

Braucht es die digitale Signatur?

Seit fünf Jahren ist die digitale Signatur der eigenhändigen Unterschrift gleichgestellt. Seit Anfang Mai gibt es auch die digitale Identität «SuisselD». Braucht man so etwas?

VON UELI GRÜTER

Eine «Digitale Identität» ist aus rechtlicher Sicht eigentlich keine Identität, sondern die Bestätigung durch einen Dritten, dass man bei einer bestimmten elektronischen Transaktion effektiv die Person ist, für die man sich ausgibt. Dafür ist eine sogenannte Public Key Infrastructure (PKI) notwendig, bei der eine glaubwürdige, staatlich anerkannte Stelle bestätigt, dass die physische mit der digitalen Identität übereinstimmt. Dabei ist die digitale Signatur Mittel zum Zweck, da damit die Identität festgestellt wird. Somit ist die Signatur online wie offline Teil der Identität einer Person, mit der sie sich eben von den andern unterscheidet und somit ausweist. Zusätzlich kann eine digitale Signatur auch dazu verwendet werden, um ein Dokument oder eine E-Mail zu verschlüsseln. So wird gewährleistet, dass wirklich besagte Person das Dokument gesendet hat und dass dieses unterwegs auch nicht verändert wurde. Eine digitale Signatur im rechtlichen Sinne ist aber nicht, wie viele meinen, eine digitalisierte Unterschrift, sondern ein Code, der Teil einer PKI ist, die hohen, gesetzlichen technischen Standards entspricht. Neben einer qualifizierten elektronischen Signatur enthält die nun angebotene SuisselD (ein Fachartikel über SuisselD im Unternehmenseinsatz folgt in der kommenden Ausgabe), die es in der Form einer Chipkarte oder eines USB-Stick gibt, zusätzliche Informationen über deren Inhaber, wobei dieser immer selber bestimmt, ob und welche zusätzlichen Informationen – insbesondere Vorname, Name, E-Mail-Adresse – dem Gegenüber zugänglich gemacht werden sollen.

Ist die elektronische Signatur sicher vor Fälschung und Missbrauch?

Bei der aktuellen Promotion der digitalen Identität «SuisselD» betont das Staatssekretariat für Wirtschaft (SECO), dass diese ID alles vereinfache, da damit all die Passwörter, die man sich kaum noch merken kann, durch eine digitale Signatur ersetzt werden. Bei dieser

Konzentration stellt sich die Frage, wie sicher eine digitale Identität respektive Signatur vor Fälschung und Missbrauch ist.

Falls die elektronische Signatur effektiv die durch das Signaturgesetz, die Signaturverordnung und die entsprechenden Ausführungsbestimmungen des Bundesamtes für Kommunikation (Bakom) gestellten technischen Anforderungen erfüllt, ist sie theoretisch sicherer vor Fälschungen als die handschriftliche Signatur. Die elektronische Signatur weist jedoch ein enormes Risiko auf. Kommen nämlich Dritte in Besitz des entsprechenden, geheimen Codes, mit dem der effektive Inhaber der elektronischen Signatur Rechtsgeschäfte abschliesst, können jene jederzeit ebenfalls Geschäfte für oder eher zu Lasten des rechtmässigen Inhabers tätigen – zum Beispiel eine Schuldanererkennung über eine Million Franken. Immerhin hat in diesem Fall die elektronische – im Gegensatz zur handschriftlichen Signatur – den Vorteil, dass man sie über die PKI sperren kann – analog der Sperrung von Kreditkarten und entsprechenden Pin-Codes.

Für welche Rechtsgeschäfte benötigt man eine elektronische Signatur?

Grundsätzlich ist festzustellen, dass schon viele digitale respektive elektronische Signaturen verwendet werden, die jedoch nicht auf staatlich anerkannten Zertifikaten basieren, sondern auf Vereinbarungen für die Abwicklung von Geschäften zwischen Unternehmen oder Privaten und Firmen, wie beispielsweise das Login für das E-Banking oder das E-Billing.

Seit dem 1. Januar 2005 ist laut dem Art. 14 des Schweizerischen Obligationenrechts (OR) eine qualifizierte elektronische Signatur einer eigenhändigen Unterschrift gleichgestellt, sofern sie durch eine durch den Bund anerkannte Stelle herausgegeben worden ist. Auch wenn entweder von Gesetzes wegen oder vertraglich vorbehalten eine eigenhändige Unterschrift nach OR verlangt wird.

IN KÜRZE

- Eine digitale Signatur stellt bei einer elektronischen Transaktion die Identität der involvierten Personen fest.
- Eine von einer Bundesstelle qualifizierte elektronische Signatur ist einer eigenhändigen Unterschrift gleichgestellt.
- Eine digitale Identität macht vor allem im Kontakt mit Behörden Sinn, im E-Commerce weniger.

