



Digitale Signatur und Revisionsicherheit

Die kommerzielle Nutzung des Internet brachte nicht nur neue Herausforderungen an die Technik. Sie warf auch Fragen auf, welche den Gesetzgeber dazu zwangen, vorhandene rechtliche Grundlagen der technischen Entwicklung anzupassen oder unter Beachtung der Besonderheiten des Internet korrekt anzuwenden. Für einen Grossteil der Verträge jedoch, welche heute über das Internet abgeschlossen werden (z.B. Kauf- oder Lizenzvertrag etc.) bestehen keine gesetzlichen Formvorschriften. Sie können sowohl mündlich als auch übers Internet gültig abgeschlossen werden. Hier ist also der Einsatz der Digitalen Signatur unnötig. Ausnahmen bestehen nur bei gesetzlichen oder vertraglichen Formvorschriften. Wie kann beispielsweise die elektronische Bewirtschaftung des Belegwesens gestaltet werden? Welche technischen Vorkehrungen sind zu treffen, um den gesetzlichen Vorgaben zu genügen?

* Maria Winkler

Es ist anzunehmen, dass mit der Diskussion um die Anerkennung der Digitalen Signatur die Frage angesprochen wurde, ob man mit dem digitalen Dokument auch beweisen kann, dass man einen Vertrag mit einem bestimmten Inhalt abgeschlossen hat. Hier herrschte lange Zeit grosse Unsicherheit.

Da die Technik wieder einmal der Gesetzgebung einige Schritte voraus war, fehlten zunächst nicht nur Normen sondern auch anerkannte Lehrmeinungen, welche sich häufig erst

ordnung geschaffen, sondern nur die bestehende Rechtsordnung sinngemäss angewandt werden muss.

Digitale Signatur in der Rechtsordnung

Kurz nachdem die EU die Richtlinie über gemeinschaftliche Rahmenbedingungen der elektronischen Signatur erliess, kam in der Schweiz die Forderung nach Anerkennung gemäss dem Vorbild der EU auf, da

man im für den Wirtschaftsstandort Schweiz Wettbewerbsnachteile befürchtete. Der Schweizerische Gesetzgeber reagierte rasch. Bereits im April 2000 erliess er die sogenannte Zertifizierungs-

Dienste-Verordnung (ZertDV). Diese regelt die Voraussetzungen für die freiwillige Anerkennung von Zertifizierungsdiensten (CAs) und ist die zur Zeit gültige gesetzliche Regelung in Bezug auf die Digitale Signatur.

Bereits am 17. Januar 2001 lag der Entwurf des Bundesgesetzes über die elektronische Signatur (BGES) vor. Nach der Vernehmlassungsfrist wurde im Juni 2001 die Botschaft zum Bundesgesetz über die Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) erlassen. Diese wurde nun im Juni 2003 vom Nationalrat Erstrat und kürzlich im Ständerat behandelt. Man rechnet allerdings nicht damit, dass das Gesetz vor Anfang 2005 in Kraft treten wird.

Was regelt das ZertES?

Das Bundesgesetz über die Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) regelt die Anerkennung von Zertifizierungsdienst-Anbietern (CA) sowie die Gleichstellung der Digitalen Signatur mit der eigenhändigen Unterschrift.

Soll die Digitale Signatur der Handunterschrift in ihren rechtlichen Auswirkungen gleichgestellt werden, so bedarf es der Mitwirkung von "vertrauenswürdigen Dritten",

Es ist nicht zu erwarten, dass in Zukunft Konsumenten, welche über das Internet CDs und Bücher kaufen, digitale Signaturverfahren anwenden.

auf der Basis von Bundesgerichtsurteilen bilden. Fundierte Publikationen zu diesen grundlegenden Fragen, haben bald einmal zur allgemeinen Überzeugung beigetragen, dass für den elektronischen Geschäftsverkehr keine neue Rechts-

die ähnlich einem Passamt die Zugehörigkeit eines öffentlichen Schlüssels zu einer bestimmten natürlichen Person bestätigen. Diese Aufgabe wird von den Zertifizierungsdienste-Anbietern (CAs) wahrgenommen, welche die Identität des Antragstellers überprüfen, indem dieser persönlich vor der CA erscheint und sich mittels ID oder Reisepass ausweist.

