

Digitale Signatur

Nutzen und Risiko für KMU

Allgemeines

Die kommerzielle Nutzung des Internet als neuen Vertriebskanal sowohl zwischen zwei Unternehmen (B2B) als auch zwischen Unternehmen und Konsumenten (B2C) brachte nicht nur neue Herausforderungen an die Technik, sondern warf auch Fragen auf, welche den Gesetzgeber dazu zwangen, die vorhandenen rechtlichen Grundlagen an die technische Entwicklung anzupassen. In anderen Fragen ist nur die korrekte Anwendung der vorhandenen Rechtsnormen unter Beachtung der Besonderheiten des Internet erforderlich.

Der Gesetzgeber ist dabei in besonderer Weise gefordert. Einerseits muss er sich intensiv mit der technischen Entwicklung auseinandersetzen und eventuelle neue Normen so formulieren, dass nicht der nächste Schritt in der technischen Entwicklung die Notwendigkeit des Erlasses neuer Normen nach sich zieht. Andererseits ist das Denken in nationalen Dimensionen in diesem Bereich verfehlt und behindert die optimale Nutzung dieses Vertriebsweges und benachteiligt die eigene Wirtschaft.

Einige Zeit hielt sich recht nachdrücklich das Gerücht, dass das Internet ein rechtsfreier Raum sei. Spätestens ab dem Zeitpunkt, in dem sich der Handel über das Internet zu intensivieren begann, stellte man aber mit Erleichterung fest, dass dies nicht der Fall ist und in der „New Economy“ die selben Rechtsnormen gelten, wie in der „Old Economy“. Der Ruf nach mehr Rechtssicherheit durch die Schaffung einheitlicher, über die nationalen Grenzen hinausgehender Normen wurde laut.

Ein technisches Verfahren, welches bereits seit längerer Zeit auf dem Markt erhältlich ist und auch insbesondere von Banken erfolgreich eingesetzt wird, ist die sogenannte digitale Signatur. Da sie ermöglicht, den Absender einer Nachricht zu identifizieren und sicherzustellen, dass der Inhalt einer Nachricht auf ihrem Weg von A nach B nicht verändert wurde, wurde sie alsbald als „der Weg“ gehandelt, um im Internet Rechtssicherheit zu schaffen.

Die EU erliess im Jahr 1999 die Richtlinie über fortgeschrittene elektronische Signaturen, welche die Mitgliedsstaaten noch vor dem 19. Juli 2001 in ihren nationalen Rechtsordnungen umsetzen müssen. Die schweizerische Wirtschaft befürchtete einen Wettbewerbsnachteil für den Wirtschaftsstandort Schweiz und trat deswegen mit der Forderung nach Anerkennung der digitalen Signatur nach dem Vorbild der EU an den Gesetzgeber heran.

Die Zertifizierungsdienstverordnung (ZertDV)

Der Schweizerische Gesetzgeber reagierte relativ rasch und erliess bereits im April 2000 die sogenannte Zertifizierungsdienstverordnung (ZertDV), welche die Anerkennung der Anbieterinnen von Zertifizierungsdiensten regelt. Sie war zum vornherein als Versuchsverordnung konzipiert und zeitlich befristet bis zum Inkrafttreten einer entsprechenden gesetzlichen Regelung, längstens aber bis zum 31. 12. 2009.

Das Bundesgesetz über die elektronische Signatur (BGES)

Bereits im Januar 2001 wurde der Entwurf über das sogenannte „Bundesgesetz über die elektronische Signatur“ (BGES) in die Vernehmlassung geschickt, welches die ZertDV ablösen soll. Das BGES bietet eine gesetzliche Grundlage für die Anerkennung der AnbieterInnen von Zertifizierungsdiensten und regelt ausserdem die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift sowie Fragen des elektronischen Geschäftsverkehrs mit Registern.

Die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift

An dieser Stelle soll zunächst die Bedeutung der Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift erörtert werden.

Das BGES sieht vor, den neuen Art. 15a ins OR einzufügen. Nach dieser Bestimmung können zukünftig alle Willenserklärungen, für welche das Gesetz die einfache Schriftform verlangt, auch auf elektronischem Weg abgegeben werden, wenn sie eine elektronische Signatur im Sinne des BGES aufweisen.

Der Begleitbericht zum Entwurf des BGES¹ besagt, dass der Empfänger einer solchen Willenserklärung zusätzlich in der Lage sein muss, diese entgegenzunehmen und seine Bereitschaft, am elektronischen Geschäftsverkehr teilzunehmen, kundgetan haben muss.

