Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 92 (2001)

Heft: 1

Artikel: Die digitale Signatur und ihre Rechtswirkung in der Schweiz

Autor: Ramsauer, Matthias

DOI: https://doi.org/10.5169/seals-855652

Die digitale Signatur und ihre Rechtswirkung in der Schweiz

Mit der raschen Entwicklung des elektronischen Geschäfts- und Behördenverkehrs wird die Sicherheit von elektronischen Transaktionen immer wichtiger. Vertrauen im weitesten Sinne bildet mehr denn je die Basis aller Geschäftsbeziehungen. Hauptmerkmale des Geschäftsabschlusses über Computer sind vor allem die grosse örtliche Distanz und die Anonymität zwischen den Geschäftspartnern. Wie kann man wissen, ob ein Kommunikationspartner wirklich derjenige ist, für den er sich ausgibt? Und wie kann sichergestellt werden, dass Meldungen und elektronische Dokumente unterwegs nicht verändert worden sind oder dass sie vom Absender tatsächlich übermittelt werden wollten? Antwort auf diese Fragen geben digitale Signaturen auf der Basis der asymmetrischen Verschlüsselungstechnik, kombiniert mit der Einhaltung verschiedener Organisations- und Sicherheitsvorschriften und der rechtlichen Anerkennung von digitalen Signaturen. Diese Kernelemente der digitalen Signatur werden im Folgenden näher vorgestellt.

Während bei der traditionellen Verschlüsselung derselbe Schlüssel zum Chiffrieren und Dechiffrieren von Dokumenten dient, erhält beim asymmetrischen Verschlüsselungsverfahren jeder Benutzer ein Schlüsselpaar.

Wie funktioniert die digitale Signatur?

Zum Verschlüsseln und zum Entschlüsseln werden zwei verschiedene Schlüssel verwendet: ein privater und ein öffentlicher. Der öffentliche Schlüssel ist allgemein zugänglich und wird an alle verteilt. Da die beiden Schlüssel durch ein äusserst komplexes System zueinander in Beziehung gesetzt werden, ist es unmöglich, den privaten Schlüssel auf Grund des öffentlichen Schlüssels zu rekonstruieren.

Für den Fall, dass der öffentliche Schlüssel zum Chiffrieren von Meldungen verwendet wurde, dient der entsprechende private Schlüssel dem Dechiffrieren dieser Nachrichten. Soll ein vertrauliches Dokument verschickt werden, kann die entsprechende Meldung mit dem öffentlichen Schlüssel des Empfängers verschlüsselt werden. Anschliessend entschlüsselt der Empfänger die Meldung mit seinem privaten Schlüssel.

Bei der Verwendung einer digitalen Signatur wird ein Dokument mit Hilfe eines privaten Schlüssels unterschrieben. Zur Überprüfung dieser Signatur dient der dazugehörige öffentliche Schlüssel. Genauer gesagt wird bei der digitalen Signatur zuerst eine mathematische Funktion – die Hashfunktion – auf das Dokument angewendet, welche eine Art von abgekürzter Version des Dokuments (Hashwert) herstellt. Anschliessend wird der für jedes Dokument einzigartige Hashwert mit dem privaten Schlüssel des Absenders verschlüsselt und an das Dokument angehängt. Dieser verschlüsselte Code bildet die digitale Signatur. Der Empfänger eines solchen Dokuments dechiffriert die digitale Signatur mit dem öffentlichen Schlüssel des Absenders und errechnet den Hashwert. Stimmen nun der übermittelte und der selber errechnete Hashwert überein, besteht die Gewissheit, dass das übermittelte Dokument seit seiner Versendung nicht verändert worden ist. Wenn zudem eine unabhängige Instanz in einem Zertifikat garantiert, dass der öffentliche Schlüssel derjenigen Person gehört, welche sich als Absenderin des Dokumentes ausgibt, hat der Empfänger auch die Gewähr betreffend die Identität seines Gegenübers.

