Schriftenreihe Rechtsinformatik

Erich Schweighofer / Thomas Menzel (Hg.) • Band 2

Menzel

Elektronische Signaturen

Verlag Österreich

Wien 2000

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Menzel, Thomas:
Elektronische Signaturen / Thomas Menzel. – Wien : Verl. Österreich, 2000
(Schriftenreihe Rechtsinformatik ; Bd. 2)
ISBN 3-7046-1593-5

Unterstützt von

der Digitalen Signatur der DATAKOM AUSTRIA

ISBN 3-7046-1593-5

(vorm. Österreichische Staatsdruckerei AG)
Verlag Österreich, Rennweg 16, A-1037 Wien
Tel.: (++431) 610 77-333, Fax: (++431) 610 77-502
e-Mail: order@verlagoesterreich.at
http://www.verlagoesterreich.at

Vorwort

Seit fast 30 Jahren wird das Internet zur globalen Kommunikation genutzt, seit etwas mehr als 20 Jahren sind revolutionäre Konzepte zur Verschlüsselung bekannt, die authentische und sichere Kommunikation aller Beteiligten im Internet erst ermöglichen, indem Identität des Senders und Integrität der übermittelten Nachricht sichergestellt werden. Die Kombination dieser beiden Technologien führt zu völlig neuen Möglichkeiten für die Verwendung dieses Mediums im Rahmen von Electronic-Commerce und Electronic Government. Stand bis vor kurzem durch das Internet nur der Austausch von rechtlich nicht verbindlichen Informationen im Vordergrund, findet in jüngster Zeit eine Entwicklung statt, dieses Medium auch für die Kommunikation von rechtsverbindlichen Willenserklärungen zu nutzen. Vertriebsfirmen, Banken und Kreditkartenunternehmen, Versicherungen, Konsumenten und nicht zuletzt diverse Behörden erkennen die Vorteile der Sicherung elektronischer Kommunikation in offenen Netzwerken wie dem Internet, die auch im Rahmen rechtsverbindlicher Kommunikation zur Verfügung stehen sollen.

Aus der bisher fehlenden rechtlichen Anerkennung folgte unzureichendes Vertrauen der Anwender und die Vermeidung der Kommunikationsmöglichkeit „Internet" im rechtsgeschäftlichen Bereich. Die Fixierung allgemein verbindlicher Normen über die Rechtswirkung elektronisch signierter Dokumente ist daher eine Voraussetzung für Electronic Commerce und Electronic Government.

Nachdem eine erste gesetzliche Regelung nun in der Europäischen Union und auch die Umsetzung in österreichisches Recht in Kraft trat, ist der erste Schritt zur rechtlichen Anerkennung und Absicherung des elektronischen Geschäfts- und Behördenverkehrs getan. Die rechtlichen Rahmenbedingungen für den Einsatz elektronischer Signaturen und deren Ausstattung mit Rechtswirkung regeln neueste Normen auf internationaler, europäischer und innerstaatlicher Ebene.

Die Notwendigkeit einer positiv-rechtlichen Regelung durch den Gesetzgeber wurde auch von der Wirtschaft erkannt und wird von ihr seit einiger Zeit gefordert. Nicht nur im ökonomischen Bereich gewinnen elektronische Signaturen immer mehr an Bedeutung, auch der Einsatz im öffentlichen Bereich wurde und wird diskutiert. Angeregt wurde die Öffnung der Verwaltung gegenüber dem Internet durch ein Grünbuch der Europäischen Kommission über die Information des öffentlichen Sektors in der Informationsgesellschaft. „help.gv.at", das Rechtsinformationssystem der Republik Österreich, der Bürgerservice der Stadt Wien und die Inter-

netpräsenz des österreichischen Parlaments liefern genügend konkrete Anregungen für einen zukünftigen Bedarf an Einsatz elektronischer Signaturen bei der Kommunikation zwischen Bürger und Verwaltungsdienststelle.

Mittlerweile liegen genügend Erfahrungswerte, Feldstudien und auch schon Gesetze über den Einsatz elektronischer Signaturen in einigen Ländern vor, um den Beginn einer breiten Anwendung der neuen Techniken im Rechtsbereich zu erwarten.

Die angestrebte Erweiterung rechtsverbindlicher Erklärungsarten erfordert sowohl von rechtswissenschaftlicher als auch von technischer Seite Impulse und Reaktionen, um gemeinsam erarbeitete, sinnvoll anwendbare rechtliche und technische Normen sowie Lösungen zu präsentieren. Die zunehmende Vernetzung der Rechnersysteme im Internet und deren Nutzung für Telekooperation im Electronic Commerce haben die Suche nach einem technischen Verfahren zur rechtsverbindlichen Willenserklärung über dieses Medium ausgelöst. Die elektronische Signatur verkörpert die passende Lösung für dieses Problem, indem sie dem Sicherheitsbedarf optimal Rechnung trägt, da sie alle Funktionen eigenhändiger Unterschriften im elektronischen Bereich erfüllt.

Dieses Buch soll einen Beitrag liefern, die Zusammenarbeit von Technikern und Juristen in diesem Gebiet zu erleichtern, indem sowohl der technische Background allgemein verständlich dargestellt als auch die Reaktion des Rechts behandelt wird.

Es sollen hauptsächlich die Regelung des österreichischen Signaturgesetzes und der Themenbereich der Richtlinie des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen und die daraus resultierenden rechtlichen Wirkungen elektronischer Signaturen diskutiert werden.

Nach einer Darstellung der derzeit angewandten Technik zur Gewährleistung der Identität des Senders und der Authentizität der im Internet übertragenen Nachrichten werden die Anforderungen der Rechtsordnung an sichere Kommunikation im Rahmen von Electronic Commerce und die Rechtswirkung, mit der sicher elektronisch signierte Dokumente ausgestattet sind, vom Standpunkt des österreichischen und des Europarechts beschrieben.

Wien, im Mai 2000 Thomas Menzel

Inhaltsverzeichnis

Abkürzungsverzeichnis

AB	Ausschußbericht
ABGB	Allgemeines Bürgerliches Gesetzbuch
ABl	Amtsblatt
Abs	Absatz
ADCert	Arge Daten Zertifizierung
AFIS	Automatisches Fingerabdruck-Identifizierungssystem
AG	Aktiengesellschaft
AIPA	Autorita per l´Informatica nella Pubblica Amministrazione
AkkG	Akkreditierungsgesetz
ANSI	American National Standardisation Institution
AnwBl	Anwaltsblatt
API	Advanced Programme Interface
Arb	Sammlung arbeitsrechtlicher Entscheidungen
ARPANET	Advanced Research Projects Agency Network
Art	Artikel
Ascii	American Standard Code for Information Interchange
ASN	Abstract Syntax Noation
Aufl	Auflage
AVG	Allgemeines Verwaltungsverfahrensgesetz
BDSG	Bundesdatenschutzgesetz
BGBl	Bundesgesetzblatt
BILETA	British & Irish Legal Education Technology Association
BMF	Bundesminister(ium) für Finanzen
BR	Bundesrat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestag - Drucksache
B-VG	Bundes-Verfassungsgesetz 1920 idF von 1929
BWG	Bankwesengesetz
CERN	Europäische Organisation für Kernforschung
Co	Company
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CRT	Chinese Remainder Theorem
dBGB	(deutsches) Bürgerliches Gesetzbuch

DES	Data Encryption Standard
DIN	Deutsche Industrienorm
DLL	Dynamic Link Library
Doc	Document
DSA	Digital Signature Algorithmus
DSG	Datenschutzgesetz
dSigG	(deutsches) Signaturgesetz
DuD	Datenschutz und Datensicherheit
E	Electronic
E	Evaluationsstufe
EBRV	Erläuternde Bemerkungen zur Regierungsvorlage
EC	European Commission
EDI	Electronic Data Interchange
EDV	Elektronische Datenverarbeitung
EESSI	European Electronic Signature Standardization Initiative
EG	Europäische Gemeinschaft
ETS	European Trusted Services
ETSI	European Telecommunication Standard Institute
EU	Europäische Union
EuGH	Euopäischer Gerichtshof
EuGVÜ	Europäisches Übereinkommen v 27.9.1968 über die gerichtliche Zuständigkeit und die Vollstreckung gerichtlicher Entscheidungen in Zivil- und Handelssachen
EvBl	Evidenzblatt
EVHGB	Vierte Verordnung zur Einführung handelsrechtlicher Vorschriften im Lande Österreich
EVÜ	Europäisches Schuldvertragsübereinkommen
EWG	Europäische Wirtschaftsgemeinschaft
f	und der, die folgende
ff	und der, die folgenden
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GASP	Gemeinsame Außen- und Sicherheitspolitik
GBG	Allgemeines Grundbuchsgesetz
GewO	Gewerbeordnung
GmbH	Gesellschaft mit beschränkter Haftung
GMD	Gesellschaft für Mathematik und Datenverarbeitung
GOG	Gerichtsorganisationsgesetz

GP	Gesetzgebungsperiode
GUIDEC	General Usage for International Digitally Ensured Commerce
GZ	Geschäftszahl
HBCI	Homebanking Computer Interface
HTL	Höhere Technische Lehranstalt
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
IAIK	Institut für Angewandte Informationsverarbeitung und Kommunikation der Technischen Universität Graz
ICC	International Chamber of Commerce
ID	Identity
IDEA	International Data Encryption Algorythm
IEEE	The Institute of Electrical and Electronic Engineers
IFIP	International Federation of Information Processing
IPRG	Internationales Privatrechtsgesetz
ISBN	Internationale Standard-Buchnummer
ISO	International Standardisation Organisation
IT	Informationstechnologie
ITU	International Telecommunication Union
IuKDG	Informations-und Kommunikationsdienste-Gesetz
iVm	in Verbindung mit
JBl	Juristische Blätter
KB	Kilobyte
KG	Kommanditgesellschaft
KOM	Dokumente der Kommission der Europäischen Gemeinschaften
LDAP	Lightweight Directory Access Protocol
LG	Landesgericht
lit	litera (Buchstabe)
MB	Megabyte
MD	Message Digest
mE	meines Erachtens
MEZ	Mitteleuropäische Zeit
MIC	Message Integrity Check
MIME	Multipurpose Internet Mail Extensions
MMR	(Zeitschrift für) Multimedia und Recht
MRG	Mietrechtsgesetz
NIST	National Institute of Standards and Technology

NJW	Neue Juristische Wochenschrift
NO	Notariatsordnung
NR	Nationalrat
NRCCL	Norwegian Research Center for Computer and Law (University of Oslo)
NSA	National Security Agency
NZ	Österreichische Notariatszeitung
NZwG	Notariatszwangsgesetz
ÖBA	Österreichisches Bankarchiv
ÖBl	Österreichische Blätter
OCG	Österreichische Computergesellschaft
OECD	Organization for Economic Co-operation and Development
OGH	Oberster Gerichtshof
ÖJZ	Österreichische Juristen-Zeitung
ÖJZ-LSK	Leitsatzkartei in der Österreichischen Juristen-Zeitung
OLG	Oberlandesgericht
PC	Personal Computer
PDF	Portable Document Format
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PIN	Personal Identity Number
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastruktur
RdW	Österreichisches Recht der Wirtschaft
RFC	Request for Comments
RSA	Rivest, Shamir, Adleman
RTF	Rich Text Format
RV	Regierungsvorlage
Rz	Randziffer
S	Seite
S/MIME	Secure Multipurpose Internet Mail Extensions
SEMPER	Secure Electronic Marketplace Europe
SET	Secure Electronic Transaction
SHTTP	Secure Hyper Text Transfer Protocol
SigG	Signaturgesetz
SigRL	Signaturrichtlinie
SigVO	Signaturverordnung
SMTP	Simple Mail Transport Protocol

SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
StGG	Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger
stRsp	ständige Rechtssprechung
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
TKG	Tele-Kommunikations-Gesetz
Tk-Rat	Telekkommunikations-Rat
TTP	Trusted Third Party
TÜV	Technischer Überwachungsverein
UK	United Kingdom
UNCITRAL	United Nations Commission for International Trade Law
URDOK	Urkundensichere Dokumentenverarbeitung
US	United States
USA	United States of America
VfGH	Verfassungsgerichtshof
WBl	Wirtschaftsrechtliche Blätter
WEG	Wohnungseigentumsgesetz
WG	Wechselgesetz
WTO	World Trade Organisation
WWW	World Wide Web
Z	Ziffer
zB	zum Beispiel
ZPO	Zivilprozessordnung
ZVR	Zeitschrift für Verkehrsrecht

1. Entwicklung des Elektronischen Geschäftsverkehrs

1.1. Entstehungsgeschichte

1.1.1. Internet[1]

Im Jahr 1999 ist es für viele selbstverständlich, sich eines der überall gegenwärtigen Computer zu bedienen und mit diesem Gerät[2], sofern es vernetzt ist, Informationen aus allen Teilen der Welt über jedes beliebige Thema abzurufen und die eigenen Informationen zu verteilen. Möglich wurde dies durch die Schaffung eines einheitlichen Standards der Kommunikation, unabhängig von verwendeten Computern, Netzwerken und Ländern.

Einzelne Computer sind nicht mehr wie früher über Leitungen verbunden, die exklusiv von wenigen miteinander kommunizierenden Rechnern verwendet wurden, sondern alle Rechner zerlegen ihre Informationen in Pakete, die durchnumeriert und mit Adressat und Absender versehen in gemeinsam benutzte Leitungen, die die einzelnen Netze verbinden, eingespielt werden. In einem Arbeitspapier[3] präsentierte *Leonard Kleinrock* diese neue Art der Kommunikation zwischen Rechnern, packet switching genannt, erstmals 1961.

1965 verband man zum ersten Mal zwei Computer, die dieses neue Verfahren benutzten. 1969 entstand ARPANET, ein Versuchsnetzwerk, in dem vier in verschiedenen Teilen der USA stehende Rechenzentren eingebunden wurden. Hier wendete man erstmals eine offene Netzwerkarchitektur an, von *Bob Kahn* 1972 entwickelt, lokale Netze mit verschiedensten Topologien konnten nun auf einer Metaebene verbunden werden. Seitdem ist es möglich, zwischen Netzen unterschiedlichster Architektur Daten zu übertragen. Die technische Realisierung geschah

---

[1] *Zarkon*, Hobbes Internet Timeline, http://info.isoc.org/guest/zakon/Internet/History/HIT.html, A Brief History of the Internet, http://info.isoc.org/internet/history/brief.html, Alle URLs wurden am 20. Mai 2000 zuletzt besucht.

[2] Wie jüngste Entwicklungen zeigen trifft dies nicht nur auf den klassischen Personal Computer zu, sondern es werden vermehrt auch andere Maschinen, wie z.B. Personal Digital Assistants, und Mobiltelefone mit Internetfunktionalität ausgestattet.

[3] *Kleinrock*, Information Flow in Large Communication Nets, RLE Quarterly Progress Report (1961).

durch die Normierung von Transmission Control Protocol/Internet Protocol (TCP/IP), welches das grundlegende Protokoll für alle Internet-Applikationen bildet. 1972 wurde der Vorläufer von TCP/IP der Öffentlichkeit vorgestellt, 1982 das Internet als die Menge aller verbundenen lokalen Netze, die mittels der Verwendung des Netzwerkprotokolls TCP/IP kommunizieren, definiert. Die universelle Portierung auf so gut wie alle verschiedenen Plattformen trug wesentlich zum Siegeszug des Internets bei. Techniken, die den Nachrichtenverkehr zwischen beliebig vielen Netzen ermöglichen, und die Tatsache, daß nun alle Computer in der Lage waren, „die gleiche Sprache zu verstehen", ermöglichten die globale Kommunikation. Die ersten Programme und Standards, um Emails zu verschicken, wurden 1972 entwickelt. Telnet und File Transfer Protocoll (FTP), Programme, um auf entfernten Rechnern zu arbeiten und Dateien zwischen eigenem und entferntem Rechner zu transferieren, folgten im nächsten Jahr. Einen großen Sprung vorwärts in der Usability des Internets gab es durch die Gründung des World Wide Web (WWW) durch *Tim Berners-Lee* im Jänner 1991.[4] Das metastrukturelle Konzept des WWW erlaubt dem Anwender, selbst mit geringsten Computerkenntnissen multimediale Daten zu erhalten.

Mittlerweile ist eine Vielzahl verschiedener Viewer[5] verfügbar, um so gut wie jede Darstellungsform von Daten am Bildschirm des Anwenders visualisieren zu können. Datenbankabfragen sind ebenso möglich wie die Darstellung bewegter Bilder und Töne. Der neueste, stark umstrittene, von Microsoft gesetzte Trend active desktop[6] führt zu einem fließenden Übergang zwischen der Verwendung lokal gespeicherter Daten und Informationen von entfernten Servern. Positiv formuliert erleichtert dies die Arbeit, da der Verbindungsaufbau zu entfernt gespeicherten Daten weitgehend automatisiert wird. ME überwiegen aber die Nachteile, da die Quellen der Daten in der Praxis nicht mehr nachgeprüft werden und dadurch Sicherheitslücken und Unsicherheit über die Qualität der Information entstehen.

Ein weiterer wichtiger Faktor für die rasante Ausbreitung des Internets ist seine dezentrale Organisation, abgesehen von der Registrierung der Domainnames, die entweder bei Internic.net oder bei Stellen in den jeweiligen Ländern erfolgt, ist keine weitere zentrale Verwaltung nötig. Neue Nodes können ohne viel Aufwand an das Internet angebunden wer-

---

[4] *Segal,* A Short History of Internet Protocols at CERN, http://home.cern.ch/~ben/TCPHIST.html.

[5] Download zB bei: http://tucows.univie.ac.at/.

[6] http://www.microsoft.com/windows/ie/features/default.asp.

den. Dies erkennt man sehr deutlich an der Zahl der Nutzer: Waren 1973 erst 23 Hosts an das Netz angebunden, so wurden 1984 über tausend gezählt, 1987 kommunizierten bereits zehntausend Hosts über TCP/IP. Die Zahl der angebundenen Server steigt exponentiell an. Der Stand Jänner 1998 läßt sich nur mehr schätzen und wird mit knapp unter 30 Millionen beziffert.[7]

Die Internationalisierung des Internets begann 1973 mit der Anbindung von Rechnern in England. Seit 1990 stehen auch in Österreich Internet-Services zur Verfügung. Bis heute wurden weltweit kontinuierlich auch die entferntesten Gebiete eingebunden, so daß (Stand 1998) 239 verschiedene nationale Toplevel-Domains adressierbar sind.[8]

1.1.2. Kommerzielle Öffnung

In den ersten Jahrzehnten wurde das Internet ausschließlich im akademischen und zu einem geringen Prozentsatz im militärischen Bereich genutzt. Als erstes bedienten sich die Institutionen, die es entwickelt hatten, seiner Dienste. Angehörige der Universitäten erkannten rasch die Möglichkeiten dieser schnellen weltweiten Kommunikation, aber auch der Zugang und die Verwendung der damals wenigen Super Computer Centers erfolgte über das Internet. Die breite Öffentlichkeit nahm von den neuen Möglichkeiten, die das Web bot, kaum Notiz.

In den frühen Achtzigerjahren begann eine Änderung durch die Implementierung von TCP/IP in kommerziell angebotene Softwarepakete. TCP/IP und damit die Kommunikation am Internet waren nicht mehr nur das „Spielzeug" einiger UNIX-Freaks, sondern begannen langsam auch in Büros und Haushalten Einzug zu finden. 1989 wurde das Unternehmen „The World"[9] gegründet und eröffnete 1990 seine Tätigkeit als erster kommerzieller Internet Dial-Up Provider. So wurde für jeden, der über Telefonanschluß, Modem und Computer verfügt, der Zugang zum Internet möglich. Die zunehmende Zahl an Anwendern machte das Internet auch für Unternehmen interessant[10], so dauerte es nicht lange, bis die ersten Firmen mit Homepages im Netz präsent waren. Zuerst wurde nur für Produkte geworben, die auf traditionelle Weise zu kaufen waren. Bald

---

[7] Internet Domain Survey, http://www.isc.org/ds/.

[8] Internet Domain Survey, January 1998, http://www.nw.com/zone/iso-country-codes.

[9] Homepage des Unternehmens: http://world.std.com/.

[10] Näheres zu Potentialen für On-line-Verkauf und – Werbung im WWW findet man bei: *Hansen*, Klare Sicht am Info-Highway, Geschäfte via Internet & Co., S. 129ff.

waren aber vor allem im EDV-Bereich erste Serviceleistungen, wie das Download von Treibern und Dokumentationen, verfügbar.

1994 wurden die ersten Möglichkeiten, über das Netz zu verkaufen, verwirklicht. Der Autor *Robert Zarkon* von „Hobbes Internet Timeline"[11] fügte im Abschnitt über das Jahr 1994 die euphorische Meldung ein: „Yes it's true – you can now order pizza from the hut online". Bald beschritten unzählige Shopping Malls, Banken, Buchgeschäfte, Blumenhandlungen und viele andere Dienstleistungsunternehmen den Distributionsweg Internet.

Gegenwärtig dominiert noch die Software- und Unterhaltungsbranche die Absatzergebnisse. Da hierbei keine physischen Waren übergeben werden, ist das Internet als Marktplatz für diesen Unternehmensbereich besonders günstig. Die Fixkosten für Verkaufsräume und gedruckte Werbung fallen weg, man braucht nur verfügbaren Webspace bei einem Provider und Datenbanken, in denen die Produkte gespeichert und abrufbar sind. Für beides gibt es mittlerweile komfortable Produkte[12] auf dem Markt. Relativ neu am Markt etablieren sich aber auch immer mehr konventionelle Supermärkte und Versandhäuser[13], die ihre Produkte im Web anbieten und nach erfolgter elektronischer Bestellung durch Botendienste zustellen. Die Bezahlung erfolgt zur Zeit meistens noch per Nachnahme oder Kreditkarte, doch wird die Entwicklung[14] von Electronic Cash[15] fleißig vorangetrieben.

Statistiken über den im Internet erzielten Umsatz sind schwer zu erstellen. In einer OECD Studie[16] wurden aber folgende Trends ausgearbeitet:

---

[11] *Zarkon,* Hobbes Internet Timeline v3.3, http://info.isoc.org/guest/zakon/Internet/History/HIT.html.

[12] ZB: http://www.intershop.de/products/index.htm http://www.pandesic.com/Channels/.

[13] ZB: http://www.billa.at/ und http://www.quelle.de.

[14] *Zuccato,* Legislation and economical aspects of Electronic Money with special viewpoint on Europe, Proceedings of the Joint IFIP WG. 8.5 and WG 9.6 Working Conference 1999, S. 161.

[15] *Hirsch,* Rechtliche Untersuchung des virtuellen Zahlungsmediums E-Cash, in: *Schweighofer/Menzel* (Hg.), E-Commerce und E-Government, aktuelle Fragestellungen der Rechtsinformatik, S. 29.

[16] OECD/GD(97)185, Committee for Information, Computer and Communications Policy: Measuring Electronic Commerce S. 3f, 1997, download: http://www.oecd.org/dsti/sti/it/ec/prod/e_97-185.htm.

- Der Absatz von Geschäften zwischen Händlern (Business to Business Bereich) übersteigt stark den Absatz von Verbrauchergeschäften (Consumer to Business Bereich).
- Den Hauptanteil bei Verbrauchergeschäften tätigt die Unterhaltungsbranche.
- Die führenden Produkte im elektronischen Geschäftsverkehr sind: Software, Reisen, Unterhaltung und Finanzdienstleistungen.
- Der elektronische Geschäftsverkehr ist gegenwärtig noch ein kleiner Bereich, es werden aber Zuwachsraten von 200 Prozent jährlich prognostiziert.
- Electronic Commerce wird sich nicht nur auf einzelne kleine Inseln des Handelns beschränken. Eines der bedeutendsten Phänomene des Electronic Commerce ist die Entwicklung elektronischer Märkte.[17]

Eine weitere OECD Studie aus dem Jahr 1998 beschreibt das Einsparungspotential der Anbieter, wenn sie ihren Vertrieb von traditioneller Distribution auf elektronischen Geschäftsverkehr umstellen. Durch den Einsatz der neuen Technologie würden sich bei bestimmten Sparten Einsparungen bis zu 98 Prozent ergeben. Im folgenden sind die Einsparungspotentiale für die Schlüsselbranchen im elektronischen Geschäftsverkehr aufgezählt.

- Airlinetickets 87%
- Banking 88%
- Versicherung 50%
- SW-Distribution 98%

In einer Studie[18] der World Trade Organisation werden Schätzungen für das Jahr 2000 angeführt, wobei die WTO hier von einem Wert des elektronischen Geschäftsverkehr von 300 Milliarden US$ ausgeht. Nach einem anderen Bericht[19] wird eine Steigerung des Umsatzes von 8 Milliarden US$ im Jahr 1997 auf 333 Milliarden US$ für das Jahr 2002 erwartet, zu diesem Zeitpunkt soll der Handel über das Internet ein Prozent der Weltwirtschaft ausmachen.

---

[17] *Bichler/Kaukal/Werthner,* Elektronische Märkte – Ein neuer Trend in der betrieblichen Beschaffung, in: *Schweighofer/Menzel* (Hg.), E-Commerce und E-Government, aktuelle Fragestellungen der Rechtsinformatik, S. 13.

[18] Electronic Commerce and the Role of WTO, WTO Publication, 1998.

[19] *Borzo,* InfoWorld Electric, http://www.infoworld.com/cgi-bin/displayStory.pl?980511.eiecomm.htm.

Betrachtet man den Anstieg der verschiedenen Domainnames über die Jahre, kann man feststellen, daß seit Juli 1994 .com Domainnames die anderen Toplevel-Domains überflügelt haben. Waren bis dahin mehr Domains im Universitätsbereich zu finden, führt die rasant steigende Zunahme kommerzieller Server dazu, daß mittlerweile ungefähr doppelt so viele Server im kommerziellen Bereich wie im Wissenschaftsbereich zu finden sind. In jüngster Zeit häufen sich sogar die Klagen, daß es zuwenig freie Namensmöglichkeiten in der .com domain gibt. Der Vorschlag, neue Toplevel-Domains einzuführen, eine davon mit der bezeichnenden Endung store, ist sicher auch ein Indiz für die zunehmende Bedeutung des elektronischen Geschäftsverkehrs im Internet.

Dem Bereich der Kommunikation mit Behörden und Banken kommt nach Einschätzung von A-Trust[20] – einem österreichischeren Zertifizierungsdiensteanbieter – eine Initiierungsfunktion für die breite Anwendung sicherer elektronischer Kommunikation im Geschäftsverkehr zu. Am Anfang wird hauptsächlich die Kommunikation zwischen Banken und Großunternehmen einerseits und den Behörden andererseits gemäß den Anforderungen des SigG abgewickelt werden. Im Anschluß ist auch eine Verbreitung bei der Kommunikation von Unternehmen untereinander zu erwarten, und erst danach wird eine vermehrte Nachfrage privater Personen um Zertifikate für die private sichere elektronische Kommunikation einsetzen. Erste Erfolge konnten aber schon verbucht werden, da versucht wird, große Institutionen zur Verwendung von Zertifikaten bei der elektronischen Kommunikation ihrer Teilnehmer zu führen.[21] Die so in den Umlauf gebrachten Zertifikate können dann nicht nur zur betriebsinternen Kommunikation verwendet werden, sondern auch von den Teilnehmern für ihre private Kommunikation mit Dritten genutzt werden, da sie jeweils auf die Namen des jeweiligen Nutzers lauten.

---

[20] Vortrag von DI *Buczolich* anläßlich eines Workshops der Gemeinde Wien über elektronische Signaturen am 14.12.1999 in Wien.

[21] So wird die Wirtschaftsuniversität Wien bis zum Jahr 2001 alle ihre Studenten zertifizieren und Studentenausweise nur mehr in Form einer Smartcard ausgeben. Mit dieser Smartcard kann jeder Student nicht nur für Handlungen bezüglich seines Studiums, sondern auch im allgemeinen Rechts- und Geschäftsverkehr sicher elektronisch signieren. Ähnliche Projekte werden soeben für die Mitarbeiter der Telekom und die Mitglieder der österreichischen Wirtschaftskammer realisiert, nur wird hier an eine Beschränkung der Verwendung auf die interne Kommunikation gedacht.

1.1.3. Geschichte der Kryptographie

Eine grundlegende Rolle für die Verwirklichung des elektronischen Geschäftsverkehrs spielen technische Verfahren. Die Wurzeln der Kryptographie sind schon vor 4000 Jahren zu finden. Ungefähr aus dem Jahr 1900 vor Christus lassen sich erste kryptographische Umformungen auf Grabsteinen nachweisen.[22] *Julius Cäsar* wird um 60 vor Christus der erste bekannte Anwender von einfachen Ersetzungschiffren für militärische Angelegenheiten. Bis 1917 verlief die Weiterentwicklung sehr langsam. In diesem Jahr wurde von *Edward Hugh Hebern* die erste Rotormaschine entwickelt. Durch diesen Quantensprung konnten die komplizierten Ver- und Entschlüsselungsabläufe automatisiert und daher auch längere Texte schnell und effizient bearbeitet werden. Vor allem in der Kriegsführung und in Nachrichtendiensten kam es nach der Konstruktion immer komplexerer Maschinen mit bis zu fünf Rotoren zu vermehrten Einsatzmöglichkeiten.

Mit der Verfügbarkeit von Computern wurden noch komplexere Verschlüsselungsroutinen entwickelt. „Lucifer", das erste von IBM 1971 entwickelte Programm, führte schließlich 1975 zu der Entwicklung des Data Encryption Standard (DES), eines Algorithmus, der bis heute verwendet wird. Durch den Einsatz der EDV konnte die Anwendung von kryptographischen Routinen so einfach und schnell durchgeführt werden, daß sie nun auch für die wirtschaftliche Verwendung interessant wurden. Die Entwicklung immer schnellerer Rechner ermöglichte es andererseits aber auch, immer längere Schlüssel zu knacken. Die kryptographischen Routinen mußten daher immer längere Schlüssel verwenden. Dieser Kreislauf dauert bis heute an und wird sich durch Verbesserungen im Bereich der Informatik auch weiter fortsetzen.

„Die Entwicklung der Public-Key-Verschlüsselung ist die größte und vielleicht einzige echte Revolution in der gesamten Geschichte der Kryptographie. ... [Sie] stellt eine radikale Abzweigung vom bisher Dagewesenen dar."[23] 1976 erfolgte die erste Veröffentlichung[24] des Public-Key Konzepts durch *Whitfield Diffie* und *Martin Hellman*, die zu dieser Zeit beide an der Universität Stanford forschten. Zwei Jahre später wurde

---

[22] *Stallings*, Sicherheit in Datennetzen, S. 36.

[23] *Stallings*, Sicherheit in Datennetzen, S. 143.

[24] *Diffie/Hellman*, Multiuser Cryptographic Techniques, AFIPS National Computer Conference 1976, *Diffie/Hellman*, New Directions in Cryptography, IEEE Transactions on Information Theory, 1976.

von *Rivest, Shamir* und *Adleman* am MIT der bis heute in Verwendung stehende Algorithmus RSA entwickelt.

Durch die neue Funktionalität, die asymmetrische Kryptographie bietet, eignet sich der Einsatz von Verschlüsselungstechniken noch besser zum sicheren Nachrichtenaustausch in offenen Netzen. Die Kryptographie hat sich als Standard im Internet etabliert und dient speziell dem sicheren Austausch von Emails. Durch die vermehrte Verwendung für wirtschaftliche Zwecke fand in jüngster Zukunft eine verstärkte technische Normierung der Verfahren statt, die sich auch in Zukunft fortsetzen wird.

1.2. Bedarf der Beteiligten

Um die Sicherheit einer Email zu veranschaulichen, wird sehr gern der Vergleich mit normaler Postbeförderung gewählt. Eine Email hätte dabei grundsätzlich ungefähr dieselben Eigenschaften wie eine offene Postkarte, die mit Bleistift beschrieben wurde. In manchen Aspekten hinkt dieser Vergleich vielleicht ein wenig, kann aber in erster Näherung als gute Veranschaulichung verwendet werden.

Damit eine universelle Lesbarkeit gewährleistet ist, muß jede Applikation, die zum Schreiben und Lesen von Emails eingesetzt wird, dieselben Algorithmen befolgen. Das Umwandeln von verständlichem Text in einzelne TCP/IP Pakete folgt einem einheitlichen Schema durch die Verwendung der Standards SMTP[25] und MIME[26]. Dieser Prozeß kann auf jedem Computer, der mit der geeigneten Software ausgestattet ist, vom Anwender wieder rückgängig gemacht werden. Außerdem bildet die gemeinsame Verwendung einer Leitung für Daten verschiedener Sender und Empfänger eine weitere Grundlage der verschiedenen Internetdienste. Dadurch ist es aber auch jedem – wenn er an diese Leitung angebunden ist und über das vielfach bekannte Wissen verfügt, wie man Pakete, die an jemanden anderen adressiert sind, empfangen kann – möglich, alle Pakete oder die von bestimmten Sendern zu lesen, ja sogar abzufangen und vielleicht manipuliert weiter zu leiten. Untersucht man nur die Daten selbst, ist auf Grund ihres digitalen Charakters eine Manipulation nicht nachweisbar. Für Hacker, die über geeignete Kenntnisse und Programme verfügen, ist es also möglich, solche Schäden zu verursachen, wobei die Gefahr, als Schädiger ausgeforscht zu werden, geringer ist als bei physischer Fälschung von Schriftstücken.

---

[25] The SMTP Model: RFC-821 Section 2, ftp://ftp.isi.edu/in-notes/rfc821.txt.

[26] Major MIME Standards, ftp://ftp.isi.edu/in-notes/rfc2045.txt.

Hauptangriffspunkt sind meistens die Paßwörter der Benutzerberechtigungen, um bestimmte Ressourcen verwenden zu können, da man durch die Kenntnis des Paßwortes die gleichen Handlungsmöglichkeiten wie der berechtigte Anwender erlangt. Angriffsversuche auf offene Netzwerke erfolgen nahezu täglich.[27] Netzwerke durch Regeln über den richtigen Umgang mit Paßwörtern, Firewalls, SNMP und ähnliche Methoden abzusichern ist zwar eine Notwendigkeit, zur Aufrechterhaltung des Vertrauens in die Daten aber zuwenig, um diese effizient zu schützen. Die Informationen müssen vielmehr in sich selbst geschützt werden, so daß eine Manipulation sofort ersichtlich ist und auch sichergestellt wird, daß Daten nur von berechtigten Personen, in der Regel den Empfängern, gelesen und verstanden werden können. Wie dies möglich ist, soll in den nächsten Kapiteln ausführlich dargelegt werden.

Um breite Anwendung zu finden, muß der elektronische Geschäftsverkehr die Unterstützung der wesentlichen Eigenschaften für eine sichere Geschäftstätigkeit gewährleisten, wie es im traditionellen Geschäftsverkehr der Fall ist. Hier werden noch überwiegend Briefe für die Übermittlung von rechtsgeschäftlichen Willenserklärungen verwendet. Meistens handelt es sich um unterschriebene Dokumente, die in zugeklebten Kuverts befördert werden. Ihr Inhalt ist durch das im § 10 StGG[28] normierte Briefgeheimnis geschützt. Mit der Unterschrift setzen die Kommunikationspartner ein auch vor Gericht anerkanntes Zeichen, daß sie an den unterzeichneten Inhalt der Urkunde gebunden sein wollen.

Wenn man die Anforderungen untersucht, die an den Briefverkehr gestellt werden, findet man folgende Notwendigkeiten, die bei Verwendung von Briefen für die Kommunikationsteilnehmer wichtig sind, damit eine sichere Geschäftsabwicklung ermöglicht wird:

- Identifikation der einzelnen Teilnehmer
- Authentizität der Mitteilungen
- Vertraulichkeit der Übermittlung
- Unabstreitbarkeit von abgegebenen Willenserklärungen

---

[27] *Bellovin*, Packets found on an Internet, 1993, http://www.research.att.com/~smb/papers/packets.pdf
Bellovin, There Be Dragons, 1992, http://www.research.att.com/~smb/papers/dragon.pdf.

[28] Staatsgrundgesetz vom 21. Dezember 1867, über die allgemeinen Rechte der Staatsbürger für die im Reichsrate vertretenen Königreiche und Länder StF: RGBl. Nr. 142/1867, idF: BGBl. Nr. 684/1988.

Um diese Funktionalität auch bei elektronischer Nachrichtenübermittlung verwenden zu können, müssen die elektronischen Kommunikationsmethoden erweitert und angepaßt werden. Dabei erfolgt die Integration von neuen Verfahren und Technologien in das System, deren Anwendung die obengenannten Ziele auch bei Verwendung elektronischer Kommunikation erreichen läßt. Notwendig ist dafür sowohl eine Erweiterung der Programme, die in den Computern der einzelnen Anwender verwendet werden, als auch eine Anpassung der Infrastruktur des Internets und die Schaffung von Institutionen, die sichere Kommunikation am Netz ermöglichen. Nicht nur die technische Ausstattung ist zu komplimentieren, eine Aufklärung und Schulung der Anwender und der Juristen, die die Gültigkeit und Echtheit des elektronisch signierten Dokuments eventuell prüfen müssen, haben gewährleistet zu sein. Wer elektronische Signaturen verwendet, muß um die Unterschiede zur handschriftlichen Unterschrift und die sich daraus ergebenden Konsequenzen Bescheid wissen. Daher soll im nächsten Abschnitt ein Überblick über die Verfahren und Komponenten, die in einer Public Key Infrastructure zum Einsatz kommen, gegeben werden.

2. Die eingesetzten Verfahren und technischen Komponenten

2.1. Symmetrische Kryptographie

Die symmetrische Kryptographie, auch als herkömmliche Verschlüsselung bezeichnet, ist die ältere Form dieser Wissenschaft und war vor Erfindung der asymmetrischen Kryptographie die einzige Art der Verschlüsselung.

Bei der symmetrischen Kryptographie wird die ursprünglich verständliche Nachricht, im folgenden als Ausgangstext bezeichnet, in äußerlich offensichtlich zufälligen Unsinn verwandelt, chiffrierter Text genannt. Für das Verschlüsselungsverfahren benötigt man einen Algorithmus und einen Schlüssel, wobei dieser ein vom Inhalt des Ausgangstextes unabhängiger Wert ist und den Verschlüsselungsalgorithmus steuert. Je nach verwendetem Schlüssel erzeugt der Algorithmus bei gleichem Ausgangstext einen anderen chiffrierten Text. Viele Benützer können also denselben Algorithmus verwenden, erhalten aber wegen der verschiedenen Schlüssel unterschiedliche chiffrierte Texte. Es ist deswegen nicht notwendig, den Algorithmus geheimzuhalten, nur der Schlüssel darf nicht an Dritte weitergegeben werden. Die Prüfung des Algorithmus auf mögliche Schwachstellen durch viele Experten ist sogar äußerst wünschenswert, da so am besten mögliche Hintertüren[29] aufgedeckt werden können. Alle in dieser Arbeit vorgestellten Algorithmen wurden veröffentlicht und sind daher von einer großen Zahl von Fachleuten auf ihre Sicherheit geprüft worden. Oft werden Preise ausgeschrieben, die jene Personen erhalten, denen es gelingt, einen neu entwickelten Algorithmus zu brechen. ME sind veröffentlichte Algorithmen gegenüber Verschlüsselungstechniken, die sich darauf stützen, daß die angewandte Methode nicht bekannt ist, auf jeden Fall zu bevorzugen. Bei geheim gehaltenen Algorithmen ist nicht sichergestellt, ob sie nicht doch Schwächen aufweisen, die es einem Hacker ermöglichen, den chiffrierten Text auch ohne Kenntnis des Schlüssels wieder in Klartext umzuwandeln. Zusätzlich bietet die öffentliche Verfügbarkeit der Algorithmen den Vorteil, daß Chips mit Verschlüsselungsprogrammen in großer Zahl und daher billig hergestellt

---

[29] Diese als Hintertüren bezeichneten Schwachstellen ermöglichen es, den chiffrierten Text auch ohne Kenntnis des Schlüssels in den Ausgangstext zurückzuverwandeln.

werden können. Die frei erhältlichen Chips können dann in verschiedene Produkte integriert werden.

Grundlegend für die symmetrische Kryptographie ist, daß die beiden Kommunikationspartner den gleichen Schlüssel einmal zum Verschlüsseln und einmal zum Entschlüsseln verwenden. Jedem, der Kenntnis des Schlüssels hat, ist es möglich, an die verschlüsselten Informationen gelangen. Dadurch ergeben sich zwei Nachteile der symmetrischen Verschlüsselung:

Man kann mit neuen Kommunikationspartnern nicht direkt über das Internet verschlüsselte Botschaften austauschen, sondern muß vorher einen gemeinsamen Schlüssel vereinbaren. Diese Vereinbarung darf nicht über den gleichen Kanal geführt werden, der auch für die nachher ausgetauschten verschlüsselten Nachrichten verwendet wird, weil sonst beim Schlüsselaustausch mitgelauscht werden kann. Der Lauscher erfährt so den Schlüssel und hat damit Zugriff auf alle Informationen, die eigentlich zum Zweck der Vertraulichkeit verschlüsselt wurden. Man muß also für die Übermittlung des Schlüssels einen anderen, sicheren Weg wählen und ist dadurch wieder auf die Verwendung anderer Medien angewiesen. Zumindest einmal muß der Schlüssel über Telefon oder brieflich übermittelt werden, sichere Kommunikation zwischen Unbekannten nur unter Verwendung des Internets ist also nicht möglich.

Weiters wächst bei Kommunikation vieler Teilnehmer die Zahl der benötigten Schlüssel viel rascher[30] als bei asymmetrischer Kryptographie. Will jeder Teilnehmer mit jedem anderen unabhängig verschlüsselt kommunizieren, werden bei n Teilnehmern n*(n-1)/2 Schlüssel benötigt. Bei Verwendung asymmetrischer Kryptographie wäre hingegen die benötigte Anzahl unterschiedlicher Schlüsselpaare gleich der Teilnehmeranzahl, wie weiter unten dargelegt wird.

Einige Verfahren sollen im folgenden beschrieben werden. Weil symmetrische Kryptographie nicht zum Erstellen und Verifizieren elektronischer Signaturen herangezogen wird, sondern ausschließlich Methoden der asymmetrischen Kryptographie zur Anwendung kommen, finden sich keine Mindestanforderungen oder Festlegung von technischen Parametern in SigG und SigVO. Da aber die symmetrische Kryptographie grundlegende Funktionen für die sichere elektronische Kommunikation bereitstellt, sobald der Erstkontakt mittels asymmetrischer Kryptographie einmal hergestellt wurde, sollen die wichtigsten Algorithmen kurz vorgestellt werden.

---

[30] *Reiser,* Internet – die Sicherheitsfragen, S. 35.

2.1.1. Data Encryption Standard (DES)[31]

DES ist das zur Zeit am häufigsten eingesetzte Verschlüsselungsverfahren und basiert auf dem 1977 vom amerikanischen National Bureau of Standards, dem heutigen National Institute of Standards and Technology (NIST), herausgegebenen Federal Information Processing Standard 46 (FIPS PUB 46).[32]

DES beruht auf einem symmetrisches Verschlüsselungsverfahren. Die Daten werden in Blöcke zu je 64 Bit unterteilt und mit einem ebenfalls 64 langen Bit Schlüssel codiert. Von den 64 Schlüsselbits enthalten aber nur 56 die geheime Schlüsselinformation, die restlichen 8 Bit dienen als Prüfsumme für die Korrektheit der Schlüsseldaten. Die eigentliche Verschlüsselung geschieht in einem mehrere Schritte umfassenden Prozeß von Permutation und Iteration der Daten.

Auf Grund seiner einfachen Operationen läßt sich DES sehr gut in Hardware implementieren, die in großen Chargen und daher kostengünstig hergestellt werden kann. Aktuelle DES Chips erreichen einen Durchsatz von mehreren Gigabyte pro Sekunde. Auch bei Software-Implementierung von Verschlüsselungsalgorithmen erfreut sich DES großer Beliebtheit. So bietet zum Beispiel das in jedem Browser verwendete SSL Protokoll[33] die Möglichkeit, für die symmetrische Verschlüsselung innerhalb des Kommunikationsablaufes DES zu verwenden. Um DES in möglichst vielen Anwendungen sinnvoll benutzen zu können, wurden 4 verschiedene Betriebsarten von DES definiert.[34] Diese sollen buchstäblich alle möglichen Anwendungen der Verschlüsselung, für die DES eingesetzt werden könnte, abdecken. Je nach den Anforderungen an die Sicherheit und Schnelligkeit kann man die passende auswählen.

Das Verfahren resultiert aus einem 1971 von IBM entwickelten Verschlüsselungsstandard namens Lucifer. Allerdings wurde bei DES die ursprüngliche Schlüssellänge von 128 Bit auf 56 Bit gekürzt, einer der Hauptkritikpunkte, die sich gegen diesen Standard vorbringen lassen. DES kann heute nicht mehr als sehr sicher angesehen werden. NIST empfiehlt den Einsatz von DES bei Anwendungen, die nicht zum Schutz geheimer Informationen gedacht sind. *William Stalling* empfahl noch 1995 prinzipiell die Verwendung von DES für kommerzielle Anwendungen,

---

[31] *Stallings*, Sicherheit im Datennetz, S. 62ff.

[32] FIPS PUB 46, 1993, download: http://www.itl.nist.gov/fipspubs/fip46-2.htm.

[33] Siehe dazu weiter unten in dieser Arbeit.

[34] FIPS PUB 74 download: http://www.itl.nist.gov/fipspubs/fip74.htm.

außer in Bereichen höchster Sicherheit.[35] Da der Algorithmus aber 1997 mittels Brute Force Attack gebrochen wurde[36], ist mE der Einsatz von DES, außer in Bereichen, in denen man nicht-sensitive Informationen verschlüsselt, nicht mehr zu empfehlen. Das Heranziehen stärkerer Algorithmen ist für die Zukunft angebrachter. Mittlerweile hat sich bei den Experten im Bereich der Verschlüsselung die Meinung allgemein durchgesetzt, für sicherheitskritische Applikationen einfachen DES nicht mehr einzusetzen.

Ein weiterer Hauptkritikpunkt an DES ist, daß Teile der internen Strukturen des Verschlüsselungsablaufes, S-Boxen genannt, bis jetzt geheimgehalten werden. Der Algorithmus konnte daher nicht in seiner ganzen Tiefe von der Wissenschaft auf seine Stärke geprüft werden, und es besteht die Möglichkeit von unbekannten Schwachpunkten, die es der amerikanischen National Security Agency (NSA) ermöglichen könnten, Nachrichten zu dechiffrieren, ohne den Schlüssel zu besitzen.

2.1.2. Triple DES[37]

Die oft kritisierte zu kurze Schlüssellänge von DES führte zu einer Weiterentwicklung dieses Standards. Prinzipiell waren dabei zwei Wege möglich: entweder die Aufgabe der Algorithmen, die in DES verwendet werden, und die Entwicklung eines völlig neuen Verfahrens mit längeren Schlüsseln oder die Anpassung des DES-Verfahrens, um eine längere Schlüssellänge zu erreichen. Der erste Weg führte zur Entwicklung von IDEA und wird im nächsten Abschnitt behandelt. Der zweite Weg, Anpassung von DES, hat den Vorteil, daß auf die bewährten Teile von DES zurückgegriffen werden kann und der Entwicklungsaufwand dadurch verkürzt wird.

Die Anpassung erfolgte durch die Festlegung des Standards Triple DES. Dessen Grundprinzip beruht auf einem dreimaligen DES-Verschlüsselungsvorgang mit jeweils verschiedenen Schlüsseln. Die Blocklänge bei Triple DES beträgt ebenso wie bei DES 64 Bit, man erreicht daher insgesamt eine Schlüssellänge von 3 * 56 Bit = 168 Bit.

Auf Grund der Verwendung deutlich längerer Schlüssel gegenüber einfachem DES gibt es zur Zeit keine brauchbaren kryptoanalytischen Angriffe gegenüber dreifachem DES[38], eine Brute Force Schlüsselsuche

---

[35] *Stallings*, Sicherheit im Datennetz, S. 63.

[36] Näheres im Kapitel: Die Bedeutung der Schlüssellänge für sichere Kommunikation.

[37] *Stallings*, Sicherheit im Datennetz, S. 90ff.

[38] *Stallings*, Sicherheit im Datennetz, S. 93.

würde eine Größenordnung von $2^{168} = 4 \times 10^{50}$ Versuchen benötigen.[39] Daher wurde dreifacher DES in eine Reihe von Schlüsselverwaltungsstandards[40] aufgenommen und wird auch in Privacy Enhanced Mail (PEM) verwendet.

2.1.3. International Data Encryption Algorythm (IDEA)[41]

Bei IDEA handelt es sich ebenfalls um einen block-orientierten, symmetrischen Verschlüsselungsalgorithmus. Er wurde 1990 von *Lei* und *Massey*[42] am Swiss Federal Institute of Technology entwickelt. Eine verbesserte Version von IDEA, die stärker gegen kryptoanalytische Angriffe abgesichert ist, wurde 1991 von den gleichen Wissenschaftlern veröffentlicht.[43] IDEA arbeitet ebenfalls mit 64 Bit Datenblöcken, verwendet aber generell eine Schlüssellänge von 128 Bit. Die Schlüssellänge und andere Spezifika von IDEA führen dazu, daß dieser Algorithmus als sehr sicher eingestuft wird und sehr oft als bester Nachfolger für DES genannt wird. *Stallings*[44] spricht überhaupt von IDEA als dem vielversprechendsten Vorschlag im Vergleich zu anderen symmetrischen Verschlüsselungsverfahren.

IDEA ist in den USA und den meisten europäischen Ländern patentiert. Das Patent wird von der Ascom Systec AG[45] gehalten. Die kommerzielle Nutzung ist kostenpflichtig, die freie Verwendung in nicht kommerziellen Anwendung ist gestattet. Alleine die Implementierung von IDEA in PGP sorgt für eine weltweite Verbreitung.

---

[39] *Coppersmith*, The Data Encryption Standard and its Strength Against Attacks, IBM Research Report RC 18613 (81421).

[40] ANSI X9.17-1985, „Financial Institution Key Management (Wholesale)," X9 Secretariat, American Bankers Association, 1985, ISO 8732 Key Management.

[41] *Stallings*, Sicherheit im Datennetz, S. 352, C'T Report, Geld Online 2 (1997), S. 23.

[42] *Lei/Massey*, A Proposal for a new Block Encryption Standard, Proceedings zu EUROCRYPT 1990.

[43] *Lei/Massey*, Markov Ciphers and Differential Cryptoanalysis, Proceedings zu EUROCRYPT 1991.

[44] *Stallings*, Sicherheit im Datennetz, S. 352.

[45] http://www.ascom.com/index-js.html.

2.2. Asymmetrische Kryptographie

2.2.1. Funktionsweise von Public Key Infrastrukturen[46]

Das grundlegende Prinzip der symmetrischen Kryptographie, die Verwendung desselben geheimen Schlüssels zur Chiffrierung und Dechiffrierung, führt zu vier systemimmanenten Nachteilen:

- Wie schon weiter oben erwähnt kann der Schlüsselaustausch nicht über dasselbe Kommunikationsmedium, welches später für die Übermittlung der verschlüsselten Information verwendet wird, erfolgen. Sonst wäre ja ein Belauschen dieses Austausches durch Dritte nicht auszuschließen und die ganze Verschlüsselung verliert ihren Sinn, da der Dritte ebenso leicht den Klartext reproduzieren kann.
- Weiters braucht jeder für die Kommunikation mit jedem anderen einen eigenen, proprietären Schlüssel. Faktisch würde das die Schlüsselverwaltung schnell an ihre Leistungsgrenzen[47] heranführen. Wäre das für Privatpersonen eventuell noch administrierbar, da sie wohl selten mehr als hundert verschiedene Kommunikationspartner haben, können Unternehmen wie Banken oder Behörden wohl kaum ihren Millionen von Kunden je einen eigenen geheimen Schlüssel zuordnen und diesen schützen und verwalten.
- Zusätzlich bietet die symmetrische Kryptographie außer der reinen Verschlüsselung keinerlei weitere Funktionalität, der Einsatz von Verschlüsselungstechniken für wirtschaftliche Zwecke bedarf aber auch der Funktionalität einer elektronischen Unterschrift.
- Schlußendlich ist bei der Verwendung symmetrischer Kryptographie der geheime Schlüssel beiden Kommunikationspartner bekannt. Man kann sich daher nie sicher sein, daß nicht der jeweils andere den Schlüssel weitergibt.[48] Bei der asymmetrischen Kryptographie hingegen ist jeder einzelne alleine über seinen privaten Schlüssel verfügungsbefugt und kann sich sicher sein, daß niemand anderer seinen privaten Schlüssel kennen kann[49], solange er ihn ordnungsgemäß verwahrt.

---

[46] *Stallings*, Sicherheit im Datennetz, S. 145ff.

[47] *Reiser*, Internet – die Sicherheitsfragen, S. 35.

[48] *Mayer-Schönberger/Pilz/Reiser/Schmölzer*, Signaturgesetz, S. 5.

[49] Zu Problemen bei der Gewährleistung der vollständigen Kontrolle des Signators über seinen privaten Schlüssel siehe: *Telekom-Control-Kommission*, Konsultation zu

Diffie und *Hellman* begannen 1975 mit der Suche nach einer Lösung für die generell formulierte Problemstellung: „Ist es möglich, eine Methode zu finden, die zur Zufriedenheit aller beweisen kann, daß eine digitale Nachricht von einer bestimmten Person stammt?" Im Jahr 1976 gelang den beiden schließlich der Durchbruch mit der Einführung der asymmetrischen Kryptographie, einer grundlegenden Revolution innerhalb der Wissenschaft der Kryptographie.

Die zur Ver- und Entschlüsselung verwendeten Schlüssel sind nicht mehr gleich, sondern es wird ein Schlüsselpaar verwendet. Der eine Schlüssel dient zur Verschlüsselung, mit dem korrespondierenden zweiten Schlüssel wird der chiffrierte Code wieder in Klartext zurück verwandelt, wobei gilt, daß es rechnerisch nicht möglich ist, den Entschlüsselungsschlüssel nur auf Grundlage des kryptographischen Algorithmus und des Verschlüsselungsschlüssels zu bestimmen. Weiters gilt bei den meisten Algorithmen, wie zum Beispiel RSA, daß jeder der beiden Schlüssel zur Verschlüsselung verwendet werden kann, mit dem jeweils anderen Schlüssel erfolgt dann die Entschlüsselung.[50]

Jeder Kommunikationsteilnehmer generiert sich nun ein Schlüsselpaar zur Ver- und Entschlüsselung von Informationen, die gesendet oder empfangen werden. Einer dieser Schlüssel wird veröffentlicht, so daß jeder darauf zugreifen kann. Der andere Schlüssel darf nicht weitergegeben werden, nur der Unterzeichner darf auf diesen Schlüssel Zugriffsmöglichkeit haben. Man bezeichnet die beiden Schlüssel daher auch als öffentlichen und privaten Schlüssel, wobei zur Unterscheidung symmetrische Schlüssel geheime Schlüssel genannt werden. Die SigRL bezeichnet den privaten Schlüssel als Signaturerstellungseinheit und den öffentlichen als Signaturprüfeinheit. Auf diese Weise stehen zwei verschiedene Möglichkeiten zur Verfügung:

- Die Nachricht kann vom Sender mit seinem privaten Schlüssel chiffriert[51] werden, oder
- sie wird von ihm mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.
- Auch die Kombination beider Methoden ist möglich.

---

den Anforderungen des Signaturgesetzes an die Geräte der Endbenutzer, S. 12, http://www.tkc.at.

[50] *Pohl*,Guidelines for the use of names and keys in a global TTP infrastructure, S. 15.

[51] *Telekom-Control-GmbH*, Wie funktionieren elektronische Signaturen? http://www.tkc.at/WWW/Signatur.nsf/pages/funktion.

Diese beiden Arbeitsweisen bilden die Basis für eine sichere elektronische Kommunikation, die Authentizität und Vertraulichkeit gewährleistet. Um wieder zu dem am Anfang gebrachten Vergleich zurückzukehren: der Gebrauch asymmetrischer Kryptographie ermöglicht erstmalig die analoge Verwendung von Briefumschlägen und Kugelschreibern im Internet.

2.2.1.1. Authentizität

Um Authentizität zu gewährleisten, muß sichergestellt sein, daß die Nachricht vom Aussteller persönlich verfaßt wurde. Ausgehend von der Grundlage, daß niemand seinen privaten Schlüssel an Dritte weitergibt, wird das folgendermaßen erreicht: Der Sender und Verfasser einer Nachricht verschlüsselt den Text oder auch andere multimediale Daten mit seinem privaten Schlüssel vor dem Verschicken. Der Empfänger erhält die Nachricht mit einem Hinweis auf den Absender und den Namen von dessen Schlüsselpaar. Er besorgt sich nun den öffentlichen Schlüssel des Senders, der in speziellen Datenbanken, sogenannten key-servern[52] gespeichert ist, und entschlüsselt mit diesem die übermittelte Information. Da eine Entschlüsselung mit sinnvollem Ergebnis nur möglich ist, wenn der öffentliche Schlüssel zu dem einzigartigen privaten Schlüssel paßt, erreicht der Empfänger Gewißheit, daß die Datei wirklich von demjenigen stammt, der eine Verfügungsberechtigung für den korrespondierenden Schlüssel hat. Die Information ist authentisch.

2.2.1.2. Vertraulichkeit

Zum Versenden vertraulicher E-Mails[53] ist der logisch umgekehrte Weg zu beschreiten. Der Sender der Nachricht verschlüsselt die Information mit dem öffentlichen Schlüssel des Empfängers, den er sich vorher von einem Key-Server besorgt hat, bevor er die Nachricht versendet. Durch das Verschlüsseln kann kein Dritter vom äußerlich offensichtlich unsinnigen, verschlüsselten Text auf den Klartext rückschließen. Die Dechiffrierung des Textes ist nur mit dem privaten Schlüssel des Empfängers möglich, der in seinem alleinigen Besitz ist. Dadurch wird sichergestellt, daß die Nachricht nur vom Empfänger gelesen werden kann.

---

[52] Wie zB den Server der Arge Daten: https://keyserver.ad.or.at/key/search.html.

[53] *Raab/Williams*, Privacy in the GII: Issues, processes and solutions, Proceedings of the Joint IFIP WG 8.5 and WG 9.6 Working Conference 1999, S. 161.

Will man nun eine Nachricht verschlüsselt senden und auch die Authentizität gewährleisten, so wendet man einfach beide Verfahren hintereinander auf den Text an. Zuerst kommt daher die Verschlüsselung des Ausgangstextes mit dem privaten Schlüssel des Senders, um die Authentizität zu gewährleisten, nachher wird dieser einmal verschlüsselte Text noch einmal mit dem öffentlichen Schlüssel des Empfängers chiffriert. Die jetzt abgeschickte Nachricht ist nun vertraulich und authentisch.

Technisch kann also ein und dasselbe Schlüsselpaar für elektronisches Signieren und zum Verschlüsseln zur Sicherstellung der Vertraulichkeit verwendet werden. Im SigG wird allerdings angeordnet, daß Signaturerstellungsdaten und Signaturprüfdaten – also privater und öffentlicher Schlüssel bei der Verwendung asymmetrischer Kryptographie – ausschließlich zum Signieren verwendet werden. Will man also Vertraulichkeit erreichen, muß noch ein zweites Schlüsselpaar, das nicht im Hauptzertifikat an den Namen des Signators gebunden ist, in der Signaturerstellungseinheit implementiert sein. Dieses zweite Paar darf dann ausschließlich zum Verschlüsseln und Entschlüsseln für die Erlangung von Vertraulichkeit verwendet werden.

2.2.2. Die eingesetzten Verfahren

Das österreichische Signaturgesetz geht mit der Signaturrichtlinie übereinstimmend von einem technologieneutralen Ansatz aus. Theoretisch müssen nicht einmal Verfahren der asymmetrischen Kryptographie eingesetzt werden, um elektronische Signaturen zu erzeugen. Beim gegenwärtigen Stand der Technik ist aber ausschließlich vom Einsatz von Methoden der asymmetrischen Kryptographie auszugehen, da noch keine andere Technologie die Anforderungen, die durch die rechtlichen Regelungen gestellt werden, erfüllen kann. Daher finden sich auch in der SigVO nähere Regelungen über die einzusetzenden technischen Komponenten und Verfahren, die sich ausschließlich auf asymmetrische Kryptographie beziehen. Die in der SigVO als sicher eingestuften Komponenten und Verfahren sollen im folgenden und im Abschnitt über die Hashverfahren vorgestellt werden. Die jeweiligen Auflagen, die durch die SigVO normiert werden, sind bei den jeweiligen Verfahren eingearbeitet.

2.2.2.1. RSA[54]

Dieser Algorithmus wurde nach seinen Entwicklern *Ron Rivest, Adi Shamir* und *Len Adleman* benannt, die ihn 1977 am MIT entwickelten. RSA ist der am weitesten verbreitete, meist implementierte und am besten untersuchte Algorithmus zur Public-Key-Verschlüsselung. Er ist sowohl zum Verschlüsseln als auch zum elektronisch Signieren von Daten gleichermaßen geeignet. In den USA ist RSA bis zum Jahr 2000 patentiert, ansonsten aber frei nutzbar.

Die Sicherheit von RSA gegenüber einem kryptoanalytischen Angriff ist bei der Verwendung entsprechend dimensionierter Schlüssel, die zumindest 1 kB lang[55] sein sollten, gewährleistet. Mathematisch basiert der Algorithmus auf dem Produkt zweier großer, zufällig gewählter Primzahlen, diese Zahlen bilden in Verbindung mit zwei anderen Zahlen – den public und private exponents – den öffentlichen und privaten Schlüssel.[56] Die Sicherheit gegenüber kryptoanalytischen und Brute-Force Angriffen beruht auf der Schwierigkeit der Faktorisierung großer Zahlen. Näheres folgt dazu unten bei den Ausführungen über die Bedeutung der Schlüssellänge.

Der Quellcode von RSA ist offengelegt und wurde von zahlreichen Wissenschaftlern auf Schwächen und Hintertüren untersucht. Dadurch ist die ziemlich hohe Sicherheit gegeben, daß die Schwierigkeit von Angriffen nicht durch neue kryptoanalytische Verfahren umgangen werden kann. RSA wird von SSL unterstützt und in zahllosen Computerprogrammen, wie zum Beispiel PGP, Netscape Navigator oder Krypto Chips, verwendet. Der neueste Trend ist, den RSA Krypto Chip direkt auf einer Smart Card zu implementieren[57], damit sensitive Daten, wie der PIN-Code für den Geldautomaten, nur mehr innerhalb der Bankomatkarte unverschlüsselt vorliegen. Wird mittels einer solchen Karte signiert, bleibt der private Schlüssel ausschließlich innerhalb der Karte. Das Schlüsselpaar wird auf der Karte erzeugt, und nur der öffentliche Schlüssel wird nachher übertragen. Bei jedem Signiervorgang wird der zu verschlüsselnde Hashwert in den Kartenprozessor geladen und dort verschlüsselt. Der verschlüsselte Hashwert, auch Chiffrat genannt, der die eigentliche elek-

---

[54] *Stallings,* Sicherheit im Datennetz, S. 160ff.

[55] *Horster/Schartner/Wohlmacher,* Keymanagment, Proceedings of the XV. IFIP World Computer Congress 1998, S. 40.

[56] *Brown,* Techniques for Implementing the RSA Public Key Cryptosystem, Computer Science Department Report, http://www.uni-siegen.de/security/krypto/rsa-tr-cs87-7.txt.

[57] *Rhein,* Digitale Signatur mittels Smart Cards, S. 44.

tronische Signatur darstellt, wird wieder von der Karte an das Gerät des Signators übertragen und von dort versandt. Dadurch ist sichergestellt, daß niemand – nicht einmal der Signator selbst – den privaten Schlüssel kennt und mißbräuchlich verwenden kann. Wird dafür sogar eine Java-fähige Smart Card eingesetzt, kann der Anwender auf einer Karte mehrere verschiedene Applikationen verwenden, wie zum Beispiel mehrere verschiedene elektronische Geldbörsen.

Die SigVO gibt bei der Verwendung von RSA für sichere elektronische Signaturen in Anhang 1 eine Mindestlänge des Schlüssels von 1024 bit vor, davon müssen 1023 bit durch tatsächliche Zufallselemente beeinflußt sein. Zu berücksichtigen ist aber auch § 18 Abs. 2 SigG, der vorgibt, daß Signaturerstellungsdaten mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen dürfen. Dies kann gewährleistet werden, indem bestimmte Teile des Signaturschlüssels (etwa die ersten 16 bit) vom Zertifizierungsdiensteanbieter numeriert werden, durch die fortlaufende Nummerierung ist die Einzigartigkeit jedes Schlüssels garantiert, auch wenn der zufällig gebildete Teil zweier Schlüsselpaare gleich sein sollte.[58] Da nach Anhang 1 zumindest 1023 bit des Schlüssels vom tatsächlichen Zufallselement beeinflußt werden, verlängert sich die gesamte Schlüsselmindestlänge dann mE um die angefügten Nummerierungsbits.

2.2.2.2. Digital Signature Algorithmus (DSA)[59]

So bietet RSA also eine Variante der sicheren asymmetrischen Verschlüsselung. Von der Regierung der Vereinigten Staaten wurde ein anderer Standard angeregt, da sie, aber auch einige europäische Staaten gegenüber der uneingeschränkten Verwendung starker Kryptographie zur Verschlüsselung von Daten ohne Schlüsselhinterlegung sehr skeptisch eingestellt sind. Von diesen Regierungen wird die These vertreten, daß die breite Verwendung von starker Verschlüsselung die Rechtsdurchsetzung verhindert, da Verbrecherorganisationen belastendes Material durch Verschlüsselung wirksam den Gerichten entziehen können. Digitales Signieren, das heißt Verschlüsselung nur des Hashwertes des Dokuments mit dem Private Key des Absenders und Versenden des unverschlüsselten Dokuments inklusive des verschlüsselten Hashwertes, wodurch die Lesbarkeit für alle erhalten bleibt, ist gewünscht, die Verschlüsselung mit

---

[58] *Horster/Schartner/Wohlmacher*, Keymanagment, Proceedings of the XV. IFIP World Computer Congress 1998, S. 40.

[59] *Stallings*, Sicherheit im Datennetz, S. 424ff
http://www.itl.nist.gov/div897/pubs/fip186.htm.

dem Public Key des Adressaten, die die Geheimhaltung gewährleistet, wird aber von diesen Regierungen als schädlich angesehen. Die duale Nutzbarkeit – sowohl signieren als auch vertraulich verschlüsseln – liegt RSA aber zugrunde. Es ist bei diesem Algorithmus nicht möglich, nur das Signieren zu ermöglichen, das Verschlüsseln aber zu unterbinden.

Deswegen veröffentlichte das amerikanische National Institute of Standards and Technology (NIST) 1994 einen neuen Algorithmus, den Digital Signature Standard (DSA).[60] Wesentlichste Motivation zur Entwicklung dieses Standards war es, ein Verfahren anzubieten, das hohe Sicherheitsstandards im Bereich des elektronischen Signierens bietet, aber möglichst nicht für die Verschlüsselung von Daten eingesetzt werden kann.[61] Die erste Version sahen Fachleuten noch als zu unsicher an, daher wurde 1993 eine überarbeitete Version vorgelegt. Ende 1998 wurde eine weitere Verbesserung durch das NIST verlautbart.[62] DSA verwendet einen Algorithmus, der nur auf die Funktion der digitalen Signatur ausgelegt ist. Im Gegensatz zu RSA kann er nicht auch zur Verschlüsselung herangezogen werden. Trotzdem handelt es sich um ein Public Key Verfahren.

Zur Generierung des Hashwertes verwendet DSA immer das Hashverfahren SHA 1, das im nächsten Abschnitt vorgestellt wird. Dieses Hashverfahren ist auch mit den Bestimmungen der Signaturverordnung kompatibel. Zur Verschlüsselung des Hashwertes kann nun entweder der RSA Algorithmus innerhalb von DSA eingesetzt werden, allerdings bietet sich auch die Möglichkeit, als zweite Variante alternativ Verfahren auf der Grundlage elliptischer Kurven anzuwenden. Auf Grund eines anderen mathematischen Verfahrens bieten hier auch schon geringere Schlüssellängen als bei Einsatz von RSA gleiche Sicherheit gegenüber Brute Force Attacken. Deswegen genügt auch die Verwendung von Schlüsseln mit einer Mindestlänge von 160 Bit, um Konformität mit dem Anhang 1 der SigVO zu gewährleisten. Wird RSA innerhalb von DSA verwendet, gelten die gleichen Mindestlängen wie bei ursprünglicher Verwendung von RSA. Auch bei der Verwendung von Teilen der Schlüsselbits für Nummerierungszwecke gilt mE das oben Ausgeführte.

---

[60] Federal Information Processing Standard (FIPS) 186 vom 19.5.1994, download unter: http://www.itl.nist.gov/div897/pubs/fip186.htm.