Um die Tragweite dieser Neuregelung verstehen zu können, benötigt der juristische Laie allerdings einige Grundinformationen darüber, welche Voraussetzungen für einen gültigen Vertragsabschluss nach OR überhaupt gegeben sein müssen.

- Neben bestimmten Eigenschaften, welche die beteiligten Parteien aufweisen müssen (z. B. Handlungsfähigkeit, etc) verlangt Art. 1 OR für das Zustandekommen eines Vertrages gegenseitige übereinstimmende Willenserklärungen.
- Diese entfalten ihre Wirksamkeit erst, wenn sie der jeweils anderen Partei zugegangen sind.
- Das schweizerische Vertragsrecht beruht auf dem Prinzip der Vertragsfreiheit. Ein Teil dieser Vertragsfreiheit ist die Formfreiheit nach OR 11 Abs. 1. Verträge bedürfen nur dann einer bestimmten Form, wenn es im Gesetz ausdrücklich vorgesehen ist. Zudem steht es den Parteien frei, die Einhaltung einer bestimmten Form zu vereinbaren.

Das Gesetz kennt verschiedene Arten von Formvorschriften:

- Die einfache Schriftform verlangt für die Gültigkeit des Vertrages die eigenhändige Unterschrift derjenigen Parteien, welche aus dem Vertrag verpflichtet werden.
- Die qualifizierte Schriftform verlangt zusätzlich, dass bestimmte Teile des Vertrages von Hand geschrieben sind.
- Die öffentliche Beurkundung setzt zwingend das Mitwirken einer Urkundsperson am Entstehen des Vertrages voraus.

Die Praxisrelevanz der Anerkennung der digitalen Signatur

Mit dem neuen Art. 15a E-OR wird die dem BGES entsprechende digitale Signatur der eigenhändigen Unterschrift gleichgestellt. Somit können nach Inkrafttreten dieses Gesetzes alle Verträge, welche die einfache Schriftform verlangen, auch digital signiert werden.

Die qualifizierte Schriftform und die öffentliche Beurkundung können allerdings durch die digitale Signatur nicht ersetzt werden.

Allerdings können aufgrund der oben erwähnten Formfreiheit nach OR 11 Abs. 1 bereits heute der Grossteil aller Verträge, welche hauptsächlich über das Internet abgeschlossen werden (dazu zählen vor allem der Kaufvertrag, der Auftrag und der Werkvertrag), formfrei und somit gültig auch über das Internet abgeschlossen werden.

Digitale Urkunden sind bereits heute als Beweismittel zugelassen und digital signierte Dokumente nach BGES werden von Gesetzes wegen keinen höheren Beweiswert haben als solche ohne digitale Signatur. In beiden Fällen unterliegen die Dokumente der freien richterlichen Beweiswürdigung. Es ist aber zu erwarten, dass ein Richter eher geneigt sein wird, Dokumenten, welche mit einer digitalen Signatur nach BGES versehen sind, einen höheren Beweiswert zuzumessen als solchen ohne digitale Signatur.

¹ Sie finden den Begleitbericht auf der Website des Bundesministeriums für Justiz unter

Den grössten Vorteil der neuen gesetzlichen Regelung erwartet man aber allgemein in der vereinfachten und effizienteren Kommunikation mit den Behörden. Obwohl das BGES 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.

Dazu einige Beispiele:

- Der Vorsteuerabzug sowie die Steuerbefreiung bei der Mehrwertsteuer² können nach heutiger Rechtslage nur geltend gemacht werden, wenn der Anspruch mittels Urkunden nachgewiesen wird. Urkunden sind aber Schriftstücke, digitale Dokumente gelten nicht als Urkunden im Sinne des ZGB.
- Solche fehlen aber, wenn beispielsweise ein ausländischer Kunde vom Server des schweizerischen Anbieters Software bezieht und mit Kreditkarte bezahlt. Das Anfang dieses Jahres in Kraft getretene Mehrwertsteuergesetz ist auf die neue technische Entwicklung bereits eingegangen und ermöglicht es in Zukunft, die entsprechenden Belege auch elektronisch einzureichen. Allerdings fehlen noch die nötigen Ausführungsbestimmungen des Eidg. Finanzdepartements. Sobald diese aber vorliegen, können in Zukunft Rechnungen und andere Belege im Zusammenhang mit der Mehrwertsteuer auch anhand von elektronischen Dokumenten vorgelegt werden.

