21.2.2002

Zu eCommerce, elektronischer Signatur usw.

Matthias Neumayr

1. Rechtliche Grundlagen ... 2
1.1. Beispiel Kauf ... 2
1.2. Vertragsschluss über das Internet ... 2
1.3. Weitere Probleme beim Vertragsschluss über das Internet ... 3
1.3.1. Schriftform ... 4
1.3.2. Zweck der Unterschrift ... 4
1.3.3. Anforderungen im elektronischen Rechtsverkehr ... 4
1.3.3.1. Elektronische Übermittlung von eigenhändigen Unterschriften? ... 5
1.3.3.2. Prüfung der Identität der Geschäftspartner ... 5
1.3.3.3. Übertragungsfehler, Verfälschung während der Übertragung ... 6
1.3.3.4. Weitere Risiken bei der elektronischen Übermittlung ... 6
1.4. Zweck der elektronischen Signatur ... 6
2. Verschlüsselungstechniken ... 8
2.1. Symmetrische Verschlüsselung ... 8
2.2. Asymmetrische Verschlüsselung ... 9
3. Digitale (Elektronische) Signatur ... 9
3.1. Eigenschaften digitaler Signaturen ... 10
3.2. Die praktische Umsetzung der elektronischen Signatur ... 11
3.2.1. Ein Beispiel ... 11
3.2.2. Zugang zum Public Key des Versenders ... 12
3.2.3. Grafik ... 13
3.3. Zertifizierungsstellen ... 13
3.4. Ausländische Zertifikate ... 15
4. Das österreichische Signaturgesetz ... 15
5. Anwendungsbereiche der elektronischen Signatur bei der Übermittlung von Daten ... 17
5.1. eCommerce, eBusiness, eBanking ... 17
5.2. Der Einsatz der Signatur in der öffentlichen Verwaltung ... 17
5.2.1. eGovernment ... 17
5.2.2. Finanz-Online ... 18
5.2.3. Gesundheitsbereich ... 19
6. Zusammenfassung zur elektronischen Signatur ... 19
7. Anpassungen des österreichischen Rechts an den eCommerce ... 20
7.1. eCommerce ... 20
7.1.1. E-Commerce-Gesetz (ECG) ... 20
7.1.2. Fernabsatzgesetz ... 21
7.2. Zahlungssysteme ... 21
7.2.1. Klassische Zahlungsarten ... 21
7.2.1.1. Zahlung mit Kreditkarte ... 21
7.2.1.2. Zahlung per Nachnahme ... 22
7.2.1.3. Zahlung per Vorauskasse ... 22
7.2.2. An das Internet adaptierte Verfahren ... 22
7.2.2.1. SET (Secure Electronic Transaction) ... 22
7.2.2.2. bezahlen.at ... 22
7.2.2.3. Cybergeld ... 23
7.2.2.4. Inkasso per Telefonrechnung ... 23

1. Rechtliche Grundlagen

1.1. Beispiel Kauf

Wenn ich in einem Geschäft eine DVD kaufe, kommt ein

V e r t r a g

zustande.

Der Vertrag beruht darauf, dass Verkäufer und Käufer einen übereinstimmenden Willen haben: Der Verkäufer möchte die DVD um einen bestimmten Preis verkaufen, und der Käufer will die DVD kaufen.

Oder mit anderen Worten:

Eine der beiden Vertragsparteien bietet etwas an, und die zweite nimmt das Angebot an.

A n g e b o t	**und**	**A n n a h m e**

Der Wille der Vertragsparteien muss nach außen zum Ausdruck kommen:

ausdrücklich	oder	**schlüssig** (konkludent)
Schriftlich oder mündlich		aus einer Handlung heraus (zB Münzeinwurf)

Beim Einkauf im „gewöhnlichen Geschäftsverkehr“ üblicherweise ist ziemlich eindeutig

- **welche Personen** den Vertrag miteinander schließen
- was der **Inhalt** des Vertrages ist.

Wichtig sind diese Elemente vor allem dann, wenn es irgendwelche Probleme gibt: Wenn ich zu Hause drauf komme, dass die DVD einen Defekt hat, kann ich mich mit dem Problem an meinen Vertragspartner wenden.

1.2. Vertragsschluss über das Internet

Es besteht kein Zweifel, dass es möglich ist, über elektronische Medien Bestellungen und Annahmeerklärungen zu übersenden, sei es beim Kauf von Waren, sei es bei der Buchung eines Fluges. Der Begriff **eCommerce** – der elektronische Geschäftsverkehr zwischen Händlern und Kunden über das Internet - ist längst in aller Munde, nicht nur in den USA, sondern auch in Europa. Die eServices im Internet und vor allem der eCommerce haben sich zu einem der wachstumsstärksten und zukunftsträchtigsten Wirtschaftsbereiche entwickelt.

Entwicklung Österreich (Salzburger Nachrichten 19.2.2002):

- *mit Ende 2001 haben 48% der Haushalte einen PC (Ende 2000: 43%)*
- *Ende 2001 sind 29% der Haushalte (930.000 Haushalte) online (Juli 2001: 23%)*
- *in jedem dieser Haushalte gibt es im Durchschnitt 2,2 Internet-User*
- *Ende 2001 waren damit etwa 2 Millionen Österreicher privat online*
- *knapp 1,3 Mio Österreicher sind in den Firmen online*
- *zusammengerechnet sind etwa 2,7 Mio Österreicher im Internet (41%)*
- *22% aller US-Haushalte shoppen im Netz*

Bei den Usern steht die Verwendung des Internet für eMail an oberster Stelle (79%). 34% führen online Überweisungen oder Kontoabfragen durch. 22% gegen online shoppen und 13% nutzen auch die Online-Buchung für Reisen oder Hotels.

Laut dem „Internet-Monitor" des Linzer Meinungsforschungsinstituts Spectra lassen die Prognosedaten eine weitere lebhafte Entwicklung in Österreich erwarten. Laut Hochrechnung sollen Ende 2002 etwa 35% der Haushalte online sein. Bemerkenswert ist (zumindest derzeit noch), dass online-Shopper im Schnitt mehr Geld ausgeben (höhere Einkommen).

„eWeihnachten"
http://futurezone.orf.at/futurezone.orf?read=detail&id=52728&tmp=6426 (27.12.2000):
Weihnachten ließ die Kassen klingeln
Die Online-Einkäufe der Amerikaner haben sich in der Zeit von Anfang November 2000 bis zum 17. Dezember 2000 im Vorjahresvergleich mehr als verdoppelt. Sie erreichten 8,7 Milliarden Dollar [9,4 Mrd €] nach 4,2 Milliarden Dollar im entsprechenden Vorjahresabschnitt 1999.

Das Recht hat beträchtliche Schwierigkeiten, mit der rasanten technischen Entwicklung Schritt zu halten. Zum Teil kann mit vorhandenen Rechtsfiguren das Auslangen gefunden werden, was aber oft beträchtliche Unsicherheit mit sich bringt, weil eine Anwendung bestehender Rechtsvorschriften nicht ganz zu den neuen Techniken und Möglichkeiten "passt".

Anders als etwa beim Kauf in einem Geschäft, bei dem Verkäufer und Käufer in einen direkten Kontakt treten, ist bei Geschäften über das Internet die **Identität der potentiellen Vertragspartner** vorerst **ungeklärt**. Es ist auch unklar, aus welchem Land sie kommen und welcher Rechtsordnung sie unterstehen.

Rein nationale Regelungen sind hier auf Dauer nicht erfolgversprechend. Gerade im Europäischen Binnenmarkt (Stichwort: „Vier Freiheiten") war es auf Dauer unumgänglich, Maßnahmen zur Sicherung der vier Freiheiten im Zeitalter des elektronischen Geschäftsverkehrs zu setzen.

1.3. Weitere Probleme beim Vertragsschluss über das Internet

1.3.1. Schriftform

Das österreichische Recht geht so wie das deutsche Recht grundsätzlich von der **Formfreiheit von Willenserklärungen** aus. Ein Vertrag kommt also auch zustande, wenn er nicht schriftlich fixiert ist.

In einigen Fällen ist aber die Schriftform erwünscht oder vorgeschrieben. Schriftform bedeutet, dass der Vertrag in **schriftlicher** Form (mit der Hand, der Maschine oder dem PC geschrieben) mit **eigenhändiger Unterschrift** vorliegen muss.