[61] *Posch*, Digitale Signatur und Zertifizierung, Vortrag im Rahmen des OCG und IAIK Arbeitskreises IT-Sicherheit, Folien verfügbar unter: http://akitsicherheit.iaik.tu-graz.ac.at/Tagung101097/rposch/sld005.htm.

[62] Federal Information Processing Standard (FIPS) 186-1 vom 15.12.1998, download unter: http://csrc.nist.gov/fips/.

Ein weiterer Nachteil ist, daß das genaue Design von DSA nie offengelegt wurde, der Algorithmus konnte daher auch nie von unabhängigen Experten und Wissenschaftlern überprüft werden. Da der Evaluierung der Routinen durch Experten eine besonders große Bedeutung zur Aufdekkung von Sicherheitsrisiken zukommt und es trotz Geheimhaltung des Verfahrens gelang, potentielle Probleme und Schwachstellen bei der Benutzung von DSA aufzuzeigen[63], ist von einer Benutzung dieses Algorithmus eher abzuraten.

Die US Regierung hält ein Patent auf DSA, wobei die Benutzung derzeit frei ist.

2.3. Die Bedeutung der Schlüssellänge für sichere Kommunikation

Elektronisch signierte Daten liegen, wie der Name schon sagt, nur in digitaler Form vor. Findet also jemand den privaten Schlüssel einer Person heraus, kann er, durch graphologische und sonstige Gutachten nicht nachweisbar, im Namen dieser Person handeln. Eine gefälschte Unterschrift kann immer noch durch Gutachter als solche aufgedeckt werden. Dies ist bei der elektronischen Signatur nicht möglich; solange der Zugriff auf den privaten Schlüssel nicht auch noch durch biometrische Überprüfung gesichert ist, kann jeder, der die Kenntnis über den privaten Schlüssel einer fremden Person durch Weitergabe des Paßwortes kennt, in deren Namen handeln. Dem Schutz der Schlüssel kommt daher höchste Bedeutung zu. Auf biometrische Verifikation als Schutz vor Schlüsselweitergabe soll weiter unten im Text genau eingegangen werden.

Eine andere Möglichkeit, einen unbekannten Schlüssel zu knacken, besteht darin, einfach alle möglichen Kombinationen, den sogenannten Schlüsselraum, durchzuprobieren, um herauszufinden, ob einer der zufällig gewählten Schlüssel „paßt".

Die Schlüssellänge wird in Bits angegeben, daher gibt es vom Binärins Dezimalsystem umgerechnet für jeden Schlüssel immer zwei hoch der Bitanzahl mögliche Schlüssel. Das wären dann bei einem 56 Bit DES-Schlüssel $7 * 10^{16}$ Möglichkeiten. Für moderne Rechner, die in einem Netzwerkverbund gemeinsam am Durchprobieren arbeiten, ist es kein großer Aufwand, einen Schlüssel mit 56 Bit Länge herauszufinden. So

---

[63] Security Server der Universität-Gesamthochschule Siegen: http://www.uni-siegen.de/security/krypto/dss.html.

setzte die RSA Data Security Inc[64] im März 1997 einen Preis in der Höhe von 10.000 Dollar für das Auffinden eines geheimen DES Schlüssels aus. Nach nur 97 Tagen Suchzeit wurde der passende Schlüssel gefunden und der verschlüsselte Text

„Strong cryptography makes the world a safer place."

wurde veröffentlicht. Die Suche hatten 78.000 Rechner, zu einem umfassenden Verbund zusammengeschlossen, durchgeführt. Der Rechner, der den passenden Schlüssel nach dem Durchsuchen von 26 % des Schlüsselraumes fand, war ein PC mit einem Pentium 90 Prozessor und 16 MB RAM.

Nur ein gutes Jahr später hat sich die Zeit für einen erfolgreichen Brute Force Angriff gegen DES-Schlüssels durch die Verwendung günstigerer Hardware noch einmal drastisch verkürzt. Der Electronic Frontier Foundation[65] gelang, es die richtigen 56 Bit des Schlüssels in nur 56 Stunden herauszufinden.[66] Durchgeführt wurde der Angriff mit einem selbstgebauten Massiv-Parallelrechner aus 1000 Prozessoren, der nur 250.000 US-Dollar kostete. Experten berechneten, daß die Aufwendungen für das Knacken pro DES-Schlüssel nur 700 US-Dollar betragen. Man sollte DES daher auf keinen Fall mehr zum Schutz sensitiver Informationen verwenden. *Robert Hettinga* bringt es, dramatisch formuliert, auf den Punkt : „DES is dead".

Auch asymmetrische Schlüsselpaare des RSA Algorithmus sind zu knacken. Im Moment ist die Grenze, bei deren Überschreitung ein Schlüssel bei Anwendung heute zu Verfügung stehender Technologien geknackt werden kann, bei mehr als 512 Bit. Hier liegt die Lösung des Problems, daß man das von RSA verwendet Produkt zweier Primzahlen faktorisieren kann, das heißt die zwei einzigen passenden Primzahlen zu finden, die dieses Produkt bilden können. Da bis jetzt noch kein mathematisches Verfahren gefunden wurde, wie diese Primzahlen durch eine Gesetzmäßigkeit herausgefunden werden können, müssen alle möglichen Kombinationen bei einer Brute Force Attacke ausprobiert werden. Bei 512 Bit Schlüssellänge hat die zu untersuchende Zahl im Dezimalsystem 152 Stellen. Trotzdem ist es auch unlängst gelungen, einen solchen Schlüssel zu knakken. Der Aufwand war höher als bei dem Experiment mit DES, so muß-

---

[64] RSA Data Security Secret Key Challenge:
http://www.rsasecurity.com/rsalabs/challenges/secretkey/secret-key.html.

[65] http://www.eff.org.

[66] http://www.heise.de/newsticker/data/fr-17.07.98-000/.

ten an die 300 schnelle Workstation – Rechner 35 Jahre daran arbeiten.[67] Trotzdem vertreten Experten die Meinung, daß nun auch Asymmetrische Schlüsselpaare des RSA Algorithmus eine Mindestlänge von 1024 Bit aufweisen sollen und die Verwendung kürzerer Schlüssellängen (insbesondere die noch weit verbreiteten 512 Bit RSA-Schlüssel) bei sicherheitskritischen Anwendungen dringend zu vermeiden sei.

Theoretisch kann natürlich jeder Schlüssel beliebiger Länge irgendwann einmal herausgefunden werden. Ein Schlüssel ist jedoch dann sicher, wenn die Kosten für das Herausfinden erheblich höher sind als der Nutzen, den man durch die Kenntnis des Schlüssels erlangt. *M. Wiener* hat sich sehr ausführlich mit der Brute Force Attacke auf DES Schlüssel beschäftigt.[68] Er kommt 1993 auf folgende Werte, wobei man für die Gegenwart noch berücksichtigen muß, daß die Hardwarepreise laufend fallen:

Kosten der Schlüsselsuchmaschine	Erwartete Suchzeit
100.000 Dollar	35 Stunden
1.000.000 Dollar	3,5 Stunden
10.000.000 Dollar	21 Minuten

DES entspricht bei der heutigen Technik daher nicht mehr den gängigen Sicherheitsstandards, um vor einem Brute-Force Angriff sicher zu sein. Besonders bei konfidenten Daten, wie zum Beispiel im Bankbereich, ist bei Verwendung symmetrischer Kryptographie eine Schlüssellänge von mindestens 128 Bit zu empfehlen, wie es bei Triple DES oder IDEA der Fall ist.

Auch die Rechtsprechung dürfte die Schwächen von DES erkannt haben. So war es bis vor kurzem ständige Judikatur, daß bei Geldabhebungen mittels gestohlener EC-Karten der PIN Code vom Täter weitgehend nur durch Unachtsamkeit des Opfers ermittelt werden konnte, er daher auch für den entstandenen Schaden haftet. Erst das Urteil des deutschen OLG Hamm vom 17. 3. 1997[69] führte durch die Aussage, „... daß ein Täter auch ohne Mitwirkung des Karteninhabers Kenntnis von der PIN ... durch Entschlüsselung anhand der auf der Karte abgespeicherten Daten erlangt haben kann", zu einer Wende in der Judikatur. Der Sachverständi-

---

[67] Pressemitteilung des CWI Amsterdam, Security of E-Commerce threatened by 512 bit number factorisation, download unter: http://www.cwi.nl/~kik/persb-UK.html.

[68] *Wiener*, Efficient DES Key Search, Proceedings zur Crypto 1993.

[69] OLG Hamm vom 17.3.1997, Az: 31 U 72/96 abgedruckt zB in: DuD (1997), S. 540.

ge legte dar, daß die PIN aus einer Zahl mit 64 Bit, die mit einfachem DES verschlüsselt wird, errechnet wird. Durch die Umwandlung hexadezimaler Werte in die dezimal aufgebaute PIN und die schwache Verschlüsselung ist nur ein sehr kleiner Schlüsselraum vorhanden, kennt der Täter das Verfahren, wie der PIN generiert wird, kann er bei dreimaligem Versuch mit einer Wahrscheinlichkeit von 1:150 auf die richtige PIN treffen.[70]

Bei asymmetrischer Kryptographie werden grundsätzlich längere Schlüssel angewendet, da Public Key Systeme von der Verwendung einer Art umkehrbarer mathematischer Funktion abhängig sind. Durch Verwendung kryptoanalytischer Methoden wären daher Schlüssel unter 512 Bit Länge leicht herauszufinden. Im Moment empfiehlt sich eine Schlüssellänge von 1024 bis 2048 Bit. Bei Verwendung eines Schlüssels mit 1024 Bit ergeben sich $1{,}8 * 10^{308}$ Möglichkeiten, man würde ungefähr 10^{30} Rechenoperationen benötigen, um diese Zahl in ihre Primfaktoren zu zerlegen. Eine Zahl mit nur 200 Stellen zu zerlegen würde bei einer Leistung von 10^{12} Rechenoperationen pro Sekunde – was selbst von den teuersten und leistungsfähigsten Computern heute nicht erreicht wird – etwa 1000 Jahre dauern.[71] Durch Verwendung von 300 Stellen und mehr verbleibt für die nächsten Jahre ein genügend großer Spielraum, um auch gegen Angriffe mit zukünftigen leistungsfähigeren Computern gesichert zu sein. Man sieht hier wieder, daß es zwar statistisch betrachtet möglich ist, Schlüssel solcher Länge durch Brute Force Attacken zu knacken, wirtschaftlich aber dazu keine Verwirklichung besteht. Solche Schlüssel werden als berechnungssicher bezeichnet.[72] Sie müssen zwei Kriterien erfüllen:

- Der Aufwand zum Knacken des Codes übersteigt den Wert der verschlüsselten Information.
- Die zum Knacken des Chiffres benötigte Zeit übersteigt die Dauer der Brauchbarkeit der Information.

Auf Grund der schnellen Änderung der Technik wurde eine Mindestlänge für Schlüssel, die zur Erzeugung von sicheren elektronischen Signaturen verwendet werden, nicht in SigG oder SigRL festgelegt, sondern ist nur in der SigVO zu finden, die im Bedarfsfall durch ein einfacheres

---

[70] *Hortmann*, Wie sicher ist die PIN? DuD (1997), S. 532.

[71] *Nechvatal*, Public Key Cryptography, in: *Simmons* (Hg.), Contemporary Cryptology: The Science of Information Integrity.

[72] *Stallings*, Sicherheit im Datennetz, S. 42.

Verfahren abgeändert werden kann. Anhang 1 leg. cit. legt eine Mindestlänge von 1024 Bit für RSA Schlüssel fest und definiert 190 Bit als die Mindestlänge für Schlüssel, die der Steuerung von Algorithmen dienen, die das Verfahren elliptischer Kurven benutzen. Weiters wurde die Geltung dieses Schwellenwerts auch zeitlich befristet. Schlüssel dieser Mindestlänge sind gemäß Anhang 1 der SigVO nur bis 31.12.2005 als sicher im Sinne des § 18 SigG anzusehen. Danach erfolgt durch ein Expertenteam eine Neubewertung der Situation, auf Grund derer durch die SigVO neue Mindestlängen festgelegt werden.

2.4. Kombinierte Verwendung symmetrischer und asymmetrischer Kryptographie

Asymmetrische Ver- und Entschlüsselung erfordert ungleich mehr Rechenaufwand als Verschlüsselung mit symmetrischen Algorithmen. Der Text von Emails wird kurz vor dem Senden verschlüsselt. Hier werden alle Daten durchgängig mit dem asymmetrischen Algorithmus verschlüsselt und dann verschickt, wenn der Sender auch die Vertraulichkeit des Inhalts bezweckt. Es kommen daher nur asymmetrische Kryptographieverfahren zur Anwendung. Der genaue technische Ablauf beim elektronischem Signieren wird im nächsten Abschnitt erläutert. Der Empfänger wendet auf die ganze Datei den korrespondierenden Schlüssel des Schlüsselpaares an. Ist Vertraulichkeit nicht erforderlich und wird nur elektronisch signiert, wendet man den Verschlüsselungsalgorithmus überhaupt nur auf den sehr kleinen Hashwert an.

Eine andere Technik kommt im Bereich der World Wide Web-Dienste zum Einsatz, wie zum Beispiel beim Online Banking oder beim elektronischen Geschäftsverkehr. Bei verschlüsselter Online – Kommunikation, wie unter anderem bei der Verwendung von https[73] beim „Surfen" auf einer sicheren Webseite, wären die beteiligten Computer schnell an die Grenzen ihrer Leistungsfähigkeit angelangt, weil man den gesamten Datenstrom mit asymmetrischen Algorithmen chiffrieren müßte. Im Gegensatz zur E-Mail fallen hier ungleich mehr Daten an, die alle mit dem langsamen asymmetrischen Verfahren verschlüsselt werden müßten. Man benutzt daher in der Praxis ein gemischtes System. Der Webbrowser erzeugt einen Sessionkey. Das ist ein zufällig generierter Schlüssel für ein symmetrisches Verschlüsselungsverfahren. Dieser Sessionkey wird mit dem öffentlichen Schlüssel des Servers der sicheren Webseite verschlüsselt

[73] Secure Hypertext Transfer Protocoll.

und an diesen übermittelt. Nur dieser Webserver kennt den korrespondierenden privaten Schlüssel und kann daher den vorgeschlagenen Sessionkey als einziger lesen. Nur die geringe Datenmenge, die den Sessionkey selbst beinhaltet, muß langsam und rechenintensiv asymmetrisch verschlüsselt werden, der eigentliche Datenstrom wird mit Hilfe schneller symmetrischer Algorithmen verschlüsselt. Als geheimer Schlüssel wird der vorher vereinbarte und asymmetrisch verschlüsselt übersendete Sessionkey verwendet.

Nach Beendigung einer Session wird der Schlüssel wertlos, da bei Aufbau einer neuen Verbindung ein neuer, zufällig generierter Sessionkey verwendet wird. Dieses Verfahren verbindet alle Vorteile der asymmetrischen Kryptographie – nämlich daß man mit unbekannten Personen oder Servern verschlüsselte Daten austauschen kann, ohne vorher den geheimen Schlüssel über einen anderen Weg zu vereinbaren – und die Geschwindigkeit der symmetrischen Verschlüsselungstechniken. Diese Mischtechnik wird unter anderem im Secure Sockets Layer Protocoll (SSL) eingesetzt.[74]

2.5. Hash-Codes[75]

Auf Grund derselben Probleme wie bei der Online Kommunikation wird auch beim Digitalen Signieren nicht der gesamte Text asymmetrisch verschlüsselt. Dies wäre zwar zur Identifikation und Feststellung der Authentizität ausreichend, in der Praxis wird aber noch ein Zwischenschritt eingefügt, der das Verfahren beschleunigt.

Es wird nicht der ganze Text mit dem privaten Schlüssel des Absenders verschlüsselt, sondern vom Text ein Hashwert gebildet, dieser wird digital signiert an den Klartext angefügt und diese Kombination dann verschickt.

Der Sinn und Zweck einer Hashfunktion ist die Erstellung eines „Fingerabdruckes" einer Datei.[76] Folgende Anforderungen muß eine sichere Hashfunktion erfüllen:

- Sie kann auf eine Datei beliebiger Länge angewandt werden.
- Die Funktion erzeugt immer eine Ausgabe fixer Länge.

---

[74] *Esslinger/Müller,* Secure Sockets Layer (SSL) Protokoll, DuD (1997), S. 691.

[75] C'T Report, Geld Online 2 (1997), S. 23
Stallings, Sicherheit im Datennetz, S. 223ff und S. 335ff.

[76] *Stallings,* Sicherheit im Datennetz, S. 223.

- Für einen erzeugten Hashwert (Output dieser Funktion) darf kein anderer Ausgangstext als der gehashte gefunden werden können.
- Es muß unmöglich sein, rechnerisch ein Paar von Ausgangsdateien zu erzeugen, die den selben Hashwert erzeugen.
- Auch geringe Änderungen im Ausgangstext müssen signifikante Änderungen im Hashwert hervorrufen.
- Der Hashwert kann für jede beliebige Ausgangsdatei schnell und einfach berechnet werden.

Die Erstellung des Hashwertes eines Dokumentes ist also der erste Schritt bei der Erstellung der elektronischen Signatur. Der gesamte Prozeß beim Abschicken eines elektronisch signierten Dokumentes läuft nun folgendermaßen ab:

Zuerst wird durch die Hashfunktion der Hashwert der zu verschickenden Datei gebildet. Dieser Wert wird mit dem privaten Schlüssel des Absenders verschlüsselt. Verschlüsselter Hashwert und unverschlüsselte Originaldatei werden zusammengefügt. Ist Vertraulichkeit gefordert, kann diese Kombination jetzt noch mit dem öffentlichen Schlüssel des Empfängers verschlüsselt werden.

Der Empfänger entschlüsselt nun den Hashwert mit dem öffentlichen Schlüssel des Senders. Dann bildet er von der mitgeschickten unverschlüsselten Datei mit derselben Hashfunktion auch den Hashwert und vergleicht den von ihm erstellten Wert mit dem mitgeschickten Hashwert. Sind beide ident, kann er sicher sein, daß die Datei während der Übermittlung nicht verändert und vom Inhaber des Schlüsselpaares gesendet wurde, mit dessen öffentlichem Schlüssel er den Hashwert entschlüsselt hat.

Zwei Hashfunktionen haben weite Verbreitung gefunden und sind in mehreren Programmen, die asymmetrische Kryptographie unterstützen, implementiert.

1993 veröffentlichte das amerikanische National Institute of Standards and Technology (NIST) eine neue Hashfunktion im FIPS 180-1.[77] Secure Hash Algorithm (SHA) liefert 160 Bit lange Werte und ist deswegen auch gegen Brute Force Attacken hinreichend geschützt. Er wurde für die Implementierung im DSA entwickelt und ist in den neuen Versionen von PGP ab 5.0 integriert. Auch bei der Verwendung von RSA kann SHA zur Erstellung des Hashwertes verwendet werden Bis jetzt sind keine

---

[77] Federal Information Processing Standards Publication 180-1, download unter: http://www.itl.nist.gov/fipspubs/fip180-1.htm.

Schwachstellen dieser Funktion bekannt, sie ist allerdings deutlich langsamer als MD 5. Gegenwärtig wird der SHA von beim NIST akkreditierten Computerlabors[78] geprüft. SHA-1 und RIPEMD-160, der ebenfalls mit einer Länge des Hashwertes von 160 Bit arbeitet, sind gemäß SigVO für den Einsatz im Bereich sicherer elektronischer Signaturen zugelassen.

Der Message Digest 5 (MD 5) wurde 1992 von *Ron Rivest* entwickelt und im RFC 1321[79] der Öffentlichkeit vorgestellt. Er verarbeitet Eingaben beliebiger Länge und erzeugt ein 128 Bit langes Ergebnis. Durch die Implementierung in RSA arbeitet er unter anderem in allen PGP Versionen, die RSA Schlüssel unterstützen. Er wurde generell für sicher gehalten[80], die potentielle Möglichkeit kryptoanalytischer Anschläge wird von einigen Personen berichtet[81], die meinen, MD 5 nicht mehr für digitale Signaturen, die mehrere Jahre Beweiskraft haben sollen, zu verwenden. Zur kurzfristigen Sicherung von Online Übertragungen kann diese Funktion allerdings unbedenklich verwendet werden. MD2 und MD4 sind die älteren Versionen dieser Gruppe von MD-Funktionen. Sie haben bekannte und publizierte Schwächen und sollten deshalb nicht mehr benutzt werden. Deswegen wird diese Gruppe von Hashverfahren auch von der SigVO als nicht verwendbar für sichere elektronische Signaturen erklärt.

2.6. Standards zur sicheren Datenübertragung im ISO Referenzmodell

2.6.1. Secure Socket Layers (SSL)[82]

Dieses Protokoll ist heute „De facto-Standard" für die sichere Kommunikation beim elektronischen Geschäftsverkehr und besitzt mit Abstand die größte Verbreitung. Netscape entdeckte früh den Bedarf an sicherer Kommunikation im offenen Internet und entwickelte dafür den Secure Socket Layers Standard. Eine erste Beta-Version wurde Ende 1994

---

[78] Eine Auflistung der einzelnen Labore ist unter http://csrc.nist.gov/cryptval/140-1/1401labs.htm verfügbar.

[79] ftp://ftp.isi.edu/in-notes/rfc1321.txt.

[80] http://www.uni-siegen.de/security/krypto/mdigest.html.

[81] C'T Report, Geld Online 2 (1997), S. 23.

[82] *Esslinger/Maik,* Secure Sockets Layer (SSL) Protokoll, DuD (1997), S. 691.

veröffentlicht, die momentan aktuelle Version 3.0[83] stammt aus dem März 1996. Die Client Version wird zusammen mit Netscape Navigator frei vergeben, was eine hohe Verbreitung sichert. Die Implementierung auf Serverseite ist käuflich erwerbbar.

Das Protokoll dient zur Sicherung der Client-Server Kommunikation, damit auch konfidente Daten, wie zum Beispiel Kreditkartennummern, über offene Netze ohne Gefahr des Mißbrauchs durch Dritte geschickt werden können. Es bietet asymmetrische Kryptographie über RSA und Authentizität bei der möglichen Verwendung von X.509 Zertifikaten, sicheren Austausch von Session Keys und symmetrisch verschlüsselte Kommunikation. Im ISO Referenzmodell[84] finden sich die SSL-Dienste zwischen dem zugrundeliegenden Transferprotokoll – im Internet also TCP/IP – und der Schicht der Anwendungsprotokolle, wie Telnet, FTP oder HTTP. Durch die eingeschobene SSL-Schicht können die Protokolle auf den höheren Ebenen ohne viel Umgestaltung auf die Sicherheitsdienste zugreifen und in einem abgesicherten Modus betrieben werden.

Die internationale Versionen der amerikanischen Browser dürfen allerdings auf Grund der Exportbestimmungen für Kryptographieprodukte der Vereinigten Staaten weltweit nur an Banken für online angebotene Finanztransaktionen mit 128 Bit langen Schlüsseln ausgeliefert werden. Bei den anderen internationalen Versionen ist innerhalb des SSL Protokolls nur RC4_40 als Verschlüsselungsalgorithmus implementiert. Hier sind von den 128 verwendeten Schlüsselbits nur 40 geheim.[85] Diese schwache Verschlüsselung wurde schon vor einiger Zeit gebrochen[86] und ist nicht als sicher anzusehen. Vermeiden läßt sich dieses Problem, indem man entweder den norwegischen Browser Opera verwendet, der volle 128 Bit Verschlüsselung im SSL-Protokoll und TLS bietet[87], oder Netscape Navigators Kryptographie – DLLs durch das Programm Fortify[88] verändert. Nach einmaligem Aufruf des Programmes arbeitet das SSL Protokoll nachher mit einem 128 Bit Verschlüsselungsalgorithmus. Problematisch ist allerdings, daß Punkt 6 i der Lizenzvereinbarung mit Netscape Navi-

---

[83] *Freier/Karlton/Kocher,* Internet-Draft The SSL Protocol 3 , http://www.alternic.com/drafts/.

[84] *Egan,* ISO OSI 7 Layer Model forced with TCP/IP, http://libweb.sonoma.edu/mike/networking/netmodels/isoosi7layermodel.html.

[85] *Brooks,* Cypherpunks „brute" key cracking ring, http://www.brute.cl.cam.ac.uk/brute/.

[86] http://www.uni-siegen.de/security/internet/ssl.html.

[87] Beschreibung des Herstellers: http://operasoftware.com/features.html.

[88] Homepage des Entwicklers: http://sunsite.bilkent.edu.tr/pub/Fortify.

gator jede Veränderung des Programmcodes durch den Anwender verbietet. Netscape hat zu diesem Problem noch nicht Stellung genommen. Nach einer Aussage des Entwicklers von Fortify wird das Programm aber auf vielen großen, kommerziellen Webseiten zum Download angeboten, ohne daß Netscape je rechtliche Schritte gegen die Verteilung und Verwendung unternommen hat.

2.6.2. Secure Hyper Text Transfer Protocoll (shttp)[89]

Hyper Text Transfer Protocoll ist das zweite Verfahren, das die Sicherheit der Kommunikation im Internet verstärkt. Es wird verwendet, um die HTML Seiten – die Inhalte des World Wide Web – vom Server zum Client zu übermitteln. Es unterstützt auch die Übertragung von Daten in die Gegenrichtung, wie etwa Angaben, die der Anwender in einem HTML-Formular eingibt. Durch Secure Hyper Text Transfer Protocoll wird das ursprüngliche Protokoll nun um alle Funktionen erweitert, die für den elektronischen Geschäftsverkehr benötigt werden, damit auch Kreditkarteninformationen und Kontomanipulationen sicher übertragen werden können. Der unbefugte Zugriff Dritter wird auf dem ganzen Weg vom Server bis zum Client verhindert. SHTTP ist variabel ausgelegt und arbeitet mit einer Vielzahl von kryptographischen Algorithmen zusammen. Durch die Integration von asymmetrischer Verschlüsselung und durch die Möglichkeit des Austausches der Zertifikate ist auch die Authentizität und richtige Identität gewährleistet. Alle gängigen Browser beherrschen dieses Protokoll. Eine Beschreibung der neuesten Version ist im WWW zu finden.[90]

---

[89] *Rescorla/Schiffman*, Internet-Draft The Secure HyperText Transfer Protocol ftp://ftp.isi.edu/in-notes/rfc2660.txt.

[90] *Rescorla/Schiffman*, SHTTP Draft, http://www.terisa.com/shttp/current.txt.

3. Die Technik zur Verwendung elektronischer Signaturen und Zertifikate innerhalb einer Public Key Infrastructure

3.1. Elektronische Signaturen

3.1.1. Technisches Verfahren

Elektronische Signaturen haben nichts mit dem Anhängen eines elektronischen Abbilds (Pixelmuster) einer handschriftlichen Unterschrift an ein Textdokument gemeinsam, da diese Methode keinen Sicherheitsgewinn bringt. Das Pixelmuster kann wie jedes andere elektronische Dokument spurlos kopiert oder verändert werden.

Der technische Ablauf, der beim elektronischen Signieren am Computer ausgeführt wird, besteht aus der Kombination von Hashen des zu signierenden Textes, der Verschlüsselung des Hashwertess mit dem privaten Schlüssel des Senders und dem gemeinsamen Verschicken der Textdatei und des Signaturdatenblocks. Nähere Erklärungen zu den einzelnen Teilen sind weiter oben im Text bereits gegeben worden. Hier soll nur kurz das Zusammenspielen der einzelnen Teile beschrieben werden. Zuerst wird von der zu signierenden Datei ein Hashwert ermittelt. Nur dieses kurze individuelle Merkmal des Dokuments wird mit dem privaten Schlüssel des Senders verschlüsselt. Anschließend werden sowohl das Dokument, das die Willenserklärung enthält, als auch der verschlüsselte Hashwert an den Empfänger übermittelt. Dieser entschlüsselt den Hashwert mit dem öffentlichen Schlüssel des Senders, den er von einem öffentlichen Verzeichnis heruntergeladen hat. Anschließend erstellt der Empfänger ebenfalls einen Hashwert vom übermittelten Dokument und vergleicht den von ihm erstellten Wert mit dem vom Empfänger übermittelten und nun entschlüsselten Hashwert. Sind beide Hashwerte ident, liegt eine gültige elektronische Signatur vor.

In der Praxis merkt der Anwender bei Verwendung von Mail-Programmen neuerer Generation nichts von diesem mehrteiligen Prozeß, sobald die Option, die versendeten E-Mails auch zu signieren, eingestellt ist, wird die elektronische Signatur des Empfängers gemeinsam mit dem Dokument übermittelt. Die Software auf der Empfängerseite verifiziert ebenso die einlangenden elektronisch signierten Dokumente automatisch, so daß Sender und Empfänger mit einem Mausklick signieren und verifi-

zieren können. Welche Anforderungen Signaturgesetz und Signaturverordnung an diese Programme stellen, soll im rechtlichen Teil weiter unten betrachtet werden.

Eine technische Definition der digitalen Signatur findet sich unter anderem im § 55a Erklärung der UNCITRAL Working Group on Electronic Commerce:

> „A digital signature is a numerical value, which is affixed to a data message and which, using a known mathematical procedure associated with the originator's private cryptographic key, makes it possible to determine uniquely that this numerical value has been obtained with the originator's private cryptographic key. The mathematical procedures used for generating authorized digital signatures under these Rules are based on public key encryption."[91]

Mit anderen Worten zusammenfassend beschrieben: Als Grundlage für die Verwendung digitaler Signaturen zur Übermittlung von rechtlich verbindlichen Willenserklärungen müssen die verwendeten mathematischen Funktionen auf asymmetrischer Kryptographie basieren, jedes Schlüsselpaar muß eindeutig nur einer Person zugeordnet sein und der private Schlüssel muß durch ein Codewort oder eine Smartcard gegen die Verwendung durch Unbefugte gesichert sein. Weiters muß gewährleistet sein, daß der Empfänger, wenn er den Text der Nachricht und den vom Sender verschlüsselten Hash-Code der Nachricht vom Sender elektronisch übermittelt bekommt, weiters den öffentlichen Schlüssel des Senders von einem für jedermann im Internet erreichbaren Key-Server herunterlädt, zuverlässig nachweisen kann, daß die Nachricht mit dem privaten Schlüssel des Empfängers verschlüsselt und während der Übermittlung nicht verändert wurde.

3.1.2. Rechtliche Definitionen elektronischer Signaturen

Im Art. 2 der Signaturrichtlinie[92] (im folgendem als SigRL bezeichnet) findet sich folgende Definition für elektronische Signaturen:

---

[91] UNCITRAL, Working Group on electronic commerce Thirty-first session, § 55a, New York, 18-28 February 1997.

[92] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Amtsblatt Nr. L 013 vom 19.1.2000, S. 0012 – 0020, CELEX Nr. 31999L0093.

„Elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen. ... Eine fortgeschrittene elektronische Signaturen ist eine elektronische Signaturen, die folgende Anforderungen erfüllt:

- Sie ist ausschließlich dem Unterzeichner zugeordnet;
- Sie ermöglicht die Identifizierung des Unterzeichners;
- Sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;
- Sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, daß eine nachträgliche Veränderung der Daten erkannt werden kann."

Das österreichische Signaturgesetz[93] (im folgendem als SigG bezeichnet) folgt dieser Definition und normiert im § 2 folgendes:

„Elektronische Signaturen sind elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators dienen."

Das SigG kennt auch nicht die fortgeschrittene elektronische Signatur, sondern definiert eine sichere elektronische Signatur, die aus der fortgeschrittenen elektronischen Signatur inklusive eines qualifizierten Zertifikats des Art. 5 SigRL besteht:

Sichere elektronische Signatur ist eine elektronische Signatur, die

- „Ausschließlich dem Signator zugeordnet ist,
- die Identifizierung des Signators ermöglicht,
- mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann,

---

[93] Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG), BGBl. I Nr. 190/1999, NR: GP XX RV 1999, AB 2065 S. 180, BR: AB 6065, S. 657.

- mit den Daten, auf die sie sich bezieht, so verknüpft ist, daß jede nachträgliche Veränderung der Daten festgestellt werden kann, sowie
- auf einem qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen des SigG und der SigVO entsprechen, erstellt wird."

Auch im Gesetz des Bundesstaates Kentucky[94] der Vereinigten Staaten von Amerika wird von „electronic signatures" gesprochen. Ähnlich der Regelung der Europäischen Union und Österreichs werden sie dort folgendermaßen definiert:

> „Electronic signature" means an electronic identifier whose use is intended by the person using it to have the same force and effect as the use of a manual signature and containing the following characteristics:
>
> - it is unique to the person using it;
> - it is capable of verification; and
> - it is under the sole control of the person using it

3.1.3. Rechtliche Definition digitaler Signaturen

Im Gegensatz zur SigRL und SigG kennen das deutsche und das italienische Signaturgesetz keine elektronischen Signaturen, sondern definieren die digitale Signatur durch die Verwendung asymmetrischer Kryptographie folgendermaßen:

> „Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüsselzertifikat einer Zertifizierungsstelle oder der Behörde nach § 3 versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt."

---

[94] Act: HB 708, http://www.state.ky.us/agencies/elecsig.

Im italienischen Recht[95,96] wurde folgende Legaldefinition für die digitale Signatur festgelegt:

> „„Digital signature" means the result of a computer-based process (validation) implementing an asymmetric cryptographic system consisting of a public and a private key, whereby the signer asserts, by means of the private key, and the recipient verifies, by means of the public key, the origin and integrity of a single electronic document or a set of such documents. „

3.1.3.1. Probleme bei der Namensgebung-Elektronische Signaturen vs. Digitale Signaturen

In Gesetzgebung und Literatur findet man unterschiedliche Bezeichnungen, wie: „elektronische Unterschrift", „digitale Unterschrift", „elektronische Signatur", „digitale Signatur". Der Begriff „Unterschrift[97]" wurde oft in den Frühzeiten der Verwendung asymmetrischer Kryptographie verwendet. Dieser Gebrauch ist allerdings verwirrend, da eine digitale Signatur nicht wie eine eigenhändige Unterschrift am Ende des Textes hinzugefügt wird, sondern durch Verschlüsseln und Hashen des ganzen Textes gebildet wird. Der Begriff „Elektronische Unterschrift" sollte für eingescannte Images von eigenhändigen Unterschriften reserviert bleiben. Das viel sicherere Verfahren der Authentifizierung durch Anwendung asymmetrischer Kryptographie auf den gesamten Text sollte zur Abgrenzung immer als „Signatur" bezeichnet werden.

Das deutsche SigG und die deutsche SigVO verwenden durchgehend den Begriff „digitale Signatur", auch ein italienisches Gesetz verwendet diesen Terminus. Er hat sich im deutschen Sprachraum seit einigen Jahren als Begriff für diese Funktion der asymmetrischen Verschlüsselung behauptet.

---

[95] http://www.aipa.it/english[4/law[3/pdecree51397.asp.

[96] §1 (b) Presidential Decree No. 513 of 10 November 1997: Dieses Dekret stützt sich auf: Section 15(2) of Law No. 59 of 15 March 1997 concerning the creation, storage and transmission of documents by means of computer-based or telematic systems http://www.aipa.it/english[4/law[3/law5997.asp.

[97] Die Unschärfe in der Verwendung der Begriffe „Unterschrift" und „Signatur" wird in der englischen Rechtssprache noch verschärft, da hier für beide deutschen Begriffe einheitlich das Wort „signature" verwendet wird.

Durch drei neue Vorschläge über Normen, die diesen Bereich regeln – eine Richtlinie der Europäischen Union, das Model-Law der UNCITRAL über elektronische Signaturen sowie ein Gesetz des Bundesstaates Kentucky - wurde neu der Terminus „elektronische Signatur" eingeführt. Auch das österreichische SigG hat diesen neuen Terminus übernommen und spricht ausschließlich von elektronischen Signaturen. Erste Überlegungen, den Geltungsbereich der Normen weiter zu fassen und dafür den Begriff „elektronische Signaturen" zu verwenden, finden sich in den §§ 14f der „United Nations Commission on international trade law, Working Group on electronic commerce, Thirty-first session, Planning of future work on electronic commerce: digital signatures, certification Authorities and related legal issues, New York, 18-28 February 1997". Besonders die amerikanischen Teilnehmer an den UNCITRAL Ausschüssen drängten auf die neue Benennung, seit dem Treffen der Arbeitsgruppe im Jänner 1998 wird in den Entwürfen der neue Begriff verwendet. Damit soll eine starre Fixierung der gesetzlichen Regelungen auf Signaturverfahren, die ausschließlich mit Methoden der asymmetrischen Kryptographie arbeiten, vermieden werden. Nach dieser Auffassung ist der Begriff „digitale Signatur" eindeutig an die Verwendung asymmetrischer Kryptographie gebunden. Sollten neue Verfahren entwickelt werden, die nicht auf asymmetrischer Kryptographie beruhen, könnte es sein, daß diese dann nicht mehr in den Geltungsbereich der bestehenden Gesetze fallen. Man will mit dem Begriff „elektronische Signaturen" einen allgemeineren Geltungsbereich als durch Verwendung des Begriffs „digitale Signatur" erlangen.[98]

Deutlich sieht man diese Trendwende beim Vergleich der oben zitierten Legaldefinitionen von elektronischer und digitaler Signatur zum ersten Mal im Kommissionsvorschlag über eine Signaturrichtlinie und dem deutschen SigG. Die Richtlinie ist technologieneutral formuliert. Sie fordert zwar, daß die verwendete Methode gewisse Kriterien, die eine sichere Übertragung und Authentizität garantieren, erfüllen muß, schreibt aber nicht wie das deutsche Gesetz die Verwendung asymmetrischer Kryptographie zum Erstellen der Signatur vor. Die Kommission begründet dies mit der raschen technologischen Entwicklung und dem globalen Charakter des Internets, die ein Konzept erfordern, das verschiedenen Technolo-

[98] Prof. *Mads Bryde Andersen* (Chairman UNCITRAL working group on digital signatures) in einem Vortrag auf der Konferenz „Electronic Commerce The real Trade" 18.6.1998, Oslo.

gien und Dienstleistungen im Bereich der elektronischen Authentifizierung offensteht.[99]

Problematisch ist hierbei, daß beim heutigen Stand der Technik nur die Verwendung asymmetrischer Kryptographie eine sichere Public Key Infrastructure gewährleistet. Asymmetrische Kryptographie wurde seit mehr als zwanzig Jahren weiterentwickelt und in dieser für Internettechnologie sehr langen Zeitspanne kam es nicht zur Entwicklung einer Alternative zu dieser Technologie. Es ist auch für die nächsten zehn Jahre äußerst unwahrscheinlich, daß Paralleltechnologien gefunden werden. Das Argument, daß durch die weitere Regelung auch biometrische Verifikationsverfahren in den Geltungsbereich des Richtlinienvorschlags fallen[100], ist mE verfehlt, da biometrische Verifikationsverfahren jetzt schon eingesetzt werden und auch unproblematisch innerhalb der Grenzen der Definition des deutschen SigG angewandt werden können. Diese Überprüfung der persönlichen Eigenschaften des Benutzers findet nämlich nur Verwendung, um lokal die Zugriffsberechtigung auf den jeweiligen privaten Schlüssel zu untersuchen. Die Kommunikation über das offene Netz erfolgt bei diesen Verfahren ebenfalls weiterhin über klassische Public Key Verfahren.

Der neue Begriff steigert auch die Unsicherheit über die Technik, die durch die verschiedenen Termini bezeichnet wird. Einige amerikanische Gesetze nennen eingescannte handschriftliche Unterschriften ebenfalls „electronic signatures". *Benjamin Wright* ist der amerikanische Proponent für das Verfahren Penops.[101] Hier werden die biometrischen Merkmale der auf einem Touchscreen geleisteten eigenhändigen Unterschrift geprüft. Stimmen sie mit den Referenzdaten überein, ist der Anwender authorisiert. *Wright* tritt dafür ein, daß diese Methode auch zu den elektronischen Signaturen zu zählen ist. Da es sich hier aber nur um eine Autorisierungsüberprüfung handelt und die Komponente der authentischen Nachrichtenübermittlung nicht gewährleistet ist, erfüllt es nicht die Anforderungen, die die SigRL und das SigG an elektronische Signaturen stellen.

Es muß aber jedenfalls vermieden werden, daß legistisch die Verwendung bloßer Images den elektronischen und digitalen Signaturverfahren gleichgestellt wird. Die Anforderungen, die die Rechtsordnung an elektronische und digitale Signaturverfahren stellt, um Authentizität und

---

[99] Erwägungsgrund Z. 7, KOM (1998) 297/10.

[100] *Brisch*, Gemeinsame Rahmenbedingungen für elektronische Signaturen, Richtlinienvorschlag der Kommission, CuR (1998), S. 494.

[101] *Wright*, The Law of Electronic Commerce, App. G:1.

Identifikation zu gewährleisten, vermögen Dateien, die um das Abbild einer eingescannten handschriftlichen Unterschrift ergänzt wurden, einfach nicht zu erfüllen. Ihnen kann daher gesetzlich nicht Rechtsfolgen wie die Schriftform zugesprochen werden. Um Unklarheiten und unscharfe Begriffe zu vermeiden ist zu hoffen, daß sich der Begriff elektronische Signatur ausschließlich als Bezeichnung für elektronische Daten, die der Authentifizierung des Signators und der Integrität des Dokumentes bei Übertragung durch offene Netze dienen, durchsetzen wird, und nicht mehr auch bloße digitale Abbildungen einer eigenhändigen Unterschrift als solche bezeichnet werden. Zumindest im deutschen Sprachraum sollte dies durch das Kunstwort Signatur gewährleistet sein, da der sprachliche Unterschied zwischen elektronischer Signatur und elektronischer Unterschrift auffällig genug ist.

3.1.4. Standards und Programme zur Erzeugung elektronischer Signaturen

3.1.4.1. PGP[102]

PGP ermöglicht es, Emails und auch Dateien einigermaßen komfortabel sowohl elektronisch zu signieren als auch zu verschlüsseln. Es war bis zur Anpassung der diversen Mail-Programme an die Anforderungen einer Public Key Infrastructure im Sinne der neueren Normen das in Verbindung mit Verschlüsselung und Signierung von E-Mails am meisten genutzten Programm.[103] Es bietet aber nur eingeschränkte Möglichkeiten, Zertifikate zu verwenden. So bestimmt jeder PGP - Signator selbst seinen Namen, der ins Zertifikat aufgenommen wird, so daß die Authentizität nicht hinreichend gewährleistet ist. Weiters akzeptiert PGP auch elektronische Signaturen, die mit Hilfe von Schlüsseln erstellt wurden, deren Gültigkeitsdatum nach dem Datum der mit ihnen erstellten elektronischen Signatur liegt.[104] Der Schlüssel dürfte also zum Zeitpunkt der Signaturerstellung noch gar nicht existieren, trotzdem wird die Signatur als gültig ausgewiesen. In das Programm wurden zwar starke kryptographische Algorithmen implementiert, die die Sicherheit gegen Attacken auch in Zu-

---

[102] PGP for Personal Privacy Version 5.5, User's Guide, Network Associates, Inc *Stallings*, Sicherheit im Datennetz, S. 445ff
http://www.momentus.com.br/PGP/doc/howpgp.html.

[103] *Reiser*, Internet - die Sicherheitsfragen, S. 39.

[104] *Camphausen*, Schlüsselzertifizierung mit PGP, DuD (1998), S. 382.

kunft gewährleisten. Doch gelang es im Sommer 1997, einige exponierte Schlüssel (darunter 2 Zertifizierungsschlüssel von Zertifizierungsdiensteanbietern[105]) zu kompromitieren, indem ein Unbekannter Fälschungen dieser Schlüssel auf das Netz der PGP Keyserver spielte. Dementsprechend groß war die Unsicherheit der Benutzer dieser Zertifizierungsstellen[106]. PGP gewährleistet also die Integrität der Nachricht bei Übermittlung in offenen Netzen, unterstützt aber nicht die ebenfalls gebotene Verifikation der Identität des Senders eines elektronischen Dokuments.

Auf Grund dieser Sicherheitsmängel und wegen der mangelnden Registrierung der Anwender durch einen Zertifizierungsdiensteanbieter, der den Anforderungen des SigG entspricht[107], gelten mit PGP erstellte elektronische Signaturen auch nicht als sichere elektronische Signaturen im Sinne des SigG.

Das Programm ist in verschiedensten Versionen für einige Betriebssysteme erhältlich, wodurch eine weite Verbreitung erreicht wurde. *Phil Zimmermann* entwickelte die erste Version von PGP in Alleinarbeit. Die Rechte der neueren Versionen liegen bei der amerikanischen Firma RSA Data Security, Inc., die das Produkt vermarktet. Mittlerweile sind sowohl frei erhältliche Versionen wie auch kommerziell vertriebene am Markt. Bis zur Version 2.6 wurde RSA als Kryptographiealgorithmus und MD5 (128 Bit) für das Hashen verwendet. Mit Erscheinen der Windows 95 kompatiblen Version 5.0 wird versucht, DSA und SHA (160 Bit) zu propagieren. Die kommerzielle Version von PGP 5.0 konnte zwar noch Schlüssel gemäß RSA generieren und verwenden, mit der frei erhältlichen Version ist der Anwender aber nicht mehr in der Lage, RSA-Schlüssel zu erzeugen, es können nur mehr alte, mit PGP 2.6 generierte RSA-Schlüssel verwendet werden. Bei der neuesten Version 5.5.3 strich man auch diese Version, der Anwender ist hier an die Verwendung von DSA Algorithmen gebunden.

Die in den kommerziellen Versionen mögliche Key-Escrow Funktion hat zu einigen Diskussionen geführt. Hier ist es dem Administrator möglich, ohne Wissen der Anwender die von ihnen generierten Schlüssel zu kopieren und dadurch verschlüsselte, vertrauliche Mails zu lesen. Interessant ist dieser Umschwung in der Produktpolitik, weil *Zimmermann* bis dahin als einer der wichtigsten Gegner der Schlüsselhinterlegungspolitik der amerikanischen Regierung auftrat.

---

[105] C't Zertifizierungsstelle und IN-Root-Zertifizierungsstelle.

[106] *Camphausen*, Schlüsselzertifizierung mit PGP, DuD (1998), S. 382.

[107] Weitere Überlegungen zum von PGP favorisierten Web of Trust finden sich im nächsten Abschnitt.

PGP darf auf Grund der amerikanischen Exportbestimmungen nicht in elektronischer Form exportiert werden. Das Problem wurde gelöst, indem der Quellcode des Programms in Amerika ausgedruckt wurde, die Papiere legal nach Europa transportiert und hier wieder eingescannt und kompiliert wurden. Deswegen erscheinen die neuen internationalen Versionen von PGP einige Monate später als die amerikanischen Originale.

3.1.4.2. Privacy Enhanced Mail (PEM)[108]

Dieser Standard wurde als Erweiterung bestehender E-Mail-Standards entwickelt, um Vertraulichkeit, Authentizität und Unleugbarkeit des Ursprungs und Integrität der Nachricht direkt in die E-Mail-Standards[109] zu integrieren. Es ist in den RFCs 1421 - 1424[110] spezifiziert. PEM ist kein externes Programm wie PGP, das die Daten vor dem Versenden verschlüsselt, damit sie danach vom Mail-Client – einem unabhängigen Programm - verschickt werden können. PEM ist in den User Agent – das Programm, das der Anwender zum Senden und Empfangen seiner E-Mails verwendet[111] - integriert. Erst nachher wird die Mail vom Message Transfer Agent an das Netzwerk abgegeben. Man erreicht dadurch eine Unabhängigkeit vom zugrundeliegenden E-Mailsystem. Dieses muß nicht an PEM angepaßt werden. Da die PEM–Nachrichten weiterhin konform mit dem vorgegebenen Mail-Format sind, ist keinerlei Anpassung der Message Transfer Agents notwendig.

PEM bietet verschiedene Betriebsmodi:

MIC-CLEAR: Hier wird ein Message Integrity Check (MIC) durch eine Hash - Funktion berechnet. Klartext und MIC werden an die Adressaten übertragen. PEM-User können dadurch die Authentizität und Inte-

---

[108] *Horster/Portz,* Privacy Enhanced Mail (PEM), Ein Standard zur Sicherung des elektronischen Nachrichtenverkehrs im Internet, DuD (1994), S. 434. *Stallings,* Sicherheit im Datennetz, S. 474ff.

[109] ftp://ftp.isi.edu/in-notes/rfc1421.txt

RFC 822 http://www.dsi.unive.it/Connected/RFC/822.

[110] Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures, ftp://ftp.isi.edu/in-notes/rfc1421.txt

Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, ftp://ftp.isi.edu/in-notes/rfc1422.txt

Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers ftp://ftp.isi.edu/in-notes/rfc1423.txt

Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services, ftp://ftp.isi.edu/in-notes/rfc1424.txt.

[111] Definiert in: RFC 822, ftp://ftp.isi.edu/in-notes/rfc822.txt.

grität des Textes prüfen. Durch Mitschicken des Klartextes ist er auch für Adressaten, die kein PEM verwenden, lesbar.

MIC-ONLY besteht aus dem gleichen Verfahren wie MIC-CLEAR, wobei die gesamte Nachricht noch mit einer Transportcodierung versehen wird, damit sichergestellt ist, daß die Nachricht an den offenen Netzwerkknoten nicht verändert wird. Sollte eine Veränderung auftreten, ist dies beim Empfänger ersichtlich, da die Verifikation unmöglich wird.

ENCRYPTED: Diese Methode basiert auf der Verwendung der Dienste von MIC-ONLY, zusätzlich wird die Nachricht noch mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Danach ist auch die Vertraulichkeit gewährleistet.

Ein besonderer Vorteil von PEM ist, daß nicht nur Verschlüsselung und Signieren wie bei PGP möglich ist, sondern darüber hinaus auch eine CCITT X.509-konforme Zertifikatsverwaltung unterstützt wird. Die Wichtigkeit von Zertifikaten und ihre absolut notwendige Verwendung im sicheren elektronischen Verkehr wird im nächsten Abschnitt dieser Arbeit erläutert. Diese Funktionalität, die Bindung an einen definierten Standard, die leichte Einbettung in bestehende Netzwerksysteme und die skalierbare Sicherheit machen PEM zum besten im Moment verfügbaren Standard in diesem Bereich. Durch die Implementierung von X.509 kann PEM unter Einhaltung der anderen Anforderungen des SigG auch zur Abgabe und Prüfung sicherer elektronischer Signaturen verwendet werden.

Die Zukunft von PEM wird sicherlich durch die Verfügbarkeit von Anwendungen, die PEM unterstützen, entscheidend beeinflußt. Im deutschsprachigen Raum ist vorläufig nur das Programmpaket SecuDe-PEM[112] erhältlich, das von der deutschen Gesellschaft für Mathematik und Datenverarbeitung entwickelt wurde. An einer Anpassung von PEM an den weitverbreiteten Standard MIME (Multipurpose Internet Mail Extensions) wird gearbeitet.

3.1.5. Sicherung durch biometrische Überprüfung

Da die privaten Schlüssel bei asymmetrischer Kryptographie – es handelt sich um eine zufällige Buchstabenkombination von der Länge einer Druckschriftseite - zu unhandlich sind, um sie bei jeder Verschlüsselung manuell einzugeben, werden diese Schlüssel maschinenlesbar gespeichert. Meist wird der Schlüssel auf Festplatte oder Diskette verwahrt,

---

[112] Näheres über SecuDe unter: http://sit.gmd.de/.

neuerdings setzt sich immer mehr die Speicherung auf Smartcards durch: Plastikkarten mit einem Mikrochip, auf dem der Schlüssel gespeichert wird und womit der RSA-Algorithmus ausgeführt werden kann. Die Verbindung zum Netzwerk erfolgt über Kontakte an der Oberfläche der Karte. Damit nur der Berechtigte Zugriff auf den gespeicherten privaten Schlüssel hat, wird dieser vom System erst nach positiver Verifikation der Identität freigegeben.

3.1.5.1. Arten der Identifikation

Die Überprüfung, ob eine Person auch diejenige ist, die sie vorgibt zu sein, ist zu einem unverzichtbaren Merkmal von Sicherheitskonzepten für IT-Systeme geworden. Alle Systeme haben ausgewählte Referenzmuster der jeweiligen Anwender gespeichert, die bei jeder Anmeldung eines Anwenders mit den aktuell eingegebenen Anmeldedaten verglichen werden. Dieser Vorgang wird als Verifikation der Identität bezeichnet, er unterscheidet sich zur Identifikation dadurch, daß bei der Verifikation der Identität das aktuell eingegebene Muster mit nur einem Referenzmuster, bei der Identifikation mit allen Referenzmustern verglichen und das passende ausgewählt wird. Für die Überprüfung der Zugriffskontrolle ist nur das Verfahren der Verifikation der Identität von Interesse.

Bei Heranziehung biometrischer Daten als Referenzmuster kann der Anwender die Referenzmuster nicht weitergeben, bei der Überprüfung anhand von Paßwörtern oder vergebenen PIN-Codes besteht üblicherweise eine vertragliche Verpflichtung des Anwenders, sein Paßwort keinem Dritten mitzuteilen.

3.1.5.1.1. Verifikation der Identität durch Besitz und Wissen

Verifikation der Identität durch Besitz ist das älteste Verfahren. Schon im Mittelalter wurden Siegel an Urkunden angebracht, die für die Verifikation erheblicher als die Unterschrift waren. Heute dienen hauptsächlich Schlüssel, Pässe, Erkennungsmarken und Smartcards der Verifikation durch Besitz. War die Verifikation durch Besitz seit der Neuzeit für den Geschäftsverkehr nur von sehr untergeordneter Bedeutung und wurde durch die Unterschrift ersetzt, gewinnt sie heute als Verifikationsverfahren mittels Smartcards für den Zugriff auf elektronische Signaturen wieder an Wichtigkeit.

Die Verwendung von Geheimcodes ist die ältere Form der Verifikation durch Wissen. In Rechnernetzwerken ist die Verifikation durch Paßwortabfrage bei Eingabe einer Benutzerkennung heute nicht mehr wegzu-

denken. Man unterscheidet frei wählbare Paßwörter und von Systembetreuern oder Programmen automatisch vergebene, fix vorgegebene PINs. Beide sind nur dem jeweils Berechtigten bekannt und dürfen nicht an Dritte weitergegeben werden.

Diese Verifikationsform bringt 2 Nachteile mit sich:

- Paßwörter, die von den Anwendern frei gewählt werden, sind meistens sehr kurz oder haben einen ausgeprägt nahen Bezug zu persönlichen Umständen des Benutzers. Fix vergebene Paßwörter werden fast immer zur Sicherheit gegen das Vergessen irgendwo notiert. Beides führt dazu, daß unbefugte Dritte leicht an die Paßwörter herankommen oder sich diese ausrechnen können.
- Es kann nicht vermieden werden, daß der Berechtigte das Paßwort und die Chipkarte an Dritte weitergibt. So konnte in der Simulationsstudie „Rechtspflege“[113] nachgewiesen werden, daß viele Rechtsanwälte, die bei ihrem elektronischen Rechtsverkehr elektronisch signierten, ihre Chipkarte an Sekretäre weitergaben. Soll die elektronische Signatur der eigenhändigen Unterschrift gleichgestellt werden, darf dies nicht möglich sein. Eine biometrische Überprüfung zur Verifikation wäre dringend zu empfehlen.

3.1.5.1.2. Verifikation der Identität durch persönliche Eigenschaften

Meist verwendetes traditionelles Verfahren ist hier die Verifikation durch eigenhändige Unterschrift, wie es im Bereich des Zahlungsverkehrs und Vertragswesens üblich ist. Auch die Verifikation durch die Stimme des Gesprächspartners beim Telefonieren oder das Erkennen der Gesichtsform und die Überprüfung der Übereinstimmung mit Fotos auf amtlichen Lichtbildausweisen unter Anwesenden wird oft verwendet. Im strafrechtlichen Bereich dienen vielfach Fingerabdrücke diesem Zweck. Seit einiger Zeit sind nun auch Verfahren entwickelt worden, die Verifikation durch persönliche Eigenschaften automatisiert durch die Verwendung geeigneter Lesegeräte für Computer ermöglichen. Diese Methoden werden als biometrische Verfahren zur Verifikation der Identität bezeichnet. Nur durch Anwendung solcher Methoden ist es zuverlässig gewährleistet, daß wirklich allein der Verfügungsberechtigte Zugriff bekommt.

---

[113] Projektgruppe verfassungsverträgliche Technikgestaltung (Provet) und Gesellschaft für Mathematik und Datenverarbeitung (GMD), Verletzlichkeit und Verfassungsverträglichkeit rechtsverbindlicher Telekooperation, DuD (1993), S. 561.

Sowohl ein Ausspionieren als auch Weitergeben der Paßwörter wird wirkungsvoll verhindert.

3.1.5.2. Prinzip der biometrischen Überprüfung

Das biometrische Verfahren beruht auf einem Merkmal, das von Person zu Person variiert, jedoch für ein- und dieselbe Person eindeutig ist. Es können nur solche Merkmale herangezogen werden, die geeignet für das Scannen sind und wobei die Datenmengen zur Aufzeichnung in akzeptablem Ausmaß bleiben.

Dieses Merkmal wird einmalig bei der zugriffsberechtigten Person eingescannt und als Referenzdatensatz zusammen mit den erteilten Zugriffsberechtigungen in einer Datenbank gespeichert, um für spätere Vergleichungen abrufbar zu sein. Will die jeweilige Person nun auf geschützte Bereiche zugreifen, werden ihre biometrischen Merkmale wieder vom Sensor erfaßt und die neuen Daten mit den Referenzdaten verglichen. Überschreitet die Übereinstimmung der beiden Datensätze einen gewissen Schwellenwert, kann das System davon ausgehen, daß der Anwender die richtige Person ist, und wird die Ressourcen freigeben.

Bei Entwicklung biometrischer Verifikationsverfahren ist es nötig, daß eine Reihe von technischen Voraussetzungen bedacht wird. Die Toleranz beim Vergleich zwischen den Daten bei der Verifizierung und dem Referenzdatensatz muß so gewählt sein, daß die Fehlerquote beim Abweisen von Berechtigten durch Falscherkennung (False Reject Rate) nicht zu hoch ist, gleichzeitig aber die Rate der Zulassung von Unberechtigten (False Accept Rate) ebenso nicht hoch steigt. In einer Studie der Europäischen Union[114] wird dargelegt, daß im britischen Bankwesen eine False Accept Rate von 1 zu 100.000 akzeptiert wird.

3.1.5.3. Bedeutung der biometrischen Überprüfung für die Identifikation

Die Verifikation der Identität durch biometrische Verfahren ist derzeit die einzige Methode, die ein Vortäuschen einer falschen Identität mit an Sicherheit grenzender Wahrscheinlichkeit ausschließt. Die Möglichkeit zur Umgehung der Identitätsfunktion durch betrügerische Inbesitznahme von fremden Signaturerstellungsdaten und den dazugehörigen Paßwörtern einerseits, aber auch die Möglichkeit der freiwilligen Weitergabe der ei-

---

[114] *Polemi*, Review and evaluation of Biometric Techniques for Identification and Authentication – Final Report, S. 8, http://www.cordis.lu/infosec/src/stud5fr.htm.

genen Signaturerstellungsdaten an Dritte ist der immer wieder vorgebrachte Hauptkritikpunkt, wenn die Sicherheit elektronisch signierter Dokumente in Frage gestellt und in weiterer Folge verlangt wird, daß die besonderen Rechtswirkungen für elektronisch signierte Dokumente nicht denen der traditionellen Urkunde in Papierform angeglichen wird.

Durch diese Absicherung erlangen die Methoden der Biometrie eine so herausragende Bedeutung für den Schutz der Signaturerstellungseinheiten. Im Moment ist zwar ein flächendeckender Einsatz noch nicht möglich, da die Produktionskosten wegen der geringen Stückzahlen relativ hoch sind. Größere Mengen würden den Preis aber durchaus in die Größenordnung von hundert bis zweihundert Schilling als einmalige Investition bringen. Daher ist der breite Ansatz biometrischer Absicherung für sensitive Anwendungen, wie zum Beispiel die EC - Kontokarte, stärkstens zu empfehlen.

3.1.5.4. Arten von biometrischen Verfahren[115]

Die Anforderung der biometrischen Verifikation an Merkmale, die bei jedem Mensch verschieden und für eine Person eindeutig sind, kann durch Vergleich von verschiedenen Stellen des Körpers und Verhaltensweisen eines Menschen erfüllt werden. Man kategorisiert in statische und dynamische Verfahren. Statisch sind die Verfahren immer dann, wenn eine anatomische Eigenschaft gemessen wird. Zu dieser Gruppe zählen: Messung des Fingerabdrucks, der Handgeometrie oder des Augenhintergrundes. Die Verifikation auf Grund genetischer Merkmale wird zur Zeit gerade erforscht. Ein Verfahren wird als dynamisch bezeichnet, wenn die Grundlage der Messung eine Handlung einer Person ist. Beispielhaft dafür sind: Dynamik der handschriftlichen Unterschrift, Sprecherverifikation oder die Messung des individuellen Verhaltens beim Tippen an einer Tastatur. Dynamische Verfahren kennzeichnen sich durch kurzfristige, physisch und psychisch bedingte Schwankungen aus, die eine oftmalige Anpassung des Referenzdatensatzes erfordern.

3.1.5.4.1. Fingerabdruck

Bei diesem Verfahren werden die bei jedem Menschen unterschiedlichen Bögen und Schleifen ausgewertet. Bei älteren Verfahren legte man die Fingerkuppen auf eine Glasplatte, der darunterliegende Scanner erstellte eine Image-Datei. Vor kurzem wurde von der Firma SGS Thomson

---

[115] C'T Report, Geld Online 2 (1997), S. 145 ff.

ein Sensor entwickelt, der das Linienmuster direkt erkennen kann. Durch die Reduktion der Größe kann nun die Überprüfung des Fingerabdruckes direkt auf der Smartcard durchgeführt werden. Dadurch müssen die Referenzdaten nicht außerhalb der Karte gespeichert werden, ein wichtiger datenschutzrechtlicher Aspekt.

Die Fehlerquote ist bei diesem Verfahren die geringste. Es wird erwartet, daß bei industrieller Produktion dieser Chips die sinkenden Preise eine weite Verbreitung erlauben. ME ist diese Methode am besten für biometrische Erkennung geeignet.

3.2. Einführung einer Public Key Infrastructure

3.2.1. Problem der nicht nachweisbaren Identität und weitere Anforderungen an sichere elektronische Kommunikation

Die Verwendung elektronischer Signaturen ohne Zertifikat ist aber noch keine vollständige Problemlösung. Es wird lediglich sichergestellt, daß das signierte Dokument von demjenigen stammt, der Verfügungsgewalt über den korrespondierenden privaten Schlüssel hat. In diesem Verwendungsstadium ist nur die Übereinstimmung der Identität des Absenders mit dem Namen, den er im öffentlichen Schlüssel angibt, gewährleistet. Schlüssel können aber von jedem - zum Beispiel unter Zuhilfenahme des weit verbreiteten Programms PGP – auf dem eigenen PC selbst hergestellt werden. Als Teil des Schlüsselgenerierungsprozesses muß nun auch der Name des Benutzers dieses Schlüsselpaars eingegeben werden. Der ehrliche Anwender trägt hier nun seinen eigenen Namen ein. Es bestehen zu diesem Zeitpunkt aber gar keine Hindernisse, einen fiktiven Namen zu verwenden. Nach erfolgreicher Erstellung des Schlüsselpaares wird nun der öffentliche Schlüssel an einen Keyserver weitergeleitet, von dem alle Internetanwender, gleich einem Telefonbuch, den öffentlichen Schlüssel eines Kontaktpartners beziehen können. Die Suche erfolgt hierbei nach dem Namen des Anwenders, dessen öffentlichen Schlüssel man benötigt. Wird ein öffentlicher Schlüssel mit einem unrichtigen Eintrag des Namens auf den Server gespielt, wird dieser bei einer Abfrage ungeprüft weitergegeben. Der Adressat hat keine Gewißheit, ob sich „hinter dem öffentlichen Schlüssel" nicht eine Person hinter falscher Identität verbirgt.

In diesem Stadium ist nur sichergestellt, daß die Nachricht nicht während der Übermittlung von Dritten verfälscht werden kann und sie so, wie sie der Adressat erhält, authentisch vom Absender stammt. Über die Per-

son des Absenders stehen keine vertrauenswürdigen Informationen zur Verfügung. Diese mangelnde Verifikation der Identität macht das Verfahren daher in diesem Entwicklungszustand für die Übermittlung rechtsverbindlicher Willenserklärungen ungeeignet. Es wird noch zusätzliche Funktionalität benötigt[116], die ein Vertrauen in die Richtigkeit der Personendaten ermöglicht. Dazu wurden zwei unterschiedliche Lösungsansätze entwickelt, wobei das ältere Verfahren im folgenden Punkt beschrieben wird und dem anderen, das unter Zuhilfenahme von Zertifizierungsdienstanbietern realisiert wird, der nächste Abschnitt gewidmet ist.

Um den Anforderungen des elektronischen Geschäftsverkehrs gerecht zu werden muß über die Gewährleistung der richtigen Identität hinaus auch noch weitere Funktionalität gewährleistet sein. Damit das Vertrauen in die Eignung der elektronischen Kommunikation über offene Netze, welches eine unerläßliche Voraussetzung für den Einsatz dieser Technik im Rechts- und Geschäftsverkehr bildet, gewährleistet ist, müssen auch alle Funktionen, die vom Geschäftsverkehr in Papierform und über geschlossene Netze verlangt werden, bei der elektronischen Kommuniaktion über offene Netze zur Verfügung stehen.

Folgende Voraussetzungen müssen daher in einem vertrauenswürdigen System zur sicheren und rechtsverbindlichen elektronischen Kommunikation eingehalten werden:

- Die Identifikation der einzelnen Teilnehmer muß für die Kommunizierenden sichergestellt werden.
- Die Authentizität der Handlungen der Teilnehmer muß gewährleistet sein, wobei die Nachricht von der angegebenen Quelle stammen muß und während der Übermittlung keine Veränderung des Inhalts vorkommen darf.
- Abgegebene Willenserklärungen dürfen nicht erfolgreich abgestritten werden können.
- Die Sicherheit der eingesetzten Verfahren und technischen Produkte soll einem hohen Standard entsprechen.
- Grenzüberschreitende, möglichst weltweite Harmonisierung der Public Key Infrastrukturen in den einzelnen Nationalstaaten und die gegenseitige Anerkennung gleichwertiger elektronischer Signaturen und Zertifikate muß erreicht werden.

---

[116] *Angel,* Why use Digital Signatures for Electronic Commerce, JILT 2 (1999), http://www.law.warwick.ac.uk/jilt/99-2/angel.html.

3.2.2. Lösungsversuch im liberalen Web of Trust, ohne Zertifizierungsdiensteanbieter

Die von *Phil Zimmermann* entwickelte Methode beruht auf einer Bewertung der Vertrauenswürdigkeit der Angaben von Namen durch die Anwender selbst, um auch für PGP-Anwender, deren Programm keine Zertifikate unterstützt, ein Vertrauen in die Richtigkeit der Angaben fremder Schlüssel zu ermöglichen. Die einzelnen Schlüsselinhaber bestätigen mit ihrer elektronischen Signatur, daß die personellen Daten, zugeordnet zu einem öffentlichen Schlüssel eines Dritten, den sie kennen, auch der Wahrheit entsprechen. Je mehr solche Bestätigungen ein öffentlicher Schlüssel aufweisen kann, desto größer ist die Wahrscheinlichkeit, daß die Personenangaben der Wahrheit entsprechen. Die Anzeige, wieviele Leute dem jeweiligen öffentlichen Schlüssel vertrauen, erfolgt direkt in PGP selbst. Die Vertrauenswürdigkeit der jeweiligen Schlüssel wird in PGP durch eine Skala angezeigt.[117] Es werden weder auf dem Client noch auf dem Keyserver zusätzliche Programme benötigt und der Aufbau einer komplexen Public Key Infrastructure entfällt. Der Vorteil liegt im völligen Wegfall einer aufwendigen Public Key Infrastructure und der Trusted Third Parties, die zur Zertifikatsverwaltung benötigt werden.

So gut dieses System für die Kommunikation in einer kleinen, überschaubaren Gruppe geeignet ist, in der weltweiten Kommunikation zwischen Unbekannten in offenen Netzen ist es nicht anwendbar, weil eine immens hohe Menge an Beglaubigungen von Privaten für jeden einzelnen öffentlichen Schlüssel notwendig ist, damit auch nur annähernd sichergestellt ist, daß ein zufällig gewählter Kommunikationspartner zumindest einen der Anwender kennt, der die Richtigkeit der Angaben des Absenderschlüssels bestätigt. Es wird auch von keinem Gesetz, das die Verwendung elektronischer Signaturen regelt, als genügend angesehen.

Die unumgehbare und abgesicherte Bindung der realen Person an ihr Handeln im Web kann auch durch ein anderes System besser gewährleistet werden.

