Gunther Ledolter

http://ledolter.n3.net

Das österreichische Signaturgesetz und sein Umfeld

Diplomarbeit zur Erlangung des Magister iuris

August 2001

Abkürzungsverzeichnis

ABGB	Allgemeines Bürgerliches Gesetzbuch
Abs	Absatz
AK	Arbeiterkammer
AkkG	Akkreditierungsgesetz
AnwBl	Anwaltsblätter
Art	Artikel
AtomHG	Atomhaftungsgesetz
AVG	Allgemeines Verwaltungsverfahrensgesetz
BGBl	Bundesgesetzblatt
BIP	Brutto-Inlands-Produkt
B-VG	Bundesverfassungsgesetz
BXA	Bureau of Export Adminstration
COCOM	Coordinating Committee for Multilateral Export Controls
DSA	Digital Signature Algorithm
DES	Data Encyption Standard
DSG	Datenschutzgesetz
DuD	Datenschutz und Datensicherheit
EAR	Export Administration Regulations
EG	Europäische Gemeinschaften
EGV	Vertrag über die Europäische Gemeinschaft
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
EWR	Europäischer Wirtschaftsraum
FEEI	Fachverbands für Elektro- und Elektronikindustrie
GmbH	Gesellschaft mit beschränkter Haftung
GOG	Gerichtsorganisationsgesetz
http	HyperText Transfer Protocol
IDEA	International Data Encryption Algorithm
ITAR	International Traffic in Arms Regulation
JAP	Juristische Ausbildung und Praxis
JBl	Juristische Blätter
KSchg	Konsumentenschutzgesetz
Lit	Litera
MA	meiner Ansicht
MD	Message Digest
MRK	Menschenrechtskonvention
NSA	National Security Agency
OECD	Organization for Economic Cooperation and Development
ÖJZ	Österreichische Juristen-Zeitung
PGP	Pretty Good Privacy
PHG	Produkthaftungsgesetz
PIN	Personal Identification Number

PKI	Public Key Infrastructur
RL	Richtlinie
RSA	Rivest, Shamir, Adleman
SET	Secure Electronic Transfer Protocol
SigG	Signaturgesetz
SigV	Signaturverordnung
SPG	Sicherheitspolizeigesetz
SSL	Secure Socket Layer
STGB	Strafgesetzbuch
StGG	Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger
StPO	Strafprozessordnung
TCK	Teleko-Control-Kommission
TKG	Telekommunikationsgesetz
Unicitral	United Nations Commission on International Trade Law
VfGH	Verfassungsgerichtshof
Vgl	vergleiche
VIW	Verband für Informationswirtschaft
VÖI	Vereinigung Österreichischer Industrieller
VPN	Virtual Private Network
VwGH	Verwaltungsgerichtshof
WA	Wassenaar Agreement
WWW	World Wide Web
ZPO	Zivilprozessordnung

1 Einleitung

Das Internet – ein neues Kommunikations- und Massenmedium, das sich von den Medien der letzten Jahrhunderte grundlegend unterscheidet, gewinnt immer mehr an Bedeutung. Die rasche Entwicklung, der das Internet unterliegt, bringt ungeahnte Möglichkeiten mit sich, aber auch Sicherheits- und Regelungsprobleme[1]. Die Wirtschaft und vor allem der Justizapparat sind gefordert, sich auf die neue Situation einzustellen. Die heikle Frage für den Gesetzgeber besteht vor allem darin, ob man schnell, nach kurzer Diskussionsphase, Anlassgesetze erlassen soll, die möglicherweise erhebliche Mängel aufweisen, oder ob man lange, ausgedehnte Verhandlungen abwarten soll, um in der Folge Normen in Geltung zu setzen, die zur Zeit des in Krafttretens schon veraltet und überholt sind[2].
Eine andere Möglichkeit besteht darin, die Internet-User sich selbst regulieren zu lassen, was bedeutet, dass man lediglich die Abläufe koordiniert und auf die Wirksamkeit der Verhaltensrichtlinien vertraut, die von den Betroffenen in „Eigenregie“ aufgestellt werden[3].

Als Argument für diese Handhabung spricht, dass der Cyberspace ein eigenes Gebiet ist, das mit Regeln des herkömmlichen Rechts nur unzureichend gelenkt werden kann und dass es als grenzenloses Medium nicht zentral zu regieren ist[4]. Außerdem sollte es ausreichen, den Benutzern Werkzeuge zur Verfügung zu stellen, um sich selbst zu schützen, womit in erster Linie Software gemeint ist, die den Zugang zu Webseiten mit Inhalten, die der persönlichen Wertvorstellung des einzelnen widerspricht, verhindert. In Ansatzpunkten mag dieses Modell vertretbar sein, doch etwa die Verbreitung nationalsozialistischen Gedankenguts im Internet nicht unter Strafe zu stellen, rein deshalb, weil Eltern ihre Kinder ohnehin durch Software vor dessen Kontakt schützen könnten, erscheint doch als sehr bedenklich.

Die zusätzliche Entwicklung von Verhaltensregeln der Internetnutzer hingegen ist auf allen Linien zu bejahen, sollte allerdings von staatlichen Sanktionsmöglichkeiten begleitet werden.
Erwähnenswert erscheint auch die Ansicht, dass das Internet leichter durch den Softwarecode zu regulieren sei als durch Gesetze. Was Computerprogramme mittels ihrer Programmierung unmöglich machen, braucht durch Gesetze nicht zusätzlich verboten werden. Wäre dies technisch, ohne Einschränkungen, tatsächlich möglich, müsste man jedoch wiederum den Programmierern rechtliche Rahmenbedingungen aufstellen, womit sich der Kreislauf schließen würde und man wieder am Anfang des Problems stünde.
Es kann jedoch ganz klar gesagt werden, dass das Internet nie ein rechtsfreier Raum war und dies auch nie sein wird.

Dadurch aber, dass nicht alle behandelnswerten Sachverhalte unter die bestehenden Tatbestände subsumiert werden können, besteht Bedarf an Spezialgesetzen, die in ihrer Gesamtheit das sogenannte Cyberlaw bilden. Dieser besondere Regelungsbedarf ist auf die Unterschiedlichkeit zu anderen Medien bzw. auf die speziellen Charakteristika des Internets zurückzuführen.

---

[1] Vgl. Thiel, C.: Marktentwicklung im Umfeld digitaler Signaturen. In: DuD – Datenschutz und Datensicherheit, 24, 2000, 77.
[2] Mayer-Schönberger, V.: Das Recht am Info-Highway. Verlag Orac, 1997, 41.
[3] Mayer-Schönberger, V.: Das Recht am Info-Highway. Verlag Orac, 1997, 123.
[4] Mayer-Schönberger, V.: Das Recht am Info-Highway. Verlag Orac, 1997, 33.

Als Besonderheiten des Internet gelten die Internationalität, die Offenheit, d.h. die Nichtausschließbarkeit von Teilnehmern und die weitgehende Anonymität der Nutzer.
Im Cyberlaw ist darauf zu achten, das richtige Mittelmass der Normierungen zu finden, um nicht durch zu restriktive oder e-Commerce-feindliche Regelungen die Betroffenen zu einer Aussiedlung in andere Staaten zu bewegen und andererseits einer „Spielwiese für Terroristen" nicht Tür und Tor zu öffnen.
Die nachteiligen Folgen für die heimische Wirtschaft, Arbeitsplatzpolitik und Verbrechensbekämpfung wären nur schwer wieder gut zu machen.

Diese angesprochenen Eigenheiten, vor allem die Unbekanntheit des Geschäftspartners, die zwar die Vorteile des Internet in seiner Gesamtheit ausmachen, bringen aber auch Sicherheitsprobleme mit sich. Die Ungewissheit, ob eine Erklärung von dem stammt, für den er sich ausgibt und ob die Erklärung überhaupt so angekommen ist, wie sie der Autor verfasst hat, kann dem e-Commerce nicht förderlich sein.
Eben diese Hemmnisse versucht das Signaturgesetz auszugleichen, indem eine vertrauenswürdige Stelle (die Zertifizierungsstelle) die Identität des Signators bestätigt und durch Verschlüsselungen die Authentizität (Echtheit) der Nachricht nachprüfbar gemacht wird.

Ziel des Signaturgesetzes ist es, einen Ausgleich zwischen freiem Wettbewerb, berechtigten Nutzerbedürfnissen und öffentlichen Ordnungsinteressen herbeizuführen, was sowohl den Einzelinteressen als auch dem e-Commerce zugute kommen wird.

2 Statistiken

Folgende Statistiken sollen zeigen, wie rasch sich das Internet mit seinem Umfeld in den letzten Jahren entwickelt hat und was Zukunftsprognosen erwarten lassen.

2.1 Internetanschluss

Insgesamt nimmt die Internet-Verbreitung in Europa laut Untersuchung drastisch zu. Im Jahr 1998 habe sich die Anzahl der Privathaushalte, die an das globale Datennetz angeschlossen sind, beinahe verdoppelt (von 4,4 auf 8,3 Prozent), teilte Harald A. Summa, Geschäftsführer des Verbandes der deutschen Internet-Wirtschaft und Vizepräsident der europäischen Spitzenorganisation Electronic Commerce Europe Association[5], auf der Uni-Org/SAP-Veranstaltung mit. Im Geschäftsleben liegen die Zahlen höher: Laut Studie nutzen 13 Prozent aller Europäer das Internet für die Arbeit.

[5] Universität Freiburg/Institut für Informatik und Gesellschaft (IIG-Telematik): Electronic Commerce Enquête. In Computer Zeitung, Gemini Consulting. Online im Internet: Url: http://telematik.iig.uni-freiburg.de/~schoder/ece/ [abgerufen am: 13.6.2000].

Allerdings haben 68 Prozent der Privathaushalte in Europa kein Interesse am Internet. Die Hälfte der Euro-Bürger hat keinen PC und will sich auch keinen zulegen. Die Anschaffung einer Settop-Box für den Internet-Zugang per Fernsehgerät erwägt nicht einmal ein Drittel aller Europäer. "Das Internet wächst kräftig, ist aber noch lange vom Massenmarkt entfernt", fasst Eco-Chef und ECE-Vize Harald A. Summa zusammen.

In Österreich verfügen momentan lediglich 7 Prozent der Privathaushalte über einen Internet Anschluss. Im Vergleich dazu haben in Schweden 39 Prozent, in Dänemark 25 Prozent in Griechenland und Portugal hingegen nur 3 Prozent die Möglichkeit von zu Hause aus ins Netz zu gelangen[6].

2.2 WWW und e-Mail-Verkehr

Im Mai 1999 sind im World Wide Web, dem multimedialen Teil des Internets, insgesamt mehr als 28 Mrd. Seiten angesehen worden - das sind fast 70 Prozent mehr als in der Vorjahresvergleichszeit. Der durchschnittliche Nutzer verbrachte im gleichen Monat 7,6 Stunden im Internet gegenüber 5,3 Stunden im Mai 1998. Die Gesamtzahl der im Internet verbrachten Stunden stieg um zwei Drittel auf 1,2 Mrd. Stunden[7].
Außerdem sind im vergangenen Jahr in den USA im Geschäftsverkehr mehr e-Mails verschickt worden, als herkömmliche Briefe. Für das Jahr 2005 erwartet die Europäische Kommission den Austausch von beinahe 2,5 Milliarden e-Mails pro Tag in Europa.
Auch die Geschäftsabwicklungen übers Internet nehmen zu, wie folgende Statistiken beweisen:

2.3 Umsatz und Zahlungsgewohnheiten

Laut einer Frost & Sullivan Studie[8] wurden 1997 noch 35.8 Mio. USD Umsatz bei einer Wachstumsrate von 554 % (also mehr als eine Verfünffachung) auf Europas Märkten erzielt. 1999 sind es schon 326,7 Mio. USD bei einem Wachstum von 155% im Vergleich zum Vorjahr. Bis ins Jahr 2004 werden die Umsätze auf 8070,6 Mio. USD bei einer Wachstumsrate von 64 % anwachsen[9].
Jeder vierte deutsche Surfer kauft online Software und Bücher, wobei 23 Prozent per Kreditkarte bezahlen.
Damit liegt Deutschland deutlich vor den beiden anderen wichtigen europäischen Online-Märkten Großbritannien (14 Prozent) und Frankreich (7 Prozent).

---

[6] Internet-Verband: Deutschland hinkt beim E-Handel hinterher, "Kräftiges Internet-Wachstum, aber noch kein Massenmarkt". Online im Internet: Url: http://www.the-bulls.com/news/news_2658.html [abgerufen am: 13.6.2000].
[7] Der Standard: Fast 62 Millionen am Netz. Online Ausgabe 6.7.1999. Online im Internet: Url: http://www.derstandard.at/ [abgerufen am: 6.7.1999].
[8] Frost & Sullivan-Studie. In: IT Business, 1-2/99, 46.
[9] Deutscher Multimedia Verband: Multimedia Marktzahlen. Online im Internet: Url: http://www.dmmv.de/multi/zahlen.html [abgerufen am: 13.6.2000].

Wenn es um das Bezahlen geht, greifen die Deutschen viel seltener zur Kreditkarte als Internet-Nutzer in den USA oder in Großbritannien. Nur 23 Prozent der deutschen Online-Käufer setzen die Plastikkarte zum Einkauf im Internet ein. 51 Prozent dagegen bevorzugen das Bankeinzugsverfahren oder eine Rechnung.[10]

2.4 Hemmnisse trotz steigender Wachstumsraten

2.4.1 Die fünf größten Hürden[11]

❖ noch keine allgemein üblichen Geschäftsgepflogenheiten	71,1%
❖ Regulatorische Defizite, z.B. für elektronisch signierte Verträge	70,0%
❖ ungeklärte rechtliche Aspekte, z.B. Haftung, Copyright	66,8%
❖ keine sichere Zahlung über das WWW möglich	65,9%
❖ Beweisbarkeit von Online-Transaktionen nicht gewährleistet.	65,5%

2.4.2 Die fünf kleinsten Hürden

❖ mangelnde Kompatibilität von Hard- und Software	29,0%
❖ zu komplizierte Technik	27,1%
❖ zu schneller technischer Wandel	26,7%
❖ unterschiedliche Produktverfügbarkeit in verschiedenen Regionen lassen sich vor dem Kunden nicht ausreichend verbergen	23,5%
❖ unser Geschäft ist nicht auf das Internet übertragbar	18,0%

2.4.3 Regulatorische Defizite

Die größte Hürde wird in der Abwesenheit allgemein üblicher Geschäftsgepflogenheiten (71,1%) und in "regulatorischen Defiziten, beispielsweise für elektronisch signierte Verträge" gesehen (70,0%).
Bezüglich Sicherheit, Recht und Zahlung gibt es die größten Klagen von Unternehmerseite.

[10] ORF on Futurezone: Deutsche führen im E-Kommerz. Online Ausgabe 28.6.1999. Online im Internet: Url: http://www.futurezone.at [abgerufen am: 28.6.1999].
[11] Universität Freiburg/Institut für Informatik und Gesellschaft (IIG-Telematik): Electronic Commerce Enquête. In: Computer Zeitung Gemini Consulting. Online im Internet: Url: http://telematik.iig.uni-freiburg.de/~schoder/ece/ [abgerufen am: 13.6.2000].

Als großes Problem werden sicherheitsrelevante Aspekte eingeschätzt; große Zustimmung erfahren die Aussagen: "ungeklärte rechtliche Aspekte, z.B. im Zusammenhang mit Haftung und Copyright" (66,8%), "keine sichere Zahlung über das WWW möglich" (65,9%), "Beweisbarkeit von Online-Transaktionen nicht gewährleistet" (65,5%) und "keine Sicherstellung vertraulicher Kommunikation (Datenschutz)" (63,8%)[12].

2.5 Verschlüsselungssoftware

Hand in Hand mit vermehrtem Handel steigt auch das Sicherheitsbedürfnis, wovon wiederum Hersteller von Verschlüsselungssoftware profitieren:
Frost & Sullivan Virtual Private Network (VPN)- und Public Key Infrastructure (PKI)-Software zufolge wird der europäische Markt für Netzsicherheits-Software von 1,13 Milliarden US-Dollar im Jahr 1998 auf mehr als 24 Milliarden US-Dollar im Jahr 2005 anwachsen.[13]

3 Technisches Grundwissen

Um die Regelungen des Signaturgesetzes zu verstehen, ist es wichtig, über ein gewisses technisches Grundwissen zu verfügen und den verwendeten Fachausdrücken die richtige Bedeutung zuordnen zu können.

3.1 Offene und geschlossene Netze

Der Unterschied zwischen offenen und geschlossenen Netzen[14] ist, dass sich bei den offenen jedermann Zugriff verschaffen kann, sofern er über die nötige Infrastruktur verfügt.
Die geschlossenen hingegen gehören meist einer Organisation oder einem Unternehmen und können nur von einer geschlossenen Benutzergruppe verwendet werden. Aber auch das sogenannte Intranet kann an das Internet angeschlossen sein und verwendet nicht immer eigene Leitungen. Da auch ein eigener e-Mail-Server üblich ist, ist die Gefahr des Abhörens versendeter Nachrichten auf eigene Angestellte beschränkt. Beim Internet selbst besteht keine Möglichkeit, einzelne Benutzer vom Zugriff auszuschließen.

---

[12] Universität Freiburg/Institut für Informatik und Gesellschaft (IIG-Telematik): Electronic Commerce Enquête. In: Computer Zeitung Gemini Consulting. Online im Internet: Url: http://telematik.iig.uni-freiburg.de/~schoder/ece/ [abgerufen am: 13.6.2000].
[13] Datakom Austria GmbH: Markt für Netzsicherheits-Software boomt. Online Ausgabe 10.7 1999. Online im Internet: Url: http://www.datakom.at/ [10.7. 1999].
[14] Vgl. Brenn, C.: Signaturgesetz. Manzsche Gesetzesausgaben, Sonderausgabe Nr.101, 1999, 50.

3.2 Digitale – elektronische Signatur

In Hinblick auf den technisch-neutralen Charakter des Signaturgesetzes und den Auftrag der Nichtdiskriminierung verschiedenster Verfahren sollte eigentlich durchgehend von der elektronischen Signatur[15] gesprochen werden. Das deshalb, weil eine elektronische Signatur auf allen möglichen Verschlüsselungsverfahren basieren kann (also auch auf symmetrischen, stenographischen oder allen noch zu entwickelnden). Die digitale hingegen ist auf die Public-Key-Verschlüsselung[16] einschränkt. Diese Formulierung, die im Signaturgesetz oftmals verwendet wird, wurde aber nicht aus Versehen, also zufällig gewählt. Vielmehr ging der Gesetzgeber zumindest bei der fortgeschrittenen, elektronischen Signatur von der Verwendung digitaler Signaturen aus.

3.3 Funktionsweise des Signierens

Fundamental für das Verständnis des Signaturgesetzes ist die Kenntnis des Ablaufs des Signiervorganges[17]:
Dieser läuft zwischen drei Beteiligten ab: einerseits dem Signator, der die signierten Daten verschickt und andererseits dem Empfänger dieser Daten, der sich des Zertifizierungsdiensteanbieters bedient. Der Zertifizierungsdiensteanbieter hat die Identität des Signators überprüft und gibt diese Informationen an den Empfänger einer signierten Erklärung weiter. Hinter diesen drei Hauptbeteiligten stehen natürlich noch weitere, indirekt Beteiligte, wie die Aufsichtsstelle, die die Zertifizierungsdiensteanbieter auf die Einhaltung der gesetzlichen Auflagen überprüft oder Softwarehersteller, die Programme erzeugen, mit welchen die Zertifikate abgerufen werden, oder auch Hardwareerzeuger.

3.4 Schlüsselerzeugung

Jedem Nutzer wird auf Antrag ein Schlüsselpaar erstellt[18]. Dieses Schlüsselpaar besteht aus je einem öffentlichen, jedermann zugänglichen Schlüssel und einem privaten, unter Verschluss zu haltenden anderen. Der öffentliche Schlüssel dient dazu die elektronische Signatur zu überprüfen, also die Authentizität festzustellen. Der private hingegen wird vom Signator dazu verwendet, die digitale Signatur zu erstellen. Erzeugt werden sie durch einen vorgegebenen kryptographischen Algorithmus, wobei der eine das exakte Komplementär zum anderen darstellt, aber der private aus dem öffentlichem Schlüssel, nach jeweiligem Stand der Technik, nicht errechenbar sein darf. Diese Verschlüsselung, bei welcher mit zwei komplementären Schlüsseln gearbeitet wird, nennt man die asymmetrische Verschlüsselung,

---

[15] Vgl. Brenn, C.: Das österreichische Signaturgesetz – Unterschriftenersatz in elektronischen Netzwerken. In: ÖJZ, 16, 54. Jg, 587.
[16] Vgl. Forgó, N.: Sicher ist sicher? – Das Signaturgesetz. In: Ecolex, 9, 1999, 607.
[17] Vgl. Holzbach, M.: Digitale Signatur – Neue Wege elektronischer Geschäftsabwicklung. Online im Internet: Url: http://akitsicherheit.iaik.tu-graz.ac.at/Tagung101097/mholzbach/sld012.htm [abgerufen am 28.3.2000].
[18] Vgl. Tauss, J.: Digitale Signatur und Verschlüsselung. Online im Internet: Url: http://www.tauss.de/bn/sigtext.html [abgerufen am 28.3.2000].

im Gegensatz zur symmetrischen Verschlüsselung, bei welcher nur ein Schlüssel zum Ver- und Entschlüsseln verwendet wird. (Näheres unter 4.1.3.).

3.5 Hash-Wert Erzeugung

Um eine Nachricht digital zu signieren, wird zuerst der Hash-Wert[19] der Daten erzeugt. Der Hash-Wert ist eine Prüfsumme fester Länge (in allen Fällen gleich lang, nämlich 128 bit), die durch einen bestimmten mathematischen Algorithmus errechnet wird. Durch diesen sogenannten Fingerabdruck werden schon kleinste Veränderungen, wie das Einfügen eines einzelnen Buchstabens oder das Ersetzen eines Beistriches durch einen Punkt, erkennbar. Der Algorithmus seinerseits ist so beschaffen, dass weder ein Rückschluss vom Hash-Wert auf die ursprünglich Nachricht möglich ist (Einwegfunktion) noch zwei unterschiedliche Datensätze denselben Wert besitzen können.

3.6 Verschlüsselung

Der Signiervorgang geht damit weiter, dass der erzeugte Hash-Wert mit dem privaten Schlüssel des Signators verschlüsselt und als elektronische Signatur der Nachricht angehängt wird. Grund für die Erzeugung des Hash-Wertes ist, dass die Prüfsumme deutlich schneller erzeugt werden kann, als die Verschlüsselung des gesamten Textes mittels des privaten Schlüssels dauern würde. Danach kann die Nachricht übermittelt werden.

3.7 Entschlüsselung

Der Empfänger kann mit dem öffentlichen Schlüssel des Signators die Signatur entschlüsseln und erhält dadurch wiederum den Fingerabdruck der empfangenen Nachricht. Errechnet der Empfänger jetzt selbstständig den Hash-Wert der angeblich signierten Daten und stimmt er mit dem zuvor aus der Signatur erhaltenen überein, kann er sich darauf verlassen, dass die Nachricht nicht verfälscht wurde und somit authentisch ist.

3.8 Zertifikat

Um zu prüfen, ob der Absender auch der ist, für den er sich ausgibt, dient das Zertifikat. Dieses elektronische Formular wird entweder automatisch der Signatur beigefügt oder ist online, über ein Verzeichnis des Zertifizierungsdiensteanbieters, abrufbar. Im Zertifikat sind

[19] Vgl. Elling, V.: Sichere Hashfunktionen und ihr Gebrauch für digitale Unterschriften. Online im Internet: Url: http://linux.fh-heilbronn.de/vortrag/Kryptographie/volker/sighash.html [abgerufen am 16.8. 1999].

Daten über den Absender vermerkt, die vom Zertifizierungsdiensteanbieter - einer unabhängigen dritten Stelle - auf ihre Richtigkeit überprüft wurden. In welcher Form die Zertifizierungsdiensteanbieter auch dafür haften, hängt davon ab, ob es sich um ein qualifiziertes oder ein einfaches Zertifikat handelt (Näheres unter 7.4.3.2).
Auch besondere Informationen (sog. Attribute) über den Signator können - auf seinen Wunsch - dem Zertifikat beigefügt werden.

Bei den Zertifikaten gibt es verschiedene Sicherheitsstufen[20]:

- Light: dabei wird die Identität des Antragstellers schnell und unkompliziert per Web und e-Mail überprüft.
- Medium: dabei erfolgt eine weitergehende Überprüfung; etwa mittels Kopie des Reisepasses oder des Führerscheines.
- Strong: hier muss die Identifikation persönlich bei einem Postamt erfolgen.
- Premium: bei diesem Zertifikat erfolgt die Identifikation auf dieselbe Weise, wie beim Strong, mit dem Unterschied, dass der private Schlüssel nicht zugeschickt wird, sondern auf einer Smart-Card gespeichert wird und persönlich abgeholt werden muss.

Welche der Klassen verwendet wird, wird meist auf den Transaktionswert des abzuschließenden Geschäfts ankommen. Kleine Summen benötigen üblicherweise weniger Sicherheit. Der Vorteil, den jede Signatur - unabhängig von ihrer Sicherheitsstufe - in gleichem Umfang bietet, ist, dass die Integrität der Nachrichten nachgeprüft werden kann. Bei einer höheren Sicherheitsstufe hat der Zertifizierungsdiensteanbieter bloß sorgfältiger überprüft, ob der Absender der ist, für den er sich zu erkennen gibt und ob auch die anderen behaupteten Merkmale der Wahrheit entsprechen. So kompliziert dies klingen mag: in Wirklichkeit sind für den gesamten Signiervorgang dank besonderer Software nur wenige Mausklicke nötig.

3.9 Attribut-Zertifikate

Neben dem herkömmlichen Inhalt von Zertifikaten, nämlich dem Namen, können auf Wunsch auch weitere rechtlich erhebliche Eigenschaften ins Zertifikat aufgenommen werden. Dazu gehört etwa die Berufsausbildung oder die Vertretungsmacht. Jene müssen ebenso zuverlässig nachgewiesen werden wie die anderen Bestandteile qualifizierter Zertifikate. Qualifizierte Zertifikate sind im Gegensatz zu einfachen Zertifikaten solche, die besonderen Ansprüchen genügen müssen. (Näheres unter 7.3.2.)

[20] Hier am Beispiel der Datakom erklärt. Online im Internet: Url: http://www.datakom.at/ [abgerufen am: 10.7. 1999].