Adresse des Autors
Matthias Ramsauer, Stv. Abteilungsleiter und Sektionschef Politik und Planung, Abt. Telekomdienste, Bundesamt für Kommunikation, 2501 Biel
matthias.ramsauer@bakom.admin.ch

Zertifizierung der öffentlichen Schlüssel

Zentrale Voraussetzung für die sichere Verwendung von digitalen Signaturen sind die Validierung und das Zur-Verfügung-Stehen der öffentlichen Schlüssel. Man kann nicht erwarten, dass in einem Kommunikationsnetz wie beispielsweise dem Internet jeder einzelne Benutzer mit allen anderen Benutzern im Voraus Beziehungen unterhält, um die öffentlichen Schlüssel untereinander auszutauschen. Stattdessen bürgt eine unabhängige Instanz für die Identität der beiden Parteien. Die Hauptaufgabe dieses vertrauenswürdigen Dritten – der Zertifizierungsbehörde oder Anbieterin von Zertifizierungsdiensten – besteht darin, die Zugehörigkeit eines öffentlichen Schlüssels zu einer bestimmten Person zu garantieren, damit sich niemand unrechtmässig als dessen Besitzer ausgeben kann. Dazu stellt sie ein Zertifikat aus, das elektronische Gegenstück zu einem Pass. Neben Informationen zur Identifizierung des Inhabers enthält es auch dessen öffentlichen Schlüssel. Um die Authentizität des öffentlichen Schlüssels eines Benutzers und der anderen Informationen eines Zertifikats zu garantieren, signiert die Anbieterin von Zertifizierungsdiensten die Informationen des Zertifikats mit ihrem eigenen privaten Schlüssel. Somit können alle, die Vertrauen in eine Anbieterin von Zertifizierungsdiensten haben, die von ihr ausgestellten Zertifikate anerkennen.

Die rechtliche Erfassung der digitalen Signatur

Eine umfassende Regelung der digitalen Signatur betrifft hauptsächlich zwei Aspekte: Einerseits geht es um die Frage der rechtlichen Verbindlichkeit von digitalen Signaturen und digital signierten

Datenmeldungen im Verhältnis zur traditionellen, handschriftlichen Unterschrift und der ordentlichen Schriftlichkeit bzw. dem Urkundenbegriff gemäss Obligationenrecht. Andererseits geht es um die für die Gewährleistung des Vertrauens im Geschäftsverkehr bzw. als Voraussetzung für die rechtliche Anerkennung von digital signierten Dokumenten notwendige «Infrastruktur».

Die Regelung der organisatorischen und der technischen Voraussetzungen für die mit asymmetrischen Verschlüsselungsverfahren in Zusammenhang stehenden Dienste wird als *Public-Key-Infrastruktur* bezeichnet.

Rechtsgrundlage für die Zertifizierung

Der Bundesrat hat am 12. April 2000 die technischen und die organisatorischen Aspekte der digitalen Signatur in der *Verordnung über Dienste der elektronischen Zertifizierung* (ZertDV) geregelt und diese per 1. Mai 2000 in Kraft gesetzt [1]. Diese Verordnung orientiert sich am schweizerischen Akkreditierungssystem. Die Anerkennung von Zertifizierungsdiensten erfolgt durch eine von der Schweizerischen Akkreditierungsstelle (SAS) akkreditierten Zertifizierungsstelle. Dabei handelt es sich normalerweise um private, in diesem Bereich spezialisierte Unternehmungen. Diese prüfen, ob Anbieterinnen von Zertifizierungsdiensten die grundlegenden Anforderungen erfüllen, welche der Gesetzgeber für die Garantie der Sicherheit und der Vertrauenswürdigkeit der digitalen Signatur festgelegt hat. Die Anerkennung ist zudem grundsätzlich freiwillig: Zertifizierungsdienste dürfen nach wie vor auch ausserhalb des geplanten Systems angeboten werden. Wer aber in den Genuss einer formellen Anerkennung kommen möchte, muss die entsprechenden Vorschriften einhalten.

Voraussetzung für die Anerkennung ist der Eintrag im Handelsregister. Anerkannt werden können aber auch Verwaltungseinheiten von Bund, Kantonen oder Gemeinden. Darüber hinaus müssen die Anbieterinnen von Zertifizierungsdiensten genügend qualifiziertes Personal beschäftigen, zuverlässige Informatiksysteme betreiben, über ausreichende Finanzmittel und Versicherungen verfügen und sich in ihren allgemeinen Geschäftsbedingungen gegenüber Dritten zu einer gewissen Haftungsübernahme verpflichten.