- Ein Vertrag soll aus Beweisgründen schriftlich erstellt werden (es geht dabei vor allem um die Gewissheit, **wer** aus dem Vertrag berechtigt und verpflichtet ist und **welche** Rechte und Pflichten eingegangen wurden. Dieser Erklärungsinhalt wird für die Zukunft festgehalten.
- Darüber hinausgehend bedarf ein Rechtsverkehr zwischen Abwesenden, wie er bei uns gang und gäbe ist, überhaupt der Möglichkeit der schriftlichen Niederlegung.
  zB Bestellung: „*Ich bestelle 50 Stück Overhead-Folien für einen Inkjet-Drucker.*“
- In manchen Fällen ist eine besondere Form gesetzlich vorgeschrieben.
  Beispiele:
  - Verpflichtungserklärung des Bürgen (Zweck?)
  - Eigenhändiges Testament: es muss nicht nur die Unterschrift vorhanden sein, sondern es ist für die Gültigkeit sogar erforderlich, den gesamten Text eigenhändig, also mit der Hand zu schreiben (Zweck?).
  - Unterschriftsleistung bei der Eröffnung eines Kontos (Zweck?)
  - Rechtsgeschäfte über Liegenschaften/Grundstücke (Zweck?)

In anderen Staaten der Welt gibt es weitergehende Regeln. In den USA beispielsweise müssen die meisten Konsumentengeschäfte ab einer Wertgrenze von US-$ 500,-- schriftlich getätigt werden.

1.3.2. Zweck der Unterschrift

Die Unterschrift dient im wesentlichen drei Zwecken:

- zum einen dient sie der Feststellung der **Identität** des Unterschreibenden;
- zum anderen wird damit in der Regel zum Ausdruck gebracht, dass sich der Unterzeichner mit dem Inhalt eines verfassten Dokuments **identifiziert** und ihn in dieser Form **akzeptiert**;
- schließlich kommt der Unterschrift auch noch eine gewisse **Warnfunktion** zu: der Unterzeichner setzt durch die Unterfertigung *bewusst* eine Handlung, an die sich Rechtsfolgen knüpfen können.

1.3.3. Anforderungen im elektronischen Rechtsverkehr

Mit der technischen Entwicklung ist der Geschäfts- und Rechtsverkehr nicht mehr auf den mündlichen und schriftlichen Nachrichtenaustausch beschränkt. Nach Telegraphie, Telefon

und Telefax steht der **direkte Filetransfer** durch Anwendungen wie eMail oder WWW im Vordergrund.

Hinter dieser Entwicklung moderner Informations- und Kommunikationstechniken stehen vor allem praktische und wirtschaftliche Gründe: Im Vergleich zu herkömmlichen Übermittlungsmethoden ermöglichen die elektronischen Medien eine schnellere und – zumindest im internationalen Verkehr – auch meist billigere Übermittlung. Außerdem lässt sich die elektronische Übermittlung problemlos an die Textverarbeitung im Büro anschließen.

1.3.3.1. Elektronische Übermittlung von eigenhändigen Unterschriften?

Überträgt man die von der österreichischen Rechtsordnung zum herkömmlichen Geschäftsverkehr aufgestellten Anforderungen an die Schriftform auf den elektronischen Geschäftsverkehr, kann man davon ausgehen, dass jedenfalls Verpflichtungserklärungen, für die die Schriftform gefordert wird, nicht über elektronische Netze übermittelt werden können, weil **keine Originalunterschrift** übermittelt werden kann.

> Weitere Problembereiche sind beispielsweise, ob eine per eMail versandte Rechnung als Beleg im Sinne des Umsatzsteuerrechts gilt.

1.3.3.2. Prüfung der Identität der Geschäftspartner

Bei Bestellungen im Internet ist die **Identität des Bestellers schwer überprüfbar**. In den meisten EDV-Systemen und auch im Internet werden Benutzer durch Eingabe eines Benutzernamens und eines Kennworts identifiziert. Der durchschnittliche Internet-Benutzer erhält vom Rechner des Service-Providers eine allgemein gültige Netzwerkadresse zugeordnet, die bei jeder Art von Übertragung in jedem Datenpaket mitgesendet wird und die sich bei jeder Internet-Sitzung ändern kann. Bei Internet-Mail erfolgt überhaupt keine Überprüfung der Identität des Absenders einer Nachricht. Es kann also praktisch jeder Internet-Benutzer unter einem beliebigen Namen Bestellungen absenden.

Neben die hier nicht näher zu thematisierende fehlende Vertraulichkeit der Kommunikation im Internet tritt also die **mangelnde Vertrautheit** mit dem Kommunikationspartner - man sieht sein Gegenüber nicht und kann nicht einschätzen, ob die Informationen tatsächlich von der Person kommen, die man erwartet.

Natürlich gibt es das auch im „normalen" Geschäftsverkehr - aber wir haben Wege gefunden, damit umzugehen. Auf die elektronische Kommunikation lassen sich unsere Erfahrungen aber nicht problemlos übertragen: „*Falsche Gesichter und verstellte Stimmen können wir leicht erkennen, eine gefälschte Email hingegen kaum.*" (*Mayer-Schönberger/Pilz/Reiser/Schmölzer*, Signaturgesetz (1999), 3).

Dafür, dass andere Personen als der Inhaber des Kennworts unter dessen Namen Bestellungen tätigen oder sonstige Willenserklärungen abgeben, kommen vor allem Personen in Frage, die in einer Nahebeziehung zum Inhaber stehen, etwa Familienmitglieder oder Unternehmensangehörige.

Bei Bestellungen von Kindern und Dritten stellt sich vor allem die **Beweisfrage**: Wer muss beweisen, dass ein Unbefugter eine fremde Identität ge- oder missbraucht hat? Wer muss beweisen, ob ein Fall einer Anscheinsvollmacht vorliegt, etwa weil der Vater dem Sohn oder der Tochter die Kennwörter anvertraut hat oder weil das Kennwort „benutzerfreundlich" abgespeichert wurde? Der Erklärungsempfänger hat regelmäßig nur Hinweise auf diejenige Person, deren Name in der Absenderadresse einer Mitteilung auftaucht.

Nach allgemeinen Regeln liegt die **Beweislast** beim **Anbieter**, dass wirklich ein bestimmter Nutzer bei ihm bestellt hat oder die Bestellung einem bestimmten Nutzer zuzurechnen ist.

1.3.3.3. Übertragungsfehler, Verfälschung während der Übertragung

Wichtig ist aber auch der Aspekt, wem mögliche **Übertragungsfehler** – etwa durch technische Gebrechen - zuzurechnen sind. Informationen werden im Internet zwar gesichert übertragen, indem der empfangende Rechner anhand einer Prüfziffer nachrechnet, ob ein übertragener Datenblock während der Übertragung verändert wurde. Allerdings bietet diese Methode keinen hundertprozentigen Schutz gegen Übertragungsfehler. Es ist also nicht auszuschließen, dass aus einer Bestellung von 10 Tonnen Papier eine solche von 100 Tonnen wird.

Auch hier gilt die allgemeine Regel, dass Erklärungen auf **Risiko des Erklärenden** reisen, bis sie in den Einflussbereich des Empfängers gelangen. In den Einflussbereich des Empfängers ist eine Nachricht gelangt, wenn er die Möglichkeit des Zugriffs auf die Mitteilung beim Provider hat. Übertragungsfehler auf dem Weg der Nachricht vom PC des Absenders bis zum Rechner des Empfängers (bzw seines Providers) sind dem Absender zuzurechnen, den auch für Beweislast für das Vorliegen eines Übertragungsfehlers trifft. Der Empfänger der Nachricht trägt das Risiko, dass die Nachricht in seinem Rechner bzw in seinem lokalen Netz verfälscht wird.

1.3.3.4. Weitere Risiken bei der elektronischen Übermittlung

Elektronische Informationen sind flüchtig und relativ **leicht veränderbar**. Sowohl technische Fehler als auch absichtliche Manipulationen können von den Betroffenen nicht oder nur schwer erkannt werden. Dadurch wird der Beweiswert elektronischer Dokumente erheblich eingeschränkt – so wie es in Ansätzen auch schon beim Telefax der Fall war, obwohl dieses noch die Sicherheit der konventionellen Schriftlichkeit suggeriert.

Man darf sich aber auch nicht der Illusion hingeben, dass ein Beharren auf der „Schriftlichkeit", so wie wir sie kennen, Probleme vermeiden helfen könnte. Hochwertige Kopiertechniken und Computerprogramme vereinfachen auch das Nachahmen und Fälschen von Schriftdokumenten. Auch der Bereich der konventionellen Schriftlichkeit wird immer mehr mit Unsicherheiten konfrontiert.

