlinie über fortschrittliche elektronische Signaturen 1999/93/EG
- ZertDV 2000
- BGES 2001
- ZertES 2001
(tritt voraussichtlich 2005 in Kraft)

ZertES

- Gleichstellung mit der eigenhändigen Unterschrift
- Haftungsfragen
- Anerkennung der Anbieterinnen von Zertifizierungsdiensten

Gleich?

- Die eigenhändige Unterschrift erzeugt ein individuelles Schriftbild, welches als Ausdruck der Persönlichkeit des Erklärenden mit diesem untrennbar verbunden ist
- Der private Schlüssel wird aber auf einem Datenträger (Smartcard) gespeichert, der nicht auf natürliche Weise mit dem Berechtigten verbunden ist
- Missbrauchspotenzial ist vorhanden!

Gleichstellung

- Wenn die Signatur die Voraussetzungen des ZertES aufweist, wird sie der eigenhändigen Unterschrift gleichgestellt
- Es wird nur die Zuordnung des Schlüssels zu einer bestimmten Person durch einen unabhängigen Dritten verlangt
- Es wird nicht anhand nicht übertragbarer (biometrischer) Merkmale überprüft, ob der tatsächlich Berechtigte den Schlüssel verwendet!

Die Folgen der Gleichstellung

- Verträge, die die eigenhändige Unterschrift verlangen, können neu auch elektronisch signiert werden
- Wegen des Prinzips der Formfreiheit (Art. 11 OR) können bereits heute die meisten Verträge gültig elektronisch abgeschlossen werden

Qualifizierte Schriftlichkeit

- Kennt das Gesetz einen **Formularzwang** (z.B. Mietzinserhöhung), dann liegt es an den Kantonen zu entscheiden, ob sie dieses Formular auch elektronisch zur Verfügung stellen wollen
- Die **Kantone** bestimmen, in welcher Weise auf ihrem Gebiet die öffentliche Beurkundung hergestellt wird

Tücken der Gleichstellung

- **Kantonale Unterschiede** im Bereich der qualifizierten Formvorschriften sind vorprogrammiert!
- Zudem führt die Gleichstellung mit der Handunterschrift **nicht** zu einer Verpflichtung auf elektronischem Wege Erklärungen entgegenzunehmen oder abzugeben!

Die Haftung (Art. 59a (neu) OR)

Der Inhaber des Signaturschlüssels haftet Dritten gegenüber für Schäden, die diese erleiden, weil sie sich auf das qualifizierte gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten verlassen haben

Die Haftung entfällt, wenn der Inhaber des Signaturschlüssels glaubhaft darlegen kann, dass er die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch des Signaturschlüssels zu verhindern

Der Bundesrat umschreibt die Sicherheitsvorkehrungen im Sinne von Absatz 2

Haftung wofür?

- Die missbräuchliche Verwendung des privaten Schlüssels erzeugt **keinen Vertrag** mit dem Inhaber des Schlüssels (keine Anscheinsvollmacht)!
- Wenn der Inhaber des Signaturschlüssels die **nötigen und zumutbaren** Sicherheitsvorkehrungen unterlässt, haftet er für den daraus entstehenden **Schaden** eines Dritten

Nötig und zumutbar?

- **Verordnung** betreffend der Sorgfaltspflicht des Inhabers des Signaturschlüssels muss erlassen werden
- Der Inhaber des Signaturschlüssels kann sich von seiner Haftung befreien, wenn er die Einhaltung dieser Sicherheitsvorkehrungen **glaubhaft machen** kann
- Der Beweis, dass das System als solches korrekt funktioniert hat, liegt weiter beim **Geschädigten**

Gültiges Zertifikat!

- Der Schlüsselinhaber haftet nur, wenn der Dritte sich auf ein **gültiges Zertifikat** verlassen hat
- Der Dritte muss somit die Gültigkeit bei Eingang einer Nachricht prüfen, damit er später evtl. Schadenersatzansprüche geltend machen kann!