3.10 Pseudonyme

Um im Geschäftsverkehr unerkannt zu bleiben besteht die Möglichkeit, anstatt seines Namens ein Pseudonym zu verwenden. Unter gewissen Umständen muss allerdings der Zertifizierungsdiensteanbieter die wahre Identität des Signators bekannt geben, da ansonsten der Zweck des Signaturgesetzes völlig verloren ginge.
Diese Umstände sind im DSG 2000 in den §§22 (2) und 8 (1) Z4 und (3) enthalten, welches ebenfalls, gleichzeitig mit dem Signaturgesetz, am 1.1.2000 in Kraft getreten ist.

3.11 Server Zertifikate

Ein Server Zertifikat[21] dient einerseits dazu eine sichere Verbindung (SSL) mit einem Web Browser aufzunehmen, indem die zu übertragenden Daten verschlüsselt werden, und andererseits dazu, dass sich jeder Nutzer genauestens über Identität des Serverbetreibers informieren kann. Mittels des Server Zertifikats kann man auch Zutrittsbeschränkungen zu Websites herstellen; dabei prüft der Server bei der Anwahl eines Browsers dessen Anwender-Zertifikat und stellt dabei den Umfang oder den Inhalt der Zutrittserlaubnis fest. In fernerer Zukunft wird diese Methode wohl die Eingabe von Passwörtern gänzlich ersetzen. Es wird dann ausreichen ein einziges Zertifikat zu besitzen, anstatt sich unzählige Logins und dazugehörige Passwörter zu merken.

3.12 Weitere Verwendungsmöglichkeiten

Die asymmetrische Verschlüsselung kann aber nicht nur zum Signieren einer Nachricht verwendet werden, sondern auch zum Verschlüsseln. Dazu muss man lediglich die Daten mit dem öffentlichen Schlüssel des Empfängers kodieren. Ausschließlich der Inhaber des dazupassenden privaten Schlüssels kann die Nachricht wiederum entschlüsseln. (Näheres unter 4.2.)

3.13 Exkurs: Biometrische Verfahren

Zweifelsohne ist dem heutigen Stand der Technik entsprechend ein biometrisches Erkennungsverfahren dem „primitiven“ Schutz durch einen PIN-Code oder eine Chip-Karte vorzuziehen[22]. Nicht nur deshalb, weil biometrische Erkennungsfaktoren nicht verloren oder gestohlen werden können, sondern auch, weil sie eine wesentlich sichere Methode zur

[21] Reif, H.: Winnetou und OLD SSLeay. Online im Internet: Url: http://www.heise.de/ix/artikel/1998/07/128/ [abgerufen am 20.9.2000].
[22] Vgl. Gundermann,L., Köhntopp,M.: Biometrie zwischen Bond und Big Brother – Technische Möglichkeiten und rechtliche Grenzen. In: DuD - Datenschutz und Datensicherheit, 3, 1999, 143.

Identifizierung zwecks Zugangsbeschränkung darstellen. Tatsächlich werden sie auch schon in den verschiedensten Bereichen, wenn auch noch vornehmlich im Ausland, verwendet. Aber auch in Österreich setzt sich allmählich die eindeutige Erkennung einer natürlichen Person durch biometrische Erkennungsfaktoren durch.

Die Forschung hat in den letzten Jahren auf diesem Gebiet beachtliche Fortschritte gemacht. So ist es heute bereits möglich, jemanden aufgrund seines Gesichtes aus einer großen Menschenmenge herauszufiltern oder aufgrund seines Körpergeruches auf sein Hygiene-, Sucht- oder Essverhalten zu schließen. Andere Verfahren wiederum reagieren nicht auf bestimmte personenbezogene Merkmale, sondern schlagen bei Bewegungsabläufen Alarm, die beispielsweise aggressivem Verhalten zueigen sind. Das Wissenschaftsmagazin „New Scientist" berichtete sogar von einem Programm, das Menschen aufgrund ihres Ganges eindeutig identifizieren kann[23]. Durch diese verschiedenartigsten Erkennungsfaktoren sind der totalen Überwachung des Individuums keine Grenzen mehr gesetzt.
Um Missbrauch zu verhindern, wurde in Österreich bereits ein Datenschutzgesetz in Kraft gesetzt. Der grenzüberschreitende Charakter des Internet verlangt aber international einheitliche Regelungen, um wirksam sein zu können.
Inwiefern können nun solche Verfahren mit dem Signaturgesetz in Zusammenhang gebracht werden?

Eine Möglichkeit wäre, biometrische Erkennungsfaktoren als Ersatz für den PIN-Code oder das Passwort zu verwenden, um den Signiervorgang auszulösen. Diese Variante wurde zwar im Signaturgesetz nicht ausdrücklich zugelassen, ja nicht einmal erwähnt, trotzdem wird es dem technologieneutralen Ansatz entsprechend wohl zulässig sein. Ein weiterer Anhaltspunkt für die Zulässigkeit ist in den Erläuterungen zu § 2 Z3 lit c SigG ausgeführt: „In Zukunft werden auch biometrische Merkmale (Fingerabdrücke, Körperfrequenzmesser, auch elektronische Schreibstifte oder Stimmerkennungsverfahren) zur Identifikation des Signators gegenüber seinem privaten Signaturschlüssel eingesetzt werden können."
Ob und wann in der Realität tatsächlich diese Methoden zugelassen werden, hängt wesentlich von der Zustimmung der EU und den nationalen Bestätigungsstellen ab. Meinungsbildend für die EU wirkt in diesem Zusammenhang der „Ausschuss für elektronische Signaturen" in einem Verfahren nach Art 9 der RL.

3.14 Zeitstempel

Da es im Geschäftsleben oft darauf ankommt, dass der genaue Zeitpunkt einer Handlung nachgewiesen werden kann, gibt es den Zeitstempel. Der Zeitstempel hält die Stunde und das Datum relevanter Vorgänge, wie z.B. des Widerrufs, der Sperre oder einfach der Versendung einer Nachricht, fest und speichert sie. Wenn nötig kann damit auch vor Gericht der Zeitpunkt eines Geschehens bewiesen werden. In Österreich wurde bereits einmal ein ähnliches Protokoll mit einem Zeitstempel als entlastendes Beweismittel in einem Verwaltungsverfahren anerkannt. Ein der Übertretung des Parkscheingesetzes Beschuldigter

[23] Vgl. ORF Futurezone: Computer erkennt Diebe am Gang. Online Ausgabe 2.12.1999. Online im Internet: Url: http://futurezone.orf.at/futurezone.orf?read=detail&id=10239&tmp=89416 [abgerufen am: 2.12.1999].

konnte anhand mehrerer e-Mail Protokolle nachweisen, dass er zu dem besagten Zeitpunkt nicht vor Ort war und wurde freigesprochen[24].

3.15 Die Akkreditierung

Wie unten (unter §17) erläutert, können sich Zertifizierungsdiensteanbieter freiwillig akkreditieren lassen, sofern sie die im Gesetz festgelegten Anforderungen erfüllen. Vorteile resultieren aber nicht nur aus besonderen Marketing- und Werbemaßnahmen, die nur den akkreditierten Zertifizierungsanbietern zustehen, sondern auch aus der Möglichkeit etwaige Regressansprüche zu minimieren, sollten sie beweisen können alle Vorkehrungen dem Gesetz entsprechend getroffen zu haben. Da bei akkreditierten Zertifizierungsanbietern das Risiko der Kompromittierung wohl erheblich geringer sein wird als bei solchen, die nicht alle Sicherheitsanforderungen erfüllen, liegt es nahe, dass diese auch weniger Versicherungsprämie zu bezahlen haben werden[25].
Im freien Wettbewerb der Zertifizierungsanbieter wird es wohl ein wichtiges Kriterium für den Erfolg sein, die höchstmögliche Sicherheit, beurkundet durch eine staatliche Einrichtung, vorweisen zu können.
Vermutlich wird es aber in der Praxis auch solche Zertifizierungsdiensteanbieter geben, die zwar alle Erfordernisse erfüllen, sich aber nicht der staatlichen Kontrolle unterwerfen wollen und somit auf ein Akkreditierung verzichten.

3.16 Die Sicherheit der Anforderungen nach dem Signaturgesetz

Die in den Anhängen II und III der SigV festgelegten Schlüssellängen dürften nach dem momentanen Stand der Technik lange genug sein, um unbefugtes Entschlüsseln verhindern zu können. Laut Punkt 4 im Anhang I wird dies auch bis 31. Dezember 2005 so bleiben.
Jedoch ist eine Kette nur so stark wie ihr schwächstes Glied. Bei an das Internet angeschlossenen Systemen kann niemals eine absolute Sicherheit gewährleistet werden.
Dass ein gewisses Restrisiko bestehen bleibt und man deswegen nicht auf jegliche hohe Sicherheitsanforderungen verzichten kann, bleibt unbestritten. In den meisten Fällen ist die Illusion der absoluten Sicherheit, die zur Unbekümmertheit führt, sogar schädlicher als das Wissen über die Verwundbarkeit des Systems.

[24] MA 67-PA-521173/8/8 vom 18.8.1998.
[25] Vgl. Belkem, M.: Die digitale Signatur kurz vor dem Start. In: DuD – Datenschutz und Datensicherheit, 24, 2000, 75.

4 Die Kryptographie-Diskussion

4.1 Aus technischem Blickwinkel

4.1.1 Terminologie

Unter Kryptographie wird eine wissenschaftliche Disziplin verstanden, die sich mit der Verheimlichung von Inhalten von Nachrichten beschäftigt, um sie vor unbefugtem Zugriff zu schützen.
Die „Komplementärdisziplin“ dazu ist die Kryptoanalyse, die sich damit beschäftigt, verschlüsselte Nachrichten zu knacken um ihren Inhalt - meist unbefugt - lesbar zu machen.
Die Kryptologie[26] ist der Oberbegriff dieser beiden Disziplinen, welche ihrerseits eine Wissenschaft aus dem Teilgebiet der angewandten Mathematik ist.
Als Klar- bzw. Chiffretext bezeichnet man ungesicherte bzw. gesicherte Nachrichten, welche durch Chiffrierung bzw. Dechiffrierung umgewandelt werden.

4.1.2 Einleitung

Da es mittlerweile ein Vielzahl von Verschlüsselungssystemen gibt, sei hier nur eine kleine Auswahl angeführt, die lediglich Basiswissen der Kryptologie vermitteln soll.
Bei einer Verschlüsselung werden üblicherweise zwei Komponenten verwendet, nämlich einerseits der Algorithmus und andererseits der Schlüssel. Der Algorithmus ist ein Verfahren, mit dem eine Nachricht verändert wird. Dieser ist konstant und kann jedem bekannt sein. Um die Nachricht bloß für den Empfänger lesbar zu machen, wird dem Algorithmus eine empfängerspezifische Variable hinzugefügt, welche als Schlüssel bezeichnet wird.

Als simples Beispiel sei die Caesar-Chiffre[27] erwähnt: Dabei wurde lediglich jeder Buchstabe im Alphabet mit dem drittfolgenden ausgetauscht. Aus einem a wurde ein d, aus dem b ein e usw. Die Verschiebung der Buchstaben stellt somit den Algorithmus dar und die Verabredung, dass die Buchstaben um drei Stellen verschoben werden sollen, den Schlüssel (die Variable). Bei diesem Verfahren könnte die Nachricht natürlich durch bloßes Durchprobieren aller möglichen Schlüssel, dem sogenannten „brute force Angriff“(übersetzt: Angriff mit roher Gewalt) in kürzester Zeit entschlüsselt werden. Diese Gefahr kann durch einen entsprechend großen Schlüssel, bei dem das „Knacken“ Jahrzehnte dauern würde,

[26] Vgl. Glintschert, A.: Kryptologie und die neuen Medien. Online im Internet: Url: http://www.educat.hu-berlin.de/publikation/student/kryptologie/einfuehrung.html [abgerufen am 5.9.2000].
[27] Heß, A.: Grundlagen der Kryptographie. Online im Internet: Url: http://www.uni-mainz.de/~hessan00/krypto/Krypto1.html [abgerufen am: 5.9.2000].

minimiert werden. Selbstverständlich sind heute die Verfahren um ein Vielfaches komplizierter, die Grundidee ist aber immer noch dieselbe.

Den endgültigen Durchbruch in Sachen sicherer elektronischer Kommunikation haben 1976 Diffie und Hellman[28] mit der Entdeckung der asymmetrischen Verschlüsselung (Näheres unter 4.1.3.2.) geschafft. In wie viel verschiedenen Bereichen heutzutage schon Verschlüsselungssysteme eingesetzt werden, lässt deren Wichtigkeit bloß erahnen. So werden sogar die Funksprüche der Formel 1 Fahrer zu ihren Boxen chiffriert, um nicht der Konkurrenz wichtige Betriebsgeheimnisse oder Marktvorsprünge zu verraten.

4.1.3 Die verschiedenen Verschlüsselungsmethoden

4.1.3.1 Die symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung[29] haben Sender und Empfänger denselben Schlüssel, der sowohl zum Ver- als auch zum Entschlüsseln verwendet wird. Diese Verfahren bedürfen üblicherweise geringeren Zeitaufwandes als asymmetrische mit vergleichbarer Sicherheit. Der Nachteil dabei ist nur, dass ein sicherer Kanal Voraussetzung ist, der benutzt werden kann, um den Schlüssel abhörsicher auszutauschen. Wenn ein solcher Kanal zu Verfügung steht, ist aber in aller Regel keine Verschlüsselung mehr nötig. Ein weiterer Nachteil ist, dass man für jeden einzelnen Kommunikationspartner einen eigenen Schlüssel benötigt. Bekanntestes Beispiel dieses Verfahrens ist: DES (Data Encyption Standard).

4.1.3.2 Die asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung[30] erhält jeder Anwender zwei Schlüssel. Einen privaten (geheimen) und einen öffentlichen (jedermann zugänglichen). Der private Schlüssel ist zwar komplementär zum öffentlichen, kann aber aus ihm quasi nicht errechnet werden. Wird also eine Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsselt, kann nur dieser sie mit seinem eigenen privaten wieder entschlüsseln. Der Nachteil bei diesem asymmetrischen System (auch Public Key Verfahren genannt) ist, dass der Schlüssel um vieles länger sein muss als bei symmetrischen und somit der Verschlüsselungsvorgang erheblich zeit- und rechnerintensiver ist. So gelten momentan bei einem symmetrischen Verfahren 128 Bit Schlüssel als sicher, bei asymmetrischen dagegen 1024 Bit Schlüssel. Von Vorteil ist es, dass kein sicherer Kanal zum Schlüsselaustausch vorhanden sein muss. Eine

---

[28] Diffie, W., Hellman, M.: New Directions in Cryptography. In: IEEE Transactions on Information Theory 1976, Vol. IT-22, 644 – 654.

[29] Vgl. Lauert, A.: Elektronisches Bezahlen. Online im Internet: Url: http://didaktik.cs.uni-potsdam.de/Lehre/e-commerce/elBez2-5/page05.html [abgerufen am 5.9. 2000].

[30] Vgl. Lauert, A.: Elektronisches Bezahlen. Online im Internet: Url: http://didaktik.cs.uni-potsdam.de/Lehre/e-commerce/elBez2-5/page06.html [abgerufen am 5.9.2000].

Einrichtung, die den Abruf des öffentlichen Schlüssels ermöglicht, muss jedoch geschaffen werden.
Bekanntestes Beispiel ist das RSA-Verfahren[31], welches von R. Rivest, A. Shamir und L. Adleman entdeckt wurde.

4.1.3.3 Pretty Good Privacy

Das laut Testversuchen[32] momentan wohl sicherste Ver- und Entschlüsselungsprogramm ist PGP[33]. 1991 wurde es erstmals von seinem Schöpfer, Philip Zimmerman, vorgestellt. PGP verwendet zur Chiffrierung einer Nachricht den IDEA-Algorithmus, mit einem einmaligen Sitzungsschlüssel zur Erzeugung des Hash-Wertes, den MD5-Algorithmus, (Message-Digest 5) und - zur Verschlüsselung des IDEA-Sitzungsschlüssels und der Prüfsumme - das RSA-Verfahren. Der Hauptvorteil von PGP liegt neben der großen Sicherheit in der hohen Aktionsgeschwindigkeit. Das deshalb, weil die hervorragenden Eigenschaften der symmetrischen und der asymmetrischen Verschlüsselung vereinigt wurden. Der IDEA-Algorithmus basiert nämlich auf der symmetrischen Verschlüsselung und das RSA-Verfahren auf der asymmetrischen.
PGP ist ein Freeware Programm für den nicht kommerziellen Gebrauch, das auch bereits dementsprechend weit verbreitet ist.

4.2 Aus rechtlichem Blickwinkel

4.2.1 Einleitung

Wie oben (unter 3.12) erwähnt kann man die Signaturschlüssel nicht nur zum Signieren, sondern auch zum Verschlüsseln einer Nachricht einsetzen. Dabei muss man die zu verschlüsselnden Daten mit dem öffentlichen Schlüssel des Empfängers chiffrieren. Diese dadurch scheinbar unlesbar gemachte Nachricht ist nur mehr mit dem dazugehörigen privaten Schlüssel des Empfängers zu dechiffrieren.
Nun stellt sich jedoch die Frage inwieweit es überhaupt rechtens ist, dass Verschlüsselungen verwendet werden. Oder sollen solche oder ähnliche kryptographische Systeme generell gesetzlich verboten werden.
Einerseits entstehen der Industrie jährlich durch das illegale Ausspähen, Fälschen und Zerstören von Daten Schäden in Milliardenhöhe, andererseits will man aber das Internet nicht zu einer Spielwiese für Terroristen erklären, indem der Staat selbst nicht zu knackende

[31] Vgl. Leipholz-Schumacher, B.: Kryptographie. Online im Internet: Url: http://www.zitadelle.juel.nw.schule.de/if/java/krypto/RSAInfo.html [abgerufen am 10.9.2000].
[32] Vgl. Datacom Austria GmbH: Die meisten Verschlüsselungsprogramme sind unsicher. Online im Internet: Url: www.datacom.at.cgi [abgerufen am: 12.7.1999].
[33] Online im Internet: Url: http://www.pgp.com/ [abgerufen am: 5.9.2000].

Verschlüsselungsprogramme zulässt. Das Problem entstand Anfang der Neunzigerjahre dadurch, dass bereits mit geringer Rechnerkapazität Daten derart verschlüsselt werden konnten, dass sogar die Geheimdienste trotz der ungleich größeren technischen Möglichkeiten befürchten mussten, ihre Abhörmöglichkeiten einzubüßen. Bisher konnten durch einfaches Ausprobieren der sogenannten Brute-Force Methode in Kürze jegliche Schlüssel geknackt werden. Erstmals in der Geschichte der Telekommunikation ist es nun möglich, selbst seine Daten zu schützen, anstatt sich auf die Netzanbieter zu verlassen.

4.2.2 Hauptargumente und rechtliche Basis der Kryptodiskussion in Österreich

Die Diskussionen darüber, ob man Verschlüsselungstechniken reglementieren[34] oder sogar unter Strafe stellen sollte, laufen bereits seit mehreren Jahren. Vor allem die USA, wo starke Verschlüsselungsalgorithmen unter das Waffenexportgesetz fallen, drängen auf eine Beschränkung der Möglichkeiten. In Österreich würde allerdings eine derartige Regelung möglicherweise gegen das Verfassungsrecht verstoßen[35]. Das Recht auf Privatsphäre (Art 8 MRK), das Recht auf Vertraulichkeit der mediatisierten Individualkommunikation (Brief- und Fernmeldegeheimnis[36] der Art 10, 10a StGG) und nicht zuletzt der Datengeheimnisaspekt des allgemeinen Datenschutzes (§ 1 DSG) wären zu berücksichtigen.

Ob eines dieser Grundrechte verletzt wird, müsste man nach den Kriterien des öffentlichen Interesses, der Eignung, der Erforderlichkeit und der Adäquanz prüfen[37].
Würde man dem entgegen die Meinung vertreten, dass das Briefgeheimnis im Internet erst durch die Kryptographie geschaffen wird, würde jede Beschränkung der Verschlüsselungsmöglichkeiten das Grundrecht verletzen und Verfassungswidrigkeit die Folge sein. Verschlüsselungseinschränkungen könnten auch in den Schutzbereich des Grundrechts auf Kommunikationsfreiheit fallen.
Laut Art 13 StGG hat jedermann das Recht, durch Wort, Schrift, Druck .... seine Meinung ... frei zu äußern. Welche Bedeutung welchem Schriftzeichen zugeordnet wird, kann dabei jeder selbst entscheiden. Bei einem Verbot würde das bei weitester Auslegung bedeuten, dass man keine Anspielungen oder Metaphern mehr verwenden dürfte.

Auf den herkömmlichen Briefverkehr umgedeutet würde ein Verschlüsselungsverbot dazu führen, dass Briefumschläge nicht mehr verwendet werden dürften oder beim Kauf eines Tresors einen Zweitschlüssel hinterlegt werden müsste. Diese Regelungen wären doch, so mag man meinen, völlig undenkbar und nur in totalitären Systemen möglich.
Auch wenn Brief- und Fernmeldegeheimnis einen hohen Stellenwert in unserer Verfassung genießen, gibt es aber doch immer wieder Situationen, in denen man über Mittel zur Erhaltung der wichtigsten Grundwerte nachdenken muss. Ob diese Grundwerte bereits heute durch organisiertes Verbrechen, Geldwäscherei oder den Drogenhandel übers Internet bedenklich beeinträchtigt wurden, bleibt dahingestellt. Ein Verbot oder zumindest ein Teilverbot der Kryptographie wäre aber theoretisch durchaus denkbar, da sowohl das Brief-

[34] Vgl. Mayer-Schönberger, V.: „Krypto-logisch“ Die neue Versuchung im Cyberlaw. Online im Internet: Url: www.normative.zusammenhänge.at [abgerufen am: 7.7.1999].
[35] Vgl. Brenn, C.: Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet. In: ÖJZ, 17, 52. Jg, 644ff.
[36] Vgl. Wessely, W.: Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? In: ÖJZ, 13, 54. Jg, 491.
[37] Öhlinger, T.: Verfassungsrecht. WUV Universitätsverlag, 3. Auflage, 1997, 285.

und Fernmeldegeheimnis als auch das Recht auf freie Kommunikation mit Gesetzesvorbehalt normiert sind und somit der Gesetzgeber „nur“ auf die Einhaltung der oben genannten Kriterien zu achten hätte.
Allerdings wird in der Realität der vom VfGH entwickelte Verhältnismäßigkeitsgrundsatz, vermutlich doch eine unüberwindbare Schranke darstellen.

Wie oben (unter 4.1.3) erwähnt gibt es Verschlüsselungsverfahren, deren Entschlüsselung in absehbarer Zukunft geradezu unmöglich ist, was zur Folge hat, dass die legitimen Abhörmaßnahmen des Staates ins Leere greifen. Zweifellos ist es aber im öffentlichen Interesse, dass eine wirksame Strafverfolgung gesichert wird, was auch das Ziel einer Kryptoregulierung wäre. Ob diese Regulierung zur Erreichung des gewünschten Zieles geeignet ist, wird jedoch vielfach verneint.

Kriminelle werden ungeachtet staatlicher Einschränkungen immer, in den meisten Fällen auch unerkannt, sichere Verfahren verwenden und solche meiden, bei denen geplante Sicherheitslücken eingebaut sind. Welche der möglichen Reglementierungen das schonendste Mittel zur Erreichung des Zweckes darstellt und ob die Mittel zur Verbrechensbekämpfung und die Einschränkung der oben genannten Grundrechte in einer angemessenen Relation zueinander stehen, bleibt zu diskutieren. Der tatsächliche Nutzen eines Verschlüsselungsverbotes wird jedoch sehr gering ausfallen, da anzunehmen ist, dass vor allem die organisierte Kriminalität über versierte Fachleute verfügt, die die Schwachstellen der einzelnen Regulierungen gekonnt zu umgehen wissen.

Zu überlegen wäre gegebenenfalls weiters, ob eine etwaige illegale Verschlüsselung unter Strafe gestellt werden soll und wenn ja, mit welchem Strafausmaß. Wenn die Kommunikation nicht gerade den Tatbestand der nationalsozialistischen Propaganda erfüllt, wäre eine Verabredung im Vorfeld einer Straftat höchstens als Vorbereitungshandlung zu werten, die an sich nicht strafwürdig ist. Daraus eine Straftat zu machen würde wohl nur schwerlich mit der Verfassung in Einklang zu bringen sein. Wenn doch, könnte das Strafausmaß jedenfalls nur sehr niedrig ausfallen, was wiederum bedeutet, dass das Risiko eine Geldstrafe zu zahlen im Hinblick auf eine abhörsichere Kommunikation gerne in Kauf genommen werden würde.

Bedacht zu nehmen ist aber nicht nur auf die Interessen der Strafverfolgung, sondern auch auf die der Industrie und der Wirtschaft und die damit verbundenen Arbeitsplätze. Ebenso hat der Bürger ein Recht auf Respektierung und Wahrung seiner Privatsphäre. Neben der Wirtschaftsspionage, die jährlich Schäden in Milliardenhöhe verursacht, stellt sich für den Einzelnen das Problem, dass sich durch dauernde Belauschung von Nachrichten Persönlichkeitsprofile ableiten lassen und es - in Hinblick auf die mögliche Kommunikation mit Ärzten, Banken und Versicherungen - zum „gläsernen Menschen“ nicht mehr weit ist.

4.2.3 Persönliche Einschätzung

Ich selbst spreche mich gegen jegliche Beschränkung der Verschlüsselungsmöglichkeiten aus. Die Nutzung des Internet für Verabredungen zu illegalen Handlungen stellt lediglich eine Randerscheinung im Hinblick auf die vielfältigen (legalen) Verwendungsmöglichkeiten des Netzes dar. Man sollte der organisierten Kriminalität nicht auf Kosten der Grundrechte der bedeutenden Mehrheit der User Herr zu werden versuchen. Immerhin gibt es eine Vielzahl

anderer Methoden die Kommunikation Krimineller zu überwachen. Zu denken ist dabei vor allem an Programme, die jeden Tastaturklick speichern und übertragen können, womit der Inhalt einer Nachricht bereits vor ihrer Versendung eruiert werden kann. Die Installation dieser Software durch stattliche Organe könnte beispielsweise durch eine Norm, die sich inhaltlich an die §§ 149a ff StPO anlehnt, legalisiert werden. Bei der Überwachung des Fernmeldeverkehrs ist ja bereits die Möglichkeit der Anbringung technischer Hilfsmittel an Geräten in Wohnungen unter strengen Voraussetzungen vorgesehen.