1.4. Zweck der elektronischen Signatur

Mit der elektronischen Signatur soll im wesentlichen die Funktion der eigenhändigen Unterschrift in den elektronischen Bereich übertragen werden. Im österreichischen Signaturgesetz (SigG) wird die elektronische Signatur als „*elektronische Daten, die anderen*

*elektronischen Daten beigefügt werden oder mit diesen verknüpft werden und die der **Authentifizierung, also der Feststellung der Identität des Signators**, dienen*“, definiert.

Dazu kommt aber auch noch der Zweck, die **Integrität der Nachricht** zu gewährleisten.

Im Moment kommt weltweit nur ein technisch ausgereiftes Konzept zum praktischen Einsatz – nämlich die Erzeugung „digitaler Signaturen“ (nunmehr spricht man allgemeiner und technologieneutraler von „elektronischen Signaturen“) mittels Anwendung ***asymmetrischer Kryptographie und Hash-Codes***: Zur Sicherung der Identität des Absenders einer Nachricht wird gemeinsam mit dem elektronisch signierten Dokument auch noch ein Zertifikat mitgeliefert, das die Identität des Senders beurkundet.

Die derzeit verwendete elektronische Signatur hat also ihren Ursprung in der Verschlüsselung – wobei beim Einsatz der elektronischen Signatur die Verschlüsselung des gesendeten Textes in den Hintergrund rückt. Entscheidend sind hier die Feststellbarkeit der **Identität des Absenders** und die Gewährleistung der **Integrität der Nachricht**.

2. Verschlüsselungstechniken

Daten können während der Übertragung auf Leitungen von technisch Versierten mitgelesen und/oder verfälscht werden. Für die sichere Übertragung von Daten stehen Verschlüsselungstechniken zur Verfügung. Die Daten werden dabei für die Dauer der Übertragung verändert und unlesbar gemacht, sodass sie für einen Außenstehenden keinen Sinn ergeben.

Bei der Verschlüsselung werden die lesbaren und zu schützenden Daten

(**Klartext**)

mit Hilfe eines mathematischen Verfahrens unter Verwendung eines

Schlüssels

(das ist eine Kombination von Zeichenketten) dermaßen abgeändert, dass sie nicht mehr erkannt werden können und bei der Betrachtung keinen Sinn ergeben

(**Schlüsseltext**).

Die

Entschlüsselung

wandelt diese unscheinbaren Daten mit einem mathematischen Verfahren, das auf die Verschlüsselung Bezug nimmt, wieder in die ursprüngliche Form, den Klartext, zurück. Der Schlüssel für Ver- und Entschlüsselung können gleich oder verschieden sein.

Je nachdem, ob der Schlüssel gleich oder verschieden ist, unterscheidet man zwei Verschlüsselungssysteme, die

symmetrische Verschlüsselung
(„Private Key-“ oder „Secret Key Encryption“)

und die

asymmetrische Verschlüsselung
(„Public Key Encryption“).

2.1. Symmetrische Verschlüsselung

Bei der **symmetrischen Verschlüsselung** erfolgen sowohl die Verschlüsselung als auch die Entschlüsselung mit einem gleichlautenden Schlüssel. Somit kann jeder, der in den Besitz des Schlüssels gelangt, die verschlüsselten Daten wieder entschlüsseln. Mit einer zunehmenden Anzahl an Teilnehmern steigt die Gefahr, dass der Schlüssel Außenstehenden bekannt wird. Außerdem kann bei der symmetrischen Verschlüsselung der Absender einer Nachricht nicht schlüssig identifiziert werden. Für den Geschäftsverkehr im Internet ist daher das System der symmetrischen Verschlüsselung nur bedingt tauglich.

2.2. Asymmetrische Verschlüsselung

Bei der **asymmetrischen Verschlüsselung** (Public-Key-Verfahren), das erstmals in den 70er Jahren von Mathematikern vorgeschlagen wurde, wird nicht mehr ein gemeinsamer vertraulicher Schlüssel verwendet, sondern zwei unterschiedliche, aber zusammengehörende Schlüssel. Das, was ein Schlüssel verschlüsselt, kann nur mit dem dazugehörigen anderen Schlüssel wieder entschlüsselt werden.

Ein Schlüssel des Schlüsselpaares – der „**Private Key**" – gehört nur dem Anwender und muss von diesem geheimgehalten werden (bzw weiß er ihn selbst nicht). Die Weitergabe des privaten Schlüssels zu verhindern ist eine Grundvoraussetzung für das Funktionieren des Systems.

Gesichert vor Zugriffen Unberechtiger wird dieser Private Key entweder mit

- einem Passwort
- einem PIN-Code (wie bei der Bankomat-Karte) oder
- durch Verwendung von eigens dafür vorgesehenen SmartCards mit Lesegeräten.

> *Anmerkung: Die Verwendung biometrischer Identifikationsdaten, etwa die Überprüfung des Fingerabdrucks des Teilnehmers, würde die Geheimhaltung ersparen, da es sich um ein einzigartiges Merkmal handelt, das nicht dupliziert werden kann. Mit der biometrischen Verifikation würde die Funktionalität der eigenhändigen Unterschrift in einem weiteren Maße erreicht.*

Der andere, dazugehörige Schlüssel – „**Public Key**" genannt – ist für alle anderen Teilnehmer gedacht, die mit dem Anwender kommunizieren wollen bzw sollen. Dieser Public Key wird öffentlich – etwa über das Internet - verbreitet und steht jedermann frei zugänglich zur Verfügung. Da aus dem öffentlichen Schlüssel nicht auf den privaten Schlüssel geschlossen werden kann, kann der öffentliche Schlüssel risikolos offengelegt werden.

> *Ein **Beispiel**: Verschlüsselt ein Absender seine Nachricht mit seinem geheimen Private Key, dann kann die Nachricht von jedermann mit dem frei zugänglichen öffentlichen Schlüssel des Absenders in lesbare Form umgewandelt werden. Aufgrund der Verschlüsselung mit dem Private Key des Absenders kann der Empfänger auch davon ausgehen, dass die Nachricht wirklich vom Absender stammt.*
>
> *Diese Technik bildet die Grundlage für die **digitale (oder elektronische) Signatur**.*

3. Digitale (Elektronische) Signatur

Einführung:

http://www.rdb.co.at/homepages/0001/cover.htm

http://www.www-kurs.de/pgp.htm

https://a-cert.argedaten.at/digsig.html

http://a-sign.datakom.at/content/zertdienst/einfuehrung/schritt1.html

http://a-sign.datakom.at/content/zertdienst/produkte/user.htm

http://www.generali.co.at/netsecurity.nsf?OpenDatabase

http://www.generali.co.at/netsecurity.nsf/0/AFBA5F8DA08404A9C12567DA00399DC4?OpenDocument (zuerst links auf „Technische Begriffe klicken“)

3.1. Eigenschaften digitaler Signaturen

Eine Nachricht, die der Anwender mit seinem geheimen Private Key verschlüsselt hat, kann von der Öffentlichkeit nur mit dem dazugehörigen Public Key des Anwenders entschlüsselt werden. Voraussetzung für die Zuordnung einer Nachricht zu einer bestimmten Person ist das Wissen, dass der Public Key dieser bestimmten Person zugeordnet werden kann. Diese Zuordnung

- das "Zertifikat" -

wird von besonderen Zertifizierungsstellen bestätigt.

> *Zertifikate sind mit Ausweisen (zB Mitgliedsausweisen) vergleichbar - sozusagen „Ausweise für das Internet“. Das Zertifikat stellt die Zuordnung einer elektronischen Signatur zu einer bestimmten Person her. Ein Zertifikat enthält den öffentlichen Schlüssel und bestimmte personenbezogene Daten, zumindest einen Namen. Es muss für den Empfänger einer digital signierten Nachricht – in der Regel online - abrufbar sein.*

Hierin liegt der **erste Vorteil** der digitalen Signatur: Es ist möglich, eine Nachricht **einem bestimmten Absender** zuzuordnen, der die Nachricht zwar nicht handschriftlich, aber eben elektronisch „signiert“ hat.