Aufgrund der Regelung im Obligationenrecht und des entsprechenden Hinweises in der Botschaft zum Signaturgesetz wurde die elektronische Signatur der eigenhändigen Unterschrift vor allem für den Einsatz im E-Commerce gleichgestellt. Im E-Commerce werden vor allem Kaufverträge (zum Beispiel Kauf von Hardware, Kauf im Rahmen von Auktionen), Mietverträge (Miete von DVD) und Lizenzverträge (Download von Software) abgeschlossen. Alle diese Verträge können nach Obligationenrecht formlos, das heisst insbesondere auch ohne eine Unterschrift, abgeschlossen werden. So gesehen ist die elektronische Signatur für den E-Commerce praktisch unnötig. Eine Anwendung ist nur da von Interesse, wo der andere Vertragspartner verlässlich wissen will oder muss, mit wem er es genau zu tun hat. Dies ist beispielsweise beim Zugang zu Online-Informationen oder beim Verkauf von Waren der Fall, die nur Personen ab einem bestimmten Alter angeboten werden dürfen (beispielsweise Pornographie oder Alkohol). Ebenfalls kann eine Identifizierung bei der Eröffnung eines Bankkontos – wegen der Gefahr der Geldwäscherei – oder für den Antrag eines fixen oder mobilen Telefonanschlusses als

Massnahme gegen terroristische Aktivitäten notwendig sein. Verträge, für deren Abschluss das Gesetz effektiv eine eigenhändige oder nun eben eine qualifizierte elektronische Signatur verlangt, dürften wohl höchst selten bis nie auf dem elektronischen Wege abgeschlossen werden. Zu solchen Verträgen gehören beispielsweise der Lehrvertrag, die arbeitsrechtliche Vereinbarung eines Konkurrenzverbots oder die Abtretung einer Forderung.

Da die nun vom SECO lancierte digitale Identität effektiv fürs Daily Business nicht gebraucht wird, versucht der Bund die Verwendung von digitalen Identitäten mit einem stark vergünstigten Preis und damit mit Subventionen in Millionenhöhe anzuheizen. Das macht möglicherweise auch Sinn. Während im E-Commerce eine digitale Identität respektive Signatur nicht wirklich gebraucht wird, kann eine solche im E-Government, also dem Kontakt zu Behörden auf elektronischem Wege, sehr nützlich sein. Aktuell ist das entsprechende Angebot noch mager. So kann man zum Beispiel einen Strafregisterauszug nun online anfordern. In Planung ist aber insbesondere die elektronische Mehrwertsteuerabrechnung, die Online-Betreibung und die elektronische Eingabe von Rechtsschriften an den schweizerischen Gerichten, was vor allem für Rechtsanwälte den Behördenkontakt enorm vereinfacht und die «papierlose Anwaltskanzlei» der Realität näher bringt.

Wo gibt es digitale Identitäten und Signaturen?

Obwohl es die zertifizierte digitale Signatur nun schon seit fünf Jahren gibt, sind die Anbieter nicht viel zahlreicher geworden. Aktuell wird die SuisseID, die auch eine zertifizierte elektronische Signatur enthält, von Quovadis Trustlink Schweiz, der Schweizerischen Post, Swisscom und für Verwaltungsstellen vom Bundesamt für Informatik und Telekommunikation angeboten. ■

DER AUTOR

Ueli Grüter, LL.M., ist Rechtsanwalt in Zürich und Luzern und Dozent an der Hochschule Luzern mit Spezialgebiet Kommunikations- und Technologierecht. In der Serie

«Informatikrecht für die Praxis» führt Grüter in 13 Folgen kurz und verständlich durch die rechtlichen Grundlagen in der Informatik und zeigt die rechtlichen Stolpersteine. Mit der letzten Folge erscheint die Serie dann auch als E-Book.



LESER FRAGEN, RECHTSANWALT GRÜTER ANTWORTET

Sie haben in Ihrer letzten Kolumne geraten, dass man mit Freelancern spezielle Vereinbarungen treffen sollte. Gibt es dafür Musterverträge?

Wir haben für das Freelancing einen Mustervertrag entwickelt, der in der Praxis schon seit langem und offenbar ohne Probleme angewandt wird. Den Freelancing-Mustervertrag können Sie unter informatikrecht@gspaw.ch für eine Schutzgebühr von 90 Franken bestellen.

Rechtsanwalt Ueli Grüter steht den LeserInnen des Swiss IT Magazine für kurze Fragen zu Informatik und Recht auch unter informatikrecht@gspaw.ch und 043 430 32 70 unentgeltlich zur Verfügung. Fragen von allgemeinem Interesse werden in anonymisierter Form publiziert.