Ein System mit eingebauten „Schlupflöchern" oder gar nur schwache Algorithmen sind mit Sicherheit keine befriedigende Lösung. Wenn der Staat im Notfall Nachrichten unbefugt entschlüsseln kann wird es in der Praxis nicht allzu lange dauern, bis das auch andere können. Zuletzt ist noch anzumerken, dass es technisch beinahe unmöglich ist, wirksam Verschlüsselungsverbote durchzusetzen. In diesem Zusammenhang erachte ich folgenden Vergleich als äußerst treffend: „Kryptographie-Einschränkung ist so wirkungsvoll wie ein Vermummungsverbot für Bankräuber."[38]

4.3 Denkbare Reglementierungsmöglichkeiten

4.3.1 Einleitung

Auch wenn man den folgenden Punkten die Annahme der rechtlichen Zulässigkeit zugrunde legt, wird man sehen, dass das Erkennen eines Vergehens in den meisten Fällen mit hohem Aufwand verbunden ist, wenn nicht gar nur durch Stichproben aufzudecken. Die Zweckhaftigkeit einer Beschränkung erscheint aus diesem Blickwinkel sehr zweifelhaft.

4.3.2 Totalverbot

Ein Totalverbot würde jegliche Verschlüsselungsanwendungen kriminalisieren. Die Durchsetzung würde allerdings in der Realität auf erhebliche technische Schwierigkeiten stoßen, da bloß zeitaufwendige Stichproben Verschlüsselungen aufdecken könnten. Grund dafür ist, dass verschlüsselte Nachrichten in der Regel die Form eines scheinbar sinnlosen Textes haben. Jedoch können Programme, die solche Zeichensalate orten, nicht zwischen verschlüsselten und beispielsweise komprimierten Daten unterscheiden, die ebenfalls diese vermeintlich sinnlose Form aufweisen.
Bei stenographischen Verschlüsselungen würde nicht einmal ein Verdacht aufkommen können.

[38] Gutenberg, J.: Grundprobleme von Datenschutz und Datensicherheit. Online im Internet: Url: http://www.uni-mainz.de/~pommeren/DSVorlesung/Grundprobleme/Kryptopolitik.html [abgerufen am 25.3.2001].

4.3.3 Verbot langer Schlüssel und starker Algorithmen

Bei dieser Variante wären lediglich schwache Verschlüsselungsalgorithmen bzw. Verfahren zugelassen. Das hätte zur Folge, dass Nachrichten zumindest vor dem Mitlesen des Normalbürgers geschützt sind. Der Geheimdienst aber könnte durch bloßes Durchprobieren den Inhalt lesbar machen. Der Nachteil dabei ist, dass auch versierte Hacker mit überdurchschnittlichen Rechnern so in vertretbarer Zeit zu ihrem Ziel kommen würden. Wie schon unter Punkt 4.3.2. stößt man auch hier auf nicht unbeachtliche Probleme bei der Erkennung. Zusätzlich besteht auch noch die Möglichkeit, die zu verschickende Nachricht zuerst mit einem illegalen starken Algorithmus zu verschlüsseln und danach noch einmal, diesmal mit einem erlaubten schwachen. Auf diese Weise würde bei einer automatisierten Prüfung kein Rechtsverstoß erkannt werden können.

4.3.4 Pflicht zur Schlüsselhinterlegung (Key Recovery)

Diese Reglementierung stellt wohl den idealsten Kompromiss zwischen Überwachungsmöglichkeit und Verschlüsselungsbefugnis dar. Dabei können alle dem modernsten Stand der Technik entsprechende Verschlüsselungsverfahren eingesetzt werden, unter der Voraussetzung, dass bei einer unabhängigen dritten Stelle ein Zweitschlüssel hinterlegt wird. Das hat den Vorteil, dass sich weder aktive noch passive Angreifer und auch nicht die Geheimdienste Zugriff zu den Daten verschaffen können, jedoch der Staat bei begründetem Verdacht einer Straftat die Herausgabe des Zweitschlüssels fordern kann. Diese unabhängige Instanz müsste natürlich entsprechend vertraulich und vor Angriffen geschützt sein und dürfte den Zweitschlüssel nur aufgrund eines richterlichen Beschlusses herausgeben. Der Nachteil hierbei ist der immense Verwaltungs- und Sicherheitsaufwand.

Außerdem könnte man mit stenographischen Verfahren oder doppelter Verschlüsselung auch diese Regelung wirksam umgehen. Zu bedenken ist außerdem, dass mit einem einmaligen Zugriff auf den Schlüssel sowohl jegliche vergangenen, gegenwärtigen als auch zukünftigen Nachrichten mitgelesen werden können. Um den Staat vor dieser Versuchung zu bewahren, wären Einmal-Passwörter durchaus ein adäquates Mittel.
Das zuletzt Gesagte gilt natürlich für alle Eingriffe, bei denen der private Schlüssel bekannt wird.

4.3.5 Verfahren mit der Möglichkeit auf Schlüsselrückgewinnung

Da dieses Verfahren mathematisch noch nicht genügend entwickelt wurde, ist es bislang bloß eine schlechte Alternative. In der Theorie funktioniert es so, dass bei der Schlüsselgewinnung ein elektronischer Hintereingang offengelassen wird, durch den bei Bedarf der wahre Schlüssel rekonstruiert werden kann. Sollte es aber in absehbarer Zukunft soweit kommen, dass dieses Verfahren, vom technischen Standpunkt aus gesehen, einsatzfähig ist, würde man sich die gesamte Infrastruktur, die für die Schlüsselhinterlegung nötig ist, ersparen. Was zuvor zu den Problemen der Kontrolle gesagt wurde, gilt auch dabei.

4.3.6 Gänzliche Zulassung

Bei einer gänzlichen Zulassung kryptographischer Methoden könnte jeder selbst entscheiden, in welchem Ausmaß und auf welche Weise er seine Nachrichten verschlüsselt. Für diese Variante sprechen sich eine Vielzahl der Diskussionsteilnehmer[39] aus, und zwar nicht nur aus rechtspolitischen Gründen, sondern auch deshalb, weil es in der Realität ohnedies nicht möglich ist, den Datenverkehr der Kriminellen zu entschlüsseln. In Wahrheit würde eine Einschränkung nur dazu führen, dass der „Normalbürger" überwacht wird und die Verbrecher weiterhin die sicheren Verschlüsselungsmöglichkeiten nutzen.

5 Ausländische Kryptopolitik

Entscheidend für die Charakteristik der Kryptopolitik eines Landes ist nicht nur der Umfang der Freigabe oder der Untersagung verschiedenster Verschlüsselungsmöglichkeiten (Nutzungsbeschränkung), sondern auch, ob Chiffriersysteme Exportbeschränkungen unterliegen oder nicht (Exportbeschränkung).

5.1 Deutschland

Die deutsche Haltung zur Frage der Nutzung kryptographischer Verfahren beim Einsatz im elektronischen Geschäftsverkehr wurde in Form von "Eckpunkten der deutschen Kryptopolitik" vom Bundeskabinett in einer Sitzung am 2. Juni 1999 festgelegt[40]. Dabei anerkennt das Kabinett das Anliegen deutscher Nutzer in den weltweiten Netzen auf sichere Kommunikation, gewährleistet durch starke Verschlüsselungsverfahren. Es wurde außerdem klargestellt, dass diese Verfahren auch zukünftig entwickelt, hergestellt, vermarktet und genutzt werden dürfen. Die Leistungs- und Wettbewerbsfähigkeit der heimischen Kryptohersteller soll gefördert werden, wofür bereits der erste Schritt in Form der Revision der EG-DUAL-USE-Verordnung[41] getan wurde. Keineswegs verkennt man jedoch die Gefahr des kriminellen Missbrauchs, weshalb eine genaue Beobachtung der Entwicklung innerhalb der nächsten beiden Jahre von den betroffenen Ministerien geplant ist. Das bislang bei der Strafverfolgung unbedeutende Problem, der nicht zu „knackenden" Kommunikation zwischen Kriminellen, soll auch weiterhin durch Verbesserung der technischen Ausstattung der Strafverfolgungs- und Sicherheitsbehörden so gering wie möglich gehalten werden.

---

[39] Vor allem Deutschland; Position und Chancen der deutschen IT-Sicherheitsindustrie im globalen Wettbewerb. Online im Internet: Url: http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=38&tdid=375 [29.1.2001].

[40] Sicherheit im Internet: Pressemitteilung des Bundesministerium für Wirtschaft und Technologie und des Bundesministerium des Innern. Online im Internet: Url: http://www.sicherheit-im-internet.de/showdoc.php3?doc=bmwi_min_doc_1999940655766&page=1 [abgerufen am: 25.10.1999].

[41] Verordnung (EG) Nr. 1334/2000des Rates vom 22.6.2000 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr von Gütern und Technologien mit doppeltem Verwendungszweck. Online im Internet: Url: http://wko.at/eu/zoll/dual-use-vo.htm [abgerufen am 2.2.2001].

5.2 USA

Die USA betreiben eine bekannt restriktive Kryptopolitik, welche zwar auf Grund des Druckes der Wirtschaft immer mehr gelockert wird, jedoch noch weit von einer Liberalisierung entfernt ist. Da bereits mehrere Versuche, wie die Einführung des Clipper Chips oder der staatlichen Schlüsselverwaltung, die Verschlüsselungen zu kontrollieren, gescheitert sind, versucht man sich jetzt in den sogenannten Key-Recovery oder Key-Escrow-Systemen. Die Clipper Chip Technik ist ein Verfahren, bei dem der geheime Schlüssel mit jeder Nachricht mitgeschickt wird und selbst durch einen „Skipjack" verschlüsselt wird[42]. Dieser „Skipjack" soll natürlich nur dem Staat bekannt sein und auf Gerichtsbeschluss der Strafverfolgungsbehörde ausgefolgt werden. Alle anderen Verschlüsselungsmethoden sollten hingegen verboten werden.

Vor allem auf Grund lautstarker Proteste der Datenschützer und Bürgerrechtler konnte sich dieses System nicht durchsetzen, wobei das Misstrauen gegen dieses Verfahren auch noch dadurch verstärkt wurde, dass es von der NSA (National Security Agency) entwickelt wurde. Dem Key-Recovery System sollen nun gewisse Exportprivilegien zum Durchbruch verhelfen. Bis zum 30.12.1996 unterlagen kryptographische Produkte noch der ITAR (International Traffic in Arms Regulation) und waren auf der United States Munition List vermerkt, was bedeutete, dass nur solche Programme ausgeführt werden durften, die eine Schlüssellänge unter 40-Bit verwendeten[43]. Nach der ersten Lockerung der Exportpolitik wurden Verschlüsselungsprodukte, die nicht mehr speziell der militärischen Nutzung zugeordnet waren, unter die Kontrolle der EAR (Export Administration Regulations) gestellt. Erstmals galten danach jene Programme nicht mehr als Kriegsmaterial, sondern als „Dual Use- Güter".

Die zuvor angesprochenen Exportprivilegien gelten nunmehr in der Form, dass Verschlüsselungsprogramme mit einer Schlüssellänge, die sogar 56-Bit übersteigen kann, ausgeführt werden dürfen, sofern sie Key-Escrow oder Key-Recovery unterstützen. Lediglich Programme mit 40-Bit Schlüsseln können nach vorheriger Genehmigung der EAR und der BXA (Bureau of Export Administration), welche ohnehin Voraussetzung für alle Kryptoexporte ist, ohne Unterstützung der Key-Recovery/Escrow Systeme ausgeführt werden. Diese Genehmigung wird im übrigen dann erteilt, wenn die US Behörden innerhalb von zwei Stunden auf den Klartext zugreifen können. Im übrigen ist eine Ausfuhr in sieben als „terroristisch" eingestufte Länder völlig ausgeschlossen.

5.3 Frankreich

Ebenfalls strengen Einschränkungen unterlagen elektronische Verschlüsselungssysteme in Frankreich[44] zwischen 1990 und 1996. Innerhalb dieses Zeitraumes galt ein Gesetz (Nr. 90-

[42] Vgl. unbekannter Autor: Clipper-Chip. Online im Internet: URL: http://www.tzi.de/~ansu/papers/crypto/cryptohtml/main-node20.html [abgerufen am: 7.11.1999].
[43] Beucher, K., Schmoll, A.: Kryptotechnologie und Exportbeschränkungen. In: Computer und Recht, 8, 1999, 529.
[44] Vgl. Couvert-Castéra, I.: Frankreich: Kryptographie liberalisiert. In: DuD – Datenschutz und Datensicherheit, 1998, 22, 338.

1170 vom 30.12.1990)[45], das Verschlüsselungen de facto verbot. Nach einer Gesetzesänderung (Nr. 92-1358 vom 28.12.1992) wurde dieses generelle Verbot insofern gelockert, dass nunmehr solche Chiffriersysteme erlaubt waren, die bei Bedarf von den Behörden entschlüsselt werden konnten. 1996 trat ein Gesetz in Kraft, das Verschlüsselungen mit bis zu 40-bit duldete. Diese Grenze wurde im Jänner 1999 auf 128-bit angehoben, wobei Strafen bis zu sechs Monaten Arrest für Zuwiderhandlungen vorgesehen sind. Die Verwendung zur Authentifikation ist in Frankreich mit vorheriger Anmeldung beim Zentralamt gestattet.
Weitere Liberalisierungen zur Beseitigung des Rückstands beim Internet sind angekündigt.

5.4 Regelungsmodelle der Organisationen

5.4.1 Die EU

Innerhalb der EU sind Massenmarktprodukte, unabhängig von ihrer Schlüssellänge, keinen Exportbeschränkungen unterworfen. Hierin unterscheidet sich die Politik der EU wesentlich von der des Wassenaar Abkommens (Näheres unter 5.4.3), bei dem uneingeschränkter Handel mit Massenmarktprodukten nur bis zu einer Schlüssellänge von 64-bit erlaubt ist. Massenmarktprodukte, auch Ladentisch Software genannt, sind allgemein zugängliche Programme (Public Domains) und werden wie jegliche andere Software behandelt. Der Public Domain ist es zu eigen, dass sie uneingeschränkt weiterverbreitet werden kann und auch auf CD gebrannt und verfügbar gemacht werden darf. Problematisch erscheint hierbei, dass unter diese Definition auch das Verschlüsselungsprogramm PGP fällt. Über einen Ausschluss dieser Software wird allerdings bereits diskutiert. Für Verfahren zur digitalen Signatur und zur Authentifizierung sind keine Exportbeschränkungen vorgesehen.

Im übrigen vertritt die EU die Meinung, dass das Key-Escrow System nicht die geeignete Politik wäre. Jedenfalls aber fordert die EU ihre Mitgliedstaaten zur Anerkennung der folgenden grundlegenden Punkte auf:
Von allen Mitgliedstaaten ist die identische Liste der Dual-Use Güter anzuerkennen, welche im Großen und Ganzen mit jener des WA übereinstimmt.
Die Mehrheit der Dual-Use Güter benötigen für den Verkehr innerhalb der EU und einiger begünstigter anderer Staaten[46] nur eine generelle Ermächtigung.
Insgesamt sollten die Mitgliedstaaten ein gemeinsames Niveau, bezüglich Exportkontrollen haben und eine Exportlizenz sollte üblicherweise auch für Güter der anderen Mitgliedstaaten gelten.

[45] Online im Internet: Url: http://home.fhtw-berlin.de/~s0291172/Semesterarbeit/frankreich.html#frankreich [abgerufen am: 31.8.200].
[46] Australia, Canada, Japan, Norway, Switzerland, und die United States.

5.4.2 Die OECD

5.4.2.1 Die Entwicklung der Richtlinie[47]

Die Organization for Economic Cooperation and Development, der momentan 29 Staaten angehören, wurde erstmals 1996 von der US Regierung dazu angehalten Richtlinien für eine internationale Kryptopolitik auszuarbeiten. Von Beginn an war die OECD dem ständigen, hartnäckigen Druck der USA ausgesetzt, die unter allen Umständen die Einführung des Key-Escrow Systems durchsetzen wollten. Unterstützt wurden die USA, beeinflusst von den Geheimdiensten und Strafverfolgungsbehörden, dabei vor allem von Frankreich und England.

Durch das Hinwirken von Japan und Skandinavien verließ man aber bereits 1997 die Key-Escrow Linie. Diesem Vorbild sind die meisten nationalen und internationalen Bewegungen gefolgt.
Die Richtlinien, wie der Name schon sagt, sollten keine bindenden Normen schaffen, sondern vielmehr ein hilfreicher Wegweiser zur vermeintlich richtigen, nationalen Kryptopolitik sein[48]. Mittels Fragebögen hat man die Freizügigkeit der einzelnen Staaten bezüglich der Kryptopolitik eruiert und sie in einer Farbskala zusammen gefasst, wobei „rot“ als sehr restriktiv und „grün“ als sehr liberal gilt. „Rot-gelb“, „gelb“, „gelb-grün“ stellen die Zwischenbereiche dar. Bei Gesamtbetrachtung dieser Einstufungen lässt sich ein gewisses Muster erkennen: „Je undemokratischer das System, desto drastischer die Krypto-Restriktionen. "Spitzenreiter" im negativen Sinn sind China, Israel, Kasachstan, Pakistan, Russland, Singapur, Tunesien, Vietnam und Venezuela.[49]“

5.4.2.2 Die wichtigsten Eckpunkte der Richtlinie

- Die kryptographischen Methoden sollen das Vertrauen der Nutzer in die Informations- und Kommunikationssysteme schüren;
- Es soll dem Nutzer freigestellt sein, welche Methoden er verwendet;
- Die Menschenrechte, wie die Kommunikationsfreiheit und das Recht auf Privatsphäre soll in der Festlegung der Kryptopolitik eine gewichtige Rolle spielen;
- Unter gesetzlich festgelegten Fällen soll es erlaubt sein, auf den Klartext zurückzugreifen;

---

[47] The OECD Cryptographie Policy Guidelines and the Report on Background and Issues of Cryptography Policy, March 1997. OCDE/GD(97)204. Online im Internet: Url: http://www.oecd.org/dsti/sti/it/secur/index.htm [abgerufen am 27.3.2001].
[48] Vgl. Brenn, C.: Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet. In: ÖJZ, 17, 52. Jg, 643ff.
[49] Medosch, A.: Alles was Sie schon immer über Krypto-Regulierungen wissen wollten. Online im Internet: Url: http://www.heise.de/tp/deutsch/html/result.xhtml?url=/tp/deutsch/inhalt/te/2932/1.html&words=OECD%20Krypto [abgerufen am: 14.1.2000].

- Die Verantwortlichkeit derjenigen, die Krypto-Dienste anbieten oder Schlüssel verwalten, soll entweder durch Vertrag oder Gesetz, jedenfalls aber klar festgelegt sein.
- Vor allem aber sollten im Namen der Kryptopolitik schwerwiegende, ungerechtfertigte Handelshemmnisse vermieden werden.

5.4.3 Wassenaar Agreement

Nachdem am 16.11.1993 das COCOM[50] (Coordinating Committee for Multilateral Export Controls), welches es sich zur Aufgabe gemachte hatte den Export von gewissen Technologien in kommunistische Staaten zu kontrollieren, seine Selbstauflösung beschloss und damit auf den Fall des Warschauer Paktes und der Soviet Union reagierte, trat an deren Stelle das Wassenaar Agreement (WA)[51].

Seit der formellen „Gründung" des WA am 19. Dezember 1994 traten dem Abkommen bislang 33[52] Industriestaaten bei - mit der Intention, den Export von Conventional Weapons und Dual Use Gütern in gefährliche und vor allem kriegsführende Länder zu beschränken. Unter die sogenannten Dual Use Güter fallen all jene Güter, die sowohl für kommerzielle als auch militärische Zwecke verwendet werden können; angesprochen sind hier etwa Computer mit extrem hoher Rechnerleistung oder Verschlüsselungsprogramme mit außergewöhnlich hoher Dechiffrierungssicherheit. In acht Kategorien wurden diese doppelverwendungsfähigen Güter unterteilt, wobei vor allem Kategorie fünf - „Information Security" - aufgrund der divergierenden Ansichten bezüglich der Kryptographiepolitik stark kritisiert wurde.
Beitrittsbeschränkungen zum WA bestehen nicht. Beitrittswerber müssen lediglich gewisse Kriterien erfüllen um aufgenommen werden zu können:

Damit ein Beitritt überhaupt Sinn macht, müssen in dem betroffenen Staat Waffen oder Dual Use Güter produziert werden. Neben dieser Basisvoraussetzung, muss als politischer Grundsatz die nicht kommerzielle Weitergabe der vom WA umfassten Güter gelten. Man hat sich an internationale Verträge und Mitglieder zu halten, die eben diesen Grundsatz vertreten, um „weltweit zu verhindern, dass es durch gezielte Einkaufsstrategien zum Aufbau destabilisierender oder friedensgefährdender Rüstungskapazitäten kommt."[53]
Außerdem muss für eine effektive Export-Kontrolle gesorgt werden.

---

[50] Hortmann, M.: Kryptoregulierung weltweit – Überblick. In: DuD – Datenschutz und Datensicherheit. 1997, 21, 214.
[51] Online im Internet: Url: http://www.wassenaar.org/docs/contacts.htm [abgerufen am 15.1.2001].
[52] Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Portugal, Romania, Russian Federation, Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, and the United States.
[53] Erläuterungen zum Bundesgesetz über die Rechtsstellung des Sekretariats des Wassenaar Arrangements in Österreich. Online im Internet: Url: http://www.parlinkom.gv.at/pd/pm/XX/I/texte/007/I00702_.html [abgerufen am: 2.9.2000].

5.4.3.1 Aufnahmekriterien[54]

Wie oben erwähnt werden in gefährliche oder kriegsführende Länder keine Waffen oder Dual Use Güter exportiert. Ob ein Staat als gefährlich eingestuft wird und somit ihm gegenüber ein Ausfuhrverbot besteht, wird anhand folgender Kriterien bestimmt:

- Einschätzung des Beweggrundes:

Was ist die militärische Doktrin des Staates? Was ist der Beweggrund für die Auffüllung der Waffenbestände? Wozu könnten diese Waffen verwendet werden? Glaubt der Staat, dass die gewünschten Waffen zu seiner Selbstverteidigung nach den Grundsätzen der UNO-Charta notwendig seien? Könnte der Staat territoriale Ansprüche geltend machen?

- Regionales Gleichgewicht der Mächte und die generelle Situation in der Region:

Wie sind die Beziehungen zu den Nachbarstaaten in der Region? Gibt es territoriale Ansprüche oder Unstimmigkeiten oder den Vorwurf einer ungesetzlichen Okkupation? Gibt es ferner wirtschaftliche, ethnische, religiöse oder andere Konflikte? Ist das Waffenarsenal größer, als durch das berechtigte Streben nach Sicherheit und Selbstverteidigung legitimiert? Was wäre die Empfindung der Nachbarstaaten über die Aufrüstung des Staates? Würden auf Grund politischer, historischer, territorialer, geographischer oder logistischer Erwägungen andere Staaten, dies als direkte Drohung empfinden? Sähen sich Gegner gezwungen Gegenmaßnahmen zu treffen oder zusätzliche Kräfte zu mobilisieren?

- Politischer/wirtschaftlicher Status des Staates:

Hat der Staat internationale oder regionale Verträge zur Waffenkontrolle und -limitierung unterzeichnet oder ratifiziert? Erfüllt er diese Verträge? Nimmt er an dem UN-Register of Conventional Arms teil? Respektiert er die allgemein anerkannten Menschenrechte, die Nichtweitergabe von Atomwaffen und antiterroristische Normen und wie viel vom BIP wird für das Militär aufgewendet?

- Ausstattung:

Würde ein zusätzlicher Erwerb, entweder durch Import oder nationale Produktion, von konventionellen Waffen eine neue Leistungsfähigkeit in der Region erzeugen? Würde ein zusätzlicher Erwerb, entweder durch Import oder nationale Produktion, von konventionellen Waffen den Staat mit zusätzlicher strategischer Möglichkeit versehen?

- Manpower:

[54] Elements for objective analysis and advice concerning potentially dastabilising accumulations of conventional weapons. Online im Internet: Url: http://www.wassenaar.org/docs/criteria.html [abgerufen am 25.10.1999].

Wird die Ausrüstung selbst die Effektivität des Menschenpotentials erhöhen?

- ❖ Anschaffung von militärischer Technologie:

Würde die Anschaffung bestimmter Technologien entweder durch fühlbare oder immaterielle Möglichkeiten oder durch einheimische Entwicklung die Fähigkeiten des Militärs mit einem erheblichen technologischen Vorteil versehen? Welche Auswirkungen hätte dies auf die regionale Balance der Mächte und die gesamte regionale Situation?

- ❖ Andere Faktoren:

Würde ein zusätzliches Waffensystem, wenn durch Import erworben, ein Risiko für die Streitmächte des Exporteurs oder der Alliierten oder für Operationen der UNSC darstellen? Erhöht die Art und Weise, die für den Import zusätzlicher Waffen gebraucht wird, die Besorgnis darüber, wie die Waffen vermutlich verwendet werden?

5.4.3.2 Die Rechtspersönlichkeit des Wassenaar Agreements

Da ursprünglich das WA lediglich als Forum für Informationsaustausche dienen sollte und es weder zum Gesetz noch zu einem Staatsvertrag oder einer internationalen Organisation erhoben wurde, stellt sich die Frage nach der rechtlichen Einstufung. Bedeutend ist die Beantwortung dieser Frage vor allem in Hinblick auf potentielle Abschlüsse von Rechtsgeschäften oder Beitrittsverträgen. Da diese Problemlösung für Österreich als Land, in dem der ständige Sitz des WA ist, besonders wichtig ist, wurde das WA mittels Bundesgesetz[55] als juristische Person österreichischen Privatrechts deklariert.
Daraus ergibt sich auch, dass Beschlüsse durch innerstaatliches Recht umgesetzt werden müssen und eine direkte Geltung ausgeschlossen ist. Ebenso sind die Folgen der Nichtbeachtung aus Vorgaben des WA national zu regeln, worin auch die grundlegende Schwäche des WA liegt. Einheitliche Sanktionen verliehen dem WA wohl größere Anwendungstreue.