> Die elektronische Signatur hat also nichts mit der handschriftlichen Unterschrift zu tun. Sie besteht vielmehr aus einem durch die Verschlüsselungssoftware errechneten
>
> **Zahlenwert.**
>
> Die digitale Signatur dient aber denselben oder zumindest gleichartigen Zwecken wie die Unterschrift auf Papier: sie bestätigt, dass der dazugehörige Text dem Absender zuzurechnen ist.

Ein **weiterer Vorteil** der digitalen Signatur besteht darin, dass jeder einzelne Buchstabe des übertragenen Textes durch die Verschlüsselung signiert wird. Der Text kann daher **nicht verändert** werden.

Bei erfolgreicher Entschlüsselung einer digital signierten Sendung kann somit zum einen

- die **Identität** des Unterzeichners (weil eine Fälschung schwieriger ist als bei einer Nachricht auf Papier) sowie der Ursprung der Nachricht und zum anderen
- die **Originalität** der gesamten Nachricht festgestellt werden. Im Gegensatz zur handschriftlichen Unterschrift wird verhindert, dass unbemerkt und unbefugt neue Textteile in das ursprüngliche Dokument eingefügt werden, die der Signierende nicht kannte oder kennen konnte. Die digitale Signatur bezieht sich zwingend auf das gesamte Dokument.

Mit anderen Worten kann mit Hilfe der elektronischen Signatur die **Authentizität** der Nachricht (von wem stammt sie?) und die **Integrität** (Unverfälschtheit) der signierten elektronischen Nachricht festgestellt werden.

Anzumerken ist, daß digitale Signaturen also nicht der Vertraulichkeit einer Nachricht dienen, wie der Begriff der Verschlüsselung nahelegen würde. Vielmehr wollen sie die **Integrität einer Nachricht und deren Urheberschaft** gewährleisten.

3.2. Die praktische Umsetzung der elektronischen Signatur

Da das asymmetrische Verschlüsselungsverfahren mehr Zeit zur Ver- und Entschlüsselung benötigt als die symmetrischen Verschlüsselungen, wird die zu signierende Nachricht mit einem Prüfsummen-Verfahren zu einem sogenannten

Hash-Code

verkürzt, der die Charakteristika der Nachricht enthält und diese eindeutig definiert wie ein Fingerabdruck. Mit dem Private Key verschlüsselt wird dieser Hash-Code anstelle der Nachricht.

Diese verschlüsselte „Kurzfassung", der sogenannte „message digest" bildet zusammen mit möglichen Zusatzinformationen wie Angaben über den Unterzeichner, Datum und Uhrzeit die eigentliche „Signatur", die an das zu übertragende Dokument angehängt an den Empfänger übermittelt wird.

Der Empfänger kann mit dem dazugehörigen Public Key des Versenders das Dokument entschlüsseln. Bei der Entschlüsselung wird wiederum der Hash-Wert errechnet und mit dem mitübersandten ersten Hash-Wert verglichen. Stimmen beide Hash-Werte überein, steht fest, daß die Nachricht nicht verändert wurde. Dieser Hash-Wert ist zwar bei jedem Dokument immer gleich lang, aber in der konkreten Ausformung verschieden, wodurch sich die digitale Signatur bei jedem Signierungsvorgang verändert und daher auch nicht kopiert werden kann.

3.2.1. Ein Beispiel

Der folgende Text soll mit Signatur verschickt werden:

Sehr geehrte Frau Müller! Vielen Dank für Ihr Angebot vom 28.1.2002. ..... Mit freundlichen Grüßen Matthias Neumayr

1. Aus dem Text wird der Hash-Code errechnet:

0000 0000 0001 1509 5863 1412 EB07 C4BA

2. Der Hash-Code wird mit dem Private-Key des Absenders verschlüsselt. Dadurch wird die Signatur erzeugt. Aus

0000 0000 0001 1509 5863 1412 EB07 C4BA

wird

49F2 CD93 2C0E 244D A8F0 9298 2F6C C5EE

3. Der Text wird mit der Signatur versendet

Sehr geehrte Frau Müller! Vielen Dank für Ihr Angebot vom 28.1.2002. ..... Mit freundlichen Grüßen Matthias Neumayr

49F2 CD93 2C0E 244D A8F0 9298 2F6C C5EE

4. Empfang von Text und Signatur durch den Empfänger.

5. Mit dem vereinbarten Prüfsummen-Verfahren wird vom Empfänger aus dem Text der Hash-Code ermittelt:

0000 0000 0001 1509 5863 1412 EB07 C4BA

6. Entschlüsselung: Die empfangene Signatur wird mit dem Public-Key des Absenders entschlüsselt: Aus

49F2 CD93 2C0E 244D A8F0 9298 2F6C C5EE

wird

0000 0000 0001 1509 5863 1412 EB07 C4BA

7. Vergleich: Wenn die entschlüsselte Signatur mit dem ermittelten Hash-Code ident ist, dann handelt es sich tatsächlich um die digitale Signatur des Absenders.

3.2.2. Zugang zum Public Key des Versenders

Wie gelangt man nun an den Public Key des Versenders, um die Authentizität der Nachricht zu überprüfen? Denkbar wäre ein persönlicher Austausch. Dies ist aber nur im privaten Kreis praktikabel, nicht aber für den geschäftlichen Verkehr, weil dies zu zeitraubend wäre. Diese Schwierigkeiten werden dadurch umgangen, dass vertrauenswürdige Zertifizierungsstellen gewerbsmäßig die Aufgabe übernehmen,

- die asymmetrischen Schlüsselpaare herzustellen und
- die Public Keys zu übernehmen und der Öffentlichkeit zur Verfügung zu stellen, sodass die öffentlichen Schlüssel via Internet abgerufen werden können. Auf diese Weise kann auf die Identität der Person geschlossen werden, der der Public Key zugeordnet ist.

Ein **Beispiel**:

1. Ich erhalte von einer Person, die ich persönlich nicht kenne, ein Angebot in Form einer eMail mit Angebotstext im Klartext und digitaler Signatur. Möchte ich die Unterschrift prüfen, benötige ich den Public Key des Absenders.

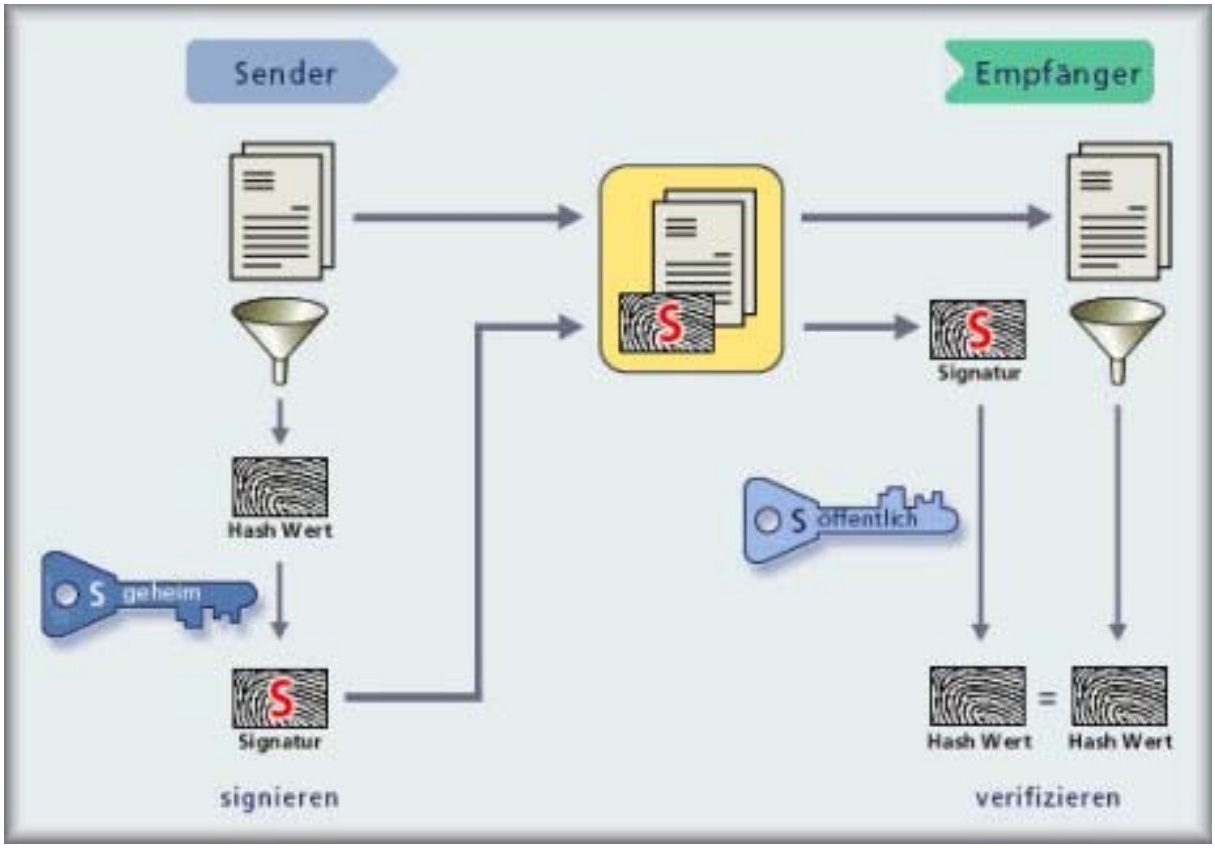
2. Es wird eine geschützte SSL-Verbindung zur nächsten Zertifizierungsstelle hergestellt. Das benötigte Zertifikat wird übersandt (signiert mit dem Private Key der Zertifizierungsstelle) und lokal auf die Festplatte geladen.