Zu den Pflichten der Anbieterinnen von Zertifizierungsdiensten gehört die Identifikation der Gesuchsteller durch persönliche Überprüfung anhand eines Passes oder einer Identitätskarte. Nur so kann gewährleistet werden, dass der Gesuchsteller mit dem Inhaber des ausgestellten Zertifikats übereinstimmt und Dritte sich auf die Authentizität eines digital signierten Dokuments verlassen können. Die Anbieterinnen von Zertifizierungsdiensten stellen nicht nur Zertifikate in einer vordefinierten Form aus, sondern sie müssen überdies Dritten den Zugang zu den von ihnen ausgegebenen Zertifikaten jederzeit elektronisch gewährleisten und diese auch nach Ablauf ihrer Gültigkeit aufbewahren. Die Verordnung enthält überdies Regeln zur Informationspflicht, zur Aufbewahrung von privaten Schlüsseln, zur Ungültigerklärung von Zertifikaten und zur Einstellung der Geschäftstätigkeit. Die Voraussetzungen für die Anerkennung und die erwähnten Pflichten der Anbieterinnen von Zertifizierungsdiensten werden in technischen und in administrativen Vorschriften des Bundesamts für Kommunikation (Bakom) konkretisiert.

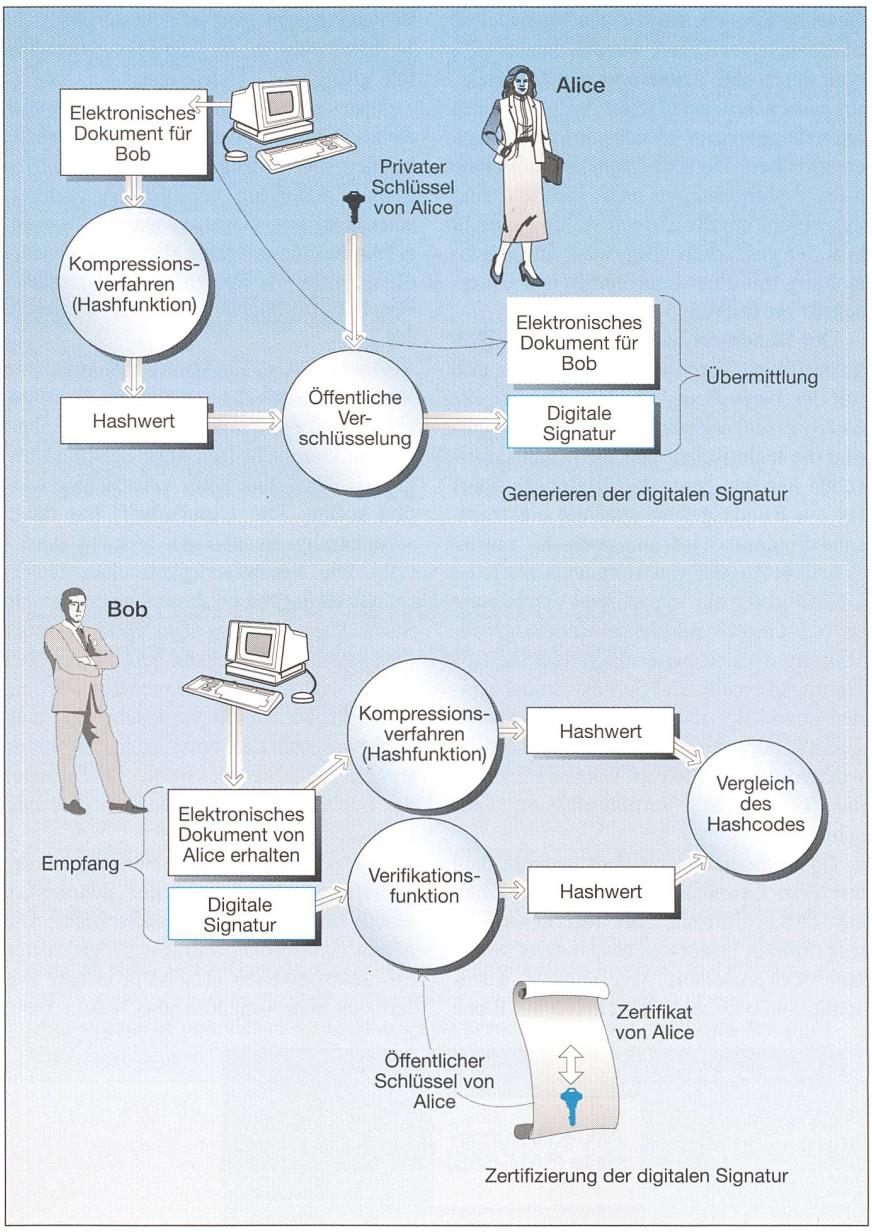

Bild 1 Ablauf von der Generierung der digitalen Verschlüsselung eines Dokuments von Alice bis zur Entschlüsselung bei Bob

