Einsatz von elektronischen Zertifikaten

Die Verwendungsmöglichkeiten elektronischer Zertifikate sind vielfältig. Einerseits kann der fachmännische Gebrauch von Zertifikaten den Geschäftsverkehr optimieren und dabei auftretende Fehler minimieren. Anderseits kann dies auch die Corporate Security erhöhen, insbesondere die bestehenden Assets wie Forschungsergebnisse besser schützen und die Nachvollziehbarkeit (interner) Prozesse verbessern.

Ronny Wittig, Sales Manager, OPENLiMiT SignCubes AG
Daniel Muster, dipl. Physiker, NDS ETHZ
Autor des Buches: „Digitale Unterschriften und PKI"

Die Verwendung von Zertifikaten ist vor allem im Bereich der elektronischen Signatur als Ersatz der Handunterschrift allgemein bekannt, doch können Zertifikate und deren Schlüssel mit den dazu passenden Sicherheitstechnologien für weitere Sicherheitsdienste genutzt werden. Letzteres wird später erläutert.

Auf sorgfältige Planung, auf stufengerechte Schulung und auf das Verfassen von Konzepten darf bei der Einführung und beim Einsatz elektronischer Zertifikate in einem Unternehmen nicht verzichtet werden.

Elektronische Signatur im Geschäftsverkehr

Die elektronische Signatur hilft, den Geschäftsverkehr und das Dokumentenmanagement zu optimieren. Insbesondere kann die Logistik (von der Warenbestellung bis zur Auslieferung) beschleunigt und die dabei auftretenden Fehler können minimiert werden. Die Bestellung mittels elektronischem (pdf) Formular reduziert Fehler infolge Missverständnisse, u.a. weil in den Bestellformularen eine Plausibilitätsprüfung eingebaut werden kann und weil dank der verbesserten Lesbarkeit elektronischer Formulare die Bestellung schneller und mit deutlich weniger Fehler erfasst und ausgelöst werden kann.

Auch die Rechnungsstellung von Dienstleistungen, welche der Mehrwertsteuer unterliegen, kann gemäss einer Verordnung (EIDI-V) des Eidgenössischen Finanzdepartements auf elektronischem Weg erfolgen und beim Empfänger schneller bearbeitet werden. Eine elektronische Signatur unter der Bestellung hilft die Abstreitbarkeit und etwelche andere Missbräuche zu unterbinden. Eine Unterschrift als Quittung bei der Abwicklung von Teilprozessen in der Logistik erhöht die Nachvollziehbarkeit und erleichtert das Controlling.

Zeitstempeldienst

Ein elektronischer Zeitstempeldienst ist eine mit einer elektronischen Signatur und Zeitangabe versehene Beglaubigung, dass ein elektronisches Dokument oder eine Datei zum besagten Zeitpunkt vorgelegen hat. Im Unterschied zur realen Welt muss für die Beglaubigung das betreffende Dokument nicht offen gelegt werden. D.h. die Vertraulichkeit wird bei der Beglaubigung nicht verletzt oder beeinträchtigt! Gerade dort, wo Forschungsergebnisse zeitkritisch wegen patentrechtlichen Implikationen gewonnen werden, drängt sich unter Umständen die Einführung von Zeitstempeldiensten zum Nachweis auf, dass allenfalls später eingereichte Patentanmeldungen Dritter zum Zeitpunkt der Einreichung bereits dem Stand der Technik entsprachen. Zeitstempeldienste müssen von einem nach ZertES anerkannten Zertifizierungsdienstanbieter angeboten und können folglich auch dort bezogen werden. Zeitstempeldienste werden ebenfalls in der elektronischen Archivierung eingesetzt, insbesondere bei der Archivierung von elektronisch signierten Dokumenten zur Wahrung der Beweiskraft der elektronischen Signatur.

Corporate Security

Mit auf elektronischen Zertifikaten basierten Sicherheitstechnologien lassen sich u.a. folgende allgemein bekannte Sicherheitsdienste realisieren:

- *Schutz der E-Mail*

Der Austausch und die Ablage der E-Mails können einfach und benutzerfreundlich bezüglich Authentizität, Integrität und Vertraulichkeit geschützt werden. Anmerkung: Das Herunterladen von E-Mails via eines Handheld wie Blackberry schützt nicht vor Einsichtnahme durch Dritte!

- *Protokollierung interner Vorgänge*

Die Protokolle von Teilprozessen oder ganzen Abläufen können elektronisch signiert werden und sind somit bezüglich Nachweisbarkeit besser abgesichert.

- *Verschlüsselte Ablage von sensitiven Informationen*

Sensitive Informationen können mittels Schlüssel und Zertifikaten chiffriert abgelegt werden. Im Unterschied zu herkömmlichen Technologien wird hier das Schlüsselmanagement enorm erleichtert.