3.2.3. Errichtung einer Public Key Infrastructure

Um auch bei der Kommunikation zwischen Unbekannten die richtige Bindung der Identität an den jeweiligen öffentlichen Schlüssels sicher zustellen, bedarf es des Zusammenwirkens mehrerer Komponenten. Eine zentrale Bedeutung kommt Stellen zu, die Zertifikate für die bei ihnen re-

[117] Manual: PGP für Personal Privacy Version 5.5, S. 69ff.

gistrierten Anwender ausstellen, in denen ein Bezug zwischen öffentlichem Schlüssel und Namen des Verfügungsberechtigten hergestellt wird. SigG und SigRL bezeichnen diese vertrauenswürdigen Dritten als Zertifizierungsdiensteanbieter.[118] Sie übernehmen die meisten Aufgaben in diesem Bereich und sind zuständig für die Registrierung der Teilnehmer, die Ausstellung des Zertifikats, Bereitsstellung aller von ihnen ausgestellten Zertifikate in einem öffentlich zugänglichen Verzeichnis und den Widerruf von Zertifikaten, falls diese nicht mehr verwendbar sind. Da mehrere Zertifizierungsdiensteanbieter existieren, die jeweils nur einen Teil der im Internet kommunizierenden Anwender registrieren, muß auch die gegenseitige Anerkennung und Zusammenarbeit der einzelnen Diensteanbieter gewährleistet sein. Schlußendlich garantiert ein hoheitliches Aufsichtssystem für die Einhaltung der Sicherheitsstandards aller Teilnehmer und kontrolliert neu entwickelte technische Komponenten und Verfahren auf ihre Eignung für die Verwendung im System. Da sich der einzelne Anwender nicht an viele verschiedene Stellen wenden soll, um elektronisch zu signieren oder eine Signatur zu prüfen, muß die reibungslose Zusammenarbeit aller am System beteiligten Stellen gewährleistet sein.

3.2.3.1. Begriff der Public Key Infrastructure

Zur Erklärung des Begriffs Public Key Infrastructure ist es vor allem notwendig zu erörtern, was allgemein unter einer Infrastruktur zu verstehen ist, um danach auf die speziellen Eigenschaften einer Public Key Infrastructure, die die Kommunikation mittels asymmetrischer Kryptographie ermöglicht, einzugehen.

3.2.3.1.1. Infrastruktur im allgemeinen

Innerhalb der Gesellschaft kann man zwischen sozialen, technischen und rechtlichen Infrastrukturen unterscheiden, die auch große Überschneidungen aufweisen. Das wesentliche Merkmal aller Infrastrukturen besteht darin, daß sie etwas zur Verfügung stellen, und der Nutzer sie verwenden kann. *Volker Hammer*[119] erarbeitete 3 Charakteristiken für Infrastrukturen:

---

[118] Auch andere Begriffe werden verwendet. So spricht das deutsche SigG von Zertifizierungsstellen, auch der Begriff Zertifizierungsinstanz ist in der Literatur zu finden. Im englischsprachigen Raum werden hauptsächlich die Begriffe Certification Authorities und Trusted Third Parties verwendet.

[119] *Hammer*, Gateway: Infrastruktur, DuD (1995), S. 293.

- das Angebot gleicher Leistung für viele Nutzer
- die zeitliche Konstanz der angebotenen Leistungen
- das Verbergen der internen Komplexität, die zur Bereitstellung der Leistung beherrscht werden muß, gegenüber den Anwendern.

Der erste Punkt ist besonders für eine Infrastruktur, die Kommunikationsdienste anbietet, bedeutend, da der einzelne Anwender möglichst viele Teilnehmer im selben Netz erreichen will. Er verwendet die Dienste der Infrastruktur nicht nur isoliert für sich selbst,[120] sondern will immer mit anderen Teilnehmern derselben Infrastruktur in Interaktion treten. Je mehr Anbieter daher von der gleichen Infrastruktur Gebrauch machen, desto eher ist gewährleistet, daß man einen potentiellen Kommunikationspartner auch innerhalb einer Infrastruktur mit der Verwendung der gleichen Technik erreichen kann und an die übermittelten elektronischen Dokumente einheitliche Rechtsfolgen geknüpft werden. Diese Überlegung ist auch in den Richtlinienvorschlag eingeflossen[121], der als erstes Ziel fordert, „ ... angemessene harmonisierte rechtliche Rahmenbedingungen für den Einsatz elektronischer Signaturen in der Europäischen Gemeinschaft zu schaffen...", und für ein Fehlen dieser Rahmenbedingungen den Schluß zieht: „Diese [vor Geltung einer europaweiten SigRL] uneinheitliche Entwicklung kann ein ernsthaftes Hindernis für die Kommunikation und den Geschäftsverkehr über offene Netze in der Europäischen Gemeinschaft darstellen."

Auch der deutsche Gesetzgeber versteht sein Signaturgesetz als gesetzliche Regelung, in der ein administrativer Rahmen geschaffen wird, der zu allgemein anerkannten digitalen Signaturen führt.[122]

Infrastrukturen müssen zeitlich konstant verfügbar und die Aufwendungen, die die einzelnen Anwender zur Nutzung der angebotenen Dienste machen, längerfristig verwendbar sein. Die Leistungsmerkmale einer Infrastruktur haben daher langlebig und stabil zu sein, so daß eine Veränderung des Angebots der Dienste nur in Zeiträumen erfolgt, die um Größenordnungen länger dauert als die einzelnen Inanspruchnahmen. Ebenso ist die Garantie einer Vorhersehbarkeit der Verwendung auch in der Zukunft erforderlich. Gerade die Schnellebigkeit der elektronischen Medien, die schnelle Aufeinanderfolge neuer Protokolle und Dienste und die teil-

[120] Wie es zum Beispiel bei der Abfallentsorgung der Fall wäre.

[121] Ziel 1, KOM (98) 297, S. 6.

[122] Begründung zum Gesetzesentwurf der Bundesregierung IuKDG, BR-Drucksache 966/96, S. 28.

weise Inkompatibilität neuer Entwicklungen zu schon länger angewandten Standards stellen eine große Hürde für die erforderliche Kontinuität dar.[123] Zur Gewährleistung der langfristigen Verfügbarkeit reicht daher die Selbstregulierung durch Markt und Gesellschaft alleine nicht aus. Eine Funktion des Gesetzgebers in diesem Regelungsbereich ist es, die langfristige Verfügbarkeit von Mindeststandards durch allgemein verbindliche Normen zu garantieren.

Weiters kann dem Anwender nicht zugemutet werden, die gesamte komplexe Funktionalität, die die Infrastruktur anbietet, detailliert zu verstehen. Expertenwissen haben die Betreiber der einzelnen Komponenten, die die Infrastruktur bilden, und die Organe, die den reibungslosen Ablauf kontrollieren. Der einzelne Anwender benötigt nur das Wissen, wie er an einer der Endstellen der Infrastruktur, wo eben ihr Service angeboten wird, andocken kann und - im Fall der Public Key Infrastructure – wen seine Informationen am anderen Ende des Netzes erreichen sollen. Auf welchem Weg die Dienste erbracht werden und welche Arbeitsschritte dafür notwendig sind, entzieht sich der Kenntnis des Anwenders.

3.2.3.1.2. Public Key Infrastructure im besonderen

Die Sicherstellung der Identität des Vertragspartners und die Authentizität seiner Willenserklärung ist die Grundlage unserer Rechtsordnung für rechtlich verbindliches Handeln. In der realen Welt wird dies meist durch von hoheitlichen Stellen ausgestellte Ausweise, durch Eintragung der Prokuristen in das Firmenbuch und der Eigentümer von Liegenschaften in das Grundbuch und ähnliches erreicht. Diese Variante eines elektronischen amtlichen Ausweises wird derzeit gerade in Finnland entwickelt. Das finnische Einwohnermeldeamt wird auch als Zertifizierungsdiensteanbieter tätig und vergibt an die Einwohner Smart Cards, die einerseits mit Lichtbild und den persönlichen Daten des Trägers bedruckt sind, andererseits aber auch im Prozessor der Karte eine elektronische Signatur und ein Zertifikat beinhalten. Die damit erzeugten elektronischen Signaturen können nicht nur im Verkehr mit der Behörde verwendet werden, sondern sind auch zur Kommunikation mit Privaten einsetzbar.

Einander bekannte Personen identifizieren sich durch ihre charakteristische eigenhändige Unterschrift, durch Photos oder durch ihre Stimmerkmale. Die Weiterleitung der Nachrichten nur an die gewünschte Person wird durch Institutionen wie Post und Telefongesellschaften gewähr-

---

[123] Mit dieser Formulierung hat *Hammer* das der SigRL zu Grunde gelegte Prinzip gerade zu vorhergesehen (Zitat FN 119, DuD (1995), S. 293).

leistet. Durch Organisationsgesetze, wie das Postgesetz 1997[124] oder das Zustellgesetz[125], Schutzbestimmungen, wie die Grundrechte auf Brief- und Fernmeldegeheimnis, spannt die Rechtsordnung ein Grundgerüst für die Wahrung der Identität und Authentizität in der konventionellen Kommunikationsinfrastruktur.

Zur Lösung des weiter oben diskutierten Problems der nicht nachweisbaren Identität wird bei der Telekooperation die institutionelle Bindung der handelnden Person an ihre Identität durch die Verwendung asymmetrischer Kryptographie und Zertifizierung der öffentlichen Schlüssel sichergestellt. Mit der Zertifizierung durch eine vertrauenswürdige Stelle ist sichergestellt, daß die jeweilige Signaturerstellungs- und Signaturprüfeinheit auch dem tatsächlich Verfügungsberechtigten zugeordnet ist.

Eine Public Key Infrastructure wird durch die Gesamtheit aller Einheiten, die zum Verwalten der öffentlichen Schlüssel benötigt werden, gebildet. In einer von der DG Informationsgesellschaft in Auftrag gegebenen Studie[126] wird eine Public Key Infrastructure als eine unterstützende Infrastruktur, die auch nicht-technische Aspekte umfaßt, für die Verwaltung öffentlicher Schlüssel definiert. Das Zusammenwirken der einzelnen Zertifizierungs- und Registrierungsdiensteanbieter sowie der Benutzer im Internet und die Kontrolle durch Regulierungs- und Aufsichtsbehörden schafft in Summe die Public Key Infrastructure. Sie bietet den Anwendern die Sicherstellung der Identität der Telekooperationspartner und die Authentizität der elektronischen Dokumente, so daß letztendlich die Dokumente, die unter Nutzung der Dienste der Public Key Infrastructure verschickt werden, die rechtlichen Anforderungen der Schriftlichkeit erfüllen und denselben Beweiswert wie ein traditionelles Schriftstück erhalten.

In der Begründung zum Signaturgesetzentwurf der Bundesregierung verwenden die Legisten auch den Begriff Sicherheitsinfrastruktur[127] in derselben Bedeutung wie Public Key Infrastructure. Eines der Ziele des Gesetzes ist es, einen administrativen Rahmen vorzugeben, daß eine sol-

---

[124] Bundesgesetz über das Postwesen (Postgesetz 1997) (NR: GP XX RV 940 AB 966 S. 105. BR: AB 5593 S. 633.) StF: BGBl. I Nr. 18/1998.

[125] Bundesgesetz vom 1. April 1982 über die Zustellung behördlicher Schriftstücke (Zustellgesetz) StF: BGBl. Nr. 200/1982.

[126] *Pohl*, Guidelines for the use of names and keys in a global TTP infrastructure, Report für DG Informationsgesellschaft (1997), S. 105.

[127] Begründung zum Gesetzesentwurf der Bundesregierung IuKDG, BR-Drucksache 966/96 S. 27.

che Infrastruktur mit hoher Qualität unter hoheitlicher Überwachung privatwirtschaftlich errichtet und betrieben werden kann.

Die Sicherstellung der qualitativen Anforderungen darf nicht nur für in Österreich oder in Mitgliedsstaaten der Europäischen Union niedergelassene Zertifizierungsdiensteanbieter gelten, sondern soll auf Grund der Grenzenlosigkeit des elektronischen Geschäftsverkehrs möglichst alle Teile des Internets umfassen. Deshalb regelt § 18 SigG die Anerkennung und Gleichstellung von qualifizierten Zertifikaten, die von einem in der Europäischen Gemeinschaft niedergelassenen Zertifizierungsdiensteanbieter ausgestellt wurden und deren Gültigkeit von Österreich aus überprüft werden kann. Zertifikate von einem Zertifizierungsdiensteanbieter, der in einem Drittstaat niedergelassen ist, werden anerkannt, wenn ihre Gültigkeit von Österreich aus überprüft werden kann. Für die rechtliche Gleichstellung qualifizierter Zertifikate aus Drittstaaten bedarf es der Einhaltung dreier alternativer Anforderungen: Entweder erfüllt der Zertifizierungsdiensteanbieter des Drittstaates die Anforderungen des SigG an Zertifizierungsdiensteanbieter für qualifizierte Zertifikate (§7 SigG) und ist unter einem freiwilligen Akkreditierungssystem eines Mitgliedstaates der Europäischen Union akkreditiert, oder die Europäische Union anerkennt in einer bilateralen oder multilateralen Vereinbarung die Zertifikate von im Drittstaat niedergelassenen Zertifizierungsdiensteanbietern oder diese Zertifizierungsdiensteanbieter als Aussteller qualifizierter Zertifikate. Am wirtschaftlich bedeutsamsten ist wohl die dritte Variante, gemäß § 24 SigG; nämlich die gesetzliche Anerkennungsvariante, daß ein in der Europäischen Union niedergelassener Zertifizierungsdiensteanbieter für qualifizierte elektronische Zertifikate haftungsrechtlich für die Zertifikate des Zertifizierungsdiensteanbieters aus einem Drittstaat einsteht.

3.2.3.2. Zertifizierungsdiensteanbieter

Zertifizierungsdiensteanbieter bieten Dienste für die Kommunikationsteilnehmer an, die diese eindeutig identifizieren und zertifizieren. Als direkte Bezugsperson sowohl bei der Ausstellung neuer Zertifikate als auch bei der Prüfung der Zertifikate des Senders durch den Empfänger und allgemein der Verwaltung aller von ihnen ausgestellten Zertifikate übernehmen sie die Hauptaufgaben innerhalb der Public Key Infrastructure. Sie benennen die Teilnehmer eindeutig und ordnen ihren öffentlichen Schlüsseln die jeweiligen Namen der verfügungsberechtigten Person zu. Dazu muß jeder Anwender einmal beim Registrierungsdiensteanbieter persönlich erscheinen, damit seine Identität überprüft werden kann.

Nachdem der Anwender sein Schlüsselpaar erstellt hat[128], wird ein Zertifikat ausgestellt, in dem Namen und eventuell noch andere Daten des Anwenders zusammen mit den Kenndaten seines öffentlichen Schlüssels und Angaben über den ausstellenden Zertifizierungsdiensteanbieters enthalten sind. Der zertifizierte Anwender schickt jedesmal mit seiner elektronischen Signatur auch noch dieses Zertifikat mit. Anhand dieses Zertifikats kann der Empfänger der Nachricht nun den Namen des Senders verifizieren. Der Zertifizierungsdiensteanbieter führt auch ein elektronisches, öffentlich zugängliches Verzeichnis[129], in dem die Gültigkeit aller von ihm ausgestellten Zertifikate überprüft wird. Jeder Zertifizierte kann die Sperrung seines Zertifikates unverzüglich verlangen, wodurch die widerrechtliche Verwendung weitergegebener privater Schlüssel angezeigt werden kann. Dieses System führt zu einer institutionellen Bindung der Person an ihre Identität im offenen Netz und damit zu einer unumgehbaren und abgesicherten Bindung der realen Person an ihr Handeln im Web.

Als Mindestanforderung muß daher der Zertifizierungsdiensteanbieter für die Anwender, die von ihm betreut werden, ein Zertifikat ausstellen, in dem zweifelsfrei die Identität des Benutzers des jeweiligen Schlüsselpaares nachgewiesen wird. Innerhalb der Infrastruktur hat gewährleistet zu sein, daß dem Aussteller von allen möglichen Adressaten des Schlüsselbenutzers Vertrauen in Bezug auf die Richtigkeit des Zertifikates entgegengebracht wird.

Auf Grund der Globalität des Internets ist es faktisch nicht möglich, diese Dienste durch nur einen Zertifizierungsdiensteanbieter anzubieten, es muß mehrere solche Stellen geben, die gleichberechtigt oder auch hierarchisch verknüpft zusammenarbeiten. Die Gesamtheit aller Einrichtungen, die mit Zertifizierung und Verwaltung der Zertifikate befaßt sind, bildet die Public Key Infrastructure.

Zusätzlich zum Ausstellen und Verwalten der Zertifikate besteht noch die Möglichkeit, als Zertifizierungsdiensteanbieter zusätzliche Dienste anzubieten, wie die Generierung der Schlüssel oder die Bestätigung der Absendezeit elektronisch signierter Dokumente.

---

[128] Unter Einhaltung besonderer Sicherheitsvorschriften kann das Schlüsselpaar für den Anwender auch vom Zertifizierungsdiensteanbieter erstellt werden.

[129] Dieses Verzeichnis wir in der Regel im Internet auf der Homepage des Zertifizierungsdiensteanbieter zur Verfügung gestellt.

3.2.3.3. Zertifikate

Als Zertifikate im Rahmen einer Public Key Infrastructure bezeichnet man eine strukturierte Nachricht, die Attribute unterschiedlicher Art in sicherer Form an einen öffentlichen Schlüssel bindet.[130] Auf Grund dieser Definition ergibt sich folgender Mindestinhalt für ein Zertifikat: Einerseits muß die Einheit genannt werden, die den zertifizierten öffentlichen Schlüssel verwendet. Aus technischer Sicht muß das keine Person sein, sondern kann zum Beispiel auch der Name eines Servers sein, der Zeitstempel vergibt. Weiters muß der öffentliche Schlüssel, der der zertifizierten Einheit zugeordnet ist, im Zertifikat enthalten sein. Schlußendlich muß das Zertifikat selbst von der ausstellenden Organisation elektronisch signiert werden, damit Manipulationen Dritter auszuschließen sind. Zertifikate müssen daher zumindest folgende Angaben enthalten, um ihre Funktionalität erfüllen zu können.

- Name des Anwenders
- öffentlicher Schlüssel des Anwenders
- elektronische Signatur des Zertifizierungsdiensteanbieters

Eine internationale Normierung[131] für den Aufbau und Inhalt von Zertifikaten erfolgte durch den Standard ITU-T[132] X.509[133,134] in der derzeit aktuellen Version 3. Da er in fast allen Ländern konform mit den gesetzli-

---

[130] *Pohl,* Guidelines for the use of names and keys in a global TTP infrastructure, Report für DG Informationsgesellschaft (1997), S. 27.

[131] Die Normierung durch die International Telekommunication Union gewährt eine weltweite Akzeptanz dieses Standards, wie es im Bereich des elektronischen Geschäftsverkehr unerläßlich ist.

[132] Die International Telecommunication Union (ITU (dt. = Internationale Fernmeldeunion)) ist eine Spezialorganisation der UNO, deren Aufgaben die Förderung der Zusammenarbeit der Völker durch einen guten Fernmeldedienst, die Zuweisung der Frequenzbereiche, die Registrierung der Frequenzzuteilungen und die Schaffung, Entwicklung und Vervollkommnung der Fernmeldeeinrichtungen und Fernmeldenetze in den Entwicklungsländern ist.

[133] X.509 ist ein Teil des ITU-T Standards X.500 der allgemein Verzeichnisdienste definiert. X.500 wird von den meistens Zertifizierungsdiensteanbietern verwendet, um ihre Zertifikatsverzeichnisse zu strukturieren. Zertifikate, die in Verzeichnissen nach diesem Standard verwaltet werden, sollten nach X.509 strukturiert sein.

[134] Auch bekannt als: ISO/IEC 9594-8 oder früher als: CCITT X.509.

chen Vorschriften über Zertifizierungsdienste ist, wird er von fast allen Zertifizierungsdiensteanbietern verwendet.[135]

Ein Zertifikat hat nach den Regeln des X.509 folgenden Inhalt und Aufbau:

- Strukturierter Datensatz, der Identität der Person und Public Key verknüpft
- Vertrauenswürdig -> deshalb von CA verschlüsselt mit Private Key
- CA bestätigt mit ihrer Dig Sig, daß Identität und Public Key übereinstimmen
- Empfänger kann von CA das Zertifikat des Senders anfordern
- Weitere Infos sind sinnvoll:

Eine detaillierte Beschreibung der Struktur der ausgestellten Zertifikate ist im Sicherheits- und Zertifizierungskonzept darzulegen. Folgende Felder sind für ein Zertifikat gemäß dem Standard CCITT X.509v3 vorgesehen:

- Version: Versionsnummer der Version von X.509, der das Zertifikat entspricht Da auch die Version 2 von X.509 dem SigG entspricht, muß ersichtlich sein, ob es sich um Version 2 oder 3 handelt.
- Seriennummer: Eine eindeutige, einzigartige Nummer für jedes Zertifikat, das ein Zertifizierungsdiensteanbieter ausstellt
- Bezeichnung des Kryptoalgorithmus, den der Zertifizierungsdiensteanbieter zur elektronischen Signierung des Zertifikats verwendet hat. Falls nötig können hier auch noch zusätzliche Parameter dieses Algorithmus angeführt werden.
- Aussteller: Name des ausstellenden Zertifizierungsdiensteanbieters in der Struktur von X.500. Durch die Ausnahmebestimmung des § 2 Z.2 SigG ist hier auch die direkte Nennung juristischer Personen möglich, soweit diese als Zertifizierungsdiensteanbieter agieren und dieses Zertifikat ausschließlich zum Signieren von Anwenderzertifikaten oder zur Erbringung anderer Zertifizierungsdienste verwenden.[136]
- Gültigkeit: Hier sind sowohl Datumsangaben für den Beginn als auch das Ende des Gültigkeitszeitraumes zu machen.

---

[135] Einige Zertifizierungsdiensteanbieter der ersten Stunde zertifizieren allerdings auch noch PGP Schlüssel, die sich bei Anwendung von X.509 nicht zertifizieren lassen.

[136] *Brenn*, Signaturgesetz, S. 54.

- Name des Signators. Der Name muß aus einem amtlichen Lichtbildausweis entnommen werden. Die Nennung von Pseudonymen ist zulässig, wobei diese zusätzlich als solches zu bezeichnen sind.
- Information über den öffentlichen Schlüssel des Zertifizierten: Sowohl die Signaturprüfdaten selbst, als auch Angaben, welchen Kryptoalgorithmus der Zertifizierte zum elektronisch Signieren verwendet, müssen angeführt werden.
- Optional können Zusatzinformationen aufgenommen werden, wie zum Beispiel Angaben über die Vertretungsmacht des Signators oder dessen Beruf.

Weiters verlangt § 5 SigG in Umsetzung des Anhangs I der SigRL noch zusätzlich folgende Angaben in qualifizierten Zertifikaten:

- Hinweis, daß es sich um ein qualifiziertes Zertifikat handelt
- Der Name des Zertifizierungsdiensteanbieter muß unverwechselbar sein, und sein Niederlassungsstaat muß angeführt sein.
- Gegebenenfalls eine Einschränkung des Anwendungsbereiches und des Transaktionswertes des Zertifikates
- Der Zertifizierungsdiensteanbieter muß das Zertifikat mit seiner sicheren elektronischen Signatur versehen

4. Rechtliche Regulierung der Public Key Infrastructure in der Europäischen Union und Österreich

4.1. Entstehungsgeschichte des SigG

Parallel zur Entstehung des deutschen SigG kam es auch in Österreich zu ersten Überlegungen über eine gesetzliche Regulierung öffentlicher Public-Key-Infrastrukturen und über die Rechtswirkung elektronischer Signaturen. Einerseits wurde Anfang 1998 ein privater Expertenentwurf[1], der inhaltlich stark an das damalige deutsche Signaturgesetz angelehnt ist, zu einem SigG veröffentlicht, andererseits beschäftigte sich die im Bundeskanzleramt für Datenschutz zuständige Abteilung mit der Problematik. Beide Vorschläge wurden aber nie im Parlament behandelt und erlangten daher auch nicht die Stellung einer Regierungsvorlage. Als im Mai 1998 der erste Entwurf[2] für eine Richtlinie der Europäischen Gemeinschaft über Rahmenbedingungen für elektronische Signaturen vorlag und in den darauffolgenden Monaten heftig diskutiert wurde, war daher noch nicht mit Sicherheit festgelegt, welcher Freiraum den einzelnen Mitgliedsstaaten zur Regelung einer Sicherheitsinfrastruktur zur Verfügung stand. Man beschloß, mit einer österreichischen Regelung zu warten, bis der Inhalt der SigRL fixiert war. Die federführende Zuständigkeit für die Ausarbeitung ging vom Bundeskanzleramt zum Justizministerium über, wobei jedoch eine enge Zusammenarbeit der beiden Ministerien stattfand.

Nicht einmal drei Monate nach dem politischen Konsens über den Gemeinsamen Standpunkt für einen Entwurf zur SigRL am 22.04.1999 wurde der österreichische Entwurf vom Parlament mit geringfügigen Abänderungen durch den Justizausschuß des Nationalrates am 14. Juli 1999 beschlossen und als Bundesgesetz am 19. August 1999 im BGBl[3] verlautbart.Am 1. Januar 2000 ist es plangemäß in Kraft getreten.[4] Österreich ist

---

[1] *Mayer-Schönberger/Pilz/Reiser/Schmölzer,* Sicher und Echt: Der Entwurf eines SigG, MuR 3 (1998), S. 107ff.

[2] KOM(1998) 297.

[3] BGBl 190/1999.

[4] Regierungsvorlage und Erläuterungen für ein Bundesgesetz über elektronische Signaturen (SigG) 1999 der Beilagen zu den Stenographischen Protokollen des Nationalrates der XX. Gesetzgebungsperiode in der Fassung nach dem Bericht des parlamentarischen Justizausschusses 2065 der Beilagen zu den Stenographischen Protokollen des

somit der dritte Mitgliedsstaat der Europäischen Union[5] mit einem Signaturgesetz (im folgenden: SigG) und gleichzeitig der erste, dessen innerstaatliche Regelungen in allen Punkten konform zur SigRL sind. Die SigRL selbst wurde in einem der Ministerräte der Europäischen Union im Jahr 2000 ohne Debatte formal verabschiedet und danach im Europäischen Parlament in zweiter Lesung behandelt. Sie wurde als Richtlinie 1999/93/EG des Europaeischen Parlaments und des Rates vom 13. Dezember 1999 ueber gemeinschaftliche Rahmenbedingungen fuer elektronische Signaturen im
Amtsblatt Nr. L 013 vom 19/01/2000 S. 0012-0020 veröffentlicht.

Auf Grund der Verordnungsermächtigung des § 25 SigG wurde Anfang Oktober 1999 ein Entwurf einer Signaturverordnung fertiggestellt. Der Entwurf wurde anschließend von Österreich der EU-Kommission notifiziert. Nach dem Notifikationsgesetz 1999[6] und der Richtlinie 98/34/EG idF. der Richtlinie 98/48/EG) lief dann eine dreimonatige Frist, innerhalb derer die anderen Mitgliedstaaten der Europäischen Union zum Verordnungsentwurf Stellung nehmen können. Die Stellungnahme ergab nur kleine Änderung bei den Anforderungen an die Mindestlänge von Schlüsseln, die bei elliptischen Verschlüsselungsverfahren eingesetzt werden. Die Signaturverordnung wurde am 2. 2. 2000 im BGBl II 30/2000 veröffentlicht und trat rückwirkend mit 1. 1. 2000 in Kraft.

4.2. Systematik des SigG

Ziel des SigG ist es, einen rechtlichen Rahmen für den Einsatz elektronischer Signaturen vorzugeben, um durch Einsatz sicherer Technologien und Verfahren die notwendige Rechtssicherheit in der Form vollwertiger Anerkennung elektronischer Signaturen im Sinn einer Gleichstellung ihrer Rechtswirkungen mit der eigenhändigen Unterschrift[7] zu gewährleisten. Dazu werden zwei wesentliche Regelungsgebiete normiert. Einerseits müssen Sicherheitsbestimmungen für die Zertifizierungsdiensteanbieter vorgegeben werden, damit das Vertrauen der Anwender in die Infrastruktur zur Bereitstellung elektronischer Signaturen gegeben ist. Andererseits bedarf es Regelungen zur rechtlichen Anerkennung der mit

---

Nationalrates der XX. Gesetzgebungsperiode. Die ö RV SigG und der Bericht des Justizausschusses sind unter folgender Adresse verfügbar:
http://www.univie.ac.at/RI/AJLI/3/index.htm.

[5] Nach Deutschland und Italien.

[6] BGBl. I Nr. 183/1999.

[7] EBRV SigG Allgemeiner Teil.

elektronischen Signaturen erzeugten Dokumente und Bestimmungen über spezielle Haftungstatbestände für Zertifizierungsdiensteanbieter.

Der Teil des SigG, der der Ausgestaltung der Infrastruktur dient, ist dem öffentlichen Recht zuzuordnen, da es sich um ordnungspolitische Vorschriften handelt, deren Einhaltung durch hoheitliche Maßnahmen[8] im Rahmen eines Aufsichtssystem vollzogen wird. Das SigG berücksichtigt hier die Definition von elektronischen Signaturen und Zertifikaten verschiedener Qualität im ersten Abschnitt, die Normierung der Tätigkeit der Zertifizierungsdiensteanbieter in Abschnitt 2 und ein System der Aufsicht im folgenden Abschnitt. Jeweils ein eigener Abschnitt ist den technischen Sicherheitserfordernissen der eingesetzten Verfahren und den Rechten und Pflichten der Anwender gewidmet. Die Nichteinhaltung aller dieser Anforderungen steht unter den Strafdrohungen einiger Verwaltungsstrafbestimmungen in § 26.[9] Schlußendlich wird der Bundeskanzler gemeinsam mit dem Bundesminister für Justiz zum Erlaß einer SigVO verpflichtet, um Details festzulegen. Dieser Teil des SigG beinhaltet quantitativ einen überwiegenden Teil der Bestimmungen und determiniert in Verbindung mit der SigVO die Ausgestaltung der Public Key Infrastructure in Österreich. Der SigVO bleibt die Regelung der technischen Details verwendeter Verfahren vorbehalten, da durch den einfacheren und schnelleren Prozeß der Normerzeugung im Verordnungsbereich besser auf technische Neuentwicklungen reagiert werden kann.

Um die erzeugten elektronischen Signaturen und Zertifikate jetzt auch im Rechtsverkehr verwenden zu können, werden im zweiten inhaltlichen Bereich die Rechtswirkungen elektronischer Signaturen festgelegt. Obwohl diesem Bereich nur 2 Abschnitte – Rechtserheblichkeit elektronischer Signaturen und die Anerkennung ausländischer Zertifikate – und ein Paragraph über die Haftung der Zertifizierungsdiensteanbieter in einem ordnungsrechtlichen Abschnitt gewidmet sind, ist seine Bedeutung sehr erheblich. Ohne rechtliche Anerkennung elektronisch signierter Dokumente wäre die elektronische Kommunikation nur für schmale Randbereiche von Bedeutung und würde keine große Verbreitung finden. Deswegen wurden auch die verschiedenen Modelle für die Ausgestaltung der Rechtswirkung sowohl auf europäischer Ebene als auch im Bereich der

---

[8] So hat die Aufsichtsstelle gemäß § 17 Abs. 6 das AVG 1991 in ihren Verfahren anzuwenden.

[9] Alle Nennungen ohne Gesetzeszitat beziehen sich auf das österreichische Signaturgesetz (SigG).

Gesetzgebung der Mitgliedsstaaten der Europäischen Union heftigst diskutiert.[10]

Österreich wählte im SigG ein Modell, das für den Bereich der elektronisch signierten Dokumente keine neue Textform und elektronischen Urkundenbeweis einführt, sondern die bestehenden Regelungen über Schriftform und Urkundenbeweis traditioneller Dokumente in Papierform mit Einschränkungen auf den Bereich der elektronischen Kommunikation anwendbar erklärt. Die einzelnen Bestimmung zur Umsetzung der Rechtswirkungen befinden sich zentralisiert im SigG. Es wurde keine Novellierung der bestehenden einzelnen Gesetze, wie ZPO oder ABGB, vorgenommen, sondern die Anwendbarkeit einzelner Bestimmungen dieser Gesetze durch § 4 auch auf elektronisch signierte Dokumente erweitert, ohne den Wortlaut in ZPO und ABGB zu verändern.

Vorerst nicht verwirklicht wurden Anregungen, einen allgemein rechtlichen Rahmen für die elektronische Signatur durch Änderungen des Strafrechts und des Verwaltungsrechts, des Gerichtsorganisationsgesetzes, der Zivilprozeßordnung, des Bundesarchivgesetzes beziehungsweise sonstiger Rechtsvorschriften zeitgleich mit dem Signaturgesetz abzustekken.[11] Diese Änderungen sind aber nicht grundsätzlich auszuschließen, sondern sollen erst nach einer Zeit der praktischen Erprobung und des Gewinnens weiterer Erfahrung erfolgen, wie dies einer Stellungnahme des OGH zum SigG bezüglich des Beweiswertes elektronischer Signaturen zu entnehmen ist.

Das SigG verzichtet auf besondere Regelungen über Anfechtung, Zugang und Widerruf elektronisch übermittelter Willenserklärungen. Die allgemeinen Vorschriften des Rechts der Willenserklärungen im ABGB, ergänzt durch die von Lehre und Rechtsprechung entwickelten Auslegungskriterien und Wertungen, bieten eine hinreichende Grundlage dafür, auch im Bereich der elektronisch übermittelten Willenserklärungen zu angemessenen und sich in das Gesamtsystem einfügenden Lösungen zu gelangen. Insbesondere das Problem der Willensbildung bei Computererklärungen, wie z.B. Angebote oder Annahmeerklärungen, die automatisch gemäß eines Programmablaufes generiert werden, kann unter allgemeine Rechtsnormen subsumiert werden. Nach herrschender Meinung handelt es sich um Willenserklärungen, da der Einsatz des Computerprogramms

---

[10] Einen Überblick über die Regelungsmodelle der verschiedenen Staaten findet man unter: http://cwis.kub.nl/~frw/people/hof/DS-lawsu.htm.

[11] EBRV zu Allgemeiner Teil Punkt 5.

letztendlich auf eine willentliche Entscheidung eines Menschen zurückgeht.[12]

Das Haftpflichtrecht wurde durch einen Spezialtatbestand der Haftung von Zertifizierungsdiensteanbietern novelliert, der auch als Bestimmung des SigG normiert wurde, wodurch auch hier keine Änderung bestehender Rechtsvorschriften, insbesondere des Schadenersatzrechtes des ABGB, erfolgte. Bei dieser Bestimmung handelt es um eine Mindesthaftung. Bestehende und künftige Haftungsbestimmungen in anderen einschlägigen Rechtsvorschriften[13] bleiben unberührt.

4.3. Abgestuftes System

Wie es die SigRL vorsieht, ermöglicht auch das SigG durch die Bestimmung in § 3 Abs. 1, einzelne Elemente der Infrastruktur auf unterschiedlichem Sicherheitsniveau zu positionieren. Je nach Aufwand erlangen die Signaturen und mit ihnen signierte elektronische Dokumente unterschiedliche Rechtserheblichkeit; auch beim Zugang zum Markt und bei der Haftung von Zertifizierungsdiensteanbietern differenziert das SigG.

Prinzipiell wird im Sinne einer gemeinschaftskonformen Nichtdiskriminierungsklausel[14] in § 3 Abs. 1 festgelegt, daß sämtliche elektronische Signaturverfahren im Rechts- und Geschäftsverkehr eingesetzt werden dürfen, soweit durch andere Rechtsvorschriften und Parteienvereinbarung nicht etwas anderes bestimmt wird. Jede Art von Signaturverfahren kann angeboten und verwendet werden, auch die Anwendung von Signaturverfahren, die nicht diesem Gesetz entsprechen, ist freigestellt. Die unterschiedlichen Sicherheitsstufen, die diese Bestimmung ermöglicht, können durch unterschiedliche aufwendige Sicherheits- und Zertifizierungskonzepte realisiert werden, auch die unterschiedliche Höhe der Haftung des Zertifizierungsdiensteanbieters für von ihm ausgestellte Zertifikate verwirklicht elektronische Signaturen und Zertifikate in unterschiedlicher Qualität, die zu verschiedenen Preisen am Markt angeboten werden können. Da die Entwicklung von Lösungen für hoch sichere Anwendungen erhebliche Investitionskosten verursacht, ist es wenig wahrscheinlich, daß es zu schnellen Realisierungen in großem Maßstab kommt. Viel wahr-

---

[12] Eine ausführlichere Abhandlung dazu bei: *Köhler*, Die Problematik automatisierter Rechtsvorgänge, insbesondere Willenserklärungen, Archiv für zivilistische Praxis (1982), S. 126.

[13] Darunter sind auch die allgemeinen Regelungen zum Schadenersatz des ABGB zu verstehen.

[14] EBRV zu § 3 Rz. 2.

scheinlicher ist es daher, daß angepaßte und kostengünstigere Anwendungen auf niedrigerem Sicherheitsniveau für solche Applikationen entstehen, für die eine große Nachfrage existiert.[15] Als Beispiel seien hier die unterschiedlichen Produkte des österreichischen Zertifizierungsdiensteanbieter A-Sign angeführt, die Zertifikate für Anwender, Server und Entwickler anbieten, wobei man bezüglich der Sicherheit bei den Anwenderzertifikaten zwischen Demo-, Light-, Medium-, Strong- und Premiumzertifikaten[16]unterscheidet. Die Anwendung elektronischer Signaturen als elektronische Identität, die einen amtlichen Lichtbildausweis ersetzt[17], stellt in der Praxis sicher nur die Spitze der Anwendungen dar. Viele andere mögliche Einsatzarten erfordern zwar ebenfalls den Einsatz elektronischer Signaturen, es kann dabei aber auf sehr hohe oder höchste Sicherheitsanforderungen verzichtet werden. Jedoch darf die freigestellte Verwendung nicht mit der Rechtswirkung elektronischer Signaturen verwechselt werden. Hier kennt das SigG nur zwei Kategorien: die einfachen elektronischen Signaturen, die die oben besprochenen allgemeinen Rechtswirkungen gemäß § 3 entfalten, und sichere elektronische Signaturen. Die elektronischen Signaturen der hohen Sicherheitsstufe werden der eigenhändigen Unterschrift gleichgestellt und erhalten bessere Beweisqualität als einfache elektronische Signaturen. Die Vermutung des § 294 ZPO über die Unverfälschtheit des Inhaltes von Privaturkunden wird auch auf elektronische Dokumente, die mit sicheren elektronischen Signaturen versehen sind, ausgedehnt. Auch einfachen elektronischen Signaturen spricht das SigG Rechtswirkungen zu, die zu einer Verbesserung der rechtlichen Qualität dieser Signaturen gegenüber der Rechtslage vor Einführung des SigG führen. Dies ist dadurch begründet, daß auch Zertifizierungsdiensteanbieter, die einfache elektronische Signaturen ohne qualifizierte Zertifikate ausstellen, Pflichten nach dem SigG treffen. So müssen sie unter anderem gemäß § 6 Abs. 2 ihre Tätigkeit der Aufsichtsstelle anzeigen und ihr spätestens mit Aufnahme der Tätigkeit oder bei Änderung der Dienste ein Sicherheitskonzept sowie ein Zertifizierungskonzept für jeden von ihnen angebotenen Signatur- und Zertifizierungsdienst samt den verwendeten technischen Komponenten und Verfahren vorlegen.

---

[15] *Welsch,* Stufenweise skalierbare Sicherheit für digitale Signaturen, DuD (1999), S. 520.

[16] http://www.a-sign.at/content/zertdienst/produkte/user.htm.

[17] Dieses Modell wird zum Beispiel in Finnland angestrebt, wo die hoheitliche Meldestelle eine einheitliche SmartCard mit darauf gespeicherter sicherer Signaturerstellungseinheit für jeden Staatsbürger ausgeben will. Diese Karte soll die Fuktion eines Personalausweises übernehmen.

Während ihrer Tätigkeit unterliegen sie der Aufsicht durch die Aufsichtsstelle. Dies alles führt zur Zuerkennung von folgenden Rechtswirkungen für einfache Signaturen ohne qualifiziertes Zertifikat, die in § 3 Abs. 2 geregelt sind: „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." Im Gerichtsverfahren können also elektronisch signierte Dokumente nicht alleine deswegen als Beweis ausgeschlossen werden, weil sie nur in elektronischer Form und nicht in Form einer Urkunde aus Papier vorgelegt werden.

So gilt also für einfache elektronische Signaturen das allgemeine Verbot des Ausschlusses der Rechtswirksamkeit, nur weil die Dokumente in elektronischer Form vorliegen. Sicheren elektronische Signaturen mit qualifiziertem Zertifikat werden darüber hinaus noch die besonderen Rechtswirkungen der Gleichstellung mit der eigenhändigen Unterschrift und die bessere Beweisqualität im Gerichtsverfahren durch § 4 zuerkannt.

Im folgenden Abschnitt sollen die unterschiedlichen Anforderungen des SigG an einfache und an sichere elektronische Signaturen aufgezeigt und die zusätzlichen Bedingungen für qualifizierte Zertifikate beschrieben werden.

4.3.1. „Einfache"[18] und sichere elektronische Signatur

Das SigG unterscheidet zwischen einfachen elektronischen Signaturen und sicheren elektronischen Signaturen, wobei die elektronische Signaturen gemäß der Begriffsbestimmung in § 2 Z 1 aus elektronischen Daten bestehen, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators, dienen. Durch diese Definition wird der technologieneutrale Ansatz der SigRL in das österreichische Recht über-

[18] Der Begriff einfache elektronische Signaturen wird weder in SigG noch der SigRL verwendet. Beide Normen bezeichnen Signaturen, die nicht den höheren Standards der sicheren elektronischen Signatur oder der fortgeschrittenen elektronischen Signatur, die mit einem qualifizierten Zertifikat verknüpft ist, entsprechen, nur als elektronische Signaturen. Zur Verdeutlichung und besseren Abgrenzung wird hier der Begriff einfache elektronische Signatur verwendet.

nommen, der Geltungsbereich des SigG wird also nicht auf nur eine bestimmte Signaturmethode eingeschränkt.[19] In anderen, meist älteren Regelungen – wie zum Beispiel im deutschen[20] und italienischen SigG oder in vielen amerikanischen Gesetzen – finden sich oft noch technologiebezogene Definitionen, die ausschließlich auf die Verwendung asymmetrischer Kryptographie abstellen.[21] Der Vorteil dieser funktionellen Beschreibung liegt darin, daß auch Verfahren, die nach dem Inkrafttreten des SigG entwickelt werden, in den Anwendungsbereich des SigG fallen, wobei in den Erläuterungen davon ausgegangen wird[22], daß die Methode der asymmetrischen Kryptographie unter Verwendung digitaler Signaturen die derzeit wichtigste eingesetzte Technologie darstellt. Riskant ist allerdings, daß durch die mangelhafte Festlegung damit schon Verfahren privilegiert werden, die noch niemand kennt. Das trifft insbesondere auch für deren Sicherheitslücken zu.[23] Entschärft wird dieses Risiko durch die Tätigkeit der Bestätigungsstellen, die gleichsam als technische Sachverständige neue Verfahren auf die Einhaltung der Sicherheitsanforderungen des SigG laufend prüfen.

An sichere elektronische Signaturen, die den Kernbereich des SigG bilden, stellt das SigG bedeutend höhere Sicherheitsanforderungen. Diese unterscheiden sich insoweit von den fortgeschrittenen elektronischen Signaturen, die auf einem qualifizierten Zertifikat beruhen (Art. 1 Abs. 1a SigRL), als sie neben den Anforderungen, die Art. 2 Abs. 2 SigRL für fortgeschrittene elektronische Signaturen stellt, gemäß § 2 Z. 3 auch auf einem qualifizierten Zertifikat beruhen und Anforderungen genügen müssen, die den Anforderungen der Anhänge I, II und III der SigRL[24] ver-

---

[19] Ein Beispiel für ein neues Verfahren ist auch das von *Ronald L. Rivest* 1998 entwickelte Chaffing and Winnowing. Weitere Information unter: http://theory.lcs.mit.edu/~rivest/chaffing.txt.

[20] Wobei in jüngster Zeit von deutscher Seite argumentiert wird, daß das dSigG gemäß § 1 Abs. 2 keine Einschränkungen der elektronischen Signaturverfahren vorsieht.

[21] Für die Signaturgesetze der US Bundesstaaten: *Miedbrodt,* Anwendungserfahrung ausgewählter US amerikanischer Signaturgesetze, DuD (1999), S. 196. *Miedbrodt,* Regelungsansätze und -strukturen US-amerikanischer Signaturgesetzgebung, DuD (1998), S. 389.

[22] EBRV Allgemeiner Teil, Punkt 1.

[23] *Grimm/Fox,* Entwurf einer EU-Richtlinie zu Rahmenbedingungen „elektronischer Signaturen", DuD (1998), S. 407.

[24] Hier werden Mindestanforderungen für den Inhalt qualifizierter Zertifikate, Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, die Signaturerstellungseinheiten (private Schlüssel) und für die Signaturprüfung (im Browser des Adressaten) festgelegt.

gleichbar sind. Dieser Weg wurde zur sprachlichen Vereinfachung gewählt[25], um nicht bei jeder Erwähnung den Terminus der SigRL „fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen" expressis verbis anführen zu müssen.[26] Folgende Anforderungen stellt schon die Legaldefinition in § 2 Z 3 für sichere elektronische Signaturen:

- Ausschließliche Zuordnung zum Signator:
  Dadurch wird die Verwendung einer gemeinsamen Signaturerstellungseinheit durch mehrere Personen verboten. Signaturerstellungsdaten und Signaturprüfdaten (in etwa privater und öffentlicher Schlüssel) müssen daher für jede Person verschieden sein und dürfen auch nicht weitergegeben werden.
- Möglichkeit der Identifizierung des Signators:
  Dies bedeutet, daß die sichere elektronische Signatur auch die grundlegendste Funktion einer eigenhändigen Unterschrift erfüllt. Dritte müssen aus der Signatur und dem Zertifikat die wahre Identität des Signators erkennen können. Wird im Zertifikat ein Pseudonym angegeben, ist es als solches kenntlich zu machen.
- Erstellung mit Mitteln, die der Signator unter seiner alleinigen Kontrolle halten kann
  Bei den gegenwärtigen Verfahren wird ein Schutz der Signaturerstellungsdaten meist mittels Zugangskontrolle durch Paßwortabfrage und die Aufbewahrung der Daten im ausschließlichen Machtbereich des Signators, wie zum Beispiel durch Speicherung auf einer Smartcard, erfolgen. Auch wird der Signator durch § 21 rechtlich verpflichtet, die Weitergabe der Signaturerstellungsdaten zu unterlassen. Die Verwendung fremder Signaturerstellungsdaten wird durch § 26 Abs. 1 mit einer Verwaltungsstrafe bis 56.000 Schilling bedroht.
- Derartige Verknüpfung mit den Daten, auf die sie sich bezieht, daß jede nachträgliche Veränderung der Daten festgestellt werden kann
  Diese Bestimmung normiert die Gewährleistung der Integritätsfunktion der eigenhändigen Unterschrift. Da sicher elektronisch signierte Dokumente meist in offenen Netzen übermittelt werden, ist eine Manipulation des Inhaltes des Dokumentes durch Dritte leicht möglich.

---

[25] EBRV zu § 2 Z. 3.

[26] Auch im Bereich der Normungsinitiative der EU (European Electronic Signature Standardization Initiative (EESSI)), Final Draft of the EESSI Expert Team Report, June 18, 1999 verfügbar unter: http://www.etsi.org/SEC/EsRep042.pdf verdrängt der Begriff „qualifizierte Signatur" den umständlichen Ausdruck der SigRL.

Die technischen Verfahren, die beim Signieren angewendet werden, müssen gewährleisten, daß eine solche Manipulation zuverlässig erkannt wird.

- Erstellung durch Zugrundelegung eines qualifizierten Zertifikats und Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen.
  Durch die verbindliche Verknüpfung mit einem qualifizierten Zertifikat wird die fortgeschrittene elektronische Signatur zur sicheren elektronischen Signatur. Die Sicherheitsanforderungen an ein qualifiziertes Zertifikat sind in § 18 geregelt und werden im nächsten Abschnitt behandelt. Der letzte Satz gewährleistet, daß trotz der Offenheit des SigG gegenüber neuen Signaturverfahren keinen risikoreich erzeugten Signaturen die Rechtswirkung sicherer elektronischer Signaturen zugesprochen wird.

In den Erläuterungen wird davon ausgegangen[27], daß beim Stand der gegenwärtigen Technik nur digitale Signaturen alle Anforderungen für sichere elektronische Signaturen erfüllen.

Natürlich darf die Sicherheit des Systems nicht an den in § 2 Z. 3 geregelten Tatbeständen für sichere elektronische Signaturen allein gemessen werden. Vielmehr ist es notwendig, auch die anderen ineinander greifenden Sicherheitsbestimmungen, ihre Kontrolle durch die Aufsichtsstelle und die Weiterentwicklung durch die Bestätigungsstellen, die an anderen Stellen im SigG zu finden sind, mit einzubeziehen, um die Sicherheit des ganzen Systems, die im Endeffekt für die Zuerkennung von Rechtswirkungen sinnvoll ist , zu beurteilen.

4.3.2. „Einfaches“[28] und qualifiziertes Zertifikat

Auch Zertifikate werden in zwei Kategorien eingeordnet. Es wird unterschieden zwischen (einfachen) Zertifikaten, die im § 2 Abs. 8 definiert sind, und qualifizierten Zertifikaten, deren Regelung im § 2 Abs. 9 iVm §§ 5 und 7 zu finden ist. Jede elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und wodurch deren Identität bestätigt wird, gilt als Zertifikat, solange sie mit der

---

[27] EBRV zu § 2 Z. 3 lit. e.

[28] Genauso wie der Begriff „einfache elektronische Signatur“ wird auch der Terminus „einfaches Zertifikat“ nicht vom Gesetzgeber verwendet. Siehe auch die Fußnote bezüglich „einfacher“ und sicherer elektronischer Signatur.

Signatur dem Nachrichtenempfänger übermittelt wird oder online abrufbar ist. Mehr als die Erfüllung dieser Hauptfunktion eines Zertifikates – die Vermittlung der Identität des Signators durch Verknüpfung seiner Personaldaten mit seinem öffentlichen Schlüssel – wird vom SigG für einfache Zertifikate nicht verlangt. Den Zertifizierungsdiensteanbietern steht es hier frei, unterschiedliche Kategorien und auch Zertifikate mit unterschiedlich hohem Informationsgehalt über die Person des Signators anzubieten. Sogar Widerrufdienste müssen für einfache Zertifizierungsdienste nicht verpflichtend geführt werden. Der Zertifizierungsdiensteanbieter muß aber gemäß § 6 Abs. 6 im von ihm festgelegten Sicherheitskonzept angeben, ob und gegebenenfalls in welcher Form Verzeichnis- und Widerrufdienste geführt werden. Einfache Zertifikate können allerdings nicht in Verbindung mit sicheren elektronischen Signaturen verwendet werden, da hier § 2 Z. 3 lit. e zwingend die Verwendung qualifizierter Zertifikate vorschreibt. Elektronische Signaturen, die mit einem einfachen Zertifikat verknüpft sind, entfalten daher nicht die besonderen Rechtswirkungen der Gleichstellung mit der eigenhändigen Unterschrift und der besseren Beweisqualität, auch wenn sie sonst allen anderen Anforderungen an sichere elektronische Signaturen genügen.

Die inhaltlichen Voraussetzungen für das qualifizierte Zertifikat sind identisch mit den Anforderungen des Anhangs I der SigRL und im § 5 geregelt. Weiter müssen auch die Anforderungen des Anhangs II an die Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, erfüllt sein, wobei hier in § 7 die SigRL konkretisiert wird. § 8 schlußendlich regelt die Durchführung der Zertifizierung.

4.3.3. Inhalt des qualifizierten Zertifikates

Folgende Inhalte müssen gemäß § 5 in einem qualifizierten Zertifikat zumindest enthalten sein, wobei durch die Zertifizierungsdiensteanbieter nach vertraglicher Zustimmung des Signators auch noch weitere Angaben aufgenommen werden können.

- **Hinweis darauf, daß es sich um ein qualifiziertes Zertifikat handelt:** Dadurch kann der Geschäftspartner, der ein Zertifikat eines Signators prüft, auf einen Blick erkennen, daß die ihm zugesandte Willenserklärung mit den besonderen Rechtswirkungen ausgestattet ist. Es muß nicht erst aufwendig geprüft werden, ob wirklich alle Anforderungen an ein qualifiziertes Zertifikat erfüllt sind. Auch für eine

Haftung mit Beweislastumkehr gemäß § 23 ist nur die Bezeichnung des Zertifikates als qualifiziertes maßgeblich.

- **unverwechselbarer Name des Zertifizierungsdiensteanbieters und Staat seiner Niederlassung:** Ein unverwechselbarer Name ist die Grundlage für eine wirksame Rechtsdurchsetzung im Fall einer gerichtlichen Klage. Die Angabe des Sitzstaates ist für die Anerkennung ausländischer Zertifikate von Bedeutung, da nur Zertifikate, die von einem in der Europäischen Gemeinschaft niedergelassenen Zertifizierungsdiensteanbieter ausgestellt wurden und deren Gültigkeit vom Inland aus überprüft werden kann, inländischen Zertifikaten gleichgestellt sind und dieselben Rechtswirkungen wie inländische Zertifikate entfalten. Für die Anerkennung von Zertifikaten aus anderen Ländern wäre eine Cross-Zertifizierung durch einen zusätzlichen Zertifizierungsdiensteanbieter innerhalb der Staaten der Europäischen Gemeinschaft notwendig.
  Auch diese Information muß der Geschäftspartner des Signators, der ja keinen unmittelbaren Kontakt zum Zertifizierungsdiensteanbieter des Absenders der Nachricht hat, in einfacher Art und Weise dem Zertifikat entnehmen können. Weiters ist dies auch von Bedeutung, da gemäß dem Entwurf der Richtlinie über bestimmte Aspekte des elektronischen Geschäftsverkehrs in Verbindung mit den anwendbaren Regeln des Internationalen Privatrechtes für das anwendbare nationale Recht der Sitzstaat des Unternehmers ausschlaggebend ist.

- **Name des Signators oder ein Pseudonym, das als solches bezeichnet sein muß:** Dieser Information kommt neben den Angaben über die Signaturprüfdaten die Hauptbedeutung der zertifizierten Daten zu. Sie sind der unverzichtbare Kernbereich eines jeden Zertifikates. Aus den Erläuterungen geht hervor, daß jeweils Vor- und Nachname angegeben werden müssen.[29] Zumindest innerhalb des Kundenbereiches eines Zertifizierungsdiensteanbieters muß sichergestellt sein, daß die Zertifikate den jeweiligen Signatoren eindeutig zuordenbar sind. Finden sich hier mehrere Signatoren mit gleichem Vor- und Nachnamen, müssen weitere Identifikationsmerkmale, wie zum Beispiel das Geburtsdatum, ins Zertifikat aufgenommen werden. Wird anstelle des wirklichen Namens ein Kunstname verwendet, muß dies gekennzeichnet sein, auch bei den Pseudonymen dürfen keine Verwechslun-

[29] EBRV zu § 5 Abs. 1 Z. 3.

gen möglich sein. Wird im Zertifikat ein Pseudonym an Stelle der Namensangabe verwendet, muß es als solches erkenntlich sein.

- **Gegebenenfalls auf Verlangen des Zertifikatwerbers Angaben über eine Vertretungsmacht[30] oder eine andere rechtlich erhebliche Eigenschaft des Signators:** Das Gesetz erlaubt hier beide technisch realisierbaren Varianten. Alle Angaben können in ein einziges Hauptzertifikat aufgenommen werden, wobei ein Signator mehrere Hauptzertifikate besitzen kann, in denen diese Eigenschaften in unterschiedlichem Maße angeführt sind. Auch ist es möglich, daß diese Daten überhaupt nicht im Hauptzertifikat enthalten sind. Dieses verweist dann nur auf eines von mehreren möglichen Attributzertifikaten, die einem Hauptzertifikat zuordenbar und in denen nur diese Zusatzinformationen enthalten sind.[31]
  Neben der im Gesetzestext genannten Vertretungsmacht für eine juristische Person fallen in die Gruppe der anderen rechtserheblichen Eigenschaften etwa auch gewerberechtliche oder berufsrechtliche Befugnisse, wie zum Beispiel für Notare[32], oder sonstige Zulassungen. Es dürfen nur tatsächlich vorliegende Eigenschaften in das Zertifikat aufgenommen werde Um dies sicherzustellen, könnten durch den Registrierungsdiensteanbieter des Hauptzertifizierungsdiensteanbieters nur die näheren Angaben zur Person bestätigt werden. Angaben über die beruflichen Eigenschaften des Signators, wie etwa die Vertretungsmacht für gewisse juristische Personen oder seine Berufszulassung als Arzt, Rechtsanwalt, Notar oder ähnliches würden direkt von der dafür zuständigen Stelle als Registrierungsdiensteanbieter in einem Attributzertifikat, das mit dem die Identität nachweisenden Hauptzertifikat verknüpft ist, bestätigt werden.

---

[30] Da juristische Personen nicht selbst signieren können, wird die Signatur (wie auch bis jetzt die eigenhändige Unterschrift) von den dazu befugten Organwaltern in deren Namen geleistet, daher ist für diesen Bereich Informationen über die Vertretungsmacht für die juristische Person von besonderer Bedeutung.

[31] Diese Variante ermöglicht auch, daß der Zertifizierungsdiensteanbieter, der das Hauptzertifikat ausstellt und die Organisation, die die Attribute festlegt, verschiedene Organisationen sein können.

[32] Notare könnten dann ihre Hauptzertifikate von einem gewerbsmäßigen Zertifizierungsdiensteanbieter beziehen, und das Attributzertifikat, welches die Zulassung als Notar bestätigt, wird davon unabhängig durch die Notariatskammer ausgestellt.

- **Die dem Signator zugeordnete Signaturprüfdaten:** Die Anführung der Signaturprüfdaten hat neben der Namensnennung die ebenfalls wichtigste Bedeutung. In der Regel werden die Zertifikate wohl Schlüsselpaaren, wie sie in der asymmetrischen Kryptographie verwendet werden, zugeordnet sein.
  Die Daten des öffentlichen Schlüssels oder zumindest der Hashwert dieser Daten unter Angabe des verwendeten Hash-Verfahrens sind dann ebenfalls ins Zertifikat aufzunehmen.

- **Beginn und Ende der Gültigkeit des Zertifikats:** Dieser Zeitraum, der festlegt, wie lange das Zertifikat zum Signieren verwendet werden darf, muß sich unter einer hoheitlich fixierten Höchstgrenze bewegen. Diese Grenze wird nicht im Gesetz selber normiert. Es enthält nur in § 25 Abs. 7 die Verpflichtung, eine Verordnung zu erlassen, die die Höchstdauer angibt. § 12 Abs. 3 SigVO setzt die Höchstdauer der Gültigkeit eines qualifizierten Zertifikates mit 3 Jahren fest. So kann leichter auf die zukünftigen Erfolge bei Brute Force Attacken zum Knacken der ja auch vom Zertifizierungsdiensteanbieter verschlüsselten Zertifikate Rücksicht genommen werden. Hier wird nur die Verwendbarkeit des Zertifikats durch den Signator geregelt, die Verfügbarkeit der Zertifikate in den Verzeichnissen der Zertifizierungsdiensteanbieter zur Verifizierung in der Vergangenheit geleisteter elektronischen Signaturen muß jedenfalls auf längere Zeit sichergestellt sein.

- **Eine eindeutige Kennung des Zertifikats:** Oft beinhalten Widerruflisten gesperrter Zertifikate nicht den ganzen Inhalt der widerrufenen Zertifikate, sondern nur die Kennung der ungültig gewordenen. Zur Prüfung dieser Listen, ob ein fragliches Zertifikat noch gültig ist, muß dem Empfänger eines Zertifikates also auch diese Kennung zur Verfügung stehen.

- **Gegebenenfalls eine Einschränkung des Anwendungsbereichs des Zertifikats** und

- **gegebenenfalls eine Begrenzung des Transaktionswerts, auf den das Zertifikat ausgestellt ist:** Diese beiden Angaben beziehen sich auf die Haftungsgrenzen des Zertifizierungsdiensteanbieters, die in einem späteren Abschnitt über haftungsrechtliche Fragen besprochen werden. Da dieser selbständig festlegen kann, wie hoch seine maxi-

male Haftung pro Geschäftsfall bei Verwendung einer bestimmten Zertifikatsklasse ist, muß auch der Geschäftspartner rasch und ohne großen Aufwand vor Vertragsabschluß erkennen können, wie weit die elektronisch signierte Willenserklärung durch eine Haftung des Zertifizierungsdiensteanbieters für die Richtigkeit der im Zertifikat enthaltenen Daten gedeckt ist.

Ist das Zertifikat mit einer sicheren elektronischen Signatur verknüpft, so muß auch diese Tatsache gemäß § 7 Abs. 5 im Zertifikat erwähnt werden oder in einem elektronisch jederzeit allgemein zugänglichen Verzeichnis aufscheinen. Hier handelt es sich ebenfalls um eine Hilfestellung für den Empfänger der sicher elektronisch signierten Willenserklärung. Er muß nicht nachprüfen, ob jede einzelne Anforderung, die das SigG an sichere elektronische Signaturen stellt, erfüllt worden ist, sondern kann durch die Erwähnung im Zertifikat darauf vertrauen, daß diese Mitteilung die besonderen Rechtswirkungen entfaltet.

Eine weitere Bestimmung über den Inhalt eines qualifizierten Zertifikates ist auch in § 17 Abs. 2 zu finden. Demnach muß der Umstand der Akkreditierung eines Zertifizierungsdiensteanbieters in die von ihm ausgestellten Zertifikate aufgenommen oder sonst in geeigneter Weise zugänglich gemacht werden, da dieser vertrauensschaffende Umstand im Außenverhältnis Bedeutung erlangt.

4.3.4. Anforderungen an Zertifizierungsdiensteanbieter für qualifizierte Zertifikate

In Übereinstimmung mit der SigRL stellt das SigG nicht dieselben strengen, sehr detaillierten Anforderungen des dSigG betreffend die Tätigkeiten des Zertifizierungsdiensteanbieters. Trotzdem werden für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, gewisse allgemeine Grundbedingungen vorgegeben. Sie müssen in einem vom Zertifizierungsdiensteanbieter selbständig erstellten Sicherheits- und Zertifizierungskonzept umgesetzt und konkret ausgestaltet werden.[33] Im Gegensatz dazu wurde in Deutschland von der Regulierungsbehörde für Post und Telekommunikation nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik ein Maßnahmenkatalog für Digitale Signatu-

[33] Der Zertifizierungsdiensteanbieter hat also einen gewissen Spielraum, in dem er mit verschiedenen Mitteln die Einhaltung der gesetzlichen Sicherheitsanforderungen verwirklichen kann. Die Konzepte jedes Zertifizierungsdiensteanbieter werden von der Aufsichtsstelle auf Einhaltung der gesetzlichen Vorschriften überprüft.

ren[34] herausgegeben. Kasuistisch aufgebaut werden hier unzählige Maßnahmen empfohlen, die beim Betrieb einer zu beachten sind.

Das SigG verlangt in § 7 nur die Sicherstellung der Einhaltung folgender Kriterien, die aber in ihrem Zusammenwirken zu einer sicheren Infrastruktur führen. Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, muß verschiedene Bedingungen erfüllen:

- **Nachweis der erforderlichen Zuverlässigkeit für die von ihm bereitgestellten Signatur- oder Zertifizierungsdienste:** Die geforderte Zuverlässigkeit soll Gewähr bieten, daß der Zertifizierungsdiensteanbieter auch alle maßgeblichen Rechtsvorschriften einhält. ME ist dies nicht nur auf das SigG und eine später zu erlassende SigVO anzuwenden, sondern bezieht auch andere relevante Rechtsvorschriften, wie Gewerbeordnung[35] oder Datenschutzgesetz, mit ein.

- **Sicherstellung des Betriebes eines schnellen und sicheren Verzeichnisdienstes sowie eines unverzüglichen und sicheren Widerrufdienstes:** Da der Betrieb eines Verzeichnis- und Widerrufdienstes nicht Voraussetzung für die Vergabe einfacher Zertifikate ist, für qualifizierte Zertifikate aber unumgänglich vorhanden sein muß, wird diese Voraussetzung hier durch § 7 normiert. Vertragspartner des Signators verwenden diese Dienste zur Überprüfung der ihnen zugesandten Zertifikate auf ihre aktuelle Richtigkeit und setzen Vertrauen in die Richtigkeit der Verzeichnisse.[36] Daher wird in § 13 SigVO festgelegt, daß sie vor Fälschung, Verfälschung und unbefugtem Abruf ausreichend geschützt sein müssen, und sicherzustellen ist , daß nur befugte Personen Eintragungen und Veränderungen in den Verzeichnissen vornehmen können.[37]
  Da das Widerrufen in der Regel[38] online durch den Signator und Zer-

---

[34] Zitat: BSI-Katalog.

[35] § 271 GewO 1994 über Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik.

[36] Zur großen praktischen Bedeutung der Widerrufsdienste siehe auch: *Bertsch/Pordesch,* Zur Problematik von Prozeßlaufzeiten bei der Sperrung von Zertifikaten, DuD (1999), S. 514.

[37] Besonders sicher sind die Verzeichnisse der Telekom Control GmbH zu gestalten, da als Verzeichnisse der österreichischen Wurzel von ihrer Sicherheit die gesamte Sicherheit der österreichischen abhängt. Deswegen sind diese in § 3 SigVO gesondert geregelt.

[38] Unter http://194.37.252.221/content/services/revoke.html findet man zum Beispiel den online Widerrufsdienst der A-Sign.

tifikatsinhaber durchgeführt wird[39], kann man davon ausgehen, daß der Widerruf bald nach Eintreffen der Meldung am Server erfolgen muß. § 13 Abs. 4 SigVO normiert eine Höchstdauer von 3 Stunden ab Bekanntwerden des Hindernisgrundes, in der während der Geschäftszeiten[40]eine Aktualisierung zu erfolgen hat. Interessanterweise wird in § 13 Abs. 4 letzter Satz SigVO weiters geregelt, daß außerhalb der Geschäftszeiten ein Widerruf jederzeit automatisiert entgegengenommen werden soll und die Sperre ausgelöst werden soll. Da die Bearbeitungszeit bei automatisiertem Widerrufs jedenfalls deutlich unter 3 Stunden beträgt, führt dies zur Situation, daß die Zertifizierungsdiensteanbieter außerhalb der Öffnungszeiten schneller widerrufen müssen als zu Geschäftszeiten.

- **Verwendung qualitätsgesicherter Zeitangaben (Zeitstempel)** in qualifizierten Zertifikaten sowie für Verzeichnis- und Widerrufsdienste und jedenfalls Sicherstellung, daß der Zeitpunkt der Ausstellung und des Widerrufs eines qualifizierten Zertifikats bestimmt werden kann:
  An den Ablauf der Zeit knüpfen sich zahlreiche Rechtsfolgen. Da elektronische Signaturen Rechtswirkungen entfalten, muß auch der Zeitpunkt feststellbar sein, an dem sie beginnen, diese zu entfalten, und an dem sie wieder ungültig werden. Die Zeitpunkte fallen mit der Gültigkeit des Zertifikates zusammen, so daß diese rechtserheblichen Zeitpunkte sicher und vertrauenswürdig aus den Verzeichnissen der Zertifizierungsdiensteanbieter für jeden ersichtlich sind. Der Diensteanbieter muß in den Zeitstempelangaben sowohl Datum als auch Uhrzeit angeben. Die Zeitstempel dürfen auch von Dritten generiert werden, so daß der Zertifizierungsdiensteanbieter dieses Verfahren auslagern kann, auf jeden Fall müssen sie aber auch qualitätsgesichert sein und die Anforderungen des § 18 an die technischen Komponenten und Verfahren für sichere elektronische Signaturen erfüllen.[41] Im Anhang der Richtlinie wird die Verwendung von Zeitstempeln nicht explizit vorgeschrieben, insofern konkretisiert hier das SigG die SigRL, doch geht aus dem Sinn hervor, daß die Zeitpunkte von Beginn und Ende der Gültigkeit eines Zertifikates auch gemäß der

---

[39] Der Widerruf eines qualifizierten Zertifikates muß aber gemäß § 13 Abs. 2 jedenfalls auch in Papierform verlangt werden können.

[40] An Werktagen: 9 bis 17 Uhr, an Samstagen: 9 bis 12 Uhr.

[41] EBRV zu § 7 Z. 3.

SigRL durch die Zertifizierungsdiensteanbieter dokumentiert werden müssen.