5.4.3.3 Die Kryptopolitik des WA

Die Ausfuhrkontrolle der Verschlüsselungsprodukte erhielt am 2. und 3. Dezember des Jahres 1998 eine entscheidende Wende. Ab diesem Zeitpunkt sollten, bei einer Gleichbehandlung von Hard- und Softwareprodukten, solche einer Kontrolle unterzogen werden, die einen 56-Bit überschreitenden Schlüssel verwenden[56]. In bestimmten Fällen ist für Massenmarktprodukte die Grenze erst bei einem 64-Bit Schlüssel festgelegt. Diese Regelung soll vorerst zwei Jahre in Geltung bleiben und dann, bei schweren Nachteilen der Wirtschaft,

[55] Rechtsstellung des Sekretariats des Wassenaar Agreements in Österreich. BGBl. I Nr. 89/1997.
[56] Public Statement of the fourth Plenary meeting in Vienna, 3.12.1998. Online im Internet. Url: http://www.wassenaar.org/docs/press_4.html [abgerufen am 20.5.2000].

überarbeitet werden oder gänzlich entfallen. Verfrüht war jedenfalls die Freude der amerikanischen Regierung, die diesen Beschluss als jene strenge Kryptopolitik ansah, die die USA vehement vertraten. Sehr deutlich heißt es aber, dass die oben genannten Verschlüsselungsprodukte einer Exportkontrolle und nicht einem Exportverbot unterworfen werden. Es würde somit der Handel im Großen und Ganzen wie bisher weiterlaufen. Jedenfalls hat man dem Key-Escrow System den Rücken zugewandt, was unter anderem vor allem auf das Hinwirken Deutschlands zurückzuführen ist und solchen Produkten nicht einmal gewisse, geringste Vorteile eingeräumt.

6 Internationale Vorgaben und Vorreiter

6.1 Die EU

6.1.1 Die Kompetenz der EU

Die Kompetenzregelungen der EU sind in zahlreichen Einzelbestimmungen der Gründungsverträge enthalten. Es gilt das Prinzip der begrenzten Einzelermächtigung. Die Befugnis die Signaturrichtlinie zu erlassen, geben die Artikel 57(2), 66, und 100a EGV. Dem Subsidiaritätsprinzip (Art 3b EGV) des Vertrags von Maastricht zufolge darf die Gemeinschaft auch nur insoweit tätig werden, „sofern und soweit die Ziele der in Betracht kommenden Maßnahmen auf Gemeinschaftsebene tatsächlich besser erreicht werden können, als auf der Ebene der Mitgliedstaaten.“[57] Im Sinne dieses Verhältnismäßigkeitsgrundsatzes erscheint die Richtlinie als geeignete Form des Rechtsinstrumentes.

6.1.2 Die Entstehung der Signaturrichtlinie

Erstmals wurde am 16. April 1997 eine Mitteilung[58] an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über eine „Europäische Initiative für den elektronischen Geschäftsverkehr” übersandt. Die Wichtigkeit dieses Vorhabens unterstrichen auch die Diskussionsergebnisse der Bonner Ministererklärung[59].

[57] Öhlinger,T.: Verfassungsrecht. WUV-Universitätsverlag, 3.Auflage, 1997, 82ff.
[58] Europäische Initiative für den elektronischen Geschäftsverkehr: Mitteilung an das Europäische Parlament, den Rat, den Wirtschaft- und Sozialausschuß der Regionen. KOM(97) 157 endg. vom 16.4.1997.
[59] Europäische Ministerkonferenz zum Thema "Globale Informationsnetze: Nutzung neuer Chancen", Bonn 6.-8.7.1997.

In einem ersten Schritt verfasste die Kommission am 8. Oktober 1997 eine Mitteilung über „Sicherheit und Vertrauen in elektronische Kommunikation - ein europäischer Rahmen für digitale Signaturen und Verschlüsselung"[60], in der sie auf die Notwendigkeit der einheitlichen Regelung auf diesem Gebiet hinwies. Am 1. Dezember 1997 forderte hierauf der Rat die Kommission auf, baldest möglich einen Entwurf vorzulegen.
Nach zahlreichen Diskussionen mit den Mitgliedstaaten und Experten der technischen Industrie wurden mehrere Punkte herausgearbeitet, die als Leitgrundsätze für die RL dienen sollten. Schließlich wurde nach zähen Verhandlungen am 13. Mai 1998 ein Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen von der Kommission gefasst. Am 16. Juni 1998 wurde der Vorschlag dem europäischen Parlament und dem Rat offiziell übermittelt. Das europäische Parlament verabschiedete am 13. Jänner 1999 in erster Lesung eine befürwortende Entschließung und machte 32 Änderungsvorschläge.

Von diesen 32 Abänderungsvorschlägen wurden 12 vollständig und 10 zum Teil oder grundsätzlich von der Kommission übernommen.
Die Änderungen dienten hauptsächlich dazu, den Wortlaut eindeutiger zu machen bzw. ihn zu vervollständigen und Hinweise darauf zu geben, auf welches Ziel die RL bis Ende 2002 überprüft werden soll.

Gründe für die Ablehnung der Vorschläge waren u.a:

- Verstoß gegen bestehende Gemeinschaftsvorschriften,
- Überflüssigkeit der Änderungen,
- Umsetzungsprobleme.

Im Speziellen verweigerte man, anstelle eines beratenden Ausschusses einen Kontaktausschuss einzusetzen und einige Konsultations- und Informationsverpflichtungen neu einzuführen, mit der Begründung, dass diese nicht den festgelegten Ausschusstypen aus dem Beschluss 87/373/EWG vom 13. Juli entsprächen. Weiters billigte man dem Parlament keinen Vorschlag für Mandate zur Aushandlung bilateraler und multilateraler Abkommen zu, da dies ausschließlich dem Rat vorbehalten sei und anderenfalls dem Art. 113 des EG-Vertrages widersprechen würde.
Da an der Verabschiedung dieses Entwurfes niemand mehr zweifelte, konnte das österreichische Signaturgesetz bereits vor diesem Zeitpunkt als EU–konform beschlossen werden.

Dabei stellt sich die Frage, warum die Diskussionen um diese RL so lange andauerten.
Die Gründe dafür liegen hauptsächlich in den Uneinstimmigkeiten, die Verschlüsselungsregelungen betreffend.
Vor allem Frankreich, das für ein Verbot starker Verschlüsselungsprogramme eintrat, behinderte das Vorankommen. Die Ansicht, dass gesetzliche Regelungen den Handel nur hemmen würden, wurde von Großbritannien, den Niederlanden, Finnland und Schweden vertreten. Weiters führten die unterschiedlichen Vorstellungen über die nötigen Sicherheitsstandards zu Verzögerungen. Deutschland trat hierbei für klare Regelungen ein,

[60] Europäische Initiative für den elektronischen Geschäftsverkehr: Mitteilung an das Europäische Parlament, den Rat, den Wirtschaft- und Sozialausschuß der Regionen. KOM(97) 503 endg. vom 8.10.1997.

was vor allem von Großbritannien, den Niederlanden, Finnland und Schweden mit dem Argument, dass zu stark determinierte Regelungen ebenfalls den Online-Handel behindern würden, kritisiert wurde[61].

Vom Ratsvorsitzenden Österreich wurde schließlich ein Kompromiss vorgeschlagen, in dem sowohl Sicherheit durch Haftung (angelsächsischer Ansatz), als auch durch hohe Sicherheitsstandards (zentraleuropäischer Ansatz) verwirklicht wurde. Jedoch scheiterte auch dieser auf Grund von Einwänden Großbritanniens.

Mitte des Jahres einigte man sich endlich auf einen Entwurf und am 13. Dezember 1999 wurde die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen verabschiedet.

6.1.3 Inhaltsverzeichnis der Richtlinie

Die RL besteht aus 15 Artikeln und 4 Anhängen:

Artikel 1: Anwendungsbereich
Artikel 2: Begriffsbestimmungen
Artikel 3: Marktzugang
Artikel 4: Binnenmarktgrundsätze
Artikel 5: Rechtswirkungen elektronischer Signaturen
Artikel 6: Haftung
Artikel 7: Internationale Aspekte
Artikel 8: Datenschutz
Artikel 9: Ausschuss
Artikel 10: Aufgaben des Ausschusses
Artikel 11: Notifizierung
Artikel 12: Überprüfung
Artikel 13: Durchführung
Artikel 14: Inkrafttreten
Artikel 15: Adressaten

Anhang I: Anforderungen an qualifizierte Zertifikate
Anhang II: Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen
Anhang III: Anforderungen an sichere Signaturerstellungseinheiten
Anhang IV: Empfehlungen für die sichere Signaturprüfung

6.1.4 Kritik an der Richtlinie

[61] vgl. Schultzki-Haddouti, C.: Markt- oder Staatsmacht - Streit um digitale Signaturen. Online im Internet: URL: http://www.heise.de/ct/99/01/058/ [abgerufen am 26.10.1999].

Kritik an der Richtlinie wurde vor allem auf Grund fehlender Definitionen von Fachausdrücken geübt. So merkte beispielsweise der Bundesverband freier Berufe Deutschlands[62] in der Stellungnahme zum Entwurf einer EU-Richtlinie für elektronischen Signaturen an, dass es unklar ist, „um welchen Tatbestand es sich bei der elektronischen Signatur im Unterschied zur digitalen Signatur handelt. ... Vielmehr sollte die Definition in Art. 2 Ziff. 1 des Entwurfs durch eine präzise Definition der digitalen Signatur auf der Grundlage asymmetrischer Kryptoverfahren ersetzt werden".
Auch eine Definition der Zertifizierungsdienste, des einfachen im Gegensatz zum qualifizierten Zertifikats und der Rechtsgültigkeit wurde vermisst.
Nur intern agierende geschlossene Benutzergruppen, die bereits heute ihre elektronische Kommunikation autonom organisieren können, sollten, da sie keiner Unterstützung zur Herstellung der Interoperabilität und der rechtlichen Verbindlichkeit bedürfen, nicht unter den Anwendungsbereich der RL fallen.

Außerdem merkte man an: „Bei Rechtsbeziehungen, die bisher keiner Formbindung unterlagen, besteht ebenfalls kein Anlass, sie zwingend dem Anwendungsbereich der Richtlinie zu unterwerfen". Vielmehr sollte darauf geachtet werden, dass die EU nicht in originäre Kompetenzen der Mitgliedstaaten eingreift. Es fällt auch auf, dass die Richtlinie von der Vernachlässigung vorsorgender Sicherheitsanforderungen und der starken Betonung von Haftungsregeln geprägt ist. Das ist nicht zuletzt aus finanziellen Überlegungen abzulehnen, da wohl bekannt ist, dass ein staatliches Vorsorgeangebot fünf bis sieben Mal geringere Kosten verursacht als Rechtssysteme, die auf nachträglicher Rechtsverfolgung basieren. Eben dieser Haftungsbereich sollte von den nationalen Gesetzgebern eigenständig geregelt werden, um einen Widerspruch mit derzeit bestehenden Normen zu vermeiden. Es wird daher vorgeschlagen, den Art 6(1) der RL zu streichen".
Nebenbei wurde es der europäischen Gemeinschaft auch mehrfach unterstellt, eine versteckte Harmonisierung des allgemeinen Zivilrechts mittels der Signatur-RL zu versuchen.

MA ist es auf dem Gebiet des Cyberlaw ungleich schwieriger, vorsorgende Maßnahmen zu treffen, als auf weniger dynamischen. Es ist beinahe unmöglich die technische Entwicklung länger als ein Jahr vorauszusehen. Fast täglich hört man von bahnbrechenden Innovationen jeglicher Art, die leider oftmals nicht nur von Kriminellen verwendet, sondern sogar von diesen kreiert werden.
Deshalb erscheint es mir als sehr sinnvoll, präzise Haftungsregeln zu schaffen, um die ständige Kontrolle der technischen Einrichtungen durch die Verantwortlichen zu gewährleisten. Leider sind diese Vorkehrungen sowohl in der Richtlinie als auch im österreichischen SigG nur mangelhaft verwirklicht worden. (Näheres unter 6.1.5)

6.1.5 Kritik an der Umsetzung der Richtlinie in nationales Recht

Dadurch, dass die Richtlinie den nationalen Gesetzgebern recht detaillierte Vorgaben stellt, bleibt ohnehin nur ein geringer Spielraum die RL an nationale Rechtseigenheiten anzupassen. Doch auch jene geringen Freiheiten wurden von Österreich nicht genutzt.

[62] Stellungnahme des Bundesverbands der freien Berufe. Online im Internet: E-Mail von Michael Leistenschneider <info@leistenschneider.de>[abgerufen am: 10.7.1999].

Angesprochen hierbei sei vor allem die Umsetzung der Haftungsfragen, die nach der RL im Großen und Ganzen zur nationalen Disposition gestellt wurden, um nicht ausweglose Probleme aufgrund der sehr unterschiedlichen Haftungssysteme, auch innerhalb Europas, zu schaffen. Von der EU wurden im Art 6 der RL Mindestanforderungen für Haftungsregeln normiert, welche auch ausdrücklich als Mindestanforderungen betitelt wurden. Nur verkannte man in Österreich die Notwendigkeit, „Mindestanforderungen“ im ausreichenden Maße zu vervollständigen, um nicht auf - schon im vorhinein prognostizierte Haftungsprobleme - zu stoßen. So ist etwa nicht geklärt, ob auch immaterielle Schäden oder Folgeschäden zu ersetzen sind.

Auch wich man insofern von der RL ab, als man nur natürlichen und nicht auch juristischen Personen Zertifikate ausstellen wird. Als Begründung wurde angeführt, dass jede juristische Person durch ihre Organwalter, somit durch natürliche Personen, tätig wird und es deshalb nicht nötig sei, für juristische Personen eigene Zertifikate auszustellen. Auch im Hinblick auf die Sicherheit der Identität des Gegenübers erscheint es als zweckdienlicher, Zertifikate nur natürlichen Personen auszustellen. Um aber Nachteile im Geschäftsleben auszuschließen, wird die Möglichkeit der Eintragung gewisser Vertretungsrechte oder anderer rechtlich relevanter Eigenschaften vorgesehen.

6.2 Die Unicitral

Die UNICITRAL (United Nations Commission on International Trade Law) verfasste im Juni 1996 ein Modellgesetz zum e-Commerce[63], in dem auch Regelungen über die Verwendung der digitalen Signaturen enthalten waren. Verstreut in mehreren Artikeln enthielt dieses Model Law Regelungen, wie sie aus dem SigG bekannt sind.

Wie zum Beispiel Art 7, welcher Regelungen über die Ersetzung von gesetzlich vorgeschriebenen handschriftlichen Unterschriften durch elektronische enthält. In Art 6 ist die Ersetzung der Erfordernis von schriftlichen durch elektronische Dokumente geregelt. Art 8 bestimmt, wann ein elektronisches Dokument als unverfälscht anzusehen ist (ohne jedoch auf die digitale Signatur einzugehen) und Art 9 trifft Aussagen über den Beweiswert elektronischer Dokumente vor Gericht.

In Anlehnung an dieses Modellgesetz setzte die UNICITRAL eine Working Group on Electronic Commerce ein um die weitere Entwicklung der digitalen Signaturen zu verfolgen. Die Ergebnisse deren Arbeit wurden in Meetings im Februar 1997[64] diskutiert und im Jänner 1998[65] in einem Report and Consultation Paper präsentiert. Der Inhalt umfaßte “the Legal Basis Supporting Certification Processes, including Emerging Digital Authentication and Certification Technology, the applicability of the certification process, the allocation of risk and liabilities of users, providers and third parties in the context of the use of certification

[63] Unicitral Model Law on electronic Commerce with Guide to Enactment. Online im Internet: Url: http://www.uncitral.org/en-index.htm [abgerufen am: 31.8.2000].
[64] Working Group on Electronic Commerce: Planning of future work on electronic commerce: Digital signatures, certification authorities and related legal issues. A/CN.9/WG.IV/WP.71, 31.12.1996.
[65] A/CN.9/WG.IV/WP.73, 12.12.1997.

techniques, the specific issues of certification through the use of registries and incorporation by reference“[66].

Zu dieser Zeit wurden von einigen nationalen Gesetzgebern bereits Signaturgesetze diskutiert oder waren bereits in Geltung. Diese waren aber nicht einheitlich und verursachten somit gerade beim grenzüberschreitenden Geschäftsverkehr Probleme. Ziel der Working Group war es, auf diese bis hierhin diskutierten Ansätze aufzubauen und ein Modellgesetz oder zumindest gewisse allgemein geltende Grundsätze zu schaffen.
Hervorzustreichen sind vor allem gewisse wegweisende Beschlüsse wie die Definition der sicheren elektronischen Signatur oder der Nichtdiskriminierungsklausel, woran sich auch die EU-Richtlinie hielt.

Aus den Ergebnissen der Diskussion folgender Punkte konnten die Gemeinschaften und die nationalen Gesetzgeber aufbauen:
Es stellte sich die Frage, ob die Signaturgesetze technisch neutral sein sollten oder Systeme vorschreiben, von denen man wusste, dass sie den gewünschte Erfolg bringen können. Weiters diskutierte man, ob die vorgeschlagenen, einheitlichen Gesetze auch in geschlossenen Systemen und gemäß privaten Vereinbarungen gelten sollten, oder ob sie zumindest nur nicht weniger gelten sollten als in den allgemeinen Gesetzen geregelt, was genaugenommen nur den Charakter der einfachen Signaturen regelt. Auch die Beziehung zwischen den Service Providern, den Usern und Third Parties wurde besprochen. Ebenso stellte sich die Frage, ob man die Service Provider reglementieren sollte oder auf freier marktwirtschaftlicher Basis agieren lassen sollte. Es wurden Legaldefinitionen vorgeschlagen, von denen viele auf Grund zu genauer, technischer Einzelheiten kritisiert wurden.

Auf vielen Gebieten konnte bis hierhin keine Übereinstimmung gefunden werden, aber es sollte ein Meeting im Juni 1998[67] und eines im Februar 1999[68] stattfinden. Schließlich fand im September 1999[69] das bisher letzte Treffen der Working Group in Wien statt. Dabei wurden der Kommission die Ergebnisse der Diskussionen der Working group on Electronic Commerce unterbreitet. Auch wenn auf anderen Diskussionsgebieten des e-Commerce immer noch keine festen Beschlüsse getroffen wurden, so konnte man doch zumindest auf dem Sektor der elektronischen Signaturen Erfolge verbuchen. Es erschien jetzt durchführbar, gemeinsame, harmonisierte Regelungen auf diesem Gebiet zu erlassen. Es war nicht das Ziel des Model-Law, sich mit Aspekten nationaler Politik oder den Einflüssen auf das Straf- oder Zivilrecht zu befassen, vielmehr wurde ein Fundament vorbereitet, durch dessen Einhaltung eine internationale Harmonisierung auf diesem Gebiet erreicht werden sollte.
Artikel 3 fordert beispielsweise die nationalen Gesetzgeber auf, technologie-neutrale Gesetze zu schaffen und nicht bestimmte Systeme auszuschließen. Artikel 6 legt die Voraussetzungen fest, unter denen die eigenhändige Unterschrift der digitalen gleichgestellt werden kann. Artikel 9 enthält die Pflichten des Signators und Artikel 13 die Anforderungen über die Anerkennung ausländischer Zertifikate und Signaturen.

[66] Online im Internet: Url: http://www.uncitral.org/en-index.htm [abgerufen am: 4.9.2000].
[67] Working Group on Electronic Commerce: Draft uniform rules on electronic signatures. A/CN.9/WG.IV/WP.76, 25.5.1998.
[68] Working Group on Electronic Commerce: Draft uniform rules on electronic signatures. A/CN.9/WG.IV/WP.79 und 80, 15.12.1998.
[69] Working Group on Electronic Commerce: Draft uniform rules on electronic signatures. A/CN.9/WG.IV/WP.82, 29.6.1999.

Bislang beinhaltet das Modellgesetz noch zahlreiche Varianten, bei denen entweder noch keine Übereinstimmung gefunden werden konnte, oder es den nationalen Gesetzgebern überlassen bleibt eine auszuwählen. Keineswegs sind bis zum heutigen Tag die Verhandlungen und Diskussionen abgeschlossen. Dennoch bot die UNICITRAL bereits ab Beginn der Arbeit der Working Group sehr brauchbare Problemaufschlüsselungen mit immer besseren Lösungen für die Erlassung eines Signaturgesetzes an.

7 Das österreichische Signaturgesetz[70]

7.1 Einleitung

Als eines der ersten seiner Art innerhalb der europäischen Gemeinschaft ist das österreichische Signaturgesetz am 1.1.2000 in Kraft getreten. Bemühungen wurden vor allem auf die frühzeitige und möglichst gemeinschaftsrechtskonforme Umsetzung der europäischen Richtlinie für elektronische Signaturen gesetzt. Neben Deutschland und Italien gab es lediglich in einzelnen Staaten der USA bereits vor diesem Zeitpunkt Gesetze, die die Anwendung von elektronischen Signaturen regelten. Nicht nur für Unternehmen und Verbraucher, die am e-Commerce teilnehmen, wird die rechtliche Anerkennung der digitalen Unterschrift Vorteile bringen, sondern auch der Verkehr mit den Behörden wird in Bezug auf Kostenaufwand und Geschwindigkeit profitieren. Die Möglichkeit der Setzung einer rechtsverbindlichen Unterschrift übers Internet ist Basisvoraussetzung für einen funktionierenden elektronischen Handel. Ohne diese rechtsverbindliche Regulierung wäre die Zukunft des weltweiten elektronischen Marktplatzes ungewiss.

7.2 Kompetenz und Quoren der Umsetzung

Wie bereits erwähnt ist das österreichische Signaturgesetz das Ergebnis der Umsetzung der „Richtlinie des europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen“.

Wer hat nun die Kompetenz zur Umsetzung innerhalb von Österreich?
Da die Verwendung und Anerkennung elektronischer Signaturen im elektronischen Geschäftsverkehr dem Zivilrechtswesen angehört, ist die Umsetzung laut Art. 10 Abs. 1 Z 6 B-VG Bundessache[71]. Auch der Zugang zur Tätigkeit als Zertifizierungsdiensteanbieter zählt zu den Angelegenheiten des Gewerbes und der Industrie, für welche gemäß Art. 10 Abs. 1 Z 8 B-VG ebenfalls Bundeszuständigkeit vorliegt. Die Kommunikation zwischen Bürgern und

[70] Signaturgesetz. BGBl. I Nr. 190/1999.
[71] Vgl. Erläuterungen zum SigG. Online im Internet: Url: http://www.parlinkom.gv.at/pd/pm/XX/I/texte/019/I01999_.html [abgerufen am 3.11.2000].

den Behörden unterliegt, soweit nicht schon im Zivilrechtswesen geregelt, dem Verwaltungsverfahren, welches bei Bedarf einheitlicher Regelungen laut Art. 11 Abs. 2 B-VG ebenso vom Bund zu regeln und zu vollziehen ist. Letztendlich wäre auch bei Eingriffen in das Post und Fernmeldewesen nach Art. 10 Abs.1 Z 9 B-VG der Bund zuständig. Somit steht die Kompetenz zur Umsetzung der RL dem Bund zu.

Ob die RL durch ein formelles Gesetz oder durch eine Rechtsverordnung umgesetzt wird, ergibt sich aus Art. 18 Abs. 2 B-VG. Da es keine hinreichende gesetzliche Grundlage zur Erlassung einer Verordnung gibt und die Richtlinie selbst nicht hinreichend determiniert ist, muss sie in Form eines Gesetzes in österreichisches Recht transformiert werden. Der Gesetzgeber hat dieser Verpflichtung innerhalb von 18 Monaten nachzukommen, widrigenfalls Entschädigungs- oder Schadenersatzpflichten auferlegt werden könnten. Ungeachtet dessen wird die RL nie unmittelbar anwendbar sein, da sie weder den Einzelnen gegenüber dem Staat begünstigt, noch hinreichend genau bestimmt ist[72].
Da durch das Signaturgesetz die Verfassung nicht geändert wird, genügt bei der Abstimmung im Ganzen die Anwesenheit von einem Drittel der Nationalratsmitglieder und die unbedingte (einfache) Mehrheit der abgegebenen Stimmen.
Tatsächlich wurde das SigG am 14.7.1999 in zweiter Lesung einstimmig angenommen.

7.3 Inhalt

7.3.1 Wichtige Eckpfeiler des Signaturgesetzes[73]

Die Grundinhalte des Signaturgesetzes, nach denen auch auftretende Unklarheiten zu interpretieren sind.

- Auf Grund der sehr raschen Entwicklung der Technik ist es nicht möglich, die Methode zur Verschlüsselung und Signierung oder ein bestimmtes Produkt gesetzlich festzulegen.

- Keine Monopolstellung einer Zertifizierungsstelle sondern frei marktwirtschaftliche Konkurrenz - bestimmt durch Angebot und Nachfrage.

- Verschiedene Zertifikatsklassen für verschiedene Sicherheitsstufen.

- Um schneller auf technische Veränderungen eingehen zu können, soll das Gesetz Grundsätze vorgeben, welche rasch - auf dem Verordnungsweg - an die veränderte Wirklichkeit angepasst werden können.

[72] Vgl. Öhlinger, T.: Verfassungsrecht. WUV Universitätsverlag, 3.Auflage, 1997, 87.
[73] Alle Paragraphen, ohne andere Angabe beziehen sich auf dieses Gesetz.

- ❖ Eine unabhängige Regulierungsbehörde soll die Zertifizierungsstellen überwachen.
- ❖ Auf die Vorgaben der EU-RL wurde geachtet; ausländische Signaturgesetze werden unter normierten Voraussetzungen anerkannt.
- ❖ Pseudonyme werden zugelassen - können und müssen aber unter bestimmten Umständen aufgedeckt werden.
- ❖ Ausschließlich natürliche Personen können Signator sein; juristische müssen hierbei durch natürliche vertreten werden (mit der einzigen Ausnahme bei Zertifikaten für Zertifizierungsdiensteanbieter).

7.3.2 Inhalt und Erläuterungen

1. Abschnitt

Gegenstand und Begriffsbestimmungen

Gegenstand und Anwendungsbereich

§ 1. (1) Dieses Bundesgesetz regelt den rechtlichen Rahmen für die Erstellung und Verwendung elektronischer Signaturen sowie für die Erbringung von Signatur- und Zertifizierungsdiensten.
(2) Dieses Bundesgesetz ist auch anzuwenden in geschlossenen Systemen, sofern deren Teilnehmer dies vereinbart haben, sowie im offenen elektronischen Verkehr mit Gerichten und anderen Behörden, sofern durch Gesetz nicht anderes bestimmt ist.

Absatz 1 steckt nach Vorgabe der Richtlinie (Näheres unter 6.1) grob den Anwendungsbereich des Signaturgesetzes ab. Ziel ist es, eine vollkommene rechtliche Anerkennung der elektronischen Signatur durch die Schaffung von rechtlichen Rahmenbedingungen sicherzustellen.