Entwurf für ein Bundesgesetz über die elektronische Signatur

Eine funktionierende und zuverlässige Public-Key-Infrastruktur ist Bedingung und Voraussetzung für die rechtliche Anerkennung von digitalen Signaturen bzw. deren Gleichstellung mit der Handunterschrift. Die Rechtssicherheit ist nur dann gewährleistet, wenn eine digital signierte

Datenmeldung anhand eines öffentlichen Schlüssels verifiziert werden kann, welcher durch eine Anbieterin von Zertifizierungsdiensten zertifiziert wurde, deren Dienste gewissen Mindestanforderungen entsprechen. Digitale Signaturen, welche diese Anforderungen nicht erfüllen, sind zwar nicht ungültig, doch sollen sie nicht von der gesetzlich vorgesehenen Gleichstellung mit einer herkömmlichen Unterschrift profitieren.

Der Bundesrat hat sich für ein zeitlich gestaffeltes Vorgehen entschieden und mit der *Verordnung über die Dienste der elektronischen Zertifizierung* vorerst einmal die technischen und die organisatorischen Aspekte geregelt. Mit dem Entwurf für ein Bundesgesetz über die elektronische Signatur wird nun auch der zweite Schritt in Angriff genommen, nämlich die Überführung der erwähnten Verordnung in ein Gesetz inklusive Regelung der Haftung von Anbieterinnen von Zertifizierungsdiensten und Schlüsselinhaberinnen sowie der rechtlichen Anerkennung von digitalen Signaturen. Dieser Entwurf wird voraussichtlich im Frühling 2001 in die öffentliche Vernehmlassung geschickt.

Das schweizerische Vertragsrecht baut auf dem Grundsatz der Vertragsfreiheit auf. Die Formfreiheit als Teil dieser Vertragsfreiheit erlaubt es also bereits heute, auf elektronischem Weg Verträge abzuschliessen oder andere rechtsverbindliche Willensäusserungen zu tätigen. Derartige Verträge sind in der Schweiz grundsätzlich gültig und durchsetzbar.

Vom Grundsatz der Formfreiheit gibt es aber etliche Ausnahmen. Einerseits können die Vertragsparteien die Schriftlichkeit freiwillig vereinbaren, andererseits wird von Gesetzes wegen für zahlreiche Rechtsgeschäfte die einfache oder die qualifizierte Schriftform vorgeschrieben (Miet-, Pacht-, Arbeits-, Kaufrecht etc.).

Gemäss Art. 13 Abs. 1 OR muss ein Vertrag, für den die schriftliche Form gesetzlich vorgeschrieben oder vereinbart ist, die Unterschriften aller Personen tragen, welche durch ihn verpflichtet werden sollen. Die Unterschrift hat dabei eigenhändig zu erfolgen (Art. 14 Abs. 1 OR). Die Eigenhändigkeit einer Unterschrift bedingt also, dass diese auf einem Stück Papier erfolgt. Ein elektronisches Dokument erfüllt dieses Erfordernis aber nicht, weshalb im erwähnten Entwurf ein neuer Artikel im OR vorgesehen ist, welcher eine nach den vorstehend erwähnten Regeln erstellte elektronische Signatur der handschriftlichen Unterschrift explizit gleichstellt.

Eine der wichtigsten Funktionen der Schriftform war bisher der Schutz vor einem übereilten Vertragsabschluss. Die neuen Techniken und Gepflogenheiten im elektronischen Geschäftsverkehr lassen den Konsumenten aber kaum mehr Zeit zur Reflexion. Rechtsgeschäfte können per Mausklick in Sekundenschnelle und praktisch von jedem beliebigen Ort zu jeder Tages- oder Nachtzeit abgeschlossen werden. Zudem wird die Gefahr von Fehlmanipulationen immer grösser. Dem Konsumentenschutz ist daher in erhöhtem Masse Rechnung zu tragen, weshalb der Entwurf verschiedene Konsumentenschutzbestimmungen vorsieht (z.B. umfassende Aufklärungs- und Informationspflichten, ein Widerrufsrecht von 7 Tagen für Käufe über das Internet, Erweiterung der Gewährleistungsregeln etc.).