- *Der online Zugriff auf sensitive Daten über das Netz*

Mit den Sicherheitstechnologien SSL/TLS, IPSec, Secure Shell (SSH) lässt sich der Zugriff auf sensitive Daten einschränken und deren Transport besser schützen. Mit SSH lassen sich entfernte (engl. remote) Server (vor

allem Unix) geschützt administrieren, während sich mit SSL/TLS der Web Zugriff, u.a. auf eine dahinterliegende Datenbank, schützen und mit IP-Sec die Kommunikation zwischen den verschiedenen Standorten des Unternehmens und die Kommunikation zu den Heimarbeitsplätzen besser absichern lässt.

- *Kommunikation zu den Prozessoren für die Sensortechnik*

Heute sind Mikroprozessoren sehr leistungsfähig geworden. Neben der SW für die automatische Erfassung und Weiterleitung von Messdaten an einen zentralen Standort kann nun auch SW einer Sicherheitstechnologie installiert und betrieben werden. Damit können die Messdaten vor Fälschung und ungewollter Einsichtnahme geschützt transportiert werden. Für in Amerika börsenkotierte Unternehmen kann sich eine verbesserte Corporate Security wegen der externen Revision infolge der Bestimmungen aus Sarbanes Oxley (in Zukunft) als erforderlich abzeichnen.

Wichtig

Es sollte unbedingt in den jeweiligen Ländern, wo ein Medikament zugelassen werden soll, vorgängig rechtlich abgeklärt werden, ob elektronische Protokolle der klinischen Untersuchungen mit einer elektronischen Signatur akzeptiert werden und welche Anforderung an die elektronische Signatur dafür besteht.

Beachtenswertes bei der Einführung von elektronischen Zertifikaten

Ohne etwelchen Anspruch auf Vollständigkeit werden im Folgenden einige Punkte aufgelistet, welche vor der Einführung und Ausbreitung von Zertifikaten zu beachten sind:

- *Rechtliche Kompatibilität*

Bevor die elektronische Signatur die Handunterschrift bei einem Prozess ablöst, sollte geklärt werden, ob dies rechtlich zulässig ist und welche Anforderungen aus den Erlassen an die elektronische Signatur gestellt werden.

- *Selber Herstellen oder Outsourcen*

Grundsätzlich stellt sich die Frage, ob die Zertifikate selber hergestellt oder von einem Dritten bezogen werden sollen. Sollen die Zertifikate zur Prüfung einer der Handunterschrift gleichgestellten Unterschrift erfolgen, so muss sich in der Schweiz der Zertifizierungsdienst anerkennen lassen, was ein nicht zu unterschätzender Kostenfaktor ist.

- *Einsatz von zertifizierten Produkten*

Der Einsatz von zertifizierten Produkten drängt sich dort auf, wo eine erhöhte Sicherheit gefordert ist, die Rechtslage dies erfordert oder wenn man Vorwürfe bezüglich Auswahl der Produkte gleich zu Beginn unterbinden will.

- *Aufbewahrung der Schlüssel und Anbindung von SmartCards*

Die zu den Zertifikaten korrespondierenden Schlüssel sollten besonders geschützt aufbewahrt werden. Unter anderem wird bei der der Handunterschrift gleichgestellten elektronischen Signatur gefordert, dass der Signierschlüssel in einem zertifizierten Produkt aufbewahrt wird. Die Kosten für die Ausbreitung von Zertifikaten und für die Einführung einer auf Zertifikat basierten Sicherheitstechnologie lassen sich nicht rechtfertigen, wenn die Schlüssel unsicher aufbewahrt werden und die Sicherheit dadurch kontaminiert wird. Deswegen sollten Smart Cards für die Aufbewahrung der Schlüssel im Benutzerumfeld eingesetzt werden. Beim Einsatz von SmartCards sollte darauf geachtet werden, dass diese sich leicht in die bestehende Sicherheitstechnologie einbinden lassen.

Klein beginnen, aber das Ganze nicht aus den Augen verlieren. Grundsätzlich sollte man klein beginnen, d.h. mit der Einführung einer zertifikatsbasierten Sicherheitstechnologie starten und dann weitere Technologien einführen. Beachten sollte man dabei, dass man sich nicht die Option, weitere Sicherheitstechnologien zu nutzen, verbaut.

- *Ablage verschlüsselter Informationen*

Bei der verschlüsselten Ablage von Informationen sollte Wert auf ein durchdachtes Schlüsselmanagement gelegt werden, ansonsten können diese Informationen bei Verlust des entsprechenden Schlüssels gegebenenfalls nicht mehr eingesehen werden.

- *Online Zugriff auf sensitive Informationen*

Beim geschützten online Zugriff auf sensitive Informationen sollte beachtet werden, dass meist nur der Transport, nicht aber die Ablage der Information geschützt wird.