In Absatz 2 wird der Anwendungsbereich des SigG eingeschränkt. In geschlossenen Systemen (Näheres unter 3.1) ist es danach nur dann anzuwenden, haben die Teilnehmer die Geltung bestimmt. Die Anwendbarkeit kann also innerhalb der Schranken bestehender anderer Gesetze, wie etwa dem Konsumentenschutzgesetz, frei vereinbart werden. Auch nur einzelne Teile können übernommen werden. Entsprechen die der Abmachung getreuen Signaturen den Anforderungen der Richtlinie, müssen aber auch diese rechtlich anerkannt werden.

Entscheidend ist weiters, dass ausdrücklich darauf hingewiesen wird, dass das SigG generell auch im öffentlichen Bereich gelten soll. Erwägungsgrund dessen ist es, in naher bis

mittelfristiger Zukunft das e-Governement voll funktionsfähig zu machen. Diese Zulassung geht aber jedenfalls nicht mit der Pflicht der Bereitstellung der technischen Infrastruktur einher.

Der Verkehr mit den Behörden kann aber gewissen Einschränkungen unterworfen werden, worauf allerdings nur in Ausnahmefällen zurückgegriffen werden sollte. (vgl. die §§ 13 AVG und 89a ff GOG). Im Großen und Ganzen ist der Ausschuss auch der Meinung, dass die bestehenden Anforderungen an die sichere elektronische Signatur auch für die Verwendung im öffentlichen Bereich ausreichen sollten[74].

Der Passus „im ... Verkehr mit Gerichten und anderen Behörden" wurde in der Richtlinie mit „öffentlicher Bereich" umschrieben, was zu Auslegungsproblemen führen könnte, was nun in diesen Bereich fällt und was nicht mehr. Die Geltung wird aber jedenfalls neben dem hoheitlichen Bereich auch für die Privatwirtschaftsverwaltung, Beliehene und Selbstverwaltungskörper anzunehmen sein[75].

2. Abschnitt

Rechtserheblichkeit elektronischer Signaturen

Allgemeine Rechtswirkungen

§ 3. (1) Im Rechts- und Geschäftsverkehr können Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen verwendet werden.
(2) Die rechtliche Wirksamkeit einer elektronischen Signatur und deren Verwendung als Beweismittel können nicht allein deshalb ausgeschlossen werden, weil die elektronische Signatur nur in elektronischer Form vorliegt, weil sie nicht auf einem qualifizierten Zertifikat oder nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder weil sie nicht unter Verwendung von technischen Komponenten und Verfahren im Sinne des § 18 erstellt wurde.

Absatz 1 normiert, dass jede mögliche Art von Signaturverfahren zugelassen werden muss, woraus man aber nicht schließen darf, dass auch alle in der selben Intensität behandelt wurden. Man kann vielmehr von einem zweigliedrigen System sprechen, bei dem sich die einfache, wenig geregelte, und die sichere, detailliert behandelte, gegenüberstehen. Wann eine sichere Signatur zu verwenden ist um bestimmte Rechtsfolgen herbeiführen zu können, ist einerseits in anderen Normen, wie etwa dem § 3 normiert und andererseits von Parteienvereinbarungen abhängig. Von der Möglichkeit, verschiedene Klassen anzubieten, haben im übrigen alle vier[76] der momentan der Telekom Control GmbH gemeldeten Zertifizierungsdiensteanbieter Gebrauch gemacht. So bietet die Datakom[77] beispielsweise vier verschiedene Klassen (Light, Medium, Strong und Premium) an.

---

[74] Vgl. Brenn, C.: Signaturgesetz. Manzsche Gesetzesausgaben, Sonderausgabe Nr.101, 1999, 51.
[75] Vgl. Brenn, C.: Signaturgesetz. Manzsche Gesetzesausgaben, Sonderausgabe Nr.101, 1999, 51.
[76] Ea Generali, Datakom Austria, Arge Daten und Crypto Consult.
[77] Online im Internet: Url: http://www.a-sign.datakom.at/ [abgerufen am 3.11.2000].

Weiters liegt dem § 3 Abs. 1 der Grundsatz der Technologieneutralität zu Grunde, welcher für Auslegung oder Interpretation zweifelhafter Bestimmungen von Wichtigkeit sein wird. Dieser Grundsatz wird jedoch wenig restriktiv ausgelegt: so spricht das SigG in häufigen Fällen von der digitalen Signatur, die auf der asymmetrischen Verschlüsselung basiert und somit die Technologieneutralität vermissen lässt. Richtigerweise müsste durchgehend der Ausdruck „elektronische Signatur“ verwendet werden, wenn auch zum momentanen Stand der Technik die Verwendung der digitalen Signatur vermutet wird.

Ein weiterer Grundsatz, normiert in Absatz 2, betrifft die Nichtdiskriminierung jeglicher Art von Signaturen. Diese Klausel ist weiter gefasst als Absatz 1 und gebietet nicht nur die Freiheit, verschiedenste Verfahren anzubieten, sondern untersagt es auch, einfache Signaturen im rechtsgeschäftlichen Verkehr zu verbieten oder nur deshalb als rechtlich unbeachtlich zu qualifizieren, weil sie in elektronischer Form vorliegen. Im behördlichen und gerichtlichen Verfahren müssen elektronisch signierte Dokumente als Beweismittel anerkannt werden. Der Grundsatz der freien Beweiswürdigung bleibt natürlich davon unberührt. Festgestellt wird lediglich, dass signierte Dokumente einer Prüfung unterworfen werden müssen, sprechen keine anderen Gründe dagegen als die elektronische Form.
Dennoch müssen auch einfache Signaturen bestimmten Mindestanforderungen genügen, um die Rechtswirkungen des § 3 Abs. 2 auszulösen. Verpflichtend dafür ist etwa die Möglichkeit der Feststellung der Identität des Signators.

Besondere Rechtswirkungen

§ 4. (1) Eine sichere elektronische Signatur erfüllt das rechtliche Erfordernis einer eigenhändigen Unterschrift, insbesondere der Schriftlichkeit im Sinne des § 886 ABGB, sofern durch Gesetz oder Parteienvereinbarung nicht anderes bestimmt ist.
(2) Eine sichere elektronische Signatur entfaltet nicht die
Rechtswirkungen der Schriftlichkeit im Sinne des § 886 ABGB bei
1. Rechtsgeschäften des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind,
2. anderen Willenserklärungen oder Rechtsgeschäften, die zu ihrer Wirksamkeit an die Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts gebunden sind,
3. Willenserklärungen, Rechtsgeschäften oder Eingaben, die zu ihrer Eintragung in das Grundbuch, das Firmenbuch oder ein anderes öffentliches Register einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts bedürfen, und
4. einer Bürgschaftserklärung (§ 1346 Abs. 2 ABGB).
(3) Die Bestimmung des § 294 ZPO über die Vermutung der Echtheit des Inhalts einer unterschriebenen Privaturkunde ist auf elektronische Dokumente, die mit einer sicheren elektronischen Signatur versehen sind, anzuwenden.
(4) Die Rechtswirkungen der Abs. 1 und 3 treten nicht ein, wenn nachgewiesen wird, daß die Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen nicht eingehalten oder die zur Einhaltung dieser Sicherheitsanforderungen getroffenen Vorkehrungen kompromittiert wurden.

§ 4 stellt das Herzstück des Signaturgesetzes dar.
Absatz 1 normiert, dass durch eine sichere elektronische Signatur generell das Schriftlichkeitserfordernis einer eigenhändigen Unterschrift erfüllt wird. Dies jedoch nur unter der Voraussetzung, dass nichts anderes vereinbart wurde, und unter Bedacht der Ausnahmen des Absatz 2.
Absatz 1 stellt demnach dispositives Recht dar, kann somit durch Parteienvereinbarung abgeändert werden – das allerdings nur in Bezug auf die Einschränkung der Regelungen. Eine Ausdehnung der Gültigkeit der sicheren Signatur auf die Ausnahmefälle des Absatz 2 kann nicht erzielt werden.

Hinzuweisen ist darauf, dass durch die Nichteinhaltung von Formerfordernissen nach dem allgemeinen bürgerlichen Gesetzbuch ein Vertrag nicht wirksam ist, jedoch eine Naturalobligation entsteht und der Mangel durch Erfüllung geheilt wird. Ist dies der Fall, hat der Leistende keinerlei Anspruch auf Schadenersatz gegenüber dem Empfänger, was dem Sinn des SigG zuwiderläuft und von der Lehre auch teilweise kritisiert wird[78].
Die Gleichstellung der Rechtswirkungen elektronischer und eigenhändiger Unterschriften soll sowohl für den zivilrechtlichen als auch den verwaltungsrechtlichen Bereich gelten.
Obwohl das österreichische Zivilrecht vom Grundsatz der Formfreiheit ausgeht, ist Absatz 1 dennoch nicht wegzudenken, sind doch einige Ausnahmen und Einschränkungen aus Gründen der Beweissicherung, der Warnung oder der Identitätsfeststellung normiert.
Aus ähnlichen Gesichtspunkten enthält auch das SigG Ausnahmen von der Gleichstellung mit eigenhändigen Unterschriften.

Bevor spezifisch auf die einzelnen Regelungen eingegangen wird, ist zu erwähnen, dass die Richtlinie in Art 9 Abs. 2 einen Ausnahmenkatalog enthält, auf den bei der Umsetzung Bedacht genommen werden soll. Es bleibt zwar den nationalen Gesetzgebern die Entscheidung, in welchen Bereichen die elektronische Form zugelassen wird, selbst überlassen, im Sinne der Richtlinie über den elektronischen Rechtsverkehr im Binnenmarkt[79] sollte aber ein möglichst breites Anwendungsfeld vorgesehen werden. Man spricht in diesem Zusammenhang auch von der „Ermöglichungsklausel“.

Absatz 2 enthält in vier Ziffern Ausnahmen, wann die elektronische Unterschrift der eigenhändigen nicht gleichgestellt wird. Es ist somit zwischen Papierform und Schriftform zu unterscheiden.
Ziffer 1 nimmt Rechtsgeschäfte des Familien- und Erbrechts aus, die an die Schriftform oder an ein strengeres Formerfordernis gebunden sind. Grund dafür ist, dass in diesem Bereich häufig vermögensrechtliche Belange besonders schutzbedürftiger Personen betroffen sind und der Beweis dabei oft nur schwer erbracht werden kann.

Ziffer 2 bestimmt, dass durch elektronische Signaturen - also auch durch sichere - lediglich dem Gebot der einfachen Schriftform entsprochen werden kann. Rechtsgeschäften, die zu ihrer Wirksamkeit die „öffentliche Form“ benötigen, bleibt der elektronische Abschluss verwehrt. Dies gilt vor allem für notariatspflichtige Rechtsgeschäfte, wie Kauf- oder Tauschverträge und Ehepakte. Ebenso bei Rechtsgeschäften (Ziffer 3), deren Wirksamkeit an die Eintragung in bestimmte Register gebunden ist.

[78] Vgl. Brenn, C.: Signaturgesetz. Manzsche Gesetzesausgaben, Sonderausgabe Nr.101, 1999, 72.
[79] Abl Nr C 30 vom 5.2.1999 S 4

Ziffern 1-3 entsprechen im großen und ganzen den europäischen Vorgaben (Näheres unter 8.2), wenn auch der Wortlaut der Richtlinie in manchen Punkten ein breiteres Spektrum an Ausnahmen vorgesehen hat. Im Hinblick auf die Ermöglichungsklausel ist die engere Fassung der Ziffern 1-3 aber durchaus richtlinienkonform.

In Ziffer 4 ist hingegen eine Ausnahme normiert, die in der Richtlinie nicht vorgesehen ist. Darin heißt es, dass Bürgschaftserklärungen eines Nichtkaufmanns nicht elektronisch abgegeben werden können. Im „Offline-Leben" wird zwar die einfache Schriftform für derartige Erklärungen als ausreichend empfunden, über das Internet aber - meint der Gesetzgeber - würden die Gefahren dem Erklärenden nicht deutlich genug vor Augen geführt werden. Eine sachliche Rechtfertigung wegen des beträchtlichen Risikos, das in der Regel mit Bürgschaften verbunden ist, sei daher gegeben.
Ein anderer Grund für den Bestand der Ziffer 4 mag wohl auch sein, dass in Österreich seit langem diskutiert wird, ob man die Bürgschaftserklärung notariatspflichtig machen soll. Mit der Ziffer 4 ist man einen ersten Schritt in Richtung der Bejahung dieser Frage gegangen.

Absatz 3 regelt den Beweiswert einer sicheren elektronischen Signatur. Näheres unter 7.4.4

Absatz 4 enthält die Sicherheitsvermutung, der zufolge elektronische Signaturen, die den Anforderungen des § 18 Abs. 5 entsprechen, als sicher angesehen werden können. Der Gegenbeweis ist zulässig und etwa dann zielführend, wenn Sicherheitsanforderungen im konkreten Fall vernachlässigt wurden oder der private Schlüssel ausgespäht wurde.

3. Abschnitt

Zertifizierungsdiensteanbieter

Tätigkeit der Zertifizierungsdiensteanbieter

§ 6. (1) Die Aufnahme und die Ausübung der Tätigkeit eines Zertifizierungsdiensteanbieters bedürfen keiner gesonderten Genehmigung.
(2) Ein Zertifizierungsdiensteanbieter hat die Aufnahme seiner Tätigkeit unverzüglich der Aufsichtsstelle (§ 13) anzuzeigen. Er hat der Aufsichtsstelle spätestens mit Aufnahme der Tätigkeit oder bei Änderung seiner Dienste ein Sicherheitskonzept sowie ein Zertifizierungskonzept für jeden von ihm angebotenen Signatur- und Zertifizierungsdienst samt den verwendeten technischen Komponenten und Verfahren vorzulegen.
.
.
.

Absatz 1 normiert das Verbot, durch spezifische Genehmigungen den Marktzugang der Zertifizierungsdiensteanbieter zu erschweren oder zu verhindern. Neben direkt darauf gerichteter Bestimmungen sind aber auch Maßnahmen gleicher Wirkung, wie ein Konzessionssystem oder Lizenzierungspflichten, untersagt. Andere generelle, für alle Unternehmen vorgesehene Genehmigungen, wie insbesondere in der Gewerbeordnung zu finden, bleiben von dieser Regelung ebenso unberührt wie das Vorsehen von Aufsichtsmaßnahmen. Es soll lediglich der freie Zugang zum Markt gesichert werden.

Kontrollen über die Einhaltung der gesetzlichen Anforderungen sind hingegen nach der Richtlinie nicht nur zulässig sondern sogar geboten. Es ist somit in jedem Mitgliedstaat ein funktionierendes Aufsichtssystem für die ansässigen Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate anbieten, einzurichten.

Um bestimmen zu können, wer oder was zu kontrollieren ist, haben die Zertifizierungsdiensteanbieter einerseits spätestens vor Aufnahme der Tätigkeit dies der Aufsichtsstelle anzuzeigen (Abs. 2) und andererseits eine Policy vorzulegen. In dieser Policy soll ein Überblick über die bereitgestellten Dienste, die Pflichten der Anwender und Anbieter, das vereinbarte Entgelt, die Zertifizierungsinfrastruktur und die Zertifizierungshierarchie enthalten sein.

Zertifizierungsdiensteanbieter für qualifizierte Zertifikate

§ 7. (1) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, hat

.
.
.

3. in qualifizierten Zertifikaten sowie für Verzeichnis- und Widerrufsdienste qualitätsgesicherte Zeitangaben (Zeitstempel) zu verwenden und jedenfalls sicherzustellen, daß der Zeitpunkt der Ausstellung und des Widerrufs eines qualifizierten Zertifikats bestimmt werden kann,

4. anhand eines amtlichen Lichtbildausweises die Identität und gegebenenfalls besondere rechtlich erhebliche Eigenschaften der Person, für die ein qualifiziertes Zertifikat ausgestellt wird, zuverlässig zu überprüfen,

.
.
.

6. über ausreichende Finanzmittel zu verfügen, um den Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen zu entsprechen, sowie Vorsorge für die Befriedigung von Schadenersatzansprüchen, etwa durch Eingehen einer Haftpflichtversicherung, zu treffen,

.
.
.

8. Vorkehrungen dafür zu treffen, daß die Signaturerstellungsdaten der Signatoren weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden können.

.
.
.

(6) Auf Ersuchen von Gerichten oder anderen Behörden hat ein Zertifizierungsdiensteanbieter die Prüfung der auf seinen qualifizierten Zertifikaten beruhenden sicheren Signaturen vorzunehmen.

Der Richtlinie entsprechend dürfen qualifizierte Zertifikate nur von solchen Anbietern bereitgestellt werden, die den Anforderungen des Anhangs II genügen. Die Umsetzung dessen erfolgte durch die Absätze 1 bis 3.

Ziffer 3 des 1. Absatzes legt dem Zertifizierungsdiensteanbieter die Pflicht auf, für einen Zeitstempel (siehe auch 3.14) zu sorgen. Ein Zeitstempel ist „eine elektronisch signierte Bescheinigung eines Zertifizierungsdiensteanbieters, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen sind.“ [80]

Zeitangaben (Datum und Uhrzeit) in qualifizierten Zertifikaten, Zertifikatsverzeichnissen oder Widerrufslisten müssen stets qualitätsgesichert sein, also den Anforderungen des § 18 entsprechen. Diese hohen Ansprüche an den Zeitstempel sind darauf zurückzuführen, dass der Zeitpunkt etwa der Sperre eines Zertifikats von Bedeutung für die Gültigkeit eines abgeschlossenen Rechtsgeschäfts ist und der Beweis vor Gericht in diesem Punkt entscheidend sein kann.

Dieser Dienst muss aber nicht notwendigerweise vom Zertifizierungsdiensteanbieter selbst erbracht werden, sondern kann auch anderen Einrichtungen übertragen werden. Geschieht das, haftet der Zertifizierungsdiensteanbieter für seine Erfüllungsgehilfen nach § 1313a ABGB.

Wichtigster Bestandteil des Zertifikats ist die Angabe der Identität des Signators. Auf diese Daten muss sich der Empfänger einer signierten Nachricht verlassen können und für deren Richtigkeit hat der Zertifizierungsdiensteanbieter einzustehen (Näheres unter 7.4.5.1). Da Name, Adresse, etc. personenbezogene Daten im Sinne des DSG darstellen, ist die Zustimmung des Betroffenen Voraussetzung für deren Veröffentlichung, ohne die ein qualifiziertes Zertifikat nicht ausgestellt werden darf.

Um die Ziffer 6 gab es im Vorstadium viele Diskussionen, weil die Meinungen, in welcher Form und in welcher Höhe die Vorsorge für die Befriedigung von Schadenersatzansprüchen getroffen werden soll, stark auseinander gingen. Grund dafür war nicht zuletzt die fehlende Erfahrung auf diesem Gebiet. Schlussendlich hat man sich darauf geeinigt, es der SigV zu überlassen dies zu regeln, um schnell auf die in der Praxis gemachten Erfahrungen reagieren zu können. Grundsätzlich ist man aber davon ausgegangen, dass der Abschluss einer Haftpflichtversicherung das geeignetste Mittel darstellen würde. Andere Sicherungsmittel, wie etwa Bankgarantien oder Bürgschaften, können aber ebenso in Betracht kommen. Jedenfalls ist man jedoch lediglich von einer Mindestversicherungssumme ausgegangen, da die Haftung der Zertifizierungsdiensteanbieter betragsmäßig nach oben hin nicht beschränkt sein sollte und somit die Zertifizierungsdiensteanbieter mir ihrem gesamten Vermögen für verschuldete Schäden aufzukommen haben.

Da es sich bei den Signaturerstellungsdaten (dem privaten Schlüssel) um sehr sensible Daten handelt, durch die, werden sie von Unbefugten missbraucht oder gefälscht, großer Schaden verursacht werden kann, ist es den Zertifizierungsdiensteanbietern verboten, diese zu speichern oder zu kopieren. Der private Schlüssel einer sicheren Signatur darf somit ausschließlich auf der Smart-Card des Signators gespeichert sein.

[80] Erläuterungen zum SigG. Online im Internet: Url: http://www.parlinkom.gv.at/pd/pm/XX/I/texte/019/I01999_.html [abgerufen am 3.11.2000].

Für die Zeit, solange elektronisch signierte Dokumente zwar als Beweismittel vor Gericht verwendet werden können, diese aber noch nicht über die nötige technische Ausstattung für die Verifikation verfügen, trägt es Abs. 4 den Zertifizierungsdiensteanbietern auf eine Signaturprüfung möglich zu machen.

Ausstellung qualifizierter Zertifikate

§ 8.
.
.
.
(4) Ein Zertifizierungsdiensteanbieter kann nach Maßgabe des Zertifizierungskonzepts auf Verlangen des Zertifikatswerbers im Zertifikat anstatt des Namens des Signators ein Pseudonym angeben. Das Pseudonym darf weder anstößig noch offensichtlich zur Verwechslung mit Namen oder Kennzeichen geeignet sein.

Der Richtlinie entsprechend müssen Zertifizierungsdiensteanbieter die Möglichkeit haben, Zertifikate unter Verwendung von Pseudonymen anzubieten. Auf diese wird in der Praxis bei Massengeschäften oder anderen geringfügigen Transaktionen zurückgegriffen werden, bei denen der Signator keine „Spur" durch das Internet hinterlassen möchte und bei denen auch der Vertragspartner (vorerst) kein besonderes Interesse daran hat, die genauen Daten des Signators zu kennen.

Die Verwendung eines Pseudonyms muss im Zertifikat ersichtlich sein und darf nicht gegen fremde Marken- oder Namensrechte verstoßen.
Die Aufklärung der wahren Identität hinter einem Pseudonym hat in Übereinstimmung mit dem § 8 Abs. 1 Z. 4 und Abs. 3 DSG zu erfolgen. Demnach sind schutzwürdige Geheimhaltungsinteressen dann nicht verletzt, wenn berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern; ferner, wenn etwa eine gesetzliche Ermächtigung oder Verpflichtung besteht, um eine gerichtlich oder verwaltungsbehördlich strafbare Handlung verfolgen zu können.

Widerruf von Zertifikaten

§ 9.
.
.
.
(2) Können die in Abs. 1 genannten Umstände nicht sofort zweifelsfrei festgestellt werden, so hat der Zertifizierungsdiensteanbieter das Zertifikat jedenfalls unverzüglich zu sperren.
(3) Die Sperre und der Widerruf müssen den Zeitpunkt enthalten, ab dem sie wirksam werden. Eine rückwirkende Sperre oder ein rückwirkender Widerruf ist unzulässig. Der Signator bzw. sein Rechtsnachfolger ist von der Sperre oder dem Widerruf unverzüglich zu verständigen.
.
.
.

Im Gegensatz zu Abs. 1, bei dem die Gründe für einen unverzüglichen Widerruf gegeben sein müssen, lässt Abs. 2 begründeten Verdacht für eine vorläufige Sperre ausreichen. Der Unterschied zwischen den beiden Vorgehensweisen ist, dass ein Widerruf eine vorzeitige Beendigung der Gültigkeit bedeutet und in der Regel nicht mehr rückgängig gemacht werden kann. Die vorläufige Sperre bedeutet hingegen nur ein vorübergehendes Aussetzen der Gültigkeit mit möglicher Widererlangung bei Unbegründetheit des Verdachts. Einzige Ausnahme der Irreversibilität eines Widerrufs ist, wenn die Telekom-Control GmbH einen Widerruf zu Unrecht anordnet und die Aufsichtsstelle diesen rückgängig macht.

Eine Sperre kann im übrigen auch deshalb kein Rückwirkung entfalten, da im entgegengesetzten Fall der Signator nach Abgabe einer signierten Erklärung selbst über die Gültigkeit entscheiden könnte[81].
Der Zeitpunkt (Datum und Uhrzeit), wann das Zertifikat widerrufen oder gesperrt wurde, ist, wie auch schon unter § 7 angedeutet, von größter Wichtigkeit. Nach diesem Zeitpunkt erstellte Signaturen sind ungültig. Als Widerrufen gilt ein Zertifikat ab Eintragung in das Widerrufsverzeichnis, was bedeutet, dass Verzögerungen zwischen Begehren des Widerrufs und dem Einsetzen der rechtlichen Wirkungen zu Lasten des Signators gehen. Für verschuldete Säumnis ist der Zertifizierungsdiensteanbieter dem Geschädigten schadenersatzpflichtig.

4. Abschnitt
Aufsicht

Aufsichtsstelle

§ 13. (1) Aufsichtsstelle ist die Telekom-Control-Kommission (§ 110 TKG). Ihr obliegt die laufende Aufsicht über die Einhaltung der Bestimmungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen.
(2) Die Aufsichtsstelle hat insbesondere
1. die Umsetzung der Angaben im Sicherheits- und im Zertifizierungskonzept zu überprüfen,

[81] Vgl. Baum, M.: Gültigkeitsmodell des SigG. In: DuD – Datenschutz und Datensicherheit, 1999, 23, 199.

2. im Fall der Bereitstellung sicherer elektronischer Signaturen die Verwendung geeigneter technischer Komponenten und Verfahren (§ 18) zu überwachen,
3. Zertifizierungsdiensteanbieter nach § 17 zu akkreditieren und
4. die organisatorische Aufsicht über Bestätigungsstellen (§ 19) durchzuführen.
(3) Die Aufsichtsstelle hat dafür Sorge zu tragen, daß ein elektronisch jederzeit allgemein zugängliches Verzeichnis der gültigen, der gesperrten und der widerrufenen Zertifikate für Zertifizierungsdiensteanbieter geführt wird. Weiters hat die Aufsichtsstelle dafür Sorge zu tragen, daß ein elektronisch jederzeit allgemein zugängliches Verzeichnis der im Inland niedergelassenen Zertifizierungsdiensteanbieter, der von ihr akkreditierten Zertifizierungsdiensteanbieter und der Drittstaatenzertifizierungsdiensteanbieter, für deren Zertifikate ein im Inland niedergelassener Zertifizierungsdiensteanbieter nach § 24 Abs. 2 Z 2 einsteht, geführt wird. Auf Antrag sind auch andere im Ausland niedergelassene Zertifizierungsdiensteanbieter in dieses Verzeichnis aufzunehmen. In das Verzeichnis der Zertifikate für Zertifizierungsdiensteanbieter sind deren qualifizierte Zertifikate für die Erbringung von Zertifizierungsdiensten einzutragen. Solche Zertifikate können auch von der Aufsichtsstelle ausgestellt werden. Die Aufsichtsstelle hat die bei ihr geführten Verzeichnisse mit ihrer sicheren elektronischen Signatur zu versehen. Das Zertifikat der Aufsichtsstelle ist im Amtsblatt zur Wiener Zeitung zu veröffentlichen.
.
.
.
(6) Die Mitglieder der Aufsichtsstelle sind gemäß Art. 20 Abs. 2 B-VG bei Ausübung ihres Amtes an keine Weisungen gebunden. Sofern gesetzlich nicht anderes bestimmt ist, hat die Aufsichtsstelle das AVG 1991 anzuwenden. Sie entscheidet in oberster Instanz. Die Anrufung des Verwaltungsgerichtshofs ist zulässig.
.
.
.