Das Bundesgesetz über die elektronischen Signaturen wird auch die Grundlage für die umfassende elektronische Registerführung schaffen. So soll dem Bundesrat insbesondere erlaubt werden, den Kantonen die elektronische Handelsregisterführung vorzuschreiben und dafür einheitliche Vorgaben zu machen. Auch im Grundbuchrecht soll der Bundesrat die Kompetenz erhalten, die elektronische Registerführung und den elektronischen Verkehr mit den Grundbuchämtern zu regeln.

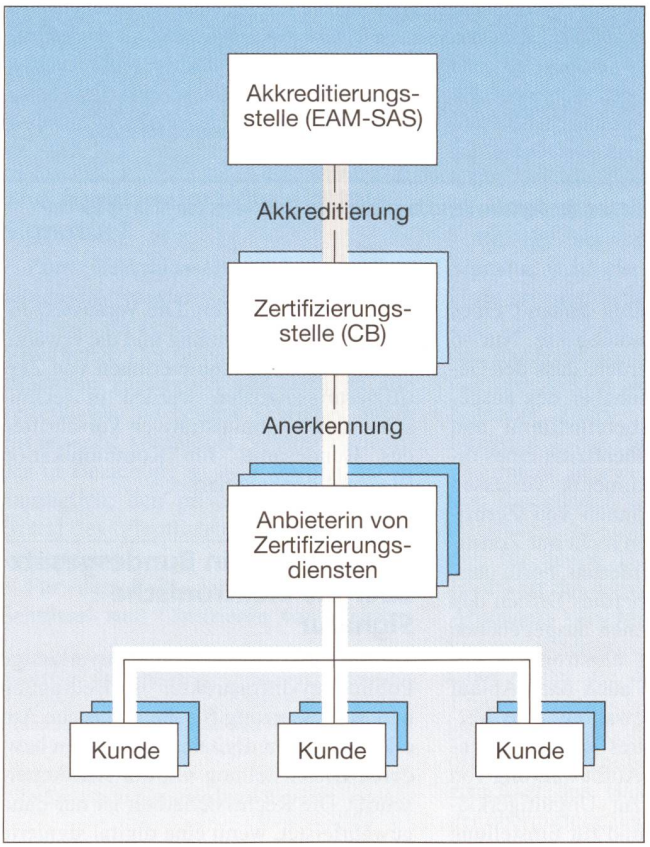

Bild 2 Die Organisation der Public-Key-Infrastruktur

Revision der Bundesrechtspflege

Die nachfolgenden Ausführungen beziehen sich lediglich auf das Bundesverwaltungsrecht, welches zurzeit in Revision ist. Eine entsprechende Vorlage dürfte im Verlauf des Jahres vom Parlament behandelt werden. Für die breite Realisierung des elektronischen Behördenverkehrs ist es aber unabdingbar, dass die kommunalen und die kantonalen Erlasse ebenfalls auf ihre elektronische Tauglichkeit hin überarbeitet werden, zumal die meisten Kontakte zwischen Privaten und der Verwaltung auf dieser Stufe stattfinden.

Neben der Gesamtreorganisation der Bundesrechtspflege enthält die Vorlage aber auch wichtige Änderungen im Zusammenhang mit dem elektronischen Behördenverkehr. So ist im neuen Bundesgerichtsgesetz vorgesehen, dass Rechtsschriften und Belege elektronisch eingegeben werden dürfen. Auch soll es für die Behörden grundsätzlich möglich sein, mit Privaten elektronisch zu verkehren. Voraussetzung dafür ist deren Einverständnis. Die Revision von Art. 34 des Verwaltungsverfahrensgesetzes wird es den Bundesbehörden neu erlauben, elektronisch zu verfügen. Die Vorlage enthält zudem detaillierte Regelungen zu Fragen, welche sich insbesondere durch den elektronischen Behördenverkehr neu stellen (z.B. zu verwendendes Format für

Eingaben, Fristenwahrung, Risikotragung bei Übermittlungsfehlern etc.). Der elektronische Behördenverkehr steht zudem immer unter dem Vorbehalt, dass elektronische Signaturen verwendet werden, welche auf der oben beschriebenen *Verordnung über Dienste der elektronischen Zertifizierung* basieren.

Die Schweiz kommt mit diesen Massnahmen auf dem Weg in die Informationsgesellschaft zweifelsohne einen grossen Schritt weiter. Das Angebot von Seiten der Behörden steht, es muss nur noch genutzt werden!