- *Schulung der Mitarbeiter*

Sicherheit bedingt auch den fachmännischen Umgang und die richtige Anwendung der Sicherheitstechnologie. Ansonsten entstehen unbeabsichtigt Sicherheitslücken. Schulung kann Abhilfe schaffen, doch wird dieser Aspekt bei Einführung neuer Sicherheitstechnologien unterschätzt und folglich vernachlässigt.

- *Konzeption*

Ein detailliertes Konzept darüber, wie die Produkte genutzt werden sollen und wie die Nutzung realisiert werden soll, ist unerlässlich.

- *Projektorganisation*

Das Projekt zur Einführung und Nutzung von Zertifikaten sollte der Unternehmensstruktur entsprechend organisiert und zusammengesetzt sein.

Zusammenfassung

Mit Zertifikaten und deren Technologien lassen sich bestehende (Geschäfts-)Prozesse optimieren und gegen verschiedenste Gefahren viel besser absichern. Die rechtliche Kompatibilität der elektronischen Signatur sollte unter anderem dann beachtet werden, wenn die Handunterschrift in den jeweiligen Abläufen durch eine elektronische Signatur ersetzt werden soll. Auf sorgfältige Planung, auf stufengerechte Schulung und auf das Verfassen von Konzepten darf bei der Einführung und beim Einsatz elektronischer Zertifikate in einem Unternehmen nicht verzichtet werden. Bei erhöhtem Sicherheitsbedarf sollte auf zertifizierte Produkte Wert gelegt werden, wie dies der Gesetzgeber bei der Aufbewahrung der Schlüssel im Zusammenhang mit der elektronischen Signatur fordert. ■

Quellenangaben

[Mu] *Muster Daniel, Digitale Unterschriften und PKI, 3. Auflage 2006, ISBN 3-9522387-3-2*

[LP] *Lahti, Christian B., Roderick Peterson, Sarbanes Oxley, Syngress Publishing, ISBN 1-59749-036-9*

Erlasse

EIDI-V *Verordnung des EFD vom 30. Januar 2002 über die elektronisch übermittelten Daten und Informationen (SR 641.201.1)*

ZertES *Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03)*

Glossar: Die wichtigsten Begriffe kurz erklärt

Anbieterin von Zertifizierungsdienst (CSP) oder Zertifizierungsstelle (CA)
Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt.

Anerkennungsstelle
Stelle, die nach dem Akkreditierungsrecht für die Anerkennung und die Überwachung der Anbieterinnen von Zertifizierungsdiensten gemäss den Anforderungen des ZertES, der VZertES und dieser TAV akkreditiert ist.

Aussage über die Zertifizierungspraxen (CPS)
Aussage über die Regeln und Richtlinien, die von der Anbieterin von Zertifizierungsdiensten für die Ausstellung von Zertifikaten effektiv umgesetzt werden.

Benutzer/in des Zertifikats
Person oder Prozess, die oder der sich bei der Verwendung dieser Zertifikats auf die überprüften elektronischen Signaturen verlässt.

Digitales Zertifikat
elektronische Bescheinigung, die einen Signaturprüfschlüssel mit dem Namen einer Person verknüpft. In diesem Dokument ist der Terminus „Zertifikat" als „qualifiziertes Zertifikat" zu verstehen.

Elektronische Signatur oder Signatur
Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dieser Daten dienen.

Generierung der Zertifikate
Dienst der Anbieterin von Zertifizierungsdiensten; Erzeugung eines digitalen Zertifikats auf der Grundlage des Namens der Antragstellerin oder des Antragsstellers eines Zertifikats und ihrer/seiner allfälliger Attribute, die bei der Registrierung überprüft werden.

Inhaber/in des Zertifikats
Natürliche Person, die Inhaberin des Signaturschlüssels ist, der dem im Zertifikat aufgeführten Signaturschlüssel zugeordnet ist.

Liste der für ungültig erklärten Zertifikate (CRL)
Von der Anbieterin von Zertifizierungsdiensten signierte Liste, die alle Seriennummern der Zertifikate enthält, welche vor Ablauf ihrer Gültigkeit für ungültig erklärt werden.

Qualifizierte elektronische Signatur
elektronische Signatur, die folgende Anforderungen erfüllt:
1. Sie ist ausschliesslich der Inhaberin oder dem Inhaber zugeordnet
2. Sie ermöglicht die Identifizierung der Inhaberin oder des Inhabers
3. Sie wird mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer/seiner alleinigen Kontrolle halten kann
4. Sie wird durch eine sichere Signaturerstellungseinheit nach Artikel 6 Absatz 1 und 2 ZertES erzeugt
5. Sie ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann
6. Sie beruht auf einem qualifizierten und zum Zeitpunkt der Erzeugung gültigen Zertifikat

Qualifiziertes Zertifikat
Digitales Zertifikat, das die Anforderungen von Artikel 7 ZertES erfüllt.