Die TCK (Telekom-Control-Kommission) ist nach § 110 TKG als eine Kollegialbehörde mit richterlichem Einschlag eingerichtet. Ihr muss mindestens ein Richter angehören, ihre Bescheide können nicht im Instanzenzug aufgehoben oder abgeändert werden und sie muss nach dem Prinzip der Kollegialität geführt werden[82]. Ohne ausdrückliche, gesetzliche Normierung wären gemäß Art 133 Z. 4 B-VG ihre Bescheide auch von der Zuständigkeit des VwGH ausgeschlossen. Durch Abs. 6 wird jedoch dem VwGH die Kompetenz zur Überprüfung der Entscheidungen übertragen.

In Abs. 2 wird beispielhaft die Tätigkeit der TCK angeführt, die vor allem in regelmäßigen Kontrollen über die Einhaltung der gesetzlichen Erfordernisse ab Antritt und während des Zertifizierungsdienstes besteht.

Der letzte Satz des Abs. 3 hat eine weit entscheidendere Bedeutung, als das auf den ersten Blick erscheinen mag. Dahinter verbirgt sich nämlich die Feststellung, dass die TCK keine „zentrale Wurzelinstanz“ sein soll.
Beim sogenannten Kettenmodell, bei dem als oberstes Glied eine zentrale Wurzelinstanz besteht, ist es für die Gültigkeit des Anwenderzertifikats notwendig, dass alle anderen übergeordneten Zertifikate (etwa die des Zertifizierungsdiensteanbieters, oder der Aufsichtsstelle) ebenfalls gültig sind. Eine Kompromittierung des privaten Schlüssels der

[82] Vgl. Öhlinger, T.: Verfassungsrecht. WUV Universitätsverlag, 3.Auflage, 1997, 256.

Aufsichtsbehörde hätte somit die Ungültigkeit aller anderen Zertifikate zur Folge[83]. Im vom öSigG vorgesehenen System bleiben in einem solchen Fall aber die untergeordneten Zertifikate unverändert bestehen – einzige Folge wäre lediglich, dass man sich kurzzeitig nicht auf Richtigkeit der von der Aufsichtsstelle geführten Verzeichnisse verlassen könnte. Das Zertifikat der TCK kann auch nicht mit gesetzlich vorgesehenen Mittel widerrufen oder gesperrt werden und auch nicht in ein anderes Verzeichnis aufgenommen werden, da es keine übergeordnete Instanz gibt. Aus diesen Gründen ist das Zertifikat der Aufsichtsstelle im Amtsblatt zur Wiener Zeitung zu veröffentlichen.

Freiwillige Akkreditierung

§ 17. (1) Zertifizierungsdiensteanbieter, die sichere elektronische Signaturverfahren bereitstellen und der Aufsichtsstelle vor der Aufnahme ihrer Tätigkeit als akkreditierte Zertifizierungsdiensteanbieter die Einhaltung der Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen nachweisen, sind auf Antrag von der Aufsichtsstelle zu akkreditieren. Akkreditierte Zertifizierungsdiensteanbieter dürfen sich mit Zustimmung der Aufsichtsstelle im Geschäftsverkehr als solche bezeichnen. Im Zusammenhang mit Signatur- und Zertifizierungsdiensten sowie mit Signaturprodukten darf diese Bezeichnung nur verwendet werden, wenn die Sicherheitsanforderungen nach § 18 erfüllt werden. Die Aufsichtsstelle hat dafür Sorge zu tragen, daß die akkreditierten Zertifizierungsdiensteanbieter in ein elektronisch jederzeit allgemein zugängliches Verzeichnis aufgenommen werden.
(2) Die freiwillige Akkreditierung eines Zertifizierungsdiensteanbieters ist in das qualifizierte Zertifikat aufzunehmen oder sonst in geeigneter Weise zugänglich zu machen.
(3) Die Aufsichtsstelle hat für die laufende Aufsicht über die von ihr akkreditierten Zertifizierungsdiensteanbieter Sorge zu tragen.

Dem Umstand entsprechend, dass keinerlei Lizenzierungs- oder Genehmigungsverfahren für Zertifizierungsdiensteanbieter vorgesehen werden dürfen, aber dennoch das Interesse der Hervorhebung besonders zuverlässiger Anbieter Relevanz hat, hat man das System der freiwilligen Akkreditierung eingeführt. Die Bescheinigung der Aufsichtstelle, dass alle gesetzlichen Sicherheits- und Qualitätsvoraussetzungen erfüllt werden, soll nicht nur beim Konsumenten Sicherheit und Vertrauen schaffen, sondern auch von den Zertifizierungsdiensteanbietern selbst für Werbe- und Marketingzwecke eingesetzt werden können – wenn sie auch nur eine zusätzliche vertrauensbildende Maßnahme ist, da ohnehin die gesetzlichen Anforderungen erfüllt sein müssen. Dass es sich um einen akkreditierten Zertifizierungsdiensteanbieter handelt, muss für den Empfänger einer signierten Erklärung erkennbar sein, also entweder ins Zertifikat aufgenommen oder auf eine andere Weise zugänglich gemacht werden.

Praktische Bedeutung wird die freiwillige Akkreditierung aber vor allem für ausländische Zertifizierungsdiensteanbieter haben, die sich damit wie inländische der Kontrolle der Aufsichtsstelle unterwerfen und ein inländisches Zertifikat ausgestellt bekommen. Außerdem

[83] Baum, M.: Gültigkeitsmodell des SigG. In: DuD – Datenschutz und Datensicherheit, 1999, 23, 200.

kann man durch die vorweggenommene Überprüfung auch die Gefahr der nachträglichen Einstellung minimieren[84].

Wollen Zertifizierungsdiensteanbieter qualifizierter Zertifikate die Vorteile der Akkreditierung nützen, müssen sie sich einer ex-ante Überprüfung unterziehen. Andere können ohne vorheriges Verfahren ihre Tätigkeit aufnehmen, haben aber danach unverzüglich ihrer Anzeigepflicht der Aufsichtsstelle gegenüber nachzukommen.

4. Abschnitt

Technische Sicherheitserfordernisse

Technische Komponenten und Verfahren für sichere Signaturen

§ 18. (1) Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer Signaturen sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar machen und die die unbefugte Verwendung von Signaturerstellungsdaten verläßlich verhindern.
(2) Die bei der Erstellung einer sicheren Signatur verwendeten technischen Komponenten und Verfahren müssen zudem sicherstellen, daß die zu signierenden Daten nicht verändert werden; sie müssen es weiters ermöglichen, daß dem Signator die zu signierenden Daten vor Auslösung des Signaturvorgangs dargestellt werden. Die Signaturerstellungsdaten dürfen mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen, sie dürfen weiters mit hinreichender Sicherheit nicht ableitbar sein; ihre Geheimhaltung muß sichergestellt sein.
(3) Bei der Erstellung und Speicherung von qualifizierten Zertifikaten sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung und Verfälschung von Zertifikaten verhindern.
(4) Für die Überprüfung von sicher signierten Daten sind solche technische Komponenten und Verfahren anzubieten, die sicherstellen, daß
1. die signierten Daten nicht verändert worden sind,
2. die Signatur zuverlässig überprüft und das Ergebnis dieser Überprüfung korrekt angezeigt wird,
3. der Überprüfer feststellen kann, auf welche Daten sich die elektronische Signatur bezieht,
4. der Überprüfer feststellen kann, welchem Signator die elektronische Signatur zugeordnet ist, wobei die Verwendung eines Pseudonyms angezeigt werden muß, und
5. daß sicherheitsrelevante Veränderungen der signierten Daten erkannt werden können.
(5) Die technischen Komponenten und Verfahren für die Erzeugung sicherer Signaturen müssen nach dem Stand der Technik hinreichend und laufend geprüft sein. Die Erfüllung der Sicherheitsanforderungen muß von einer Bestätigungsstelle (§ 19) bescheinigt sein.

In § 18 sind die sicherheitstechnischen Zielvorgaben, denen Signaturprodukte und Verfahren zu entsprechen haben, enthalten. Es muss vor allem dafür gesorgt werden, dass eine sichere Signatur nicht unbemerkt gefälscht oder signierte Daten verfälscht werden können. Dies kann

[84] Vgl. A-Sit: Fragen und Antworten zur elektronischen Signatur. Online im Internet: Url: http://www.a-sit.at/TEXTE/FAQ_Signatur/# [abgerufen am 7.1.2001].

dadurch gewährleistet werden, dass der private Schlüssel auf einer Smart-Card gespeichert wird und der Auslösevorgang durch einen Pin oder ein Passwort geschützt ist. In diesem Fall sind die signierten Daten mit an Sicherheit grenzender Wahrscheinlichkeit vor Fälschung oder Verfälschung gesichert.

Zusätzlich ist ein Prüfmechanismus zur Verfügung zu stellen, der eine Fehlermeldung bei Fälschung oder Verfälschung erfolgen lässt.
Für den Signator ist es weiters von Bedeutung, dass ihm die zu signierenden Daten in vollem Umfang vor dem Signiervorgang dargestellt werden, um sicherzugehen zu können, dass ausschließlich die gewünschten Daten - diese jedoch vollständig - signiert werden. Dies geschieht durch besondere Software mittels sogenannter Viewer-Funktion (Abs. 2).
Welche Algorithmen oder Schlüssellängen als sicher eingestuft werden können, wird in internationaler Diskussion ständig von neuem beurteilt und den Voraussetzungen der SigV zugrundegelegt.

Rechte und Pflichten der Anwender

Allgemeine Informationspflichten der Zertifizierungsdiensteanbieter

§ 20. (1) Ein Zertifizierungsdiensteanbieter hat den Zertifikatswerber vor Vertragsschließung schriftlich oder unter Verwendung eines dauerhaften Datenträgers klar und allgemein verständlich über den Inhalt des Sicherheits- und des Zertifizierungskonzepts zu unterrichten. Bei der Ausstellung eines qualifizierten Zertifikats hat der Zertifizierungsdiensteanbieter zudem die Bedingungen der Verwendung des Zertifikats, wie etwa Einschränkungen seines Anwendungsbereichs oder des Transaktionswerts, bekanntzugeben; weiters ist auf eine freiwillige Akkreditierung (§ 17) sowie auf besondere Streitbeilegungsverfahren hinzuweisen.
(2) Auf Verlangen sind die in Abs. 1 genannten Angaben auch Dritten, die ein rechtliches Interesse daran glaubhaft machen, zugänglich zu machen.
(3) Ein Zertifizierungsdiensteanbieter hat weiters den Zertifikatswerber darüber zu unterrichten, welche technischen Komponenten und Verfahren für das verwendete Signaturverfahren geeignet sind, gegebenenfalls auch darüber, welche technischen Komponenten und Verfahren sowie sonstigen Maßnahmen die Anforderungen für die Erzeugung und Prüfung sicherer Signaturen erfüllen. Ferner ist der Zertifikatswerber über die möglichen Rechtswirkungen des von ihm verwendeten Signaturverfahrens, über die Pflichten eines Signators sowie über die besondere Haftung des Zertifizierungsdiensteanbieters zu belehren. Der Zertifikatswerber ist auch darüber zu unterrichten, daß und wie gegebenenfalls eine neue elektronische Signatur anzubringen ist, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

In § 20 sind zweierlei Belehrungspflichten des Zertifizierungsdiensteanbieter gegenüber dem Signator vermerkt: Einerseits ist über das Sicherheits- und Zertifizierungskonzept und andererseits über die möglichen rechtlichen Auswirkungen der Verwendung elektronischer Signaturen zu informieren. Ziel dessen ist es, eine missbräuchliche Verwendung aufgrund von Wissensmängeln zu verhindern. Dazu ist es notwendig, dass der Signator die Informationen schriftlich oder elektronisch zugestellt bekommt und diese für ihn dauerhaft zugänglich bleiben, also ausgedruckt oder gespeichert werden können.

Abs. 2 erlaubt es den Zertifizierungsdiensteanbietern, über den Signator erhobene Informationen auch an Dritte weiterzugeben, sofern diese ein Interesse daran glaubhaft machen können. In der Regel wird das solche Fälle betreffen, in denen der Empfänger einer signierten Erklärung eine Signaturprüfung unter Heranziehung des Zertifikats vornehmen will. Zu den datenschutzrechtlichen Einschränkungen gilt das zu § 7 Gesagte.
Der Signator ist weiters über Pflichten, die Verwahrung des privaten Schlüssels betreffend, nämlich über das Geheimhalten des Pins oder des Passwortes und das sorgfältige Aufbewahren der Smart-Card zu unterrichten.

Pflichten des Signators

§ 21. Der Signator hat die Signaturerstellungsdaten sorgfältig zu verwahren, soweit zumutbar Zugriffe auf Signaturerstellungsdaten zu verhindern und deren Weitergabe zu unterlassen. Er hat den Widerruf des Zertifikats zu verlangen, wenn die Signaturerstellungsdaten abhanden kommen, wenn Anhaltspunkte für eine Kompromittierung der Signaturerstellungsdaten bestehen oder wenn sich die im Zertifikat bescheinigten Umstände geändert haben.

Zu den Pflichten des Signators und den Folgen bei Missachtung derer in Punkt 7.4.1.

Haftung der Zertifizierungsstellen

§ 23. (1) Ein Zertifizierungsdiensteanbieter, der ein Zertifikat als qualifiziertes Zertifikat ausstellt oder für ein solches Zertifikat nach § 24 Abs. 2 Z 2 einsteht, haftet gegenüber jeder Person, die auf das Zertifikat vertraut, dafür, daß
1. alle Angaben im qualifizierten Zertifikat im Zeitpunkt seiner Ausstellung richtig sind,
2. der im qualifizierten Zertifikat angegebene Signator im Zeitpunkt der Ausstellung des Zertifikats im Besitz jener Signaturerstellungsdaten ist, die den im Zertifikat angegebenen Signaturprüfdaten entsprechen,
3. die Signaturerstellungsdaten und die ihnen zugeordneten Signaturprüfdaten einander bei Verwendung der von ihm bereitgestellten oder als geeignet bezeichneten Produkte und Verfahren in komplementärer Weise entsprechen,
4. das Zertifikat bei Vorliegen der Voraussetzungen unverzüglich widerrufen wird und die Widerrufsdienste verfügbar sind sowie
5. die Anforderungen des § 7 erfüllt und für die Erzeugung und Speicherung von Signaturerstellungsdaten technische Komponenten und Verfahren nach § 18 verwendet werden.
(2) Ein Zertifizierungsdiensteanbieter, der sichere elektronische Signaturverfahren bereitstellt, haftet zudem dafür, daß für die von ihm bereitgestellten oder als geeignet bezeichneten Produkte, Verfahren und sonstigen Mittel für die Erstellung elektronischer Signaturen sowie für die Darstellung zu signierender Daten nur technische Komponenten und Verfahren nach § 18 verwendet werden.
(3) Der Zertifizierungsdiensteanbieter haftet nicht, wenn er nachweist, daß ihn und seine Leute an der Verletzung der Verpflichtungen nach Abs. 1 und 2 kein Verschulden trifft. Kann

der Geschädigte als wahrscheinlich dartun, daß die Verpflichtungen nach Abs. 1 und 2 verletzt oder die zur Einhaltung der Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen getroffenen Vorkehrungen kompromittiert wurden, so wird vermutet, daß der Schaden dadurch verursacht wurde.
(4) Enthält ein qualifiziertes Zertifikat eine Einschränkung des Anwendungsbereichs, so haftet der Zertifizierungsdiensteanbieter nicht für Schäden, die sich aus einer anderen Verwendung des Zertifikats ergeben. Enthält ein qualifiziertes Zertifikat einen bestimmten Transaktionswert, bis zu dem das Zertifikat verwendet werden darf, so haftet der Zertifizierungsdiensteanbieter nicht für Schäden, die sich aus der Überschreitung dieses Transaktionswerts ergeben.
(5) Die Haftung eines Zertifizierungsdiensteanbieters nach Abs. 1 bis 3 kann im vorhinein weder ausgeschlossen noch beschränkt werden.
(6) Bestimmungen des Allgemeinen Bürgerlichen Gesetzbuchs und anderer Rechtsvorschriften, nach denen Schäden in anderem Umfang oder von anderen Personen als nach diesem Bundesgesetz zu ersetzen sind, bleiben unberührt.

Zu den Haftungsregeln der Zertifizierungsdiensteanbieter in Punkt 7.4.3.2.

7. Abschnitt

Anerkennung ausländischer Zertifikate

Anerkennung

§ 24. (1) 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. Qualifizierte Zertifikate solcher Zertifizierungsdiensteanbieter entfalten dieselben Rechtswirkungen wie inländische qualifizierte Zertifikate.
(2) Zertifikate, die von einem in einem Drittstaat niedergelassenen Zertifizierungsdiensteanbieter ausgestellt wurden und deren Gültigkeit vom Inland aus überprüft werden kann, werden im Inland anerkannt. Qualifizierte Zertifikate werden inländischen qualifizierten Zertifikaten rechtlich gleichgestellt, wenn
1. der Zertifizierungsdiensteanbieter die Anforderungen nach § 7 erfüllt und unter einem freiwilligen Akkreditierungssystem eines Mitgliedstaates der Europäischen Union akkreditiert ist,
2. ein in der Europäischen Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen nach § 7 erfüllt, für das Zertifikat haftungsrechtlich einsteht oder
3. im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Europäischen Gemeinschaft einerseits und Drittstaaten oder internationalen Organisationen andererseits das Zertifikat als qualifiziertes Zertifikat oder der Zertifizierungsdiensteanbieter als Aussteller qualifizierter Zertifikate anerkannt ist.
.
.
.

Bei „ausländischen Zertifikaten“ ist zwischen Zertifikaten der Europäischen Gemeinschaft und solchen des EU-Auslands zu unterscheiden. Nach Abs. 1 sind erstere den inländischen immer dann gleichzustellen, kann eine ordnungsgemäße Überprüfung der Signatur vom Inland aus durchgeführt werden. Verzeichnis- oder Widerrufsdienste müssen dementsprechend, in der Regel online, von Österreich aus abgerufen werden können. Ist das der Fall, entfalten nicht nur die einfachen sondern sogar die qualifizierten Zertifikate dieselben Rechtswirkungen, wie inländische.

Qualifizierte Zertifikate des EU-Auslands müssen, da sie nicht dem einheitlichen Aufsichtssystem der Europäischen Gemeinschaft unterliegen, strengeren Anforderungen genügen, um eine Gleichstellung zu erfahren.
So ist etwa ein EU-Zertifizierungsdiensteanbieter zu finden, der für die fremden Zertifikate in gleicher Weise wie für die eigenen haftet. Diese Haftung wird und darf aber nur dann übernommen werden, wenn sichergestellt ist, dass die entsprechenden Sicherheitsstandards eingehalten werden. Weiters besteht auch die Möglichkeit sich freiwillig akkreditieren zu lassen oder durch eine bi- oder multilaterale Vereinbarung anerkannt zu werden.
Nicht so bei den einfachen Zertifikaten, die nach Abs. 2 lediglich unter der Voraussetzung, dass ihre Gültigkeit vom Inland aus überprüft werden kann, den inländischen gleichgestellt sind, also die Rechtswirkungen des § 3 Abs. 2 entfalten.

7.4 Spezielle juristische Fragenkomplexe

7.4.1 Die Funktionen der Schriftlichkeit

Um die digitale der eigenhändigen Unterschrift gleichzustellen, sind nicht nur die technischen Anforderungen des § 18 zu erfüllen, sondern auch die seit Jahrhunderten eingebürgerten, in beinahe allen Rechtssystemen anerkannten Funktionen der Unterschrift gleichermaßen durch entsprechende elektronische zu ersetzen.

Für die Identifikations-, Abschluss-, Warn- und Beweisfunktion sind somit technische Vorgänge zu schaffen, die als elektronische Äquivalente zu den herkömmlichen angesehen werden können[85].
So wird versucht, die Identifikationsfunktion dadurch zu befriedigen, dass der Empfänger einer signierten Nachricht den Namen und etwaige andere rechtlich relevante Daten des Signators über das Zertifikat beim Zertifizierungsdiensteanbieter abfragen kann. Eine unzweideutige Verbindung zwischen Zertifikat und Signator muss dafür sichergestellt sein.

Die Warn- und Abschlussfunktion wird durch spezielle Software erreicht, welche mittels der sog. Viewer Funktion dem Signator den zu signierenden Text vor dem Signieren darstellt, ihn mehrmals auf die kommende Anwendung (das Signieren) aufmerksam macht und ihn dadurch

[85]Jud, W., Högler-Pracher, R.: Die Gleichsetzung elektronischer Signaturen mit der eigenhändigen Unterschrift. In: Ecolex, 9, 1999, 610.

vor unüberlegtem und übereiltem Abschluss warnt. Wird ein Abschluss mit darauffolgendem, stattgebendem Mausklick getätigt, kann der dabei ausgedrückte Wille des Signators als vollständig und inhaltlich richtig angenommen werden[86].
Während der Diskussionsphase und vor In-Kraft-Treten des SigG wandten Konsumentenschützer mehrfach ein, dass die Warnfunktion zu gering ausgeprägt sei. Die Nutzer wären sich zu wenig über die möglichen rechtlichen Folgen eines Mausklicks bewusst. Um diese Gefahr zu minimieren, hat man die Informationspflicht der Zertifizierungsdiensteanbieter nach § 20 über mögliche Rechtswirkungen normiert.

Die Beweisfunktion ist der herkömmlichen Funktion am ähnlichsten. So wie Verträge oder Urkunden aufbewahrt werden können, können auch Protokolle oder e-Mails gespeichert werden.

MA kann an der Erfüllung der Schriftlichkeitsfunktionen durch die elektronische Unterschrift nicht gezweifelt werden. Man kann sogar davon ausgehen, dass die elektronische Form der Unterschrift mehr Informationen über den Geschäftspartner enthält und dadurch das Risiko der Fälschung noch geringer ist, als bei der handschriftlichen. Auch ist es technisch gesehen vielfach einfacher eine handschriftliche Unterschrift mittels Scanner und besonderer Hardware zu fälschen, als den privaten Schlüssel eines Signators zu kompromittieren.
Dem Argument der zu geringen Ausgestaltung der Warnfunktion ist ebenfalls nicht zuzustimmen. Jemand der sich die Mühe macht, sich eine sichere elektronische Signatur anzuschaffen und dafür mehrere Tausend Schilling pro Jahr bezahlt, hat sich in der Regel nicht nur über die möglichen Rechtsfolgen eines Mausklicks informiert, sondern sich gerade deretwegen die Signatur zugelegt. Ein ohnehin nur geringes notwendiges Maß an Verantwortungsbewusstsein kann der Informationsgesellschaft zweifellos zugemutet werden.
Außerdem gehe ich davon aus, dass in Fällen von Vertragsstreitigkeiten, die Leistung der Unterschrift weitaus seltener bestritten wird, als das Vorliegen irgendwelcher anderer Mängel behauptet wird. Auch aus diesem Grund sollten keine Bedenken gegen das elektronische Setzen einer Unterschrift bestehen.

7.4.2 Der Beweiswert einer signierten Erklärung

Gemäß § 4 Abs. 3 gilt § 294 ZPO auch für sichere elektronische Signaturen. Danach begründet eine sichere elektronische Signatur dafür vollen Beweis, dass die Erklärung von dem Unterzeichner stammt. Diese Ausdehnung der Anwendbarkeit der ZPO ist durchaus notwendig, da ohne diese Erweiterung nur Urkunden in Papierform relevant wären. Zu erwähnen ist aber, dass eben nur diese eine Norm auf die digitale Signatur anwendbar ist und nicht generell alle, die Privaturkunden behandeln[87]. So kann vor allem nicht die Echtheit der elektronischen Unterschrift vermutet werden, solange der Gegner des Beweisführers diese nicht bestritten hat – erst der Beweis der Identität wird unter der Berücksichtigung des

[86] Höhne, S.: Auswirkungen des Signaturgesetzes auf das Internet. Online im Internet: Url: http://www.iri.uni-hannover.de/seminararbeiten/ [abgerufen am 22.1.2001].
[87] Vgl. Menzel,T., Schweighofer, E.: Das österreichische Signaturgesetz. In: DuD – Datenschutz und Datensicherheit, 23, 1999, 503.

Prinzips der freien Beweiswürdigung dazu führen. Ein qualifizierte Echtheitsvermutung liegt nur in Bezug auf den Erklärungstext bzw. –inhalt vor[88].

Aufgrund mangelnder Praxiserfahrung ist in den erläuternden Bemerkungen auch ausdrücklich darauf hingewiesen worden, dass es keineswegs eine gesetzliche Vermutung dafür gibt, dass die Signatur tatsächlich vom Signator stammt[89]. Eine derartige Annahme wäre erst unter Einsatz biometrischer Verfahren denkbar. Bis dahin bleibt das nicht unerhebliche Risiko des Missbrauchs der Smart-Card oder des Knackens des Codes bestehen.
Unsicher signierte Dokumente stellen hingegen lediglich Augenscheinsobjekte dar, deren Beweiswert in der Praxis vermutlich durch einen technischen Sachverständigen festzustellen sein wird[90].

7.4.3 Die Haftungsregeln des SigG

7.4.3.1 Haftung des Users

Gemäß § 21 hat der Signator den privaten Schlüssel sorgfältig zu verwahren, fremde Zugriffe zu verhindern und die Weitergabe zu unterlassen. Sind die Signaturerstellungsdaten dennoch abhanden gekommen, liegen Hinweise auf eine Kompromittierung vor oder haben sich die im Zertifikat bescheinigten Umstände geändert, hat der Signator den Widerruf zu veranlassen.
Handelt der User nicht mit der vorgeschriebenen Sorgfalt des § 21, kann es aufgrund der Deutung dieser Norm als Schutzgesetz im Sinne des § 1311 ABGB zur Schadenersatzpflicht kommen[91]. Wird eine Schutznorm verletzt, hat dies zur Folge, dass nach der Rechtsprechung die Anforderungen an den Nachweis des Kausalzusammenhangs weniger streng sind, da die Missachtung der gebotenen Sorgfalt als ausschlaggebend für den Erfolg vermutet wird.
Zu einer Minderung, wenn nicht gar zu einem Ausschluss der Schadenersatzpflicht kann es aber dann kommen, wenn der Zertifizierungsdiensteanbieter seine Belehrungs- bzw Informationspflichten (§ 20) missachtet hat.