Das ZertES sieht vor, dass natürliche oder juristische Personen und Verwaltungseinheiten des Bundes, der Kantone und der Gemeinden als CA tätig werden können. Ob eine CA die Voraussetzungen erfüllt, wird von einer Anerkennungsstelle des Bundes überprüft. Eine Anerkennung ist für eine CA jedoch freiwillig, weshalb sich keine CA strafbar macht, wenn sie Zertifizierungsdienste anbietet, ohne vorher um Anerkennung gemäss ZertES nachgesucht zu haben. Aber nur Digitale Signaturen, die auf einem Zertifikat einer anerkannten CA beruhen – so genannte qualifizierte Zertifikate – entfalten die gesetzlichen Rechtswirkungen betreffend Gleichstellung mit der eigenhändigen Unterschrift, Haftung etc.

Gleichstellung der Digitalen Signatur

Mit dem ZertES soll ein neuer Artikel 14 Absatz 2 ins Obligationenrecht eingefügt werden, wonach in Zukunft Willenserklärungen, für welche das Gesetz die einfache Schriftform verlangt, auch auf elektronischem Weg abgegeben werden können, wenn sie die Digitale Signatur im Sinne des ZertES aufweisen.

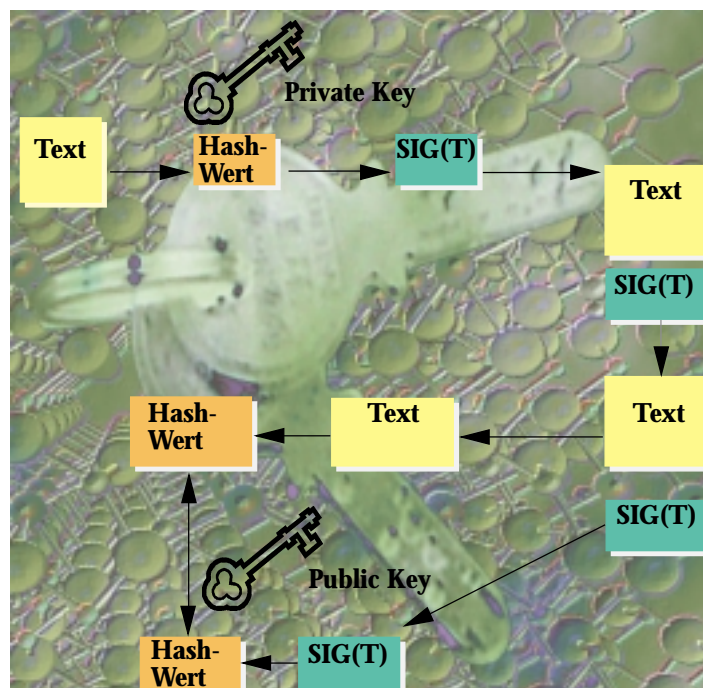
Einfache Schriftlichkeit bedeutet, dass ein Dokument die eigenhändige Unterschrift der Parteien enthalten muss, welche aus diesem Dokument verpflichtet werden. Heute kann diese eigenhändige Unterschrift nur ausnahmsweise durch mechanische Nachbildungen ersetzt werden.

In der Schweizerischen Privatrechtsordnung herrscht der Grundsatz der Privatautonomie. Die Parteien können ihre rechtlichen Beziehungen zueinander so gestalten, wie sie es für richtig finden, sofern sie nicht gegen zwingende gesetzliche Normen, welche die Ausnahme darstellen, verstossen. Ein Teil der Privatautonomie ist die sogenannte Formfreiheit. Die Parteien müssen im Rahmen des Privatrechts Formvorschriften nur dann einhalten, wenn das Gesetz oder eine Parteienvereinbarung dies ausdrücklich vorseht. Ansonsten können Verträge jederzeit gültig formfrei und somit auch über Internet abgeschlossen werden. In der Praxis wird sich Art. 14 Abs. 2 (neu) OR somit nur auf die Vertragsverhältnisse auswirken, bei denen das Gesetz oder die Parteienvereinbarung Schriftlichkeit ausdrücklich vorsehen.

Haftungsfragen

Das ZertES sieht eine milde Kausalhaftung mit Beweislastumkehr für die CA vor. Das bedeutet, dass bei Eintreten eines Schadens grundsätzlich eine Pflichtverletzung durch die CA vermutet wird und sie sich von der Haftung nur dann befreien kann, wenn sie beweist, dass sie allen ihren gesetzlichen Pflichten nach ZertES nachgekommen ist.