Registrierung
Dienst der Anbieterin von Zertifizierungsdiensten, der darin besteht, die Identität und wenn nötig die Attribute jeder Antragsstellerin und jedes Antragstellers eines Zertifikats zu überprüfen, bevor ihr/sein Zertifikat erzeugt oder die Aktivierungsdaten (oder das Passwort) zur Aktivierung der Nutzung des Signaturschlüssels zugewiesen werden.

Schlüsselpaar
Signaturschlüssel und dazugehörender Signaturprüfschlüssel, die mathematisch durch einen asymmetrischen Signaturalgorithmus miteinander verknüpft sind.

Übersicht zu den rechtlichen Aspekten der elektronischen Signatur in der Schweiz

Seit dem Inkrafttreten des Bundesgesetzes über die elektronische Signatur (ZertES) am 1. Januar 2005 sind mehrere neue Erlasse in Kraft getreten und bestehende Gesetze im Zusammenhang mit der elektronischen Signatur überarbeitet worden.

Dr. iur. Thomas Hügi, Rechtsanwalt, Chief Operating Officer OPENLiMiT SignCubes AG
Daniel Muster, dipl. Physiker, NDS ETHZ
Autor des Buches: „Digitale Unterschriften und PKI"

Weitgehend praxisorientierte Gesetze, insbesondere im europäischen Umfeld, führen zu international zahlreichen Rechtsnormen betreffend die elektronische Signatur mit hohem „Ähnlichkeitsfaktor". Die Einhaltung internationaler Standards erlaubt die leichte Integration von am Markt vorhandenen Signaturlösungen in bestehende Anwendungen, was die technische Umsetzung der elektronischen Signatur wesentlich vereinfacht. Vielzählige Projekte in den Bereichen e-Government, e-Invoicing, e-Archiving, e-Banking oder e-Forms belegen die beschleunigte Entwicklung der elektronischen Signatur, nachdem diese während Jahren nur für technische Spezialisten ein Thema war.

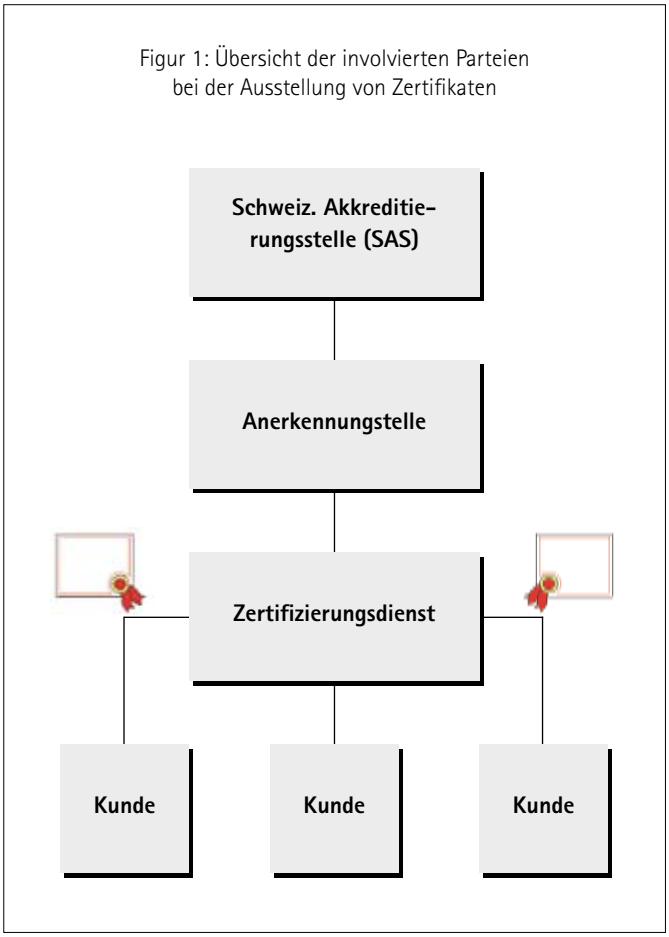
Die anerkannten Zertifizierungsanbieter der Schweiz sind unter www.sas.ch publiziert.

Bekanntlich hat der Schweizer Gesetzgeber die Thematik ebenfalls aufgenommen und entsprechende Regelungen getroffen. Dabei werden im ZertES insbesondere die Arten der elektronischen Signatur (qualifiziert, fortgeschritten und einfach) sowie die Rechte und Pflichten der Zertifizierungsdiensteanbieter geregelt. Von grosser Bedeutung ist die Gleichstellung der qualifizierten elektronischen Signatur mit der eigenhändigen Unterschrift im Schweizerischen Obligationenrechts (OR). Diese Regelung ist mittlerweile in allen EU-Mitgliedstaaten sowie weiteren europäischen und auch aussereuropäischen Ländern und damit international anerkannt getroffen worden.