Ein weiteres Beispiel:

- Vertragsabschlüsse über das Internet sind, wie erwähnt, auch ohne die Anerkennung der digitalen Signatur bereits jetzt gültig und durchsetzbar. Ergeben sich aus einer solchen Geschäftsbeziehung allerdings rechtliche Probleme, beispielsweise durch einen zahlungsunwilligen Kunden, ist dem Gläubiger die Einreichung eines provisorischen Rechtsöffnungsgesuchs verwehrt. Dazu bedarf

www.bj.admin.ch unter der Rubrik Vernehmlassungen.

² Siehe dazu Roger M. Cadosch, Die digitale Signatur im Mehrwertsteuerrecht und die Auswirkungen auf den Electronic Commerce, in: Jusletter 5. Februar 2001, zu finden unter www.weblaw.ch

es nach der heutigen Rechtslage einer unterzeichneten Schuldanererkennung. Ein bloss auf elektronischem Wege abgeschlossener Vertrag (ob mit oder ohne digitale Signatur) erfüllt diese Voraussetzung nicht.

Hier muss der Gesetzgeber somit noch einiges an Arbeit leisten, um im Verkehr zwischen den Bürgern und den Behörden eine effiziente Form der elektronischen Kommunikation zu etablieren. Nicht zu vergessen sind natürlich auch die finanziellen Aufwendungen, welche in diesem Zusammenhang notwendig sein werden.

Die Anerkennung der AnbieterInnen von Zertifizierungsdiensten

Damit die digitale Signatur die Authentizität und die Integrität elektronischer Dokumente garantiert, bedarf es der Mitwirkung von „vertrauenswürdigen Dritten“, welche bestätigen, dass ein öffentlicher Prüfschlüssel einer bestimmten natürlichen Person zugeordnet werden kann. Diese Rolle übernehmen die AnbieterInnen von Zertifizierungsdiensten (sogenannte Certification Authorities oder CA's).

Das BGES regelt deren Anerkennung und übernimmt dabei im Wesentlichen die Regelungen der ZertDV.

CA's müssen bestimmte Eigenschaften aufweisen, damit sie von einer durch den Staat dafür bestimmten Stelle anerkannt werden. Die Anerkennung ist freiwillig. Das bedeutet, dass sich keine CA strafbar macht, wenn sie Zertifizierungsdienste anbietet, ohne vorher um Anerkennung nachgesucht zu haben oder wenn sie andere oder mehr Zertifizierungsdienste anbietet, als in diesem Gesetz vorgesehen sind.

Allerdings entfalten nur diejenigen digitalen Signaturen, welche von anerkannten CA's zertifiziert wurden, die entsprechenden gesetzlichen Rechtswirkungen betreffend Gleichstellung mit der eigenhändigen Unterschrift, Haftung, etc.

Die Anerkennung ist ein privatrechtliches Rechtsgeschäft und keine öffentlichrechtliche Verfügung. Man muss somit mit den Mitteln des Privatrechts dagegen vorgehen, sollte man aus irgendwelchen Gründen damit nicht einverstanden sein.

Anerkannt als CA werden natürliche oder juristische Personen und Verwaltungseinheiten des Bundes, der Kantone und der Gemeinden.

Das elektronische Zertifikat nach BGES

Mit der Ausstellung eines elektronischen Zertifikates bestätigt die CA, dass ein öffentlicher Prüfschlüssel einer bestimmten natürlichen Person zugeordnet werden kann. Zertifikate werden nur auf natürliche Personen ausgestellt. Der Gesetzgeber hat sich zu diesem grundsätzlichen Vorgehen aus der Überlegung heraus entschlossen, dass auch im „normalen Geschäftsleben“ grundsätzlich natürliche Personen Verträge unterzeichnen und nicht die juristische Person als solche.

Grundsätzlich dürfen die CA's auch die kryptografischen Schlüssel für ihre Kunden generieren, aber aus Gründen der Rechtssicherheit ist es ihnen untersagt, eine Kopie des privaten Schlüssels zurückzubehalten.

Das von einer CA ausgestellte elektronische Zertifikat muss gemäss Art. 8 BGES einen bestimmten Mindestinhalt aufweisen. Bestehen Nutzungsbeschränkungen (z. Bsp. es dürfen mit der digitalen Signatur nur Geschäfte bis zu einem Wert von Fr. 100'000.-- abgeschlossen werden), dann muss auf diese im Zertifikat hingewiesen werden.