- **Zuverlässige Überprüfung anhand eines amtlichen Lichtbildausweises der Identität und gegebenenfalls der besonderen, rechtlich erheblichen Eigenschaften der Person, für die ein qualifiziertes Zertifikat ausgestellt wird:** Auch diese Anforderung ist so nicht in der SigRL zu finden. Sie wurde durch eine Stellungnahme des Bundesministeriums für Finanzen[42] in den Entwurf des SigG aufgenommen. Die Überprüfung der Identität durch ein amtlich ausgestelltes Dokument ergibt sich aber zwingend logisch aus den hohen Anforderungen, die das System sicherer elektronischer Signaturen an die Gewährleistung der Identität des Signators stellt, die ja auch durch die Haftung des Zertifizierungsdiensteanbieters für die Richtigkeit der Daten sichergestellt wird. Berücksichtigt man die datenschutzrechtliche Bestimmung des § 22, daß Zertifizierungsdiensteanbieter die Daten über die Identität des Zertifizierten nicht von Dritten erheben dürfen, sondern daß sie vom Zertifikatswerber selbst stammen müssen, kommt man zum Schluß, daß bei Verweigerung der Ausweisleistung durch den Zertifikatswerber kein qualifiziertes Zertifikat ausgestellt werden darf. Auch für die sonstigen rechtlich erheblichen Eigenschaften, die auf Verlangen des Zertifikatswerbers in das Zertifikat aufgenommen werden müssen, werden Nachweise gleicher beweisrechtlicher Qualität wie ein amtlicher Lichtbildausweis bezüglich der Identität erbracht werden müssen.[43]

- **Beschäftigung von zuverlässigem Personal**[44] mit den für die bereitgestellten Dienste erforderlichen Fachkenntnissen, Erfahrungen und

---

[42] Stellungnahme des BMF zu einem Entwurf für ein Bundesgesetz über elektronische Signaturen, Begutachtungsverfahren zu Zl. 7.051C/50-I.2/1999
GZ. (des BMF) 13 1074/1-II/14/99.

[43] Eine weitere Möglichkeit zur Sicherstellung, daß nur richtige Berufsangaben ins Zertifikat aufgenommen werden, besteht darin diese Angaben in ein Attributzertifikat aufzunehmen, dessen Ausstellung die zuständige Berufsvertretung vornimmt.

[44] § 10 Abs. 4 SigVO regelt die strafbaren Handlungen, die durch das Personal nicht begangen sein dürfen (insbes. Vermögensdelikte, Urkundenfälschungen und Vorsatzdelikte). Alle im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste tätigen Personen sind jedes zweite Jahr zu überprüfen. Da dies auch für die Personen, die in der Registrierung neuer Anwender tätig sind betrifft, und mittels Übermittlung eines Strafregisterauszuges durchgeführt werden soll, wird diese Bestimmung von allen größeren Zertifizierungsdiensteanbietern in Übereinstimmung als undurchführbar angese-

Qualifikationen, insbesondere mit Managementfähigkeiten sowie mit Kenntnissen der Technologie elektronischer Signaturen und angemessener Sicherheitsverfahren, und Einhaltung geeigneter Verwaltungs- und Managementverfahren, die anerkannten Normen entsprechen. § 10 Abs. 5 SigVO fordert hierzu eine Ausbildung in 4 Bereichen: allgemeine EDV-Ausbildung, Sicherheitstechnologie, Kryptographie, elektronische Signatur und Public Key Infrastructure, technische Normen sowie Hard- und Software. Die fachliche Ausbildung muß zumindest in jedem Bereich ein Jahr in einer HTL, Fachhochschule oder Absolvierung eines einschlägigen Studiums dauern, jedes Jahr schulischer Ausbildung kann durch 3 Jahre Praxis ersetzt werden. ME sind diese Anforderungen sehr hoch gegriffen, da Techniker eines Zertifizierungsdiensteanbieter dann zumindest 4 Jahre einschlägige Ausbildung im Bereich der Public Key Infrastructure nachweisen müssen.
Die Sicherung dieser Ansprüche ist im Sicherheitskonzept etwa durch festgelegte Schulungsmaßnahmen und Ausbildungserfordernisse der Mitarbeiter der Zertifizierungsdiensteanbieter festzulegen und wird von der Aufsichtsstelle überprüft.

- **Verfügung über ausreichende Finanzmittel**, 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:
Zur Sicherstellung der Deckung der Haftpflichtansprüche, die einen Zertifizierungsdiensteanbieter potentiell treffen könnten, schreibt § 7 Abs. 1 Z 6 vor, daß Zertifizierungsdiensteanbieter für qualifizierte Zertifikate über ausreichende Finanzmittel verfügen müssen, um Vorsorge für die Befriedigung von Schadenersatzansprüchen zu treffen. Das Eingehen einer Haftpflichtversicherung wird als Beispiel angeführt. Der Abschluß einer solchen ist gemäß der Auffassung des Justizausschusses[45] ein probates Mittel zur Abdeckung dieses Risikos. Grundsätzlich kommen aber gemäß § 7 Abs. 1 Z. 6 SigG auch andere Sicherungsmittel, wie etwa Bankgarantien oder Bürgschaften, in Be-

---

hen, hieße das doch von z.B allen Postangestellten, als auch allen Bankangestellten, die Zertifizierungsanträge entgegennehmen, regelmäßig Strafregisterauszüge zu verlangen. Dies wird wahrscheinlich an einem Veto der Personalvertretungen scheitern.

[45] 2065 der Beilagen zu den Stenographischen Protokollen des NR der XX. GP, S. 2.

tracht, wobei der Sicherungsgrad allerdings mit jenem einer Haftpflichtversicherung vergleichbar sein muß.[46] Allerdings wird durch § 2 Abs. 3 SigVO die Haftpflichtversicherung wieder verbindlich eingeführt[47]. § 2 Abs. 2 der SigVO normiert für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, daß sie das Eingehen einer Haftpflichtversicherung mit einer Mindestversicherung von 1.000 000 Euro je Versicherungsfall der Aufsichtsstelle nachzuweisen haben.

- **Aufzeichnung aller maßgeblichen Umstände über ein qualifiziertes Zertifikat** während eines für den Verwendungszweck angemessenen Zeitraums, gegebenenfalls auch elektronisch, so daß insbesondere in gerichtlichen Verfahren die Zertifizierung nachgewiesen werden kann:
  Die Aufzeichnungspflicht wird in Streitfällen vor Gericht bedeutsam, wenn die Integrität einer sicheren elektronischen Signatur abgestritten wird, damit durch den Wegfall der besonderen Rechtswirkungen eine Vernichtbarkeit des Rechtsgeschäftes, dem eine sichere elektronische Signatur zu Grunde liegt, erreicht werden kann. Da im Zivilrecht die Verjährungsfrist 30 Jahre beträgt, müssen auch die Verzeichnisse mindestens eben so lang einsehbar bleiben. Berücksichtigt man auch Dauerschuldverhältnisse, führt dies zu einem noch längeren Zeitraum.

- **Erstellung von Vorkehrungen, daß die Signaturerstellungsdaten der Signatoren weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden können:** Verboten ist also nur die Speicherung der Signaturerstellungsdaten durch den Zertifizierungsdiensteanbieter. Er kann sie aber sehr wohl für seine Kunden erzeugen, wenn er nachher alle Signaturerstellungsdaten in seinem Herrschaftsbereich wieder löscht.[48] Diese letzte Ziffer führte zum (vorläufigen) Ende der politisch hochbrisanten und von kontro-

---

[46] Dadurch änderte der Justizausschuß die Bestimmung der RV, die ausschließlich die Haftpflichtversicherung vorsah.

[47] Ausgenommen sind davon nur Bund, Länder und Gemeinden.

[48] Zur Kontroverse, wo die Signaturerstellungsdaten erzeugt werden sollen siehe auch: *Federrath,* Schlüsselgenerierung in Trust Centern? DuD (1997), S. 98. *Nehl,* Schlüsselgenerierung in Trust Centern? DuD (1997), S. 100.

versiellen Standpunkten geprägten Kryptodebatte.[49] Durch das explizite Verbot der Speicherung oder Weitergabe von Signaturerstellungsdaten, die bei Verwendung der asymmetrischen Kryptographie den privaten Schlüsseln entsprechen, ist auch ein staatliches System zur Schlüsselhinterlegung nicht mehr realisierbar, soweit keine gegenteilige gesetzliche Regelung erlassen wird. Dies ist zum gegenwärtigen Zeitpunkt nicht in Planung. Wie schon oben ausführlicher ausgeführt führt die Zugriffsmöglichkeit eines Unbefugten auf die Signaturerstellungsdaten eines Dritten dazu, daß er ununterscheidbare Willenserklärungen anstelle des wahren Signators abgeben kann. Die Möglichkeit zur Weitergabe der Schlüssel muß daher auf jeden Fall vermieden werden und ist durch technische Maßnahmen und rechtliche Verpflichtungen zu verhindern. Die Verpflichtung des Zertifizierungsdiensteanbieters, die Weitergabe zu vermeiden, ist hier normiert und wird ergänzt durch die Pflicht des Signators, die Signaturerstellungsdaten sicher zu verwahren und die Weitergabe zu unterlassen. Auch eine Weitergabe durch den Zertifizierungsdiensteanbieter von Informationen über die Algorithmen, mit denen die Signaturerstellungsdaten generiert werden, ist nicht statthaft.

Natürlich sind nicht nur die Signaturerstellungsdaten der einzelnen Signatoren vor Weitergabe zu schützen. In noch viel höherem Maße sind die Signaturerstellungsdaten des Zertifizierungsdiensteanbieters zu schützen, da ein Mißbrauch dieses einen Signaturerstellungsdatensatz den Verlust der Integrität und damit des Widerrufes aller damit ausgestellten Zertifikate eines Zertifizierungsdiensteanbieters zur Folge hätte. In § 7 Abs. 3 wird dies in einem eigenem Absatz noch einmal festgestellt. Dabei wird aus den Erläuterungen[50] ersichtlich , daß an den Schutz dieses Schlüssels ungleich höhere Anforderungen als an den Schutz der Signaturerstellungsdaten einzelner natürlicher Personen gestellt werden. Sie gehen über die bloße Geheimhaltung weit hinaus und erfassen auch den Schutz durch bauliche Maßnahmen, wie etwa die Aufbewahrung des Datenträgers, auf dem die Signaturerstellungsdaten des Zertifizierungsdiensteanbieters gespeichert sind, in einem Tresor.

---

[49] Für Argumente pro und kontra bietet der Security Server der Gesamtuniversität Siegen im Bereich Kryptographie Regulierung einen guten Überblick: http://www.uni-siegen.de/security/policies/index.html.

[50] EBRV zu § 7 Abs. 3.

4.3.5. Ausstellung qualifizierter Zertifikate

In § 8 regelt das SigG den Ablauf der Ausstellung qualifizierter Zertifikate. Hauptsächlich wird hier allerdings nur noch einmal wiederholt, was schon in den Bestimmungen über den Inhalt qualifizierter Zertifikate in § 3 und über Zertifizierungsdiensteanbieter für qualifizierte Zertifikate in § 7 angeordnet wurde: Die Prüfung der Identität hat an Hand eines amtlichen Lichtbildausweises zu erfolgen. Rechtlich erhebliche Eigenschaften des Signators sind auf dessen Verlangen ins Zertifikat aufzunehmen. Allerdings muß auch die Richtigkeit der rechtserheblichen Tatsachen bei der Registrierung nachgewiesen werden. Die Verwendung eines Pseudonyms ist zulässig, wobei hier noch näher ausgeführt wird, daß das Pseudonym weder anstößig noch offensichtlich zur Verwechslung mit Namen oder Kennzeichen geeignet sein darf. Die Verpflichtung zur Kennzeichnung eines Pseudonyms als solches im Zertifikat ist nicht nochmals erwähnt.

Von weitaus größerer Bedeutung für Organisation und Struktur der Zertifizierungsdiensteanbieter ist § 8 Abs. 2, der es ermöglicht, die Registrierung der einzelnen Zertifikatswerber auch auszulagern. Sie besteht aus der Erhebung der persönlichen Daten des Zertifikatswerbers und im Rahmen dessen der Überprüfung der Identität. Der hohe technische Aufwand, der an Zertifizierungsdiensteanbieter für qualifizierte Zertifikate gestellt wird, führt zu wenigen spezialisierten Rechenzentren pro Land, die den Anforderungen des § 18 SigG an die eingesetzten technischen Komponenten und Verfahren für sichere Signaturen und des § 7 SigG an Zertifizierungsdiensteanbieter für qualifizierte Zertifikate gerecht werden. Da der Zertifikatswerber in der Regel zumindest einmal persönlich zur Überprüfung der Identität beim Zertifizierungsdiensteanbieter erscheinen muß, würde es zu langen Anfahrtszeiten kommen, wenn der Signator direkt beim Firmensitz der wenigen Zertifizierungsdiensteanbieter persönlich erscheinen müßte. Eine Auslagerung der Registrierung an ein flächendeckendes Netz von Registrierungsstellen verschafft hier Abhilfe. Die Zertifizierungsdiensteanbieter alleine könnten keine flächendeckende Versorgung zur Verfügung stellen. Deswegen ist es nötig, die Registrierung von Unternehmen oder Unternehmensteilen der Zertifizierungsdiensteanbieter durchführen zu lassen, die schon ein dichtes Filialnetz betreiben[51], aber per se keine eigenen Zertifizierungsdienste anbieten. Nach ei-

[51] A-Sign verwendet zur Registrierung die überall in Österreich gut erreichbaren Postämter für Zertifikate gehobener Klasse. A-TRUST will die Registrierung durch Bankfilialen durchführen lassen.

ner deutschen Meinung[52] liegt hierin sogar ein Hauptproblem für Zertifizierungsdiensteanbieter. Den größten Teil der Kosten bei der Ausstellung eines Zertifikates verursacht die Registrierung – sowohl für den Schlüsselinhaber selbst (Wegzeiten) als auch für den Anbieter (Identifizierung, Einweisung, Dokumentation). Für den Anbieter rechnet sich die Dienstleistung nur dann, wenn er bei der Registrierung ein eigenes oder externes Filialnetz mit Kundennähe nutzen kann.

Haftungsrechtlich fällt auch eine Registrierungsstelle unter die Haftungsbestimmung des § 23, so daß ein Dritter auch gegen sie seine Haftungsansprüche erfolgreicher als nach allgemeinem Schadenersatzrecht durchsetzen kann. Wobei beide, wohl für die von in ihrem Machtbereich verursachten Schäden, gemäß § 23 haften. Weiters kann er sich bei Fehlverhalten der Registrierungsstelle auch direkt an den Zertifizierungsdiensteanbieter wenden, für den die Registrierungsstelle arbeitet, da die Registrierungsstelle als Erfüllungsgehilfe des Zertifizierungsdiensteanbieters angesehen wird. Aus dem Tätigwerden der Registrierungsstelle dürfen dem Zertifikatswerber allerdings keine Nachteile entstehen.

4.4. Rechtspersönlichkeit und Geschäftsfähigkeit des Signators

Die SigRL überläßt es den einzelnen Mitgliedstaaten, ob nur natürliche Personen oder auch juristische Personen signieren dürfen. Während der Ratsverhandlungen über diesen Punkt konnte keine Einigung erzielt werden, da in Mitgliedsstaaten mit einer Civil Law Tradition eine rechtsverbindliche Willenserklärung meist eine Stellvertretung durch natürliche Personen voraussetzt, in einigen Common Law Jurisdiktionen[53] sich die Abgabe einer Erklärung direkt im Namen der juristischen Person aber auch durch Siegel und Stempel einer juristischen Person berwerkstelligen läßt.[54] Bewußt wird in der Legaldefinition des Signators nur der Begriff Person verwendet, so daß beide Auslegungen durch die Mitgliedsstaaten möglich sind. Die österreichische Regelung schließt sich der Regelung in § 2 Abs.2 dSigG an und erlaubt – geprägt von dem Leitsatz, elektronische

---

[52] *Fox*, Eine kritische Würdigung des SigG, DuD (1999), S. 508.

[53] *Mayson*, French and Ryan on Company Law, S. 584.

[54] *Gravesen/Dumortier/Van Eecke*, Die europäische Signaturrichtlinie – Regulative Funktion und Bedeutung der Rechtswirkung, MMR (1999), S. 577.

Signaturen möglichst der natürlichen Unterschrift nachzugestalten[55] – nur für natürliche Personen die Verwendung von Signaturen. Während der Entstehung des Gesetzes wurde diskutiert, ob nicht auch juristische Personen Signatoren im Sinne des SigG sein können. Dies wäre einerseits empfehlenswert, da im Gegensatz zur eigenhändigen Unterschrift auch Computer automatisch elektronische Signaturen erzeugen und zustellen können[56], andererseits würde dies dem Grundprinzip, elektronische Signaturen möglichst der eigenhändigen Unterschrift gleich zu gestalten, widersprechen.[57] Es wurde dann aber richtig entschieden, in diesem Fall eine Analogie zur Rechtsauffassung bezüglich des Automatenkaufs zu ziehen und die dahinterstehende Willensbildung durch die Aufstellung des Computers durch den Betreiber zu sehen. In dessen Namen werden auch die elektronischen Signaturen durch das Gerät abgegeben.[58] Die vom Computer automatisch ausgestellten elektronischen Signaturen müssen also den Namen einer natürlichen Person als Signator – in der Regel der Betreiber der Anlage – enthalten. Gemäß § 4 iVm § 2 Z. 2 entfaltet daher eine sichere elektronische Signatur, die sich auf ein qualifiziertes Zertifikat stützt und dessen Namensangabe auf den Namen einer juristischen Person lautet, nicht die besonderen Rechtswirkungen sicherer elektronischer Signaturen.

Als einzige Ausnahme gemäß § 2 Z 2 aus organisatorischen Gründen beziehen sich die Zertifikate für Zertifizierungsdiensteanbieter auf den Zertifizierungsdiensteanbieter selbst. Falls der Diensteanbieter ein Unternehmen in Form einer juristischen Person oder eine Personengesellschaft ist, tritt als Signator hier wirklich das Unternehmen im eigenen Namen und nicht dessen Vertreter auf, nur diese sind im Zertifikat genannt. Diese Zertifikate dürfen aber nur für die Erbringung von Zertifizierungsdiensten

---

[55] Anders als im Bereich Common Law verlangt der österreichische Gesetzgeber, daß die Unterschrift den eigenen Namen des Unterschreibenden erhalten muß. So kann etwa der Prokurist, wenn er für sein Unternehmen tätig ist, nicht mit dem Namen des Unternehmens zeichnen.

[56] So werden unter anderem Zeitstempel automatisch durch Computer ausgestellt, indem sie die an sie gerichteten Dokumente mit einer Zeitangabe versehen und das dadurch erweiterte Dokument sicher elektronisch signieren und an den Absender zurückschicken.

[57] So können juristische Personen auch nicht im eigenen Namen unterschreiben. Die eigenhändige Unterschrift besteht aus dem Namen des Vertretungsbefugten.

[58] Zwar nicht der Klassifizierung als Automatenkauf zustimmend, aber über Angebot und Annahme durch Webserver: *Madl,* Vertragsabschluß im Internet, ecolex (1996), S. 79.

genutzt werden, das Signieren anderer rechtserheblicher Willenserklärungen ist nicht erlaubt.

Die Notwendigkeit dieser Ausnahme sieht man bei näherer Betrachtung der Situation in Deutschland. Gemäß deutschem Recht müssen sich auch die Zertifikate der deutschen Zertifizierungsstellen auf natürliche Personen beziehen. Um bei Kündigung eines Mitarbeiters den Schlüssel des Zertifizierungsdiensteanbieters nicht zurückrufen zu müssen, behilft man sich dort mit der Verwendung eines eigentlich aus Datenschutzgründen im dSigG vorgesehenen Mechanismus: dem Pseudonym. Der dem Pseudonym zugeordnete Mitarbeiter kann wechseln, der Schlüssel bleibt erhalten. Grundsätzlich widerspricht dieses Prinzip den Vorstellungen des SigG und dSigG, da die Identität des Schlüsselinhabers wechselt. Wahrscheinlich wird dieser Umweg auch von vielen anderen zertifizierten juristischen Personen beschritten werden.

Die Nichteinhaltung dieser Anordnung, die im § 2 Z. 2 im Rahmen der Legaldefinition des Signators eingefügt ist, führt wohl zur Aberkennung der besonderen Rechtswirkungen, die sicher elektronisch signierte Dokumente entfalten. Sie ergeben daher keine Schriftförmlichkeit, unterliegen aber der freien Beweiswürdigung. Die Ausnahme ist darin begründet, daß dadurch verhindert wird, den Bestand eines Zertifikates für Zertifizierungsdiensteanbieter vom aufrechten Organschafts- oder Vollmachtsverhältnis der handlungsbefugten Person abhängig zu machen. Auch die Aufsichtsstelle, die ja als Telekom-Control Kommission keine natürliche Person ist, kann als Signator genannt werden[59], soweit ihre sichere elektronische Signatur im Rahmen von Rechtsakten der Aufsicht Verwendung findet. Ob diese Ausnahme auch für Bestätigungsstellen gilt, die zum Beispiel in der Form eines Vereines organisiert sind[60], ist weder dem Gesetzestext noch den Erläuterungen direkt zu entnehmen, da sie aber von der Aufsichtsstelle delegierte Aufsichtsmaßnahmen übernehmen sollen, werden wohl auch sie namentlich als Signatoren auftreten können.

In geschlossenen Systemen können freilich auch elektronische Signaturen an Signatoren vergeben werden, die keine natürlichen Personen sind. So könnten etwa Firmen in ihrer internen Kommunikation auch einzelnen Abteilungen direkt eine sichere elektronische Signatur zuordnen. Wird dies durchgeführt, ist aber das SigG zur Gänze nicht mehr anzuwenden.

---

[59] EBRV zu § 2 Z. 2.

[60] Siehe dazu: die Statuten von A-SIT, veröffentlicht in, *Brenn*, Signaturgesetz, S. 167ff.

Das SigG läßt die Frage offen, ob sichere elektronische Signaturen anerkannt werden, die an ein Zertifikat gebunden sind, in dem eine juristische Person angeführt ist. Das Problem entsteht, falls in einem ausländischen Staat juristische Personen als Signatoren zulässig werden und diese juristische Person – z.B. Online Shops – nun mit österreichischen Kunden über das Internet Rechtsgeschäfte abschließen.

Zwei Lösungen sind denkbar: Einerseits erfüllen sie nicht mangels zulässigem Namen im Zertifikat die Anforderungen des SigG. Das führt zu der unerfreulichen Situation, daß beispielsweise ein zwischen einem österreichischen Konsumenten und einer ausländischen juristischen Person, die in ihrem Zertifikat als eben solche bezeichnet ist, abgeschlossener Vertrag nicht die Erfordernisse der Schriftform erfüllt. Durch die Formfreiheit des Vertragsrechts ist der Vertrag auch mit einer „einfachen" elektronischen Signatur nach wie vor gültig abgeschlossen. Die besonderen Vorteile im Beweisrecht, die im SigG gerade für sichere elektronische Signaturen eingeräumt werden, stehen nicht zur Verfügung.

Andererseits könnte das Wahlrecht der SigRL im Zusammenhang mit der Verpflichtung zur gegenseitigen Anerkennung so verstanden werden, daß im jeweiligen Sitzstaat der juristischen Person über die rechtsgültige Signatur entschieden wird. Die anderen Mitgliedsstaaten sind zur Anerkennung dieser Zertifikate verpflichtet. Dies wäre auch mit den Regelungen des Personalstatuts juristischer Personen in § 10 IPRG vereinbar, wonach das Recht des Staates anzuwenden ist, in dem der Rechtsträger den tatsächlichen Sitz seiner Hauptverwaltung hat. Die Führung des Namens einer Person und wohl auch analogerweise die Unterschrift richten sich nach ihrem Personalstatut. Wenn diese Rechtsordnung juristische Personen als Signatoren zuläßt, müßten auch österreichische Gerichte diese Regeln anwenden. Nicht ausjudiziert ist, ob das ganze SigG durch das Recht des anderen Staates über diese Materie ersetzt wird oder die österreichischen Bestimmungen über die Haftung anwendbar blieben, weil § 41 IPRG hier das Rechts des Staates des Verbrauchers zwingend für anwendbar erklärt. Geht man vom Sachverhalt aus, daß die juristische Person ein Online Unternehmen im Ausland und dessen sichere elektronische Signatur von einem Zertifizierungsdiensteanbieter in dessen Sitzstaat ausgestellt ist, der Konsument von Österreich aus mit einer von einem österreichischen Zertifizierungsdiensteanbieter ausgestellten sicheren elektronischen Signatur Warenbestellungen durchführt, wäre es im Sinne des Konsumentenschutzes höchst sinnvoll, die Bestimmungen des SigG über Haftung und Rechtswirkungen der sicheren elektronischen Signatur auch für die Signatur des Online Unternehmens anwenden zu können.

Auch die Anwendbarkeit des EVÜ[61,62] ist in dessen eingeschränktem Geltungsbereich[63] zu bejahen. Art. 9 EVÜ bestimmt nun, daß bei Verträgen zwischen Personen in zwei verschiedenen Staaten ein Vertrag gültig zustande gekommen ist, wenn er den Formvorschriften einer der Staaten entspicht. Erfreulicherweise könnte dann also bei einem Vertrag zwischen einer natürlichen Person in Österreich und einer juristischen Person in einem anderen Vertrag für die Zulässigkeit einer juristischen Person als Signator das Recht des andereren Staates angewandt werden, für sonstige Streitigkeit aber die Bestimmungen des österreichischen Signaturgesetzes. Probleme bereiten auch hier wieder die Rechtsgeschäfte österreichischer Verbraucher, da nach Art. 5 EVÜ, der gemäß Art 9 Abs. 5 EVÜ ausdrücklich zu berücksichtigen ist, bei bestimmten Verbraucherverträgen das Recht des Wohnsitzstaates des Verbrauchers anzuwenden ist.

Die Geltung ausländischer elektronischer Signaturen von juristischen Personen kann allerdings auch auf die Anerkennungsregelung in § 24 gestützt werden, da hier bei Einhaltung der aufgestellten Bedingungen Zertifikate ausländischer Zertifizierungsdiensteanbieter inländischen Zertifikaten gleichgestellt werden. Problematisch ist mE, daß § 24 aber nur die Anerkennung von Zertifikaten regelt, die besonderen Rechtswirkungen sich jedoch auf elektronische Signaturen beziehen. In den Erläuterungen[64] wird festgehalten: „Die rechtliche Anerkennung qualifizierter Zertifikate ist *eine* der Voraussetzungen, daß mit einer „ausländischen" elektronischen Signatur *besondere Rechtswirkungen* im Sinn des § 4 verknüpft sein können. Neben diesen Anforderungen (Anhang I und II der SigRL) müssen aber ... *auch* die Sicherheitsvoraussetzungen des Anhangs III zur Richtlinie eingehalten sein. Bei Vorliegen aller Voraussetzungen liegt eine sichere elektronische Signatur im Sinn des Art. 5 Abs. 1 der Richtlinie vor." Zu untersuchen ist nun, ob die Auflage in der Definition des Signators als natürliche Person durch § 2 Z. 2 auch eine Voraussetzung im Sinne des zitierten Absatzes aus den Erläuterungen ist. Kommt man zu die-

---

[61] Übereinkommen über das auf vertragliche Schuldverhältnisse anzuwendende Recht - EVÜ vom 16.9.1980 (Abl 1980 L 266, 1) in der Fassung des Übereinkommens vom 26.11.1996 über den Beitritt der Republik Österreich, Beitrittsübereinkommen in Ö kundgemacht: BGBl III 1998/166, konsolidierte Fassung des EVÜ kundgemacht in: Abl 1998 C 27, 34 und in BGBl III 1998/208, RV:1232 BlgNR 20. GP.

[62] *Klauser*, EuGVÜ und EVÜ, ecolex Spezial (1999), S. 211ff.

[63] Siehe § 1 Abs. 2, das Kerneinsatzgebiet des elektronischen Geschäftsverkehrs, der Kauf von Waren oder Dienstleistungen fällt allerdings nicht unter die Ausnahmebestimmungen des EVÜ.

[64] EBRV zu § 24 Punkt 3.

sem Schluß, wären ausländische sichere elektronische Signaturen, die durch eine juristische Person abgegeben werden, nach österreichischem Recht nicht mit den besonderen Rechtswirkungen gemäß § 4 auszustatten.

ME beziehen sich die in § 24 verlangten Anforderungen für ausländische elektronische Signaturen aber nur auf die Anforderungen, die durch die SigRL vereinheitlicht werden sollen[65], da darüber hinaus gehende, von den Mitgliedsstaaten festgelegte Mindestanforderungen, deren europaweite Einhaltung Grundlage für die Zuerkennung besonderer Rechtswirkungen ist, den Sinn des freien elektronischen Geschäftsverkehr zwischen den Mitgliedsstaaten verhindern würden. Auch eine sichere elektronische Signatur einer ausländischen juristischen Person könnte daher nach dem öSigG bei Einhaltung aller anderen Anforderungen mit den besonderen Rechtswirkungen des § 4 ausgestattet werden.

Es bleibt abzuwarten, wie die Gerichte dieses Problem lösen werden. Eine konsumentenfreundliche Spruchpraxis wäre wünschenswert, die auf die Anerkennung ausländischer sicherer elektronischer Signaturen und Zertifikate, deren Zertifizierungsdiensteanbieter die Kriterien der allgemeinen Anforderungen zur Anerkennung ausländischer Zertifikate des § 24 erfüllen, abstellt und daher auch Zertifikate mit dem Namen juristischer Personen als qualifizierte Zertifikate anerkennt. In diesen Fällen wird dadurch das ausgewogene und dem österreichischen Konsumenten vertrautere österreichische Gesetz anwendbar.

Weiters wurde in Österreich über ein Mindestalter für Signatoren diskutiert. Da die Wirtschaftsuniversität Wien auch für ihre achtzehnjährigen Studenten Zertifikate vergeben will, stellte sich die Frage, ob minderjährigen Personen Zertifikate ausgestellt werden können. Die Telekom Control GmbH kommt nach einer Prüfung der Rechtslage zum Ergebnis, daß weder § 5 noch die SigVO dazu explizite Regelungen enthalten. Im Justizausschußbericht wurde zu § 5 Abs. 1 Z 3 festgehalten, daß sich die Möglichkeiten des Erwerbs eines Zertifikats und der Verwendung der Signatur nach den allgemeinen zivilrechtlichen Bestimmungen des ABGB richten. Ab dem siebten Lebensjahr besteht eine beschränkte Geschäftsfähigkeit, deren Umfang ab dem vierzehnten Lebensjahr erweitert ist. Der Ausstellung eines qualifizierten Zertifikats steht der Umstand, daß der Si-

---

[65] Für die Erlangung der Rechtswirkungen gemäß Art. 5 SigRL wären folgende Auflagen zu erfüllen (nach: *Gravesen/Dumortier/Van Eecke*, Europäische Signaturrichtlinie, MMR (1999), S. 579). Es liegt eine fortgeschrittene elektronische Signatur vor. Diese ist dem Signierenden durch ein qualifiziertes Zertifikat zugeordnet und von einer sicheren Signaturerstellungseinheit generiert worden.

gnator noch nicht volljährig – daher unter neunzehn Jahre – ist, also nicht entgegen.

4.5. Freier Marktzugang für Zertifizierungsdiensteanbieter

Das SigG folgt der SigRL und verneint für die Aufnahme und die Ausübung der Tätigkeit eines Zertifizierungsdiensteanbieters das Erfordernis einer hoheitlichen Genehmigung, übernimmt aber auch – soweit möglich – Aspekte des deutschen SigG, um die Gewährleistung von Sicherheit und Qualität in der Public-Key-Infrastruktur nicht alleine den Kräften des freien Marktes zu überlassen.

Das Verbot einer Genehmigungspflicht war einer der Hauptdiskussionspunkte während der Entstehung der Richtlinie, ursprünglich war ein noch liberaleres System vorgesehen, in dem nicht alle Anforderungen der vier Anhänge der SigRL vorgesehen sind. Dies fand jedoch von deutscher und in gemilderter Form auch von österreichischer Seite zuviel Widerspruch, so daß zu der Einführung einer prinzipiellen Genehmigungsfreiheit im Gegenzug die Anforderungen an Zertifizierungsdiensteanbieter, qualifizierte Zertifikate und Signaturprodukte im Entwurf gesteigert wurden. Die Auflagen sind gestaffelt für Anbieter einfacher Zertifikate, Anbieter qualifizierter Zertifikate und schlußendlich für Zertifizierungsdiensteanbieter, die sich einer freiwilligen Akkreditierung unterzogen haben. Begründet wird das Verbot der Genehmigungspflicht durch das Grundprinzip des freien Waren- und Dienstleistungsverkehr innerhalb des Europäischen Wirtschaftsraumes. In der Begründung heißt es dazu, daß der Binnenmarkt den Zertifizierungsdiensteanbietern gestattet, grenzüberschreitend tätig zu werden, um ihre Wettbewerbsfähigkeit zu steigern und damit Verbrauchern und Unternehmen neue Möglichkeiten des sicheren, grenzenlosen Informationsaustausch und elektronischen Geschäftsverkehr zu eröffnen.[66]

Die Mitgliedsstaaten sollen gehindert werden, mittels vordergründig technisch bedingter Zulassungsnormen Bewerbern aus anderen Mitgliedsstaaten den Zugang zu ihren nationalen Märkten zu verhindern, wie das in der Vergangenheit der EuGH schon oft feststellte. Die Qualität der angebotenen Zertifizierungsdienste können durch die freien Kräfte des Marktes, eine verschärfte Haftung für Fehler der Zertifizierungsdiensteanbieter und durch das Systems einer freiwilligen Akkreditierung besser gesichert

---

[66] Erwägungsgrund Z. 8 SigRL.

werden als durch ein hoheitliches Genehmigungssystem. Von dem Verbot der Genehmigungspflicht ist das Gebot der Durchführung staatlicher Aufsichtsmaßnahmen, also eine Überwachung des laufenden Betriebs, zu unterscheiden. Es wird in Art. 3 Abs. 3 der SigRL ausdrücklich gefordert.

4.5.1. Zugang für Anbieter einfacher elektronischer Signaturen ohne qualifiziertes Zertifikat

Das Prinzip der Genehmigungsfreiheit wird durch ein Verbot im § 6 Abs. 1 der speziellen Genehmigung für die Tätigkeit als Zertifizierungsdiensteanbieter verwirklicht. Nicht nur die explizit angeordnete Genehmigungspflicht ist nicht gestattet, auch die Anordnung von sonstigen Maßnahmen mit gleicher Wirkung ist damit untersagt.[67]

Im Gegensatz dazu bleiben aber allgemeine Zulassungsvoraussetzungen, wobei hier besonders die Gewerbeordnung berücksichtigt werden muß, nach der Zertifizierungsdiensteanbieter als Datenverarbeiter zu qualifizieren[68] und daher der Kategorie der anmeldungspflichtigen freien Gewerbe[69] zuzuordnen sind.[70] Falls die in diesem Verfahren gestellten Anforderungen durch einen Anbieter von Zertifizierungsdiensten nicht erbracht werden können, dann ist es der zuständigen Behörde gemäß Gewerbeordnung möglich, die Aufnahme der Tätigkeit zu verweigern. Diese Kontrolle ist unabhängig von der Aufsicht durch die Aufsichtsstelle gemäß dem SigG. Hier können Anbieter also sehr wohl durch Rechtsnormen mit anderem Regelungsgebiet einem Genehmigungssystem unterworfen sein. Das Genehmigungssystem darf aber nicht ausschließlich für Zertifizierungsdiensteanbieter gelten.

Im folgenden sollen nur die Anforderungen des SigG besprochen werden. Verwirklicht wird im 4. Abschnitt des SigG (§§ 13 ff.) ein System der Aufsicht, das nach der SigRL zulässig und geboten ist.[71] In dessen Rahmen haben alle Zertifizierungsdiensteanbieter ein Sicherheitskonzept, das Aussagen des Diensteanbieters über seine Sicherheitsstandards sowie die infrastrukturellen, personellen und organisatorischen Maßnahmen enthält, und ein Zertifizierungskonzept über die bei der Ausstellung

---

[67] Erwägungsgrund Z. 10 SigRL, der auch in die Erläuterungen zur Regierungsvorlage SigG übernommen wurde.

[68] § 271 GewO 1994: Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik.

[69] Die Verfahrensvorschriften für die Anmeldung finden sich in § 339f GewO 1994.

[70] EBRV zu § 6 Abs. 1.

[71] Art. 3 Abs. 3 SigRL.

und dem Widerruf von Zertifikaten eingehaltene Vorgangsweise spätestens mit Aufnahme der Tätigkeit[72] einer Aufsichtsstelle vorzulegen. Die Ausgestaltung der Konzepte erfolgt durch die Anbieter, die einfache Zertifizierungsdienste erbringen, nach ihrem eigenen Ermessen. Sie sind insbesondere nicht an die deutlich kasuistischeren Auflagen für Anbieter sicherer elektronischer Signaturen und qualifizierter Zertifikate gebunden, müssen aber wohl die deutlich milderen allgemeinen Anordnungen des SigG beachten. Trotzdem gelten auch für Anbieter einfacher elektronischer Signaturen ohne qualifiziertes Zertifikat folgende Bestimmungen des SigG:

- § 2: die Begriffsbestimmungen,
- § 9: die Regelung über Widerruf von Zertifikaten,
- § 10: über Zeitstempeldienste (soweit sie erbracht werden)
- § 11: die Anordnungen über Dokumentation
- § 12: Einstellen der Tätigkeit
- § 20: allgemeine Informationsverpflichtung der Zertifizierungsdiensteanbieter
- § 22: Datenschutz

4.5.2. Sicherheits- und Zertifizierungskonzept

Die Einhaltung dieser Sicherheitsanforderungen ist gemäß § 6 Abs. 3 von jedem Zertifizierungsdiensteanbieter in einem Sicherheits- und Zertifizierungskonzept darzulegen, das nach § 6 Abs. 2 spätestens mit Aufnahme der Tätigkeit der Aufsichtsstelle in elektronischer Form vorzulegen ist. Die Sicherheits- und Zertifizierungskonzepte, die meist als Policies bezeichnet werden, sind auch auf den Internetseiten der Zertifizierungsdiensteanbieter veröffentlicht, da die Zertifizierungsdiensteanbieter gemäß § 15 Abs. 2 SigVO die beiden Konzepte im Format RTF, PDF oder Postscript elektronisch jederzeit allgemein abrufbar zu halten haben. Ein Zertifizierungsdiensteanbieter kann auch mehrere Klassen an elektronischen Signaturen zu unterschiedlichen Preisen anbieten, denen dann ebenfalls unterschiedliche Policies zugeordnet sind. Bei nicht erfolgter Umsetzung der Konzepte, die allerdings selbst vom Anbieter erstellt werden und nicht starr durch die Behörde vorgegeben sind, hat die Aufsichts-

---

[72] Wobei die Telekom Control GmbH davon ausgeht, daß die neu auftretenden Zertifizierungsdiensteanbieter die Konzepte rechtzeitig vor dem Aufnehmen ihrer Tätigkeit einbringen, und diese nicht erst im Zeitpunkt der Aufnahme der Tätigkeit zu übermitteln.

stelle Maßnahmen zu ergreifen, die bis zur Einstellung des Betriebes des Zertifizierungsdiensteanbieters führen können.

Bei einem Sicherheitskonzept handelt es sich um die festgelegten Aussagen eines Zertifizierungsdiensteanbieters über technische und organisatorische Sicherheitsmaßnahmen und die für die von ihm bereitgestellten Signaturverfahren einzuhaltenden Sicherheitsanforderungen. Der Zertifizierungsdiensteanbieter hat in diesem Konzept darzulegen, welchem Sicherheitsniveau die von ihm eingesetzten und bereitgestellten Signaturverfahren und Produkte sowie die von ihm bereitgestellten Dienste entsprechen, welche Sicherheitsanforderungen hierfür festgelegt sind und durch welche Maßnahmen diese erreicht werden. Anhand des Sicherheitskonzepts muß eine verläßliche Aussage über die Vertrauenswürdigkeit des Betriebes des Zertifizierungsdiensteanbieters getroffen werden können.[73] In § 15 SigVO findet sich eine demonstrative Aufzählung der Mindestinhalte eines Sicherheits- und Zertifizierungskonzeptes. Folgende Sicherheitsanforderungen sind insbesondere darzulegen:

- Infrastrukturelle Sicherheitsanforderungen:
  - geeignete Räumlichkeiten
  - Schutz vor Zutritt unbefugter Personen
  - Schutz der technischen Ausstattung vor unbefugtem Zugriff[74]
  - Aufbewahrung der Produkte und des Schlüsselmaterials
- Personelle Sicherheitsanforderungen:
  - Zuverlässigkeit und Fachkunde[75]
  - Schulungsmaßnahmen
  - Unbescholtenheit[76]
- Organisatorische Maßnahmen:
  - sichere Protokollierung und Archivierung der Zertifizierungsdaten[77]
  - geeignetes Backup
  - Verhinderung des unbefugten Zugriffs auf private Schlüssel und Verzeichnisse
  - geeignete Vernichtung nicht mehr benötigter oder ungültiger Daten

---

[73] 1999 der Beilagen zu den Stenographischen Protokollen des NR der XX. Gesetzgebungsperiode, S. 29.

[74] Näher geregelt in § 10 Abs. 2 und 3 SigVO.

[75] Näher geregelt in § 10 Abs. 5 SigVO.

[76] Näher geregelt in § 10 Abs. 4 SigVO.

[77] Verzeichnis- und Widerrufsdienst sind in § 13 SigVO normiert.

- Technische Sicherheitsanforderungen.[78]
  - gegebenenfalls sichere Schlüsselgenerierung und -speicherung[79]
  - sichere Erzeugung und Speicherung von Zertifikaten
  - Verhinderung der Aktivierung des privaten Signaturschlüssels durch Unbefugte
  - Maßnahmen bei Verlust oder Kompromittierung des eigenen Signaturschlüssels
  - Notfallvorsorge

verständliche und nachvollziehbare Darlegung der zugrundeliegenden technischen und kryptographischen Normen Bei einem Zertifizierungskonzept handelt es sich um die festgelegten Aussagen eines Zertifizierungsdiensteanbieters über die bei der Ausstellung von Zertifikaten eingehaltene Vorgangsweise. Darin wird die Art der Erbringung der Zertifizierungsdienste näher beschrieben. Insbesondere sind folgende Punkte zu regeln:

- Art und Weise der Identifizierung der Anwender[80]
  - Es genügt lediglich die Existenz der E-Mail-Adresse.
  - Eine Personenidentifizierung anhand übermittelter Dokumente ist notwendig.
  - Die Personenidentifizierung anhand vorgelegter Dokumente und persönliches Erscheinen ist gefordert.
- Modus der Antragstellung[81]
- Generierung der Signaturerstellungsdaten und der korrespondierenden Signaturprüfdaten
  - Die Selbstgenerierung durch den Zertifikatswerber oder
  - Generierung durch den Zertifizierungsdiensteanbieter; wobei Vernichtung der Signaturerstellungsdaten beim Zertifizierungsdiensteanbieter gewährleistet sein müssen.
- Erhalt des Zertifikats
  - Es kann per E-Mail erhalten werden.
  - Das Zertifikat wird durch Download von einem Verzeichnis übermittelt.
- Information des Signators[82]

---

[78] Siehe in § 6 SigVO.

[79] Vorschriften über die Erzeugung von Signaturerstellungsdaten für sichere elektronische Signaturen finden sich in § 3 Abs. 3 SigVO.

[80] Bezüglich qualifizierter Zertifikate näher geregelt in § 11 SigVO.

[81] In § 11 SigVO näher geregelt.

- Erneuerung des Zertifikats
  - Eine nochmalige Zertifizierung derselben Signaturprüfdaten ist nötig.
  - Angaben über die maximale Gesamtdauer bei der Erneuerung sind zu machen.
  - keine neuerliche persönliche Überprüfung der Identität, die Verlängerung kann auch durch ein sicher elektronisch signiertes Dokument beantragt werden (§ 11 Abs. 1 SigVO).
- Art und Weise des Abrufs und der Überprüfung der Zertifikate
  - Meist ist dies ein Verzeichnisdienst[83]
- Widerruf von Zertifikaten
  - Der Widerruf erfolgt persönlich durch den Signator.
  - Er kann auch durch bestimmte staatliche Stellen angeordnet werden.
  - Die Information des Signators über den Widerruf muß gewährleistet sein.
  - Kein rückwirkender Widerruf ist möglich.
  - Der Widerruf kann nicht mehr rückgängig gemacht werden.
  - Die einzige Ausnahme ist der als Aufsichtsmaßnahme von der Telekom-Control GmbH zu unrecht angeordnete Widerruf von Zertifikaten. Da die Aufsichtsmaßnahmen der Telekom-Control GmbH vorläufiger Natur sind, kann dieser Widerruf von der Aufsichtsstelle rückgängig gemacht werden.

4.5.3. Zugang für Anbieter sicherer elektronischer Signaturen

Anbieter sicherer elektronischer Signaturverfahren haben die Einhaltung aller Sicherheitsanforderungen des SigG darzulegen. Auch sie unterliegen wie alle Diensteanbieter ab Anzeige der Tätigkeit der Kontrolle der Aufsichtsstelle.

Da den sicheren elektronischen Signaturen erhöhte Rechtswirkung gegenüber einfachen elektronischen Signaturen zukommt, ist auch die Erfüllung von höheren Sicherheitsanforderungen durch Diensteanbieter sicherer elektronischer Signaturen zu gewährleisten. Sie müssen die Um-

---

[82] Gemäß § 10 SigVO ist der Signator schriftlich oder mit einem dauerhaften Datenträger (Disketten sind zulässig, E-Mail nicht) über alle sicherheitsrelevanten Maßnahmen klar und allgemein verständlich zu informieren.

[83] Der Abruf qualifizierter Zertifikate muß über einen Verzeichnisdienst, der dem ITU-T X.500 Standard entspricht, erfolgen.

setzung aller Maßnahmen des SigG sicherstellen. Nur die vorgesehene Kombination aller Sicherheitsanforderungen gewährleistet die zuverlässige Zuordnung elektronischer Signaturen und damit verknüpfter qualifizierter Zertifikate an die natürliche Person des jeweiligen Signators. Erst dadurch ist der Einsatz sicherer elektronischer Signaturen auch im Rechtsverkehr ermöglicht.

Im Sicherheits- und Zertifizierungskonzept müssen daher über die generellen Anforderungen an Zertifizierungsdiensteanbieter hinaus insbesondere die Einhaltung der Regelungen der Anhänge des SigRL, die in den Bestimmungen des SigG über Inhalt qualifizierter Zertifikate, Tätigkeit der Zertifizierungsdiensteanbieter qualifizierter Zertifikate und technische Komponenten und Verfahren für sichere Signaturen umgesetzt sind, plausibel und nachvollziehbar dokumentiert werden. Muß der Anbieter einfacher elektronischer Signaturen sein Sicherheits- und Zertifizierungskonzept nur der Aufsichtsstelle vorlegen, so hat der Anbieter sicherer elektronischer Signaturen gemäß § 6 Abs. 3 darüber hinaus auch die Einhaltung der Sicherheitsanforderungen des SigG darzulegen. Dadurch wird er verpflichtet, die tatsächliche Einhaltung der sich ihm selbst auferlegten Sicherheitsmaßnahmen auch zu begründen.

4.5.4. Zugang für akkreditierte Zertifizierungsdiensteanbieter

Die SigRL führte in Art.3 Abs. 2 die Möglichkeit freiwilliger Akkreditierung für höherwertige Zertifizierungsdienste gewissermaßen als Ergänzung zum System der staatlichen Aufsicht ein. In den Erläuterungen zur RV SigG[84] wird die Einführung und europarechtliche Zulässigkeit der freiwilligen Akkreditierung aus europäischer Sicht „quasi als Ausgleich für das Verbot [der SigRL] von Genehmigungs- bzw Lizenzierungsverfahren" gesehen Aus der Begründung zur SigRL ist zu entnehmen, daß darunter Zertifizierungsdiensteanbieter mit hohem Sicherheitsniveau zu verstehen sind.[85]

Die Kommission ist der Überzeugung, daß freiwillige Akkreditierungssysteme geeignet sind, um das auf dem Markt geforderte Maß an Vertrauen, Sicherheit und Qualität zu erreichen.[86] Gemeinsam mit den Haftungsbestimmungen soll das Institut der freiwilligen Akkreditierung

---

[84] EBRV zu § 17 Abs. 1.

[85] Begründung Z. 3 SigRL.

[86] Erwägungsgrund Z. 9 SigRL.

die Stabilität der Infrastruktur gewährleisten, damit das Modell eines hoheitlichen Genehmigungssystems vermieden werden kann.

Die Signatoren in ihrer Rolle als Konsumenten würden nach dieser Überlegung freiwillig akkreditierten Zertifizierungsdiensteanbietern besonderes Vertrauen entgegenbringen und diese bei der Wahl des Anbieters bevorzugen. Auf Grund dieses Drucks des Marktes würden sich die meisten Anbieter fortgeschrittener elektronischer Signaturen mit qualifiziertem Zertifikat einer freiwilligen Akkreditierung unterziehen.

Die Sinnhaftigkeit dieses Instruments ist allerdings zu diskutieren. Bei der freiwilligen Akkreditierung und der Überprüfung nach der Meldung der Aufnahme der Tätigkeit eines Zertifizierungsdiensteanbieters für sichere elektronische Signaturen werden durch die gleiche Behörde – es ist beide Male die Aufsichtsstelle zuständig – die Einhaltung derselben Anforderung der §§ 5, 7 und 18 untersucht. Es ist nicht ganz ersichtlich, wie durch eine doppelte, aber gleichartige Überprüfung das Qualitätsniveau gehoben werden kann. Letztlich bleibt aber abzuwarten, wie der Markt auf die Akkreditierung reagiert, sollte es tatsächlich – wie in den Erläuterungen angenommen – in den Augen der Konsumenten als eine zusätzliche vertrauensbildende Maßnahme gesehen werden, ist das Instrument der Akkreditierung als sinnvolles, benötigtes Instrument zu werten, da bei der heute noch vorherrschenden Ansicht über die mangelnde Sicherheit beim rechtsgeschäftlichen Verkehr über das Internet jede zusätzliche vertrauensbildende Maßnahme begrüßt werden muß.

An und für sich ist die Akkreditierung kein Kriterium für eine Bedingung zum freien Marktzugang, weil jeder Zertifizierungsdiensteanbieter auch ohne Akkreditierung nach Meldung bei der Aufsichtsstelle die Tätigkeit aufnehmen kann. Da aber schon im vorigen Punkt der Zugang für Diensteanbieter einfacher und sichere elektronischer Signaturen besprochen worden ist, soll auch der Weg eines Zertifizierungsdiensteanbieters zu seiner Akkreditierung hier besprochen werden. Es handelt sich hier also genau genommen nicht um den Zugang zum Markt, sondern um den Zugang zur Bewilligung der Akkreditierung.

Das österreichische SigG übernimmt dieses Modell und gestaltet es in § 17 SigG näher aus. Nach Auffassung des nationalen Gesetzgebers ist die freiwillige Akkreditierung als Erlaubnis der Überwachungsbehörde zu verstehen, mit der Rechte und Pflichten eines Zertifizierungsdiensteanbieters auf seinen Antrag hin festgelegt werden.

Dem gemäß können akkreditierungswillige Zertifizierungsdiensteanbieter bei der Aufsichtsbehörde die Akkreditierung beantragen, die Aufsichtsstelle ihrerseits kann aber nur auf Antrag eines Zertifizierungsdien-

steanbieters tätig werden. Eine Akkreditierung durch die Aufsichtsstelle aus eigener Initiative ist nicht vorgesehen. Nach dem eingegangenen Antrag prüft die Aufsichtsstelle die Einhaltung der Sicherheitsanforderungen, wobei, wie im Wortlaut des SigG erwähnt, insbesondere die Einhaltung der Bestimmungen des § 18 geprüft wird. Aber auch die nur in den Erläuterungen erwähnte Prüfung der Einhaltung der §§ 5 und 7 ist Bestandteil der Akkreditierung.

Die Rechtsform der Entscheidung der Aufsichtsstelle bezüglich der Akkreditierung ist noch unklar. Die Erläuterungen[87] sprechen von einem „Bescheid", verwenden das Wort also nur in Anführungszeichen. Da die Aufsichtsstelle aber eine hoheitliche Behörde ist, die Prüfung auf Antrag erfolgt und die SigRL ja ein hoheitliches System zur Beaufsichtigung der Akkreditierung fordert, wäre mE die Entscheidung in Form eines Bescheides den Umständen angepaßt, und die Anwendbarkeit des AVG auch auf die Akkreditierung zu bejahen. Eine Entscheidung in dieser Form würde auch die Abgrenzung des hoheitlichen Handelns der Aufsichtsstelle, wenn sie Zertifizierungsdiensteanbieter akkreditiert, zum rein privatrechtlich verliehenen (Qualitäts-)Zertifikat für Zertifizierungsdiensteanbieter durch autorisierte Prüfstellen verdeutlichen. Dieses Verfahren wird am Ende dieses Punktes besprochen.

Durch die Akkreditierung erwirbt der Zertifizierungsdiensteanbieter besondere Rechte. Als solche kommen besondere Werbe- und Marketingmaßnahmen, wie die Bezeichnung als „akkreditierter Zertifizierungsdiensteanbieter" im Geschäftsverkehr oder die Verwendung eines Logos, in Betracht. Die Bezeichnung „akkreditierter Zertifizierungsdiensteanbieter" kann etwa auf dem Briefpapier oder einer Webseite verwendet werden. Die besonderen Rechtswirkungen nach § 4 SigG dürfen aber nicht von einer Akkreditierung abhängig gemacht werden.[88] Sie müssen auch im Außenverhältnis bei der Kommunikation mit dem Signator und seinen Geschäftspartnern ersichtlich sein.[89] Deshalb darf sich nicht nur der Zertifizierungsdiensteanbieter in Logo und Geschäftsbezeichnung als freiwillig akkreditiert bezeichnen, sondern weiters ist auch die erfolgte Akkreditierung eines Zertifizierungsdiensteanbieters daher sogar verpflichtend laut § 17 Abs. 2 in den von ihm ausgestellten qualifizierten Zertifikaten kenntlich oder sonst in geeigneter Weise zugänglich zu machen. Gemäß § 17 Abs.1 letzter Satz ist die Aufsichtsstelle auch dazu an-

---

[87] EBRV zu § 17 Rz. 1.
[88] EBRV zu § 17 Rz. 1.
[89] EBRV zu § 17 Rz. 2.

gehalten, ein allgemein jederzeit zugängliches Verzeichnis zu führen, in dem alle freiwillig akkreditierten Zertifizierungsdiensteanbieter angeführt sind.

Diese Rechte dürfen erst nach der Zustellung des Bescheides an den Zertifizierungsdiensteanbieter ausgeübt werden. Die Überprüfung durch die Aufsichtsstelle ist daher als ex-ante Überprüfung zu qualifizieren. Der Antrag auf Akkreditierung muß aber nicht vor Aufnahme der Geschäftstätigkeit gestellt werden. Auch Zertifizierungsdiensteanbieter, die schon am Markt tätig sind, können später einen Antrag auf Akkreditierung stellen.

§ 17 Abs. 3 stellt noch sicher, daß die laufende Aufsicht durch die Aufsichtsstelle von dem einmaligen Verfahren der Akkreditierung unberührt bleibt. Die Einhaltung aller gesetzlichen Anforderungen ist unabhängig vom Verfahren der Akkreditierung permanent zu gewährleisten.

4.5.4.1. Zertifizierung (Akkreditierung) durch private Prüfanstalten

Im Gegensatz zur Akkreditierung durch die Aufsichtsstelle, die hoheitlich durchgeführt wird, da es sich bei der Telekom-Control Kommission als Aufsichtsstelle um eine Behörde handelt[90], versteht man unter Zertifizierung von Zertifizierungsdiensteanbietern eine Sicherheitskontrolle durch privatrechtliche Prüfungsvereine[91] mit den Rechtsinstituten des Zivilrechts. Oft wird aber auch die privatrechtliche Zertifizierung als Akkreditierung bezeichnet. Um Verwechslungen zu vermeiden, bezieht sich die Verwendung des Begriffs Zertifizierung von Zertifizierungsdiensteanbietern in dieser Arbeit immer auf den privatrechtlichen Bereich.

Allerdings kann sich nach § 15 Abs. 2 Z. die Telekom-Control Kommission auch der Telekom-Control GmbH zur Durchführung der Akkreditierung bedienen. Trotz privatrechtlicher Natur wird die Gesellschaft aber als beliehenes Unternehmen tätig und alle ihre Rechtsakte in Bezug der Akkreditierung sind hoheitlicher, öffentlich-rechtlicher Natur. Sie ist den Weisungen der Telekom-Control Kommission unterworfen.

Zertifizierungen im Sinne von Akkreditierung durch private Prüfanstalten werden allerdings von unabhängigen Prüfanstalten vorgenommen. Sie kommen der Forderung der Konsumenten nach zusätzlichen Quali-

---

[90] Eingerichtet durch das TKG

[91] In Österreich übernimmt zum Beispiel der Technische Überwachungsverein (TÜV) solche Aufgaben.

tätsaussagen über die geprüften Zertifizierungsdiensteanbieter von einer unabhängigen Stelle nach, die über die nötigen Einrichtungen, die fachliche Kompetenz und Erfahrung verfügt.[92] Die Tätigkeiten eines solchen Prüflaboratoriums müssen auch einem internationalen Regelwerk genügen, damit Prüfungen desselben Zertifizierungsdiensteanbieters durch verschiedene Anstalten zu vergleichbaren Ergebnissen führen. In Europa hat sich der Standard der europäischen Norm „DIN EN 45010-Allgemeine Anforderungen an die Begutachtung und Akkreditierung von Zertifizierungsstellen" durchgesetzt.[93] Im Zuge des Prüfungsverfahrens werden die eingesetzten IT-Installationen[94] im allgemeinen und die besonderen Anforderungen des SigG geprüft.

In Deutschland hat die Regulierungsbehörde für Telekommunikation und Post neben dem Bundesamt für Sicherheit in der Informationstechnik, das laut dSigG für die Erteilung von Sicherheitszertifikaten[95] zuständig ist, bis jetzt 3 private Zertifizierungsstellen[96] anerkannt.[97]

Man könnte argumentieren, daß auch in Österreich private Prüfstellen zu einer der Akkreditierung gemäß § 17 äquivalenten Prüfung berechtigt sind. Einerseits ist es auf Grund der Systematik des SigG und der Aufgaben, die es an die Bestätigungsstellen delegiert, denkbar, daß die Bestätigungsstellen dies übernehmen können. Da A-SIT[98] als erste Bestätigungsstelle in Form eines privatrechtlichen Vereines errichtet ist, könnte man hier von einer Analogie zur deutschen Situation sprechen. Andererseits ist weder im Gesetzestext noch in den parlamentarischen Materialien eine Übernahme dieser Aufgabe von Bestätigungsstellen vorgesehen. Auch kann es sich trotz Tätigwerden dieser Vereine immer noch um eine Beleihung handeln, wodurch die Akkreditierung wieder als hoheitlicher Akt zu

---

[92] *Rohde/Witzel*, Akkreditierung von Prüflaboratorien, „to trust or not to trust, that is the question", DuD (1998), S. 203.

[93] *Witzel*, Gateway: Akkreditierung, DuD (1998), S. 226.

[94] *Schütz*ig, Prüfung und Zertifizierung von IT-Installationen, DuD (1998), S. 207.

[95] Die Sicherheitszertifikate des dSigG entsprechen der Überprüfung im Rahmen einer Akkreditierung gemäß dem SigG. Sie sind aber verpflichtend einzuholen, da das dSigG (noch) ein Genehmigungssystem verlangt.

[96] In diesem Zusammenhang sind keine Zertifizierungsdiensteanbieter gemeint, sondern Stellen, die die Zertifizierung von Diensteanbietern durchführen.

[97] *Roßnagel*, Anerkennung von Prüf- und Bestätigungsstellen nach dem [deutschen] Signaturgesetz, MMR (1999), S. 342. *Blattner-Zimmermann*, Warum (BSI-) Zertifikate? DuD (1998), S. 222.

[98] Die Statuten des Vereines „Zentrum für sichere Informationstechnologie" (A-SIT) sind in: *Brenn*, Signaturgesetz, S. 167 ff abgedruckt.

sehen ist. Auch in den Zielen der SigRL[99] wird davon gesprochen, die Akkreditierung als öffentliches Serviceangebot für Zertifizierungsdiensteanbieter, die hochwertige Dienste anbieten möchten, zu verstehen. Auch dies ist ein Indiz für die Durchführung der Akkreditierung ausschließlich durch hoheitlich handelnde Stellen.

4.5.4.2. Anwendbarkeit des Akkreditierungsgesetzes

Mögliche Probleme werden auch in Verbindung mit dem Akkreditierungsgesetz[100] in einer Stellungnahme der Bundeswirtschaftskammer[101] gesehen. Dort wird darauf hingewiesen, daß das SigG hinsichtlich seiner Einordnung in das bestehende Rechtssystem einige Unklarheiten in sich birgt: So ist dessen Verhältnis zum bereits länger bestehenden Akkreditierungsgesetz, das sich ebenfalls mit der Akkreditierung von beschäftigt und somit vor allem in terminologischer Hinsicht Verwirrung stiften könnte, nicht eindeutig. Dieses Gesetz regelt die Akkreditierung von Prüf-, Überwachungs- und Zertifizierungsstellen und legt die hierzu erforderlichen Verfahrensbestimmungen fest. Obwohl das Akkreditierungsgesetz von Zertifizierungsstellen spricht, das SigG im Gegensatz dazu aber von Zertifizierungsdiensteanbietern, könnte dies leicht verwechselt werden, da auch der Begriff für Zertifizierungsdiensteanbieter sehr oft verwendet wird.[102] ME ist dieses Problem aber durch die Bestimmung in § 1 Abs. 2 Akkreditierungsgesetz gelöst, die regelt, daß das Akkreditierungsgesetz nur für Prüf-, Überwachungs- und Zertifizierungsstellen in Bereichen, in denen der Bund für die Gesetzgebung und Vollziehung zuständig ist, gilt, sofern die diese Bereiche regelnden Bundesgesetze keine den Bestimmungen dieses Bundesgesetzes entsprechenden Festsetzungen über die Akkreditierung solcher Stellen enthalten. Solche Bestimmungen werden durch dieses Bundesgesetz nicht berührt. Da § 17 explizit eigene Regelungen für die Akkreditierung von Zertifizierungsdiensteanbietern nor-

---

[99] Ziel 4, S.7, KOM(98)207.

[100] Bundesgesetz über die Akkreditierung von Prüf-, Überwachungs- und Zertifizierungsstellen, (Akkreditierungsgesetz-AkkG) (NR: GP XVIII RV 508 AB 624 S. 77. BR: AB 4322 S. 557.) StF: BGBl. Nr. 468/1992.

[101] Stellungnahme der Bundeswirtschaftskammer im Rahmen des Begutachtungsverfahren zu einem Entwurf für ein Bundesgesetz über elektronische Signaturen vom 9. Mai 1999, GZ 7.051C/50-I.2/99.

[102] Zum Beispiel spricht das dSigG nur von Zertifizierungsstellen.

miert, ist klargestellt, daß die Anwendung von § 17 als lex specialis dem Akkreditierungsgesetz vorgezogen wird.[103]

4.6. Aufsicht über Zertifizierungsdiensteanbieter

In den Anfangszeiten der Verwendung elektronischer Signaturen und von Zertifikaten wurde noch über die institutionell-organisatorische Gestaltung informationstechnischer Sicherungsinfrastrukturen[104] diskutiert und überlegt, ob nicht alle Zertifizierungsdienste durch Behörden im Rahmen der Hoheitsverwaltung erbracht werden sollen, da ja auch die analog anzusehenden Personalausweise hoheitlich vergeben werden. Spätestens mit dem erfolgreichen Abschluß der Liberalisierung des Telekommunikationsmarktes erkannte man aber, daß auch die Zertifizierungsdienste privatwirtschaftlich erbracht werden sollen, wie es durch die SigRL und ihr folgend das SigG vorgesehen ist. Lediglich in Finnland existiert ein Gesetzesentwurf, der davon ausgeht, daß Zertifizierungsdienste hoheitlich vorgesehen werden. Hierzu soll jedem Bürger eine „digital ID Card" ausgestellt werde. Zertifizierungsdiensteanbieter soll hierbei das Einwohnermeldeamt sein.[105] Geblieben ist aber eine staatliche Aufsicht über die Zertifizierungsdiensteanbieter, wie es auch im Telekommunikationsbereich zur Regulierung verwirklicht ist.

Durch die politische Entscheidung des Verbots eines ex ante Genehmigungssystem für Zertifizierungsdiensteanbieter auf europäischer Ebene muß die Qualität der Public Key Infrastructure auf andere Weise gesichert werden. Neben dem Übermitteln der Sicherheits- und Zertifizierungskonzepte und deren Prüfung durch die Aufsichtsstelle bei Aufnahme der Tätigkeit hat die laufende Aufsicht über die Zertifizierungsdiensteanbieter eine bedeutende Stellung innerhalb der Maßnahmen zur Qualitätssicherung in der Infrastruktur. Jeder Mitgliedsstaat wird durch Art. 3 Abs. 3 SigRL zur Schaffung eines geeigneten Aufsichtssystem zur Überwachung der in seinem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter verpflichtet.

Der Gesetzgeber hat die Bedeutung dieser Maßnahmen erkannt und der Regelung der Aufsicht über die Zertifizierungsdiensteanbieter einen eigenen, umfangreichen Abschnitt des SigG gewidmet. Im Rahmen dieses

---

[103] *Mayer-Schönberger/Pilz/Reiser/Schmölzer,* Signaturgesetz, S. 124.

[104] *Roßnagel,* Institutionell-organisatorische Gestaltung informationstechnischer Sicherungsinfrastrukturen, DuD (1995), S. 259.

[105] *Boriths Müller/Roessler,* Zur rechtlichen Anerkennung elektronischer Signaturen in Europa, DuD (1999), S. 497.

Abschnitts wird die Struktur der Aufsichtsstelle, der Umfang der Aufsicht, die Aufgaben der Wurzel, die Maßnahmen, die zur Durchführung der Aufsicht ergriffen werden können und die faktische Durchführung der Aufsicht festgelegt.

4.6.1. Aufsichtsstelle

4.6.1.1. Telekom-Control Kommission

Das SigG schafft keine neue Behörde für diese Aufgabe, sondern greift auf die bewährten Regelungen des Telekommunikationsgesetzes zurück, das in den §§ 107 und 110 TKG die Telekom-Control Kommission und ihr zur Seite gestellt die Telekom-Control GmbH als Aufsichtstelle und Regulator über die Anbieter im Telekommunikationsbereich einrichtet. Sie ist als von den Telekommunikationsunternehmen rechtlich getrennte und funktionell unabhängige Behörde gestaltet.[106] Die Telekom-Control-Kommission[107] ist als weisungsfreie Kollegialbehörde mit richterlichem Einschlag eingerichtet worden. In § 13 Abs. 6 wird die Weisungsfreiheit auch für alle Aufgaben im Rahmen des SigG ausdrücklich noch einmal angeordnet. Sie besteht aus 3 Mitgliedern, die von der Bundesregierung für fünf Jahre ernannt werden. Die Kommission entscheidet in erster und letzter Instanz; gegen ihre Entscheidungen ist eine Beschwerde an den VwGH nicht zulässig, weil eine solche gemäß Art 133 Z 4 B-VG nicht ausdrücklich für zulässig erklärt wurde. Beschwerden können daher ausschließlich an den VfGH gerichtet werden.[108] Bei ihren Entscheidungen hat die Kommission das AVG[109] anzuwenden.

Durch § 13 wird die Telekom-Control Kommission auch als oberste Aufsichtsbehörde für Zertifizierungsdiensteanbieter eingesetzt. Der Verzicht auf die Schaffung einer neuen Behörde wurde erwogen, weil zu erwarten ist, daß vorläufig der Aufsichtsaufwand für die oberste Behörde nicht sehr hoch ist und von der Telekom-Control Kommission mit betreut

---

[106] *Eisenberger/Zuser,* Behörden und Zuständigkeiten nach dem Telekommunikationsgesetz 1997 unter besonderer Berücksichtigung der neu geschaffenen Regulierungsbehörde, MuR (1998), S. 90.

[107] Eine kurze Selbstdarstellung der Kommission und die Aufzählung ihrer Mitglieder findet man auf den Seiten der Telekom-Control GmbH im Internet unter: http://www.tkc.at/www/tkc_main.nsf/pages/TKCHome.

[108] *Schmelz/Stratil,* Das neue Telekommunikationsgesetz, ecolex (1998), S. 267.

[109] Allgemeines Verwaltungsverfahrensgesetz 1991.

werden kann. Durch diese Organisation ist die Belastung des Budgets durch die Einführung des SigG sehr gering zu halten.