   Beispiel: https://a-cert.argedaten.at/
   A-CERT Public Key-Suche nach Familienname (als Beispiel kann etwa der Familienname “Zeger” eingegeben werden, dann erhält man den Public Key).

3. Der Public Key wird entnommen; damit wird der Signaturblock des Angebots entschlüsselt.

4. Aus dem Klartext des Angebots wird mit dem öffentlich bekannten Hash-Verfahren der Signaturblock errechnet; die Ergebnisse werden verglichen. Bei Übereinstimmung sind sowohl Nachricht als auch Unterschrift echt.

3.2.3. Grafik



3.3. Zertifizierungsstellen

Zertifizierungsstellen stellen die Zuordnung eines öffentlichen Schlüssels zu einer bestimmten Personen durch die „Zertifikate“ sicher. Ausreichende Sicherheit des beschriebenen Systems der digitalen Signatur kann ja nur dann bestehen, wenn **beide Schlüssel eindeutig einer bestimmten Person zugeordnet** werden können. Das Zuordnungsrisiko muss minimiert werden, weil hier eine Schwachstelle für den elektronischen Geschäftsverkehr liegt. Es muss also eine Person oder Institution geschaffen werden, zu der beide Parteien Vertrauen haben – eben die Zertifizierungsstelle, die mit ihrer digitalen Unterschrift bestätigt, dass der im Zertifikat enthaltene „Public Key“ der angegebenen Person gehört – also eine Art „elektronischer Notar“.

Den Zertifizierungsstellen kommt daher im eBusiness eine zentrale Rolle zu, weil ihr Zertifikat die Grundlage für das Vertrauen bildet, dass ein Schlüssel einer bestimmten Person gehört. Der Aufbau eines Netzes von geeigneten Zertifizierungsstellen ist eine grundlegende rechtliche Rahmenbedingungen für das Funktionieren von elektronischen Signaturen.

Der Zertifizierungsstelle kommen demnach **zwei wesentliche Funktionen** zu:

- sie stellt den **Konnex** zwischen einer bestimmten Person und ihrem öffentlichen Schlüssel her, indem der Name des Schlüsselinhabers und einige weitere Informationen wie Zeitpunkt der Ausstellung, Name der Zertifizierungsstelle etc offengelegt werden (Zertifikat) und
- sie führt **Verzeichnisse** über die an bestimmte Personen ausgegebenen Schlüssel, aber auch über deren **Widerruf** und die genauen Zeiten dieser Vorgänge, damit auch im nachhinein genau festgestellt werden kann, ob eine elektronische Signatur zu einem bestimmten Zeitpunkt ordnungsgemäß war oder nicht.

Grundsätzlich sind zwei Arten von Zertifikaten und damit auch zwei Arten von Zertifizierungsstellen vorgesehen.

- „**Einfache“ Zertifikate** können von Zertifizierungsstellen mit minimaler staatlicher Kontrolle ausgegeben werden.
- Soll jedoch eine elektronische Signatur das rechtliche Erfordernis der eigenhändigen Unterschrift erfüllen, weil 100%ig sichergestellt ist, dass sie einer ganz eindeutig bestimmten Person zugeordnet ist („**sichere elektronische Signatur**”), so hat dies mit Hilfe eines **qualifizierten Zertifikates** zu erfolgen, welches wiederum von einem Anbieter zu erstellen ist, der besonderen rechtlichen Pflichten unterworfen ist. Diese Pflichten sind in § 7 des österreichischen Signaturgesetzes angeführt (Nachweis besonderer Zuverlässigkeit, ausreichender Finanzmittel einschließlich eines Haftungsfonds, des Einsatzes geprüfter Hard- und Software sowie qualifizierten Personals und des Einhaltens aller von der staatlichen Aufsichtsstelle angeordneten Auflagen).

  In der Praxis gibt es zahlreiche unterschiedliche Sicherheitsstufen, die durch unterschiedlich aufwendige Sicherheits- und Zertifizierungskonzepte realisiert werden.

Die Aufnahme der Tätigkeit einer Zertifizierungsstelle unterliegt **keiner besonderen Genehmigung**, sie ist jedoch anzuzeigen, und zwar bei der Rundfunk und Telekom Regulierungs-GmbH, die in Österreich die staatliche Aufsicht über die Zertifizierungsstellen (nach der österreichischen Diktion "**Zertifizierungsdiensteanbieter**") ausübt.

In Österreich sind derzeit (Stand 17.2.2002) fünf aktive Zertifizierungsstellen im Aufsichtsbereich der Rundfunk und Telekom Regulierungs-GmbH (http://www.tkc.at) gemeldet:

http://www.signatur.rtr.at/de/providers/providers.html

- die Datakom Austria (eine Tochter der Telekom Austria AG, die das Zertifikat “a-sign“ anbietet),

  http://www.datakom.at/

  http://a-sign.at/

- die Generali Office-Service und Consulting AG,
  http://www.generali.co.at/netsecurity.nsf?OpenDatabase

- der Verein ARGE Daten („adcert“),

  http://www.a-cert.at/

https://a-cert.argedaten.at/

- A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH, ein Zusammenschluss von großen österreichischen Geldinstituten, Nationalbank, Wirtschaftskammer, Notariatskammer, Rechtsanwaltskammertag und Telekom Austria („a-trust“)
  http://www.a-trust.at/

- Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (Euro-PKI Austria)

  http://europki.iaik.at

Ein qualifiziertes Zertifikat, das Voraussetzung für die Gleichstellung der Signatur mit der eigenhändigen Unterschrift ist, gibt es seit Dezember von a-sign und von a-trust. Dieses qualifizierte Zertifikat funktioniert nämlich nur mit einer SmartCard samt Lesegerät.

3.4. Ausländische Zertifikate

Zertifikate, die von einem in der Europäischen Gemeinschaft niedergelassenen Zertifizierungsdiensteanbieter ausgestellt wurden und deren Gültigkeit vom Inland aus überprüft werden kann, sind inländischen Zertifikaten **gleichgestellt**.

4. Das österreichische Signaturgesetz

Auf europäischer Ebene wurde die Richtlinie 1999/93/EG des europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingunen für elektronische Signaturen erlassen. Diese Richtlinie ist in den Mitgliedstaaten bis zum 19.7.2001 umzusetzen.

Das österreichische Signaturgesetz wurde vom Nationalrat am 14.7.1999 einstimmig beschlossen. Am 1.1.2000 ist es in Kraft getreten.

Das Gesetz unterscheidet richtlinienkonform zwischen „**einfachen**“ elektronischen Signaturen (§ 2 Z 1) und „**sicheren** elektronischen Signaturen“ (§ 2 Z 3). Diese Unterscheidung ist deshalb von Bedeutung, weil nach § 4 Abs 1 SigG nur eine „sichere elektronische Signatur“ das rechtliche **Erfordernis einer eigenhändigen Unterschrift** erfüllt. Es kann also nur mit einer „sicheren elektronischen Signatur“ das Erfordernis der Schriftlichkeit erfüllt werden. Die Wortwahl ist etwas unglücklich, weil das Wort „sicher” suggeriert, dass einfache Signaturen unsicher sind. Die Richtlinie verwendet den Begriff der „fortgeschrittenen” elektronischen Signatur.