Die CA ist verpflichtet, die Identität des Antragstellers zu überprüfen. Dieser muss in der Regel persönlich vor der CA erscheinen und sich dort auszuweisen. Der Bundesrat kann aber auch Ausnahmen von dieser Pflicht vorsehen. Der Begleitbericht zum Entwurf geht davon aus, dass die CA's diese Aufgabe der Identitätsprüfung in Zukunft beispielsweise an Banken oder Poststellen delegieren können.

Die CA's sind auch verpflichtet, ein öffentliches Verzeichnis der von ihr ausgestellten Zertifikate zu führen. Interessant ist dabei, dass der Antragsteller nicht verpflichtet ist, sich in dieses Verzeichnis eintragen zu lassen. Sie sind ausserdem verpflichtet, ein Verzeichnis der für ungültig erklärten oder suspendierten Zertifikate zu führen. In dieses Verzeichnis müssen auch diejenigen ungültigen Zertifikate aufgenommen werden, welche im ersten Verzeichnis nicht eingetragen waren.

Die CA ist zudem verpflichtet, ihre Kunden spätestens bei der Ausstellung des Zertifikates über die Folgen des Missbrauchs oder des Verlustes des privaten Schlüssels sowie über geeignete Massnahmen zum Schutz des privaten Schlüssels aufzuklären.

Zu den Pflichten der CA gehört auch das Führen eines Tätigkeitsjournals, welches in erster Linie der Beaufsichtigung der CA durch die Anerkennungsstelle dient.

Die Haftung der CA

Die CA haftet dem Inhaber des privaten Schlüssels und Dritten gegenüber für alle Schäden, welche diese erleiden, weil die CA ihre Pflichten aus dem Gesetz verletzt hat. Die Haftung tritt unabhängig vom Verschulden der CA ein, sie haftet also beispielsweise auch dann, wenn ein Mitarbeiter einen Fehler gemacht hat, weil er an diesem Tag krank war.

Die CA kann sich aber aus der Haftung befreien, indem sie beweist, dass die ihren Pflichten aus dem BGES oder der dazugehörigen Verordnung nachgekommen ist. Dies stellt eine Beweislastumkehr dar, da ohne diese Bestimmung derjenige, der behauptet, dass er einen Schaden erlitten hat, weil die CA ihren Pflichten nicht nachgekommen ist, dies auch beweisen müsste.

Art. 18 Abs. 3 BGES verbietet es der CA ihre Haftung gegenüber dem Inhaber des privaten Schlüssels oder gegenüber Dritten wegzubedingen.

Die Haftung des Inhabers des privaten Schlüssels

Der Inhaber des privaten Schlüssels muss diesen so aufbewahren, dass eine Verwendung durch unbefugte Dritte ausgeschlossen ist. Erleidet ein Dritter einen Schaden, weil der Inhaber des privaten Schlüssels dieser Pflicht widerrechtlich und schuldhaft nicht nachgekommen ist, dann haftet ihm dieser für den Ersatz des Schadens. Der Dritte profitiert dabei von der Beweislastumkehr – nicht er muss beweisen, dass der Inhaber des privaten Schlüssels seinen Pflichten nicht

nachgekommen ist, sondern dieser muss beweisen, dass der Schlüssel ohne seinen Willen verwendet wurde.

Wenn der Inhaber des privaten Schlüssels allerdings nachweisen kann, dass er alle vom Gesetz verlangten Massnahmen zur Geheimhaltung getroffen hat, dann entfällt die Haftung.

Die Chancen und Risiken für KMU

Zusammenfassend kann gesagt werden, dass die Chancen im Zusammenhang mit der Anerkennung der digitalen Signatur für KMU einerseits in der vermehrten Sicherheit durch die Identifizierbarkeit des Kunden bei Vertragsabschluss liegen, digital signierte Dokument sicher auch einen grösseren Beweiswert bei Streitigkeiten vor Gericht haben werden und der Grundstein dafür gelegt ist, dass der Verkehr mit den Behörden in Zukunft effizienter und schneller sein wird.

Die Risiken beim Einsatz der digitalen Signatur liegen in jedem Fall in der Haftung des Inhabers des privaten Schlüssels. Denn mit der Regelung, wie sie das BGEN getroffen hat, kann der Händler nicht darauf vertrauen, dass der Inhaber des privaten Schlüssels (somit der Kunde) für die missbräuchliche Verwendung des Schlüssels in jedem Fall haftet, da dieser sich aus der Haftung befreien kann.

Zudem ist auch vorauszusehen, dass die Motivation der Kunden, sich freiwillig der digitalen Signatur zu bedienen, recht gering sein wird, da ja bereits heute ohne zusätzlichen technischen Aufwand Vertragsabschlüsse gültig über das Internet getätigt werden können.