4.6.1.2. Aufgaben der Aufsichtsstelle

Im wesentlich lassen sich die Aufgaben der Aufsichtsstelle in fünf grundlegende Tätigkeitsbereiche gliedern, die § 13 Abs. 2 beispielhaft aufzählt. Da es sich um eine deklarative Aufzählung handelt, kann der Aufgabenbereich gegebenenfalls noch erweitert werden.

- Sie übernimmt die Rolle einer Wurzelzertifizierungsinstanz für Österreich und übt damit die Tätigkeit eines Zertifizierungsdiensteanbieters aus. Der Unterschied zum normalen Zertifizierungsdiensteanbieter besteht darin, daß ihre Zertifikate nicht von Signatoren gemäß § 2 Abs. 1 Z. 2 SigG verwendet werden, sondern diese Wurzel nur die anderen in Österreich tätigen Zertifizierungsdiensteanbieter zertifiziert.
- Weiters muß sie die laufende Kontrolle der Tätigkeit der Zertifizierungsdiensteanbieter durchführen, um eine gleichmäßige Qualität der Diensteanbieter und die Beibehaltung der Sicherheitsstandards zu gewährleisten. Die Bestätigungsstellen sind zwar im Rahmen ihrer technischen Gutachten weisungsfrei, die organisatorische Aufsicht ist aber von der Aufsichtsstelle zu übernehmen.
- Sie hat auch im Fall der Bereitstellung sicherer elektronischer Signaturen die Verwendung geeigneter technischer Komponenten und Verfahren nach § 18 zu überwachen.
- Schlußendlich muß ihr die Aufnahme der Tätigkeit eines Zertifizierungsdiensteanbieters gemeldet und ein Sicherheits- und Zertifizierungskonzept übermittelt werden. Im Rahmen der Aufsicht prüft sie die Einhaltung aller gesetzliche Anforderungen und führt auf Antrag eine Akkreditierung des Zertifizierungsdiensteanbieters durch.

Der letzte Punkt wurde schon im Rahmen der Abhandlung über den freien Marktzugang für Zertifizierungsdiensteanbieter weiter oben besprochen, die anderen werden im nächsten Abschnitt unmittelbar nach der Beschreibung der Telekom-Control GmbH eingehender abgehandelt, da diese große Teile der Durchführung der Aufgaben übernimmt.

Die Finanzierung dieser Tätigkeit erfolgt durch die Zertifizierungsdiensteanbieter. Sie müssen für konkret erbrachte Leistungen eine in der

SigVO festgelegte Gebühr leisten. Die Liste der Leistungen[110] findet sich in § 1 SigVO und deckt sich in etwa mit den Aufgaben der Aufsichtsstelle, die in unmittelbarem Zusammenhang mit der Überprüfung der Zertifizierungsdiensteanbieter stehen. Die Gebühren werden von der Aufsichtsstelle gemäß § 1 Abs. 3 SigVO mit Bescheid vorgeschrieben. Die Leistungen sind zeitlich determiniert, die Gebühr wird nach Stundensätzen bemessen, die Festlegung der Höhe der Stundensätze ist am Grundsatz der Kostendeckung fixiert. Wird eine Bestätigungsstelle oder die Telekom-Control GmbH herangezogen, so sind deren Kosten ebenfalls den Gesamtkosten für das Aufsichtsverfahren zu zuschlagen.

4.6.1.3. Beleihung der Telekom-Control GmbH

Da die Telekom-Control Kommission nur ein dreiköpfiges Gremium ist, das alle zwei Wochen zu Sitzungen zusammentritt, werden von ihr ausschließlich die Entscheidungen getroffen. Zur laufenden Aufsicht, dem operativen Tagesgeschäft und zum Betrieb der Wurzel kann die Telekom-Control Kommission die Telekom-Control GmbH heranziehen.

Die Telekom-Control GmbH[111] ist die in Privatrechtsform errichtete, aus der allgemeinen Behördenorganisation des Staates ausgegliederte Gesellschaft, die mit allen übrigen Regulierungsaufgaben betraut wurde. Diese Form wurde gewählt, um der Behörde eine ausreichende personelle Ausgestaltung und ein Maximum an Flexibilität zu sichern. Die GmbH ist nicht gewinnorientiert. Sie steht in 100-prozentigem Eigentum des Bundes, ihr Sitz ist gemäß § 108 TKG Wien.

Auch hier folgt das SigG dem Modell des TKG. Zur Entlastung der Kommission bestimmt § 15, daß die Telekom-Control GmbH die laufende Aufsicht über die Diensteanbieter zu kontrollieren hat, die Aufgabe der österreichischen Wurzel übernimmt und die organisatorische, laufende Aufsicht über die Zertifizierungsdiensteanbieter führt. Sprachlich verwendet das SigG weiterhin nur für die Telekom-Control Kommission den Begriff Aufsichtsstelle. Die Telekom-Control GmbH wird für die Kommission tätig und ist nur Beliehener der Kommission und nicht die Aufsichtsstelle selbst. Die Telekom-Control GmbH ist an die Weisungen der

---

[110] Wurde zuerst gedacht für die Tätigkeit der Mitarbeiter Gebühren in der Form von Stundensätzen für die aufgewendete Arbeit zu verlangen, wird nun die Gebühr abstrakt, je nach Tätigkeit berechnet. Man erwartet sich von dieser Art der Berechnung mehr Objektivität.

[111] Im Internet ist die Telekom-Control GmbH unter http://www.tkc.at/ vertreten.

Kommission gebunden und wird jeweils auf Anordnung der Kommission tätig.

4.6.1.4. Aufgaben der Telekom-Control GmbH

Die Generalklausel in § 15 Abs. 1 ermächtigt die Aufsichtsstelle, die Telekom-Control GmbH für jede Tätigkeit im Rahmen der Aufsicht heranzuziehen. Insbesondere handelt es sich um vorbereitende und unterstützende Tätigkeit für die Aufsichtsstelle. Konkretisiert wird die Ermächtigung durch § 15 Abs.3, der Unterstützung durch die Telekom-Control GmbH in organisatorischer Hinsicht und im operativen Bereich anordnet. Ist für die Telekom-Control GmbH Unterstützung in technischer Hinsicht erforderlich, so kann sie ebenfalls eine Bestätigungsstelle hinzuziehen. Als beliehenes Unternehmen, das hoheitlich tätig wird, unterliegt sie der Amtsverschwiegenheit nach Art. 20 B-VG. Diese gilt für ihr Personal und auch die sonst für sie tätigen Personen.

Auch im judiziellen Bereich übernimmt die Telekom-Control GmbH eine Aufgabe. Sie kann als Streitschlichtungsstelle von Kunden eines Zertifizierungsdiensteanbieters oder von Interessenvertretern angerufen werden[112], wenn dieser glaubt, im Betrieb eines Zertifizierungsdiensteanbieters liegen Mängel vor. Die Zertifizierungsdiensteanbieter trifft eine Mitwirkungspflicht und Auskunftspflicht in diesem Verfahren. Durch diese Tätigkeit wird versucht die Streitbeilegung durch einvernehmliche Lösung herbeizuführen. Gelingt dies nicht bleibt den Parteien die Anrufung der ordentlichen Gerichte unbeschadet.

§ 15 beschreibt die Aufgaben der Telekom-Control GmbH beispielhaft. Die Telekom-Control GmbH hat insbesondere

- die Aufsichtsstelle bei der laufenden Aufsicht der Zertifizierungsdiensteanbieter zu unterstützen und die technischen Produkte, Verfahren und sonstigen Mittel, die im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste eingesetzt werden, sowie die Qualifikation des Personals zu überprüfen.
- Hier handelt es sich um regelmäßige Überprüfungen vor Ort und Überprüfungen im Anlaßfall, sollte sie von Mängeln oder Mißständen Kenntnis erlangen. Die Erläuterungen[113] bezeichnen die Tätigkeit als „Tagesgeschäft" der Durchführung der Aufsicht. Die Kontrollen ha-

[112] Damit wird dem Trend gefolgt, daß immer mehr Streitigkeiten im Bereich des Informationstechnologierechtes außergerichtlich gelöst werden.
[113] EBRV zu § 15 Rz. 2.

ben gemäß § 18 SigVO zumindest alle zwei Jahre stattzufinden. Gesonderte Kontrollen sind auch bei sicherheitsrelevanten Veränderungen des Sicherheits- und Zertifizierungskonzeptes durchzuführen. Bei den Kontrollen sind insbesondere die technischen Mittel zu prüfen, ob sie noch immer allen Anforderungen genügen. Auch die Zuverlässigkeit und Fachkenntnis des Personals sind laufend zu kontrollieren.

- Eine weitere Aufgabe ist es, im Fall des begründeten Verdachts, daß die Sicherheitsanforderungen dieses Bundesgesetzes oder der auf seiner Grundlage ergangenen Verordnungen nicht eingehalten werden, oder auf Verlangen eines Zertifizierungsdiensteanbieters unmittelbar die vorläufige Untersagung der Tätigkeit des Zertifizierungsdiensteanbieters oder vorläufig Maßnahmen im Sinne des § 14 Abs. 1 anzuordnen.
- Ergänzend zu den regelmäßigen Prüfungen, die die Telekom-Control GmbH standardmäßig durchführt, muß auch bei Gefahr im Verzug sofort gehandelt werden können. § 15 Abs. 1 Z. 7 gibt der Telekom-Control GmbH dafür die Legitimierung. In diesem Fall ist eine Weisung der Telekom-Control Kommission nicht Voraussetzung für ein Eingreifen der ausführenden Stelle. Maßnahmen wie Untersagung ungeeigneter technischer Komponenten, Sperre von Zertifikaten oder ein gänzliches Verbot der Tätigkeit sind unverzüglich anzuordnen, wenn etwa die Kompromittierung des Signaturschlüssel eines Zertifizierungsdiensteanbieters eingetreten sind. Diese Handlungen entfalten aber nur vorläufig Wirkung und bedürfen einer nachträglichen Entscheidung der Kommission zur endgültigen Wirkung. Wurden Maßnahmen nach Auffassung der Kommission zu Unrecht angeordnet, so kann sie diese auch wieder rückgängig machen. Auch die Sperrung von Zertifikaten kann ausnahmsweise in diesem Fall rückwirkend aufgehoben werden. Da unter solchen Umständen wohl keine Zeit bleibt, Bescheide auszustellen, kann man diese Hoheitsakte am ehesten den Akten unmittelbarer Befehls- und Zwangsgewalt zuordnen.
- Die folgenden drei Bestimmungen betreffen alle die Aufgabe der Telekom-Control GmbH, die Führung der Wurzelzertifizierungsinstanz zu übernehmen. Sie werden daher zusammengefaßt und die Erläuterungen am Schluß für alle drei Bestimmungen gemeinsam aufgeführt. Die GmbH hat die Aufgaben:
  - die Zertifizierungsdiensteanbieter nach der Anzeige der Aufnahme ihrer Tätigkeit zu registrieren,

- Verzeichnisse der Zertifikate für Zertifizierungsdiensteanbieter und der Zertifizierungsdiensteanbieter (§ 13 Abs. 3) sowie ein Verzeichnis der akkreditierten Zertifizierungsdiensteanbieter (§ 17 Abs. 1) zu führen,
- für den Fall der Einstellung oder Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters einen Widerrufsdienst zu führen, sofern keine Übernahme im Sinne der §§ 12 oder 14 Abs. 5 erfolgt.

Das Betreiben der österreichischen Wurzel erfordert die Einhaltung höchster Sicherheitsansprüche, da von dieser zentralen Stelle die Sicherheit und damit Vertrauenswürdigkeit aller Zertifizierungsdiensteanbieter in Österreich und aller von ihnen ausgestellten Zertifikate abhängt. Ihr kommt für die Akzeptanz elektronischer Signaturen durch die Anwender eine zentrale Bedeutung zu. Die von ihr ausgestellten Zertifizierungsdienste für Zertifizierungsdiensteanbieter basieren gemäß § 5 SigVO auf der Grundlage qualifizierter Zertifikate und sicherer elektronischer Signaturen. Auf Grund der Wichtigkeit der Wurzelzertifizierungsinstanz werden aber in den §§ 3-5 SigVO noch zusätzliche Sicherungsmaßnahmen für deren Betrieb festgelegt. Sie sind in Verordnungsform erlassen und nicht direkt in das SigG aufgenommen worden, damit die rechtlichen Bestimmungen schneller und kontinuierlich an Änderungen im technischen Bereich angepaßt werden können. So sind die Verfahren für die Erstellung des Hashwerts und der Verschlüsselung mit SHA-1 und RSA determiniert. Die Mindestschlüssellänge weicht allerdings nicht von der allgemein für sichere elektronische Signaturen festgelegten ab. Daher muß auch die Aufsichtsstelle nur mindestens Schlüssel mit 1023 Bit Schlüssellänge gemäß Anhang 2 SigVO verwenden. Das Erzeugungssystem für die Signaturerstellungsdaten muß isoliert, ausschließlich für diesen Zweck bestimmt und auf angemessene Weise vor Eingriffen und Störungen gesichert sein.

Auch für den unwahrscheinlichen Fall der Kompromittierung ist durch ein Notfallskonzept Vorsorge getroffen. Bei Verwendung eines einzigen Schlüsselpaares zum Signieren der Zertifikate der untergeordneten Zertifizierungsdiensteanbieter würde die Sicherheit jedes einzelnen in Österreich ausgestellten Zertifikates von der Integrität dieses Schlüsselpaares abhängen. Deshalb sieht § 3 Abs. 1 SigVO ein Sicherheitssystem vor. Die Aufsichtsstelle hat zu ihren Signaturerstellungsdaten ein Zweitsystem an Signaturer-

stellungsdaten zu generieren und alle eigenen Signaturen auch mit diesem Zweitschlüssel als Backup zu signieren. Der öffentliche Zweitschlüssel wird mit den Hauptsignaturerstellungsdaten signiert. Das Zweitsystem ist unter Verschluß zu halten, also auch der öffentliche Schlüssel erst im eingetretenen Notfall zu veröffentlichen. Falls die Hauptschlüssel der Aufsichtsstelle kompromittiert werden, kann der Betrieb mit dem zweiten Schlüsselpaar aufrecht erhalten werden. Als oberste Instanz stellt sich die Aufsichtsstelle ihr eigenes Zertifikat aus. Dieses ist auch im Amtsblatt der Wiener Zeitung zu veröffentlichen.

Die Anordnung, im Falle der Einstellung oder Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters dessen Widerrufsdienste zu führen, sichert die Kontinuität der Verfügbarkeit dieser unerläßlichen Information. In diesem Fall verwaltet die Wurzelzertifizierungsinstanz nicht die Zertifikate anderer Zertifizierungsdiensteanbieter, sondern unmittelbar die der einzelnen Anwender.

- Außerdem obliegt es der GmbH, auf Anordnung der Aufsichtsstelle die Erfüllung der Voraussetzungen einer freiwilligen Akkreditierung (§ 17) zu erheben und
- bei der Feststellung der Gleichwertigkeit von Prüfberichten aus Drittstaaten im Sinne des § 24 Abs. 3 mitzuwirken.

4.6.1.5. Durchführung der Aufsicht

Zur Durchsetzung dieser Aufsichtsbefugnisse sind den Zertifizierungsdiensteanbietern gewisse Kooperationspflichten vorgeschrieben, da ohne ihr Mitwirken die meistens Aufsichtsmaßnahmen nicht durchgeführt werden könnten. Den Kontrollorganen müssen bestimmte Eingriffsbefugnisse eingeräumt werden.

§ 16 regelt die Mitwirkungspflicht der Zertifizierungsdiensteanbieter bei den Kontrollen und unterstützt dadurch die Telekom-Control GmbH bei der faktischen Durchführung der Aufsicht. Die Mitarbeiter, die die Kontrollen durchführen, haben das Recht, während der Geschäftszeiten die Büro- und Betriebsräume der Zertifizierungsdiensteanbieter zu betreten, und dürfen in die Geschäftsunterlagen einsehen.

§ 16 Abs. 3 sichert die Stellung der Zertifizierungsdiensteanbieter in diesem Verfahren gegenüber unbotmäßigem Verhalten der Aufsichtsorgane. Bei der Durchführung der Aufsicht ist die Einhaltung der Sicherheit des Zertifizierungsgebietes oberste Maxime, so darf natürlich keinesfalls

der private Schlüssel eines Zertifizierungsdiensteanbieters durch die Aufsichtsorgane eruiert werden. Auch ist bei allen Akten der Verhältnismäßigkeitsgrundsatz zu beachten, so daß die gelindesten zum Erfolg führenden Mittel eingesetzt werden müssen. Auskunfts- und Mitwirkungspflichten, die durch andere gesetzliche Bestimmungen statuiert werden, sind von den Regelungen des SigG unberührt. Auch nach anderen Gesetzen bestehende Verschwiegenheitspflichten und Auskunftsverweigerungsrechte bleiben gegenüber den für die Aufsichtsstelle handelnden Kontrollorganen weiterhin aufrecht.

4.6.2. Bestätigungsstelle

Die Bestätigungsstelle gemäß § 19 hat vor allem die Einhaltung der vorgeschriebenen Sicherheitsanforderungen durch Signaturprodukte und Verfahren zu beurteilen und durch ihre Expertise die Sicherheit festzustellen.[114] Die Erläuterungen zum SigG sehen insbesondere bei der Verwendung von Chipkartentechnologie oder Technologie für Sicherheitsmodule die Bereitstellung von technischen Prüfergebnissen durch die Bestätigungsstellen vor. Ihre Hauptaufgabe ist die Unterstützung der Aufsichtsstelle durch Einbringung ihres technischen Know How. Das Institut der Bestätigungsstelle wird durch Art. 3 Abs. 4 SigRL eingeführt, der vorsieht, daß eine geeignete öffentliche oder private Überwachungsstelle die Übereinstimmung der verwendeten sicheren Signaturerstellungseinheiten mit den Anforderungen des Anhangs III an sichere Signaturerstellungseinheiten der SigRL überprüft. Sie hat sich dabei an den von der Europäischen Kommission im Komitologieverfahren noch zu erlassenden Kriterien und den technischen Normierungen der SigVO zu richten. Das SigG erweitert den Prüfbereich der Bestätigungsstellen auf die Überprüfung aller bei den Zertifizierungsdiensteanbietern verwendeten Systeme, Produkte und Verfahren (§§ 7 Abs. 2 iVm 18 Abs. 5), und beauftragt die Bestätigungsstellen mit der Beratung der Aufsichtsstelle und der Telekom-Control GmbH bei ihrer Tätigkeit (§§ 13 Abs. 5 und 15 Abs. 3). Durch die Änderung des jeweiligen Standes der Technik kommt der laufenden Technologiebeobachtung durch die Bestätigungsstelle eine wichtige Bedeutung zu.

---

[114] Die Wichtigkeit dieser Kontrolle zeigen *Fox* und *Dobbertin* in Untersuchungen über die Fälschbarkeit durch die Anwendung verschiedener Algorithmen: *Fox*, Fälschungssicherheit digitaler Signaturen, eine Übersicht, DuD 2 (1997), S. 69. *Dobbertin*, Digitale Fingerabdrücke, Sichere Hashfunktionen für digitale Signaturen, DuD 2 (1997), S. 82.

Im Gegensatz zur Aufsichtsstelle wird die Bestätigungsstelle nicht hoheitlich tätig. Ihre Aufgaben sind rein zivilrechtlicher Natur. Ihre Äußerungen zu einem konkreten Sachverhalt sind als Gutachten beziehungsweise Stellungnahmen gegenüber dem Auftraggeber zu werten. Auch im Falle des Anforderns von Gutachten unabhängiger Prüfinstitute durch die Bestätigungsstelle ist das Rechtsverhältnis rein zivilrechtlicher Natur. Daher erfolgt auch die Vorschreibung des Entgelts nicht als Bescheid und ist auch der Höhe nach nicht, wie noch in der Regierungsvorlage zum SigG vorgesehen, gesetzlich geregelt. Wird die Bestätigungsstelle allerdings in Vollziehung des SigG tätig, handelt sie als Beliehener. In diesem Fall kommt ihr Beamtenstatus zu, und ihr Personal unterliegt der Amtsverschwiegenheit. Aus Gründen der Unvereinbarkeit ist es Institutionen, die als Bestätigungsstelle tätig werden, auch nicht erlaubt, Zertifizierungsdienste zu betreiben.

Es werden keine bestimmten Einrichtungen durch das SigG für geeignet erklärt, sondern Anforderungen an Organisationen, die diese Tätigkeit übernehmen wollen, genannt, und es wird normiert, daß nur solcherart geeignete Stellen als Bestätigungsstellen einzusetzen sind. § 19 Abs.2 fordert die Zuverlässigkeit der Institution und des von ihr beschäftigten Personals mit den für diese Aufgaben erforderlichen Fachkenntnissen, qualifizierte technische Ausstattung und Unabhängigkeit, Unbefangenheit und Unparteilichkeit.

Verfassungsrechtliches Neuland wird bei der rechtstechnischen Umsetzung der Einsetzung neuer Bestätigungsstellen betreten. Sie erfolgt auf Antrag in einer Verordnung. Da die Verordnung als generell abstrakte Norm charakterisiert ist, sind auch die Rechtsschutzmöglichkeiten des einzelnen nicht so stark ausgeprägt wie zur Bekämpfung individuell konkreter Normen. Die Zulassung oder Ablehnung eines bestimmten Vereines oder einer ähnlichen Institution ist aber durch individuell konkrete Merkmale gekennzeichnet, so daß eher die Anwendung des Bescheides, der in der österreichischen Rechtsordnung für individuell konkrete Hoheitsakte der Verwaltung vorgesehen ist, angemessener erscheint als die Regelung im Verordnungsweg, da janusköpfige Verwaltungsakte nach herrschender Lehre abzulehnen sind.[115]

Als erste Bestätigungsstelle sehen die Erläuterungen zum SigG den Verein „Zentrum für sichere Informationstechnologie (ASIT)" vor, dessen

---

[115] *Antoniolli-Koja*, Allgemeines Verwaltungsrecht[3], *Adamovich/Funk*, Verwaltungsrecht.

Statuten[116] im Mai 1999 ausgefertigt wurden. Der nicht auf Gewinn ausgelegte Verein bezweckt gemäß Art. 2 seiner Statuten die kompetente Zusammenführung und Weiterentwicklung fachlicher Inhalte aus dem Bereich der technischen Informationssicherheit mit dem Ziel der umfassenden Unterstützung seiner Mitglieder, des Gesetzgebers, der Behörden und der Sozialpartner. Er wird sich auf folgende Agenden konzentrieren: Evaluierung sicherer Infrastrukturen, Ansprech- und Koordinationsstelle für Belange der Sicherheit in der Informationstechnik, öffentliche Bewußtseinsbildung betreffend die Verwendung sicherer Informationstechnik, Technologiebeobachtung und die technische Hilfestellung für öffentliche Einrichtungen und Betreiber von Informationsdiensten.

Diesem Verein soll aber keineswegs Monopolstellung zukommen. Einrichtungen, die die im Entwurf genannten Anforderungen erfüllen, werden auf deren Antrag durch Verordnung als Bestätigungsstelle zugelassen, wenn sie die gesetzlichen Kriterien erfüllen. Bis zum Herbst 1999 gibt es allerdings noch keinen Antrag eines zweiten Vereins auf die Zulassung als Bestätigungsstelle.

4.6.3. Aufsichtsmaßnahmen

Bei Mängeln im Betrieb eines Zertifizierungsdiensteanbieters, der daher die für seine Tätigkeit nach dem SigG notwendigen Voraussetzungen nicht mehr zu erfüllen imstande ist, kann die Aufsichtsstelle Maßnahmen ergreifen, damit diese beseitigt werden oder zumindest der mangelhafte Betrieb eingestellt wird. Aufsichtsmaßnahmen können gegenüber allen Zertifizierungsdiensteanbietern ergriffen werden, auch gegen solche, die nur einfache Signaturen ohne (qualifizierte) Zertifikate anbieten.

In § 14 findet sich eine demonstrative Aufzählung der Maßnahmen, die die Aufsichtsstelle ergreifen kann, um Mißstände im Bereich der Public Key Infrastructure zu verhindern. In der Normierung der verschiedenen Sanktionen, die die Einhaltung unterschiedlicher Standards für die Kategorien der angebotenen Dienste vorschreibt, spiegelt sich auch wieder sehr deutlich das abgestufte System verschiedener Qualitätsklassen elektronischer Signaturen wider, von dem das SigG geprägt ist.

So kann es für den Zertifizierungsdiensteanbieter zum Verbot der Verwendung ungeeigneter technischer Komponenten kommen. Den Anforderungen des Gesetzes widersprechende Zertifikate von Anwendern, aber auch von Zertifizierungsdiensteanbietern können aufgehoben wer-

---

[116] Die Statuten sind in: *Brenn*, Signaturgesetz, S. 167ff, abgedruckt.

den, falls der Zertifizierungsdiensteanbieter nicht den generell im SigG und SigVO für alle Zertifizierungsdiensteanbieter angeordneten und im § 14 Abs. 2 noch einmal spezifizierten Anforderungen[117] entspricht. Für die Anbieter qualifizierter Zertifikate werden die Anforderungen durch § 14 Abs. 3 auf die Einhaltung aller Bestimmungen des SigG und SigVO ausgedehnt. Insbesondere ergibt sich daraus die Einhaltung der Anforderungen der §§ 5 und 7.

Auch für die Bereitstellung sicherer elektronischer Signaturen verpflichtet § 14 Abs. 4 die jeweiligen Anbieter darüber hinaus zur Einhaltung der Sicherheitserfordernisse bezüglich der verwendeten technischen Komponenten, womit die Anforderungen des § 18 besonders geschützt werden.

Die ultima ratio der Anordnung, die die Einstellung der Tätigkeit eines Zertifizierungsdiensteanbieters betrifft, wird allerdings durch die Einführung des Prinzips der Verhältnismäßigkeit der Maßnahmen zu den Mißständen begleitet. So sind von der Aufsichtsbehörde jedenfalls gelindere Mittel als Maßnahmen zu verordnen, wenn diese zur Beseitigung der Mißstände ausreichen.

4.7. Haftung der Zertifizierungsdiensteanbieter

Im Zuge der Entstehung der SigRL und des SigG war die Frage höchst umstritten, wie die Haftungsregeln der Zertifizierungsdiensteanbieter hinsichtlich Schäden, die durch mangelhafte Zertifikate kausal begründet werden, ausgestaltet werden sollen.[118] Eine Haftung der Zertifizierungsdiensteanbieter käme bei Fällen in Betracht, in denen die haftungsbegründenden Ereignisse aus deren eigenem Einflußbereich stammen, wie technische Defekte, betrügerische Manipulation oder fahrlässiges Fehlverhalten von Mitarbeitern. Da elektronische Signaturen und deren Zertifikate maßgeblich die Sicherheit der Telekooperation gewährleisten, sind fehlerhafte Zertifikate daher ein Rückabwicklungsgrund für alle dadurch irrtümlich abgeschlossenen Rechtsgeschäfte. Inwieweit Zertifizierungsdiensteanbieter auch verschuldensunabhängig haften sollen, ist deshalb besonders für Dritte von großer Bedeutung, insbesonders wenn sie auf den ursprünglichen Vertragspartner nicht mehr zurückgreifen können. Im

---

[117] Dazu zählen: Zuverlässigkeit, Fachkunde, ausreichende Finanzmittel, ordnungsgemäß geführte Verzeichnis- und Wiederrufsdienste.

[118] Besonders Deutschland vertrat den Standpunkt, daß die Haftung nach den allgemeinen Regeln des Schadenersatzrechtes auch im Bereich der Zertifizierungsdiensteanbieter durchaus ausreiche.

Rahmen des allgemeinen Schadenersatzes nach ABGB wäre es höchst schwierig für einen Dritten, auf den Diensteanbieter zurückzugreifen. Spezielle Tatbestände, die in gewissen Grenzen eine Gefährdungshaftung für Diensteanbieter vorsehen, werden daher besonders von Konsumentenschutzvereinen eingefordert, und man begrüßt die durch den Richtlinienvorschlag der Kommission initiierte neue Entwicklung sehr.

Im Bereich der Normen über elektronische Signaturen finden sich zwei unterschiedliche Regelungsmodelle. In den Regelungen der SigRL[119] ist für gewisse Tatbestände eine Gefährdungshaftung der Zertifizierungsdiensteanbieter gegenüber jedermann vorgesehen, im Gegensatz dazu versteht der deutsche, schweizerische[120] und italienische Gesetzgeber sein Signaturgesetz im wesentlichen als Technologiegesetz, das nur die Infrastruktur der Zertifizierungsstellen regelt. Über die Rechtswirkung digitaler Signaturen im allgemeinen und Haftungsregeln für falsch ausgestellte Zertifikate im besonderen sind keine speziellen Regelungen vorgesehen. Der deutsche Gesetzgeber beläßt die Subsumption haftungsrechtlicher Sachverhalte unter das allgemeine Schadenersatzrecht. Der Gesetzgeber in Österreich hat sich für einen Mittelweg entschieden und normiert in § 23 für gewisse Inhalte qualifizierter Zertifikate eine Verschuldenshaftung mit Umkehr der Beweislast und einer eingeschränkten Verursachungsvermutung zu Lasten des Zertifizierungsdiensteanbieters.

Im folgenden soll in diesem Kapitel zuerst die Haftung von Zertifizierungsdiensteanbietern nach der Rechtslage vor dem SigG betrachtet werden, um die Probleme der Anwendbarkeit des allgemeinen Haftungsrechtes aufzuzeigen, die spezielle Haftungstatbestände für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, nötig gemacht haben. Weiters sind die Regelungen des allgemeinen Haftungsrechts auch für die Haftung für alle anderen als qualifizierte Zertifikate weiterhin alleine anwendbar, da die Geltung der besonderen Haftungsregelung im SigG auf qualifizierte Zertifikate beschränkt ist. Im Anschluß soll die neue Rechtslage, die durch das SigG eingeführt wurde untersucht werden. Als Abschluß werden die Haftungsregelungen im Vorschlag der Kommission besprochen.

---

[119] Art. 6 SigRL.

[120] Art. 20 des Entwurfs für eine Verordnung über eine Public Key Infrastruktur in der Schweiz, bestimmt, daß sich die Haftung der anerkannten Anbieter von Zertifizierungsdiensten nach dem allgemeinen Schweizer Obligationenrecht bestimmt.

4.7.1. Haftung gemäß allgemeiner Haftungsnormen

Der deutsche Gesetzgeber entschied sich nach langer Diskussion, auf besondere Haftungsregeln zu verzichten und dadurch dem Vorschlag der Bundesregierung zu folgen: „Mögliche Haftungsfragen sind aus den jeweiligen Verantwortlichkeiten und dem allgemeinen Haftungsrecht zu beantworten (jeder haftet für sein schuldhaftes Handeln oder Unterlassen)".[121] Der Bundesrat sah in den fehlenden Haftungsregeln und Bestimmungen über eine Pflichtversicherung der Zertifizierungsstellen einen schweren Mangel der Norm und wollte unter anderem aus diesem Grund das Signaturgesetz zu diesem Zeitpunkt überhaupt noch nicht beschlossen sehen.[122] Auf Grund der Notwendigkeit der Regelungen[123] wurde es aber am 13. Juni 1997 ohne besondere Haftungsregeln vom Bundestag beschlossen.

Auch in Österreich gibt es nur besondere Haftungsregelung für gewisse Inhalte qualifizierter Zertifikate im Bereich der elektronischer Signaturen, ansonst ordnet das SigG die Anwendbarkeit von Bestimmungen des ABGB und anderer Rechtsvorschriften, nach denen Schäden in anderem Umfang oder von anderen Personen als nach dem SigG zu ersetzen sind, durch § 23 Abs. 6 explizit an. Treten daher Schadenssituationen ein, die nicht unter die Haftungstatbestände des § 23 subsumierbar sind, müssen auch im österreichischen Rechtsbereich die allgemeinen Schadenersatzregelungen herangezogen werden. Je nachdem, ob der Schaden beim Zertifizierten oder bei einem Dritten eintritt, der mit dem Zertifizierten im Vertragsverhältnis steht, nicht aber mit dem Zertifizierungsdiensteanbieter, kann man verschiedene Fallgruppen bilden, denen zwar allen gemeinsam ist, daß der Schaden auf Grund von Manipulation oder Fehlern bei Ausgabe oder Verwaltung der Zertifikate entstanden ist, die essentielle Regelung der Beweislastverteilung aber zu sehr unterschiedlichen Ergebnissen führt.

---

[121] Begründung zum Gesetzesentwurf der Bundesregierung IuKDG, BR-Drucksache 966/96, S. 28.

[122] Stellungnahme des Bundesrates zum Gesetzesentwurf der Bundesregierung IuKDG, BR-Drucksache 966/96, S. 19 und S. 21.

[123] *Roßnagel*, Das Signaturgesetz jetzt verbessern und verabschieden, DuD (1997), S. 287. *Grimm*, Wir brauchen das digitale Signaturgesetz, DuD (1997), S. 286.

4.7.1.1. Vertragshaftung zwischen Zertifizierungsdiensteanbieter und Anwender

Zwischen dem Inhaber eines Zertifikates und dem Zertifizierungsdiensteanbieter besteht ein Vertragsverhältnis, auf Grund dessen der Zertifizierungsdiensteanbieter die Ausstellung und Verwaltung des Zertifikates und oft auch die Generierung und Verwaltung des dazugehörigen Schlüsselpaares schuldet, der Inhaber des Zertifikates hingegen ein Entgelt. Es handelt sich um einen Vertrag sui generis mit hauptsächlich dienst- und werkvertraglichen Elementen[124].

Aus diesem Schuldverhältnis ergeben sich auch Schutz- und Fürsorgepflichten gegenüber dem Vertragspartner. Beim Zertifizierungsvertrag zählen folgende Leistungen zu Haupt-, Schutz- und Fürsorgepflichten:

- ordnungsgemäße Schlüsselzuordnung
- ordnungsgemäße Schlüsselverwaltung
- Ausstellung eines gültigen Signaturschlüsselzertifikats
- korrekte Wiedergabe der Daten des Signators im Zertifikat
- Einrichtung und Aufrechterhaltung ausreichender Sicherheitsvorkehrungen
- richtige Auskunftserteilung bei Signaturschlüssel- und Zertifikatsabfrage
- Richtigkeit des Zeitstempeldienstes
- unverzüglicher Widerruf bei Vorliegen der Voraussetzungen, falls ein Widerrufdienst vertraglich vereinbart wurde[125]
- korrekte Generierung des Schlüsselpaares, falls vereinbart

Bei verschuldetem Verstoß gegenüber einer dieser Pflichten haftet der Zertifizierungsdiensteanbieter dem Inhaber des Zertifikates aus positiver Vertragsverletzung für den Schaden am Zertifikat gemäß § 1295 Abs. 1 ABGB. Die Haftung für Mangelfolgeschäden[126] ergibt sich aus den §§ 932 Abs. 1 letzter Satz iVm 1435 ABGB. Die positive Vertragsverletzung umfaßt alle Sachverhalte des schädigenden Vertragspartners, die zu einem Schaden des Gläubigers führen, der von dem Schaden verschieden ist, welcher dem Zertifikatsinhaber durch gänzliche oder teilweise Nichter-

---

[124] Ausführlicher dazu: *Timm*, Signatur und Haftungsrecht, DuD (1997), S. 525.

[125] Gemäß § 7 Abs 1 Z. 2 sind nur Diensteanbieter für qualifizierte Zertifikate zu Führung eines Widerrufsdienstes verpflichtet, Diensteanbieter gemäß § 6 müssen keine Verzeichnisdienste führen.

[126] *Rummel*, ABGB[2] § 932 Rz. 20.

bringung der Ausstellung und Verwaltung des Zertifikates entstanden wäre. Bei Verletzung der Schutzpflichten gegenüber dem Zertifikatsinhaber haftet ihm der Zertifizierungsdiensteanbieter auf Grund positiver Vertragsverletzung.

Mitarbeiter des Zertifizierungsdiensteanbieters und auch ausgegliederter Registrierungsdiensteanbieter[127] und deren Mitarbeiter, die für den Zertifizierungsdiensteanbieter tätig werden, sind als Erfüllungsgehilfen[128] gemäß § 1313a ABGB zu werten. Auch für das Fehlverhalten seiner Mitarbeiter haftet der Zertifizierungsdiensteanbieter wie für sein eigenes Verschulden. Der Inhaber eines Zertifikates kann sich an den meist wirtschaftlich stärker gestellten Betreiber des Zertifizierungsdiensteanbieters wenden, um Schadenersatz für schuldhaftes Fehlverhalten seiner Gehilfen zu fordern.

Auch die in der Praxis meist sehr erhebliche Verfahrenserleichterung für den Geschädigten, die Beweislastumkehr für das Verschulden gemäß § 1298 ABGB, kommt bei positiver Vertragsverletzung des Zertifizierungsvertrages zur Anwendung. Allerdings bezieht sich die Beweislastumkehr in diesem Fall grundsätzlich nur auf das Verschulden, der Beweis der Kausalität obliegt weiter dem Gläubiger[129]. In einem anderen Urteil[130] bezüglich Schadenersatzes bei ärztlichen Behandlungsfehlern wird vom OGH die Beweislastumkehr auch auf die Kausalität ausgedehnt, „weil hier wegen der in diesen Fällen besonders vorhandenen Beweisschwierigkeiten des Patienten, die Kausalität nachzuweisen, nur dem zur Haftung herangezogenen Arzt die Mittel und Sachkunde zum Nachweis zur Verfügung stehen, daher von einer „prima-facie-Kausalität" auszugehen ist". Eine weitere analoge Ausdehnung auch auf komplexe Computeranlagen und Programme, bei denen Kunden kein Einblick in den Programmablauf gewährt wird und die deshalb aus gleichen Gründen wie Patienten bei medizinischer Behandlung die Kausalität des fehlerhaften Programms nicht nachweisen können, ist aber spätestens mit in Kraft treten des SigG zumindest für Zertifizierungsdiensteanbieter zu verneinen.

---

[127] *Schwimann*, ABGB[2] VII, § 1313a Rz. 7.

[128] Falls die Haftung des Zertifizierungsdiensteanbieters, der sich eines ausgegliederten Registrierungsdiensteanbieters bedient, bezüglich Gehilfen des Registrierungsdiensteanbieters begründet werden soll, ist die Einverständnis des Zertifizierungsdiensteanbieters zur Heranziehung weiterer Erfüllungsgehilfen notwendig. *Schwimann/Harrer*, ABGB[2] VII, § 1311a RZ. 9. Zur Erfüllungsgehilfenkette auch: SZ 66/69.

[129] OGH in NZ 1987, 42, JBl 1993, 316.

[130] OGH in SZ 63/90, JBl 1992, 522.

Aus dem Bericht des Justizausschusses[131] zur RV SigG geht eindeutig hervor, daß die Verursachungsvermutung nicht zu einer Beweislastumkehr führen soll. Da § 23 Abs. 3 nur für qualifizierte Zertifikate gilt, können nicht für Zertifizierungsdiensteanbieter, die einfache Zertifikate ausstellen und nur nach allgemeinem Schadenersatzrecht haften, strengere Beweislastregeln gelten.

Bei leichter Fahrlässigkeit seitens der Zertifizierungsdiensteanbieters ist nach § 1324 ABGB nur der positive Schaden im Rahmen des § 1323 ABGB zu ersetzen. Handelt der Zertifizierungsdiensteanbieter grob fahrlässig oder vorsätzlich oder geht es um ein Handelsgeschäft im Sinne von Art. 8/2 der 4. EVHGB, ist immer volle Genugtuung zu leisten. Zusätzlich zum positiven Schaden muß auch der entgangene Gewinn ersetzt werden. Die Beweislast für das Vorliegen grober Fahrlässigkeit im Anlaßfall obliegt dem Geschädigten.[132]

Die Haftung des Zertifizierungsdiensteanbieters gegenüber ihrem Vertragspartner bewegt sich also bei Heranziehung des geltenden allgemeinen Schadenersatzrechts sehr wohl auf hohem Niveau. Die Inhaber der Schlüssel können ihre Schadenersatzansprüche ausreichend geltend machen und durchsetzen. Im Gegensatz zu haftungsrechtlichen Ansprüchen zwischen Zertifizierungsdiensteanbietern und Dritten, die gleich anschließend behandelt werden, ist hier keine Normierung besonderer Gefährdungshaftungstatbestände oder die analoge Heranziehung bestehender Tatbestände nötig.

4.7.1.2. Haftung des Zertifikatsinhabers gegenüber seinen Vertragspartnern

Die einfachste Möglichkeit für einen Dritten[133] bestände darin, einen Haftungsanspruch gegenüber seinem Vertragspartner, dem Inhaber des fehlerhaften Zertifikates, durchzusetzen. Alle Benefizien, die die Rechtsordnung bei vertraglichem Schadenersatz und der Culpa in Contrahendo gewährt, werden damit auch dem Dritten, als Vertragspartner des Zertifikatsinhabers, zugänglich.

Voraussetzung hierfür ist allerdings ein Verschulden des Zertifikatsinhabers, zumindest leicht fahrlässiges Handeln muß vorliegen. In vielen Fällen wird der Zertifikatsinhaber aber nicht schuldhaft handeln,

---

[131] 2065 der Beilagen zu den Stenographischen Protokollen des NR der XX. GP, S. 4.

[132] stRsp: JBl 1977, 648, 1982, 211, 219, Arb 9862, JBl 1986, 587f.

[133] Gemeint ist ein Vertragspartner des Zertifizierten, der Dritter in Bezug auf den Vertrag zwischen Zertifizierungsdiensteanbieter und Zertifiziertem ist.

sondern das Verschulden beim Zertifizierungsdiensteanbieter liegen. Man könnte zum Beispiel an die Fallgruppe denken, daß der Zertifikatsinhaber einen Fehler seines Zertifikates bemerkt, sofort eine Sperrmeldung zum Diensteanbieter schickt, dort aber die Sperrung fahrlässig nicht durchgeführt wird. Unter diesen Umständen könnte der Dritte keinen Anspruch gegenüber dem Zertifikatsinhaber durchsetzen. Gemäß § 1295 Abs. 1 ABGB haftet jeder Beschädiger nur für den Ersatz des Schadens, welchen dieser dem Geschädigten aus eigenem Verschulden zugefügt hat. Er kann in diesem wie in den meisten anderen Fällen einen Haftungsanspruch nur gegenüber dem Zertifizierungsdiensteanbieter, mit dem er nicht in Vertragsbeziehung steht, geltend machen, womit, wie im folgenden gezeigt, die Fälle der erfolgreichen Geltendmachung des Schadenersatzes für ihn stark gemindert werden.

Auch in der Fallgruppe, bei der der Zertifizierte ein gefälschtes oder unter falschen Angaben vom Zertifizierungsdiensteanbieter erschlichenes Zertifikat verwendet, ist eine in Anspruchnahme des Betrügers, der ja der Vertragspartner des geschädigten Dritten ist, nicht möglich. Gerade die Daten im Zertifikat sind die einzigen Grundlagen für eine Verfolgung des Betrügers, entsprechen eben diese auf Grund des Betruges nicht den Tatsachen, kann der Betrogene sein Recht gegenüber dem Betrüger schon alleine dadurch nicht durchsetzen, weil er ihn nicht ergreifen kann.

4.7.1.3. Haftung der Zertifizierungsdiensteanbieter gegenüber Vertragspartnern des Zertifikatsinhabers

Anders sieht die Situation bei Haftungsansprüchen Dritter, also Vertragspartnern des Zertifikatsinhabers, gegen den Zertifizierungsdiensteanbieter aus. Vertragspartner des Inhabers von Zertifikaten können durch dessen falsches Zertifikat getäuscht werden und Rechtsgeschäfte abschließen, die sie gar nicht oder nicht so gewollt hatten. Zu untersuchen ist, wie der Ersatz solcher Schäden durch Dritte gegenüber den Diensteanbietern im Rahmen des geltenden Rechts, das bis jetzt noch keinerlei spezielle Haftungstatbestände für die Betreiber von Zertifizierungsdiensten kennt, durchgesetzt werden kann. Besonders die Probleme des Haftungsdurchgriffes des Dritten auf die Betreiber des Zertifizierungsdiensteanbieters auf Grund des geltenden Rechts sollen erörtert werden.

4.7.1.3.1. Vertragshaftung

Generell wird zwischen dem Vertragspartner des Zertifizierten und dem Zertifizierungsdiensteanbieter kein Vertrag bestehen, und die beiden

befinden sich auch nicht im Stadium der Vertragsanbahnung, die für eine Haftung aus Culpa in Contrahendo ausreicht. Die Haftung des Zertifizierungsdiensteanbieters auch für Vermögensschäden läßt sich nicht nur wegen positiver Vertragsverletzung begründen, auch die Annahme einer Sachverständigenhaftung im Rahmen des § 1300 ABGB sollte geprüft werden.

Der OGH entschied[134]: „[Wenn] ein Vermögens- und Anlageberater von seiner Klientin kein Honorar begehrt, sondern Provision von deren Vertragspartnerin erhofft, steht den (vor-) vertraglichen Pflichten nichts entgegen. Daher erfolgte sein Rat nicht aus Gefälligkeit, sondern im Rahmen eines Schuldverhältnisses, also gegen Belohnung iS [des § 1300 ABGB]. Seine Schadenersatzpflicht für die Erteilung des Rates wird dann durch jedes Versehen ausgelöst, wobei der Schaden auch [den Vermögensschaden] umfaßt."

Bei analoger Anwendung dieses Judikates wäre die Haftung des Zertifikatsinhabers gegenüber seinen Vertragspartnern, die auf das Zertifikat vertraut haben, denselben Kriterien zu unterziehen wie die Haftung des Zertifizierungsdiensteanbieters gegenüber dem Inhaber des Zertifikats. Diese Situation spiegelt sich allerdings nur sehr bedingt in den Beziehungen zwischen Zertifizierungsdiensteanbietern und Vertragspartnern des Zertifikatsinhabers wider.

In diesem vom Gericht zu beurteilenden Sachverhalt erhofft sich hier der Vermögensberater eine konkrete Belohnung von einer Person, die ihm schon als zukünftiger vermutlicher Vertragspartner seiner Klientin bekannt ist. Zertifizierungsdiensteanbieter müssen zwar definitionsgemäß die von ihnen Zertifizierten „kennen", handeln aber im Normalfall nicht, weil sie sich eine „Belohnung" durch die Vertragspartner ihrer Kunden, mit denen sie im Zeitpunkt der Zertifizierung in keinem Kontakt stehen, erwarten.

Allenfalls könnten etwa Banken als eine Gruppe der Betreiber von Zertifizierungsdiensteanbietern, die eine solche nur betreiben, um dadurch Kunden als Vertragspartner für ihre Haupttätigkeit zu gewinnen, von diesem Urteil betroffen sein. Eine Erhöhung des gesamten Umsatzes und damit des Gewinns des Unternehmens durch die Betreibung eines Zertifizierungsdienstes könnte von den Gerichten als Belohnung im Sinne des § 1300 ABGB angesehen werden. Es ist aber zweifelhaft, ob die bloße Förderung der Erweiterung der Geschäftstätigkeit von Bankkunden durch Anbieten von Zertifizierungsdiensten des jeweiligen Institutes, durch die

---

[134] JBl 1985, 38.

einfacheres Handeln der Zertifizierten auch im Internet ermöglicht wird, eine erhöhte Geschäftstätigkeit im Sinne einer Belohnung konkretisiert.Weiters ließe sich diese Entscheidung nur für die Sachverhalte heranziehen, in denen der Zertifizierungsdiensteanbieter neben seiner Tätigkeit im Bereich der Zertifizierung auch andere Geschäfte betreibt, deren Umsatz durch die Verträge der Zertifizierten mit Dritten belebt wird.

4.7.1.3.2. Vertrag zugunsten Dritter

Die beiden anderen Möglichkeiten, die günstigen Regelungen der Vertragshaftung auch auf einen Vertragspartner des Zertifizierten auszudehnen, wären, den Vertrag zwischen Zertifizierungsdiensteanbieter und Zertifikatinhaber als Vertrag zugunsten Dritter oder als Vertrag mit Schutzwirkung zugunsten Dritter zu qualifizieren.

Gemäß § 881 ABGB müßte sich der Zertifikatinhaber von dem Zertifizierungsdiensteanbieter eine Leistung an einen Dritten versprechen lassen, schon zum Zeitpunkt des Vertragsabschlusses soll diesem Dritten die Leistung zu Gute kommen. Der Begünstigte muß unmittelbar aus dem Vertrag ein Forderungsrecht erwerben[135] Im Zertifizierungsvertrag kommt die Leistung des Zertifizierungsdiensteanbieters aber nur dem Zertifikatsinhaber zu Gute. Weiters sind zum Zeitpunkt dieses Vertragsabschlusses die vermeintlichen Dritten noch gar nicht konkretisiert, da sie ja zukünftige Vertragspartner des Zertifikatinhabers sind und damit noch gar nicht bekannt sein müssen.

Ein Vertrag zugunsten Dritter kann demzufolge nicht angenommen werden. Der Dritte kann keinen Schadenersatz aus diesem Titel heraus verlangen.

4.7.1.3.3. Vertrag mit Schutzwirkung zugunsten Dritter

Die Durchsetzbarkeit der vertraglichen Schutzpflichten gegenüber Dritten wird auch durch den Vertrag mit Schutzwirkung zugunsten Dritter erreicht. Hier würde die Hauptleistung, in unserem Fall also das Erstellen und Verwalten des Zertifikats und eventuell des Schlüsselpaares, dem Zertifikatsinhaber zukommen. Dritte könnten aber Schadenersatz, der aus der Nichteinhaltung der Schutzpflichten entsteht, gemäß der Vertragshaftung einfordern, da diese Pflichten wegen ihrer Schutzwürdigkeit auch auf diesen Personenkreis erweitert wurden. Die Vertragspartner des Zertifikatsinhabers hätten daher die Möglichkeit, sich unmittelbar an die Zerti-

---

[135] *Schwimann/Apathy*[2] V § 882 Rz. 4.

fizierungsdiensteanbieter zu wenden, falls diese die Einrichtung ausreichender Sicherheitsvorkehrungen unterlassen oder bei der Zertifikatsverwaltung nicht die erforderliche Zuverlässigkeit gezeigt hat.

Koziol[136] grenzt den Kreis der geschützten Personen nach folgenden Kriterien ab: Es bedarf erstens eines erhöhten Schutzbedürfnisses der Dritten, das bei jenen Personen besteht, die durch verstärkte Einwirkungsmöglichkeit in erhöhtem Maße gefährdet sind. Zweitens müssen sie der Interessensphäre des einen Partners angehören.

Bydlinski[137] umschreibt den Bereich der begünstigten Personen als „dritte, deren Kontakt mit der vertraglichen Hauptleistung beim Vertragsabschluß voraussehbar war und die der Vertragspartner entweder erkennbar durch Zuwendung der Hauptleistung begünstigte oder denen er selbst offensichtlich rechtlich zur Fürsorge verpflichtet ist."

Die Voraussehbarkeit des Kontakts mit den Dritten und auch die rechtliche Verpflichtung zur Fürsorge gegenüber zukünftigen Vertragspartnern liegt aber zum Zeitpunkt des Vertragsschlusses zwischen Zertifizierungsdiensteanbieter und Zertifikatsinhaber nicht vor. Die zukünftigen Vertragspartner des Zertifikatsinhabers genießen also nicht die gleichen Schutzwirkungen wie der Zertifikatsinhaber. Schon aus dieser Erwägung kann eine Vertragshaftung wegen Schutzwirkung zugunsten Dritter nicht begründet werden.

Es wäre auch nicht sinnvoll, aus diesem Titel zu argumentieren, da nach überwiegender Meinung aufgrund der Schutzwirkung zugunsten Dritter nur die Haftung für Leben und Sachen des Dritten begründet wird. Bloße Vermögensschäden, wie sie typischerweise durch Fehler bei der Zertifizierung entstehen, könnten daher durch dieses Rechtsinstitut, auch wenn es anwendbar wäre, nicht eingeklagt werden.

4.7.1.3.4. Produkthaftung

Die letzte Möglichkeit des Dritten, Anbieter von Zertifizierungsdiensten verschuldensunabhängig haftbar zu machen, wäre die Anwendung des Produkthaftungsgesetzes. Denkbar könnte hier besonders ein Schaden wegen eines fehlerhaften Produktes durch die Generierung ungeeigneter Schlüssel oder ein Zertifikat mit falschen Inhalten sein. Problematisch ist hier die nach dem Produkthaftungsgesetz geforderte Produkteigenschaft. Gemäß § 4 PHG sind Produkte, für die die Haftungsregeln dieses Gesetzes gelten, nur bewegliche körperliche Sachen einschließlich Ener-

---

[136] *Koziol*, Österreichisches Haftpflichtrecht II², S. 86

[137] JBl 1960, 363, ihm folgend OGH in SZ 47/72 = JBl 1974,573.

gie. Zertifikate und Schlüssel sind digitale Information und daher keine körperliche Sache. Eventuell könnte man überlegen Zertifikate als Software[138] zu kategorisieren. Hier ist es äußerst umstritten, ob Software eine Sache im Sinne des § 4 PHG ist. Die rezentesten Lösungen im Schrifttum unterscheiden zwischen Betriebssystemen und anderen massenweise erzeugten Standardanwendungen, die in den Geltungsbereich des § 4 PHG fallen und Individualprogrammen, die nicht der Produkthaftung unterliegen, da hier die geistige Leistung im Vordergrund steht. Zertifikate, die für jeden Anwender individuell erstellt werden, fallen sicher in die zweite Kategorie. Sie erfüllen deswegen nicht die Anforderungen, die das PHG für Produkte erfordert. Aus dem Produkthaftungsgesetz können somit keine Ansprüche Dritter gegen Zertifizierungsdiensteanbieter abgeleitet werden.

4.7.1.3.5. Deliktische Haftung

Da keine der oben angeführten Anspruchsgrundlagen, ausgenommen die nur unter stark eingeschränkten Bedingungen anwendbare Sachverständigenhaftung für den Dritten Vorteile bringenden Haftungsregeln, im Normalfall herangezogen werden können, muß die Haftung der Anbieter von Zertifizierungsdiensten gegenüber Dritten den Regeln der deliktischen Haftung folgen.

Im Bereich der deliktischen Haftung außerhalb vertraglicher Verpflichtungen ist die nur fahrlässige Zufügung reiner Vermögensschäden nicht rechtswidrig und macht also grundsätzlich Zertifizierungsdiensteanbieter gegenüber Dritten nicht ersatzpflichtig. Aus den allgemeinen Bestimmungen des §1295 Abs. 1 ABGB kann daher in der Regel keine Haftung der Zertifizierungstelle für Vermögensschäden gegenüber Vertragspartnern des Zertifikatsinhabers abgeleitet werden.

Zu untersuchen ist, welche der Bestimmungen des SigG sich als Schutzgesetz im Sinne des § 1311 ABGB qualifizieren. Dies trifft eindeutig für die Haftungsbestimmungen des § 23 zu, wie es in den Erläuterungen der RV[139] auch explizit aufgeführt wird. Gerade diese Bestimmung trifft jedoch nur für die Haftung für qualifizierte Zertifikate zu. Die Anwendung der Normen der deliktischen Haftung werden sich aber immer auf einfache Zertifikate beziehen, worauf § 23 als lex specialis nicht heranzuziehen ist und daher auch keine Schutzgesetzwirkung entfaltet. Inwieweit die anderen Bestimmungen des SigG dieselbe Wirkung erbrin-

---

[138] *Schwimann/Posch*, ABGB[2] VIII § 4 PHG Rz. 10.

[139] 1999 der Beilagen zu den Stenographischen Protokollen des NR der XX. GP, S. 43.

gen oder nur generell abstrakte Regelungen sind[140], wie es im dSigG der Fall ist, muß von den Gerichten noch geklärt werden.[141]

In Deutschland existiert zwar ein Gesetz über digitale Signaturen. Doch ergibt eine nähere Betrachtung, daß es nicht als Schutzgesetz zu werten ist[142], da ein Schutzgesetz nicht nur dem Schutz der Allgemeinheit dienen, sondern der Schutz des einzelnen zumindest auch bezweckt sein muß. In der Begründung zum Signaturgesetz ist das Ziel des Gesetzes definiert als Vorgabe eines administrativen Rahmen, von dem auch eine „bundesweite Infrastruktur für die Zuordnung der Signaturschlüssel zu natürlichen Personen"[143] erfaßt sein soll. Das Gesetz ist also als generell abstrakte Regelung der Verfahrensweise und der Infrastruktur zu sehen, dem die Intention des Individualschutzes fehlt. Im deutschen Recht ist die Haftung der Zertifizierungsdiensteanbieter bei fahrlässigem Verhalten gegenüber Dritten für Vermögensschäden durch eine Schutzgesetzverletzung nicht zu begründen.

Ähnlich wie der OGH in der weiter oben besprochenen Entscheidung die Vertragshaftung in einer besonderen Konstellation auch auf eigentlich Dritte ausdehnt, findet sich eine weitere Entscheidung des OGH[144], die bestimmt, daß Dritte ausnahmsweise auch bei Fahrlässigkeit für Vermögensschaden haften. Im vorliegenden Sachverhalt wurde der Geschäftsherr und Vertragspartner des Käufers während der Verkaufsverhandlung von seiner Tochter vertreten, die dabei dem Kaufgegenstand fahrlässig falsche, für den Käufer aber wichtige Eigenschaften zuschrieb. Der Käufer begehrte nicht nur vom Geschäftsherrn auf Grund der Erfüllungsgehilfenhaftung, sondern auch von dem Vertreter selbst Ersatz des Vermögensschadens.

Mit folgender Begründung gab der Gerichtshof dem Kläger statt: „Eine kumulative Verantwortlichkeit von Vertretenem und Vertreter wird ... bejaht, wenn der Vertreter ein erhebliches und unmittelbares eigenwirtschaftliches Interesse am Zustandekommen des Vertrages hatte oder bei den Vertragsverhandlungen im besonderen Maße persönliches Vertrauen in Anspruch genommen und die Verhandlung dadurch beeinflußt hat. ...

---

[140] Für eine Rechtssprechungsübersicht zu Normen, denen Schutzgesetzwirkung zukommt siehe: *Schwimann/Harrer*, ABGB[2] VII § 1311 Rz. 24.

[141] Die Regelungen über Rechte und Pflichten des Signators lassen aber eher auf eine intendierte Schutzgesetzwirkung schließen.

[142] *Timm*, Signatur und Haftungsrecht, DuD (1997), S. 525.

[143] Begründung zum Gesetzesentwurf der Bundesregierung IuKDG, BR-Drucksache 966/96, S. 28.

[144] SZ 56/135 = JBl 1984, 669.

[Es muß sich aber] um ein ausgeprägtes wirtschaftliches Interesse des Vertreters handeln, das gerade im Verhältnis zum Gegenkontrahenten bestehen müsse und daher mit einem bloßen Entgeltanspruch aus dem Innenverhältnis zum Vertretenen nicht gleichzusetzen ist."

Interessant ist hier insbesondere "das im besonderen Maße in Anspruch genommene persönliche Vertrauen" des Dritten auf die Richtigkeit der zertifizierten Daten. Die gesamte Infrastruktur des elektronischen Geschäftsverkehrs im weiteren Sinn und der Zertifizierungsinfrastruktur beruht definitionsgemäß im Vertrauen auf die Richtigkeit der Angaben im Zertifikat, für die der Zertifizierungsdiensteanbieter verantwortlich ist und keine andere auch nur annähernd ähnlich effiziente Methode zur Verfügung steht. Probleme bei der Anwendung dieser Entscheidung auf die Haftung zwischen Zertifizierungsdiensteanbieter und Dritten bereitet aber, daß bei Vertragsverhandlungen zwischen Zertifikatsinhaber und Drittem der Zertifizierungsdiensteanbieter im Normalfall nie als Vertreter auftritt. Er handelt nicht für den Zertifikatsinhaber, sondern stellt nur seine Dienste für die Prüfung der Identität des Zertifikatsinhabers im Internet zur Verfügung. Wegen des fehlenden direkten Kontaktes zwischen Zertifizierungsdiensteanbieter und Drittem bei der Verhandlung der inhaltlichen Komponente der Übereinstimmung kann dieses Judikat mE nicht auf die Haftung des Zertifizierungsdiensteanbieters bei fahrlässigem Verhalten gegenüber dem Vertragspartner des Zertifikatsinhabers auf den Vermögensschaden ausgedehnt werden.

Die Erfüllungsgehilfenhaftung nach § 1313a ABGB ist mangels Vertragsbeziehung nicht anwendbar. Es bleibt alleine die Haftung für Besorgungsgehilfen gemäß § 1315 ABGB. Der Zertifizierungsdiensteanbieter haftet für die Handlungen seiner Gehilfen nur, wenn er sich einer untüchtigen oder wissentlich gefährlichen Person bedient.

Nach derzeit geltendem österreichischem Recht haftet der Zertifizierungsdiensteanbieter für einfache Zertifikate daher nur bei vorsätzlicher Schädigung für Vermögensschäden des Dritten. Im Bereich der Gehilfenhaftung kommt nur die Regelung des §1315 ABGB zur Anwendung. Der Betreiber haftet für seine Mitarbeiter, die dem Dritten gegenüber Besorgungsgehilfen sind, solange er als Betreiber nachweisen kann, daß er bei Auswahl und Überwachung die im Verkehr übliche Sorgfalt hat walten lassen. Der Vertragspartner des Zertifikatsinhabers kann sich nur direkt an den wirtschaftlich meist weniger potenten Gehilfen wenden, um den Schaden, der durch dessen schuldhaftes Handeln verursacht wurde, ersetzt zu bekommen.

4.7.2. Haftungsregelung des SigG

Nach diesem Überblick über die für Dritte unerfreuliche Situation hat das SigG erfreulicherweise die von der SigRL erstmals vorgesehenen Tatbestände einer abstrakten Haftung von Zertifizierungsdiensteanbietern gegenüber jedermann im § 23 übernommen. Auf die Haftungsbestimmungen kann sich jeder, der sich auf ein Zertifikat verlassen hat und diesem gutgläubig gegenübersteht, berufen. Insbesondere Vertragspartner von Zertifikatsinhabern, die ja in keinerlei vertragsrechtlichem Verhältnis zum Zertifizierungsdiensteanbieter stehen, trifft dadurch eine ungleich geringere Beweislast zur Durchsetzung von Schadenersatzansprüchen gegenüber Zertifizierungsdienstanbietern als nach dem deliktischen Schadenersatzrecht[145]. Die Haftung gilt jedoch nicht nur für den Zertifizierungsdiensteanbieter im engeren Sinn. Da Anbieter von Registrierungsdiensten gemäß der Legaldefinition des § 2 Z 11 ebenfalls in den Bereich der Zertifizierungsdiensteanbieter fallen, trifft auch sie die Haftungsverpflichtung nach § 23 für in ihrer Sphäre verursachte Schäden.

Der Geltungsbereich von § 23 erstreckt sich aber nur auf qualifizierte Zertifikate. Maßgeblich ist, daß der Zertifizierungsdiensteanbieter „ein Zertifikat als qualifiziertes ausstellt". Dabei kommt es darauf an, daß es vom Diensteanbieter als „qualifiziertes Zertifikat" bezeichnet wird, diese Worte müssen im Zertifikat selbst lesbar beinhaltet sein, wie es auch durch § 5 Abs. 1 Z 1 für diese Zertifikatsklasse vorgeschrieben wird.

Die in der SigRL enthaltenen Haftungsbestimmungen für qualifizierte Zertifikate, für die eine Verschuldenshaftung mit umgekehrter Beweislastverteilung statuiert wird, werden wörtlich übernommen. Da dieser Artikel der SigRL aber nur als Normierung der Mindeststandards zu verstehen ist, erweitert das SigG den Bereich noch. Zusätzlich zu den in Art. 6 Abs. 1 lit. a-c genannten Haftungstatbeständen der SigRL haftet ein Diensteanbieter auch für die Einhaltung der Anforderungen und Empfehlungen der Anhänge II, III und IV[146] und für sonstige technische Sicherheitserfordernisse, die zusätzlich im SigG normiert sind. Der Zertifizierungsdiensteanbieter haftet in Österreich auch dafür, daß von ihm als ge-

---

[145] *Menzel/Schweighofer,* Liability of Certification Authorities, Proceedings of the Joint IFIP WG 8.5 and WG 9.6 Working Conference 1999, S. 161.

[146] Die Anhänge beinhalten: Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen und Anforderungen an die Signaturerstellungseinheiten. Sie sind in den §§ 7 und 18 SigG umgesetzt.

eignet bezeichnete Produkte und Verfahren alle Anforderungen – auch die Empfehlungen des Anhanges IV[147] – der SigRL erfüllen.

Folgende Tatbestände werden von § 23 umfaßt:

Haftung für

- die Richtigkeit aller Angaben im qualifizierten Zertifikat (Z. 1) (Z. 1 bezieht sich auf den Inhalt des Zertifikats und stellt auf alle Anforderungspunkte an ein qualifiziertes Zertifikat ab, die in Anhang I SigRL beziehungsweise § 5 Abs. 1 geregelt sind.)
- den Besitz der Signaturerstellungsdaten durch den im Zertifikat angegebenen Signator zum Zeitpunkt der Ausstellung des Zertifikates (Z. 2 ist die Haftungsregel für die Verpflichtung der Zertifizierungsdiensteanbieter, gemäß § 2 Z 1 die Zuordnung der Signaturprüfdaten zum Signator korrekt abzuwickeln.)
- die komplementäre Entsprechung von Signaturerstellungsdaten und ihnen zugeordneten Signaturprüfdaten bei der Verwendung vom Zertifizierungsdiensteanbieter bereitgestellten oder als geeignet bezeichneten Produkten
  (Z. 3 bezieht sich auf die sicherheitsrelevante Anforderung, daß Signaturerstellungsdaten und Signaturprüfdaten komplementäre Komponenten sind. Aus den Erläuterungen zur RV geht hervor, daß dies für sämtliche Signaturverfahren gelten muß, unabhängig ob die Daten vom Zertifizierungsdiensteanbieter oder Signator selbst erstellt wurden.)
- die Einhaltung der Anforderungen des § 7 und die ausschließliche Verwendung von technischen Komponenten und Verfahren gemäß § 18
  (Diese Haftungsregel dient wie oben besprochen der Sicherstellung der Einhaltung aller Anhänge der SigRL.)

Rechtstechnisch wird durch § 23 Abs. 3 eine Verschuldenshaftung des Diensteanbieters mit Beweislastumkehr zugunsten des Geschädigten statuiert. Der Zertifizierungsdiensteanbieter muß beweisen, daß ihn an dem für den Schadensfall relevanten pflichtwidrigen Verhalten kein Verschulden trifft. Eine Gefährdungshaftung der Zertifizierungsdiensteanbieter konnte allerdings nicht normiert werden, da auf europäischer Ebene keine Einigung zugunsten dieses Modells gefunden wurde. Weiters gilt auch die

---

[147] Empfehlung über Anforderungen an Signaturprüfdaten, die im § 18 SigG umgesetzt sind.

Erfüllungsgehilfenhaftung des Zertifizierungsdiensteanbieters gegenüber jedermann. Die Beweislastumkehr im vollen Ausmaß bezieht sich allerdings – wie schon im vorigen Abschnitt erwähnt – nicht auf die Kausalität. Trotzdem gewährt § 23 Abs. 3 dem Geschädigten auch beim Beweis der Kausalität eine Erleichterung. Diese Kausalität wahrscheinlich zu machen ist ausreichend für eine Haftung, solange der Diensteanbieter nicht im Gegenzug die Kausalität seiner Pflichtwidrigkeit ebenfalls zweifelhaft macht. In diesem Fall träfe den Geschädigten wieder der volle Beweis der Kausalität.

Die Haftung kann zwar der Höhe nach und für gewisse Transaktionsarten durch den Diensteanbieter beschränkt werden, dabei wird aber bis zur beschränkten Höhe für jede einzelne Transaktion gehaftet. Durch diese Einführung einer Haftungshöchstgrenze übernimmt § 23 Abs. 4 ein charakteristisches Merkmal der Gefährdungshaftung. Interessant ist, daß die Höchstgrenze nicht fix durch den Gesetzgeber vorgegeben ist, wie es für die meisten Gefährdungshaftungstatbestände üblich ist, sondern variabel vom Zertifizierungsdiensteanbieter festgesetzt werden kann. Dadurch wird es der Wirtschaft ermöglicht, verschieden teure Zertifikate mit unterschiedlichen Haftungshöchstgrenzen innerhalb der Klasse der qualifizierten Zertifikate zu schaffen. Die Einschränkungen im Transaktionsbereich können sich zum Beispiel nur auf bestimmte Arten von Verträgen beziehen. Aus Gründen der Objektivität und Erkennbarkeit durch den Dritten müssen diese Beschränkungen im Zertifikat angegeben werden.