Voraussetzungen für die Anwendung der elektronischen Signatur

Damit elektronische Signaturen verifiziert werden können, ist das zur Signatur passende Zertifikat erforderlich. Für die Erzeugung der Signatur benötigt der Anwender zusätzlich den zum Zertifikat passenden Signierschlüssel, der zusammen mit dem Zertifikat auf einer SmardCard gespeichert wird. Zudem sind ein Kartenleser für die Anbindung der SmartCard sowie eine Signatursoftware erforderlich. Im Zertifikat enthalten sind u.a. die Angaben des Inhabers des Zertifikats zu seiner (natürlichen oder juristischen) Person und der Schlüssel, welcher für die Erzeugung und Prüfung der Signatur benötigt wird. Die Zertifikate werden von einem Zertifizierungsdiensteanbieter (auch Trust Center) an dessen Kunden ausgestellt (s. Figur 1).

Figur 1: Übersicht der involvierten Parteien bei der Ausstellung von Zertifikaten



Weil die Zuordnung der „Unterschrift zur Person" im (elektronischen) Geschäftsverkehr wesentlich und in der digitalen Welt höheren Bedrohungen als in der realen Welt ausgesetzt ist, sind erhöhte Anforderungen an den Zertifizierungsdienstanbieter gestellt, welcher insbesondere qualifizierte Zertifikate zur Erzeugung und Prüfung einer der Handunterschrift gleichgestellten elektronischen Signatur ausstellt.

Ob die entsprechenden Anforderungen durch die Zertifizierungsdiensteanbieter erfüllt und eingehalten werden, wird von einer Anerkennungsstelle festgestellt (s. Figur 1). Die anerkannten (zertifizierten)

Zertifizierungsdienstanbieter in der Schweiz sind bei der Schweizerischen Akkreditierungsstelle (SAS) publiziert (s. Link [1]). Die Anerkennungsstelle selber wird wiederum von der Schweizerischen Akkreditierungsstelle, SAS (s. Link [2]) überwacht und zugelassen.

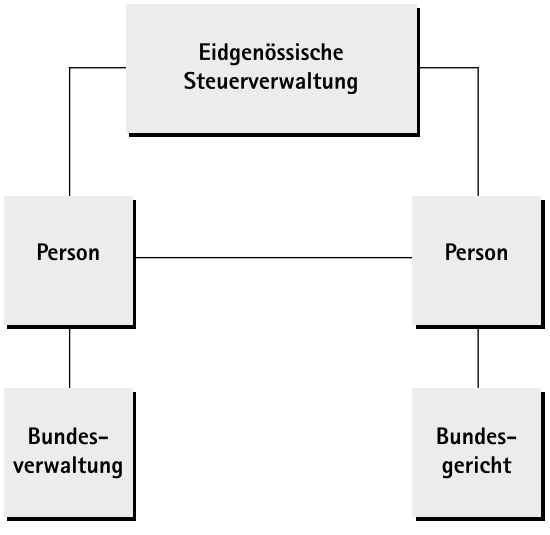
In Teilbereichen des eGovernments ist die elektronische Signatur bereits der Handunterschrift gleichgestellt.

Der Einsatz der elektronischen Signatur ermöglicht im Geschäftsverkehr die (rechtsverbindliche) medienbruchfreie Abwicklung von elektronischen Transaktionen wie beispielsweise bei der elektronischen Rechnungslegung, elektronischen Formularen (für Versicherungsanträge, Behördengesuche, etc.) oder der elektronischen, revisionssicheren Archivierung. Dies führt bei allen Beteiligten zu erheblichen Kosteneinsparungen und beschleunigten sowie weniger fehleranfälligen Prozessen.

Neben dem medienbruchfreien elektronischen Geschäftsverkehr unter Einsatz der elektronischen Signatur zwischen Unternehmungen oder Privaten existieren weitere Einsatzmöglichkeiten für die elektronische Signatur im behördlichen Umfeld (s. Figur 2). Seit dem 1. Januar 2007 können bei den Verwaltungsverfahren auf Bundesebene und beim Rechtsverkehr mit dem Bundesgericht und dem Bundesstrafgericht Rechtsschriften elektronisch eingereicht werden.

Mehrwertsteuerpflichtige Rechungen, die elektronisch abgewickelt werden, unterliegen gewissen Anforderungen, deren Einhaltung durch den Rechnungssteller von der Eidgenössischen Steuerverwaltung geprüft werden (s. Figur 2).

Figur 2: Einsatzmöglichkeiten der rechtsverbindlichen elektronischen Signatur.