Referenzen

[1] Verordnung vom 12. April 2000 über Dienste der elektronischen Zertifizierung (Zertifizierungsdiensteverordnung, ZertDV), SR 784.103, http://www.admin.ch/ch/d/as/2000/1257.pdf.

Weitergehende Literatur

Bundesamt für Justiz: Digitale Signatur und Privatrecht (Vertragsrecht). Verwaltungspraxis der Bundesbehörden (VPB), Nr. 63.46, 1999, S. 441–466.

U. Bürge: Digitale Signatur und Recht – Voraussetzungen, Stand und Aussichten der rechtlichen Anerkennung in der Schweiz. Die Volkswirtschaft – Das Magazin für Wirtschaftspolitik, 72. Jahrgang, Nr. 6/99, Juni 1999, S. 40–44.

R. Dietschi, J.-M. Geiser: Digitale Signatur – Entwurf einer Regelung für eine Public-Key-Infrastruktur (PKI) in der Schweiz. Die Volkswirtschaft – Das Magazin für Wirtschaftspolitik, 72. Jahrgang, Nr. 6/99, Juni 1999, S. 36–39.

C. Graber: Digitale Zertifikate: Infrastruktur für ein sicheres Internet. *R. H. Weber, R. M. Hilty, R. Auf der Maur* (Hrsg.): Geschäftsplattform Internet, Schulthess, Zürich, 2000, S. 9–17.

G. G. Gravesen, J. Dumortier, P. Van Eecke: Die europäische Signaturrichtlinie – Regulative Funktion und Bedeutung der Rechtswirkung. Multimedia und Recht (MMR), 3. Jahrgang, Nr. 10/1999, S. 577–585.

M. Jaccard: Les relations juridiques et les responsabilités dans une infrastructure à clé publique. *R. H. Weber, R. M. Hilty, R. Auf der Maur* (Hrsg.): Geschäftsplattform Internet, Schulthess, Zürich, 2000, S. 19–37.

F. S. Jörg, O. Arter: Digitale Signaturen: Die Public-Key-Infrastruktur nach der neuen Zertifizierungsdiensteverordnung. ZBJV, Band 136, 2000, S. 449–484.

T. Legler: Electronic Commerce mit digitalen Signaturen in der Schweiz – Kurzkommentar zur Verordnung über Dienste im Zusammenhang mit der elektronischen Zertifizierung. Stämpfli-Verlag, Bern, 2000.

M. Ramsauer: Die Regelung der Public Key Infrastruktur in der Schweiz. *R. H. Weber, R. M. Hilty, R. Auf der Maur* (Hrsg.): Geschäftsplattform Internet, Schulthess, Zürich, 2000, S. 59–94.

M. Ramsauer: Die Digitale Signatur – technische, organisatorische und rechtliche Aspekte. *A. Meier:* Internet & Electronic Business, Herausforderung an das Management. Orell Füssli, Zürich, 2001, S. 185–211.

F. Schöbi: Vertragsschluss auf elektronischem Weg: Schweizer Recht heute und morgen. *R. H. Weber, R. M. Hilty, R. Auf der Maur* (Hrsg.): Geschäftsplattform Internet, Schulthess, Zürich, 2000, S. 95–108.

R. H. Weber, Y. Jöhri: Vertragsschluss im Internet. *R. H. Weber, R. M. Hilty, R. Auf der Maur* (Hrsg.): Geschäftsplattform Internet, Schulthess, Zürich, 2000, S. 39–57.

Links

http://europa.eu.int
http://www.ispo.cec.be
http://www.oecd.org
http://www.uncitral.org
http://www.bakom.ch

La signature numérique et sa validité juridique en Suisse

Etant donné le développement vertigineux des échanges commerciaux et officiels par moyens électroniques, la sécurité des transactions électroniques joue un rôle toujours plus important. La confiance au sens le plus large constitue de plus en plus la base de toutes les relations commerciales. La conclusion d'affaires par ordinateur est caractérisée avant tout par la grande distance géographique et l'anonymat entre les partenaires. Comment savoir si un partenaire de communication est vraiment celui qu'il prétend être? Et comment s'assurer que les messages et documents électroniques n'ont pas été modifiés en route ou que l'expéditeur voulait effectivement les transmettre? La réponse à ces questions est donnée par l'utilisation de signatures numériques sur la base de la technique asymétrique de codification en combinaison avec le respect de diverses prescriptions organisationnelles et de sécurité et de la reconnaissance juridique des signatures numériques.