Zur Sicherstellung der Deckung der Haftpflichtansprüche, die einen Zertifizierungsdiensteanbieter potentiell treffen könnten, schreibt § 7 Abs. 1 Z 6 vor, daß Zertifizierungsdiensteanbieter für qualifizierte Zertifikate über ausreichende Finanzmittel verfügen müssen, um Vorsorge für die Befriedigung von Schadenersatzansprüchen zu treffen. Das Eingehen einer Haftpflichtversicherung wird als Beispiel angeführt. Der Abschluß einer solchen ist gemäß der Auffassung des Justizausschusses[148] ein probates Mittel zur Abdeckung dieses Risikos. Grundsätzlich kommen aber auch andere Sicherungsmittel, wie etwa Bankgarantien oder Bürgschaften, in Betracht, wobei der Sicherungsgrad allerdings mit jenem einer Haftpflichtversicherung vergleichbar sein muß.

Letztendlich erklärt das SigG Haftungsbestimmungen anderer Rechtsvorschriften, nach denen über die Begrenzung hinausgehende Schäden geltend gemacht oder andere Personen in Anspruch genommen werden können, als unberührt und ebenfalls anwendbar. Da dem § 23 SigG im

---

[148] 2065 der Beilagen zu den Stenographischen Protokollen des NR der XX. GP, S. 2.

Gegensatz zum deutschen SigG[149] Schutzgesetzwirkung zukommt, ergibt sich auch nach deliktischem Schadenersatzrecht, daß der Ersatz für bloß fahrlässig zugefügten Vermögensschaden einklagbar ist. Dies dürfte bei Überschreitung der Haftungshöchstgrenzen – trotz Beweislast des Geschädigten – in Zukunft von Bedeutung sein.

Die Anwendbarkeit der Haftungsbestimmung und anderer zivilrechtlicher Regelungen richtet sich nach dem Internationalen Privatrecht. Auch die Vorschriften über die Zuständigkeiten der innerstaatlichen Gerichte bleiben durch das SigG unberührt.

4.7.3. Regelung in der SigRL

In der SigRL ist kein Genehmigungsverfahren für die Betreiber von Zertifizierungsdiensten vorgesehen, Verfahren, die die vorherige Erteilung einer Genehmigung durch Behörden der Mitgliedstaaten voraussetzen, sind zu vermeiden.[150] Die Kommission erwartet sich dadurch einen europaweiten freien Marktzugang für Provider, die Zertifizierungsdienste anbieten wollen. Um einen hohen Standard der Infrastruktur zu gewährleisten bedient sich diese Richtlinie keiner technischen Zulassungsüberprüfung wie in Deutschland, sondern normiert detaillierte Haftungstatbestände für Anbieter von Zertifizierungsdiensten. Durch diese strenge Gefährdungshaftung sollen die Zertifizierungsdiensteanbieter motiviert werden, eine qualitativ hochwertige Infrastruktur bereitzustellen. Um unterschiedliche Haftungsnormen in den einzelnen Mitgliedsstaaten zu vermeiden, dienen die Haftungsregelungen im Art. 6 auch der Rechtsvereinheitlichung im europäischen Wirtschaftsraum, die ja wegen der grenzüberschreitenden Tätigkeiten im Internet dringend verwirklicht werden sollte. Die Richtlinie versucht Unterschiede bezüglich der Reichweite und des Inhaltes der Haftungsregelungen in den Mitgliedsstaaten zu vermeiden und grenzüberschreitendes Handeln auch im Bereich des elektronischen Geschäftsverkehrs zu fördern.[151]

Nach Art. 6 haftet ein Diensteanbieter, der ein qualifiziertes Zertifikat ausstellt, jeder Person, die vernünftigerweise auf das Zertifikat vertraut, daß

---

[149] *Timm*, Signaturgesetz und Haftungsrecht, DuD 9 (1997), S. 525, etwas vorsichtiger: *Emmert*, Haftung der Zertifizierungsstellen, CuR 4 (1999), S. 244.

[150] Erwägungsgrund 8, SigRL.

[151] Erwägungsgrund 12, SigRL.

- alle Informationen im qualifizierten Zertifikat zum Zeitpunkt seiner Ausstellung richtig sind, soweit der Diensteanbieter im Zertifikat nichts Gegenteiliges angegeben hat;
- alle Anforderungen des Anhanges I dieser Richtlinie bei der Ausstellung des qualifizierten Zertifikats eingehalten wurden;
- der im qualifizierten Zertifikat angegebene Inhaber zum Zeitpunkt der Ausstellung des Zertifikates im Besitz der Signaturerstellungseinheit ist, die der im Zertifikat angegebenen bzw. identifizierten Signaturprüfeinheit entspricht;
- in Fällen, in denen der Zertifizierungsdiensteanbieter sowohl die Signaturerstellungseinheit als auch die Signaturprüfeinheit erzeugt, beide Komponenten in komplementärer Weise funktionieren.

Für die korrekte Identitätsprüfung haftet der Diensteanbieter nach dem Vorschlag „jeder Person", unabhängig ob ein Vertragsverhältnis zwischen Diensteanbieter und dem Geschädigten existiert. Die Richtlinie führt daher für die angeführten Tatbestände eine vertragsunabhängige Gefährdungshaftung bei Organisationsverschulden gegenüber Dritten ein. Die Haftungsregeln beziehen sich aber nur auf qualifizierte Zertifikate gemäß Anhang I, weil in diesen ja die Erfüllung eines besonderen Vertrauenstatbestandes zu sehen ist. Spezielle Haftungsnormen, die für alle Zertifikate gelten, sind in der Richtlinie nicht zu finden. Ebensowenig erstreckt sich die Haftung auf die Zertifikate für Programme oder Server, es fallen gemäß Art. 6 (1) lit. c nur „im qualifizierten Zertifikat angegebene Inhaber" in den Geltungsbereich der Haftung.

4.7.3.1. Haftungshöchstgrenzen

Allerdings werden in der Richtlinie keine fixen Haftungshöchstgrenzen festgelegt; anders als in den meisten Normen, für die eine Gefährdungshaftung zutrifft, in denen auch fixe Haftungshöchstgrenzen vorgesehen sind, gibt die Richtlinie vor, daß die Parteien die Haftungshöchstgrenzen für die verschiedenen Gruppen von Zertifikaten selber vereinbaren

Dem Diensteanbieter selbst steht es frei, seine Haftung auf zweifache Weise beschränken. Einerseits kann er gemäß Art. 6 Abs. 3 den Anwendungsbereich des Zertifikats festlegen. In der Richtlinie wird nicht näher erläutert, was unter Anwendungsbereich zu verstehen ist. Sinnvollerweise ist damit eine Einschränkung auf bestimmte Arten von Rechtsgeschäften oder der Ausschluß bestimmter Rechtsgeschäfte gemeint. Andererseits hat

der Diensteanbieter gemäß Art. 6 Abs. 4 auch die Möglichkeit, im Zertifikat den Wert der Transaktionen zu begrenzen. Dies erlaubt den Diensteanbietern den Handlungsspielraum, verschiedene Zertifikatsklassen zu schaffen, die durch eine unterschiedlich hohe Haftung des Diensteanbieters gedeckt werden. Diesen Umstand nützen zum Beispiel A-Sign im Feldversuch, die der österreichischen Datakom, oder Verisign, ein amerikanischer Zertifizierungsdiensteanbieter, schon sehr erfolgreich , indem sie zu verschiedenen Preisen Zertifikate mit verschiedenen Haftungshöhen anbieten.

Für Schäden jenseits der Höchstgrenze ist der Diensteanbieter nach Art. 6 nicht haftbar. Der Richtlinie ist nicht zu entnehmen, ob sich der Diensteanbieter auch bei vorsätzlicher Schädigung auf die Haftungsgrenze berufen kann. Das österreichische Recht kennt keine Grenzen bei der Verschuldenshaftung. Schäden, die über der Haftungshöchstgrenze liegen, können zum Beispiel im Bereich des EKHG jederzeit über Ansprüche aus dem allgemeinen Schadenersatzrecht des ABGB eingefordert werden, da im § 19 EKHG die Anwendbarkeit der allgemeinen Schadenersatzregelungen für die Schadensteile, die die Haftungshöchstgrenze überschreiten, ausdrücklich bejaht wird. Auch das SigG läßt die Anwendung der Bestimmungen des allgemeinen Schadenersatzrechtes unberührt. Trotzdem muß wohl auch bei dem Fehlen eines eindeutigen Verweises auf die allgemeine Verschuldenshaftung diese subsidiär anzuwenden sein. Ein Dritter kann daher auch gegenüber einem Diensteanbieter die Schadensteile, die über der Wertgrenze nach Art. 6 Abs. 4 liegen, gemäß den Regelungen des deliktischen Schadenersatzes fordern.

Die Beschränkungen müssen für Dritte erkennbar sein, woraus folgt, daß sie der Zertifizierungsdiensteanbieter in jedem einzelnen qualifizierten Zertifikat angeben muß.

4.7.3.2. Das Vertrauen auf das Zertifikat „in vernünftiger Weise"

Eine weitere Voraussetzung ist das Vertrauen des Geschädigten auf das Zertifikat in vernünftiger Weise. In einer deutschen Besprechung[152] des Richtlinienvorschlags wird kritisiert, daß „dieser Terminus in der deutschen Rechtssprache unbekannt ist" und daher eine Beschreibung des Begriffs in der Richtlinie nötig ist. Im österreichischen Recht ist der Be-

---

[152] *Brisch*, Gemeinsame Rahmenbedingungen für elektronische Signaturen, Richtlinienvorschlag der Europäischen Kommission, CuR (1998), S. 498.

griff aber einige Male in Verwendung. So findet man etwa im § 5 Produktsicherheitsgesetz (BGBl 306/1994) die Regelung, daß ein Produkt als sicher anzusehen sei, „wenn es bei bestimmungsgemäßer oder vernünftigerweise vorhersehbarer Verwendung ... keine Gefahren ... birgt".

Die Verwendung dieses Terminus soll daher, wie schon in anderen Normen sinngemäß gleichlautend geregelt, auch in der Richtlinie die Haftung des Zertifizierungsdiensteanbieters für gewisse Ereignisse ausschließen, die sich im Nahbereich der Undenkbarkeit und Absurdität befinden, die also ein durchschnittlicher Nutznießer einer Public Key Infrastructure sofort als falsches Zertifikat erkennen sollte. Der Ausdruck „in vernünftiger Weise" wurde nicht ins österreichische SigG übernommen, da die Judikatur in Österreich eine Haftung auf Grund absurder Angaben ausschließen würde.

Eine weitere Einschränkung der Haftung findet sich auch im Art. 6 Abs. 3. Der Zertifizierungsdiensteanbieter ist für Fehler im qualifizierten Zertifikat, die auf Informationen beruhen, die er von der Person erhält, für die das Zertifikat ausgestellt wird, nicht haftbar, wenn er nachweisen kann, daß er alle zumutbaren Schritte unternommen hat, um diese Information zu überprüfen. Zusammen mit der Anforderung des Anhangs II an Diensteanbieter, „ ... mit geeigneten Mitteln die Identität und Handlungsbefugnis der Person zu überprüfen...", findet man hier die Sorgfaltsvorschriften für Diensteanbieter, die allerdings durch die Richtlinie nicht sehr detailliert spezifiziert wird. Man wird wohl noch erste Judikate zu diesem Bereich abwarten müssen, bis man sich eine genaue Vorstellung über den Begriff „alle zumutbaren Schritte" machen kann.

4.7.3.3. Haftung gegenüber dem Zertifikatsinhaber

In der Richtlinie finden sich auch keine besonderen Regelungen über die Haftung des Diensteanbieters gegenüber von ihnen zertifizierten Personen. Besondere Regelungen sind in diesem Bereich aber auch nicht nötig, da ja zwischen dem Diensteanbieter und seinen Kunden, die er zertifiziert hat, Vertragsbeziehungen bestehen. Es ist daher möglich, daß in den Policies besondere Haftungsregelungen im Rahmen der Disposität des Schadenersatzrechtes zwischen den Parteien vereinbart werden. Weiters kommen dem Kläger auch die besonderen Regelungen der Beweislastumkehr und der Erfüllungsgehilfenhaftung für Schäden aus Vertragsverhältnissen zugute. Deswegen erscheint zwischen diesen Personen eine besondere Haftungsregelung nicht notwendig. Schäden, die dem Zertifizierten

entstehen und über den Bereich des Art. 6 hinausgehen, sind daher nach der allgemeinen Verschuldenshaftung zu ersetzen.

4.8. Anerkennung ausländischer Zertifikate

4.8.1. Anerkennung von Zertifikaten aus anderen Mitgliedsstaaten der Europäischen Union

Ein wesentliches Anliegen der SigRL ist die Harmonisierung der Regelung in den einzelnen Mitgliedsstaaten der Europäischen Union. Dadurch sollen zumindest im europäischen Raum die faktische grenzüberschreitende elektronische Kommunikation und der Elektronische Geschäftsverkehr zwischen Personen verschiedener Nationalität auch durch rechtliche Hindernisse nicht eingeschränkt werden. Grundsätzlich normiert § 24 der SigRL entsprechend, daß Zertifikate, die von einem in der Europäischen Union niedergelassenen Zertifizierungsdiensteanbieter ausgestellt wurden und deren Gültigkeit vom Inland aus überprüft werden kann, inländischen Zertifikaten gleichzustellen sind. Die Möglichkeit der Überprüfung aus Österreich bedeutet nur, daß die Verzeichnis- und Widerrufsdienste von Österreich aus erreichbar sein müssen. Da diese üblicherweise im Internet weltweit abrufbar sind, ist die Erreichbarkeit fast immer gegeben.

Die Entfaltung der besonderen Rechtswirkungen ist in Österreich an die Einhaltung der Sicherheitsanfordernisse des § 18 SigG, der dem Anhang III der SigRL entspricht, und an die der §§ 5 und 7, die den Anhängen I und II nachempfunden sind, gebunden, daher muß im Streitfall über ein ausländisches sicher elektronisch signiertes Dokument auch die Einhaltung dieser Erfordernisse nach dem SigG stattfinden. Dies bereitet den Zertifizierungsdiensteanbietern, die qalifizierte Zertifikate ausstellen, bezüglich der Anforderungen an qualifizierte Zertifikate und bezüglich der Anforderungen an sichere Signaturerstellungseinheiten keine besonderen Probleme, da diese Punkte in den Anhängen I bis III zwingend geregelt sind und daher bald in allen Rechtsordnungen der Mitgliedsstaaten harmonisiert sein sollten. Allerdings müssen gemäß § 24 für die österreichische Anerkennung sicherer elektronischer Signaturen, die in anderen Mitgliedsstaaten ausgestellt wurden, auch die Anforderungen des § 18 Abs. 4 an sichere Signaturprüfeinheiten eingehalten werden. In der SigRL haben diese Merkmale des Anhang IV aber nur empfehlenden Charakter, der auf einem Kompromiß innerhalb der Ratsarbeitsgruppe für Telekommunikation zwischen den Mitgliedsstaaten, die auf die Sicherstellung eines aus-

reichenden Sicherheitsstandards wert legten, und den eher liberaleren Mitgliedsstaaten beruht.

Ähnlich wie beim Problemkreis der Zertifikate von juristischen Personen stellt sich hier die Frage, ob nun für ausländische sicher elektronisch signierte Dokumente die hohen Anforderungen des SigG gelten, oder ob auch niedrigere Standards, die die SigRL den Mitgliedsstaaten ermöglicht, in Österreich die besonderen Rechtswirkungen der Schriftform und des Beweiswertes entfalten. Insbesondere Irrtumsmöglichkeiten, die durch die Problematik der dadurch eventuell nicht sichergestellten Viewer-Funktion verursacht werden, sind zumindest aus der Sicht des Verbraucherschutzes bedenklich. Diese und auch andere europäische Regulierungssprobleme im Bereich des Informationsrechts, die zur Zeit unter anderem im Bereich der Harmonisierung des Urheberrechtsschutzes[153] auftreten, sollten bald einer europäischen Lösung zugeführt werden, damit Kriterien und Vorgaben für die europaweite Einsatzbarkeit der Produkte gewährleistet sind.

4.8.2. Anerkennung von Zertifikaten aus Drittstaaten

Die grenzüberschreitende Bedeutung der elektronischen Kommunikation gebietet aber eine über den Raum der Europäischen Region herausgehende Regelung. § 24 Abs. 2 setzt dazu die Bestimmungen des Art. 7 Abs. 2 SigRL um. Hier wird wieder je nach Qualität der Signatur und des Zertifikates abgestuft vorgegangen. Einfache Zertifikate von Zertifizierungsdiensteanbietern aus Drittstaaten sind in Österreich anzuerkennen, wenn ihre Gültigkeit vom Inland aus überprüft werden kann. Sie entfalten die allgemeinen Rechtswirkungen gemäß § 3 Abs. 2.

An die Anerkennung qualifizierter Zertifikate aus Drittstaaten sind weitere Bedingungen geknüpft, da diese Anerkennung die Voraussetzung für die Verknüpfung sicherer elektronischer Signaturen mit den besonderen Rechtswirkungen darstellt. Um in Österreich anerkannt zu werden, sieht das SigG zwei Möglichkeiten vor. Einerseits kann sich ein Zertifizierungsdiensteanbieter aus einem Drittstaat, der die Anforderungen an Zertifizierungsdiensteanbieter für qualifizierte Zertifikate des § 7 erfüllt, der freiwilligen Akkreditierung in einem Mitgliedsstaat unterziehen. Diese Überprüfung und die damit verbundene Aufsicht garantieren die Einhaltung der Sicherheitsstandards durch Anbieter aus Drittstaaten. Ihren

---

[153] Dazu ausführlicher: *Geiger*, Europäische Grundlagen des Informationsrechts, Proceedings zu der Jahrestagung der Deutschen Gesellschaft für Recht und Informatik E.V. 1999.

Zertifikaten und den damit verknüpften elektronisch signierten Dokumenten kommen die besonderen Rechtswirkungen des § 4 zu Gute.

Wichtigster Aspekt für die Sicherheit ausländischer Zertifikate ist im Bereich der Anerkennung die Haftung des Anbieters aus Drittstaaten. Daher genügt es gemäß § 24 Abs. 2 Z. 2 auch, wenn für einen Diensteanbieter aus einem Drittstaat ein innerhalb der Europäischen Union niedergelassener Zertifizierungsdiensteanbieter haftungsrechtlich einsteht. Er übernimmt damit die Haftung gemäß § 23. Über diese Anbieter aus Drittstaaten ist bei der Aufsichtsbehörde ebenfalls ein Verzeichnis zu führen.

5. Rechtswirkung elektronischer Signaturen

5.1. Allgemeines

5.1.1. Funktionen der eigenhändigen Unterschrift und ihre Übertragung auf elektronisch signierte Dokumente

In allen Rechtsordnungen kommt der eigenhändigen Unterschrift rechtserhebliche Bedeutung zu. Der Rechtsunterworfene ist sich bewußt, daß er durch seine Unterschrift eine rechtsverbindliche Willenserklärung finalisiert, sie gilt gemäß § 294 ZPO vor Gericht als Beweis, daß der unterschriebene Text vom Aussteller stammt. Wenn der Gesetzgeber die Schriftform vorschreibt, bedeutet dies immer auch, die handschriftliche Unterschrift unter das Dokument, welches die Willenserklärung beinhaltet, zu setzen. Der Text kann dabei in eigener Handschrift, in Maschinschrift oder gedruckt abgefaßt sein. Die Unterschrift muß dagegen grundsätzlich eigenhändig sein. § 886 ABGB läßt eine mechanische Nachbildung des Namenszuges nur zu, wenn dies im Geschäftsverkehr üblich ist.[290] Daher sind gemäß der Rechtslage vor Einführung des SigG elektronische Signaturen der handschriftlichen Unterschrift noch nicht gleichgestellt.

Der Aussteller eines elektronischen Dokuments kann dieses aber nicht mit seinem Namenszug unterfertigen, ihm stehen nur die Möglichkeiten der elektronischen Signatur zur Verfügung. Im Laufe der Entwicklung unserer Rechtssysteme wurden die Formalerfordernisse für Rechtsgeschäfte laufend reduziert. Die Anerkennung elektronischer Signaturen und elektronisch signierter Dokumente durch die Rechtsordnung setzt diese langfristige Wirkung fort. Es bedarf nicht mehr der eigenhändigen Unterschrift, wenn die Substitution durch neue Techniken den Anforderungen, die an die eigenhändige Unterschrift und an schriftförmliche Dokumente gestellt werden, gerecht wird. Der Unterschied und die Gemeinsamkeiten zwischen elektronischer Signatur und eigenhändiger Unterschrift sollen an Hand von fünf Funktionen[291], die der eigenhändigen Unterschrift zugeordnet werden, erörtert werden. Diese Funktionen sind von Lehre und

---

[290] *Koziol/Welser*, Grundriß des Bürgerlichen Rechts[10], S. 150.

[291] *Bizer*, Das Schriftformprinzip im Rahmen rechtsverbindlicher Telekooperation, DuD (1992), S. 169.

Rechtsprechung ausgearbeitet worden, um die Anforderungen, die der Rechtsverkehr an die Verkörperlichung von Willenserklärungen stellt, festzulegen.

5.1.1.1. Identitätsfunktion

Eigenhändige Unterschriften sind dadurch gekennzeichnet, daß die Identität des Ausstellers der Unterschrift gegeben ist.[292] Die Lehre hat hierzu festgestellt, daß das eigenhändige Schreiben des Familiennamens oder Künstlernamens ausreicht, im Familienkreis auch der Vorname.[293] Sogar die nicht leserliche Paraphierung[294] genügt. Für den Bereich elektronischer Signaturen bedeutet dies, daß eine Nennung zumindest des Familiennamens oder eines Pseudonyms im Zertifikat gemäß § 5 Abs. 1 Z. 3 SigG zur Identifizierung ausreicht. Eine Definition der American Bar Association[295]stellt darauf ab, daß eine Unterschrift die Person, die ein Dokument unterschrieben hat, anzeigen und für andere Personen als den Unterzeichner schwierig nachmachbar sein soll.

Durch die eigenhändige Unterschrift wird zum einen der Aussteller der Urkunde erkennbar. Darüber hinaus soll der Erklärende identifiziert werden können, weil die unverwechselbare Unterschrift eine unzweideutige Verbindung zur Person des Unterzeichners herstellt.

Die Gewährleistung der Identitätsfunktion durch elektronische Signaturen und Zertifikate ist von zentraler Bedeutung in der Systematik des SigG. Die Anwender sollen Vertrauen in die elektronische Kommunikation setzen. Grundlage dieses Vertrauens in die elektronischen Netze und Instrumente ist zunächst die Sicherstellung der Identität der an den Kommunikationsabläufen bzw. den rechtlichen und wirtschaftlichen Transaktionen beteiligten Kommunikations- oder Geschäftspartner. Diese Feststellung wird in den Erläuterungen gleich zu Beginn des allgemeinen Teils getroffen. Gemäß der Legaldefinition § 2 Z.1 der elektronischen Signatur dient diese der Authentifizierung, also der Feststellung der Identität des Signators. Definitionsgemäß (§ 2 Z. 8) verwirklicht auch das Zertifikat die Bestätigung der Identität. Die Identität der Zertifikatswerber muß durch den Zertifizierungsdiensteanbieter bei der Registrierung an Hand

---

[292] *Brunner,* Das elektronisch gespeicherte Dokument und dessen Beweischarakter, NZ (1996), S. 161.

[293] *Gschnitzer,* Allgemeiner Teil des Bürgerlichen Rechts[2], S. 734.

[294] *Rummel,* ABGB[2] § 886 Rz. 3.

[295] *Baum* (Editorial Committee Chair), Digital Signature Guidelines, American Bar Association 1996.

eines amtlichen Lichtbildausweises geprüft werden. Die Aushöhlung der Identitätsfunktion durch Verwendung der Signaturerstellungsdaten von jemandem anderen als dem Signator wird gemäß § 21 untersagt und durch § 26 Abs. 1 mit Verwaltungsstrafe bis 56.000 S bedroht.

Alle diese Maßnahmen technischer und rechtlicher Natur stellen sicher, daß sichere elektronische Signaturen und Zertifikate die Identitätsfunktion theoretisch zumindest in gleichem Maße erfüllen wie eigenhändige Unterschriften. Was den Umfang der Identifikationsdaten angeht, leistet die elektronische Signatur sogar deutlich mehr. Die eigenhändige Unterschrift ist so vorzunehmen, daß eine eindeutige Feststellung des Unterzeichners möglich ist. Zu unterschreiben ist grundsätzlich mit dem eigenen, und zwar mit dem verkehrsüblichen Namen.[296] Im Zertifikat können auch zusätzliche Angaben des Signators[297] aufgenommen werden, die eine Identifizierung vereinfachen.

5.1.1.2. Echtheitsfunktion

Sie bietet Gewähr, daß die Willenserklärung – also der unterschriebene Text – vom Aussteller, der das Dokument signiert hat, stammt. Im Bereich der eigenhändigen Unterschrift wird dies durch die räumliche Verbindung der Unterschrift mit der Urkunde, die den Erklärungstext enthält, verwirklicht. Hierdurch wird ein enger Zusammenhang zwischen Dokument und Unterschrift hergestellt. Beim Einsatz elektronischer Signaturen wird diese Funktion noch besser verwirklicht, da die Signatur nicht nur unter dem Text steht, sondern die Signaturdaten im Rahmen des Hashens mit den ganzen Daten der Erklärung verwoben sind. Nachdem die Identität des Signators geklärt ist, bestätigt die elektronische Signatur, daß der gesamte Text des Dokuments vom Signator herrührt. Entgegen der Situation bei Verwendung der eigenhändigen Unterschrift, bei der eine Manipulation des Textes durch das nachträgliche Einfügen von Textteilen[298] möglich ist, kann dieses Problem bei elektronischen Signaturverfahren nicht so leicht auftreten, da sich bei Verwendung asymmetrischer Kryptographie die Signatur immer auf den ganzen Text bezieht. Auch die Veränderung eines einzigen Buchstaben ist sofort auffällig.

---

[296] *Stahr*, Die Unterschrift, Allgemeine Richtlinien, in: Steuer- und Wirtschaftskartei (1981), S. BV7.

[297] So ist geplant, daß Zertifikate, die im Verkehr mit der Behörde verwendet werden, auch die Sozialversicherungsnummer beinhalten müssen.

[298] Bezüglich Testamente: OGH in SZ 43/74 und SZ 47/18.

Um das Problem der Textverfälschung durch unterschiedliche Darstellungsarten der diversen Textverarbeitungsprogramme auszuschließen, normiert § 7 Abs. 2 SigVO, daß die von den Signatoren eingesetzten technischen Komponenten und Verfahren zur Erstellung sicherer elektronischer Signaturen die vollständige Anzeige der zu signierenden Daten ermöglichen müssen. Für zu signierende Daten dürfen nur vom Zertifizierungsdiensteanbieter empfohlene Formate verwendet werden. So ist z. B. die Verwendung des weitverbreiteten Formats Microsoft Word als Träger sicher elektronisch signierter Dokumente zum Zeitpunkt des Inkrafttretens der SigVO ausgeschlossen, da in § 7 Abs. 2 SigVO die allgemeine Verfügbarkeit von den technischen Komponenten und Formaten, die für die Anzeige sicher elektronisch signierter Daten verwendet werden, gefordert wird. Microsoft hat bis jetzt die Struktur des Dateiformats, das Microsoft Word zur Speicherung verwendet, nicht offengelegt.

In den Erläuterungen zum SigG wird bezüglich dieser Funktion zwischen Authentizität und Integrität elektronischer Daten unterschieden. Unter dem ersten Begriff wird die Echtheit der Daten verstanden, der zweite Begriff bezeichnet die Unverfälschtheit. Diese Unterscheidung ist aber bei der Anwendung asymmetrischer Kryptographie nicht von großer Bedeutung, da bei diesem Verfahren immer beide Funktionen zusammen gewährleistet sind. Bei korrekter Anwendung der Verfahren ist durch die vorgeschriebenen Sicherheitsvorkehrungen auch die Erfüllung dieser Funktion durch elektronische Signaturen gegeben.

Bizer geht noch einen Schritt weiter[299], wenn er meint daß gegenüber dem Papierdokument die Echtheitsfunktion sogar verbessert werden kann, da sie nicht nur die Echtheit der Willenserklärung, sondern sogar die Echtheit des Dokuments gewährleistet.

5.1.1.3. Beweisfunktion

Der Beweispflichtige kann später mit dem Dokument als Beweismittel zeigen, daß die unterschriebenen Erklärungen auch vom Aussteller stammen. Die Beweisführung wird durch das Dokument stark erleichtert. Zur Erfüllung dieser Funktion ist nicht die technische Ausgestaltung des Signatur- und Zertifizierungsverfahren maßgeblich, sondern die Rechtsordnung regelt selbst, inwieweit elektronisch signierten Dokumente vor Gericht Beweiswert zukommt. Da die einschlägigen Bestimmungen des § 4 Abs. 3 weiter unten ausführlich dargelegt werden, soll hier nur kurz ein

---

[299] *Bizer*, Das Schriftformprinzip im Rahmen rechtsverbindlicher Telekooperation, DuD (1992), S. 169.

Vergleich mit den Beweisregeln für konventionelle Schriftstücke mit eigenhändiger Unterschrift getroffen werden. Die sichere elektronische Signatur ist in Bezug auf die Identitätsfunktion[300] dem nicht signierten, unsicher übertragenen elektronischen Dokument gleichgestellt. Erst wenn der Beweis der Identität gelungen ist, also nachgewiesen ist, daß die Unterschrift echt[301] ist, gilt für den Beweis der Authentizität die Erleichterung für den Beweisführer, daß voller Beweis durch Vorlage der sicher elektronisch signierten Dokumente begründet wird.

Ob die elektronische Unterschrift vor Gericht dieselbe Beweisfunktion erbringen wird, hängt also von der zukünftigen Spruchpraxis der Gerichte ab. Bei breiter Anwendung sicherer Signaturverfahren im Geschäftsverkehr kann aber optimistischerweise von einer prozessualen Gleichbehandlung ausgegangen werden.

5.1.1.4. Abschlußfunktion

Sie bringt zum Ausdruck, daß die Willenserklärung mit der Unterschrift abgeschlossen, das heißt vollendet und nicht mehr in der Entwurfsphase ist. Die Funktion der eigenhändigen Unterschrift besteht hier in einem räumlichen Abschluß eines Textes, der durch das Anbringen des Namenszuges unter dem Text der Erklärung[302] realisiert wird. Durch die elektronische Signatur wird die Abschlußfunktion noch verbessert, da die Änderung elektronisch signierter Dokumente nach dem Zeitpunkt des Signierens sofort bemerkt wird. Die Abschlußfunktion richtet sich an den Adressaten des Dokuments. Er erkennt durch die angebrachte Unterschrift oder Signatur, daß dies die letztgültige Version des Dokuments ist.

Das Konzept des räumlichen Abschlusses in dem Sinne, daß die Signatur unter dem signierten Text stehen soll, muß allerdings aufgegeben, werden, da die elektronische Signatur ja, wie es auch in der Definition des § 2 Z. 1 beschrieben ist, aus elektronischen Daten besteht, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft sind. In der Praxis wird entweder eine Datei übermittelt, die in zwei Blöcken sowohl den Text des Dokuments beinhaltet als auch den dazu passenden

---

[300] Nähere Ausführungen zur Identitätsfunktion: *Menzel/Schweighofer,* Securing Electronic Commerce with Digital Signatures, Proceedings zur BILETA Konferenz 1999, http://www.bileta.ac.uk/99papers/menzel.htm.

[301] *Rechberger*, ZPO Kommentar § 294 Rz. 1.

[302] Nähere Ausführung zur Unterscheidung zwischen Unterschrift, Oberschrift, Querschrift: *Münch,* Die Reichweite der Unterschrift im Wechselrecht, Ein Plädoyer für die Maßgeblichkeit des räumlichen Zusammenhangs, S. 67.

verschlüsselten Hashwert, der die elektronische Signatur darstellt, oder Dokument und Signaturdaten werden in zwei Dateien an den Empfänger übermittelt. Beide Varianten sind mit dem SigG vereinbar. Theoretisch wäre es sogar möglich, ein Dokument unsigniert zu versenden oder es zu einem späteren Zeitpunkt elektronisch zu signieren und dann nur die Signatur zu versenden. Sobald dann beides beim Empfänger angelangt ist, liegt ein elektronisch signiertes Dokument im Sinne des SigG vor.

Im Bereich der elektronischen Dokumentenverwaltung sollte zur Einhaltung dieser Funktion bei der Verwendung elektronischer Signaturen auch ein effizientes System zum Dokumentmanagement verwendet werden. Gerade im Bereich der gemeinsamen Dokumentbearbeitung im Netzwerk entstehen im Laufe der Arbeit an einem Dokument oft sehr viele Varianten aus verschiedenen zeitlichen Stadien, die sich nur durch geringfügige Unterschiede in der Bezeichnung unterscheiden. Um Irrtümer in der Willenserklärung zu vermeiden, fordert deswegen § 7 Abs. 3 SigVO, daß die technischen Komponenten, die bei den Anwendern sicherer elektronischer Signaturen eingesetzt werden, vor dem Anbringen der Signatur den kompletten signierten Inhalt anzeigen müssen. Ob dieser in der Praxis dann auch noch einmal vom Anwender gelesen wird, ist fraglich, da das Leseverhalten beim Betrachten von Bildschirmtexten deutlich unterschiedlich zum Verhalten beim Lesen von Information in Papierform ist. Auch bieten die meisten am Markt verbreiteten Produkte diese Viewerfunktion nicht, um ihre Produkte kompatibel zu den Anforderungen von SigG und SigVO zu machen, es müßten also die betroffenen Mailprogramme durch Plug-Ins nachgerüstet werden.

5.1.1.5. Warnfunktion

Diese schützt den Unterzeichner vor Übereilung bei der Abgabe seiner Willenserklärung. Die Untersuchung des dabei gezeigten Verhaltens bei der Abgabe zeigt, daß die Tätigkeit des Unterschreibens dem Unterzeichner die Rechtsverbindlichkeit deutlich macht. Allerdings haben sich im Rechtsverkehr auch andere Handlungen mit derselben Funktion ausgebildet. Traditionell wird ein mündlich abgeschlossener Vertrag „mit Handschlag besiegelt". Erst diese Geste drückte beim Laien die Rechtsverbindlichkeit aus. Aber auch bei Verwendung der eigenhändigen Unterschrift, um die Anforderungen der Schriftform im traditionellen Geschäftsverkehr nachzuweisen, wurde die Bedeutung der Warnfunktion ge-

schwächt, da für Bürgschaften nach neuerer Rechtssprechung[303] eine Blankounterschrift reicht und auch die Ausstellung einer nicht näher konkretisierten Vollmacht zur Abgabe von Vollmachten erteilt werden kann.[304]

Am anderen Ende der zeitlichen Entwicklung zeigt sich auch im elektronischen Geschäftsverkehr, daß bei der Gestaltung des Vertragsabschlusses im Internet oft eine eigene Seite kurz vor dem Absenden der eigentlichen Willenserklärung durch den Konsumenten deutlich auf die Bindungswirkung der Erklärungshandlung hinweist. Art. 10 des Entwurfs der Europäischen Kommission für eine Richtlinie über bestimmte Aspekte des elektronischen Geschäftsverkehrs fordert, daß das Verfahren für das Zustandekommen eines elektronischen Vertrages vom Diensteanbieter klar und unzweideutig erläutert wird. In diesen Erläuterungen ist auch auf die Bindungswirkung der vom Anwender abgegebenen Erklärungen einzugehen.

Das SigG und die SigVO dienen zwar nicht primär zur Regelung des Vertragsabschlusses bei der Verwendung elektronischer Kommunikationsmittel, doch wird die Gewährleistung der Warnfunktion bei der Verwendung elektronischer Signaturen sichergestellt.

Der Anwender ist gemäß § 20 Abs. 2 im Rahmen seiner Zertifizierung über die Rechtswirkungen, die durch seine Signatur ausgelöst werden, zu informieren. § 7 Abs. 3 der SigVO berücksichtigt in seinen Anforderungen an die Signaturerstellungseinheiten der Anwender auch diesen Aspekt, indem er sicherstellt, daß die Signaturfunktion nur nach Verwendung von Autorisierungscodes ausgelöst werden darf und weiters die Anzahl der Signaturen, die pro Autorisierung ausgelöst werden, dem Signator bekannt sein muß. Die Authorisierungscodes dürfen nicht vom Programm gespeichert werden, und Eingabeerleichterungen müssen bei mehrmaliger Eingabe ausgeschlossen sein. Da die meisten marktüblichen Signaturerstellungseinheiten noch Paßwörter als Authorisierungscodes verwenden, ist durch die jedesmal erforderliche Eingabe des Paßwortes die Warnfunktion erfüllt.

Bei der Überprüfung biometrischer Merkmale im Rahmen der Autorisierung ist allerdings nur ein kurzer Blick oder Fingerdruck notwendig, um den Prozeß des Signierens auszulösen. Jedoch wird auch bei elektronischem Verfahren ein genügend starker Warneffekt erzeugt, da gerade der Blick in eine Vorrichtung zum Scannen des Augenhintergrund oder

---

[303] OGH 14.7.1988, 6 Ob 617/88, Besprechung in ÖBA 1989/134.

[304] *Schwimann/Apathy*, ABGB[2] § 886 Rz. 5.

ein Fingerabdruck durchaus nicht alltäglich zur Abgabe von Willenserklärungen verwendet werden.

5.1.2. Definition eines elektronisch signierten Dokuments[305]

§ 4 SigG stellt die sichere elektronische Signatur nur mit der eigenhändigen Unterschrift gleich und stellt fest, daß dadurch die Schriftlichkeit insbesondere im Sinne des § 886 ABGB erfüllt wird. Da die österreichische Legaldefinition der Schriftform fast ausschließlich auf eine eigenhändige Unterschrift abstellt[306], bereitet die Erfüllung der Anforderungen an die Schriftform beim Einsatz sicherer elektronischer Signaturen weniger Probleme. Allerdings ist die eigenhändige Unterschrift und dadurch die auch die elektronische Signatur stark mit der unterschriebenen Urkunde verknüpft, wie sich im Bereich des räumlichen Sinnzusammenhangs einer Unterschrift[307], der Problematik im Bereich der Blankounterschriften[308], der teilweisen Anerkennung einer Bankomatkarte als Urkunde in strafrechtlichen Verfahren[309] und der Problematik der Bezugnahme auf andere Urkunden in schriftförmlichen Willenserklärungen[310] zeigt.

Im § 2 finden sich zwar Legaldefinitionen für die elektronische Signatur und das Zertifikat, eine gesetzliche Regelung, was unter einem elektronisch signierten Dokument zu verstehen ist, wurde aber nicht aufgenommen. Daher ergeben sich für die Schriftförmlichkeit und den Beweiswert elektronisch signierter Dokumente eine qualitativ unterschiedliche Anerkennung durch die Rechtsordnung.

---

[305] § 4 Abs. 3 bezeichnet solche Willenserklärungen als elektronische Dokumente, die mit einer sicheren elektronischen Signatur versehen sind, zwecks sprachlicher Vereinfachung werden sie in dieser Arbeit als elektronisch signiertes Dokument oder sicher elektronisch signiertes Dokument bezeichnet.

[306] So ist es unbeachtlich wer den unterschriebenen Text verfaßt hat und in welcher Form oder Sprache er unterschrieben wurde. Ebenso ist eine Datums- und Zeitangabe nicht notwendig (*Schwimann/Apathy*, ABGB[2] § 886 Rz. 1).

[307] *Münch*, Die Reichweite der Unterschrift im Wechselrecht, Ein Plädoyer für die Maßgeblichkeit des räumlichen Zusammenhangs.

[308] Dagegen: *Rummel/Gamerith*, ABGB[2] § 1346 Rz. 8, *Wilhelm*, WBl 1989, 21, dafür: *Gschnitzer/Wahle*, Österreichisches Bankarchiv 1989/134, *Schwimann/Apathy*, ABGB[2] V §886 Rz.5.

[309] SSt 55/87 = EvBl 1985/146 S 659 = AnwBl 1985, 277 (Anmerkung Mirecki) = ÖJZ-LSK 1985/23.

[310] *Schwimann/Apathy*, ABGB[2] V §886 Rz.3.

Im Bereich der Schriftförmlichkeit wird auch nie auf das Vorliegen eines Dokuments abgestellt, dadurch gewährleistet die im § 4 Abs. 1 vollzogene Gleichsetzung der elektronischen Signatur mit der eigenhändigen Unterschrift die Erfüllung der Schriftform durch sicher elektronisch signierte Dokumente. Das Beweisrecht stellt allerdings beim Beweis durch Privaturkunden auf die Manifestation der Gedanken auf einem physischen Trägermaterial ab. Sicher elektronisch signierte Dokumente gründen daher nur durch die Gleichstellung von eigenhändiger Unterschrift und sicherer elektronischer Signatur nicht denselben Beweiswert wie Privaturkunden. Weil in § 4 Abs. 3 für sicher elektronisch signierte Dokumente nur die Bestimmung des § 294 ZPO über die Vermutung der Echtheit des Inhalts einer unterschriebenen Privaturkunde anwendbar erklärt wird, sind die weiteren Bestimmungen der ZPO über den Beweiswert von Privaturkunden nicht anwendbar.

Da der Gesetzgeber im Bereich des Beweisrechts nur von Urkunden, jedoch nie von Dokumenten oder Unterschriften spricht, ist eine Klarstellung des Unterschiedes erforderlich. Im Rahmen der Vorbereitungsarbeiten zur SigRL wurde in Studien[311] folgende nicht – technische Definition ausgearbeitet:

Elektronische Dokumente sind Dokumente, die mit einem Computer erstellt wurden. Im allgemeinen kann zwischen einem elektronischen Dokument im engeren und im weiteren Sinn unterschieden werden. Im engeren Sinn versteht man darunter ein Dokument, welches in digitaler Form gespeichert ist und von einem Menschen ohne Hilfe eines Computers nicht wahrgenommen werden kann. Es ist auf einem magnetischen Datenträger gespeichert und kann gelöscht, verändert und umgeschrieben werden, ohne Spuren zu hinterlassen. Die Integrität eines nicht signierten elektronischen Dokumentes ist kaum zu verifizieren.

Erst durch die sichere elektronische Signatur erfährt das elektronische Dokument eine Verbesserung der Qualität, die es mit einem traditionell erstellten Dokument gleichstellt.

Vier Komponenten machen die Eigenschaften eines traditionellen Dokumentes aus:

- Trägermaterial (Papier)
- Text und Bilder (physischer Aufdruck)
- Information über den Aussteller

---

[311] ISTEV, Legal and Regulatory Issues for the European Trusted Services Infrastructure, European Commission, S. 13.

– Unterschrift als Maßnahme zur Sicherung der Authentizität

Sie können auf Grund die Funktionalität der sicheren elektronischen Signatur im Bereich der elektronisch signierten Dokumente durch diese substituiert werden. Es bleibt nur die Ununterscheidbarkeit zwischen Original und Kopie im digitalen Bereich, die aber durch die Anbringung von Zeitstempel gelöst werden kann.

5.2. Allgemeine Rechtswirkungen

Die Europäische Kommission ist sich der Bedeutung der elektronischen Signaturen für den Elektronischen Geschäftsverkehr bewußt. Damit dieses nicht durch die Rechtssysteme einzelner Mitgliedsstaaten unterlaufen werden kann, legt sie in Art. 5 Abs. 1 SigRL fest, daß einer elektronischen Signatur die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel nicht allein deshalb abgesprochen wird, weil sie in elektronischer Form vorliegt, nicht auf einem qualifizierten Zertifikat oder nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder nicht von einer sicheren Signaturerstellungseinheit erstellt wurde. Es ist den Mitgliedsstaaten verwehrt, die allgemeine Rechtswirkung der elektronischen Signatur von bestimmten Qualitätsmerkmalen abhängig zu machen. Weitergehende besondere Rechtswirkungen – wie insbesondere die Schriftform und die Gleichstellung mit dem Urkundenbeweis – können sehr wohl an die Einhaltung besonderer Anforderungen gebunden werden. Die Kommission will mit dieser Regelung einer weitreichenden Rechtswirksamkeit elektronischer Signaturen zu deren Verwendung und rechtlichen Anerkennung in der Europäischen Union beitragen.[312]

Mit anderen Worten in Anlehnung an Grundrechte formuliert: „Vor dem Gesetz sind alle Nachrichten gleich".[313]

Österreich setzt diesen Grundsatz in § 3 wörtlich um. Die Zertifizierungsdiensteanbieter können jede Art. von Signaturverfahren anbieten, auch die Anwendung von Verfahren, die nicht den Regelungen des SigG und der SigVO entsprechen, ist freigestellt. Analog gilt das oben Besprochene, daß weitergehende Rechtswirkungen des § 4 aber sehr wohl an die Einhaltung aller gesetzlichen Voraussetzungen gebunden sind. Die Be-

---

[312] Erwägung Z. 10 SigRL.

[313] *Riedl*, Auch die UNCITRAL mengt sich in den elektronischen Geschäftsverkehr ein, ecolex (1999), S. 241.

stimmung regelt jedoch nicht die Frage der Zulässigkeit elektronischer Kommunikation im Rechtsverkehr, wie zum Beispiel Regeln über die Annahme und den Zugang von Willenserklärungen in elektronischer Form. Dies bleibt allgemeinen Regeln über den elektronischen Geschäftsverkehr vorbehalten, die im Rahmen der Umsetzung einer zukünftigen Richtlinie über bestimmte Aspekte des elektronischen Geschäftsverkehr zu erfolgen haben.

Regelungsbereich des SigG ist die Erstellung elektronischer Signaturen, § 3 bezieht sich daher nur auf die Nichtdiskriminierung im Rahmen des Geltungsbereiches. Auch einfache elektronische Signaturen dürfen also im Rechtsverkehr nicht einfach verboten werden. Im Rahmen der Privatautonomie können Vertragsparteien aber sehr wohl die Verwendung elektronisch signierter Dokumente ausschließen, da nach § 884 ABGB vermutet wird, daß die Parteien, die eine bestimmte Form[314] für den Vertragsabschluß vereinbart haben, vor der Erfüllung dieser Form nicht gebunden sein wollen. Prinzipiell[315] ist man im Rahmen der Privatautonomie nicht daran gebunden, auf Anbote zu antworten. Der Angeschriebene kann daher alle an ihn gerichteten elektronisch signierten Dokumente ignorieren.[316] Sowohl im behördlichen als auch gerichtlichen Verfahren müssen elektronisch signierte Dokumente aber im Beweisverfahren gewürdigt werden.

Diese Anforderungen wurden aber schon vor dem In Kraft Treten des SigG erfüllt. Das AVG gewährleistet in § 13 Abs. 1, daß schriftliche Anbringen nach Maßgabe der zur Verfügung stehenden technischen Mittel auch telegraphisch, fernschriftlich, im Wege automatisationsunterstützter Datenübertragung oder in jeder technisch möglichen Weise eingebracht werden können. Werden allerdings sichere elektronische Signaturen benutzt, so kann die öffentliche Hand auch noch zusätzliche Sicherheitsanforderungen zu den im SigG vorgesehenen festlegen.[317]

---

[314] In diesem Fall ist also der Vertragsabschluß in der Form sicher signierter elektonischer Dokumente auszuschließen.

[315] Anderes gilt für die dem Kontrahierungszwang unterliegenden Basisversorger.

[316] Vergleiche auch die Ausführungen der Telekom Control GmbH über häufige Fragen zur elektronischen Signatur. verfügbar unter: http://www.tkc.at/www/TKC_main.nsf/pages/Signatur.

[317] So ist geplant, daß Zertifikate, die im Verkehr mit der Behörde verwendet werden, auch die Sozialversicherungsnummer beinhalten müssen.

5.3. Besondere Rechtswirkungen

Die Nichtdiskriminierung jeder elektronischen Signatur ist aber nur ein kleinster gemeinsamer Nenner, der für alle elektronischen Signaturen gilt. Sichere elektronische Signaturen, die allen Sicherheitsansprüchen des SigG genügen, bieten daher ein viel größeres Maß an Sicherheit und kommen, wie anhand der Überprüfung der Erfüllung aller fünf Funktionen, die an eigenhändige Unterschriften gestellt werden, deutlich wird, diesen in allen rechtserheblichen Aspekten gleich.

Daraus ergibt sich die Konsequenz, sie auch bezüglich ihrer Rechtserheblichkeit an die Regelungen für Schriftstücke in Papierform anzuknüpfen und sicher elektronisch signierte Dokumente mit diesen auszustatten.

Die Erläuterungen zu § 4 gehen von einer Gleichstellung sicherer elektronischer Signaturen mit der eigenhändigen Unterschrift aus und erklären, daß gemäß den Vorgaben der SigRL die besonderen Rechtswirkungen, die nach dem österreichischen Rechtssystem einer eigenhändigen Unterschrift zukommen, auch für die sicheren elektronischen Signaturen gemäß SigG gelten. Dies ist mE etwas über das Ziel schießend, da das SigG einerseits einige Ausnahmen statuiert, wo die Schriftform durch sichere elektronische Signaturen nicht erfüllt wird, andererseits im Beweisrecht nicht nur das Faktum der Unterschrift oder Signatur für die Beweisqualität entscheidend ist, sondern auch die Urkundeneigenschaft eines Dokuments. Daher sind zwar die Rechtswirkungen von eigenhändiger Unterschrift de jure weitgehend der elektronischer Signaturen gleichgestellt, allerdings findet man bei der wichtigen Regelung über Rechtswirkung der Beweiskraft doch noch unterschiedliche Behandlung von Dokumenten in Papierform und sicher elektronisch signierten Dokumenten. De facto kann dies eine Ungleichbehandlung der beiden Beweise im Gerichtsverfahren zur Folge haben.

5.3.1. Schriftförmlichkeit elektronisch signierter Dokumente im Zivilrecht

5.3.1.1. Rechtslage vor dem Signaturgesetz

Die Frage, ob ein Telefax den Anforderungen der Schriftform genügt, bei dem eine Faksimilekopie der eigenhändigen Unterschrift übermittelt wird, startete die Diskussion über die Möglichkeit zur Einhaltung der Formerfordernisse im elektronischen Geschäftsverkehr. Ausgehend von der Feststellung, daß das eigenhändige Schreiben des Familien- oder

Künstlernamens[318] die Anforderungen an die eigenhändige Unterschrift erfüllt, wurden aber zuvor schon in einer Reihe von Entscheidungen Formmängel bei anderen Methoden als der eigenhändigen Unterschrift festgestellt. Eine mechanische Nachbildung der Unterschrift durch Faksimilestempel reicht nur, wenn sie im Geschäftsverkehr üblich ist[319], was nur bei die Massenaussendungen anzunehmen ist[320], auch entsprechen Telegramme oder Fernschreiben[321, 322] nicht der Schriftform.

Da beim Telefax – wie beim elektronischen Geschäftsverkehr eine elektronische Übertragung erfolgt, wurde die Diskussion rund um die Schriftform eines Telefax auch analog auf andere elektronische Dokumente, wie zum Beispiel E-Mails, angewandt. *Rummel*[323] meinte, daß dies vom Formzweck abhängt und kommt nach einer Detailuntersuchung zum Schluß, in der Regel würde ein Fax der Schriftform entsprechen. Dem widerspricht *Wilhelm*[324] in einer Besprechung aus dem Jahr 1990, in der er feststellt: Über all den Warn-, Übereilungsschutz-, Beweissicherungs-, Gläubigerschutz- und Publikationszwecken darf der erste und wichtigste Zweck der Schriftform nicht vergessen werden: möglichst jeden Zweifel daran auszuschließen, daß die Erklärung wirklich von dem stammt, von dem zu stammen sie vorgibt. Deshalb wird eigenhändige Unterschrift verlangt. Sie garantiert Authentizität natürlich auch nicht, Fälschung der Unterschrift läßt sich nicht ausschließen. Aber unvergleichlich leichter ist es, eine Originalunterschrift zu kopieren, die Kopie auf ein vorbereitetes Textblatt zu legen, das ganze zu faxen und, bei der bekannt schlechten Qualität der Telekopien, beim Empfänger den Eindruck der Kopie als einer original gefertigten Urkunde zu erwecken. Der Formzweck gebietet ein strenges Verständnis der Formvorschrift, um solche Machenschaften zu verhindern: Der Schriftform genügt nur eine Urkunde mit Originalunterschrift.

Auch der OGH[325] folgte dieser Auffassung und einer ähnliche Entscheidung des BGH[326] und verneinte für eine per Fax übermittelte Bürg-

---

[318] *Gschnitzer*, AT[2], S. 734 zitiert in *Schwimann/Apathy*, ABGB[2] V § 886 Rz. 9.

[319] *Koziol/Welser*, Grundriß des Bürgerlichen Rechts[10], S. 150.

[320] *Rummel* in *Rummel* ABGB[2] § 886 Rz. 7.

[321] SZ 58/85.

[322] SZ 25/302 im Bereich des Verfahrensrechts, SZ 47/35 allgemein.

[323] *Rummel*[2], RZ. 1 zu § 886 ABGB.

[324] *Georg*, Telefax: Zugang, Übermittlungsfehler und Formfragen, ecolex (1990), S. 208.

[325] OGH 27. 3. 1995, 1 Ob 515/95, JBl 1995, 656 = ÖBA 1996, 73 (mit ablehnender Anmerkung von *Rummel*).

schaft die Erfüllung der geforderten Schriftform, da der Übereilungsschutz nicht gewährleistet sei. Bezüglich der Einhaltung des Übereilungsschutzes ist der Kritik an dieser Entscheidung in einer Besprechung von *Peter Bydlinski*[327] durchaus zu zustimmen, doch mangelt es beim Telefax deutlich an der Gewährleistung der Identitäts- und Echtheitsfunktion. Mit modernen Grafikprogrammen ist die Fälschung von per Fax übermittelten Unterschriften zu einfach durchzuführen. Somit sind die Anforderungen an eigenhändige Unterschriften nicht gegeben, und ein Telefax erfüllt nicht die Schriftform.

Auch E-Mails und andere elektronisch übermittelte Dokumente, die nicht sicher elektronisch signiert sind, enthalten kein Element, das der von § 886 ABGB für die Schriftlichkeit geforderten eigenhändigen Unterschrift gleichkommt. Sie entfalten daher nicht die Rechtswirkung der Schriftförmlichkeit. Daran ändert sich auch nichts, nachdem das SigG in Kraft tritt, da diesen Dokumenten alle Sicherheitselemente sicherer elektronischer Signaturen fehlen, die ja Voraussetzung für die besonderen Rechtswirkungen sind. In Österreich gibt es zwar keine Judikatur, die explizit ausspricht, daß nicht signierte elektronische Dokumente nicht die Anforderungen der Schriftform erfüllen, doch ist die Analogie zu Entscheidung über Fax und Papierform augenscheinlich und von der herrschenden Lehre anerkannt. Einer Verwendung dieser Kommunikation für formfreie Willenserklärungen steht aber nichts im Wege.

5.3.1.2. Einführung der Textform und der elektronischen Form

Vor dem Votum der SigRL für die Schriftform diskutierte man besonders in Deutschland auch die Einführung einer neuen gesetzlichen Form, die der rechtlichen Anerkennung elektronischer Dokumente zum Durchbruch verhelfen soll. Hierzu wurde vom deutschen Bundesminister für Justiz die Einführung einer neuen Formvorschrift, der sogenannten „Textform", in einem neu einzufügenden § 126a dBGB vorgeschlagen.[328] Nach dieser Bestimmung soll es bei der Textform lediglich auf die Lesbarkeit eines Erklärungstextes ankommen. Diese Form wird als eine neue und verkehrsfähige in das deutsche BGB integriert, ist gegenüber der Schriftform erleichtert, denn sie verlangt nur noch eine in lesbaren Schriftzei-

---

[326] NJW 1993, 1126.

[327] *Bydlinski*, Telefaxbürgschaft: OGH folgt BGH, RdW (1996), S. 196.

[328] Entwurf eines Gesetzes vom 31.1.1997 GZ 3414/2 zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr.

chen fixierte Erklärung oder Mitteilung und verzichtet auf die eigenhändige Unterschrift. Insbesondere benötigt ein elektronisches Dokument, das der Textform entspricht, keine elektronische Signatur. In den Fällen, in denen durch Gesetz die Textform vorgeschrieben ist, wird also auf das Erfordernis der eigenhändigen Unterschrift sowie der Papierform verzichtet.[329] Sie ersetzt die Schriftform insbesondere in den Bereichen, in denen es sich um Erklärungen ohne erhebliche Beweiswirkung sowie mit nicht erheblichen oder leicht wieder rückgängig zu machenden Rechtsfolgen handelt.

Weiters wird eine neue elektronische Form als Option zur Schriftform eingeführt. Die elektronische Form verzichtet, an die neuen Kommunikationstechniken angepaßt, notwendigerweise auf das Merkmal der Verkörperung, erfordert aber, über die Kriterien der Textform hinausgehend, eine digitale Signatur unter Anwendung eines Verfahrens, das die Voraussetzungen des dSigG erfüllt.

Dadurch will Deutschland die unerwünschte, völlige Gleichstellung elektronisch übermittelter Dokumente und traditioneller Dokumente in Papierform vermeiden. Bezüglich der gewillkürten Schriftform sollen §§ 126, 127 dBGB novelliert werden, und ein neuer § 126a dBGB eingefügt werden, so daß im Falle eines durch ein Rechtsgeschäft vereinbarten Schriftlichkeitserfordernisses im Zweifel angenommen werden solle, daß die Einhaltung der Textform diese Form wahrt. Bis jetzt stellt das deutsche Recht im Gegensatz zur österreichischen Rechtsordnung nicht nur auf das Vorliegen einer eigenhändigen Unterschrift ab, sondern verlangt das Vorliegen einer Urkunde[330] als physisches Trägermaterial der schriftlichen Erklärung zusätzlich zur Anforderung der eigenhändigen Unterschrift.[331]

Das Modell der Einführung einer neuen Textform hat allerdings den Nachteil, daß alle Rechtsvorschriften, die Formvorschriften festsetzen, an die zusätzliche Form angepaßt werden müssen. Das deutsche Bundesministerium für Justiz geht von 452 zivil-, handels- und wirtschaftsrechtlichen Bestimmungen aus, die Schriftformbestimmungen zum Inhalt haben. ME ist die Zahl dieser Bestimmungen – zumindest im österreichischen Recht – um einiges größer.[332] Die Prüfung all dieser Bestimmung auf die

---

[329] *Brenn*, Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet, ÖJZ (1997), S. 641.

[330] *Palandt*, Bürgerliches Gesetzbuch[57] § 126 Rz. 2.

[331] *Palandt*, Bürgerliches Gesetzbuch[57] § 126 Rz. 5.

[332] Eine Volltextsuche in der Bundesnormendatenbank des Rechtsinformationssystem des Bundes nach den Suchbegriffen „schriftf?rm* oder unterschrift*" ergab 1008 Be-

Tauglichkeit für die Textform und Novellierung aller betroffenen Gesetze wäre rechtstechnisch komplizierter als die Zuerkennung der einfachen Schriftform für gewisse sichere elektronische Dokumente, wie es das SigG auch vorsieht. Weiters würde sich durch die Schaffung der neuen Formen die Anzahl der verschiedenen Abstufungen der Schriftform auf fünf[333] erhöhen, was auch nicht im Sinne einer Rechtsvereinheitlichung förderlich wäre.

5.3.1.3. Rechtslage nach dem Signaturgesetz

Die Regelungen des Artikels 5 SigRL besagen nur, daß „elektronische Signaturen, die auf einem qualifizierten Zertifikat basieren, welches von einem Zertifizierungsdiensteanbieter erteilt wurde, der den Anforderungen in Anhang II genügt, zur Erfüllung des rechtlichen Erfordernisses einer handschriftlichen Unterschrift anerkannt werden".[334] Die Europäische Kommission interpretiert diese Bestimmung dahin, daß Daten, die mit einer fortgeschrittenen elektronischen Signatur verknüpft sind, daher die Erfordernisse der Schriftform erfüllen. Dies ist in Österreich auch der Fall, da gemäß § 886 ABGB für die einfache Schriftform normiert ist, daß ein Vertrag durch die Unterschrift der Parteien zustande kommt. Anders als in Deutschland, wo im § 126 dBGB noch das Vorliegen eines Trägermediums gefordert wird[335], wird im österreichischen Recht das Erfordernis der Schriftform daher allein durch die Unterschrift der Parteien erfüllt. Diese Bestimmung ist auch auf andere, von Verträgen unterschiedliche Rechtsgeschäfte analog anwendbar. Durch die Gleichstellung der eigenhändigen Unterschrift mit der sicheren elektronischen Signatur, die § 4 Abs. 1 und 2 normieren, erfüllen also elektronische Dokumente, die sicher elektronisch signiert sind, prinzipiell alle Erfordernisse der einfachen Schriftform.

Da die meisten Rechtsgeschäfte nicht die Schriftform erfordern, sondern der Formfreiheit unterliegen und die Fragen des Beweiswerts elektronisch signierter Dokumente extra geregelt sind, ist diese Bestimmung

---

stimmungen, die diesen Bereich regeln. Durch landesrechtliche Bestimmungen erhöht sich die Zahl noch.

[333] Die eigenhändig geschriebene Form, die allographe Form, die öffentliche Form und eben die Textform und die elektronische Form.

[334] COM(1999)195, Änderungsantrag 18.

[335] Die Signaturrichtlinie wird allerdings in diesem Punkt durch die ebenfalls geplante Richtlinie über Electronic Commerce (KOM(1998)586) ergänzt, die in Art. 9 normiert, daß Formvorschriften, die nicht durch elektronische Mittel erfüllt werden können, angepaßt werden müssen.

hauptsächlich für Rechtsgeschäfte bedeutsam, die der Schriftform zum gültigen Abschluß bedürfen. In Österreich betrifft das unter anderem die Abgabe einer Bürgschaftserklärung durch einen Nichtkaufmann[336], die Begründung von Wohnungseigentum[337], den Abschluß eines befristeten Mietvertrags[338], die Eintragung von Rechten im Grundbuch[339] und den Bauträgervertrag.[340] Weiters erfüllen Banken, die einen Verbraucherkreditvertrag oder einen Verbrauchergirokontovertrag[341] nicht in der Schriftform abschließen, einen Verwaltungsstraftatbestand.

Grundsätzlich erfüllen also formgebundene Verträge, die sicher elektronisch signiert worden sind, ex lege alle Voraussetzungen. Die SigRL in Verbindung mit Art. 9 Abs. 2 des Entwurfs einer Richtlinie über bestimmte Aspekte des elektronischen Geschäftsverkehrs erlaubt aber einige wenige Ausnahmen für Rechtsgeschäfte, bei denen entweder die bei Verwendung elektronischer Signaturen nur schlecht verwirklichte Warnfunktion eine große Bedeutung hat oder die auch schon beim traditionellen Geschäftsabschluß qualifizierteren Voraussetzungen der einfachen Schriftform unterliegen. Die taxative Aufzählung in § 4 Abs. 2 des SigG umfaßt folgende Rechtsgeschäfte:

- Rechtsgeschäfte des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind;
  Diese Ausnahme ist durch die besondere Sensibilität dieser Geschäfte gerechtfertigt. Vorallem im Familienrecht handelt es sich oft um Rechtsgeschäfte, die die vermögensrechtliche Stellung Minderjähriger betreffen. Hier ist die Vermeidung der elektronischen Kommunikation durchaus angebracht. Das SigG nutzt nicht einmal den ganzen Bereich, der durch Art. 9 Abs 2 der Richtlinie über elektronischen Geschäftsverkehr den nationalen Gesetzgebern zugestanden wird. Die Richtlinie ermöglicht generell den Ausschluß der Rechtsgeschäfte des Familien- und Erbrechtes. Im SigG sind aber nur Rechtsgeschäfte in diesem Bereich, die schon vor Einführung des SigG an die Schriftform gebunden waren, ausgenommen. Die Ausnahme erstreckt sich auch auf die Erstellung eines eigenhändigen Testaments.

---

[336] § 1346 Abs. 2 ABGB.
[337] § 2 Abs. 2 Z. 1 WEG.
[338] § 29 Abs. 1 Z. 3 MRG.
[339] § 26 GBG.
[340] § 3 Abs. 1 BTVG.
[341] §§ 33f BWG.

– andere Willenserklärungen oder Rechtsgeschäfte, die zu ihrer Wirksamkeit an die Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts gebunden sind;
Die Einbeziehung elektronisch signierter Dokumente erstreckt sich daher nur auf die einfache Schriftform. Die Gleichstellung der öffentlich beglaubigten Urkunden wurde bewußt noch ausgelassen, wird aber nach einem mittelfristigen Erprobungszeitraum und nach Berücksichtigung der gesammelten Erfahrungen zu überlegen sein. Die öffentliche Form ist durch die Mitwirkung eines Notars oder Gerichts definiert. Bei der Mitwirkung durch einen Notar kann man zwischen Notariatsakt gemäß §§ 2, 52ff NO und der notariellen Beurkundung nach § 76 NO unterscheiden. Ein solcher dient vor allem dazu, Willenserklärungen von Parteien eine besondere urkundliche Beweiskraft zu verleihen. Errichtung einer GmbH und Übertragung von GmbH-Anteilen, Urkunden über Rechtsgeschäfte unter Lebenden, welche von Blinden, die nicht lesen können, oder von Stummen, die nicht schreiben können, errichtet werden, Erbverzicht, Erbschaftskauf, Ehepakte, Kauf-, Tausch-, und Darlehensverträge unter Ehegatten, Schenkungsverträge ohne Übergabe und die Errichtung einer Privatstiftung bedürfen zum Beispiel der Form des Notariatsaktes.[342] Die Aufgabe des Notars ist es, bei Aufnahme des Notariatsaktes die Geschäftsfähigkeit der Partei und deren formelle Berechtigung zum Abschluß des Geschäftes zu prüfen.[343] Dies könnte eventuell noch den Angaben eines extensiven, qualifizierten Zertifikates entnommen werden. Weiters hat ein Notar aber auch den Willen der Parteien zu erforschen[344] und sie über die Auswirkungen ihrer Willenserklärung zu informieren.[345] Diese Beratungspflicht, die ein stark ausgeprägtes Element des Übereilungsschutzes verwirklicht[346], sprengt jedoch den Rahmen eines sinnvollen Einsatzes elektronischer Kommunikation, so daß es durchaus angepaßt ist, notariatsaktpflichtige Willenserklärungen vom Einsatz elektronischer Signaturen auszuschließen. Die Nichteinhaltung der gesetzlichen Formvorschriften führt zur Nichtigkeit des Rechtsgeschäftes.

---

[342] *Koziol/Welser*, Grundriß des Bürgerlichen Rechts[10], S. 151.
[343] *Wagner*, Notariatsordnung[4] § 52 Rz. 2.
[344] *Wagner*, Notariatsordnung[4] § 52 Rz. 8.
[345] *Wagner*, Notariatsordnung[4] § 76 Rz. 6f.
[346] *Bydlinski*, Die Notariatsaktpflicht 1850 und heute, NZ (1990), S. 289.

Andere Funktion hat die notarielle Beurkundung. Sie dient der Beurkundung der sich persönlich und unmittelbar vor dem Notar abspielenden Tatsachenfeststellungen und abgegebenen Wissenserklärungen.[347] Im Rahmen der Unterschriftsbeglaubigung bestätigt der Notar, daß die beglaubigte Unterschrift auch von einer bestimmten Person stammt. In der notariellen Praxis wird aber oft nicht direkt bei Anwesenheit des Notars unterschrieben, sondern ihm von seinem Büropersonal nur die unterschriebene Urkunde und ein Lichtbildausweis zum Nachweis der Identität vorgelegt. Auf Grund dieser Daten wird die Authentizität der Unterschrift dann von ihm beglaubigt. Besonders die Belehrungspflicht entfällt für diese Formkategorie. Man könnte also hier – eventuell nach Verstreichen einer Evaluierungsperiode – durchaus dem Vorschlag der Notariatskammer[348] folgen, die der Auffassung ist, daß sich dieser Ausschluß nicht auf die fakultative notarielle Beglaubigung von Unterschriften erstreckt. Doch könnten alle Rechtsgeschäfte, die nicht dem NZwG[349] unterworfen sind, trotzdem nicht notariell beurkundet werden, da die § 54 Abs. 2 NO in der gegenwärtigen Fassung für notarielle Beurkundungen der Echtheit einer Unterschrift oder in Zukunft einer sicheren elektronischen Signatur nur die eigenhändige Unterschrift vorsieht.[350] Die Stellungnahme kommt daher zu der Schlußfolgerung, daß das derzeitige notarielle Instrumentarium im Bereich der elektronischen Dokumente durch die „textliche, sicher elektronisch signierte, notarielle Urkunde, die mit einer sicheren elektronischen Signatur samt Hinweis auf die notarielle Berechtigung des Notars versehen ist", zu erweitern sei.

Beglaubigungen der Kanzleien in Verwaltungsbehörden im Sinne der Beglaubigungsverordnung[351] fallen nicht unter die Ausnahmebestimmung des § 4 Abs. 2 Z. 2. Sie dienen nur der Beglaubigung für die Richtigkeit der Ausfertigung. Soweit entsprechende Infrastrukturen vorhanden sind, können hier elektronische Signaturen eingesetzt werden.