„Einfache“ Signaturen können im elektronischen Geschäftsverkehr verwendet werden, und sie können auch als Beweismittel im gerichtlichen oder behördlichen Verfahren dienen. Das Signaturgesetz lässt Signaturverfahren mit unterschiedlichen Sicherheitsstufen zu. Auf diese Weise sollen unterschiedliche Anwendungsbereiche ausreichend abgedeckt werden:

Für den online-Einkauf um geringe Beträge genügen technisch einfachere und weniger aufwendige Anforderungen als beispielsweise für den Rechtsverkehr von Notaren, Rechtsanwäl-

ten, Banken oder Ziviltechnikern. Mit anderen Worten: Je größer die Risiken eines über das Internet abgewickelten Geschäfts sind, desto höher sind die Anforderungen, die an die Sicherheit des verwendeten Zertifikats zu stellen sind.

> Digitale Signatur ohne Zertifikat klingt überraschend, macht aber dennoch Sinn: Es wird geprüft, ob das Dokument auf dem Weg zum Empfänger nochmals verändert wurde; außerdem wird zumindest die eigene eMail-Adresse „geschützt".
>
> Zieht man den Vergleich mit dem täglichen Einkauf von Lebensmitteln etc heran, ist zu konstatieren, dass sich hier niemand um die Identität des Käufers kümmert. Man braucht keinen Ausweis vorzeigen, seinen Namen nicht nennen etc. Die Einführung einer digitalen Signatur bringt zweifellos die Gefahr mit sich, dass es zu einer weit stärkeren Offenlegung der Person des Käufers kommt. Um dies so weit wie möglich zu verhindern, werden auch einfache Zertifikate zugelassen.
>
> Der Erwerb einer „einfachen" Signatur ist tatsächlich einfach: bei der niedrigsten Sicherheitsstufe genügt eine eMail-Adresse. Mittlere Zertifikate erhält man nach telefonischer Identitätsüberprüfung oder Übermittlung einer Kopie eines Personalausweises mittels Fax. Inhaber solcher Signaturen können sich also durchaus hinter einem **Pseudonym** „verstecken". Für Zertifikate der höchsten Sicherheitsstufe muss man zur Zertifizierungsstelle gehen und einen Lichtbildausweis vorlegen. Als Lizensierungsstellen werden in der Praxis Banken und Postämter fungieren.

Die ausdrückliche rechtliche Gleichstellung der „sicheren" elektronischen Signatur mit der eigenhändigen Unterschrift ist allerdings im österreichischen Signaturgesetz eingeschränkt: In bestimmten sensiblen Bereichen wird die Rechtsgültigkeit NUR aus der handschriftlichen Unterschrift abgeleitet. Elektronische Signaturen sind ungültig bei folgenden Verwendungen:

- an (zumindest) die Schriftform gebundene Rechtsgeschäfte des Familien- und Erbrechts - ein digital signiertes Testament ist ungültig;
- Rechtsgeschäfte und Willenserklärungen bzw Einträge (Firmenbuch und Grundbuch), bei denen die Unterschrift öffentlich, gerichtlich oder notariell beglaubigt werden muss oder ein Notariatsakt notwendig ist - es ist nicht vorgesehen, dass digitale Signaturen notariell beglaubigt werden können; hier ist immer noch die handschriftliche Unterschrift notwendig;
- **Bürgschaftserklärungen** von Nicht- und Minderkaufleuten.

Die Ausnahmen betreffen im wesentlichen Rechtsgeschäfte, bei denen entweder die bei Verwendung elektronischer Signaturen nur schlecht verwirklichte Warnfunktion eine große Bedeutung hat oder die auch schon beim traditionellen Geschäftsabschluss qualifizierteren Voraussetzungen als der einfachen Schriftform unterliegen.

5. Anwendungsbereiche der elektronischen Signatur bei der Übermittlung von Daten

Mit der weiteren Entwicklung des eBusiness werden Fragen des elektronischen Verkehrs immer mehr an Bedeutung gewinnen. Im Gegenzug geht die Bedeutung des Telefax merklich zurück.

5.1. eCommerce, eBusiness, eBanking

Unter e-Business versteht man alle Formen der elektronischen Geschäftsabwicklung. Dazu gehören z.B. der elektronische Handel zwischen Händlern und Kunden (eCommerce), aber auch elektronischen Formen des Einkaufs und der Beschaffung in Unternehmen (eProcurement), eBanking usw. Dabei ist das Internet das Hauptmedium.

http://www.www-kurs.de/e-business.htm

http://www.www-kurs.de/e-shopping.htm

Billa-Online Shop: http://www.billa.at/billa/default.asp

http://www.i4j.at/e-commerce/ec0.htm

Die potentiellen Anwendungsbereiche elektronischer Geschäfte – und damit auch mögliche Anwendungsbereiche der elektronischen Signatur – sind weiter als man es sich gemeinhin vorstellt. Betroffen sind nicht nur die schon jetzt bekannten Dienstleistungen, die vollständig von der Bestellung bis zur Erfüllung und Bezahlung elektronisch abgewickelt werden können (Abruf von Informationen, Unterhaltung, Geldgeschäfte), und die Geschäfte, die elektronisch angebahnt, aber konventionell abgewickelt werden (**Teleshopping**). Im Bankenbereich soll die digitale Signatur den Zahlungsverkehr absichern, einerseits zwischen Bank und Kunden, andererseits zwischen den Geldinstituten.

http://www.www-kurs.de/homebank.htm (BRD)

http://banking.raiffeisen.at/

http://www.psk.at/produkte/sofabankingcenter/s-index.html

> Es bleibt abzuwarten, ob sich im Bereich elektronischer Zahlungen nicht SET (*Secure Electronic Transaction*) durchsetzen wird, ein Sicherheitssystem, das von den Kreditkartenfirmen Visa und Eurocard entwickelt wurde (siehe näher unten)

5.2. Der Einsatz der Signatur in der öffentlichen Verwaltung

5.2.1. eGovernment

http://www.help.gv.at/
Formulare zum Downloaden: http://www.help.gv.at/77/Seite.770000-10240.html
http://www.www-kurs.de/e-government.htm (BRD)
Stadt Salzburg (Mit der Mouse den Hund anmelden): http://www.diepresse.at/archiv.taf?_function=read&_UserReference=243CA05730816FA93A159A80&_id=709375

Demo Hundeanmeldung:
https://link.help.gv.at/pilotweg/db/formallg.form?behoerde=62&verf=1

Die digitale Signatur wird aber auch in der öffentlichen Verwaltung eine zunehmende Rolle spielen. Die Stichworte „**Electronic Government**“ oder „eGovernment“ und @MTSWEG online sind schon gefunden. Im Bereich eGovernment geht es vor allem um Transaktionen zwischen der Verwaltung auf der einen Seite und Bürger und Wirtschaft auf der anderen Seite.

So können etwa Meldeangelegenheiten mit Hilfe einer sicheren digitalen Signatur relativ einfach elektronisch abgewickelt werden. Die Frage ist derzeit jedoch mehr, ob sich der Aufwand für den einzelnen lohnt. Man kann schwerlich von allen Bürgern verlangen, dass sie die technische Ausstattung mit Lesegerät und SmartCard besorgen, um sich einen einzigen Gang zum Meldeamt pro Jahrzehnt zu ersparen. Die geforderten Sicherheitsstandards bei „sicheren elektronischen Unterschriften“ sind jedenfalls sehr hoch, und das schlägt sich einerseits auf die Kosten, andererseits aber auch die Bereitschaft nieder, so ein System zu verwenden.

Natürlich darf bei dieser Diskussion nicht verkannt werden, dass die Veränderung und Fälschung elektronischer Dokumente um einiges leichter geht und auch schwerer erkennbar ist als bei klassischen Dokumenten auf Papier.

Insgesamt läuft eGovernment mit dem Ziel, dass bis 2005 die wesentliche Amtswege vom Bürger über das Internet abgewickelt werden können. Derzeit kann man sich Formulare zwar über help.gv im Internet herunterladen; ausfüllen und an eine Behörde schicken muss man sie aber noch auf dem konventionellen Weg.

Bürgerkarte: http://www.buergerkarte.at/Buergerkarte.htm

In der Regierungsklausur vom 20. November 2000 wurde einstimmig der Einsatz von Chipkartentechnologie zur Vereinfachung der Amtsgeschäfte des Bürgers vereinbart. Die durch den Hauptverband der Sozialversicherungen ausgeschriebene Sozialversicherungskarte könnte durch Ergänzung mit elektronischen Signaturen als Keykarte zur „Bürgerkarte“ werden, da die Ressourcen der SV-Karte durch die Anwendung "Krankenscheinersatz" nicht voll ausgelastet sind.

