

Ursula Sury

Digitale Signatur – quo vadis

VERTRAUEN

Traditionelle Schriftlichkeit genießt in unserem Kulturkreis grosses Vertrauen. Wir sind uns seit Jahrhunderten gewohnt, Schriftstücke zu verfassen, die den Parteiwillen ausdrücken und dies mit einer Unterschrift bestätigen. Seit Generationen verwenden wir diese Formen des Festhaltens eines Parteiwillens auf einem Schrifträger und in Verbindung mit einer eigenhändigen Unterschrift, weshalb viele Geschäftsprozesse daran anknüpfen, resp. darauf aufbauen.

Fälschungen und Verfälschungen von Dokumenten und Unterschriften kommen zwar vor, im Verhältnis zur Anzahl der erstellten Dokumente und Unterschriften sind sie aber sehr selten. Zudem ist für uns der Vorgang der Fälschung und Verfälschung von Inhalten und Unterschriften vorstellbar, nachvollziehbar und somit relativ einschätzbar.

INTEGRITÄT UND AUTHENTIZITÄT

Das Gesetz schreibt die Schriftlichkeit für sehr wenige Verträge zwingend vor. Die allermeisten Verträge des Wirtschaftslebens können jedoch formlos abgeschlossen werden. Trotzdem verwenden und wünschen die Vertragsparteien in der Praxis sehr häufig die Schriftlichkeit, weil es ihnen ein grosses Anliegen ist, beweisen zu können, wer was mit wem vereinbart hat.

Die Kriterien Integrität und Authentizität erfüllen traditionell das Bedürfnis, in zwischenmenschlichen (Geschäfts-)Beziehungen beweisen zu können, wer sich wann zu was verpflichtet hat oder was erhalten, resp. geliefert hat. Denselben Kriterien entspricht auch die digitale Signatur in der Ausgestaltung, welche der eigenhändigen Unterschrift in technischer Hinsicht und gemäss länderspezifischer gesetzlicher Definition entspricht.

VERBREITUNG DER DIGITALEN SIGNATUR

Obwohl sehr viele traditionelle Businessprozesse an die Schriftlichkeit anknüpfen und die Vertragsparteien sich dies aus Gründen der Beweisbarkeit auch unbedingt wün-

schen, ist der Einsatz der digitalen Signatur kaum verbreitet. Die Abbildung der traditionellen Schriftlichkeit in der digitalen Welt ist also bis heute nicht erreicht. Ein Grund dafür ist sicher, dass die IT-Infrastrukturen bis heute nicht entsprechend (einfach) eingerichtet sind und die Benutzer somit ungenügend unterstützen. Dazu kommt, dass der Erwerb eines Zertifikates relativ umständlich und relativ teuer ist und sich viele fragen „wozu“, zumal eben der Einsatz nicht verbreitet ist.

DIE GLEICHE SITUATION FINDEN WIR IM E-GOVERNMENT-BEREICH

Auch das Verhältnis zwischen Bürger und Staat oder den Behörden unter sich verlangt in vielen Situationen zwingend Schriftlichkeit und eigenhändige Unterschrift. Die „Digitalisierung“ des Rechtsverkehrs zum Staat und innerhalb des Staates ist also ohne Verwendung einer rechtskonformen digitalen Signatur in vielen Fällen unmöglich.

UMGEHUNGSLÖSUNGEN

Im elektronischen Geschäftsverkehr arrangiert man sich heute mit verschiedenen Instrumenten und geht pragmatisch mit der Situation der fehlenden Beweisbarkeit um. Bei Webshops z.B. wird häufig nur gegen Vorauszahlung geliefert, folglich ist der Webshopbetreiber nicht mehr auf den Beweis des Vertragsabschlusses angewiesen. Für den Kunden (Customer) bedeutet dies, dass er bei der Auswahl des Webshopbetreibers sorgfältig sein muss und dessen Seriosität sinnvollerweise vorher abklärt, da sonst sein Geld verloren ist. Falls ihm die Ware nämlich nicht geliefert wird, kann er den Vertragsabschluss nicht beweisen.

Im B2B-Bereich, insbesondere wenn es sich um länger dauernde Verhältnisse handelt, wird das Grundverhältnis in einem Rahmenvertrag mit traditioneller Schriftlichkeit geregelt und dann die Risiken der Beweisbarkeit oder der Folgen der Beweislosigkeit in diesem traditionellen Vertrag abgehandelt. Das konkrete operative Tagesgeschäft läuft dann rein elektronisch. Dies findet sich z.B. bei automatisierten Bestellvorgängen im Verhältnis zu Zulieferanten.

TRUSTED THIRD PARTY

Ein anderes Thema ist die Frage, ob man beweisen kann, dass zu einem bestimmten Zeitpunkt ein Informationstransfer stattgefunden hat. Üblicherweise wird dieses Ziel mit der Einschaltung einer trusted third party sichergestellt. Bei traditionellen Briefen mit der Post übernimmt diese Rolle ein vertrauenswürdiger Dritter, wenn beispielsweise etwas

per Einschreiben übergeben wird. Im elektronischen Geschäftsverkehr kann dies mit einer speziellen Mail-Infrastruktur, welche beispielsweise auch von der Post zur Verfügung gestellt wird (in der Schweiz z.B. Inca-Mail), erreicht werden.

ZUSAMMENFASSUNG

Die digitale Signatur erfüllt die gleichen Voraussetzungen wie die eigenhändige Unterschrift. Da sich diese in der Praxis noch nicht durchgesetzt hat, versucht man diese Ziele mit anderen Mitteln zu erreichen. Für eine effektive und effiziente Umsetzung des E-Business und E-Government ist aus heutiger Sicht die Verbreitung der digitalen Signatur aber zwingend. Es ist deshalb dringend notwendig, dass eine optimale technische Infrastruktur zur Unterstützung des Einsatzes der digitalen Signatur zur Verfügung gestellt wird.

Ursula Sury ist selbständige Rechtsanwältin in Luzern (CH) und leitet das Kompetenzzentrum Management and Law an der Hochschule Luzern – Wirtschaft. Sie ist zudem Dozentin für Informatikrecht an verschiedenen Nachdiplomstudien, welche am Institut für Wirtschaftsinformatik der Hochschule durchgeführt werden. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig.

09.12.2009 / Ursula Sury