

## **Das Gesetz: Bundesgesetz über die elektronische Signatur – Die elektronische Unterschrift kommt sicher?!**

Am 1. Januar 2005 ist das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES) und die ausführende Verordnung des Bundesrates (VZertES) in Kraft getreten.

Mit der Einführung des Gesetzes und der damit verbundenen Anpassungen des Obligationenrechts (OR) hat der Gesetzgeber die qualifizierte elektronische Signatur, die auf einem qualifizierten Zertifikat beruht, der eigenhändigen Unterschrift gleichgestellt, sofern die Anbieterin des Zertifikates über eine Anerkennung nach dem ZertES verfügt.

Zum jetzigen Zeitpunkt fehlt es noch an anerkannten Anbieterinnen. Die Swisscom Solutions, die Genfer Ofac Group und die Zürcher Swiss Sign bemühen sich um die Anerkennung. Mit der ersten Anerkennung und dem Einsatz der ersten qualifizierten Zertifikate ist nicht vor Winter 2005 zu rechnen.

Die folgenden Ausführungen geben einen kurzen Überblick über die Funktionalität und den Zweck der elektronischen Signatur, den Inhalt des ZertES sowie eine Betrachtung der Auswirkungen auf den eCommerce.

### **Der Ablauf – kurz erklärt**

Jeder, der Mitteilungen signiert, besitzt einen geheimen Signierschlüssel und einen öffentlichen Schlüssel. Die Kombination des Signierschlüssels mit dem Hashwert des zu „signierenden“ Dokuments ergeben eine digitale Signatur. Ändert das Dokument, ändert auch die Signatur.

Mit dem öffentlichen Schlüssel des Absenders kann der Empfänger die Signatur auf ihre Echtheit prüfen. Das übermittelte digitale Zertifikat bestätigt, dass der Prüfschlüssel zu einer bestimmten Person gehört. Das Zertifikat wird von einem vertrauenswürdigen Dritten (Zertifizierungsdiensteanbieter) ausgestellt.

### **Was bezweckt die zertifizierte elektronische Signatur?**

Die elektronische Signatur bezweckt die Integrität und Authentizität. Dem Empfänger der Nachricht wird bestätigt, dass die Mitteilung von einer bestimmten Person kommt und nicht durch einen Dritten abgeändert wurde. Nicht abgedeckt wird die Vertraulichkeit. Elektronisch signierte E-Mails sind nicht per se verschlüsselt. Elektronisch signierte E-Mail sind daher generell für Unbefugte einsehbar.

Die (theoretischen) Einsatzmöglichkeiten der elektronischen Signatur sind mannigfaltig:

- es können rechtsverbindliche elektronische Dokumente versendet werden
- überall wo eine Authentifizierung verlangt wird, kann dies über die elektronische Signatur geschehen (z.B. eBanking, Erwachseneninhalte im Internet)
- Rechtsverkehr mit und zwischen den Behörden

## **Inhalt des Bundesgesetzes über die elektronische Signatur**

Das ZertES definiert die Voraussetzungen, unter denen Anbieterinnen von Zertifizierungsdiensten anerkannt werden können und regelt ihre Tätigkeiten im Bereich der elektronischen Zertifikate (Art. 3 ff. ZertES). Zudem bestimmt das Gesetz die Bedingungen, die eine elektronische Signatur erfüllen muss, um dieselbe Wirkungen wie eine handschriftliche Unterschrift erzielen zu können (Art. 7 ZertES). Ebenso regelt es die Verantwortung der Anbieterinnen von Zertifizierungsdiensten, der Anerkennungsstellen und der Inhaber von Signaturschlüsseln in Missbrauchsfällen (Art. 16 ff. ZertES).

Wichtig sind auch die im **Anhang** zum Gesetz aufgeführten Änderungen des bisherigen Rechts. So wird insbesondere der allgemeine Teil des Obligationenrechts (OR) um zwei zu erläuternde Artikel ergänzt.

## **Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift**

Artikel 14 Abs. 2bis OR stellt die elektronische Signatur der eigenhändigen Unterschrift gleich.