Als ein weiterer Bereich, der besonders hohe Sicherheitsanforderungen stellt, sind im übrigen noch **elektronische Ausschreibungen** zu erwähnen.

5.2.2. Finanz-Online

Ein Schritt in Richtung eGovernment ist „Finanz-Online“, womit man auf seine Finanzamtsdaten zugreifen und die Steuererklärungen elektronisch verschicken kann. „**Finanz-Online**“ gibt es seit 8.3.1998; es ist derzeit auf die Gruppe der Wirtschaftstreuhänder beschränkt und wird auf Notare und Rechtsanwälte erweitert. Wenn die digitale Signatur ausreichend implementiert ist, soll jeder Bürger, der will, Zugang dazu bekommen können.

Ein Blick über die Grenzen: Im Finanzgericht Hamburg läuft seit Anfang August 1999 ein Feldversuch zum papierlosen Rechtsverkehr, an dem 25 Rechtsanwalts- und Steuerbüros teilnehmen. Sie kommunizieren per eMail mit dem Finanzgericht.

5.2.3. Gesundheitsbereich

Auch im Gesundheitsbereich geht man mit hoch vertraulichen Informationen um, etwa Diagnosen, Krankengeschichten, Laborberichte und Ausweisen. Um sicher zu gehen, dass Daten bei der Übermittlung nicht verändert werden, besteht daher auch in der medizinischen Kommunikation ein Anwendungsbereich für die digitale Signatur, ebenso bei der Übermittlung von Rezepten und bei Abrechnungen.

6. Zusammenfassung zur elektronischen Signatur

Zusammengefasst kann man sagen, dass die elektronische Signatur derzeit – zwei Jahre nach Inkrafttreten des Gesetzes - noch kaum eine nennenswerte Rolle spielt. Zur Frage, ob hohe Sicherheitsstandards eine positive oder negative Wirkung auf die Ausbreitung haben, gibt es geteilte Ansichten. Man wird man aber annehmen können, dass die praktische Bedeutung der elektronischen Signatur langsam zunehmen wird, zwar nicht in allen Lebensbereichen, vor allem aber im Behördenbereich, im Bankenbereich und in den Wirtschaftsbereichen.

Zumindest dort kann es heißen: „Unterschreiben Sie hier! Aber per Mausklick!“

Die Presse 8.3.2001

Fast perfekte Sicherheit: Digitale Signatur und intelligente Füllfeder

Welche Technologien siegen werden, ist vorerst noch ungewiß - sicher ist, daß Sicherheit bei elektronischen Transaktionen ein boomender Markt ist.

VON PETER MARTOS

WIEN. "Die Verpackung muß sich ändern: Sie muß für den Konsumenten gebaut sein, nicht für Lou Gerstner." Sam Asseer, Kanadier an der Spitze des niederländischen Konzerns LCI, will nicht IBM-Chef Gerstner kritisieren, sondern die gesamte Computerindustrie. LCI hat vor kurzem ein Gerät in Wien vorgestellt, das laut Asseer der Inbegriff der gewandelten Einstellung zum Kunden ist: SmartPen sieht aus wie ein Kugelschreiber - und ist auch einer. Allerdings mit zusätzlichen Fähigkeiten: Es ist ein biometrisches Minisystem, das über ein hochkomplexes Innenleben aus Sensoren, Analog-Digital-Wandlern, anderen Elektronik-Bausteinen und Software den Urheber der Unterschrift erkennt. Nicht am Schriftzug, der gefälscht werden kann, sondern am Schreibverhalten: Da werden Schreibdynamik, Neigungswinkel und Druckstärke der Hand mit dem Original verglichen. Ist das Ergebnis positiv, wird der Schriftzug in eine digitale Signatur umwandelt und über einen winzigen Sender an den Computer übermittelt. Asseer betrachtet SmartPen als das Werkzeug, mit dem Sicherheit in der elektronischen Welt vergrößert werden kann. "Die Erkennung des Fingerabdrucks ist unsicher: Auch Tote haben einen. Die Iris eines Menschen läßt sich durch vorgehaltene Bilder fälschen." SmartPen hingegen garantiere für den Urheber. Die Größenordnung des potentiellen Marktes? "Gegenwärtig werden allein in den USA 1,8 Billionen Dollar (26,75 Billionen Schilling) pro Jahr bei Internet-Transaktionen umgesetzt. Sicherheitsvorkehrungen machen davon zwei Prozent aus. Wir wollen fünf Prozent dieses Kuchens - 1 Milliarde Dollar." Und Europa? Der Markt für biometrische Identifizierungssysteme auf dem Alten Kontinent wächst laut einer Studie der Unternehmensberatung Frost & Sullivan von umgerechnet 634,5 Millionen Schilling im Vorjahr bis 2006 auf 2,4 Milliarden Schilling. Wichtigster Bereich bleibe die Fingerabdruckerkennung mit etwa der Hälfte des Umsatzes, gefolgt von Stimm-, Hand- und Gesichtserkennung.

"Technik sekundär"

"Die Erkennungstechnik ist sekundär - wichtig ist die Integration ins Sicherheitssystem", erzählt Olaf

Ahlburg, Geschäftsführer des Wiener Spezialunternehmens RKK, der "Presse". Die frühere Tochter der Avolon-Gruppe, von Ahlburg im Jänner in einem Management-buy-out übernommen, hat für den Mobilfunkbetreiber One eine Lösung aufgesetzt, die mit einer kreditkartengroßen Chip-Karte funktioniert. "One setzt sie sowohl als Zugangssicherung bei Türen samt Zeiterfassung als auch für den PC ein." Die Identität des Inhabers kann als elektronischer Fingerabdruck auf der Chip-Karte liegen oder als Abbild der Iris. Bei One wird diese Möglichkeit nicht genutzt. Iris-Erkennung ist aus RKK-Sicht problematisch: "Die Leute wollen keinen Laserstrahl im Aug'." Ahlburg hört schon die Zukunftsmusik: eine Kombination von Chipkarte und einem qualitativ hochwertigen Scanner, der den Fingerabdruck prüft und sich von einem Photo nicht überlisten läßt. Unabhängig davon, welche Systeme eingesetzt werden - fast alle Experten betrachten die digitale Signatur als Lösung vieler Probleme. Auch Asseer. Sie sichere aber nur, daß der Vorgang korrekt abgelaufen sei. "Niemand garantiert, daß der private Schlüssel nicht gestohlen wurde. Er ist ja nur ein elektronischer Code." Das Prinzip der digitalen Signatur funktioniert nach einem klar definierten Schema: Ein Computernutzer, der ein Dokument elektronisch unterschreiben will, kombiniert es mit einem Software-Code ("privater Schlüssel"), der ihn einwandfrei identifiziert, das Dokument verschlüsselt und versendet. Beim Empfänger wird beim Entschlüsseln das frei erhältliche Gegenstück des Codes ("öffentlicher Schlüssel") dem Dokument hinzugefügt. Sind die beiden Codierungen identisch, wird der Urheber "erkannt" und das Dokument entschlüsselt. Setzt sich - in Kombination mit technischen Vorkehrungen - die digitale Signatur durch, naht laut Ahlburg die fast perfekte Sicherheit. Was fehle, sei die EU-weite Regelung. "Die österreichische Gesetzgebung ist gut, jetzt müssen die beiden Konsortien ihre Lösungen vermarkten."

7. Anpassungen des österreichischen Rechts an den eCommerce

7.1. eCommerce

7.1.1. E-Commerce-Gesetz (ECG)

http://www.i4j.at/e-commerce/ec0.htm

Am 1.1.2002 ist in Österreich das E-Commerce-Gesetz (ECG) in Kraft getreten. Damit wird die „E-Commerce-Richtlinie“ der Europäischen Gemeinschaft in das österreichische Recht umgesetzt. Im Zentrum der Richtlinie steht die Vorschrift, dass die Mitgliedstaaten darauf zu achten haben, dass ihre Rechtsvorschriften den Abschluss elektronischer Verträge ermöglichen (Art 9 Abs 1). In Österreich war aufgrund der Formfreiheit rechtlich ein elektronischer Vertragsabschluß bereits nach geltendem Recht möglich. Für das Zustandekommen eines Vertrages sind übereinstimmende Willenserklärungen der Vertragsparteien erforderlich, und es besteht kein Zweifel, dass eine Willenserklärung auch per E-Mail oder auf sonstigem elektronischem Wege geäußert werden kann.