Damit ist dargelegt, dass sich der Einsatz der elektronischen Signatur für alle elektronischen Geschäftsprozesse eignet und der Kreis der Anwender weit gezogen werden kann.

Geltende Regelungen

Das ZertES definiert vorab Begriffe im Zusammenhang mit der elektronischen Signatur und Zertifikaten (Art. 2, vgl. dazu Zitat Seite 11), regelt die Verwendungund Generierung der Schlüssel zur Erzeugung der elektronischen Signatur (Art. 6), legt die Aufgaben eines anerkannten Zertifizierungsdienstanbieters fest (Art. 8 – 14) und reglementiert deren Haftung (Art. 16) sowie diejenige der Anerkennungsstelle (Art. 17) für die Ausstellung elektronische Zertifikate zur (Erzeugung und) Prüfung von der eigenhändigen Unterschrift gleichgestellten elektronischen Signaturen. In der Verordnung zum ZertES (VZertES) und den technischen und administrativen Vorschriften des Bundesamtes für Kommunikation (TAV) werden u.a. die Aufgaben und Pflichten des anerkannten Zertifizierungsdienst anbieters, der Umgang mit den Schlüsseln zur Generierung der elektronischen Signatur mit den dazu passenden Zertifikaten näher umschrieben.

Art. 14 Abs. 2bis OR regelt, welche elektronische Unterschrift der eigenhändigen Unterschrift gleichgestellt ist. Die normalen obligationenrechtlichen Haftungsregeln werden ergänzt mit der Haftung für Signaturschlüssel in Art. 59a OR für der handschriftlichen Unterschrift gleichgestellte elektronische Signatur, die jedoch entfällt, wenn der Inhaber des Signaturschlüssel glaubhaft darlegen kann, dass er die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehren getroffen hat, um Missbrauch mit dem Signaturschlüssel zu verhindern. Der Einsatz zertifizierter Produkte wie Kartenleser oder Signatursoftware erleichtert dem Signaturschlüsselinhaber diese Haftungsabwendung.

Der elektronische Austausch von Rechtsschriften und die elektronische Eröffnung von Verfügungen im Verwaltungsverfahren auf Bundesebene werden im Bundesgesetz über das Verwaltungsverfahren (Art. 21a Abs. 1 VwVG) geregelt und in der Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens näher definiert. Bei Zustimmung der Parteien und bei Nennung einer Zustelladresse können Zustellungen der Behörden elektronisch erfolgen (Art. 11b Abs. 2 VwVG). So können Verfügungen im Verwaltungsverfahren bei Einverständnis der Partei auf elektronischem Weg eröffnet werden (Art. 34 Abs. 1bis VwVG). Der Bundesrat kann auf dem Verordnungsweg in den kommenden Jahre die elektronische Eingabe von Schriften für bestimmte Behörden und Verfahren während der nächsten 10 Jahren einschränken oder ausschliessen.

Der elektronische Zugang ans Bundesgericht wird im Bundesgerichtsgesetz (Art. 42 Abs. 4 BGG) und im Bundesgesetz über die Bundesstrafrechtspflege (Art. 99 BStP) festgehalten und im Regelement des Bundesgerichts (ReRBGer) näher bestimmt. Zudem können bei Einverständnis der Parteien Zustellungen vom Bundesgericht auch elektronisch erfolgen (Art. 39 Abs. 2 BGG). So kann ein Entscheid des Bundesgerichts auf elektronischem Weg eröffnet werden (Art. 60 Abs. 3 BGG).

Wie die mehrwertsteuerkonforme elektronische Rechnungsstellung ausgestaltet sein muss, wird in der Verordnung des Eidgenössischen Finanz-

departements über elektronische Daten und Informationen (EIDI-V) und in den technischen und administrativen Vorschriften des EFD [TAV-EFD] geregelt.

Schlussbemerkungen

Die gesetzlichen Regelungen für den Einsatz der elektronischen Signatur im Hinblick auf die medienbruchfreie (rechtsverbindliche) Gestaltung von elektronischen Geschäftsprozessen sind vorhanden – in der Schweiz und flächendeckend im europäischen Umfeld. Für die Unterstützung der weiteren Verbreitung des E-Government auf kantonaler und kommunaler Ebene scheinen Erlasse auf diesen Stufen in Ergänzung zu den bundesrechtlichen Vorschriften sinnvoll.

Regelungsbedarf besteht noch im Bereich der Archivierung elektronisch signierter Dokumente, insbesondere im Zusammenhang mit der Erhaltung der Beweiskraft der geleisteten elektronischen Signatur. International anerkannte Standards wie CWA 14170 und 14171 könnten als Grundlage für entsprechende Regelungen herangezogen werden.