Das Ablaufschema der Verschlüsselung: Der private Schlüssel wird zur Verschlüsselung einer Nachricht verwendet, der öffentliche Schlüssel dient ausschliesslich der Entschlüsselung einer erhaltenen Nachricht und passt nur zu einem bestimmten privaten Schlüssel.



Praxisrelevanz

Die vorhergehenden Überlegungen haben gezeigt, dass die Anerkennung der Digitalen Signatur nur in Ausnahmefällen (in denen das Gesetz die einfache Schriftlichkeit verlangt) nötig ist, um in Zukunft gültige Verträge über das Internet abzuschliessen zu können.

Zudem wird das neue ZertES auch an den vorhandenen Beweisregeln nichts ändern. Elektronische Dokumente sind Gegenstand eines sogenannten Augenscheinbeweises. Ein elektronisches Dokument, welches mit einer Digitalen Signatur versehen ist, wird dabei eine erheblich grössere Beweiskraft haben als eines, das ohne eine solche technische Sicherungsmassnahme versandt worden ist. Ob die Verwendung einer qualifizierten Digitalen Signatur nach ZertES dabei eine im Vergleich zu einer von einer nicht anerkannten CA stammenden Digitalen Signatur erhöhte Beweiskraft haben wird, bleibt abzuwarten.

Funktionsweise der Digitalen Signatur:

Aus dem ursprünglichen Text wird mit Hilfe eines speziellen Verfahrens ein so genannter "Hashwert", eine Art Komprimat des Textes, gebildet. Nur der Hashwert wird nun mit Hilfe des privaten Schlüssels verschlüsselt. Es entsteht Sig (T).

Sig (T) wird an den ursprünglichen Text gehängt und versandt. Der Empfänger bildet einerseits einen Hashwert aus dem Text und andererseits entschlüsselt er mit dem öffentlichen Schlüssel Sig (T). Daraus entsteht der entschlüsselte Hashwert.

Sind beide Hashwerte identisch, ist die Identität des Absenders bezeugt und der Empfänger kann sicher sein, dass die Information während der Übermittlung nicht verändert wurde.

Mit Hilfe der Digitalen Signatur kann somit einerseits die Identität des Verfassers nachgewiesen und andererseits die Authentizität des elektronischen Dokuments sichergestellt werden. Ein mit einer Digitalen Signatur versehener Text ist allerdings nicht verschlüsselt, im Sinn beispielsweise einer SSL-Verschlüsselung. Will man den gesamten Text geheim halten, muss noch zusätzlich ein weiteres Verschlüsselungsverfahren verwendet werden.

Revisionsicherheit

Obwohl das ZertES grundsätzlich nur Fragen des Privatrechts regelt und den elektronischen Behördenverkehr (e-Government) nur am Rande berührt (z. B. Handelsregister), wird allgemein erwartet, dass die Gleichstellung der Digitalen Signatur mit der eigenhändigen Unterschrift den Grundstein für die vereinfachte Kommunikation mit den Behörden legen wird.

Der Gesetzgeber hat z.B. sowohl im Steuerrecht (MwSt) als auch im Handelsrecht (GeBüV) die Verwendung von digitalen Signaturverfahren vorgesehen. So konnten der Vorsteuerabzug sowie die Steuerbefreiung bei der Mehrwertsteuer bis zum Inkrafttreten des neuen Mehrwertsteuergesetzes (MwStG) am 01.01.2001 nur geltend gemacht werden, wenn der Anspruch mittels Rechnungen in Papierform nachgewiesen wurde. Solche fehlen aber, wenn beispielsweise ein ausländischer Kunde vom Server des schweizerischen Anbieters Software bezieht und mit Kreditkarte bezahlt. Das neue Mehrwertsteuergesetz ist auf die neue technische Entwicklung bereits eingegangen und ermöglicht es in Zukunft, die entsprechenden Belege auch elektronisch zu übermitteln und aufzubewahren. Die dazu gehörende Verordnung über elektronisch übermittelte Daten und Informationen (EIDI-V) des Eidg. Finanzdepartements ist am 01. März 2002 in Kraft getreten. Die Beweiskraft elektronischer Dokumente ist nach Art. 3 der EIDI-V erfüllt, wenn die Übermittlung und die Aufbewahrung von Da-

Integrität

Die Gewährleistung der Integrität elektronischer Daten ist ein wichtiges Element in der IT-Governance mit angemessenen IT-Sicherheitsstandards. Ganz allgemein erhöht dies den Bedarf an vertrauenswürdiger Hardware und den Einsatz von Verschlüsselungsalgorithmen, um die Authentizität und Integrität der Datenübermittlung und -verwahrung sicherzustellen. Aus informationstechnischer Sicht spielen folgende Bestandteile eines IT-Governance-Konzepts eine wesentliche Rolle:

- Verfügbarkeit der Daten
- Integrität der Datenbearbeitung
- Prüfbarkeit von Daten und Vorfällen
- Lückenlosigkeit und Verbindlichkeit der Datenverwahrung
- Vertraulichkeit der Daten bzw. kontrolliertes Bekanntgabekonzept (Zugangskontrollen).