---

[347] *Wagner*, Notariatsordnung[4] § 76 Rz. 1.

[348] Stellungnahme der Notariatskammer zur RV SigG, GZ 214/99, Wien 4.6.1999.

[349] Notariatsaktsgesetz, Gesetz vom 25. Juli 1871, RGBl. Nr. 76, betreffend das Erfordernis der notariellen Errichtung einiger Rechtsgeschäfte.

[350] *Wagner*, Notariatsordnung[4] § 54 Rz. 15.

[351] BGBl.Nr. 445/1925, Verordnung der Bundesregierung vom 28. Dezember 1925 über die Beglaubigung der schriftlichen Ausfertigungen der Verwaltungsbehörden durch die Kanzlei. StF: BGBl. Nr. 445/1925.

- Willenserklärungen, Rechtsgeschäfte 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;
  Eintragungen in öffentliche Bücher führen zu einer besonderen Verfestigung der eingetragenen Rechte, wie zum Beispiel das Eigentum an einer Liegenschaft. Dies kann bei falschen Eintragungen aber auch zu stärkeren Nachteilen führen. Der eigentlich Berechtigte, aber nicht Eingetragene kann sein Recht gegen den Eingetragenen auf Grund des Vertrauensgrundsatzes schwerer durchsetzen. Diese Tatsache berücksichtigend nimmt das SigG auch diese Willenserklärungen von der elektronischen Kommunikation unter Verwendung sicherer elektronischer Signaturen aus. Hier zieht der österreichische Gesetzgeber analog zur Bestimmung über Schriftform von Rechtsgeschäften des Familien- und Erbrechtes den Kreis der ausgeschlossenen Willenserklärungen enger, als es Art. 9 Abs. 2 der Richtlinie über elektronischen Geschäftsverkehr fordert, da ebenfalls nur Willenserklärungen, Rechtsgeschäfte und Eingaben ausgeschlossen sind, die schon vor Inkrafttreten des SigG der öffentlichen Form bedurften. Fraglich ist nur der Sinn der Wiederholung dieser Ausnahmeregelung, da ja schon durch § 4 Abs. 2 Z. 2 alle Willenserklärungen, die zu ihrer Wirksamkeit an die öffentliche Form gebunden sind, ausgenommen werden. Auch Einbringen zur Eintragung in ein öffentliches Register werden dadurch miterfaßt. Dadurch ist eine explizite, eigene Regelung mE nicht mehr nötig.
- Bürgschaftserklärungen von Nicht- und Minderkaufleuten gemäß § 1346 Abs. 2 ABGB
  Der Ausschluß der Rechtswirkung elektronisch signierter Bürgschaften wird allerdings schon in den neuesten Besprechungen[352] kritisiert, es wird gefordert, daß auch dieses Rechtsgeschäft mit den Mitteln der sicheren elektronischen Signatur abgeschlossen werden kann. Das Formgebot der Schriftlichkeit soll den Bürgen vor Übereilung schützen, da er mit der Bürgschaft für die Schulden eines Dritten ein hohes Risiko eingeht. Durch die Warnfunktion der Unterschrift soll dieser Schutz gewährleistet sein. Warum diese Warnfunktion in Bezug auf die Abgabe von Bürgschaften durch die elektronische Signatur nicht

---

[352] *Jud/Högler-Pracher*, Die Gleichsetzung elektronischer Signaturen mit der eigenhändigen Unterschrift, ecolex (1999), S. 610.

gewährleistet ist, wird in den Erläuterungen zum SigG nicht näher ausgeführt. Offenbar geht der Gesetzgeber aber davon aus, daß elektronische Signaturen sehr schnell, vielleicht sogar automatisiert den versendeten Nachrichten beigefügt werden. Dann wäre die Ausnahmebestimmung über elektronisch signierte Bürgschaften sinnvoll und angebracht. Die Version einer „Verbürgung durch Mouse-Click“[353], vielleicht beim nur flüchtigen Besuch einer WWW-Seite, soll natürlich keine Rechtswirksamkeit erlangen können. Doch spricht vieles dafür, daß elektronische Signaturen auch in einer Art eingesetzt werden können, daß sie eine für die Verbürgung ausreichende Warnfunktion vermitteln. Wenn der Zertifizierungsdiensteanbieter genügend Informationsarbeit gegenüber seinen Antragstellern leistet, zu der er ja durch § 20 verpflichtet ist, und die Anwender Signaturerstellungseinheiten verwenden, die bei der Abgabe der Signatur die Aufmerksamkeit des Signators erfordern, kann durchaus das Rechtsgeschäft der Bürgschaft für die elektronische Signatur zugänglich gemacht werden.

Willenserklärungen und Rechtsgeschäfte, die als elektronisch signierte Dokumente vorliegen, erfüllen aber auch die Anforderungen der vertraglich vereinbarten Schriftform und gelten grundsätzlich im öffentlichen Bereich, wobei der Wunsch besteht, für den behördlichen elektronischen Schriftverkehr eine erweiterte Ermächtigung für den öffentlichen Bereich vorzusehen, damit die betroffenen Institutionen das Recht haben, zusätzliche qualitative Anforderungen zu stellen.

5.3.2. Beweiswert elektronisch signierter Dokumente

5.3.2.1. Im Zivilgerichtlichen Verfahren vor den ordentlichen Gerichtshöfen

Die Beweisregeln der Zivilprozeßordnung stellen im Gegensatz zu den Regeln der einfachen Schriftform nicht (nur) auf die Unterschrift ab, die ja durch die SigRL und das SigG mit sicheren elektronischen Signaturen gleichgestellt sind. Die ZPO regelt den Beweiswert von Urkunden und umfaßt ohne Erweiterung ihres Anwendungsbereiches durch Bestimmungen des SigG nur Urkunden, die aus einem festen Trägermaterial

---

[353] *Brenn*, Verbürgung durch mouse-click? ecolex (1999), S. 243.

bestehen[354], da es sich um schriftliche Verkörperungen von Gedanken[355] handelt. Damit sind alle anderen Aufzeichnungsformen, wie Schallplatten, Lochkarten[356] und eben elektronisch signierte Dokumente generell nicht vom Urkundenbegriff der ZPO umfaßt. Durch das SigG werden generell ausschließlich sichere elektronische Signaturen der eigenhändigen Unterschrift gleichgestellt. Dadurch erfüllen aber in Österreich im allgemeinen[357] sicher elektronisch signierte Dokumente die Anforderungen der Schriftform, die ja gemäß § 886 ABGB durch das Anbringen der eigenhändigen Unterschrift definiert ist. Die Gleichstellung von sicherer elektronischer Signatur und eigenhändiger Unterschrift gewährleistet dies.

Anders ist die Rechtslage im Beweisrecht ausgestaltet. Hier wird nicht nur auf die eigenhändige Unterschrift abgestellt, der Beweis durch Privaturkunden setzt voraus, daß den Urkunden die Funktion der Verkörperung eines Gedankens durch die menschliche Tätigkeit zukommt. Der Begriff der Urkunde wird zwar in der ZPO nicht definiert, doch ergibt sich aus den Vorschriften über den Urkundenbeweis folgende Begriffsbestimmung der Urkunde für den Zivilprozeß: Urkunden sind Schriftstücke, also Aufzeichnungen von Gedanken in Form der menschlichen Schrift, die im Regelfall Tatsachen festhalten.[358] Damit fallen einfache und sicher signierte elektronische Dokumente ohne gesetzliche Erweiterung des zivilprozeßrechtlichen Urkundenbegriff nicht in den Bereich der Privaturkunden, sondern müssen nach den Regeln des Augenscheins vom Gericht behandelt werden.

Wurde in den ersten Versionen des Art. 5 Abs. 1 SigRL[359] auch für das Gerichtsverfahren noch die Gleichstellung fortgeschrittener elektronischer Signaturen, die auf einem qualifizierten Zertifikat beruhen, mit eigenhändigen Unterschriften festgesetzt, so fand diese Bestimmung im Telekommunikationsrat keinen Konsens bei den Vertretern der Mitgliedsstaaten. Als Kompromiß wurde im gemeinsamen Standpunkt nur mehr festgelegt, daß elektronische Signaturen in Gerichtsverfahren als Be-

---

[354] Die Urkunde muß daher nicht unbedingt aus Papier bestehen, auch Verkörperungen von Gedanken auf Metall, Holz, Plastik, Tontafeln oder anderem Trägermaterial erfüllen den Begriff der Privaturkunde. Elektronisch gespeicherte Daten gelten aber nach der Rechtslage vor dem SigG nicht als Privaturkunden.

[355] *Rechberger*, ZPO Vor § 292 Rz. 10.

[356] *Fasching*, Zivilprozeßrecht[2] Rz. 944.

[357] Die Rechtsgeschäfte, Willenserklärungen und Anbringen, die durch § 4 Abs. 2 ausgeschlossen sind, müssen aber weiterhin in konventioneller Form übermittelt werden.

[358] *Fasching*, Lehrbuch des österreichischen Zivilprozeßrechts[2], S. 494.

[359] KOM (1998) 297.

weismittel zugelassen werden müssen. Es wird aber europarechtlich nicht mehr gefordert, daß sicher elektronisch signierte Dokumente im Beweisverfahren den Privaturkunden gleichzustellen sind.

Das SigG erweitert durch § 4 Abs. 3 allerdings nicht die Anwendbarkeit aller Bestimmungen über die Beweiskraft von Privaturkunden auch auf elektronisch signierte Dokumente, sondern erklärt auf Grund mangelnder Erfahrungswerte im Umgang mit elektronisch signierten Dokumenten nur jene einzelne Bestimmung des § 294 ZPO anwendbar, die normiert, daß in Privaturkunden enthaltene Erklärungen von dem Aussteller herrühren, sofern die Urkunden von diesem unterschrieben sind. Es wird also nur eine qualifizierte Echtheitsvermutung für den Erklärungsinhalt angeordnet. Diese Vorschrift setzt allerdings voraus, daß die Signatur echt ist.[360, 361] Insbesondere ist die Regelung[362], in der die Echtheit der Unterschrift vermutet wird[363], solange der Gegner des Beweisführers diese nicht bestreitet, auf elektronisch signierte Dokumente nicht anwendbar. Diese Regelung in § 312 ZPO begründet aber nicht nur die Vermutung über die Echtheit des Inhalts, sondern auch eine Vermutung der Echtheit der Unterschrift, solange dies vom Prozeßgegner nicht bestritten wird.[364] In den Erläuterungen wird ausgeführt, warum von der widerlegbaren Vermutung, daß die Signaturerstellungseinheit vom Signator verwendet wurde, doch nicht in das SigG aufgenommen wurde. Diese Regelung würde zu einer Besserstellung sicherer elektronischer Signaturen gegenüber der eigenhändigen Unterschrift führen. Diese Ausführungen sind mE nicht richtig, da ja ebenfalls eine Erklärung der Anwendbarkeit von § 312 für sicher elektronisch signierte Dokumente durch § 4 Abs. 3 normiert werden könnte. Die Echtheit der sicheren elektronischen Signatur würde dann ebenfalls nur vermutet werden, falls dies durch den Prozeßgegner nicht bestritten wird. Es würde sich also nur um eine Gleichstellung, aber keinenfalls um eine Besserstellung handeln.

Für eine derartige Maßnahme reichen die Erfahrungen mit dem Umgang sicherer elektronischer Signaturen im Beweisverfahren noch nicht aus. Das SigG differenziert daher bezüglich ihres Vertrauens in die aus-

---

[360] *Fasching*, Kommentar zu den Zivilprozeßgesetzen, Bd. III, S. 379.

[361] *Brenn*, Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet, ÖJZ (1997), S. 641.

[362] *Fasching*, Kommentar zu den Zivilprozeßgesetzen, Bd. III, S. 400.

[363] Falls der Beweisgegner die Echtheit einer vom Beweisführer vorgelegten Privaturkunde nicht bestreitet, gilt die Vermutung der Echtheit, d. h. daß die Identität des Ausstellers mit der Unterschrift übereinstimmt.

[364] *Rechberger*, ZPO § 312 Rz. 2.

reichende Gewährleistung der unterschiedlichen Funktionen einer eigenhändigen Unterschrift durch sichere elektronische Signaturen. Es setzt bezüglich der Wahrung der Authentizität elektronisch signierter Dokumente Vertrauen in die neue Technologie, steht aber der Verwirklichung korrekter Identifikation durch sichere elektronische Zertifikate skeptischer gegenüber. Dies ist durchaus begründet, da der elektronischen Signatur ohne biometrische Verifikation der Identität des Signators in diesem Punkt eben nicht gleiche Funktionalität wie der eigenhändigen Unterschrift zukommt. Durch Eigentümlichkeiten des Schriftzuges ist der Unterschrift eine biometrische Kontrolle inhärent, die Berechtigung zur Verwendung der Signaturerstellungseinheit kann aber weitergegeben werden. Dies ist zwar durch die Bestimmung des § 21 im SigG untersagt und wird auch bei Verwendung fremder Signaturerstellungseinheiten ohne Wissen und Willen des Signators[365] durch § 26 Abs. 1 mit einer Verwaltungsstrafe bis ATS 56.000.- sanktioniert, kann aber faktisch jederzeit durchgeführt werden und wird auch angewandt, wie Simulationsstudien[366] belegen. Durch die Verwendung digitaler Daten ist es nicht zu unterscheiden, ob der Zertifizierte oder ein anderer für ihn unterschreibt.

Durch diese Beschränkung der Anwendung der Beweisregeln für klassische Privaturkunden ist es für den Beweisführer daher notwendig, den Richter im Rahmen der freien Beweiswürdigung von der Identität der im Zertifikat angegebenen Person mit dem echten Autor des sicher elektronisch signierten Dokuments zu überzeugen. Sollte die Identität nicht außer Streit gestellt werden[367], bedarf es der Beweisführung durch Aufzeichnungen von Seiten des Zertifizierungsdiensteanbieters. Wird sie aber nicht außer Streit gestellt, jedoch trotzdem vom Prozeßgegner nicht bestritten, muß weiterhin über die Authentizität des Signators ein Augenscheinsbeweis[368] erbracht werden. Wahrscheinlich werden auch im jeweiligen Verfahren individuelle Gutachten über die Sicherheit der strittigen elektronischen Signatur eingeholt werden müssen. Die sichere elek-

---

[365] Widersprüchlicherweise verbietet zwar § 21 jegliche Weitergabe der Signaturerstellungsdaten, doch wird nur die Verwendung fremder Signaturerstellungsdaten ohne Wissen und Willen des Signators sanktioniert. Die Weitergabe durch den Signator wird daher vom Gesetzgeber konkludent geduldet.

[366] *Pordesch/Roßnagel/Schneider*, Erprobung sicherheits- und datenschutzrelevanter Informationstechniken mit Simulationsstudien, DuD 9 (1993), S. 491.

[367] *Rechberger/Simotta*, Grundriß des österreichischen Zivilprozeßrechts[4], S. 312.

[368] Zumindest anfänglich bedeutet dies sicher auch die Zuziehung eines Sachverständigen in jedem einzelnen Fall, wodurch Prozeßkosten und Prozeßzeit größer werden.

tronische Signatur ist also in Bezug auf die Identitätsfunktion[369] dem nicht signierten, unsicher übertragenen elektronischen Dokument gleichgestellt. Erst wenn der Beweis der Identität gelungen ist, gilt für den Beweis der Authentizität die Erleichterung für den Beweisführer, daß voller Beweis durch Vorlage der sicher elektronisch signierten Dokumente begründet wird.

Wie umstritten die Beweisqualität sicherer elektronischer Signaturen bezüglich der korrekten Identifizierung ist, zeigt sich auch daran, daß § 4 Abs. 3 des SigG die Gleichstellung sicher elektronisch signierter Dokumente mit Privaturkunden erst in der letzten Version auf die Authentizität beschränkt hat. In den vorherigen Versionen des SigG begründete eine sichere elektronische Signatur noch die Vermutung, daß die Signaturerstellungsdaten vom Signator verwendet wurden.[370] Diese Vermutung wurde auf Anregung der Gerichtsbarkeit[371] gestrichen.

Es bleibt zu hoffen, daß das österreichische Zivilprozeßrecht[372], welches bisher der elektronischen Kommunikation und der Verwendung des elektronischen Grundbuches und Firmenbuches gegenüber sehr aufgeschlossenen ist, auch die beweisrechtliche Stellung sicherer elektronischer Signaturen in hohem Maße anerkennt. So besteht die Möglichkeit der auswärtigen Abfrage unter Verwendung des elektronischen Rechtsverkehrs schon seit 1994, allgemein wurde der elektronische Rechtsverkehr überhaupt schon 1990 durch §§ 89a ff GOG eingeführt. Die Verwendung der – allerdings bis jetzt nur in geschlossenen Netzen abgewickelten – elektronischen Kommunikation bei Gericht und zwischen Richtern und Anwälten sollte auch Einfluß auf die beweisrechtliche Würdigung der elektronischen Kommunikation zwischen den Parteien haben.

5.3.2.2. Rechtslage in Deutschland

In Deutschland will man ebenfalls eher restriktiv vorgehen und sicher elektronisch signierte Urkunden vorläufig nicht generell mit den Privaturkunden gleichsetzen. Auch der Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts an den modernen Geschäftsverkehr

---

[369] Nähere Ausführungen zur Identitätsfunktion: *Menzel/Schweighofer*, Securing Electronic Commerce with Digital Signatures, Proceedings zur BILETA Konferenz 1999, http://www.bileta.ac.uk/99papers/menzel.htm.

[370] Sicher elektronisch signierte Dokumente wären also beweisrechtlich den Privaturkunden vollkommen gleichgestellt.

[371] Stellungnahme des OGH zur RV SigG.

[372] *Britz*, Urkundenbeweisrecht und Elektroniktechnologie, S. 74.

geht einen Schritt weiter und führt durch eine Novellierung der betroffenen Bestimmungen der dZPO zwei neue Rechtsvermutungen ein. Zum einen wird vermutet, daß eine Erklärung in elektronischer Form vom Signaturschlüssel-Inhaber abgegeben worden ist. Zum anderen besteht die Vermutung, daß ein Dritter, der die Erklärung mit dem privaten Schlüssel des Signaturschlüssel-Inhabers abgegeben hat, von diesem bevollmächtigt war.

Bestreitet der Beweisgegner die Echtheit der in elektronischer Form dokumentierten Erklärung, obliegt es grundsätzlich ihm, zur Überzeugung des Gerichts darzulegen und zu beweisen, daß die Erklärung nicht vom Inhaber des Signaturschlüssels abgegeben worden ist. Damit gewährleisten die Vermutungsregeln nach Ansicht des Gesetzgebers einen weitergehenden Schutz des Erklärungsempfängers, als es die Vorschriften der dZPO über den Beweis durch Schrifturkunden vermögen, da nach diesen eine entsprechende Verlagerung der Beweislast nicht eintritt, sondern der Erklärungsempfänger die Echtheit einer von dem Beweisgegner nicht anerkannten Namensunterschrift beweisen muß.

Auffällt, daß in Deutschland genau die andere Funktion der Signatur mehr Vertrauen findet. So führt diese Vermutung zu einer besseren Position im Verfahren bezüglich der Identitätsfunktion, wobei in Österreich diese Vermutung nicht festgelegt wurde mit der Begründung, daß genau hier noch zuwenig Erfahrung im praktischen Einsatz bestehe. Andererseits ist in Österreich die gesetzliche Vermutung über die Integrität elektronisch signierter Dokumente auch auf elektronisch signierte Dokumente anwendbar, die im deutschen Entwurf aber nicht eingeführt wurde.

Stark zu kritisieren ist die Vermutung über die Vollmacht eines faktischen Signators, der nicht Inhaber des privaten Signaturschlüssels ist. Das ganze System der Public Key Infrastructure ist (sowohl in Deutschland als auch in Österreich) darauf ausgestellt, daß einzig und allein der berechtigte Inhaber, der mit seinem Namen im Zertifikat erwähnt ist und eine natürliche Person sein muß, seinen privaten Signaturschlüssel verwendet. So ist es auch nach Auffassung des Fachverbandes für Informationstechnik im VDMA und ZVEI eine Kernvoraussetzung für eine branchen- und anwendungsübergreifende digitale Identität bezüglich Geschäfte und Kommunikation in weltweiten Netzen, daß sich die digitale Identität nur auf natürliche Personen bezieht. Sie stellt ein digitales Pedant zu einem konventionellen Ausweis dar, welches die sichere Authentifizierung einer

Person in der virtuellen Welt erlaubt.[373] Im Rahmen der Stellvertretung muß systemimmanent daher der Stellvertreter mit seinem eigenen Namen und Signaturschlüssel in Vertretung signieren. Auch im traditionellen Bereich bei Verwendung eigenhändiger Unterschrift macht der Stellvertreter ja nicht den Namenszug des Vertretenen nach, sondern zeichnet mit seinem eigenen Namen in Vertretung.

Über die Einfügung dieser zwei Vermutungen hinaus sieht der Entwurf kein Bedürfnis für eine Änderung oder Ergänzung der prozeßrechtlichen Beweisvorschriften. Man ist der Auffassung, daß das deutsche Prozeßrecht im Unterschied zu dem Recht anderer Staaten keine Einschränkungen, die eine Beweisführung mit Hilfe elektronischer Dokumente in irgendeiner Weise behindern, kennt. Eine solche fällt in die Kategorie der Vorschriften über den Beweis durch Augenschein, der als besonders zuverlässiges Beweismittel bewertet und empfohlen wird.

5.3.2.3. Im Schiedsgerichtsverfahren

Anders gestaltet sich die Lage im Schiedsgerichtsverfahren. Auf Grund der raschen, weitgehend formfreien und in großen Teilen dispositiven Gestaltung des Schiedsgerichtsverfahrens erfreut es sich im Bereich der EDV großer Beliebtheit.[374] In den meisten EDI[375] Rahmenverträgen wird im Streitfall die Austragung vor einem Schiedsgericht vereinbart.

Durch die Zivilverfahrensnovelle 1983 wurde § 577 Abs. 3 ZPO insoweit an die internationale Entwicklung[376] angepaßt, als entsprechend dem UN-Übereinkommen[377] und dem Europäischen Übereinkommen[378] der Passus hinzugefügt wurde, daß Schiedsverträge auch in Telegrammen und Fernschreiben[379, 380] enthalten sein können, die die Parteien gewech-

---

[373] *Welsch*, Stufenweise skalierbare Sicherheit für digitale Signaturen, DuD (1999), S. 520.

[374] *Hytha*, Schlichten statt streiten? Vor- und Nachteile von EDV-Schiedsgerichten, EDV und Recht (1988), S. H 3,2.

[375] *Kilian*, Möglichkeiten und zivilrechtliche Probleme eines rechtswirksamen elektronischen Datenaustauschs (EDI).

[376] Dazu näher: *Fasching*, Die Form der Schiedsvereinbarung – Schriftform und neu zugelassene technisch bedingte Übermittlungsformen (§ 577 Abs 3 ZPO), ÖJZ (1989), S. 289.

[377] Übereinkommen vom 10. 6. 1958 BGBl 1961/200 über die Anerkennung und Vollstreckung ausländischer Schiedssprüche.

[378] Europäisches Übereinkommen vom 21.4.1961 BGBl 1964/107 über die internationale Handelsschiedsgerichtsbarkeit.

[379] *Rechberger*, ZPO § 577 Rz. 12.

selt haben.[381] Auf das Unterschriftserfordernis wird vollständig verzichtet. Schiedsverfahren können also auf Grund sicherer elektronisch signierter Dokumente rechtswirksam und bindend vereinbart werden.

Auch die Möglichkeiten für die Abwicklung des Schiedsgerichtsverfahren kommen der Einbeziehung sicherer elektronischer Signaturen in die elektronischen Signaturen zu Gute. Da insbesondere die Mündlichkeit und Unmittelbarkeit nicht zwingend vorausgesetzt sind, kann das Verfahren unter alleiniger Verwendung sicher elektronisch signierter Dokumente abgewickelt werden. Die beweis- und verfahrensrechtliche Gleichstellung dieser Dokumente mit Privaturkunden unterliegt der freien Vereinbarung der Parteien, solange die Identität und die Authentizität der Mitteilung gewährleistet sind. Da für die Klarstellung der Identität im Schiedsgerichtsverfahren schon die Telegrammadresse oder ein Codewort ausreicht, kommen Jud und Högler-Pacher[382] zu dem Schluß, daß zwar der Abschluß von Schiedsvertägen per (einfacher) E-Mail wegen der fehlenden Übermittlungssicherheit dieses Kommunikationsweges nicht den Anforderungen entspricht, die Verwendung einer sicheren elektronischen Signatur beim Abschluß des Schiedsvertrages aber die völlige Gleichstellung der Rechtswirkungen mit jenen eines eigenhändig unterschriebenen Schiedsvertrags gemäß ermöglicht. Auch die Prozeßhandlungen der Parteien und die Unterfertigung des Schiedsspruches können auf Grund der weiten Dispositivität der gesetzlichen Regelungen über das Schiedsverfahren durch sicher signierte elektronische Kommunikation durchgeführt werden.

5.3.3. Elektronisch signierte Dokumente im Behördenverkehr

Das SigG gilt gemäß § 1 Abs. 2 grundsätzlich auch im öffentlichen Bereich zum Rechtsverkehr mit Behörden und Gerichten. Art. 3 Abs. 4 SigRL ermöglicht es aber den Mitgliedsstaaten, an die sichere elektronische Kommunikation in diesem Bereich zusätzliche Anforderungen zu stellen. Im SigG selbst sind zwar keine besonderen Regelungen für den Verwaltungsbereich vorhanden, doch müssen die schon bestehenden Vorschriften für den elektronischen Verkehr mit den Verwaltungsbehörden

---

[380] *Fasching*, Die Form der Schiedsvereinbarung, Schriftform und neu zugelassene technisch bedingte Übermittlungsformen (§ 577 Abs 3 ZPO), ÖJZ (1989), S. 289.

[381] *Jud/Högler-Pracher*, Schiedsverfahren mit modernen Kommunikationstechniken, ecolex (1999), S. 601.

[382] Siehe oben.

beachtet werden. Im privaten Bereich gilt grundsätzlich, daß die technische Ausstattung zur sicheren elektronischen Kommunikation vorhanden sein muß. In Übereinstimmung mit § 13 AVG ist dies nur nach Maßgabe der zur Verfügung stehenden technischen Mittel möglich. Gemäß § 3 Abs. 1 ist die Regelung des Zugangs eines sicher signierten elektronischen Dokuments aber nicht Gegenstand des SigG, sondern bleibt der Umsetzung des Entwurfs für eine Richtlinie über bestimmte Aspekte des elektronischen Geschäftsverkehrs vorbehalten.

Da jedoch die sichere elektronische Signatur generell die Schriftform erfüllt und Verwaltungsanbringen nach § 4 Abs. 2 nicht davon ausgenommen sind, kann man davon ausgehen, daß nicht nur allgemeine Anbringen gemäß § 13 Abs. 1 AVG, sondern auch jene Anbringen, die an eine Frist gebunden sind und nach § 13 Abs. 2 AVG schriftlich eingebracht werden müssen, in Form sicher elektronisch signierter Dokumente an die Behörde elektronisch rechtskräftig übermittelt werden können. Dementsprechend kann die Behörde dann auch bei der Verwendung elektronischer Erledigungen gemäß § 18 Abs. 3 AVG die neue Infrastruktur zur Zustellung einsetzen.

Bezüglich der Beweiskraft von öffentlichen und Privaturkunden im Verwaltungsverfahren verweist § 47 AVG auf die Bestimmungen in der Zivilprozeßordnung, die auch in Verwaltungsverfahren anzuwenden sind. Da § 4 Abs. 3 SigG die Bestimmung des § 294 ZPO für sicher elektronisch signierte Dokumente anwendbar erklärt, gilt das oben Angeführte zur Beweiswirkung sicher elektronisch signierter Dokumente auch im Verwaltungsverfahren. Allerdings wird im SigG ausdrücklich nur von Privaturkunden gesprochen. Öffentliche Urkunden in der Form von sicher elektronisch signierten Dokumenten sind daher noch nicht möglich.

Die Möglichkeit des Einsatzes elektronischer Signaturen wurde im öffentlichen Bereich gerade zum richtigen Zeitpunkt realisiert, da viele Projekte im Bereich des Electronic Government durch die Möglichkeit des Einsatzes sicherer elektronischer Signaturen überhaupt erst ermöglicht werden. Auf europäischer Ebene wird diese Entwicklung durch die Impulse des Grünbuches der Europäischen Kommission über die Information des öffentlichen Sektors in der Informationsgesellschaft[383] vorangetrieben. „help.gv.at", das Projekt[384] der österreichischen Bundesregierung in diesem Bereich, genießt international hohes Ansehen. Können bis zum Inkrafttreten des SigG in der Projektphase @mtshelfer online nur

---

[383] KOM (1998) 585.

[384] Help.gv.at = @mtshelfer online ist im Internet unter: http://www.help.gv.at/ präsent.

Formulare zum Download und Ausdrucken angeboten werden, ist in nächster Zukunft auch die Realisierung der Stellung eines Antrages (@ntrag online) und darauf folgend die komplette Abwicklung des Amtsweges über das Internet (@mtsweg online) geplant. Für den zweiten Schritt, spätestens aber für die Realisierung der Endausbaustufe, ist die Einbeziehung sicherer elektronischer Signaturen auf Grund ihrer nach neuer Rechtslage besonderen Rechtswirkungen unbedingt erforderlich und von den Projektverantwortlichen vorgesehen.

Neben dem Einsatz bei „help.gv.at" werden die folgenden Bereiche als vordringliche Anwendungsfelder für elektronische Signaturen im Verwaltungsbereich gesehen:[385]

- Öffentliche Ausschreibungen
- Steuerverwaltung
- Meldewesen
- Kraftfahrzeugverwaltung
- Genehmigungsverfahren
- Online-Mitwirkung bei kommunalen Planungs- und Entscheidungsprozessen

[385] *Aichholzer/Schmutzer*, Bericht/Information E-Government – Elektronische Informationsdienste auf Bundesebene in Österreich, Studie im Auftrag des Bundeskanzleramtes (1999), S. 80.

6. Die Situation in anderen Rechtsordnungen

Das Internet, der darüber abgewickelte elektronische Geschäftsverkehr und – als Hilfsmittel damit verbunden – die elektronischen Signaturen kennen keine nationalstaatlichen Grenzen, und sie reichen auch über die Grenzen der regionalen Wirtschaftsräume. Besonders bei rechtserheblichen Geschäften im Internet ist der Jurist aufgefordert, die einschlägigen Quellen des Völkerrechts und die anderen innerstaatlichen Regelungen zu betrachten. Der Marktplatz Internet ermöglicht nur schrankenlose Geschäfte[386], wenn auch die Rechtsordnungen der einzelnen Staaten über die Harmonisierung im Raum der Europäischen Union hinaus durch Internationale Übereinkünfte aufeinander abgestimmt werden. Ein Blick auf diese Übereinkünfte und die innerstaatlichen Regelungen einzelner ausgewählter Staaten soll im Anschluß vorgestellt werden.[387] Die Harmonisierungsvorstellungen der Europäischen Kommission für den Europäischen Wirtschaftsraum und die Regelungen in Deutschland werden hier nicht mehr extra angeführt, da sie bei den jeweiligen Kapiteln innerhalb der vorliegenden Arbeit berücksichtigt und erläutert wurden. Auch bezieht sich dieser Teil hauptsächlich auf die Regelung rechtlicher Aspekte, da die technischen Normierungen und Standards, die sich innerhalb der einzelnen Länder kaum unterscheiden, allgemein im zweiten Teil behandelt wurden.

6.1. UNCITRAL: Uniform Rules on Electronic Signatures und Model Law on Electronic Commerce

Seit 1992 beschäftigt man sich auch auf völkerrechtlicher Ebene mit den Problemen des elektronischen Geschäftsverkehr und elektronischer Signaturen. Die United Nations Commission on Interbational Trade Law

---

[386] *Jaburek/Wölfl*, Cyber-Recht, Marktplatz Internet – schrankenlose Geschäfte, S. 95.

[387] Neben den Materialien der UN waren der Digital Signature Law Survey von Van der Hof (http://cwis.kub.nl/~frw/people/hof/DS-lawsu.htm) und die Gespräche mit Prof. *Andresen* (Universität Kopenhagen, Dänemark, Chairman der UNCITRAL Working Group on Electronic Commerce), Prof. *Bing/Risnes* (NRCCL, Norwegen), Prof. *Cabell* (MIT, USA), Prof. *Dumortier/van Eecke* (Universität Leuven, Belgien), Prof. *Galindo* (Universität Zaragoza, Spanien) sehr hilfreich für die Einblicke in die Regelungen außerhalb Österreichs.

UNCITRAL setzte damals eine Arbeitsgruppe ein, die Lösungen für den Bereich entwickeln soll. Sie trifft sich zwei Mal jährlich in Wien und New York an den Amtssitzen der UNCITRAL zu jeweils zweiwöchigen Besprechungen. Die bis heute letzte Sitzung fand vom 5. bis 19. 2. 1999 in Wien statt.

Im Gegensatz zu den europäischen Regelungen beschäftigte sich die Gruppe zuerst mit den allgemeinen Fragen des elektronischen Geschäftsverkehrs. 1996 wurde ein von der Arbeitsgruppe erstelltes Model Law on Electronic Commerce[388] (im folgenden kurz als Model Law bezeichnet) von UNCITRAL angenommen. Es ist authentisch in den Sprachen Arabisch, Chinesisch, Englisch, Französisch, Russisch und Spanisch. Erst unmittelbar danach begann die Gruppe mit den Arbeiten an den Draft Uniform Rules on Electronic Signatures[389] (im folgenden kurz als Uniform Rules bezeichnet). Die Arbeit an den Uniform Rules ist noch nicht abgeschlossen, so daß der Text noch nicht von UNCITRAL angenommen wurde.

Im Art. 5 des Model Law wird festgelegt, daß einer Datennachricht generell die Rechtswirkung nicht abgesprochen werden darf, nur weil sie eine solche ist, also in elektronischer Form vorliegt. Mittels dieser Datennachrichten haben die Rechtsunterworfenen nach Art. 11 Model Law die Möglichkeit, Verträge durch die Abgabe von Angebot und Annahme in Form der Datennnachrichten elektronisch abzuschließen. Die Schriftform gilt als eingehalten, wenn auf die Information der Nachricht zugegriffen werden kann und sie als Referenz verwendbar ist. Verlangt das Gesetz die Schriftform, dann gilt das gemäß Art. 7 für die Datennachricht unter der Bedingung, daß eine Methode verwendet wird, die den Sender identifiziert und die Zustimmung des Senders zum Inhalt der Nachricht verdeutlicht. Genauer bezieht sich das Model Law nicht auf elektronische Signaturen nicht. Die Erläuterungen zu Art. 7 gehen von einem funktionalen Verständnis der Signaturen aus. Weitere Regelungen sollen nicht ins Model Law aufgenommen werden, sondern außerhalb geregelt werden.

Die Uniform Rules gliedern sich in der aktuellen Version in 3 Blöcke:

- Generelle Bestimmungen und Anwendungsbereich
- Regeln über elektronische Signaturen

---

[388] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996, http://www.uncitral.org/english/texts/electcom/ml-ec.htm.

[389] UNCITRAL Draft Uniform Rules on Electronic Signatures, Version vom 23. Nov 1998, A/CN.9/WG.IV/WP.79, http://www.uncitral.org/english/sessions/wg_ec/wp-79.htm.

– Bestimmungen über Zertifizierungsdiensteanbieter

Diskussionsansatz sind nunmehr sehr allgemein formulierte Bestimmungen, die dem Grundsatz der media neutrality Genüge tun und eine Anwendung auf alle möglichen und unmöglichen, gegenwärtigen und zukünftigen technischen Systeme erlauben.[390]

In Art. 1 wurde folgende Definition für elektronische Signaturen gewählt: „Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, and [that may be] used to [identify the signer of the data message and indicate the signer's approval of the information contained in the data message][satisfy the conditions set forth in article 7(1)(a) of the UNCITRAL Model Law on Electronic Commerce];"

Ebenfalls werden (einfache) elektronische Signaturen und fortgeschrittene elektronische Signaturen unterschieden, wobei letztere fast gleichlautend wie in der SigRL definiert sind.

Über die SigRL hinausgehend, kannten die Uniform Rules aber sehr wohl auch zwei weitere Definitionsvarianten, die spezifisch auf die Verwendung asymmetrischer Kryptographie zugeschnitten sind und digitale Signaturen auf der Grundlage der Verwendung von öffentlichem und privatem Schlüssel festlegen.

In weiterer Folge werden die Begriffe Zertifizierungsstellen, Zertifikate, Zertifizierungskonzept und Unterzeichner vorgestellt, wobei auch die Uniform Rules offenlassen, ob der Unterzeichner eine natürliche Person sein muß oder auch eine juristische Person sein kann.

Auf Grund eines Vorschlags der Vereinigten Staaten[391], die mit der Version, die vor Juli 1998 Gegenstand der Verhandlungen war, nicht einverstanden waren, da dieser Draft zu theoretisch sei und zu wenig Raum für vertragliche Vereinbarungen der Parteien zulasse, wurde ein Vorschlag für eine neue Fassung im Rahmen einer informellen Expertensitzung von neunzehn auf acht Artikel reduziert.[392] In der letzten Arbeitssitzung in Wien wurde der neue Entwurf von den Delegierten diskutiert. Insbesonders die deutschen Vertreter wandten sich gegen den amerikani-

---

[390] *Riedl*, Auch die UNCITRAL mengt sich in den elektronischen Geschäftsverkehr ein, ecolex (1999), S. 241.

[391] Proposal by the United States of America, A/CN.9/WG.IV/WP.79, eingebracht während der 33. Arbeitssitzung 29. Juni-10. Juli 1998.

[392] Die neue Form wurde von Dr. *Riedl* anläßlich eines Seminars der Wiener Arbeitsgruppe Rechtsinformatik vorgestellt. Die Vortragsunterlagen stehen unter http://www.univie.ac.at/RI/AJLI/3/riedl/sld001.htm zur Verfügung.

schen Vorschlag, wodurch die Uniform Rules so verkürzt wurden, um überhaupt einen Kompromiß finden zu können.

Art. A beinhaltet die, nun noch allgemeiner gehaltenen, notwendigen Definitionen. Die Regelung, welche Ansprüche eine elektronische Signatur erfüllen muß, damit sie der Schriftform genügt, findet sich in Art. B. Weiters fordert Art. C, daß die verwendete elektronische Signatur einem gewissen Sicherheitsstandard entspricht, damit die Integrität des sicher elektronisch signierten Dokuments gewährleistet ist und es analog zur Vorlage einer Urschrift verwendet werden kann. Art. D führt auch für die neue Version der Uniform Rules das abgestufte System ein. Eine staatliche Behörde kann festlegen, daß eine bestimmte Art. der elektronischen Signatur eine qualifizierte elektronische Signatur ist. In Art. E wird der schon im Model Law statuierte Grundsatz der Vertragsfreiheit noch einmal aufgeführt. Die Obliegenheiten, die ein Unterzeichner einhalten muß, finden sich in Art. F, und Art. G normiert, daß man auf eine qualifizierte elektronische Signatur vertrauen kann, wenn man alle vernünftigen Schritte unternimmt, um festzustellen, daß sie gültig ist. Verpflichtungen der Zertifizierungsdiensteanbieter werden in Art. H festgelegt.

Insbesonders die Regeln über die Haftung der Zertifizierungsdiensteanbieter sind den Kürzungen zum Opfer gefallen. Waren noch in der vorigen Version gleich zwei Artikel über diesen Bereich enthalten, die sowohl den Bereich der Vertragshaftung regelten als auch eine der SigRl angepaßte Bestimmung über die abstrakte Haftung der Zertifizierungsdiensteanbieter gegenüber betroffenen Dritten enthielten, wurde dieser Bereich wegen mangelnder Übereinstimmung unter den Delegierten ersatzlos gestrichen.

Auch während der letzten Sitzung in Wien war es oft sehr schwierig, einen Konsens über die Formulierung der einzelnen Vorschriften zu finden. Wann das Endprodukt fertig sein wird und wie es letzten Endes aussehen wird, ist noch nicht abzusehen. Diese zähen Verhandlungen führten auch schon relativ früh im Entstehungsprozeß des Model Law zur Entscheidung, daß keine völkerrechtlich bindende Konvention geschaffen werden soll, da hier wahrscheinlich länger keine Lösung gefunden werden könnte, die ein überwiegender Teil der Staatengemeinschaft ratifizieren würde. Daß die Regelungen nun nur als Softlaw vorliegen, steigert die Bedeutung der wesentlich verbindlicheren sektoralen Regelungen, wie der SigRL.

6.2. Spanien

Spanien hat zwar erst in jüngster Vergangenheit, am 17. September 1999, ein königliches Dekret über Elektronische Signaturen beschlossen, doch sind sie unter Anwendung allgemeiner Normen schon länger in die Realität des spanischen elektronischen Rechtsverkehrs eingeflossen.

Auf Grundlage einer Novellierung des Art. 230 Organic Law of Judicial Power können Tribunale nun jede Art von Telekommunikation für ihre Funktionsausübung heranziehen. Solange Authentizität, Integrität und Einhaltung des Prozeßrechtes gewährt sind, werden elektronisch übermittelte Dokumente den traditionellen gleichgestellt, verspricht Abs. 2 dieser Norm. Diese Regelung wurde auch im General Law of Telecommunications und im Law of Public Administration berücksichtigt. Erstmalig in Europa nahm ein Höchstgericht in einem Urteil zu den Möglichkeiten der elektronischen Kommunikation in Verbindung mit elektronischen Signaturen Stellung. Elektronische Dokumente können (speziell im Bereich der Wirtschaft) ohne eigenhändige Unterschrift verwendet werden und ersetzen die Voraussetzung der eigenhändigen Unterschrift, wenn kryptographische Hilfsmittel eingesetzt werden, die die Identität und Integrität des elektronischen Dokuments sicherstellen.

Auf diesen rechtlichen Grundlagen aufbauend begann im Mai 1998 die Arbeit an den Projekten FESTE und AEQUITAS, die in Zusammenarbeit der spanischen Regierung und der Universität Zaragoza entstanden. Diese beiden mittlerweile abgeschlossenen Arbeiten fanden ihre Fortsetzung im Projekt EMERITUS. Es wurden juristische Grundlagen für die Kommunikation aller Bürger unter Verwendung elektronischer Signaturen im allgemeinen ausgearbeitet und ein in der Praxis in Spanien bereits eingesetztes System für den elektronischen Rechtsverkehr zwischen Richtern, Prokuratoren und Rechtsanwälten geschaffen. Anders als der Elektronische Rechtsverkehr in Österreich, der noch immer in geschlossenen Netzwerken ohne die Anwendung elektronischer Signaturen abläuft, basiert das spanische Modell für die Kommunikation zwischen Gerichten und Anwälten auf der Einbeziehung elektronischer Signaturen, die eine sichere Gewährleistung von Identität des Ausstellers und Integrität der übermittelten Schriftstücke gewährleisten.

Auf Grund der Erfahrung des frühen Einsatzes von elektronischen Signaturen in Verwaltung und Gerichtswesen wurde das Dekret über elektronische Signaturen am 17. September 1999 erlassen. Die Norm hält sich eng an die Vorgaben der SigRL und beinhaltet eine umfassende Regelung dieses Bereichs. Art. 2 beinhaltet die Definitionen elektronischer und

fortgeschrittener elektronischer Signatur, des Zertifizierungungsdiensteanbieters und der Signaturerstellungs- und Prüfeinheiten.. Die Rechtswirkungen und prozessualen Vorschriften werden in Art. 2 geregelt. Der folgende Artikel behandelt den freien Marktzugang, wobei die Zertifizierungsdiensteanbieter in einer Wurzelzertifizierungsstelle, die vom spanischen Justizministerium betrieben wird, registriert sind, welches auch die Funktion der Aufsichtsstelle für die spanische Public Key Infrastructure übernimmt. Im Unterschied zur Zweiteilung der österreichischen Regelung in Gesetz und Verordnung beinhaltet das Dekret auch die Gebühren, die für die Tätigkeit der Aufsichtsstelle vom Zertifizierungsdiensteanbieter zu leisten sind. Ebenfalls der SigRL entsprechend sind Haftungsregeln vorgesehen. Den Bestimmungen über die Verwendung elektronischer Signaturen im Bereich der Verwaltung ist im Unterschied zum österreichischen Gesetz und der SigRL ebenfalls ein eigener Artikel gewidmet. Die Vorschrift von Sanktionen bei Übertretung der Bestimmungen des Dekrets schließen die spanische Norm ab.

6.3. Italien

Italien bildete zusammen mit Deutschland die Vorreiter der gesetzlichen Regulierung elektronischer Signaturen im Raum der Europäischen Union. Wie in Deutschland wurde auch hier noch vor einem konkreten Entwurf für eine Richtlinie, wie er mit der Fassung des Gemeinsamen Standpunktes seit 28. Juni 1999 vorliegt, die Materie innerstaatlich geregelt.

Die italienische Signaturgesetzgebung besteht im Moment aus drei staatlichen Normen[393], die im Zeitraum von März 1997 bis Februar 1999 erlassen wurden:

- Art. 15.2 des Law No. 59 vom 15. März 1997 enthält, die generellen Grundsätze über die Rechtswirksamkeit elektronischer Dokumente. Verfahren, Daten und elektronische Dokumente, die von Verwaltung[394] und von Privatpersonen in Verbindung mit Computern und dem Einsatz von Telematik verwendet werden, um Verträge abzuschließen, diese zu archivieren, zuzustellen und abzuschließen, sollen für alle rechtsgeschäftlichen Zwecke gültig und anerkannt sein. Die

---

[393] *Van der Hof*, Digital Signature Law Survey, http:// cwis.kub.nl/~frw/people/hof/DS-lawsu.htm.

[394] *Auerhammer*, Italien: Digitale Signaturen in der öffentlichen Verwaltung.

Bedingungen und Methoden für die Anwendung im öffentlichen Bereich und für Privatpersonen sollen in spezifischen Normen geregelt werden.

- Das Presidential Decree No. 513 vom 10. November 1997, verlautbart in der Gazzetta Ufficiale am 13. 3. 1998, dient der Umsetzung des sehr allgemein gehaltenen Grundsatzes des Art. 15.2 und beinhaltet die rechtlichen Tatbestände und Voraussetzungen für die Schaffung einer italienischen Public Key Infrastructure, ohne vorerst technische Standards einzubeziehen.
- Erst am 8. Februar 1999 – mehr als ein Jahr später – erging ein Prime Minister Decree über die technische Regelung der Public Key Infrastructure, das am 15. April 1999 in der Gazzetta Ufficiale veröffentlicht wurde.
- Ein Regelwerk über die technischen Voraussetzungen für digitale Signaturen stellte die Behörde für Informationstechnologie in der Verwaltung – Autorita per l'Informatica nella Pubblica Amministrazione (AIPA) schon am 6. August 1998 vor, um das Presidential Decree No. 513 in dieser Hinsicht näher auszugestalten.

Die italienische Rechtslage geht, wie auch Deutschland, vom technologiebezogenen Ansatz der digitalen Signaturen aus. Andere Formen der Vermittlung von Integrität eines elektronischen Dokuments und der Identität des Unterzeichners in Form der allgemeiner definierten elektronischen Signatur werden vom Dekret nicht reguliert und mit Rechtswirkung ausgestattet. Die Definition digitaler Signaturen erfolgt durch die Heranziehung asymmetrischer Kryptographie unter Verwendung von öffentlichen und privaten Schlüsseln. Interessant ist, daß auch biometrische Schlüssel im Gesetz vorgestellt werden. Sie sind computerbasierte Daten, die zur Überprüfung der Identität des Unterzeichners an Hand von personenbezogenen physischen Eigenschaften verwendet werden. Die Bezeichnung der Methode zur Verifikation der Identität mittels biometrischer Daten als „biometrischer Key" führt aber mE zur einer weiteren sprachlichen Verwischung der Unterschiede zwischen Zugangskontrolle zu Signaturerstellungseinheiten (in der Regel der private Schlüssel) und dem dadurch erst ausgelösten Prozeß des elektronischen Signierens eben mit dem privatem Schlüssel. Biometrische Verifikation der Identität und Vergleich dieser Prüfdaten mit den Kenndaten des Berechtigten sind eben keine elektronischen Signaturen, sondern kontrollieren nur den Zugriff auf solche.

Wie das dSigG kennt das Dekret kein abgestuftes System, sondern definiert nur eine Klasse digitaler Signaturen und Zertifikate, denen aber im Unterschied zur Rechtslage in Deutschland weitestgehende Rechtswirkungen zugestanden werden. Die generöse Gleichstellung mit der eigenhändigen Unterschrift und mit traditionell erstellten Dokumenten ist charakterisierend für die italienische Regelung. Interessant ist auch, daß diese Rechtswirkungen über ein Jahr ohne genauere Regelung der technischen Voraussetzungen für digitale Signaturen zugestanden wurden. Digitale Signaturen erfüllen generell die Schriftform und ersetzen auch jede Form von Siegeln, Zeichen und anderen Marken. Signierte elektronische Dokumente werden weiters prozeßrechtlich den Privaturkunden gleichgestellt. Sie erfüllen den gleichen Beweiswert. Wurde eine Signatur von einem Notar beglaubigt, wird sie einer notariell beglaubigten eigenhändigen Unterschrift gleichgestellt.

Das Dekret des Premierministers setzt in Art. 2 die verwendeten Algorithmen zur Verschlüsselung fest (RSA, DAS), gibt die zu verwendenden Hash Funktionen vor (RIPEMD-160, SHA-1) und führt mit Art. 4 drei verschiedene Schlüsselarten ein (Signaturschlüssel, Schlüssel für Zertifizierungsstellen und Zeitstempelschlüssel). Jeder Schlüssel muß mindestens eine Länge von 1024 Bit haben. Als Wurzelzertifizierungsstelle wird AIPA eingesetzt.

7. Acht Thesen zur rechtlichen Anerkennung elektronischer Signaturen

- Durch den sich rasch entwickelnden elektronischen Geschäftsverkehr ergibt sich ein dringender Bedarf an Rechtssicherheit für die Beteiligten. Um dies zu erreichen ist die rechtlich Anerkennung der neu eingesetzten Kommunikationsmittel eine Grundvoraussetzung.

- Elektronisch signierte Dokumente sollen in ihrer Funktionalität möglichst den traditionell eingesetzten Methoden zur Übermittlung von Willenserklärungen im Rechtsverkehr gleich gestaltet sein. Da die Rechtsordnung diesbezüglich hauptsächlich von der eigenhändigen Unterschrift ausgeht, müssen auch elektronische Signaturen den von Lehre und Rechtssprechung entwickelten funktionalen Anforderungen dafür entsprechen:

  - Identitätsfunktion
  - Echtheitsfunktion
  - Beweisfunktion
  - Abschlußfunktion
  - Warnfunktion.

- Weiters muß das ganze System einer Public Key Infrastructure jenen Anforderungen gerecht werden, die auch an traditionelle Übermittlung von Willenserklärungen gestellt werden:

  - Ausschluß der Abstreitbarkeit Dokumente erstellt oder empfangen zu haben
  - Nachweisbarkeit von Zeitpunkten im Kommunikationsfluß
  - Archivierbarkeit der Dokumente

- Bei Erfüllung dieser Bedingungen soll elektronisch signierten Dokumenten die gleiche Rechtswirkung wie herkömmlichen Dokumenten zukommen. Rechtliche Regelung muß das für die Kommunizierenden notwendige Maß an Rechtssicherheit gewährleisten.

- Zur Gewährleistung dieser Anforderungen ist ein Regulativ zu schaffen, das über unmittelbar beim Endanwender eingesetzte Verfahren hinausgeht und nur durch rechtliche Rahmenbedingungen für eine

komplexe Public Key Infrastrucure, in der insbesondere vertrauenswürdigen Dritten als Zertifizierungsdiensteanbietern eine besondere Bedeutung zukommt, verwirklicht werden kann. Die Rechtsordnung muß die Voraussetzungen für die Sicherheit dieser Infrastruktur schaffen, deren Einhaltung durch ein Aufsichtssystem sichern und Haftungsbestimmungen festlegen.

- Durch kontinuierliche Evaluation des gegenwärtigen Standes der Technik ist zu gewährleisten, daß durch die rechtlichen Normierungen auch eine Weiterentwicklung der eingesetzten Komponenten und Verfahren berücksichtigt wird.

- Auf Grund der besonderen Bedeutung des grenzüberschreitenden elektronischen Geschäftsverkehrs ist eine weltweite Harmonisierung der Vorschriften zu erreichen.

- Um auch kleineren Unternehmen, wie sie im Bereich des elektronischen Geschäftsverkehrs oft vorkommen, den Zugang zum Markt der Zertifizierungsdiensteanbieter zu gewährleisten und den vielfältigen Einsatzgebieten elektronischer Signaturen gerecht zu werden, wäre bezüglich der Sicherheitsanforderungen und der daran verknüpften Rechtswirkungen ein stärker abgestuftes System marktgerechter gestaltet.

Anhang

Signaturrichtlinie

Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

ABl. Nr. 290/1999

Das Europäische Parlament und der Rat der Europäischen Union -
gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 47 Absatz 2, Artikel 55 und 95,
auf Vorschlag der Kommission[1],
nach Stellungnahme des Wirtschafts- und Sozialausschusses[2],
nach Stellungnahme des Ausschusses der Regionen[3],
gemäss dem Verfahren des Artikels 251 des Vertrags[4],
in Erwägung nachstehender Gründe:

(1) Am 16. April 1997 hat die Kommission dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuss und dem Ausschuss der Regionen eine Mitteilung mit dem Titel „Europäische Initiative für den elektronischen Geschäftsverkehr" vorgelegt.

(2) Am 8. Oktober 1997 hat die Kommission dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuss und dem Ausschuss der Regionen eine Mitteilung über „Sicherheit und Vertraün in elektronische Kommunikation – Ein europäischer Rahmen für digitale Signaturen und Verschlüsselung" unterbreitet.

(3) Am 1. Dezember 1997 hat der Rat die Kommission aufgefordert, so bald wie möglich einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über digitale Signaturen vorzulegen.

---

[1] ABl. C 325 vom 23.10.1998, S. 5.

[2] ABl. C 40 vom 15.2.1999, S. 29.

[3] ABl. C 93 vom 6.4.1999, S. 33.

[4] Stellungnahme des Europäischen Parlaments vom 13. Januar 1999 (ABl. C 104 vom 14.4.1999, S. 49). Gemeinsamer Standpunkt des Rates vom 28. Juni 1999 (ABl. C 243 vom 27.8.1999, S. 33) und Beschluss des Europäischen Parlaments vom 27. Oktober 1999 (noch nicht im Amtsblatt veröffentlicht). Beschluss des Rates vom 30. November 1999.

(4) Elektronische Kommunikation und elektronischer Geschäftsverkehr erfordern „elektronische Signaturen"; und entsprechende Authentifizierungsdienste für Daten. Divergierende Regeln über die rechtliche Anerkennung elektronischer Signaturen und die Akkreditierung von Zertifizierungsdiensteanbietern in den Mitgliedstaaten können ein ernsthaftes Hindernis für die elektronische Kommunikation und den elektronischen Geschäftsverkehr darstellen. Klare gemeinschaftliche Rahmenbedingungen für elektronische Signaturen stärken demgegenüber das Vertraün und die allgemeine Akzeptanz hinsichtlich der neün Technologien. Die Rechtsvorschriften der Mitgliedstaaten sollten den freien Waren- und Dienstleistungsverkehr im Binnenmarkt nicht behindern.

(5) Die Interoperabilität von Produkten für elektronische Signaturen sollte gefördert werden. Gemäss Artikel 14 des Vertrags umfasst der Binnenmarkt einen Raum ohne Binnengrenzen, in dem der freie Warenverkehr gewährleistet ist. Es sind grundlegende Anforderungen zu erfüllen, die speziell für Produkte für elektronische Signaturen gelten, um so den freien Verkehr im Binnenmarkt zu gewährleisten und das Vertraün in digitale Signaturen zu fördern, wobei die Verordnung (EG) Nr. 3381/94 des Rates vom 19. Dezember 1994 über eine Gemeinschaftsregelung der Ausfuhrkontrolle von Gütern mit doppeltem Verwendungszweck[5] und der Beschluss 94/942/GASP des Rates vom 19. Dezember 1994 über die vom Rat angenommene gemeinsame Aktion zur Ausfuhrkontrolle von Gütern mit doppeltem Verwendungszweck[6] unberührt bleiben.

(6) Mit der vorliegenden Richtlinie wird die Erbringung von Dienstleistungen im Bereich der Vertraulichkeit von Informationen nicht harmonisiert, wenn für derartige Dienstleistungen einzelstaatliche Vorschriften hinsichtlich der öffentlichen Ordnung oder Sicherheit gelten.

(7) Der Binnenmarkt gewährleistet die Freizügigkeit von Personen, wodurch Bürger und Gebietsansässige der Europäischen Union zunehmend mit Stellen in anderen Mitgliedstaaten als demjenigen ihres Wohnsitzes in Verbindung treten müssen. Die Möglichkeit der elektronischen Kommunikation könnte in dieser Hinsicht von grossem Nutzen sein.

(8) Die rasche technologische Entwicklung und der globale Charakter des Internet erfordern ein Konzept, das verschiedenen Technologien und Dienstleistungen im Bereich der elektronischen Authentifizierung offensteht.

---

[5] ABl. L 367 vom 31.12.1994, S. 1. Verordnung geändert durch die Verordnung (EG) Nr. 837/95 (ABl. L 90 vom 21.4.1995, S. 1).

[6] ABl. L 367 vom 31.12.1994, S. 8. Beschluss zuletzt geändert durch den Beschluss 1999/193/GASP (ABl. L 73 vom 19.3.1999, S. 1).

(9) Elektronische Signaturen werden bei einer Vielzahl von Gegebenheiten und Anwendungen genutzt, die zu einem grossen Spektrum neür Dienste und Produkte im Zusammenhang mit oder unter Verwendung von elektronischen Signaturen führen. Die Definition solcher Produkte und Dienste sollte sich nicht auf die Ausstellung und Verwaltung von Zertifikaten beschränken, sondern sollte auch alle sonstigen Dienste und Produkte einschliessen, die elektronische Signaturen verwenden oder mit ihnen zusammenhängen, wie Registrierungsdienste, Zeitstempel, Verzeichnisdienste, Rechnerdienste oder Beratungsdienste in Verbindung mit elektronischen Signaturen.

(10) Der Binnenmarkt ermöglicht es Zertifizierungsdiensteanbietern, grenzüberschreitend tätig zu werden, um ihre Wettbewerbsfähigkeit zu steigern und damit Verbrauchern und Unternehmen ohne Rücksicht auf Grenzen neü Möglichkeiten des sicheren Informationsaustausches und elektronischen Geschäftsverkehrs zu eröffnen. Um das gemeinschaftsweite Anbieten von Zertifizierungsdiensten über offene Netze zu fördern, sollten Anbieter von Zertifizierungsdiensten diese ungehindert ohne vorherige Genehmigung bereitstellen können. Vorherige Genehmigung bedeutet nicht nur eine Erlaubnis, wonach der betreffende Zertifizierungsdiensteanbieter einen Bescheid der einzelstaatlichen Stellen einholen muss, bevor er seine Zertifizierungsdienste erbringen kann, sondern auch alle sonstigen Massnahmen mit der gleichen Wirkung.

(11) Freiwillige Akkreditierungssysteme, die auf eine Steigerung des Niveaus der erbrachten Dienste abzielen, können Zertifizierungsdiensteanbietern den geeigneten Rahmen für die Weiterentwicklung ihrer Dienste bieten, um das auf dem sich entwickelnden Markt geforderte Mass an Vertraün, Sicherheit und Qualität zu erreichen. Diese Systeme sollten die Entwicklung bester Praktiken durch Zertifizierungsdiensteanbieter fördern. Zertifizierungsdiensteanbietern sollte es freistehen, sich akkreditieren zu lassen und Akkreditierungssysteme zu nutzen.

(12) Zertifizierungsdienste sollten entweder von einer öffentlichen Stelle oder einer juristischen oder natürlichen Person angeboten werden können, sofern diese im Einklang mit den einzelstaatlichen Rechtsvorschriften niedergelassen ist. Die Mitgliedstaaten sollten es Anbietern von Zertifizierungsdiensten nicht untersagen, auch ohne freiwillige Akkreditierung tätig zu sein. Es ist darauf zu achten, dass Akkreditierungssysteme den Wettbewerb im Bereich der Zertifizierungsdienste nicht einschränken.

(13) Die Mitgliedstaaten können entscheiden, wie sie die Überwachung der Einhaltung der Bestimmungen dieser Richtlinie gewährleisten.

Diese Richtlinie schliesst nicht aus, dass privatwirtschaftliche Überwachungssysteme geschaffen werden. Diese Richtlinie verpflichtet die Zertifizierungsdiensteanbieter nicht, eine Überwachung im Rahmen eines geltenden Akkreditierungssystems zu beantragen.

(14) Es ist wichtig, ein ausgewogenes Verhältnis zwischen den Bedürfnissen der Verbraucher und der Unternehmen herzustellen.

(15) Anhang III enthält die Anforderungen für sichere Signaturerstellungseinheiten zur Gewährleistung der Funktionalität fortgeschrittener elektronischer Signaturen. Er deckt nicht die gesamte Systemumgebung ab, in der die Einheit betrieben wird. Das Funktionieren des Binnenmarktes verlangt von der Kommission und den Mitgliedstaaten, rasch zu handeln, damit die Stellen benannt werden können, die für die Bewertung der Übereinstimmung von sicheren Signaturerstellungseinheiten mit den Anforderungen des Anhangs III zuständig sind. Um den Markterfordernissen zu entsprechen, muss die Bewertung der Übereinstimmung rechtzeitig und effizient erfolgen.

(16) Diese Richtlinie leistet einen Beitrag zur Verwendung und rechtlichen Anerkennung elektronischer Signaturen in der Gemeinschaft. Es bedarf keiner gesetzlichen Rahmenbedingungen für elektronische Signaturen, die ausschliesslich in Systemen verwendet werden, die auf freiwilligen privatrechtlichen Vereinbarungen zwischen einer bestimmten Anzahl von Teilnehmern beruhen. Die Freiheit der Parteien, die Bedingungen zu vereinbaren, unter denen sie elektronisch signierte Daten akzeptieren, sollte respektiert werden, soweit dies im Rahmen des innerstaatlichen Rechts möglich ist. Elektronischen Signaturen, die in solchen Systemen verwendet werden, sollte die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht abgesprochen werden.

(17) Diese Richtlinie zielt nicht darauf ab, nationales Vertragsrecht, insbesondere betreffend den Abschluss und die Erfüllung von Verträgen, oder andere, ausservertragliche Formvorschriften bezüglich der Unterschriften zu harmonisieren. Deshalb sollten die Regelungen über die rechtliche Wirksamkeit elektronischer Signaturen unbeschadet einzelstaatlicher Formvorschriften gelten, die den Abschluss von Verträgen oder die Festlegung des Ortes eines Vertragsabschlusses betreffen.

(18) Das Speichern und Kopieren von Signaturerstellungsdaten könnte die Rechtsgültigkeit elektronischer Signaturen gefährden.

(19) Elektronische Signaturen werden im öffentlichen Bereich innerhalb der staatlichen und gemeinschaftlichen Verwaltungen und im Kommunikationsverkehr zwischen diesen Verwaltungen sowie zwischen diesen und den Bürgern und Wirtschaftsteilnehmern eingesetzt, z. B. in den

Bereichen öffentliche Auftragsvergabe, Steürn, soziale Sicherheit, Gesundheit und Justiz.

(20) Durch harmonisierte Kriterien im Zusammenhang mit der Rechtswirkung elektronischer Signaturen lässt sich gemeinschaftsweit ein kohärenter Rechtsrahmen aufrechterhalten. In den einzelstaatlichen Rechtsvorschriften sind verschiedene Anforderungen für die Rechtsgültigkeit handschriftlicher Unterschriften niedergelegt. Zertifikate können dazu dienen, die Identität einer elektronisch signierenden Person zu bestätigen. Auf qualifizierten Zertifikaten beruhende fortgeschrittene elektronische Signaturen zielen auf einen höheren Sicherheitsstandard. Fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und von einer sicheren Signaturerstellungseinheit erstellt werden, können nur dann gegenüber handschriftlichen Unterschriften als rechtlich gleichwertig angesehen werden, wenn die Anforderungen für handschriftliche Unterschriften erfüllt sind.

(21) Um die allgemeine Akzeptanz elektronischer Authentifizierungsmethoden zu fördern, ist zu gewährleisten, dass elektronische Signaturen in allen Mitgliedstaaten in Gerichtsverfahren als Beweismittel verwendet werden können. Die rechtliche Anerkennung elektronischer Signaturen sollte auf objektiven Kriterien beruhen und nicht mit einer Genehmigung für den betreffenden Zertifizierungsdiensteanbieter verknüpft sein. Die Festlegung der Rechtsgebiete, in denen elektronische Dokumente und elektronische Signaturen verwendet werden können, unterliegt einzelstaatlichem Recht. Diese Richtlinie lässt die Befugnis der einzelstaatlichen Gerichte, über die Übereinstimmung mit den Anforderungen dieser Richtlinie zu befinden, unberührt; sie berührt auch nicht die einzelstaatlichen Vorschriften über die freie gerichtliche Würdigung von Beweismitteln.

(22) Diensteanbieter, die ihre Zertifizierungsdienste öffentlich anbieten, unterliegen den einzelstaatlichen Haftungsregelungen.

(23) Die Entwicklung des internationalen elektronischen Geschäftsverkehrs erfordert grenzüberschreitende Vereinbarungen unter Beteiligung von Drittländern. Um die weltweite Interoperabilität zu gewährleisten, könnten Vereinbarungen mit Drittländern über multilaterale Regeln betreffend die gegenseitige Anerkennung der Zertifizierungsdienste nützlich sein.

(24) Zur Stärkung des Vertraüns der Nutzer in die elektronische Kommunikation und den elektronischen Geschäftsverkehr müssen die Zertifizierungsdiensteanbieter die Vorschriften über den Datenschutz und den Schutz der Privatsphäre achten.

(25) Die Bestimmungen über die Nutzung von Pseudonymen in Zertifikaten hindern die Mitgliedstaaten nicht daran, eine Identifizierung der Personen nach Gemeinschaftsrecht oder einzelstaatlichem Recht zu verlangen.

(26) Die zur Durchführung dieser Richtlinie erforderlichen Massnahmen sind gemäss Artikel 2 des Beschlusses 1999/468/EG des Rates vom 28. Juni 1999 zur Festlegung der Modalitäten für die Ausübung der der Kommission übertragenen Durchführungsbefugnisse[7] zu erlassen.

(27) Die Kommission nimmt zwei Jahre nach der Umsetzung dieser Richtlinie eine Überprüfung vor, um unter anderem sicherzustellen, dass der technologische Fortschritt oder Änderungen des rechtlichen Umfelds keine Hindernisse für die Realisierung der erklärten Ziele dieser Richtlinie mit sich gebracht haben. Sie sollte die Auswirkungen verwandter technischer Bereiche prüfen und dem Europäischen Parlament und dem Rat hierüber einen Bericht vorlegen.

(28) Nach den in Artikel 5 des Vertrags niedergelegten Grundsätzen der Subsidiarität und der Verhältnismässigkeit kann das Ziel der Schaffung harmonisierter rechtlicher Rahmenbedingungen für die Bereitstellung elektronischer Signaturen und entsprechender Dienste von den Mitgliedstaaten nicht ausreichend erreicht werden und lässt sich daher besser durch die Gemeinschaft verwirklichen. Diese Richtlinie geht nicht über das zur Erreichung dieses Ziels erforderliche Mass hinaus - haben folgende Richtlinien erlassen:

Artikel 1
Anwendungsbereich

Diese Richtlinie soll die Verwendung elektronischer Signaturen erleichtern und zu ihrer rechtlichen Anerkennung beitragen. Sie legt rechtliche Rahmenbedingungen für elektronische Signaturen und für bestimmte Zertifizierungsdienste fest, damit das reibungslose Funktionieren des Binnenmarktes gewährleistet ist.

Es werden weder Aspekte im Zusammenhang mit dem Abschluss und der Gültigkeit von Verträgen oder anderen rechtlichen Verpflichtungen, für die nach einzelstaatlichem Recht oder Gemeinschaftsrecht Formvorschriften zu erfüllen sind, erfasst, noch werden im einzelstaatlichen Recht oder im Gemeinschaftsrecht vorgesehene Regeln und Beschränkungen für die Verwendung von Dokumenten berührt.

---

[7] ABl. L 184 vom 17.7.1999, S. 23.