Weil der elektronische Behördenzugang landesweit nicht einheitlich geregelt worden ist, besteht die Gefahr, dass einzelne Behörden dazu unterschiedliche Vorschriften erlassen, welche mit bereits bestehenden Erlassen (technisch oder rechtlich) kollidieren könnten. Dies würde den optimalen Einsatz der elektronischen Signatur und damit wirtschaftliches Sparpotenzial beeinträchtigen. Eine übergeordnete Aufsichtsinstanz zu Erlassen im Zusammenhang mit der elektronischen Signatur zwecks Vermeidung widersprüchlicher Regelungen könnte Abhilfe schaffen. Im Grundsatz aber liegt es jetzt an Wirtschaft und Verwaltung, durch den Einsatz der elektronischen Signatur das enorme Sparpotenzial des medienbruchfreien Workflows zu nutzen. ■

Quellenangaben

[1] *Link zur Liste der anerkannten Zertifizierungsdienstanbieter http://www.seco.admin.ch/sas/00229/00251/index.html?lang=de*

[2] *Link zur Schweizerischen Akkreditierungsstelle: www.sas.ch*

CWA 14170 *CEN (European Committee for Standardization), Security Requirements for Signature Creation Applications, May 2004 (http://www.cen.eu/cenorm/homepage.htm)*

CWA 14171 *CEN (European Committee for Standardization), General Guidelines for electronic signature verification, May 2004 (http://www.cen.eu/cenorm/homepage.htm)*

DigSig *Dokument DigSig der gleichnamigen Fachgruppe des Vereins eCH zur Standardisierung im eGovernment. Das Dokument kann dort (www.ech.ch) kostenlos heruntergeladen werden. Darin ist unter anderem auch ein Glossar enthalten und das Prinzip von PKI kurz dargestellt.*

Erlasse

[TAV] *Technische und administrative Vorschriften des BAKOM vom 6. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1). Die dritte Fassung ist seit 1.12.06 in Kraft.*

[TAV-EFD] *Technische und administrative Vorschriften vom 12. Oktober 07 über Zertifizierungsdienste im Bereich der EIDI-V im Zusammenhang mit der Ausstellung von Zertifikaten basierend auf fortgeschrittenen Signaturen (SR 641.201.11 /Anhang)*

1999/93/EG *Richtlinie der Europäischen Union über die gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*

AkkBV *Verordnung vom 17. Juni 1996 über das Schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitätsbewertungs-, Anmelde- und Zulassungsstellen (SR 946.512)*

BGG *Bundesgesetz vom 17. Juni 2005 über das Bundesgericht (SR 173.110)*

BStP *Bundesgesetz 15. Juni 1934 über die Bundesstrafrechtspflege (SR 312.0)*

EIDI-V *Verordnung des EFD vom 30. Januar 2002 über die elektronisch übermittelten Daten und Informationen (SR 641.201.1)*

OR *Schweizerisches Obligationenrecht vom 30. März 1911 (SR 220)*

ReRBGer *Regelement des Bundesgerichts vom 5. Dezember 2006 über den elektronischen Rechtsverkehr mit Parteien und Vorinstanzen (SR 173.110.29)*

VwVG *Verordnung vom 17. Oktober 2007 über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (172.012.2)*

VG *Bundesgesetz vom 14. März 1958 über die Verantwortlichkeit des Bundes sowie seiner Behördemitglieder und Beamten (Verantwortlichkeitsgesetz) (SR170.32)*

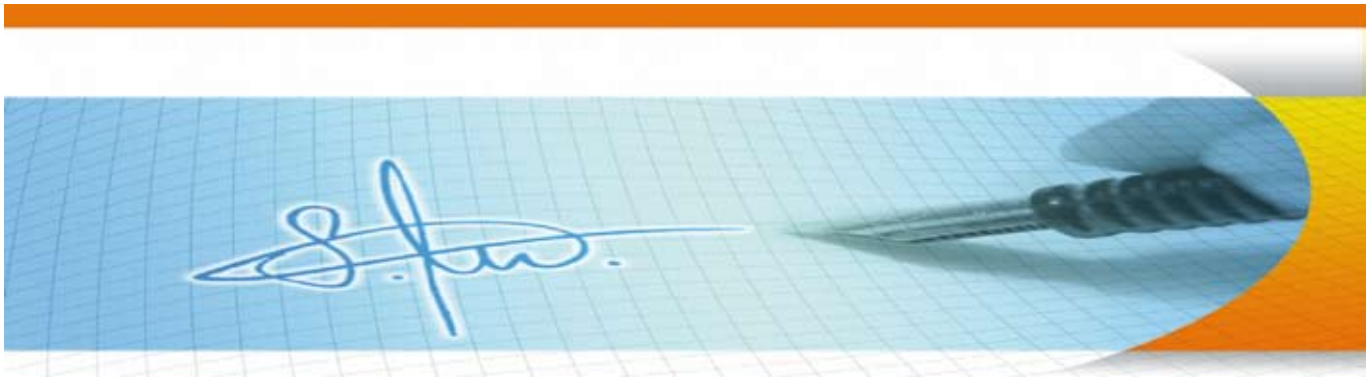
VGG *Bundesgesetz vom 17. Juni 2005 über das Bundesverwaltungsgericht (SR 173.32)*