Kasten *Maria Winkler

ten mittels Digitaler Signatur abgesichert ist. Da es in der Schweiz zur Zeit keine CA gibt, werden von der Eidgenössischen Steuerverwaltung (ESTV), gestützt auf Art. 12 Abs. 2 EIDI-V, seit Dezember 2002 Zertifikate der TC Trust Center AG mit Sitz in Hamburg anerkannt. Alle in der Schweiz ansässigen Unternehmen können ein solches Zertifikat bei der EAN Schweiz beantragen, das aber von der ESTV ausschliesslich für diesen Zweck anerkannt wird. Die Zertifikate können nicht für andere Zwecke (z.B. für Secure Email) genutzt werden. Seit 01. Juni 2002 die Verordnung über die Führung und Aufbewahrung von Geschäftsbüchern (GeBüV) in Kraft getreten

ist, ist die elektronische Verwahrung von Belegen grundsätzlich zulässig.

Gemäss GeBüV können zur Archivierung auch veränderbare Informationsträger verwendet werden, deren gespeicherte Daten geändert oder gelöscht werden können, ohne dass die Änderung oder Löschung auf dem Informationsträger nachweisbar ist. Dabei muss jedoch die Integrität der gespeicherten Information beispielsweise durch den Einsatz von digitalen Signaturverfahren gewährleistet werden, der Zeitpunkt der Speicherung der Information (z.B. Zeitstempel) nachweisbar sein, die Vorschriften über den Einsatz der betreffenden technischen Verfahren eingehalten sowie die Abläufe und Verfahren dokumentiert werden.

Die Bestimmung GeBüV verweist allgemein auf die Digitale Signatur, ohne ausdrücklich auf das ZertDV Bezug zu nehmen. Da es zur Zeit keine schweizerische CA gibt und sich die Anerkennung der TC Trust Cen-

ter AG ausdrücklich nur auf den Anwendungsbereich der EIDI-V bezieht, ist die Anwendungsmöglichkeit der Digitalen Signatur im Bereich der Archivierung nach GeBüV unklar.

Der Gesetzgeber (Kantone und Bund) hat es somit versäumt, die Voraussetzungen der Anwendbarkeit der Digitalen Signatur im Handelsrecht und im Steuerrecht gleich zu regeln, was zu Unklarheiten in einem neuen und daher an und für sich noch mit grossen Unsicherheiten belasteten Gebiet führt.

Ausblick

Es ist nicht zu erwarten, dass in Zukunft Konsumenten, welche über das Internet CDs, Bücher oder Fanartikel ihres Superstars erwerben wollen, vermehrt interessiert sein werden, digitale Signaturverfahren anzuwenden.

Vielmehr kann damit gerechnet werden, dass mit Inkrafttreten des ZertES die Möglichkeiten, mit Behörden über das Internet zu kommunizieren, vielfältiger werden. Man rechnet hier mit einem grossen Einsparpotential für Unternehmen auf Grund der rascheren und dadurch billigeren Kommunikationsmöglichkeit.

Wie so oft bringt die neue gesetzliche Lösung aber auch neue Probleme. Dem grossen Einsparpotenzial stehen beispielsweise hohe Prozesskosten gegenüber, wenn für die Erzeugung jeder einzelnen Signatur ein PIN-Code eingegeben werden muss. Es muss somit ein Weg gefunden werden, um die Signaturen massenhaft zu erzeugen, um die Einsparungen auch realisieren zu können. Ob das ZertES alle Fragen, die sich dabei stellen werden auch lückenlos löst, ist anzuzweifeln.

Grundsätzlich kann davon ausgegangen werden, dass digitale Signaturverfahren technisch ausgereift und wirtschaftlich effizient sind. Welche rechtlichen Probleme mit dem Einsatz der Digitalen Signatur noch auf uns zukommen werden, bleibt abzuwarten.