Das E -Commerce-Gesetz (ECG)sieht für alle Dienste, die

- in der Regel gegen Entgelt
- elektronisch
- im Fernabsatz
- gegen individuellen Abruf des Empfängers

erbracht werden, beispielsweise diverse **Informationspflichten** vor, etwa Name, Firma, Adresse (einschließlich eMail-Adresse) des Unternehmers (§ 5 ECG) und eine **eindeutige Preisauszeichnung**. Auch für Vertragsabschlüsse gibt es zwingende Informationspflichten (§ 9 ECG). Vorzusehen sind technische Mittel zum Erkennen und Berichtigen von Eingabefehlern.

In § 12 ECG wird der Zugang einer elektronischen Erklärung mit dem Zeitpunkt gleichgesetzt, zu dem sie der Erklärungsempfänger "unter gewöhnlichen Umständen" abrufen kann.

7.1.2. Fernabsatzgesetz

http://www.i4j.at/e-commerce/ec0.htm

Mit dem österreichischen Fernabsetzgesetz (in Kraft seit 1.6.2000) wird die Fernabsatz-Richtlinie der Europäischen Gemeinschaft in das österreichische Recht umgesetzt. Das Gesetz enthält Schutzbestimmungen für Konsumenten, wenn ein Vertrag nur im Wege von Fernkommunikationsmitteln abgeschlossen worden wurde, es also keinen persönlichen Kontakt der Vertragspartner vor Vertragsabschluss gegeben hat.

Auch das Fernabsatzgesetz sieht verschiedene Informationspflichten vor Vertragsabschluss vor (Name und Anschrift des Unternehmers, wesentliche Eigenschaften und Preis der Ware oder Dienstleistung, Einzelheiten der Zahlung und der Lieferung oder Erfüllung, Bestehen eines Rücktrittsrechts usw).

Der Konsument ist berechtigt, innerhalb von 7 Tagen vom Vertrag zurückzutreten. Bei Verletzung der Informationspflicht beträgt die Frist 3 Monate.

7.2. Zahlungssysteme

http://www.i4j.at/intern26.htm

Das Problem mit der Zahlung im Internet ist einer der Gründe, warum das Business-to-Consumer-Geschäft (B2C) - ganz im Gegensatz zum Business-to-Business-Geschäft (B2B) - nicht so boomt wie es eigentlich könnte. Während nämlich in Amerika die Zahlung mit Kreditkarte zum Standard geworden ist, ist dieses Zahlungsmittel in Europa immer noch ein Nischenprodukt. Im Internet scheint die Angst vor der Weitergabe der Kreditkartennummer besonders groß zu sein:

http://futurezone.orf.at/futurezone.orf?read=detail&id=54728&tmp=52127 (15.1.2001):
Erlagschein beliebter als Kreditkarte – Kunden zahlen lieber traditionell

Es gibt derzeit verschiedene Varianten von Zahlsystemen im Internet, aber keinen einheitlichen Standard. Immer geht es aber um das Bemühen, einerseits den Kunden vor dem Missbrauch der Kreditkartendaten zu bewahren und dem Händler die Bezahlung seiner Ware zu gewährleisten.

Aufgrund des Argwohns gegenüber der Kreditkarte wurden verschiedene alternative Zahlungsmethoden entwickelt, die entweder auf dem "prepaid"-Gedanken basieren oder über eine zweite Verbindung, beispielsweise über Mobiltelephon die Zahlungsfreigabe bewerkstelligen.

7.2.1. Klassische Zahlungsarten

7.2.1.1. Zahlung mit Kreditkarte

Die Gefahr für den Kreditkarteninhaber ist bei weitem nicht so hoch, wie sie eingeschätzt wird. Für österreichische Verbraucher wurde im Konsumentenschutz-Gesetz (KSchG) eine Schutzbestimmung gegen Kreditkartenbetrug verankert. Nach § 31a KSchG kann ein Verbraucher, dessen Kreditkarte bei einem Vertragsabschluss im Fernabsatz (zB im Internet) missbräuchlich verwendet wird, vom Aussteller der Karte, also von der Kreditkartenfirma, verlangen, dass die Buchung oder Zahlung wieder rückgängig gemacht bzw. erstattet wird. Ein vertraglicher Ausschluss dieser Schutzbestimmung zu Lasten des Verbrauchers ist nicht möglich. Sehr wohl können aber Kreditkartenunternehmen, z.B. in ihren Allgemeinen Geschäftsbedingungen, vereinbaren, dass sie nicht haften, wenn der Verbraucher nicht bestimmte Sicherheitsmaßnahmen einhält, beispielsweise sich nicht eines sicheren Übertragungswegs bei der Weitergabe der Kreditkartendaten bedient.

So ein sicherer Übertragungsweg ist Secure Socket Layer (SSL). SSL ist ein offener Standard der Firma Netscape Communications für die gesicherte Datenübertragung im Internet. Damit soll ein unberechtigter Zugriff auf sicherheitsrelevante Informationen, wie Kreditkartennummern, verhindert werden. Eine derartige Verbindung ist für den User daran ersichtlich, dass in der Statuszeile des Browsers anstelle von http://.... https:// erscheint.

7.2.1.2. Zahlung per Nachnahme

Bezahlt wird Zug um Zug gegen Erhalt der Ware. Setzt Vertrauen des Verkäufers voraus und ist relativ teuer.

7.2.1.3. Zahlung per Vorauskasse

Der Käufer übermittelt zunächst den Kaufpreis per Scheck oder Überweisung, die Ware wird erst nach Einlösung des Schecks oder Erhalt der Überweisung ausgeliefert. Setzt Vertrauen des Käufers voraus.

7.2.2. An das Internet adaptierte Verfahren

7.2.2.1. SET (Secure Electronic Transaction)

Von VISA entwickelt. Sowohl Händler als auch Karteninhaber benötigen hierfür ein digitales Zertifikat. Der Kunde klickt bei der Bestellung im Internet auf SET als bevorzugte Zahlungsart. Zur Zahlung verwendet er seine persönliche elektronische Geldbörse (kann man bei VISA oder anderen Kreditkartenanbietern downloaden), die mit einem Passwort geschützt ist. Die Bestellung (inkl. Kreditkartendaten) wird bei diesem Vorgang automatisch verschlüsselt, elektronisch unterschrieben und dem Händler zugeschickt. Der Händler entschlüsselt die für ihn relevanten Bestellinformationen und leitet die für die Kreditkartenfirma notwendigen Daten weiter. Die Kontodaten oder die Kreditkartennummer sind für den Händler bei der SET-Transaktion nicht einsehbar. Der Händler erhält dann von VISA die Bestätigung der Zahlung, der Kunde die Bestätigung für die Bestellung.
Nachteil: Neben dem Händler muss auch der Kunde die SET-Software installiert haben.

7.2.2.2. bezahlen.at

bezahlen.at ist eine Plattform, auf der Österreichs Unternehmen Rechnungen präsentieren. Diese werden über das Clearinghaus P.S.K. im Wege des Interbankverkehrs durchgeführt. Es verbindet Rechnungsleger (Unternehmer), Zahlungspflichtige und Banken. Der Käufer wird von der PSK per E-Mail verständigt, wenn dort die Rechnung eingeht; er ruft die Seite mit seinen Rechnungen bei bezahlen.at auf und gibt die Rechung nach Prüfung frei. Der Auftrag wird zum Zahlungstermin von der PSK zur Bank des Käufers zur Buchung weitergeleitet. Problem: Mitgliedschaft.

7.2.2.3. Cybergeld

Der User legt sich bei einem Anbieter ein virtuelles Konto an und erwirbt ein Guthaben, aus dem er die Zahlungen begleicht, ähnlich den Wertkarten bei Telephon und Handy. Man spricht, da es meist um kleinere Geldbeträge geht, auch von Micro-Payment- oder Prepaid-Systemen. Das Problem dabei ist die Beschränkung der Zahlungsmöglichkeit auf die Vertragspartner des Anbieters.

7.2.2.4. Inkasso per Telefonrechnung

Bei Inanspruchnahme eines Dienstes wird eine besonders tarifierte Verbindung aufgebaut (z.B. 0190); die Abrechung erfolgt über die Telefonrechnung. Derartige Verrechnungssysteme werden häufig von Erotikseiten eingesetzt.