Art. 14 Abs. 2bis OR

*Der eigenhändigen Unterschrift gleichgestellt ist die qualifizierte elektronische Signatur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes über die elektronische Signatur vom 19. Dezember 2003 beruht. Abweichende gesetzliche oder vertragliche Regelungen bleiben vorbehalten.*

Verträge, für die von Gesetzes wegen die Einhaltung der einfachen Schriftform (eigenhändige Unterschrift) vorausgesetzt wird, können nun auch elektronisch abgeschlossen werden (Bsp. die Abtretung einer Forderung).

Den Vertragsparteien steht es zudem offen, für Verträge, die an sich „formfrei“ (mündlich, per unsigniertem E-Mail etc.) abgeschlossen werden könnten, die einfache Schriftform als Voraussetzung zum Vertragsabschluss zu vereinbaren (Art. 16 Abs. 2 OR). Das vertraglich vereinbarte Erfordernis der einfachen Schriftform könnte mit elektronisch signierten Dokumenten eingehalten werden.

## **eCommerce und elektronische Signatur**

Die Bedeutung der Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift ist in Bezug auf den eCommerce zu relativieren.

Für die im Internet üblichen und relevanten Kauf-, Miet-, Dienstleistungs- und Lizenzverträge sieht das Gesetz kein besonderes Formerfordernis vor. Der Grossteil der Internetverträge kann ohne Unterschrift und demnach auch ohne elektronische Signatur gültig abgeschlossen werden.

Der Einsatz der elektronischen Signatur wird in den Fällen Sinn machen, in denen der Internet-Anbieter zwingend wissen muss, mit wem er es zu tun hat (z.B. Angebote für Erwachsene; Identifizierung zur Eröffnung eines Bankkontos etc.)

Abgesehen von der Tatsache, dass es noch keine anerkannten Zertifizierungsdiensteanbieter auf dem Markt gibt und die Internetverträge grundsätzlich ohne Unterschrift abgeschlossen werden können, gibt es weitere Hindernisse für einen Durchbruch der elektronischen Signatur im Bereich B2C, z.B. die Anschaffung der notwendigen aber wenig vertrauten Technologien (SmartCard), das Identifikationsprozedere, der zu erwartende hohe Preis für digitale Zertifikate der anerkannten Anbieterinnen etc.

## **Wer haftet bei Missbrauch des Signaturschlüssels?**

**Art. 59a OR** erklärt den Inhaber eines Signaturschlüssels für haftbar, wenn dieser den Missbrauch seines Signaturschlüssels verantworten muss.

Art. 59aOR

### *F. Haftung für Signaturschlüssel*

*<sup>1</sup>Der Inhaber eines Signaturschlüssels haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich auf das qualifizierte gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes über die elektronische Signatur vom*

*19. Dezember 2003 verlassen haben.*

*<sup>2</sup>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.*

*<sup>3</sup>Der Bundesrat umschreibt die Sicherheitsvorkehrungen im Sinne von Absatz 2.*

Der Inhaber des Signaturschlüssels haftet nicht kausal. Der geschädigte Dritte (z.B. eShop-Betreiber, Bank) muss ein Verschulden des Schlüsselinhabers beweisen. Dem Geschädigten kommt die Regelung insoweit entgegen, als die Beweislast für den geforderten sorgfältigen Umgang mit dem Signaturschlüssel beim Inhaber liegt. Dem Inhaber reicht jedoch die Glaubhaftmachung, dass die vom Gesetz und von der Verordnung geforderten Sicherheitsvorkehrungen getroffen wurden. Die Verordnung sieht in Art. 11 insb. vor, dass der Inhaber eines qualifizierten Zertifikats die Signaturerstellungseinheit keiner anderen Person anvertrauen darf. Er muss diese, soweit zumutbar, auf sich tragen oder wegschliessen. Im Falle des Verlusts oder Diebstahls der Signaturerstellungseinheit ist der Inhaber des qualifizierten Zertifikats verpflichtet, so rasch wie möglich dessen Ungültigerklärung zu beantragen.

In der Praxis wird diese (nicht zwingende) gesetzliche Regelung in vielen Fällen durch eine vertragliche Risikoverteilung abgelöst werden. Ein Anbieter wird Fälschungs- und Missbrauchsrisiken im Rahmen des gesetzlich Möglichen auf den Kunden (Inhaber des Signaturschlüssels) abwälzen und nur mehr für sorgfältige Legitimationsprüfung und Risikoaufklärung einstehen.