Zusammenfassung

- Handunterschrift und digitale Signatur sind nicht gleich
- Die missbräuchliche Verwendung der digitalen Signatur führt nicht zu einem Vertrag mit dem Schlüsselinhaber
- In einer neuen Verordnung werden die Sorgfaltspflichten des Schlüsselinhabers geregelt
- Der Empfänger muss die Gültigkeit des Zertifikats überprüfen

Anerkennung der CA

- Natürliche oder juristische Personen, Verwaltungseinheiten des Bundes, der Kantone oder Gemeinden
- Anerkennung ist freiwillig!
- Mangels Schweizerischer CA werden zur Zeit die Zertifikate der TC Trust Center AG in Hamburg für Zwecke des E-Billings anerkannt

Elektronische Signatur in der Praxis

- Mehrwertsteuer (EIDI-V)
- Kaufmännische Buchführung (GeBüV)

Digitale Signatur und MwSt

- Die elektronische Übermittlung und Aufbewahrung von MwSt-relevanten Belegen ist zulässig (E-Billing)
- EIDI-V ist seit 2002 in Kraft

Archivierung von MwSt-Belegen

- Werden Belege gemäss EIDI-V nur mehr elektronisch erstellt und versandt, dann müssen diese zwingend vom Absender und vom Empfänger elektronisch archiviert werden

Beweiskraft

- Absicherung durch digitale Signatur
- gültiges Zertifikat
- Überprüfung der Daten durch Verifikation der digitalen Signatur
- Archivierung des öffentlichen Prüfschlüssels
- keine Pseudonyme
- kein Zweifel an der Sicherheit der Schlüssel im Zeitpunkt der Verwendung

Integrität

- EIDI-V verlangt den Einsatz der qualifizierten digitalen Signatur nach ZertDV
- ESTV anerkennt die Zertifikate der TC Trust Center AG in Hamburg, die bei der EAN in Basel bezogen werden können

Digitale Signatur und kaufmännische Buchführung

- Bücher, Buchungsbelege und die Geschäftskorrespondenz dürfen auch elektronisch geführt und aufbewahrt werden
- Die elektronisch geführten und aufbewahrten Dokumente haben dieselbe Beweiskraft wie Papierdokumente, wenn die Voraussetzungen der GeBüV erfüllt sind

Integrität

Art. 9 GeBüV verlangt bei einer Aufbewahrung auf veränderbare Informationsträgern die Sicherung durch

- technische Massnahmen (z.B. digitale Signatur)
- Zeitstempel
- korrekter Einsatz der technischen Verfahren
- Dokumentation der Abläufe (Logfiles)

Die Tücken der Gesetzgebung

- EIDI-V verlangt zwingend den Einsatz der **qualifizierten** digitalen Signatur
- GeBüV verlangt Sicherung der Integrität **z.B.** durch digitale Signatur
- Die Zertifikate der TC Trust Center AG werden ausschliesslich für Zwecke der EIDI-V ausgegeben und enthalten eine entsprechende **Nutzungsbeschränkung**

Die Sache mit dem Zeitpunkt

- Elektronisch übermittelte und aufbewahrte Dokumente haben dieselbe Beweiskraft wie Papierdokumente, wenn die verwendeten Schlüssel **im Zeitpunkt der Speicherung sicher** waren (EIDI-V)
- Im Zweifelsfall muss der Steuerpflichtige die Beweise erbringen
- Zeitstempeldienste müssen zusätzlich eingesetzt werden!

Signaturerneuerung

- Wer Dokumente gemäss EIDI-V oder GeBüV elektronisch archiviert, muss deren **Integrität** und **Verfügbarkeit** während der gesamten Aufbewahrungsdauer sicherstellen
- Was passiert, wenn die digitale Signatur wegen der höheren Rechnerleistungen nicht mehr sicher ist?

Nachweis wovon?

- Der Zeitstempel beweist, dass ein Dokument zu einem bestimmten Zeitpunkt **existiert** hat
- Der Zeitstempel beweist **nicht** den Zeitpunkt des Entstehens von Daten!

Massensignaturen

- Einsparungspotenzial bei E-Billing und elektronischer Archivierung schwindet, wenn jeder einzelne Beleg durch Eingabe des PIN-Code signiert werden muss
- Sind Massensignaturen zulässig?

Fazit – Es gibt noch zu tun!

- Das ZertES wird Anfang 2005 in Kraft treten
- Fragen wie die Erneuerung von unsicher gewordenen Signaturen, die Zulässigkeit von Massensignaturen, etc. werden die Techniker und die Juristen noch beschäftigen
- Ein Blick über die Grenzen zeigt, dass die Probleme lösbar sind!

Literaturangaben

- Simon Schlauri, Elektronische Signaturen, Schulthess 2002
- Felix Schöbi, Zivilrechtliche Aspekte des Internets, in: Jusletter 1. März 2004
- Detlef Hühnlein, Yvonne Knosowski, Aspekte der Massensignatur (www.secunet.de)
- Signaturerneuerung : www.archisig.de

Ich danke für
Ihre Aufmerksamkeit !

HINWEISE AUF PUBLIKATIONEN

www.advokatinnen.ch

mag. iur. Maria Winkler
Advokatur SURY BRUN HOOL
Frankenstrasse 12
6002 Luzern