AMERIKANISCHE DOTCOM-DROHUNG – ICANN-SCHIEDSGERICHT

Unsere Firmen-Homepage läuft auch unter einer .com-Adresse. Nun haben wir Post aus den USA bekommen. Ein amerikanisches Unternehmen behauptet, eine ähnliche Marke zu haben wie unsere Firma und verlangt von uns, umgehend den .com-Domainnamen zu übertragen. Das amerikanische Unternehmen droht uns mit einem ICANN-Dispute-Resolution-Verfahren in den USA. Was ist das und was sollen wir tun?

Wenn man eine sogenannte Generic-Top-Level-Domain, wie zum Beispiel .com, aber auch .org, .biz und .net, bei einem Domain-Anbieter wie Register.com registriert, unterwirft man sich mit der Annahme der allgemeinen Geschäftsbedingungen automatisch der ICANN-Schiedsgerichtsbarkeit, dem ICANN-Dispute-Resolution-Verfahren. ICANN ist die Internet Corporation for Assigned Names and Numbers, eine Stiftung mit Sitz in den USA. ICANN entscheidet über die Grundlagen der Verwaltung der Top-Level-Domains, und auf diese Weise koordiniert ICANN technische Aspekte des Internet. ICANN wurde bis vor kurzem direkt durch die amerikanische Regierung kontrolliert. Nach einer Öffnung haben nun auch andere Regierungen und Organisationen die Möglichkeit, auf ICANN Einfluss zu nehmen. Ein Schiedsgericht ist ein nichtstaatliches, also eigentlich ein privates Gericht. Schiedsgerichte gibt es auch in anderen Bereichen. Die Vorteile eines Schiedsgerichtes sind schnelle und in der Regel auch fachlich qualifizierte Entscheide in einem bestimmten Gebiet. Von ICANN sind vier Schiedsgerichte anerkannt: das Asian Domain Name Dispute Resolution Centre mit Büros in China, Südkorea und Malaysia, das National Arbitration Forum in den USA, die World Intellectual Property Organization (WIPO) in der Schweiz und das Czech Arbitration Court Center for Internet Disputes.

Für Schweizer Unternehmen, die durch amerikanische Kläger in ein ICANN-Schiedsverfahren involviert werden, sind drei Umstände besonders ungünstig. Erstens wird der amerikanische Kläger das amerikanische Schiedsgericht National Arbitration Forum wählen. Zweitens wird das Verfahren regelmässig in Englisch geführt, da .com-Domains in englischer Sprache registriert werden. Sollte drittens der amerikanische Kläger das ICANN-Schiedsverfahren verlieren, kann er die Sache an ein amerikanisches Gericht ziehen, da die Registrierstelle von .com-Domains ihren Sitz regelmässig in den USA haben. Damit kommt ein Schweizer Unternehmen in einer solchen Situation nicht darum herum, einen Anwalt zu konsultieren, der in der Lage ist, ein entsprechendes Schiedsverfahren in englischer Sprache zu führen. Es ist zwar kein Problem, einen solchen Anwalt in der Schweiz zu finden. Die Kosten dürften jedoch relativ schnell relativ hoch werden. Richtig teuer wird es, wenn man für einen allfälligen Prozess in den USA einen amerikanischen Anwalt beiziehen müsste.

Solange man einen .com-Domainnamen in guten Treuen reserviert hat, hat man im ICANN-Schiedsverfahren eigentlich nichts zu befürchten. Noch besser ist die Ausgangsposition, wenn man eine ähnliche oder sogar identische Marke oder Firma im Markenregister respektive im Handelsregister registriert hat. Da dies in der vorliegenden Sache der Fall ist, würde ich empfehlen, einen entsprechenden Anwalt beizuziehen. Entsprechende Verfahren wurden bereits geführt und gewonnen, wobei die Kosten zwischen 5000 und 6000 Franken lagen. Sollte man verlieren, muss man übrigens nur seine eigenen Anwaltskosten, jedoch nicht die Verfahrenskosten tragen; ausser wenn man mehr als einen Schiedsrichter verlangt. Die eigenen Anwaltskosten muss man jedoch auch tragen, wenn man gewinnt; was in der Schweiz nicht üblich ist. Alternativ könnte man auch in der Schweiz eine Klage einreichen, mit der festgestellt wird, dass man den Domainnamen in guten Treuen hält. Ein solches Verfahren ist jedoch schnell viel teurer als das ICANN-Schiedsverfahren.

Übrigens: auch für Domainnamen unter der Country-Domain .ch gibt es die Möglichkeit eines Schiedsverfahrens (weitere Informationen dazu unter www.switch.ch).