Handelt der Signator pflichtwidrig, hat dies dennoch keine verwaltungsstrafrechtlichen Folgen, da dieser Sachverhalt nicht in den Tatbestandskatalog des § 26 aufgenommen wurde. In der Praxis wird es dem Durchschnittsuser aber nur schwer möglich sein Kompromittierungen zu erkennen.

[88] Brenn, C.: Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet. In: ÖJZ, 17, 52. Jg, 641.
[89] Benn-Ibler, G., Held, G.: Schrift und Unterschrift – elektronisch. In: AnwBl., 1999, 732.
[90] Vgl. Mayer-Schönberger, V., Pilz, M., Reiser, C., Schmölzer, G.:Signaturgesetz. Orac, 1999, 78.
[91] Benn-Ibler, G., Held, G.: Schrift und Unterschrift – elektronisch. In: AnwBl., 1999, 732.

7.4.3.2 Haftung der Zertifizierungsdiensteanbieter

Die von der Richtlinie vorgegebenen Haftungsregeln stellen lediglich ein zu gewährleistendes Minimum dar. Es wurde nicht angestrebt, eine „verdeckte“ Harmonisierung des Haftungsrechts im Zuge der Signaturrichtlinie zu erreichen. Im österreichischen SigG wurde das mit dem Abs. 6 des § 23 verdeutlicht, nach dem ausdrücklich Schadenersatzregelungen anderer Gesetze als unberührt und ebenfalls anwendbar gelten sollen.

§ 23, in dem die Haftung der Zertifizierungsdiensteanbieter für qualifizierte Zertifikate geregelt ist, listet eine Reihe von Diensten auf, für deren Richtigkeit, Vollständigkeit und Verfügbarkeit die Zertifizierungsdiensteanbieter einzustehen haben.
Ein Schaden kann grundsätzlich bei dem Sender oder Empfänger einer signierten Nachricht, einem Dritten oder beim Zertifizierungsdiensteanbieter selbst eintreten.
Eine Haftung kann sich etwa aus folgenden Pflichtverletzungen ergeben[92]:

- Falschangaben im Zertifikat,
- Falschangaben im Verzeichnis,
- unberechtigte Preisgabe der Identität bei Pseudonymen,
- Speicherung des privaten Schlüssels,
- fehlende Veröffentlichung im Verzeichnis,
- verspätete oder unterbliebene Sperrung,
- fehlende Erreichbarkeit des Verzeichnisdienstes,
- fehlende Betragsbeschränkung.

Abs. 3 setzt die für den harmonisierten Bereich vorgesehene Verschuldenshaftung mit Umkehr der Beweislast zu Lasten des Zertifizierungsdiensteanbieters in österreichisches Recht um. Danach hat der Zertifizierungsdiensteanbieter im Schadensfall nachzuweisen, dass ihn und seine Gehilfen an der schadensbegründenden Pflichtverletzung bzw. der objektiven Sorgfaltswidrigkeit kein Verschulden trifft. Da die Absätze 1 und 2 ebenfalls Schutznormen darstellen, gilt in Bezug auf den Kausalitätsbeweis das unter 7.4.3.1. Gesagte.
Für die Normierung der Umkehr der Beweislast spricht vor allem die Nähe zum Beweis und die technische Komplexität hinter den Verfahren, deren Mangelhaftigkeitsbeweis dem Durchschnittsbürger nicht zugemutet werden kann.

Hervorzuheben ist weiters, dass die Haftung der Zertifizierungsdiensteanbieter gegenüber jedermann übernommen werden muss (Abs.2), also auch gegenüber Personen, mit denen diese nicht in einem Vertragsverhältnis stehen[93]. Dazu zählen etwa Empfänger einer signierten Nachricht, die sich gutgläubig auf gefälschte Angeben im Zertifikat verlassen haben.

Die von den Konsumentenschützern vielfach geforderte Gefährdungshaftung wurde nicht ins österreichische SigG übernommen, da sie einerseits nicht sachgerecht wäre, als auch andererseits den allgemeinen Grundsätzen über die Gefährdungshaftung widersprechen

[92] Emmert, U.: Haftung der Zertifizierungsstellen. In: Computer und Recht, 4, 1999, 245.
[93] Vgl. Menzel,T., Schweighofer, E.: Das österreichische Signaturgesetz. In: DuD – Datenschutz und Datensicherheit, 23, 1999, 507.

würde. Eine derartige Haftung kann in Analogie zu den Haftpflichtgesetzen, wie PHG oder AtomHG, nur für Personen- oder Sachschäden aus besonders gefährlichen Betrieben angenommen werden[94]. Dafür müsste das übliche Ausmaß der Gefährdung wesentlich überschritten werden und der Schadenseintritt hoch wahrscheinlich sein. All das kann aber wohl nicht für die Tätigkeit der Zertifizierungsdiensteanbieter zutreffen.

Die Haftung der Zertifizierungsdiensteanbieter kann im Vorhinein weder beschränkt noch ausgeschlossen werden (Abs.5), sehr wohl besteht aber die Möglichkeit, Einschränkungen des Anwendungsbereichs oder des Transaktionswertes festzulegen (Abs.4). Das hat zur Folge, dass für Schäden oberhalb der sachlichen und betragsmäßigen Grenze eine Haftungsbefreiung eintritt.
Nicht übersehen werden darf allerdings, dass bisher angesprochene Haftungsregeln ausschließlich für Anbieter qualifizierter Zertifikate gelten – Zertifizierungsstellen für einfache Zertifikate haften hingegen nach den allgemeinen Regeln des Schadenersatzrechts des ABGB. Dies erscheint vor allem im Hinblick auf die geringere staatliche Kontrolle und die dadurch potentiell unsichereren Zertifikate bedenklich[95].

Nach allgemeinem Schadenersatzrecht haftet der Zertifizierungsdiensteanbieter seinen Kunden gegenüber für die Verletzung vertraglich übernommener Pflichten. Dritten gegenüber kann sich eine Haftung nur auf deliktisches Verhalten, also schuldhaftes, rechtswidriges, kausales Handeln oder Unterlassen, gründen.
In beiden Fällen ist aber die Haftung lediglich eine subsidiäre, was bedeutet, dass auch bei fehlerhaftem Verhalten der Zertifizierungsdiensteanbieter nur dann auf diese zurückgegriffen wird, können nicht vorgelagerte Personen wie etwa der Aussteller in Anspruch genommen werden.

8 Kritik am SigG

Daran, dass dieses Regelungswerk wünschenswert und für den Wirtschaftsstandort Österreich unbedingt notwendig ist, besteht kein Zweifel. Dies wurde auch von keiner Seite (Presse, Verbände) bestritten, allerdings ist sowohl an dem Procedere der Entstehung als auch am Inhalt gewisse Kritik geübt worden.

8.1 Das Procedere

Als „Husch-Pfusch“ Akt wurde das SigG etwa von der Tageszeitung „Die Presse“[96] bezeichnet. Ausschließlich politische Erwägungen seien nach langer Untätigkeit des Gesetzgebers Grund für den überhasteten Gesetzgebungsablauf gewesen.

[94] Vgl. Brenn, C.: Signaturgesetz. Manzsche Gesetzesausgaben, Sonderausgabe Nr.101, 1999, 136.
[95] Vgl. Mayer-Schönberger, V., Pilz, M., Reiser, C., Schmölzer, G.:Signaturgesetz. Orac, 1999, 32.
[96]Martos, P.: Elektronische Signatur – Husch-pfusch statt sicherem e-commerce? In: Die Presse: Online Ausgabe vom 15.6.1999. Online im Internet: Url:

Italien und Deutschland haben ja bereits seit mehr als zwei Jahren entsprechende Signaturgesetze - auch in Österreich gab es schon 1998 einen privaten Experten-Entwurf, der sogar schon bei den Interessensverbänden und den Koalitionsparteien Zustimmung fand, sich allerdings dennoch im Sand verlief. Um das SigG noch vor der Sommerpause durchs Parlament zu peitschen, wurde die Thematik fast ausschließlich interministeriell diskutiert - und nicht einmal hier mit allen betroffenen Ministerien - und die Begutachtungszeit auf ein Minimum reduziert.

8.2 Inhaltliche Mängel

Da VÖI, FEEI, VIW die umfangreichste Stellungnahme abgegeben haben und sich diese mit der der anderen Institutionen teilweise überschneidet, wird der erste Punkt detailliert ausgeführt. Dann erfolgt eine Beschränkung auf die Besonderheiten.

8.2.1 Stellungnahme von VÖI, FEEI und VIW[97]

In erster Linie wurde beanstandet, dass das österreichische SigG mit den anderen nationalen Gesetzen nicht übereingestimmt wurde und dass erhebliche Abweichungen zur Richtlinie zu erkennen sind – und das, obwohl der Gesetzgeber mehrmals betonte, das erste SigG in Übereinstimmung mit der EU-Richtlinie verabschiedet zu haben.
Vor allem die Beziehung zu dem Akkreditierungsgesetz blieb ungeklärt und könnte Probleme aufwerfen. Von allen Seiten gelobt hingegen wird, dass die Zertifizierungsdiensteanbieter keinen Zugangsbeschränkungen unterworfen sein sollen.

Verfassungswidrig erscheint allerdings die Bestimmung in § 19 (3), nach der der Bundeskanzler in Form einer Verordnung auf Antrag der betreffenden Einrichtung die Eignung einer Bestätigungsstelle feststellt. „Eine Verordnung darf verfassungsgemäß nicht auf Antrag erlassen werden und eine individuelle Norm enthalten. Diese Normwirkung kommt nur dem Bescheid zu.[98]“ Deshalb dürfte eine solche Feststellung nur von der Aufsichtsstelle – in Bescheidform – getroffen werden.
Es wurde also offensichtlich eine Verordnung mit einem Bescheid verwechselt.

Der sicheren elektronischen Signatur werden zwar in Erfüllung der Richtlinie besondere Rechtswirkungen wie etwa die Anerkennung als Beweismittel zugestanden, weitergehende Rechtswirkungen wie die Gleichstellung mit einer Privaturkunde, wie im italienischen SigG,

---

http://www.diepresse.at/archiv.taf?_function=read&_UserReference=FA7DCBD31F90AF0737F48075&_id=547335 [abgerufen am 22.1.2001].

[97] Presseaussendung der Vereinigung Österreichischer Industrieller (VÖI), des Fachverbands für Elektro- und Elektronikindustrie (FEEI) und des Verbands für Informationswirtschaft (VIW). Online im Internet: E-Mail von Gerhard Wagner <gkwagner@via.at> [abgerufen am: 19.8.1999].

[98] Presseaussendung der Vereinigung Österreichischer Industrieller (VÖI), des Fachverbands für Elektro- und Elektronikindustrie (FEEI) und des Verbands für Informationswirtschaft (VIW). Online im Internet: E-Mail von Gerhard Wagner <gkwagner@via.at> [abgerufen am: 19.8.1999].

fehlen allerdings - wären aber wünschenswert gewesen. Ohne diese Gleichstellung ist der Nutzen dieses Gesetzes nur undurchsichtig erkennbar.

Bemängelt werden auch fehlende Jugend- und Konsumentenschutzbestimmungen mit Haftungsfestsetzungen für Eltern, e-Commerce- und Zertifizierungsdiensteanbieter. Vor allem nicht obligatorische Altersangaben können bei unmündigen Minderjährigen zu Problemen bei Vertragsschlüssen führen.

Diesem Punkt ist mA vollinhaltlich zuzustimmen, bedenkt man vor allem auch, dass man in näherer Zukunft die elektronische Signatur als Zugangskontrolle zu Web-Sites oder Datenbanken verwenden könnte. Internetnutzer müssten sich nicht mehr unzählige Benutzernamen mit dem zugehörigen Passwort merken, sondern könnten anhand ihres Zertifikats eindeutig identifiziert werden. Eine wirksamer Schutz Minderjähriger vor pornographischen Inhalten im Internet wäre durch eine verpflichtende Altersangabe im Zertifikat bestmöglich gewährleistet.

Geklärt sollten auch die Folgen bei Straf- oder Verwaltungsrechtsverletzungen werden. So würde der Verweis auf die strafrechtlichen Folgen bei Urkundendelikten den Vertrauensschutz erhöhen.
Auffallend ist auch, dass biometrische Erkennungsmethoden nicht erwähnt werden, woraus man schließen könnte, dass sie sogar untersagt sind.
Das österreichische SigG hätte sich wie seine Vorläufer aus Deutschland und Italien in ein Rahmengesetz einfügen sollen, um eine Begriffsdefinition für alle Gesetze einheitlich zu schaffen und nicht jene Arbeit der Rechtsprechung zu überlassen.

Eine Benachteiligung privater Bestätigungsstellen könnte durch den Verein A-Sit vermutet werden, da er ausschließlich öffentliche Stellen als Vereinsmitglieder zulässt. Wettbewerbsverzerrungen und Unvereinbarkeiten könnten die Folge sein.
Problematisch erscheint auch die Regelung über die Aufnahme von Angaben über eine Vertretungsmacht oder andere rechtlich erheblich Eigenschaften. Die Richtigkeit dieser wird vom Zertifizierungsdiensteanbieter bezeugt, jedoch nur zum Ausstellungszeitpunkt. Der Signator ist zwar gemäß § 21 dazu verpflichtet, den Widerruf seines Zertifikates zu verlangen, „wenn sich die im Zertifikat bescheinigten Umstände geändert haben“, es sollte aber auch die Veränderung des Zertifikates möglich sein sowie das Unterlassen dieser „Richtigstellungspflicht“ in den Tatbestandskatalog des §26 aufgenommen werden[99].

Kritikpunkte im Detail:

Die Kritik im Einzelnen richtet sich hauptsächlich gegen Abweichungen von der EU-Richtlinie, die vor allem in terminologischer Hinsicht vermieden werden sollten, da es andernfalls im grenzüberschreitenden Geschäftsverkehr zu Ungereimtheiten kommen könnte.

In § 2 Z. 2 wird ein Signator als eine natürliche Person beschrieben, wobei in der RL von einer „Person“ gesprochen wird, also auch eine juristische mitumfasst ist. Im Geschäftsleben an sich bringt das keine nennenswerten Probleme, da auch juristische Personen ohnehin durch ihre Organe, also natürliche Personen, tätig werden - allerdings können sehr wohl

[99] vgl. Forgó, N.: Sicher ist sicher? - Das Signaturgesetz. In: Ecolex, 9, 1999, 609.

ausländische Signatoren juristische Personen sein, worauf die Rechtsordnung gefasst sein sollte. Nicht ganz klar ist, warum die österreichische Rechtsordnung sich in diesem Punkt von den anderen europäischen unterscheiden möchte.

§ 4 enthält vier Ziffern mit Ausnahmen, bei denen sichere elektronische Signaturen nicht der eigenhändigen Unterschrift gleichgestellt werden. Ziffer 1 scheint, nach Meinung der Verbände, als einzige gerechtfertigt zu sein. Der Rest des Abs. 2 sollte der Richtlinienvorgabe entsprechend auf „Verträge, die die Mitwirkung eines Notars erfordern", eingeschränkt bleiben.

Andere[100] fügen hinzu, dass beinahe in allen Ziffern Abweichungen zu vermerken sind, jedoch nicht alle Anlass zur Kritik geben.
Bei den Rechtsgeschäften des Familien- und Erbrechts aberkennt die RL grundsätzlich aufgrund der vermögensrechtlichen Belange besonders schutzwürdiger Personen den elektronischen Abschluss. Das österreichische SigG schränkt die elektronische Form jedoch bloß auf jene Rechtsgeschäfte ein, „die an die Schriftform oder ein strengeres Erfordernis gebunden sind". Ein Grundsatz der Richtlinie ist, den Abschluss möglichst aller Verträge via Computer zuzulassen. Somit ist man mit der geringeren Einschränkung des österreichischen SigG dem Willen der Gemeinschaft noch eher gerecht geworden als bei direkter Übernahme ins nationale Recht.

Aus dem selben Grund rechtfertigt sich auch die Abweichung zur Richtlinie in der Ziffer 3 des zweiten Absatzes. Die RL ordnet zwar als Ausnahme jene Verträge an, bei denen eine Registereintragung Voraussetzung für die Wirksamkeit ist, das österreichische SigG begnügt sich jedoch damit, diese Verträge auszunehmen, die die öffentliche Form der Eintragung, also eine öffentliche Beglaubigung, eine gerichtliche oder notarielle Beurkundung oder einen Notariatsakt zur Wirksamkeit benötigen.
Eine hingegen nicht durch die RL gedeckte Ausnahme stellt die Ziffer 4 dar. Die hierin normierte Nichtzulassung von elektronischen Bürgschaftserklärungen ist der RL fremd. Verwunderlich ist diese Abweichung deshalb, weil auch nach österreichischem Recht (§ 1346 Abs. 2 ABGB) für die Verbürgung von Nicht- oder Minderkaufmännern(!) lediglich die einfache Schriftform vorgesehen ist.

Zu §5:
Da der Inhalt des Attribut-Zertifikats gleich zuverlässig wie das Zertifikat selbst zu überprüfen ist, sollte auch bei einer allfälligen Streichung des Attributes untersucht werden, ob das Zertifikat als solches weiterbestehen kann.
Eine Beschränkung des Transaktionswertes nach §5 (1) Z. 9 ist zwar zu begrüßen, da aber eine Vielzahl von Geschäften beinahe gleichzeitig abgewickelt werden kann, wird wohl eine Beschränkung pro Unterschrift nicht ausreichend sein.

Dass ein qualifiziertes Zertifikat als solches erkennbar sein soll ist gerechtfertigt. Wie allerdings eine nachträgliche Änderung technisch möglich ist, ist nicht vollständig geklärt. Ebenso muss man sich überlegen, inwieweit ein solches Attributzertifikat, das beispielsweise

[100] so Jud,W, Högler-Pracher, R.: Die Gleichsetzung elektronischer Signaturen mit der eigenhändigen Unterschrift. In: Ecolex, 9, 1999, 610.

die Zugehörigkeit zu einem bestimmten Unternehmen bescheinigt, von dem entsprechendem Inhaber auch privat verwendet werden darf. Problematisch bei Bejahung dieser Frage könnte sich vor allem auswirken, dass es dem einzelnen möglich wäre, den guten Ruf einer Firma für Privatgeschäfte zu missbrauchen und sich Vertragskonditionen zu erschleichen, die sonst nur großen, anerkannten Unternehmen zugebilligt werden würden.

In §6(2)f
könnte in Verbindung mit § 14 eine versteckte Genehmigungspflicht gesehen werden. Nicht nur die Vorlage umfangreicher Unterlagen, sondern auch die Dienstuntersagungsmöglichkeiten durch die Aufsichtsstelle des § 14(2),(3) erschweren die Aufnahme und Fortführung der Tätigkeit möglicherweise beträchtlicher als dies von der RL vorgesehen wurde.

Diesem Vorwurf ist durchaus zuzustimmen, allerdings scheint es mir keine andere Alternative zu geben. Abstriche in den Kontrollbefugnissen der Aufsichtsstelle würden möglicherweise auf Kosten der Sicherheit geben. Das fatalste für die Anwendung der digitalen Signaturen wären sicherlich Nachrichten über den Missbrauch oder die Kompromittierung der Privaten Schlüssel oder die Fälschung von Zertifikaten. Gerade diese Unsicherheiten versucht das SigG zu minimieren. Außerdem hat die Aufsichtsstelle wohl keine Interessen oder Nutzen aus einer ungerechtfertigte Nichtzulassung eines Bewerbers.

Die Anreize für die freiwillige Akkreditierung sollten etwas üppiger - vor allem in rechtlichen Besserstellungen - ausfallen, als bloß in eine Liste aufgenommen zu werden.

Zu § 19 wurde angemerkt:
Bestätigungsstellen können laut RL geeignete private und öffentliche Stellen sein. Da der Bundeskanzler seine eigenen Stellen als geeignet bestimmen kann, ist zumindest die Optik der Vertrauenswürdigkeit etwas getrübt. Es sollte hier also das Subsidiaritätsprinzip gelten und staatliche Stellen nur kontaktiert werden, wenn keine geeigneten privaten zur Verfügung stehen.

8.2.2 Stellungnahme der Arbeiterkammer

Auch die Arbeiterkammer übt harsche Kritik am neuen SigG. Ein Problem sieht die AK vor allem darin, dass es zukünftig zwei Klassen von Signaturen geben wird - "eine kaum geregelte Signatur und eine sichere Signatur. ... Erst die sichere Signatur wird qualitative Mindeststandards haben[101]". Die Konsumentenschützer fordern eine Gefährdungshaftung für die technischen Systeme bei der die Zertifizierungsdiensteanbieter unabhängig von ihrem Verschulden für den, bei der Verwendung von elektronischen Signaturen entstandenen Schaden haften. Außerdem sollen Verträge, die aus Verbraucherschutzgründen schriftlich

[101] ORF on Futurezone: Arbeiterkammer übt harte Kritik am Signaturgesetz. Online Ausgabe vom 11.6.1999. Online im Internet: Url: http://futurezone.orf.at/futurezone.orf?read=detail&id=1704&tmp=59952 [abgerufen am 13.6.1999].

abgeschlossen werden müssen, nicht der elektronischen Form zugänglich sein. Laut Karl Kollmann[102], AK-Konsumentenpolitiker, erfüllt die elektronische Unterschrift die Warnfunktion nur in unzureichendem Maße.

Sämtliche Kritikpunkte der AK sind mA ungerechtfertigt. Zum ersten bedarf die einfache Signatur keinerlei besonderer Regelungen. Diese wird nämlich hauptsächlich für die Überprüfung der Integrität der Nachricht verwendet werden. Außerdem ist aus dem Zertifikat ersichtlich, ob es sich um eine sichere Signatur handelt oder nicht – der Empfänger signierter Daten ist daher darüber informiert, wie zuverlässig die Identität des Signators überprüft wurde.

Zum zweiten wurde die Einführung der Gefährdungshaftung im Entstehungsstadium des SigG zwar diskutiert, aber wohl nie ernsthaft in Erwägung gezogen. Vergleicht man das SigG mit anderen Gesetzen, in denen eine Haftung bloß aus dem Betrieb einer Anlage normiert ist, kann die besondere Gefährlichkeit bei der Führung einer Zertifizierungsstelle nicht gesehen werden. (Näheres unter 7.4.3.2)
Zur vermeintlich mangelhaften Warnfunktion einer digitalen Erklärung und der daraus nicht resultierenden Ausdehnung der Ausnahmen auf Verbraucherverträge unter 7.4.1.

8.2.3 Stellungnahme der Rechtsanwaltskammer

Hauptkritikpunkt der Rechtsanwaltskammer ist, dass nur Zertifizierungsstellen und nicht auch die Rechtsanwälte selbst elektronische Rechtsgeschäfte beglaubigen können.
Es sei nicht einzusehen, warum private Zertifizierungsstellen vertrauenswürdiger sein sollen als Rechtsanwälte.

Weiters gibt der Umstand, dass Rechtsgeschäfte, die bisher von Notaren zu beglaubigen waren, nicht in elektronischer Form abgeschlossen werden können, Anlass zur Kritik. Die digitale Signatur stellt ja nichts anderes dar als die Verifizierung, von wem eine Erklärung stammt. Sollte also die Ausnahme in § 4 auch die bloße Beglaubigung von Unterschriften umfassen, wäre diese Regelung zu weit gefasst und widerspräche den Vorgaben der Richtlinie.

Im übrigen spricht sich die Rechtsanwaltskammer für eine Versicherungspflicht aus, welche bereits im Gesetz verpflichtend und nicht erst in der Verordnung als Möglichkeit normiert werden sollte. Auch über den Zeitpunkt des Wirksamwerdens der Sperre oder des Widerrufs eines Zertifikates wurde diskutiert und im Lauf der Verhandlungen den Forderungen nachgegeben.

Hingewiesen wurde ebenfalls auf die Gefahr der umfassenden Eingriffsrechte der Aufsichtsstelle. Um Grundrechtseingriffe zu vermeiden, wurde vorgeschlagen, den Zugriff von außen ohne das Wissen der Betroffenen jedenfalls zu untersagen.

---

[102] ORF on Futurezone: Arbeiterkammer übt harte Kritik am Signaturgesetz. Online Ausgabe vom 11.6.1999. Online im Internet: Url: http://futurezone.orf.at/futurezone.orf?read=detail&id=1704&tmp=59952 [abgerufen am 13.6.1999].

Als notwendige, noch zu behandelnde Fragenkreise wurden an dieser Stelle genannt:

- Die Rahmenbedingungen für den elektronischen Vertrag (RL über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs),
- elektronischer Rechtsverkehr mit den Behörden,
- Durchsetzbarkeit von Ansprüchen im Ausland, insbesondere in Nicht EU Staaten,
- strafrechtlicher Schutz der elektronischen Signatur und der elektronisch übermittelten Daten.

8.2.4 Stellungnahme der Industriellenvereinigung

Die Industriellenvereinigung wies gleich zu Beginn ihrer Aussendung darauf hin, dass sie es für sehr bedenklich halte, dass eine schwierige Thematik wie die des SigGes fast ausschließlich interministeriell diskutiert wurde. Die Wirtschaft erst nach beschlossenem Entwurf zu kontaktieren und dann nur eine derart kurze Begutachtungsfrist anzusetzen, sei nicht verständlich. Außerdem kritisierte man, dass das zuständige Wirtschaftsministerium weder als Verordnungsgeber eingesetzt wurde noch mit der Vollziehung des Gesetzes betraut wurde.

Inhaltlich wurde gefordert, bei Begriffsbestimmungen nicht von den Vorgaben der EU-Richtlinie abzugehen, sondern diese wortident zu übernehmen, um die Rechtssicherheit nicht zu gefährden.

Die Genehmigungsfreiheit für die Aufnahme des Zertifizierungsdienstes wurde begrüßt, jedoch sieht man in den umfangreichen Unterlagen, die vorgelegt werden müssen, und in der Vielzahl der Gründe, wann die Aufsichtstelle einem Zertifizierungsdiensteanbieter die Tätigkeit untersagen kann, erst recht wieder eine versteckte Genehmigungspflicht. Generell sei die Durchführung der Aufsicht zu undetailliert geregelt – so fehle vor allem der Hinweis, dass Zugriffe auf Daten der Zertifizierungsdiensteanbieter von außen ohne deren Wissen verboten sind. Auch sollte die Haftung der Aufsichtsstelle bei ungerechtfertigtem oder verspätetem Widerruf von Zertifikaten geregelt werden.