VwVG *Bundesgesetz vom 20. Dezember 1968 über das Verwaltungsverfahren (SR 172.021)*

VZertES *Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032)*

ZertES *Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektro-*

OPENLiMiT Just sign it – Einfach verbunden



OPENLiMiT ist ein führendes IT-Unternehmen für Sicherheits-, Dokumenten- und Archivtechnologien im Zusammenhang mit elektronischen Signaturen mit Sitz in Baar/Schweiz und einer Niederlassung in Berlin/Deutschland. OPENLiMiT ist an der Deutschen Börse in Frankfurt (General Standard) und Berlin Bremen, München, Düsseldorf und Stuttgart (Freiverkehr) notiert (WKN/Symbol/ISIN: A0F5UQ/O5H/CH0022237009).

Unterschrift per Mausklick

Dokumente müssen ausgedruckt, versendet und auf der Empfängerseite wieder in einen Rechner eingegeben werden. Kostenintensive Medienbrüche und ein erhebliches Potential für Eingabefehler entstehen. Die Online-Abwicklung von Transaktionen zwischen Unternehmen, Behörden und Privatpersonen unter Einsatz der elektronischen Signatur können diese Verfahren erheblich beschleunigen und Kosten deutlich senken. Auch bei der elektronischen Archivierung. Den Schlüssel dazu bietet OPENLiMiT.

Kompetenz durch Innovation

OPENLiMiT zeichnet sich aus durch die hochstehende Entwicklung und Vermarktung von kundenorientierter, zuverlässiger und international zertifizierter Signatursoftware. Gleichzeitig steht OPENLiMiT seinen Kunden mit fachlicher Kompetenz und bestem Service zur Seite.

Partnerschaftliche Synergien

OPENLiMiT arbeitet eng mit namhaften Partnern wie Adobe Systems, CSC, Fujitsu Siemens Computers, Ingram Micro, Microsoft, Sun Microsystems, dem Deutschen Sparkassenverlag und Swisscom Solutions zusammen. Adobe Systems hat die "Intelligente PDF-Datei" mit integriertem Feld zur Signaturerzeugung entwickelt. Bei Online-Formularen kann neben weiteren multimedialen Inhalten eine qualifizierte elektronische Signatur mit der OPENLiMiT-Signatursoftware erzeugt werden. Diese ist in den EU-Mitgliedstaaten, der Schweiz und vielen anderen Ländern gesetzlich der handschriftlichen Unterschrift gleichgestellt.

OPENLiMiT Produkte

Die Sicherheitstechnologien von OPENLiMiT bestehen aus einer universell anwendbaren Signatursoftware mit Verschlüsselungsfunktion, die als derzeit einzige weltweit nach Common Criteria EAL4+ zertifiziert ist. Die OPENLiMiT-Dokumenten- technologien stellen einen PDF-, PDF/A- und TIFF-Producer zur Verfügung und ermöglichen zum Beispiel die Zusammenführung oder Reparatur von PDF-Dokumenten. Die Archivtechnologien von OPENLiMiT ergänzen Archivlösungen im Hinblick auf das gesetzeskonforme und revisionssichere Langzeitarchiv.

OPENLiMiT Services

Neben Implementation-, Consulting- und Training Services bietet OPENLiMiT über seinen Partner Fujitsu Siemens Computers europaweit umfassende Support-Dienstleistungen für alle OPENLiMiT-Produkte an. Der Kunde kann eine kostenpflichtige Hotline anrufen, ein Support-Package für ein Jahr Softwarepflege erwerben oder einen Softwarepflegevertrag abschliessen.

Die Vorteile liegen auf der Hand

Die elektronische Signatur ist der Schlüssel für den medienbruchfreien elektronischen Workflow. Zusätzlich zur OPENLiMiT Signatur Software benötigt man ein elektronisches Zertifikat (z.B. auf einer Signaturkarte in Checkkartenformat mit einem Kartenlesegerät, das mit dem PC verbunden wird). Der Empfänger kann den Autor einer elektronischen Nachricht einwandfrei prüfen (Authentizität) und feststellen, ob die empfangene Datei während der Datenübermittlung verändert wurde (Integrität). Dies führt bei allen Beteiligten zu erheblichen Kosteneinsparungen. ■

OPENLiMiT SignCubes AG – Zugerstrasse 76b – CH-6341 Baar
Phone. +41 41 560 10 20 – Fax +41 41 560 10 39
info@openlimit.com – www.openlimit.com