8.2.5 Stellungnahme des Verbands österreichischer Banken und Bankiers

Die österreichischen Banken und Bankiers kritisieren in erster Linie die Ausnahme der elektronischen Abgabe einer Bürgschaftserklärung. Das Argument des Übereilungsschutzes bzw. der besonderen Warnfunktion sei nicht stichhaltig, da Nichtkaufleute, die die Vertragskonditionen auf ihrem Monitor in Ruhe durchlesen können, sich dabei, im Vergleich zur körperlichen Anwesenheit in einer Bank, viel eher der Tragweite ihres Handelns bewusst werden.

8.2.6 Stellungnahme des Bundesministeriums für wirtschaftliche Angelegenheiten

Nach Ansicht des Wirtschaftministeriums bestehen Bedenken gegen die Erfüllung der Anforderungen, die grundsätzlich nach der europäischen Normenserie EN 45000 an nationale Akkreditierungssysteme gestellt werden. Die Telekom-Control-Kommission, die aus einem Mitglied aus dem Richterstand und aus zwei weiteren Mitgliedern, von denen eines über juristisch- ökonomische und das andere über technische Kenntnisse verfügen muss, zusammengesetzt ist, mag möglicherweise nicht über das benötigte technische Wissen verfügen. Außerdem sei für die freiwillige Akkreditierung von Zertifizierungsdiensteanbietern die Akkreditierungsstelle des BmwA zuständig. Das deshalb, weil gemäß § 1 Abs.2 AkkG das Akkreditierungsgesetz nur dann gilt, wenn in Materiengesetzen des Bundes keine den Bestimmungen des AkkG entsprechenden Regelungen über die Akkreditierung enthalten sind – und im SigG kann eine entsprechende Regelung nicht gefunden werden.

8.2.7 Stellungnahme der Bundesministerin für Frauenangelegenheiten und Verbraucherschutz

Die Bundesministerin sprach sich für eine Erweiterung des Ausnahmenkatalogs in § 4 auf Verträge zur Begründung von Wohnungseigentum, auf befristete Mietverträge, auf Bauträgerverträge, auf Wohnungsverbesserungsverträge, auf in § 31 KSchG bestimmte Vereinbarungen im Maklerverträgen, auf Verbraucherkreditverträge, auf Verbrauchergirokontoverträge und Verträge über Abzahlungsgeschäfte aus.

Außerdem forderte sie, dass von allen Zertifizierungsdiensteanbietern, also auch jenen, die keine qualifizierte Zertifikate anbieten, Verzeichnis- und Widerrufsdienste geführt werden müssen. Diese Grundkriterien sollten aus Sicht des Verbraucherschutzes erfüllt werden, da auch einfache Signaturen gewisse Rechtswirkungen auslösen.
Der Abschluss einer Haftpflichtversicherung sollte ebenfalls zwingend vorgeschrieben werden, da nur diese im Falle einer Insolvenz den Konsumenten wirksam schützen kann. Ein unmittelbarer Rechtsanspruch gegen den Versicherer sollte unbedingt sichergestellt werden.

8.2.8 Stellungnahme des Bundesministeriums für Inneres

Im Vergleich zu den bisher angesprochenen Verbänden und Ministerien, die im Großen und Ganzen dieselben, auf die eigenen Interessen zugeschnittenen Forderungen erhoben haben, sind die des Innenministeriums einzigartig.

Unter anderem sprach sich das Innenministerium dafür aus, nach einer mehrjährigen Übergangsfrist nur mehr qualifizierte Zertifikate zuzulassen, da andernfalls die Rechtsunsicherheit steigen würde und ein nicht zu unterschätzender volkswirtschaftlicher Schaden die Folge wäre. Eine Reihe unterschiedlicher Zertifikatsklassen gestalte den Markt unübersichtlich und würde dazu führen, dass Konsumenten auf Billigangebote mit unsicherer Technologie hereinfallen würden.

Dazu sei vermerkt, dass die Richtlinie ausdrücklich vorschreibt mehrere Sicherheitsstufen anzubieten. Eine den Forderungen des Innenministeriums gerecht werdende Regelung würde

eine Haftung des Staates wegen Unterlassen korrekter und fristgerechter Umsetzung einer Richtlinie nach sich ziehen[103].

Die Möglichkeit der Verwendung eines Pseudonyms ist ein weiterer Punkt, der ausschließlich vom Innenministerium kritisiert wurde. Man ist der Meinung, dass dies in hohem Maße den vom Innenministerium wahrzunehmenden Sicherheitsinteressen widerspreche.

8.3 Die entscheidendsten Änderungen zum Entwurf

- Die Aufsichtsstelle gilt nicht als zentrale Wurzelinstanz, was zur Folge hat, dass nicht nur die Aufsichtsstelle Zertifikate für Zertifizierungsdiensteanbieter ausstellen kann, sondern die Zertifizierungsanbieter auch selbst. Der Vorteil liegt vor allem darin, dass Zertifizierungsdiensteanbieter ihre Arbeit auch schon aufnehmen können, bevor die Aufsichtsstelle ihre nötige Infrastruktur aufgebaut hat, was in Deutschland immerhin etwa zwei Jahre gedauert hat.

- Der Abschluss einer Haftpflichtversicherung wird nicht mehr als die einzig mögliche Sicherung möglicher Ansprüche angesehen, auch Bankgarantien, Bürgschaften oder ausreichende Finanzmittel gelten als ausreichend. Es soll mangels Erfahrung auch keine Mindestsumme im Gesetz normiert werden; sehr wohl kann diese allerdings in der SigV enthalten sein.

- Widerruf und Sperre werden erst mit dem Eintrag ins Sperr- oder Widerrufsregister gültig. Damit wird dem Vertrauensschutz auf die Gültigkeit des Zertifikates besonders Rechnung getragen. Demnach können ähnlich dem Firmenbuch nur eingetragene Tatsachen gegen einen Dritten wirken.

- Zu Zwecken der Verwaltungsvereinfachung soll die Verordnungsermächtigung dem Bundeskanzler und dem Bundesminister für Justiz allein zustehen. Die vorigen vier eingebundenen Verordnungskompetenzträger wurden nunmehr auf zwei reduziert.

- Klarstellung, dass Zertififzierungsdiensteanbieter neben Signier- auch Verschlüsselungsverfahren anbieten dürfen.

[103] Vgl. Öhlinger, T.: Verfassungsrecht. WUV Universitätsverlag, 3.Auflage, 1997, 84.

8.4 Die Signaturgesetzesnovelle[104]

8.4.1 Einleitung

Wie bereits angesprochen ist das österreichische SigG schon vor der formellen Verabschiedung der Signaturrichtlinie der EU in Kraft getreten. Darauf zurückzuführende Änderungen und der notwenige Ersatz der Anlaufkosten der Aufsichtsstelle sind die Hauptgründe für den Erlass der Novelle. Außerdem mussten Anpassungen aufgrund der Ausdehnung der Geltung der Sig-Richtlinie auf den Europäischen Wirtschaftsraum vorgenommen werden.

Das Problem der Finanzierung der Aufsichtsstelle ist zwar vom wirtschaftlichen Standpunkt gesehen äußert prekär, machten die Anlaufkosten bislang an die 30 Mio. ATS aus. Aus juristischer Sicht hingegen sind die Änderungen bezüglich dieses Punktes von geringerer Bedeutung und werden hier nicht behandelt.

8.4.2 Änderungen im Detail:

Der § 2 erhält eine Ziffer 15, in der die Begriffsbestimmung der Signaturrichtlinie enthalten ist. Darin heißt es dass unter der Signaturrichtlinie, die „Richtlinie des Europäischen Parlamentes und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L Nr. 13 vom 19. Jänner 2000, S 12." zu verstehen ist.
Diese Ziffer hat die Aufgabe, es sich durch eine eindeutige Kennzeichnung am Beginn des Gesetzes zu ersparen, bei jeder Erwähnung den vollen Titel anführen zu müssen. Vor allem die leichtere Lesbarkeit der Normen soll dadurch gewährleistet werden.

Von Bedeutung sind vor allem die Änderungen im § 5 Abs. 3. War bisher vorgesehen, dass ein qualifiziertes Zertifikat mit einer sicheren elektronischen Signatur des Zertifizierungsdienseanbieters versehen sein muss, wurde diese Bestimmung nun dahin gehend gelockert, dass die elektronische Signatur weder auf einem qualifiziertem Zertifikat beruhen muss, noch bestimmte technische Komponenten und Verfahren zwingend verwendet werden sollen. Diese Liberalisierung der Anforderungen wird aber nicht zu Lasten der Sicherheit gehen. Es wird lediglich angenommen, dass durch die von der Aufsichtsstelle ausgestellten qualifizierten Zertifikate ausreichende Sicherheitsvorkehrungen getroffen seien.

In § 7 Abs. 1 Z. 3. wird davon ausgegangen, dass qualitätsgesicherte Zeitangaben durch einen Zeitstempel erbracht werden. Die Richtlinie nimmt hingegen nicht dazu Stellung, auf welche Art und Weise Datum und Uhrzeit der Ausstellung oder des Widerrufs eines Zertifikats genau

[104] Bundesgesetz, mit dem das Signaturgesetz geändert wird. BGBl. I Nr. 137/2000.

bestimmt werden sollen. Die Angleichung in diesem Punkt wird mit dem in Klammer stehenden Ausdruck „zB sichere Zeitstempel“ durchgeführt.

Zu erheblichen Problemen könnte die Einführung des § 15 Abs. 4 führen, mit dem ein Streitschlichtungsverfahren unter der Voraussetzung der Zustimmung des Antragstellers auch elektronisch durchgeführt werden kann. Dies ist zwar grundsätzlich zu begrüßen, aber präzise Bestimmungen über Ablauf und vorgeschriebene Sicherheitsmaßnahmen sind mE unerlässlich.

Absätze 5 und 6 des § 18 normieren die Verpflichtung Sicherheitsbescheinigungen von Bestätigungsstellen aus dem Raum der Europäischen Gemeinschaft oder dem Europäischen Wirtschaftsraum anzuerkennen. Erst im Zuge der Novellierung ist die Geltung der Signaturrichtlinie auf den Europäischen Wirtschaftsraum ausgedehnt worden. Diesbezügliche Anpassungen sind auch im § 24 zu finden.

Im § 19 wird ein neuer dritter Absatz hinzugefügt, der festlegt, dass die von dem Komitologieausschuss ausgearbeiteten Mindestkriterien für die Benennung von Bestätigungsstellen maßgeblich sind. Diese Kriterien sind nach Art. 9 der Richtlinie zum 30. Juni 2000 angenommen worden und müssen vom Bundeskanzler im Einvernehmen mit dem Justizminister mit Verordnung kundgemacht werden. Die Benennung der weiteren Absätze verschiebt sich jeweils um eine Zahl.

Die Haftungsbestimmungen des § 23 Abs. 1 Z. 1 und 5 werden in Anlehnung an die Änderungen bezüglich des sicheren Zeitstempels (siehe oben) angepasst. Außerdem wurden die Geldbeträge der Verwaltungsstrafbestimmungen im § 26 in Euro umgerechnet und „geglättet“.

Mit Ausnahme des geänderten § 13 sollen die Modifikationen mit dem auf die Kundmachung dieses Bundesgesetzes folgenden Tag in Kraft treten. § 13 wird bereits ab 1. Oktober 2000 in Geltung gesetzt, damit die Aufsichtsstelle unverzüglich erforderliche Finanzierungsmaßnahmen in die Wege leiten kann.

9 Resumé

Abschließend kann gesagt werden, dass das SigG einen weiteren, gelungenen Beitrag dazu liefert, das Internet für den e-Comerce fit zu machen. Ohne die rechtliche Anerkennung der digitalen Unterschrift würde Europa und mit ihm Österreich dem internationalem Trend hinterher hinken und großen wirtschaftlichen Schaden erleiden. Gegnern ist insofern zuzustimmen, als man tatsächlich darauf achten sollte, das Netz der Netze nicht mit Gesetzesfluten zu über regulieren. Allerdings kann eine Thematik, wie die des SigG nicht mit Verhaltensrichtlinien der User geregelt werden – die gesetzliche Anerkennung ist unersetzlich.

Einzigartig auf dem Gebiet des Cyberlaw ist das SigG insofern, als in der Regel auf aufgetretene Missstände per Gesetz reagiert wurde, in diesem Fall aber Problemen vorgegriffen wurde. So wurde etwa die Darstellung pornographischer Bilder mit Minderjährigen verschärfteren Strafen unterzogen, als derartige Web-Sites nicht mehr nur Einzelfälle waren. Weiters wird wohl eine gesetzliche Regelung der Online-Auktionen nicht mehr allzu lang auf sich warten lassen, nachdem bereits heute große Rechtsunsicherheit auf diesem Gebiet besteht und Betrugsfälle regelmäßig auftreten. Das SigG hingegen ist ohne bedeutenden Druck von jeglichen Seiten zu einer Zeit erlassen worden, zu der nur wenige vom Bestehen derartiger technische Möglichkeiten wussten.

Ich bin davon überzeugt, dass die digitale Signatur sowohl im Geschäftsleben, als auch im Verkehr mit den Behören ein breites Anwendungsfeld finden wird. Um die Sache allerdings ins Rollen zu bringen müsste von stattlicher Stelle oder den Kammern aus, an die Masse der Bevölkerung zu günstigsten Konditionen sichere Signaturen ausgegeben werden. An der Wirtschaftsuniversität Wien hat man beispielsweise bereits überlegt, in Zusammenarbeit mit der Datakom allen Studenten eine elektronische Signatur auszustellen.
Wer sich schon heute mit den technischen und rechtlichen Hintergründen der digitalen Signatur vertraut macht, wird vielleicht schon morgen einen von der Konkurrenz nur mehr schwer aufzuholenden Vorsprung haben.

Literaturverzeichnis:

Bücher:

- Brenn, C.: Signaturgesetz. Manzsche Gesetzesausgaben, Sonderausgabe Nr.101, 1999.
- Mayer-Schönberger, V., Pilz, M., Reiser, C., Schmölzer, G.:Signaturgesetz. Orac, 1999.
- Mayer-Schönberger, V.: Das Recht am Info-Highway. Verlag Orac, 1997.
- Öhlinger, T.: Verfassungsrecht. WUV Universitätsverlag, 3. Auflage, 1997.

Zeitschriften:

- Baum, M.: Gültigkeitsmodell des SigG. In: DuD – Datenschutz und Datensicherheit, 1999, 23, 199
- Belkem, M.: Die digitale Signatur kurz vor dem Start. In: DuD – Datenschutz und Datensicherheit, 24, 2000, 75.
- Benn-Ibler, G., Held, G.: Schrift und Unterschrift – elektronisch. In: AnwBl., 1999, 732.
- Beucher, K., Schmoll, A.: Kryptotechnologie und Exportbeschränkungen. In: Computer und Recht, 8, 1999, 529.
- Brenn, C.: Das österreichische Signaturgesetz – Unterschriftenersatz in elektronischen Netzwerken. In: ÖJZ, 16, 54. Jg, 587.
- Brenn, C.: Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet. In: ÖJZ, 17, 52. Jg, 644ff.
- Couvert-Castéra, I.: Frankreich: Kryptographie liberalisiert. In: DuD – Datenschutz und Datensicherheit, 1998, 22, 338.
- Diffie, W., Hellman, M.: New Directions in Cryptography. In: IEEE Transactions on Information Theory 1976, Vol. IT-22, 644 – 654.
- Emmert, U.: Haftung der Zertifizierungsstellen. In: Computer und Recht, 4, 1999, 245.
- Forgó, N.: Sicher ist sicher? – Das Signaturgesetz. In: Ecolex, 9, 1999, 607.
- Gundermann,L., Köhntopp,M.: Biometrie zwischen Bond und Big Brother – Technische Möglichkeiten und rechtliche Grenzen. In: DuD - Datenschutz und Datensicherheit, 3, 1999, 143.
- Hortmann, M.: Kryptoregulierung weltweit – Überblick. In: DuD – Datenschutz und Datensicherheit. 1997, 21, 214.
- Jud, W., Högler-Pracher, R.: Die Gleichsetzung elektronischer Signaturen mit der eigenhändigen Unterschrift. In: Ecolex, 9, 1999, 610.
- Menzel,T., Schweighofer, E.: Das österreichische Signaturgesetz. In: DuD – Datenschutz und Datensicherheit, 23, 1999, 503.
- Thiel, C.: Marktentwicklung im Umfeld digitaler Signaturen. In: DuD – Datenschutz und Datensicherheit, 24, 2000, 77.
- Wessely, W.: Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? In: ÖJZ, 13, 54. Jg, 491.

Web-Literatur:

- A-Sit: Fragen und Antworten zur elektronischen Signatur. Online im Internet: Url: http://www.a-sit.at/TEXTE/FAQ_Signatur/# [abgerufen am 7.1.2001].
- Datacom Austria GmbH: Die meisten Verschlüsselungsprogramme sind unsicher. Online im Internet: Url: www.datacom.at.cgi [abgerufen am: 12.7.1999].
- Datakom Austria GmbH: Markt für Netzsicherheits-Software boomt. Online Ausgabe 10.7 1999. Online im Internet: Url: http://www.datakom.at/ [10.7. 1999].
- Der Standard: Fast 62 Millionen am Netz. Online Ausgabe 6.7.1999. Online im Internet: Url: http://www.derstandard.at/ [abgerufen am: 6.7.1999].
- Deutscher Multimedia Verband: Multimedia Marktzahlen. Online im Internet: Url: http://www.dmmv.de/multi/zahlen.html [abgerufen am: 13.6.2000].

- Elements for objective analysis and advice concerning potentially dastabilising accumulations of conventional weapons. Online im Internet: Url: http://www.wassenaar.org/docs/criteria.html [abgerufen am 25.10.1999].
- Elling, V.: Sichere Hashfunktionen und ihr Gebrauch für digitale Unterschriften. Online im Internet: Url: http://linux.fh-heilbronn.de/vortrag/Kryptographie/volker/sighash.html [abgerufen am 16.8. 1999].
- Glintschert, A.: Kryptologie und die neuen Medien. Online im Internet: Url: http://www.educat.hu-berlin.de/publikation/student/kryptologie/einfuehrung.html [abgerufen am 5.9.2000].
- Gutenberg, J.: Grundprobleme von Datenschutz und Datensicherheit. Online im Internet: Url: http://www.uni-mainz.de/~pommeren/DSVorlesung/Grundprobleme/Kryptopolitik.html [abgerufen am 25.3.2001].
- Heß, A.: Grundlagen der Kryptographie. Online im Internet: Url: http://www.uni-mainz.de/~hessan00/krypto/Krypto1.html [abgerufen am: 5.9.2000].
- Höhne, S.: Auswirkungen des Signaturgesetzes auf das Internet. Online im Internet: Url: http://www.iri.uni-hannover.de/seminararbeiten/ [abgerufen am 22.1.2001].
- Holzbach, M.: Digitale Signatur – Neue Wege elektronischer Geschäftsabwicklung. Online im Internet: Url: http://akitsicherheit.iaik.tu-graz.ac.at/Tagung101097/mholzbach/sld012.htm [abgerufen am 28.3.2000].
- Internet-Verband: Deutschland hinkt beim E-Handel hinterher, "Kräftiges Internet-Wachstum, aber noch kein Massenmarkt". Online im Internet: Url: http://www.the-bulls.com/news/news_2658.html [abgerufen am: 13.6.2000].
- Lauert, A.: Elektronisches Bezahlen. Online im Internet: Url: http://didaktik.cs.uni-potsdam.de/Lehre/e-commerce/elBez2-5/page05.html [abgerufen am 5.9. 2000].
- Lauert, A.: Elektronisches Bezahlen. Online im Internet: Url: http://didaktik.cs.uni-potsdam.de/Lehre/e-commerce/elBez2-5/page06.html [abgerufen am 5.9.2000].
- Leipholz-Schumacher, B.: Kryptographie. Online im Internet: Url: http://www.zitadelle.juel.nw.schule.de/if/java/krypto/RSAInfo.html [abgerufen am 10.9.2000].
- Martos, P.: Elektronische Signatur – Husch-pfusch statt sicherem e-commerce? In: Die Presse: Online Ausgabe vom 15.6.1999. Online im Internet: Url: http://www.diepresse.at/archiv.taf?_function=read&_UserReference=FA7DCBD31F90AF0737F48075&_id=547335 [abgerufen am 22.1.2001].
- Mayer-Schönberger, V.: „Krypto-logisch“ Die neue Versuchung im Cyberlaw. Online im Internet: Url: www.normative.zusammenhänge.at [abgerufen am: 7.7.1999].
- Medosch, A.: Alles was Sie schon immer über Krypto-Regulierungen wissen wollten. Online im Internet: Url: http://www.heise.de/tp/deutsch/html/result.xhtml?url=/tp/deutsch/inhalt/te/2932/1.html&words=OECD%20Krypto [abgerufen am: 14.1.2000].
- ORF on Futurezone: Arbeiterkammer übt harte Kritik am Signaturgesetz. Online Ausgabe vom 11.6.1999. Online im Internet: Url: http://futurezone.orf.at/futurezone.orf?read=detail&id=1704&tmp=59952 [abgerufen am 13.6.1999].
- ORF on Futurezone: Computer erkennt Diebe am Gang. Online Ausgabe 2.12.1999. Online im Internet: Url: http://futurezone.orf.at/futurezone.orf?read=detail&id=10239&tmp=89416 [abgerufen am: 2.12.1999].
- ORF on Futurezone: Deutsche führen im E-Kommerz. Online Ausgabe 28.6.1999. Online im Internet: Url: http://www.futurezone.at [abgerufen am: 28.6.1999].
- Presseaussendung der Vereinigung Österreichischer Industrieller (VÖI), des Fachverbands für Elektro- und Elektronikindustrie (FEEI) und des Verbands für Informationswirtschaft (VIW). Online im Internet: E-mail von Gerhard Wagner <gkwagner@via.at> [abgerufen am: 19.8.1999].
- Reif, H.: Winnetou und OLD SSLeay. Online im Internet: Url: http://www.heise.de/ix/artikel/1998/07/128/ [abgerufen am 20.9.2000].
- Schultzki-Haddouti, C.: Markt- oder Staatsmacht - Streit um digitale Signaturen. Online im Internet: URL: http://www.heise.de/ct/99/01/058/ [abgerufen am 26.10.1999].
- Sicherheit im Internet: Pressemitteilung des Bundesministerium für Wirtschaft und Technologie und des Bundesministerium des Innern. Online im Internet: Url: http://www.sicherheit-im-internet.de/showdoc.php3?doc=bmwi_min_doc_1999940655766&page=1 [abgerufen am: 25.10.1999].
- Stellungnahme des Bundesverbands der freien Berufe. Online im Internet: E-Mail von Michael Leistenschneider <info@leistenschneider.de>[abgerufen am: 10.7.1999].
- Tauss, J.: Digitale Signatur und Verschlüsselung. Online im Internet: Url: http://www.tauss.de/bn/sigtext.html [abgerufen am 28.3.2000].
- Unbekannter Autor: Clipper-Chip. Online im Internet: URL: http://www.tzi.de/~ansu/papers/crypto/cryptohtml/main-node20.html [abgerufen am: 7.11.1999].

- Universität Freiburg/Institut für Informatik und Gesellschaft (IIG-Telematik): Electronic Commerce Enquête. In Computer Zeitung, Gemini Consulting. Online im Internet: Url: http://telematik.iig.uni-freiburg.de/~schoder/ece/ [abgerufen am: 13.6.2000].

Parlamentarische und Materialien von Organisationen:

- Bundesgesetz, mit dem das Signaturgesetz geändert wird. BGBl. I Nr. 137/2000.
- Erläuterungen zum Bundesgesetz über die Rechtsstellung des Sekretariats des Wassenaar Arrangements in Österreich. Online im Internet: Url: http://www.parlinkom.gv.at/pd/pm/XX/I/texte/007/I00702_.html [abgerufen am: 2.9.2000].
- Erläuterungen zum Signaturgesetz. Online im Internet: Url: http://www.parlinkom.gv.at/pd/pm/XX/I/texte/019/I01999_.html [abgerufen am 3.11.2000].
- Europäische Initiative für den elektronischen Geschäftsverkehr: Mitteilung an das Europäische Parlament, den Rat, den Wirtschaft- und Sozialausschuß der Regionen. KOM(97) 157 endg. vom 16.4.1997.
- Europäische Initiative für den elektronischen Geschäftsverkehr: Mitteilung an das Europäische Parlament, den Rat, den Wirtschaft- und Sozialausschuß der Regionen. KOM(97) 503 endg. vom 8.10.1997.
- Französisches Bundesgesetz über Kryptographiebeschränkungen. Nr. 190-1170. Online im Internet: Url: http://home.fhtw-berlin.de/~s0291172/Semesterarbeit/frankreich.html#frankreich [abgerufen am: 31.8.200].
- Public Statement of the fourth Plenary meeting in Vienna, 3.12.1998. Online im Internet. Url: http://www.wassenaar.org/docs/press_4.html [abgerufen am 20.5.2000].
- Rechtsstellung des Sekretariats des Wassenaar Arrangements in Österreich. BGBl. I Nr. 89/1997.
- Signaturgesetz. BGBl. I Nr. 190/1999.
- The OECD Cryptographie Policy Guidelines and the Report on Background and Issues of Cryptography Policy, March 1997. OCDE/GD(97)204. Online im Internet: Url: http://www.oecd.org/dsti/sti/it/secur/index.htm [abgerufen am 27.3.2001].
- Unicitral Model Law on electronic Commerce with Guide to Enactment. Online im Internet: Url: http://www.uncitral.org/en-index.htm [abgerufen am: 31.8.2000].
- Verordnung (EG) Nr. 1334/2000des Rates vom 22.6.2000 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr von Gütern und Technologien mit doppeltem Verwendungszweck. Online im Internet: Url: http://wko.at/eu/zoll/dual-use-vo.htm [abgerufen am 2.2.2001].
- Working Group on Electronic Commerce: Draft uniform rules on electronic signatures. A/CN.9/WG.IV/WP.73, 12.12.1997.
- Working Group on Electronic Commerce: Draft uniform rules on electronic signatures. A/CN.9/WG.IV/WP.76, 25.5.1998.
- Working Group on Electronic Commerce: Draft uniform rules on electronic signatures. A/CN.9/WG.IV/WP.79 und 80, 15.12.1998.
- Working Group on Electronic Commerce: Draft uniform rules on electronic signatures. A/CN.9/WG.IV/WP.82, 29.6.1999.
- Working Group on Electronic Commerce: Planning of future work on electronic commerce: Digital signatures, certification authorities and related legal issues. A/CN.9/WG.IV/WP.71, 31.12.1996.