Artikel 2
Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

1. „elektronische Signatur"; Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen;
2. „fortgeschrittene elektronische Signatur"; eine elektronische Signatur, die folgende Anforderungen erfüllt:

a) Sie ist ausschliesslich dem Unterzeichner zugeordnet;
b) sie ermöglicht die Identifizierung des Unterzeichners;
c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;
d) sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann;

3. „Unterzeichner" eine Person, die eine Signaturerstellungseinheit besitzt und die entweder im eigenen Namen oder im Namen der von ihr vertretenen Stelle oder juristischen oder natürlichen Person handelt;
4. „Signaturerstellungsdaten"; einmalige Daten wie Codes oder private kryptographische Schlüssel, die vom Unterzeichner zur Erstellung einer elektronischen Signatur verwendet werden;
5. „Signaturerstellungseinheit"; eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturerstellungsdaten verwendet wird;
6. „sichere Signaturerstellungseinheit"; eine Signaturerstellungseinheit, die die Anforderungen des Anhangs III erfüllt;
7. „Signaturprüfdaten"; Daten wie Codes oder öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden;
8. „Signaturprüfeinheit"; eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturprüfdaten verwendet wird;
9. „Zertifikat" eine elektronische Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und die Identität dieser Person bestätigt wird;
10. „qualifiziertes Zertifikat" ein Zertifikat, das die Anforderungen des Anhangs I erfüllt und von einem Zertifizierungsdiensteanbieter bereitgestellt wird, der die Anforderungen des Anhangs II erfüllt;

11. „Zertifizierungsdiensteanbieter" eine Stelle oder eine juristische oder natürliche Person, die Zertifikate ausstellt oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellt;
12. „Produkt für elektronische Signaturen"; Hard- oder Software bzw. deren spezifische Komponenten, die von einem Zertifizierungsdiensteanbieter für die Bereitstellung von Diensten für elektronische Signaturen verwendet werden sollen oder die für die Erstellung und Überprüfung elektronischer Signaturen verwendet werden sollen;
13. „freiwillige Akkreditierung" eine Erlaubnis, mit der die Rechte und Pflichten für die Erbringung von Zertifizierungsdiensten festgelegt werden und die auf Antrag des betreffenden Zertifizierungsdiensteanbieters von der öffentlichen oder privaten Stelle, die für die Festlegung dieser Rechte und Pflichten sowie für die Überwachung ihrer Einhaltung zuständig ist, erteilt wird, wenn der Zertifizierungsdiensteanbieter die sich aus der Erlaubnis ergebenden Rechte nicht ausüben darf, bevor er den Bescheid der Stelle erhalten hat.

Artikel 3
Marktzugang

(1) Die Mitgliedstaaten machen die Bereitstellung von Zertifizierungsdiensten nicht von einer vorherigen Genehmigung abhängig.

(2) Unbeschadet des Absatzes 1 können die Mitgliedstaaten freiwillige Akkreditierungssysteme einführen bzw. beibehalten, die auf die Steigerung des Niveaus der erbrachten Zertifizierungsdienste abzielen. Alle mit diesen Systemen verknüpften Anforderungen müssen objektiv, transparent, verhältnismässig und nichtdiskriminierend sein. Die Mitgliedstaaten dürfen die Zahl der akkreditierten Zertifizierungsdiensteanbieter nicht aus Gründen einschränken, die in den Geltungsbereich dieser Richtlinie fallen.

(3) Die Mitgliedstaaten tragen dafür Sorge, dass ein geeignetes System zur Überwachung der in ihrem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter, die öffentlich qualifizierte Zertifikate ausstellen, eingerichtet wird.

(4) Die Übereinstimmung sicherer Signaturerstellungseinheiten mit den Anforderungen nach Anhang III wird von geeigneten öffentlichen oder privaten Stellen festgestellt, die von den Mitgliedstaaten benannt werden. Die Kommission legt nach dem Verfahren des Artikels 9 Kriteri-

en fest, anhand deren die Mitgliedstaaten bestimmen, ob eine Stelle zur Benennung geeignet ist. Die von den in Unterabsatz 1 genannten Stellen vorgenommene Feststellung der Übereinstimmung mit den Anforderungen des Anhangs III wird von allen Mitgliedstaaten anerkannt.

(5) Die Kommission kann nach dem Verfahren des Artikels 9 Referenznummern für allgemein anerkannte Normen für Produkte für elektronische Signaturen festlegen und im Amtsblatt der Europäischen Gemeinschaften veröffentlichen. Die Mitgliedstaaten gehen davon aus, dass die Anforderungen nach Anhang II Buchstabe f) und Anhang III erfüllt sind, wenn ein Produkt für elektronische Signaturen diesen Normen entspricht.

(6) Die Mitgliedstaaten und die Kommission arbeiten unter Berücksichtigung der Empfehlungen für die sichere Signaturprüfung in Anhang IV und im Interesse des Verbrauchers zusammen, um die Entwicklung und die Nutzung von Signaturprüfeinheiten zu fördern.

(7) Die Mitgliedstaaten können den Einsatz elektronischer Signaturen im öffentlichen Bereich möglichen zusätzlichen Anforderungen unterwerfen. Diese Anforderungen müssen objektiv, transparent, verhältnismässig und nichtdiskriminierend sein und dürfen sich nur auf die spezifischen Merkmale der betreffenden Anwendung beziehen. Diese Anforderungen dürfen für grenzüberschreitende Dienste für den Bürger kein Hindernis darstellen.

Artikel 4
Binnenmarktgrundsätze

(1) Jeder Mitgliedstaat wendet die innerstaatlichen Bestimmungen, die er aufgrund dieser Richtlinie erlässt, auf die in seinem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter und deren Dienste an. Die Mitgliedstaaten dürfen die Bereitstellung von Zertifizierungsdiensten, die aus anderen Mitgliedstaaten stammen, in den unter diese Richtlinie fallenden Bereichen nicht einschränken.

(2) Die Mitgliedstaaten tragen dafür Sorge, dass Produkte für elektronische Signaturen, die den Anforderungen dieser Richtlinie entsprechen, frei im Binnenmarkt verkehren können.

Artikel 5
Rechtswirkung elektronischer Signaturen

(1) Die Mitgliedstaaten tragen dafür Sorge, dass fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und die von einer sicheren Signaturerstellungseinheit erstellt werden,

a) die rechtlichen Anforderungen an eine Unterschrift in bezug auf in elektronischer Form vorliegende Daten in gleicher Weise erfüllen wie handschriftliche Unterschriften in bezug auf Daten, die auf Papier vorliegen, und
b) in Gerichtsverfahren als Beweismittel zugelassen sind.

(2) Die Mitgliedstaaten tragen dafür Sorge, dass einer elektronischen Signatur die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen wird,

- weil sie in elektronischer Form vorliegt oder
- nicht auf einem qualifizierten Zertifikat beruht oder
- nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder
- nicht von einer sicheren Signaturerstellungseinheit erstellt wurde.

Artikel 6
Haftung

(1) Die Mitgliedstaaten gewährleisten als Mindestregelung, dass ein Zertifizierungsdiensteanbieter, der ein Zertifikat als qualifiziertes Zertifikat öffentlich ausstellt oder für ein derartiges Zertifikat öffentlich einsteht, in bezug auf Schäden gegenüber einer Stelle oder einer juristischen oder natürlichen Person, die vernünftigerweise auf das Zertifikat vertraut, dafür haftet, dass

a) alle Informationen in dem qualifizierten Zertifikat zum Zeitpunkt seiner Ausstellung richtig sind und das Zertifikat alle für ein qualifiziertes Zertifikat vorgeschriebenen Angaben enthält,

b) der in dem qualifizierten Zertifikat angegebene Unterzeichner zum Zeitpunkt der Ausstellung des Zertifikats im Besitz der Signaturerstellungsdaten war, die den im Zertifikat angegebenen bzw. identifizierten Signaturprüfdaten entsprechen,

c) in Fällen, in denen der Zertifizierungsdiensteanbieter sowohl die Signaturerstellungsdaten als auch die Signaturprüfdaten erzeugt, beide Komponenten in komplementärer Weise genutzt werden können,es sei denn, der Zertifizierungsdiensteanbieter weist nach, dass er nicht fahrlässig gehandelt hat.

(2) Die Mitgliedstaaten gewährleisten als Mindestregelung, dass ein Zertifizierungsdiensteanbieter, der ein Zertifikat als qualifiziertes Zertifikat öffentlich ausgestellt hat, in bezug auf Schäden gegenüber einer Stelle oder einer juristischen oder natürlichen Person, die vernünftigerweise auf das Zertifikat vertraut, für den Fall haftet, dass der Widerruf des Zertifi-

kats nicht registriert worden ist, es sei denn, der Zertifizierungsdiensteanbieter weist nach, dass er nicht fahrlässig gehandelt hat.

(3) Die Mitgliedstaaten tragen dafür Sorge, dass Zertifizierungsdiensteanbieter in einem qualifizierten Zertifikat Beschränkungen für die Verwendung des Zertifikates angeben können; diese Beschränkungen müssen für Dritte erkennbar sein. Der Zertifizierungsdiensteanbieter haftet nicht für Schäden, die sich aus einer über diese Beschränkungen hinausgehenden Verwendung des qualifizierten Zertifikats ergeben.

(4) Die Mitgliedstaaten tragen dafür Sorge, dass Zertifizierungsdiensteanbieter in dem qualifizierten Zertifikat eine Grenze für den Wert der Transaktionen angeben können, für die das Zertifikat verwendet werden kann; diese Grenze muss für Dritte erkennbar sein.
Der Zertifizierungsdiensteanbieter haftet nicht für Schäden, die sich aus der Überschreitung dieser Höchstgrenze ergeben.

(5) Die Absätze 1 bis 4 gelten unbeschadet der Richtlinie 93/13/EWG des Rates vom 5. April 1993 über missbräuchliche Klauseln in Verbraucherverträgen[8].

Artikel 7
Internationale Aspekte

(1) Die Mitgliedstaaten tragen dafür Sorge, dass Zertifikate, die von einem Zertifizierungsdiensteanbieter eines Drittlandes öffentlich als qualifizierte Zertifikate ausgestellt werden, den von einem in der Gemeinschaft niedergelassenen Zertifizierungsdiensteanbieter ausgestellten Zertifikaten rechtlich gleichgestellt werden, wenn

a) der Zertifizierungsdiensteanbieter die Anforderungen dieser Richtlinie erfüllt und im Rahmen eines freiwilligen Akkreditierungssystems eines Mitgliedstaats akkreditiert ist oder

b) ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen dieser Richtlinie erfüllt, für das Zertifikat einsteht oder

c) das Zertifikat oder der Zertifizierungsdiensteanbieter im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Gemeinschaft und Drittländern oder internationalen Organisationen anerkannt ist.

(2) Um grenzüberschreitende Zertifizierungsdienste mit Drittländern und die rechtliche Anerkennung fortgeschrittener elektronischer Signaturen, die aus Drittländern stammen, zu erleichtern, unterbreitet die Kommission gegebenenfalls Vorschläge mit dem Ziel, die effiziente Umset-

---

[8] ABl. L 95 vom 21.4.1993, S. 29.

zung von Normen und internationalen Vereinbarungen über Zertifizierungsdienste zu erreichen. Insbesondere unterbreitet sie dem Rat bei Bedarf Vorschläge zur Erteilung von geeigneten Mandaten zur Aushandlung bilateraler und multilateraler Vereinbarungen mit Drittländern und internationalen Organisationen. Der Rat beschliesst mit qualifizierter Mehrheit.

(3) Wird die Kommission über Schwierigkeiten unterrichtet, auf die Unternehmen der Gemeinschaft beim Marktzugang in Drittländern stossen, so kann sie erforderlichenfalls dem Rat Vorschläge für ein geeignetes Mandat zur Aushandlung vergleichbarer Rechte für Unternehmen der Gemeinschaft in diesen Drittländern vorlegen. Der Rat beschliesst mit qualifizierter Mehrheit.

Die gemäss diesem Absatz ergriffenen Massnahmen lassen die Verpflichtungen der Gemeinschaft und der Mitgliedstaaten im Rahmen der einschlägigen internationalen Übereinkünfte unberührt.

Artikel 8
Datenschutz

(1) Die Mitgliedstaaten tragen dafür Sorge, dass Zertifizierungsdiensteanbieter und die für die Akkreditierung und Aufsicht zuständigen nationalen Stellen die Anforderungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[9] erfüllen.

(2) Die Mitgliedstaaten tragen dafür Sorge, dass Zertifizierungsdiensteanbieter, die öffentlich Zertifikate ausstellen, personenbezogene Daten nur unmittelbar von der betroffenen Person oder mit ausdrücklicher Zustimmung der betroffenen Person und nur insoweit einholen können, als dies zur Ausstellung und Aufrechterhaltung des Zertifikats erforderlich ist. Die Daten dürfen ohne ausdrückliche Zustimmung der betroffenen Person nicht für anderweitige Zwecke erfasst oder verarbeitet werden.

(3) Unbeschadet der Rechtswirkungen, die Pseudonyme nach einzelstaatlichem Recht haben, hindern die Mitgliedstaaten Zertifizierungsdiensteanbieter nicht daran, im Zertifikat ein Pseudonym anstelle des Namens des Unterzeichners anzugeben.

---

[9] ABl. L 281 vom 23.11.1995, S. 31.

Artikel 9
Ausschuss

(1) Die Kommission wird von einem „Ausschuss für elektronische Signaturen"; (im folgenden „Ausschuss" genannt) unterstützt.

(2) Bei einer Bezugnahme auf diesen Absatz finden die Artikel 4 und 7 des Beschlusses 1999/468/EG Anwendung, wobei Artikel 8 desselben Beschlusses zu beachten ist.

Der Zeitraum nach Artikel 4 Absatz 3 des Beschlusses 1999/468/EG wird auf drei Monate festgesetzt.

(3) Der Ausschuss gibt sich eine Geschäftsordnung.

Artikel 10
Aufgaben des Ausschusses

Der Ausschuss präzisiert die in den Anhängen festgelegten Anforderungen, die Kriterien nach Artikel 3 Absatz 4 und die allgemein anerkannten Normen für Produkte für elektronische Signaturen, die gemäss Artikel 3 Absatz 5 festgelegt und veröffentlicht werden, nach dem Verfahren des Artikels 9 Absatz 2.

Artikel 11
Notifizierung

(1) Die Mitgliedstaaten übermitteln der Kommission und den übrigen Mitgliedstaaten folgende Informationen:

a) Angaben zu nationalen freiwilligen Akkreditierungssystemen einschliesslich zusätzlicher Anforderungen gemäss Artikel 3 Absatz 7,

b) Namen und Anschriften der für Akkreditierung und Aufsicht zuständigen nationalen Stellen und der in Artikel 3 Absatz 4 genannten Stellen sowie

c) Namen und Anschriften aller akkreditierten nationalen Zertifizierungsdiensteanbieter.

(2) Die Informationen gemäss Absatz 1 und diesbezügliche Änderungen sind von den Mitgliedstaaten so bald wie möglich zu übermitteln.

Artikel 12
Überprüfung

(1) Die Kommission überprüft die Durchführung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat spätestens zum 19. Juli 2003 darüber Bericht.

(2) Bei der Überprüfung ist unter anderem festzustellen, ob der Anwendungsbereich dieser Richtlinie angesichts der technologischen und rechtlichen Entwicklungen und der Marktentwicklung geändert werden sollte. Der Bericht umfasst insbesondere eine Bewertung der Harmonisierungsaspekte auf der Grundlage der gesammelten Erfahrungen. Gegebenenfalls sind dem Bericht Vorschläge für Rechtsvorschriften beizufügen.

Artikel 13
Durchführung

(1) Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie vor dem 19. Juli 2001 nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Wenn die Mitgliedstaaten diese Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten innerstaatlichen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 14
Inkrafttreten

Diese Richtlinie tritt am Tag ihrer Veröffentlichung im Amtsblatt der Europäischen Gemeinschaften in Kraft.

Artikel 15
Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am 13. Dezember 1999.

Im Namen des Europäischen Parlaments

Die Präsidentin

N. FONTAINE

Im Namen des Rates
Der Präsident
S. HASSI

Anhang I

Anforderungen an qualifizierte Zertifikate

Qualifizierte Zertifikate müssen folgende Angaben enthalten:

a) Angabe, dass das Zertifikat als qualifiziertes Zertifikat ausgestellt wird;

b) Angabe des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist;

c) Name des Unterzeichners oder ein Pseudonym, das als solches zu identifizieren ist;

d) Platz für ein spezifisches Attribut des Unterzeichners, das gegebenenfalls je nach Bestimmungszweck des Zertifikats aufgenommen wird;

e) Signaturprüfdaten, die den vom Unterzeichner kontrollierten Signaturerstellungsdaten entsprechen;

f) Angaben zu Beginn und Ende der Gültigkeitsdaür des Zertifikats;

g) Identitätscode des Zertifikats;

h) die fortgeschrittene elektronische Signatur des ausstellenden Zertifizierungsdiensteanbieters;

i) gegebenenfalls Beschränkungen des Geltungsbereichs des Zertifikats und

j) gegebenenfalls Begrenzungen des Wertes der Transaktionen, für die das Zertifikat verwendet werden kann.

Anhang II

Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen

Zertifizierungsdiensteanbieter

a) müssen die erforderliche Zuverlässigkeit für die Bereitstellung von Zertifizierungsdiensten nachweisen;

b) müssen den Betrieb eines schnellen und sicheren Verzeichnisdienstes und eines sicheren und unverzüglichen Widerrufsdienstes gewährleisten;

c) müssen gewährleisten, dass Datum und Uhrzeit der Ausstellung oder des Widerrufs eines Zertifikats genau bestimmt werden können;

d) müssen mit geeigneten Mitteln nach einzelstaatlichem Recht die Identität und gegebenenfalls die spezifischen Attribute der Person überprüfen, für die ein qualifiziertes Zertifikat ausgestellt wird;

e) müssen Personal mit den für die angebotenen Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen beschäftigen; dazu gehören insbesondere Managementkompetenzen, Kenntnisse der Technologie elektronischer Signaturen und Vertrautheit mit angemessenen Sicherheitsverfahren; sie müssen ferner geeignete Verwaltungs- und Managementverfahren einhalten, die anerkannten Normen entsprechen;

f) müssen vertraünswürdige Systeme und Produkte einsetzen, die vor Veränderungen geschützt sind und die die technische und kryptographische Sicherheit der von ihnen unterstützten Verfahren gewährleisten;

g) müssen Massnahmen gegen Fälschungen von Zertifikaten ergreifen und in den Fällen, in denen sie Signaturerstellungsdaten erzeugen, die Vertraulichkeit während der Erzeugung dieser Daten gewährleisten;

h) müssen über ausreichende Finanzmittel verfügen, um den Anforderungen der Richtlinie entsprechend arbeiten zu können. Sie müssen insbesondere in der Lage sein, das Haftungsrisiko für Schäden zu tragen, zum Beispiel durch Abschluss einer entsprechenden Versicherung;

i) müssen alle einschlägigen Informationen über ein qualifiziertes Zertifikat über einen angemessenen Zeitraum aufzeichnen, um insbesondere für Gerichtsverfahren die Zertifizierung nachweisen zu können. Die Aufzeichnungen können in elektronischer Form erfolgen;

j) dürfen keine Signaturerstellungdaten von Personen speichern oder kopieren, denen Schlüsselmanagementdienste angeboten werden;

k) müssen, bevor sie in Vertragsbeziehungen mit einer Person eintreten, die von ihnen ein Zertifikat zur Unterstützung ihrer elektronischen Signatur wünscht, diese Person mit einem daürhaften Kommunikationsmittel über die genaün Bedingungen für die Verwendung des Zertifikats informieren, wozu unter anderem Nutzungsbeschränkungen für das Zertifikat, die Existenz eines freiwilligen Akkreditierungssystems und das Vorgehen in Beschwerde- und Schlichtungsverfahren gehören. Diese Angaben müssen schriftlich - gegebenenfalls elektronisch übermittelt – in klar verständlicher Sprache vorliegen. Wichtige Teilinformationen werden auf Antrag auch Dritten zur Verfügung gestellt, die auf das Zertifikat vertraün;

l) müssen vertraünswürdige Systeme für die Speicherung von Zertifikaten in einer überprüfbaren Form verwenden, so dass

- nur befugte Personen Daten eingeben und ändern können;
- die Angaben auf ihre Echtheit hin überprüft werden können;
- Zertifikate nur in den Fällen öffentlich abrufbar sind, für die die Zustimmung des Inhabers des Zertifikats eingeholt wurde;

– technische Veränderungen, die die Einhaltung dieser Sicherheitsanforderungen beeinträchtigen, für den Betreiber klar ersichtlich sind.

Anhang III

Anforderungen an sichere Signaturerstellungseinheiten

1. Sichere Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass

a) die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten praktisch nur einmal auftreten können und dass ihre Geheimhaltung hinreichend gewährleistet ist;

b) die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die Signatur vor Fälschungen bei Verwendung der jeweils verfügbaren Technologie geschützt ist;

c) die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten von dem rechtmässigen Unterzeichner vor der Verwendung durch andere verlässlich geschützt werden können.

2. Sichere Signaturerstellungseinheiten verändern die zu unterzeichnenden Daten nicht und verhindern nicht, dass diese Daten dem Unterzeichner vor dem Signaturvorgang dargestellt werden.

Anhang IV

Empfehlungen für die sichere Signaturprüfung

Während des Signaturprüfungsvorgangs ist mit hinreichender Sicherheit zu gewährleisten, dass

a) die zur Überprüfung der Signatur verwendeten Daten den Daten entsprechen, die dem Überprüfer angezeigt werden,

b) die Signatur zuverlässig überprüft wird und das Ergebnis dieser Überprüfung korrekt angezeigt wird,

c) der Überprüfer bei Bedarf den Inhalt der unterzeichneten Daten zuverlässig feststellen kann,

d) die Echtheit und die Gültigkeit des zum Zeitpunkt der Überprüfung der Signatur verlangten Zertifikats zuverlässig überprüft werden,

e) das Ergebnis der Überprüfung sowie die Identität des Unterzeichners korrekt angezeigt werden,

f) die Verwendung eines Pseudonyms eindeutig angegeben wird, und

g) sicherheitsrelevante Veränderungen erkannt werden können.

Österreichisches Signaturgesetz

Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG)

BGBl. I 190/1999

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.

Begriffsbestimmungen

§ 2. Im Sinne dieses Bundesgesetzes bedeuten

1. elektronische Signatur: elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators, dienen;
2. Signator: eine natürliche Person, der Signaturerstellungsdaten und die entsprechenden Signaturprüfdaten zugeordnet sind und die entweder im eigenen oder im fremden Namen eine elektronische Signatur erstellt, oder ein Zertifizierungsdiensteanbieter, der Zertifikate für die Erbringung von Zertifizierungsdiensten verwendet;
3. sichere elektronische Signatur: eine elektronische Signatur, die
   a) ausschließlich dem Signator zugeordnet ist,
   b) die Identifizierung des Signators ermöglicht,
   c) mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann,
   d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, daß jede nachträgliche Veränderung der Daten festgestellt werden kann, sowie

e) auf einem qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen, erstellt wird;

4. Signaturerstellungsdaten: einmalige Daten wie Codes oder private Signaturschlüssel, die vom Signator zur Erstellung einer elektronischen Signatur verwendet werden;
5. Signaturerstellungseinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturerstellungsdaten verwendet wird;
6. Signaturprüfdaten: Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden;
7. Signaturprüfeinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturprüfdaten verwendet wird;
8. Zertifikat: eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird;
9. qualifiziertes Zertifikat: ein Zertifikat, das die Angaben des § 5 enthält und von einem den Anforderungen des § 7 entsprechenden Zertifizierungsdiensteanbieter ausgestellt wird;
10. Zertifizierungsdiensteanbieter: eine natürliche oder juristische Person oder eine sonstige rechtsfähige Einrichtung, die Zertifikate ausstellt oder andere Signatur- und Zertifizierungsdienste erbringt;
11. Signatur- und Zertifizierungsdienste: die Bereitstellung von Signaturprodukten und -verfahren, die Ausstellung, Erneürung und Verwaltung von Zertifikaten, Verzeichnis-, Widerrufs-, Registrierungs- und Zeitstempeldienste sowie Rechner- und Beratungsdienste im Zusammenhang mit elektronischen Signaturen;
12. Zeitstempeldienst: eine elektronisch signierte Bescheinigung eines Zertifizierungsdiensteanbieters, daß bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen sind;
13. Signaturprodukt: Hard- oder Software bzw. deren spezifische Komponenten, die für die Erstellung und Überprüfung elektronischer Signaturen oder von einem Zertifizierungsdiensteanbieter für die Bereitstellung von Signatur- oder Zertifizierungsdiensten verwendet werden;

14. Kompromittierung: die Beeinträchtigung von Sicherheitsmaßnahmen oder Sicherheitstechnik, sodaß das vom Zertifizierungsdiensteanbieter zugrundegelegte Sicherheitsniveau nicht eingehalten ist.

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.

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.

Qualifizierte Zertifikate

§ 5. (1) Ein qualifiziertes Zertifikat hat zumindest folgende Angaben zu enthalten:

1. den Hinweis darauf, daß es sich um ein qualifiziertes Zertifikat handelt,
2. den unverwechselbaren Namen des Zertifizierungs-diensteanbieters und den Staat seiner Niederlassung,
3. den Namen des Signators oder ein Pseudonym, das als solches bezeichnet sein muß,
4. gegebenenfalls auf Verlangen des Zertifikatswerbers Angaben über eine Vertretungsmacht oder eine andere rechtlich erhebliche Eigenschaft des Signators,
5. die dem Signator zugeordneten Signaturprüfdaten,
6. Beginn und Ende der Gültigkeit des Zertifikats,
7. die eindeutige Kennung des Zertifikats,
8. gegebenenfalls eine Einschränkung des Anwendungsbereichs des Zertifikats und
9. gegebenenfalls eine Begrenzung des Transaktionswerts, auf den das Zertifikat ausgestellt ist.

(2) Auf Verlangen des Zertifikatswerbers können weitere rechtlich erhebliche Angaben in das qualifizierte Zertifikat aufgenommen werden.

(3) Ein qualifiziertes Zertifikat muß mit der sicheren elektronischen Signatur des Zertifizierungsdiensteanbieters versehen sein.

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.

(3) Ein Zertifizierungsdiensteanbieter, der sichere elektronische Signaturverfahren bereitstellt, hat in seinem Sicherheitskonzept die Einhaltung der Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen darzulegen.

(4) Ein Zertifizierungsdiensteanbieter hat die im Sicherheits- und im Zertifizierungskonzept dargelegten Angaben sowohl bei der Aufnahme als auch während der Ausübung seiner Tätigkeit zu erfüllen.

(5) Ein Zertifizierungsdiensteanbieter hat alle Umstände, die eine ordnungsgemäße und dem Sicherheits- sowie dem Zertifizierungskonzept entsprechende Tätigkeit nicht mehr ermöglichen, unverzüglich der Aufsichtsstelle anzuzeigen.

(6) Stellt ein Zertifizierungsdiensteanbieter Zertifikate aus, so hat er im Sicherheitskonzept darzulegen, ob und gegebenenfalls in welcher Form Verzeichnis- und Widerrufsdienste geführt werden.

(7) Ein Zertifikat für Zertifizierungsdiensteanbieter darf von diesen nur für die Erbringung von Zertifizierungsdiensten verwendet werden.

Zertifizierungsdiensteanbieter für qualifizierte Zertifikate

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

1. die erforderliche Zuverlässigkeit für die von ihm bereitgestellten Signatur- oder Zertifizierungsdienste aufzuweisen,
2. den Betrieb eines schnellen und sicheren Verzeichnisdienstes sowie eines unverzüglichen und sicheren Widerrufsdienstes sicherzustellen,
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,
5. zuverlässiges Personal mit den für die bereitgestellten Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Managementfähigkeiten sowie mit Kenntnissen der Technologie elektronischer Signaturen und angemessener Sicherheitsverfahren, zu beschäftigen und geeignete Verwaltungs- und Managementverfahren, die anerkannten Normen entsprechen, einzuhalten,
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,
7. alle maßgeblichen Umstände über ein qualifiziertes Zertifikat während eines für den Verwendungszweck angemessenen Zeitraums – gegebenenfalls auch elektronisch – aufzuzeichnen, sodaß insbesondere in gerichtlichen Verfahren die Zertifizierung nachgewiesen werden kann, sowie
8. Vorkehrungen dafür zu treffen, daß die Signaturerstellungsdaten der Signatoren weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden können.

(2) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, hat für die Signatur- und Zertifizierungsdienste sowie für die Erstellung und Speicherung von Zertifikaten vertraünswürdige Systeme, Produkte und Verfahren, die vor Veränderungen geschützt sind und für die technische und kryptographische Sicherheit sorgen, zu verwenden. Er hat insbesondere geeignete Vorkehrungen dafür zu treffen, daß Signaturerstellungsdaten geheimgehalten werden, daß Daten für qualifizierte Zertifikate nicht unerkannt gefälscht oder verfälscht werden können und daß diese Zertifikate nur mit Zustimmung des Signators öffentlich abrufbar sind. Für die Bereitstellung von Signaturerstellungsdaten sowie für die Erstellung und Speicherung von qualifizierten Zertifikaten sind technische Komponenten und Verfahren, die den Anforderungen des § 18 entsprechen, zu verwenden.

(3) Signaturerstellungsdaten der Zertifizierungsdiensteanbieter sind vor unbefugtem Zugriff zu sichern.

(4) Für sichere elektronische Signaturen kann das Vorliegen der Voraussetzungen der Abs. 1 bis 3 im Rahmen der freiwilligen Akkreditierung (§ 17) bescheinigt werden.

(5) Stellt der Zertifizierungsdiensteanbieter ein sicheres elektronisches Signaturverfahren bereit, so muß der Umstand, daß es sich um eine sichere elektronische Signatur handelt, im Zertifikat oder in einem elektronisch jederzeit allgemein zugänglichen Verzeichnis aufscheinen.

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

Ausstellung qualifizierter Zertifikate

§ 8. (1) Ein Zertifizierungsdiensteanbieter hat die Identität von Personen, denen ein qualifiziertes Zertifikat ausgestellt werden soll, anhand eines amtlichen Lichtbildausweises zuverlässig festzustellen. Er hat die Zuordnung bestimmter Signaturprüfdaten zu dieser Person durch ein qualifiziertes Zertifikat zu bestätigen.

(2) Das Verlangen auf Ausstellung eines qualifizierten Zertifikats kann auch bei einer im Auftrag des Zertifizierungsdiensteanbieters tätigen anderen Stelle eingebracht werden, die die Überprüfung der Identität des Zertifikatswerbers vorzunehmen hat.

(3) Ein Zertifizierungsdiensteanbieter hat nach Maßgabe des Zertifizierungskonzepts auf Verlangen des Zertifikatswerbers Angaben über seine Vertretungsmacht oder eine andere rechtlich erhebliche Eigenschaft in das qualifizierte Zertifikat aufzunehmen, sofern ihm oder einer anderen Stelle (Abs. 2) diese Umstände zuverlässig nachgewiesen werden.

(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.

Widerruf von Zertifikaten

§ 9. (1) Ein Zertifizierungsdiensteanbieter hat ein Zertifikat unverzüglich zu widerrufen, wenn

1. der Signator oder ein im Zertifikat genannter Machtgeber dies verlangt,

2. der Zertifizierungsdiensteanbieter Kenntnis vom Ableben des Signators oder sonst von der Änderung im Zertifikat bescheinigter Umstände erlangt,
3. das Zertifikat auf Grund unrichtiger Angaben erwirkt wurde,
4. der Zertifizierungsdiensteanbieter seine Tätigkeit einstellt und seine Verzeichnis- und Widerrufsdienste nicht von einem anderen Zertifizierungsdiensteanbieter übernommen werden,
5. die Aufsichtsstelle gemäß § 14 den Widerruf des Zertifikats anordnet oder
6. die Gefahr einer mißbräuchlichen Verwendung des Zertifikats besteht.

(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, ab dem sie wirksam werden, enthalten. Wird ein Widerrufsdienst geführt, so werden die Sperre und der Widerruf mit der Eintragung in das entsprechende Verzeichnis wirksam. Eine rückwirkende Sperre oder ein rückwirkender Widerruf ist unzulässig. Der Signator bzw. sein Rechtsnachfolger ist von der Sperre oder dem Widerruf unverzüglich zu verständigen.

(4) Ein Zertifizierungsdiensteanbieter hat ein elektronisch jederzeit allgemein zugängliches Verzeichnis der gesperrten und der widerrufenen qualifizierten Zertifikate zu führen.

(5) Die Aufsichtsstelle hat das Zertifikat eines Zertifizierungsdiensteanbieters unverzüglich zu widerrufen, wenn

1. dem Zertifizierungsdiensteanbieter die Ausübung seiner Tätigkeit untersagt wird und seine Verzeichnis- und Widerrufsdienste nicht von einem anderen Zertifizierungsdiensteanbieter übernommen werden oder
2. der Zertifizierungsdiensteanbieter seine Tätigkeit einstellt und seine Verzeichnis- und Widerrufsdienste nicht von einem anderen Zertifizierungsdiensteanbieter übernommen werden.

Zeitstempeldienste

§ 10. Stellt ein Zertifizierungsdiensteanbieter Zeitstempeldienste bereit, so hat er im Sicherheits- und im Zertifizierungskonzept die näheren Angaben darzulegen. Für sichere Zeitstempeldienste sind technische Komponenten und Verfahren zu verwenden, die die Richtigkeit und Unverfälschtheit der Zeitangabe sicherstellen und den Anforderungen des § 18 entsprechen.

Dokumentation

§ 11. (1) Ein Zertifizierungsdiensteanbieter hat die Sicherheitsmaßnahmen, die er zur Einhaltung dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen getroffen hat, sowie das Ausstellen und gegebenenfalls die Sperre und den Widerruf von Zertifikaten zu dokumentieren. Dabei müssen die Daten und ihre Unverfälschtheit sowie der Zeitpunkt ihrer Aufnahme in das Protokollierungssystem jederzeit nachprüfbar sein.

(2) Auf Ersuchen von Gerichten oder anderen Behörden hat ein Zertifizierungsdiensteanbieter die Dokumentation nach Abs. 1 auszufolgen.

Einstellung der Tätigkeit

§ 12. Ein Zertifizierungsdiensteanbieter hat die Einstellung seiner Tätigkeit unverzüglich der Aufsichtsstelle anzuzeigen. Weiters hat er die im Zeitpunkt der Einstellung seiner Tätigkeit gültigen Zertifikate zu widerrufen oder dafür Sorge zu tragen, daß zumindest seine Verzeichnis- und Widerrufsdienste von einem anderen Zertifizierungsdiensteanbieter übernommen werden. Die Signatoren sind von der Einstellung der Tätigkeit sowie vom Widerruf oder der Übernahme unverzüglich zu verständigen. Auch im Fall des Widerrufs der Zertifikate hat der Zertifizierungsdiensteanbieter sicherzustellen, daß die Widerrufsdienste weitergeführt werden; kommt er dieser Verpflichtung nicht nach, so hat die Aufsichtsstelle für die Weiterführung der Widerrufsdienste auf Kosten des Zertifizierungsdiensteanbieters Sorge zu tragen.

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,
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.

(4) Die Aufsichtsstelle hat den Zertifizierungsdiensteanbietern für ihre Tätigkeit und für die Heranziehung der Telekom-Control GmbH eine mit Verordnung festgelegte kostendeckende Gebühr vorzuschreiben. Die Einnahmen aus dieser Gebühr fließen der Aufsichtsstelle zu und sind nach Heranziehung der Telekom-Control GmbH oder der Bestätigungsstelle nach deren Aufwand weiterzuleiten.

(5) Die Aufsichtsstelle kann sich zur Beratung geeigneter Personen oder Einrichtungen wie etwa einer Bestätigungsstelle (§ 19) bedienen.

(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.

(7) Die Tätigkeit der Aufsichtsstelle nach diesem Bundesgesetz ist von ihrer Tätigkeit nach anderen Bundesgesetzen organisatorisch und finanziell zu trennen.

Aufsichtsmaßnahmen

§ 14. (1) Die Aufsichtsstelle hat den Zertifizierungsdiensteanbietern Maßnahmen zur Sicherstellung der Erfüllung der Pflichten aus diesem

Bundesgesetz und der auf seiner Grundlage ergangenen Verordnungen vorzuschreiben. Sie kann einem Zertifizierungsdiensteanbieter insbesondere die Verwendung ungeeigneter technischer Komponenten und Verfahren oder die Ausübung der Tätigkeit ganz oder teilweise untersagen. Weiters kann die Aufsichtsstelle Zertifikate für Zertifizierungsdiensteanbieter oder von Signatoren widerrufen oder den Widerruf der Zertifikate von Signatoren durch den Zertifizierungsdiensteanbieter anordnen.

(2) Sofern nicht nach Abs. 6 gelindere Mittel in Betracht kommen, ist einem Zertifizierungsdiensteanbieter die Ausübung der Tätigkeit ganz oder teilweise zu untersagen, wenn

1. er oder sein Personal nicht die für die bereitgestellten Signatur- oder Zertifizierungsdienste erforderliche Zuverlässigkeit aufweist,
2. er oder sein Personal nicht über die erforderlichen Fachkenntnisse verfügt,
3. ihm keine ausreichenden Finanzmittel zur Verfügung stehen,
4. er bei der Ausübung seiner Tätigkeit die im Sicherheits- oder im Zertifizierungskonzept dargelegten Angaben nicht erfüllt,
5. er die vorgeschriebenen Verzeichnis- oder Widerrufsdienste nicht oder nicht ordnungsgemäß führt oder der Sperr- oder Widerrufspflicht (§ 9) nicht oder nur unzureichend nachkommt oder
6. er der Anzeigepflicht nach § 6 Abs. 2 nicht nachkommt.

(3) Sofern nicht nach Abs. 6 gelindere Mittel in Betracht kommen, ist einem Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, die Ausübung seiner Tätigkeit zudem ganz oder teilweise zu untersagen, wenn die übrigen für die Ausübung einer solchen Tätigkeit erforderlichen Voraussetzungen nach diesem Bundesgesetz oder den auf seiner Grundlage ergangenen Verordnungen nicht erfüllt werden.

(4) Sofern nicht nach Abs. 6 gelindere Mittel in Betracht kommen, ist einem Zertifizierungsdiensteanbieter, der sichere elektronische Signaturverfahren bereitstellt, die Ausübung seiner Tätigkeit auch dann ganz oder teilweise zu untersagen, wenn die verwendeten technischen Komponenten und Verfahren nicht die Sicherheitsanforderungen nach § 18 erfüllen.

(5) Wenn die Aufsichtsstelle einem Zertifizierungsdiensteanbieter die Ausübung seiner Tätigkeit untersagt, hat sie für den Widerruf der Zertifikate des Zertifizierungsdiensteanbieters und der Signatoren Sorge zu tragen oder die Übernahme der erbrachten Signatur- und Zertifizierungsdienste oder zumindest seiner Verzeichnis- und Widerrufsdienste durch einen anderen Zertifizierungsdiensteanbieter zu veranlassen, sofern die beteiligten Zertifizierungsdiensteanbieter der Übernahme zustimmen. Die Signatoren sind von der Untersagung sowie vom Widerruf oder der Über-

nahme unverzüglich zu verständigen. Auch im Fall des Widerrufs der Zertifikate hat der Zertifizierungsdiensteanbieter sicherzustellen, daß die Widerrufsdienste weitergeführt werden; kommt er dieser Verpflichtung nicht nach, so hat die Aufsichtsstelle für die Weiterführung der Widerrufsdienste auf Kosten des Zertifizierungsdiensteanbieters Sorge zu tragen.

(6) Die Aufsichtsstelle hat von einer Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters abzusehen, soweit die Anordnung gelinderer Mittel ausreicht, um die Einhaltung der Bestimmungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen sicherzustellen. Sie kann insbesondere Auflagen erteilen oder unter Setzung einer angemessenen Frist zur Behebung von ihr aufgezeigter Mängel Maßnahmen androhen.

Heranziehung der Telekom-Control GmbH

§ 15. (1) Die Aufsichtsstelle kann sich bei der Durchführung der Aufsicht der Telekom-Control GmbH (§ 108 TKG) bedienen.

(2) Die Telekom-Control GmbH hat insbesondere

1. die Aufsichtsstelle bei der laufenden Aufsicht der Zertifizierungsdiensteanbieter zu unterstützen und die technischen Produkte, Verfahren und sonstigen Mittel, die im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste eingesetzt werden, sowie die Qualifikation des Personals zu überprüfen,
2. die Zertifizierungsdiensteanbieter nach der Anzeige der Aufnahme ihrer Tätigkeit zu registrieren,
3. Verzeichnisse der Zertifikate für Zertifizierungsdiensteanbieter und der Zertifizierungsdiensteanbieter (§ 13 Abs. 3) sowie ein Verzeichnis der akkreditierten Zertifizierungsdiensteanbieter (§ 17 Abs. 1) zu führen,
4. für den Fall der Einstellung oder Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters einen Widerrufsdienst zu führen, sofern keine Übernahme im Sinne der §§ 12 oder 14 Abs. 5 erfolgt,
5. auf Anordnung der Aufsichtsstelle die Erfüllung der Voraussetzungen einer freiwilligen Akkreditierung (§ 17) zu erheben,
6. bei der Feststellung der Gleichwertigkeit von Prüfberichten aus Drittstaaten im Sinne des § 24 Abs. 3 mitzuwirken und
7. im Fall des begründeten Verdachts, daß die Sicherheitsanforderungen dieses Bundesgesetzes oder der auf seiner Grundlage ergangenen Verordnungen nicht eingehalten werden, oder auf Verlangen eines Zertifizierungsdiensteanbieters unmittelbar die vorläufige Untersa-

gung der Tätigkeit des Zertifizierungsdiensteanbieters oder vorläufig Maßnahmen im Sinne des § 14 Abs. 1 anzuordnen.

(3) Die Telekom-Control GmbH hat alle organisatorischen Vorkehrungen dafür zu treffen, daß sie ihre Aufgaben erfüllen und die Aufsichtsstelle bei Erfüllung ihrer Aufgaben unterstützen kann. Sie kann sich zur Beratung geeigneter Personen oder Einrichtungen wie etwa einer Bestätigungsstelle (§ 19) bedienen. Die Wahrnehmung ihrer Aufgaben in technischen Belangen hat in Abstimmung mit einer Bestätigungsstelle (§ 19) zu erfolgen. Im Rahmen ihrer Tätigkeit für die Aufsichtsstelle ist das Personal der Telekom-Control GmbH an die Weisungen des Vorsitzenden oder des in der Geschäftsordnung bezeichneten Mitgliedes gebunden.

(4) Unbeschadet der Zuständigkeit der ordentlichen Gerichte können Kunden oder Interessenvertretungen Streit- oder Beschwerdefälle, insbesondere über die Qualität eines Zertifizierungsdienstes, die mit dem Zertifizierungsdiensteanbieter nicht befriedigend gelöst worden sind, der Telekom-Control GmbH vorlegen. Die Telekom-Control GmbH hat sich zu bemühen, innerhalb angemessener Frist eine einvernehmliche Lösung herbeizuführen. Die Zertifizierungsdiensteanbieter sind verpflichtet, an einem solchen Verfahren mitzuwirken und alle zur Beurteilung der Sachlage erforderlichen Auskünfte zu erteilen. Die Telekom-Control GmbH hat Richtlinien für die Durchführung dieses Verfahrens festzulegen, die in geeigneter Form zu veröffentlichen sind.

(5) § 13 Abs. 7 über die organisatorische und finanzielle Trennung ist auf die Tätigkeit der Telekom-Control GmbH anzuwenden.

Durchführung der Aufsicht

§ 16. (1) Die Zertifizierungsdiensteanbieter haben den im Auftrag der Aufsichtsstelle handelnden Personen das Betreten der Geschäfts- und Betriebsräume während der Geschäftszeiten zu gestatten, die in Betracht kommenden Bücher und sonstigen Aufzeichnungen oder Unterlagen einschließlich der Dokumentation nach § 11 vorzulegen oder zur Einsicht bereitzuhalten, Auskünfte zu erteilen und jede sonst erforderliche Unterstützung zu gewähren. Bestehende gesetzliche Verschwiegenheits- und Aussageverweigerungsrechte bleiben unberührt.

(2) Die Organe des öffentlichen Sicherheitsdienstes haben der Aufsichtsstelle und den in ihrem Auftrag handelnden Personen über deren Ersuchen zur Durchführung der Aufsicht im Rahmen ihres gesetzmäßigen Wirkungsbereichs Hilfe zu leisten.

(3) Die Durchführung der Aufsicht nach den Abs. 1 und 2 ist unter möglichster Schonung der Betroffenen und ohne unnötiges Aufsehen so

durchzuführen, daß dadurch die Sicherheit der Signatur- und Zertifizierungsdienste nicht verletzt wird.

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.

5. 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. 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.

Bestätigungsstelle

§ 19. (1) Die nach diesem Bundesgesetz und den auf seiner Grundlage ergangenen Verordnungen einer Bestätigungsstelle zugewiesenen Aufgaben können nur von einer dazu geeigneten Einrichtung wahrgenommen werden.

(2) Eine Einrichtung ist zur Wahrnehmung der einer Bestätigungsstelle zugewiesenen Aufgaben geeignet, wenn sie

1. die erforderliche Zuverlässigkeit aufweist,
2. zuverlässiges Personal mit den für diese Aufgaben erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Kenntnissen über elektronische Signaturen, angemessene Sicherheitsverfahren, Kryptographie, Kommunikations- und Chipkartentechnologien sowie die technische Begutachtung solcher Komponenten, beschäftigt,
3. über ausreichende technische Einrichtungen und Mittel sowie eine ausreichende wirtschaftliche Leistungsfähigkeit verfügt und

4. die erforderliche Unabhängigkeit, Unparteilichkeit und Unbefangenheit sicherstellt.

(3) Der Bundeskanzler hat im Einvernehmen mit dem Bundesminister für Justiz mit Verordnung festzustellen, daß eine Einrichtung als Bestätigungsstelle geeignet ist. Eine solche Verordnung kann nur auf Antrag der betreffenden Einrichtung erlassen werden. Die Eignung kann nur festgestellt werden, wenn die Einrichtung nach ihren Statuten oder Satzungen oder nach ihrem Gesellschaftsvertrag, nach ihrer Organisation und nach ihrem Sicherheits- und Finanzierungskonzept die in Abs. 2 genannten Anforderungen erfüllt.

(4) Eine Bestätigungsstelle kann zur Erfüllung der ihr nach diesem Bundesgesetz oder der auf seiner Grundlage ergangenen Verordnungen zugewiesenen Aufgaben von anderen Einrichtungen oder Stellen Prüfberichte zu technischen Komponenten und Verfahren einholen.

6. Abschnitt
Rechte und Pflichten der Anwender

Allgemeine Informationspflichten der Zertifizierungsdiensteanbieter

§ 20. (1) Ein Zertifizierungsdiensteanbieter hat den Zertifikatswerber vor Vertragschließung schriftlich oder unter Verwendung eines daürhaften 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 neü elektronische Signatur anzubringen ist, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

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.

Datenschutz

§ 22. (1) Ein Zertifizierungsdiensteanbieter darf nur jene personenbezogenen Daten verwenden, die er zur Durchführung der erbrachten Dienste benötigt. Diese Daten dürfen nur unmittelbar beim Betroffenen selbst oder mit seiner ausdrücklichen Zustimmung bei einem Dritten erhoben werden.

(2) Bei Verwendung eines Pseudonyms hat der Zertifizierungsdiensteanbieter die Daten über die Identität des Signators zu übermitteln, sofern an der Feststellung der Identität ein überwiegendes berechtigtes Interesse im Sinne des § 8 Abs. 1 Z 4 und Abs. 3 DSG glaubhaft gemacht wird. Die Übermittlung ist zu dokumentieren.

(3) Die Auskunfts- und Mitwirkungspflichten des Zertifizierungsdiensteanbieters gegenüber Gerichten und anderen Behörden bleiben unberührt.

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 den Abs. 1 und 2 kein Verschulden trifft. Kann der Geschädigte als wahrscheinlich dartun, daß die Verpflichtungen nach den 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. Diese Vermutung ist widerlegt, wenn der Zertifizierungsdiensteanbieter als wahrscheinlich dartut, daß der Schaden nicht durch eine Verletzung bzw. Kompromittierung der im zweiten Satz genannten Verpflichtungen und Vorkehrungen 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.

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.

(3) Ist in einem Mitgliedstaat der Europäischen Union oder in einem Drittstaat zum Nachweis der Sicherheitsanforderungen für sichere elektronische Signaturen eine staatlich anerkannte Stelle eingerichtet, so werden Bescheinigungen dieser Stelle über die Einhaltung der Sicherheitsanforderungen für die Erzeugung sicherer elektronischer Signaturen den Bescheinigungen einer Bestätigungsstelle (§ 19) gleichgehalten, soweit die Aufsichtsstelle feststellt, daß die den Beurteilungen dieser Stellen zugrunde liegenden technischen Anforderungen, Prüfungen und Prüfverfahren jenen der Bestätigungsstelle gleichwertig sind.

8. Abschnitt
Schlußbestimmungen

Signaturverordnung

§ 25. Der Bundeskanzler hat mit Verordnung im Einvernehmen mit dem Bundesminister für Justiz die nach dem jeweiligen Stand der Wissenschaft und Technik zur Durchführung dieses Bundesgesetzes erforderlichen Rechtsvorschriften zu erlassen über

1. die Festsetzung pauschaler kostendeckender Gebühren für die Leistungen der Aufsichtsstelle und der Telekom-Control GmbH sowie die Vorschreibung dieser Gebühren,
2. die Festsetzung der zur Erfüllung der Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen ausreichenden Finanzmittel sowie der für die Abdeckung des Haftungsrisikos der Zertifizierungsdiensteanbieter ausreichenden Finanzmittel, insbesondere die Festsetzung einer Mindestversicherungssumme für eine Haftpflichtversicherung,
3. die Zuverlässigkeit des Zertifizierungsdiensteanbieters und seines Personals (§§ 7 Abs. 1 und 14 Abs. 2),
4. die näheren Anforderungen an die technischen Komponenten und Verfahren sowie die technischen Produkte und sonstigen Mittel zur Anwendung der §§ 7 Abs. 2, 10 und 18, die Durchführung der Prüfung der technischen Komponenten und Verfahren nach § 18 sowie die Ausstellung der Bestätigung, daß diese Anforderungen erfüllt sind,
5. die Daür der Weiterführung der Widerrufsdienste durch die Aufsichtsstelle (§ 12 und § 14 Abs. 5),
6. die Anwendungsbereiche, Anforderungen und Toleranzen von sicheren Zeitstempeldiensten,
7. die Gültigkeitsdaür und die Erneürung der qualifizierten Zertifikate sowie den Zeitraum und das Verfahren, nach denen eine neü elektronische Signatur angebracht werden sollte (Nachsignieren),
8. die Form, Darstellung und Verfügbarkeit des Zertifizierungskonzepts (zB Klartext),
9. die Daür der Aufbewahrung einer Dokumentation (§ 11) und
10. die Art und Form der Kennzeichnung akkreditierter Zertifizierungsdiensteanbieter.

Verwaltungsstrafbestimmungen

§ 26. (1) Eine Verwaltungsübertretung begeht und ist mit Geldstrafe bis zu 56 000 S zu bestrafen, wer fremde Signaturerstellungsdaten ohne Wissen und Willen des Signators mißbräuchlich verwendet.

(2) Ein Zertifizierungsdiensteanbieter begeht eine Verwaltungsübertretung und ist mit Geldstrafe bis zu 112 000 S zu bestrafen, wenn er

1. entgegen § 9 Abs. 1 seine Widerrufspflicht verletzt,
2. entgegen § 11 seine Dokumentationspflicht verletzt,
3. entgegen § 16 Abs. 1 nicht Einsicht in die dort genannten Bücher, sonstige Aufzeichnungen oder Unterlagen gewährt oder nicht die notwendigen Auskünfte erteilt oder
4. entgegen § 20 Abs. 1 und 3 den Zertifikatswerber nicht unterrichtet.

(3) Ein Zertifizierungsdiensteanbieter begeht eine Verwaltungsübertretung und ist mit Geldstrafe bis zu 224 000 S zu bestrafen, wenn er

1. entgegen § 6 Abs. 2 die Aufnahme seiner Tätigkeit nicht anzeigt oder das Sicherheitskonzept oder das Zertifizierungskonzept nicht vorlegt,
2. entgegen § 6 Abs. 5 nicht alle Umstände, die eine ordnungsgemäße und dem Sicherheits- sowie dem Zertifizierungskonzept entsprechende Tätigkeit nicht mehr ermöglichen, der Aufsichtsstelle anzeigt,
3. entgegen § 7 Abs. 1 Z 2 keinen geeigneten Widerrufsdienst oder keinen geeigneten Verzeichnisdienst führt,
4. entgegen § 7 Abs. 1 Z 8 keine geeigneten Vorkehrungen dafür trifft, daß die Signaturerstellungsdaten der Signatoren weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden können,
5. entgegen § 18 keine geeigneten technischen Komponenten und Verfahren für sichere elektronische Signaturen verwendet, bereitstellt oder bezeichnet oder
6. trotz Untersagung durch die Aufsichtsstelle (§ 14 Abs. 2 bis 4) die ihm untersagte Tätigkeit weiterhin ausübt.

(4) Eine Verwaltungsübertretung gemäß den Abs. 1 bis 3 liegt nicht vor, wenn die Tat den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist.

(5) Im Straferkenntnis können die Gegenstände, mit denen die strafbare Handlung begangen wurde, für verfallen erklärt werden.

Inkrafttreten und Verweisungen

§ 27. (1) Dieses Bundesgesetz tritt mit 1. Jänner 2000 in Kraft.

(2) Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

Vollzug

§ 28. Mit der Vollziehung dieses Bundesgesetzes sind betraut:

1. hinsichtlich der §§ 3, 4 und 23 der Bundesminister für Justiz,
2. hinsichtlich der §§ 13 bis 17 der Bundesminister für Wissenschaft und Verkehr,
3. hinsichtlich der §§ 22 und 26 der Bundeskanzler,
4. hinsichtlich der §§ 7 Abs. 1 Z 6 und 13 Abs. 4 der Bundeskanzler im Einvernehmen mit dem Bundesminister für Justiz und dem Bundesminister für Finanzen und
5. hinsichtlich der übrigen Bestimmungen der Bundeskanzler im Einvernehmen mit dem Bundesminister für Justiz.

Österreichische Signaturverordnung

Verordnung über elektronische Signaturen (Signaturverordnung - SigV)

BGBl. II Nr. 30/2000

Auf Grund des § 25 Signaturgesetz, BGBl. I Nr. 190/1999, wird im Einvernehmen mit dem Bundesminister für Justiz verordnet:

Inhaltsübersicht

Gebühren für Aufsichtstätigkeiten

§ 1. (1) Für folgende individülle Leistungen der Aufsichtsstelle und der Telekom-Control GmbH sind von den Zertifizierungsdiensteanbietern nachstehende Gebühren zu entrichten:

1. Überprüfung und Registrierung eines Zertifizierungsdiensteanbieters anlässlich der Anzeige der Aufnahme seiner Tätigkeit (§ 6 Abs. 2 SigG),

   a) sofern der Zertifizierungsdiensteanbieter keine qualifizierten Zertifikate ausstellt und keine sicheren elektronischen Signaturverfahren bereitstellt: ..... 100 Euro;

   b) sofern der Zertifizierungsdiensteanbieter qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt: ..... 6 000 Euro;

2. Überprüfung eines Zertifizierungsdiensteanbieters anlässlich der Anzeige eines weiteren Sicherheits- und Zertifizierungskonzepts,

   a) sofern der Zertifizierungsdiensteanbieter keine qualifizierten Zertifikate ausstellt und keine sicheren elektronischen Signaturverfahren bereitstellt: ..... 50 Euro;

b) sofern der Zertifizierungsdiensteanbieter qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt:

aa) bei der Anzeige eines weiteren Sicherheits- und Zertifizierungskonzepts mit sicherheitsrelevanten Veränderungen: ..... 4 000 Euro;

bb) bei der Anzeige eines weiteren Sicherheits- und Zertifizierungskonzepts ohne sicherheitsrelevante Veränderungen: ..... 1 000 Euro;

3. Überprüfung eines Zertifizierungsdiensteanbieters anlässlich seiner beantragten Akkreditierung (§ 17 SigG): ..... 6 000 Euro;

4. Überprüfung eines Zertifizierungsdiensteanbieters im Falle der Anzeige grundlegender sicherheitsrelevanter Veränderungen eines bestehenden Sicherheits- und Zertifizierungskonzepts (§ 6 Abs. 5 SigG), wenn der Zertifizierungsdiensteanbieter qualifizierte Zertifikate ausstellt: ..... 4 000 Euro;

5.

a) regelmäßige Überprüfung eines Zertifizierungsdiensteanbieters
(§ 13 Abs. 1 SigG): ..... 4 000 Euro;

b) zusätzliche Überprüfung eines Zertifizierungsdiensteanbieters, wenn ein nicht nur unerheblicher Verstoß gegen die Bestimmungen des Signaturgesetzes oder der auf seiner Grundlage ergangenen Verordnungen festgestellt wird: ..... 6 000 Euro;

c) Überprüfung eines Zertifizierungsdiensteanbieters bei sicherheitsrelevanten Veränderungen des Sicherheits- und Zertifizierungskonzepts, sofern diese nicht der Aufsichtsstelle angezeigt wurden: ..... 6 000 Euro;

6. bescheidmäßig erteilte Auflagen bei sicherheitsrelevanten Mängeln
(§ 14 Abs. 6 SigG): ..... 1 000 Euro;

7. bescheidmäßige Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters
(§ 14 Abs. 2 bis 4 SigG): ..... 1 000 Euro;

8. Kontrolle der Einstellung der Tätigkeit eines Zertifizierungsdiensteanbieters
(§ 12 SigG): ..... 100 Euro;

9. Weiterführung des Widerrufsdienstes eines Zertifizierungsdiensteanbieters durch die Aufsichtsstelle (§ 12 und § 14 Abs. 5 SigG):
1 Euro pro im Widerrufsdienst geführtem Zertifikat und Jahr;

10. Führung der Verzeichnisse bei der Aufsichtsstelle (§ 13 Abs. 3 und § 17 Abs. 1 SigG): ..... 500 Euro pro Zertifizierungsdiensteanbieter und Jahr;
11. Beurteilung der Gleichwertigkeit von Prüfberichten einer staatlich anerkannten Stelle eines Drittstaates (§ 24 Abs. 3 SigG): ..... 6 000 Euro.

(2) Zur Abdeckung der laufenden Fixkosten der Aufsichtsstelle und der Telekom-Control GmbH haben die Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, eine Gebühr von 2 Euro pro ausgestelltem und gültigem qualifizierten Zertifikat und Jahr zu entrichten.

(3) Soweit sich die Aufsichtsstelle oder die Telekom-Control GmbH im Rahmen der Aufsicht nach dem Signaturgesetz oder der auf seiner Grundlage ergangenen Verordnungen einer Bestätigungsstelle oder anderer nichtamtlicher Personen oder Einrichtungen bedient, werden deren Gebühren nach § 53a AVG bestimmt und dem betroffenen Zertifizierungsdiensteanbieter als Barauslagen im Sinn des § 76 AVG vorgeschrieben.

(4) Die Gebühren werden von der Aufsichtsstelle mit Bescheid vorgeschrieben. Die Gebühren nach Abs. 2 werden anteilig für jedes Quartal im Nachhinein eingehoben. Zu diesem Zweck haben die Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, der Aufsichtsstelle jeweils bis zum 15. eines jeden Monats die Anzahl der von ihnen ausgestellen qualifizierten Zertifikate, die am Monatsersten gültig waren, bekanntzugeben.

Finanzielle Ausstattung der Zertifizierungsdiensteabieter

§ 2. (1) Die für die Ausübung der Tätigkeit als Zertifizierungsdiensteanbieter regelmäßig zur Verfügung stehenden Finanzmittel sind der Aufsichtsstelle mit Anzeige der Aufnahme der Tätigkeit nach § 6 Abs. 2 SigG bekanntzugeben. Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, haben ein Mindestkapital in Höhe von 300 000 Euro aufzuweisen. Dieses Mindestkapital muß in Form von Eigenmitteln im Sinn des § 224 Abs. 3A und B HGB vorliegen. Unter Nennkapital im Sinn des § 224 Abs. 3A HGB ist das eingezahlte Kapital im Sinn des § 23 Abs. 3 BWG zu verstehen.

(2) Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, haben zudem der Aufsichtsstelle mit Anzeige der Aufnahme der Tätigkeit nach § 6 Abs. 2 SigG das Eingehen einer Haftpflichtversiche-

rung mit einer Mindestversicherungssumme von 1 000 000 Euro je Versicherungsfall nachzuweisen.

(3) Von den Verpflichtungen nach den Abs. 1 und 2 sind der Bund, die Länder, Gemeindeverbände und Ortsgemeinden mit mehr als 50 000 Einwohnern befreit.

Erzeugung von Signaturerstellungsdaten für sichere elektronische Signaturen

§ 3. (1) Die Signaturerstellungsdaten der Aufsichtsstelle müssen dem Anhang I Punkt 1. entsprechen (Hauptsystem). Das Erzeugungssystem muss isoliert, ausschließlich für diesen Zweck bestimmt und auf angemessene Weise vor Eingriffen und Störungen geschützt sein. Die Aufsichtsstelle hat zu ihren Signaturerstellungsdaten ein Zweitsystem an Signaturerstellungsdaten (Zweitschlüssel) zu erzeugen und alle eigenen elektronischen Signaturen, mit denen die bei ihr geführten Verzeichnisse signiert werden, auch mit diesem Zweitsystem als Backup durchzuführen. Die Signaturprüfdaten (der öffentliche Signaturschlüssel) des Zweitsystems sind mit den Signaturerstellungsdaten der Aufsichtsstelle zu signieren. Das Zweitsystem ist unter Verschluss zu halten. Die Signaturprüfdaten des Zweitsystems dürfen nur bei einem Ausfall des Hauptsystems verwendet werden, sodass auch in einem solchen Fall der ungestörte Betrieb der Signatur- und Zertifizierungsdienste der Aufsichtsstelle sichergestellt ist. Werden von der Aufsichtsstelle zusätzlich auch andere als die im Anhang I Punkt 1. genannten Signaturerstellungsdaten eingesetzt, so sind die Zertifikate, die die entsprechenden Signaturprüfdaten enthalten, mit dem Hauptsystem zu signieren und elektronisch jederzeit allgemein abrufbar zu halten. Die Aufsichtsstelle hat sicherzustellen, dass die von ihr eingesetzten Signaturerstellungsdaten und die Signaturprüfdaten des entsprechenden Zertifikats in komplementärer Weise anwendbar sind.

(2) Die Signaturerstellungsdaten der Zertifizierungsdiensteanbieter müssen in deren Signaturerstellungseinheit erzeugt werden und dürfen diese nicht verlassen. Die erzeugten Signaturprüfdaten müssen der Aufsichtsstelle im Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters bekanntgegeben werden. Im Übrigen gelten die Anforderungen für sichere elektronische Signaturen der übrigen Signatoren.

(3) Die Signaturerstellungsdaten für sichere elektronische Signaturen der Signatoren müssen die im Anhang I Punkt 2. festgesetzte Mindestlänge aufweisen. Im Sicherheitskonzept des Zertifizierungsdiensteanbieters ist die tatsächliche Schlüssellänge der bereitgestellten Signaturverfahren unter Angabe des oberen und des unteren Grenzwertes anzuführen.

Die verwendeten Algorithmen müssen offengelegt sein. Die Signaturerstellungsdaten für sichere elektronische Signaturen dürfen mit an Sicherheit grenzender Wahrscheinlichkeit ausschließlich beim Signator vorkommen. Sie müssen nach dem jeweiligen Stand der Technik den eindeutigen Rückschluss auf den Signator ermöglichen. Die wiederholte Erzeugung von Signaturerstellungsdaten für sichere elektronische Signaturen darf nicht dazu führen, dass sich die Schlüsselqualität unter das für das jeweilige Signaturverfahren maßgebliche Sicherheitsniveau vermindert.

(4) Wiederholte Anwendungen der Signaturerstellungsdaten für sichere elektronische Signaturen dürfen nicht zu einer Verminderung der Schlüsselqualität führen. Anwendungen, die die Qualität der Signaturerstellungsdaten vermindern können (z.B. RSA-Anwendungen auf zufällig gewählte Daten), müssen wirksam ausgeschlossen sein. Die Signaturerstellungsdaten dürfen nur für diejenigen Zwecke verwendet werden, für die sie bestimmt sind.

(5) Die Erzeugung der Signaturerstellungsdaten für sichere elektronische Signaturen muss auf einer tatsächlichen Zufälligkeit beruhen, der ein technischer Zufall oder ein Signator-bezogener Zufall zu Grunde liegt. Die Signaturerstellungsdaten müssen in der im Anhang 1 Punkt 3. festgelegten Anzahl von Bitstellen durch tatsächliche Zufallselemente beeinflusst sein (qualitätsvoller Zufall). Die Zufallselemente müssen auf ihre Eignung hin ausreichend geprüft sein. Pseudozufallszahlen dürfen nicht als Ausgangsbasis verwendet werden. Wird das Erzeugungssystem für Signaturerstellungsdaten unterschiedlicher Signatoren eingesetzt, so ist ein verwendeter technischer Zufall periodisch, zumindest in Abständen von einem Monat, auf die statistische Zufallsqualität zu überprüfen. Die Prüfprotokolle sind zu dokumentieren. Liegt ein negatives Prüfergebnis vor, so sind die auf den betroffenen Signaturerstellungsdaten beruhenden Zertifikate, die seit dem letzten Prüfzeitpunkt mit positivem Ergebnis ausgestellt wurden, zu widerrufen.

(6) Werden die Signaturerstellungsdaten für sichere elektronische Signaturen beim Zertifizierungsdiensteanbieter erzeugt, so hat dieser geeignete Vorkehrungen zu treffen, die ein Bekanntwerden der Signaturerstellungsdaten oder anderer Daten, von denen sich die Signaturerstellungsdaten ableiten lassen, sowie eine Speicherung dieser Daten außerhalb der Signaturerstellungseinheit des Signators ausschließen. Dies gilt auch für die Übertragung solcher Signaturerstellungsdaten auf die Signaturerstellungseinheit des Signators sowie für die Daten zur Identifikation des Signators gegenüber der Signaturerstellungseinheit (z.B. PIN). Erfolgt die

Erzeugung der Signaturerstellungsdaten außerhalb der Signaturerstellungseinheit des Signators, so sind Erzeugungssysteme zu verwenden, die auf angemessene Weise vor Eingriffen und Störungen geschützt sind. Der Zugriff auf das Erzeugungssystem muss überwacht, jeder Anwender identifiziert und jede Verwendung registriert werden.

(7) Werden die Signaturerstellungsdaten für sichere elektronische Signaturen in der Signaturerstellungseinheit des Signators erzeugt, so darf der Zertifizierungsdiensteanbieter für die Erzeugung sowie die Speicherung der Signaturerstellungsdaten nur technisch geeignete Signaturerstellungseinheiten bereitstellen oder empfehlen.

Speicherung von Signaturerstellungsdaten für sichere elektronische Signaturen

§ 4. (1) Die Speicherung der Signaturerstellungsdaten für sichere elektronische Signaturen hat so zu erfolgen, dass deren Bekanntwerden ausgeschlossen ist und ihre Verwendung unter der ausschließlichen Kontrolle des Signators steht. Das Duplizieren von Signaturerstellungsdaten nach deren Erzeugung ist nicht zulässig.

(2) Zu besonderen Sicherheitszwecken können die Signaturerstellungsdaten für sichere elektronische Signaturen auf mehrere Signaturerstellungseinheiten verteilt werden. Die Sicherheitsanforderungen müssen in diesem Fall durch die Gesamtheit der betroffenen Signaturerstellungseinheiten erfüllt sein. Der Signator ist über die zur Auslösung der Signaturfunktion erforderlichen Maßnahmen zu unterrichten (§ 10 Abs. 7).

Technische Komponenten und Verfahren der Ausichtsstelle

§ 5. Die von der Aufsichtsstelle eingesetzten Systeme, insbesondere Produkte und technische Verfahren, müssen den Sicherheitsanforderungen für sichere elektronische Signaturen entsprechen. Die Aufsichtsstelle darf nur Algorithmen, die im Anhang 2 genannt sind, einsetzen.

Technische Komponenten und Verfahren der Zertifzierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen

§ 6. (1) Die von einem Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, eingesetzten Systeme, insbesondere Produkte und technische Verfahren, sind entsprechend ihrem aktüllen Stand und auf nachprüfbare Weise zu dokumentieren. Das Vorhandensein nicht doku-

mentierter Systemelemente sowie ein sicherheitsrelevantes Abweichen von der Dokumentation ist als Kompromittierung der Sicherheitsvorkehrungen zu werten. Dies gilt auch dann, wenn diese Systemelemente nicht für die Erbringung der Signatur- oder Zertifizierungsdienste notwendig sind. Werden die Systemelemente, die der Zertifizierungsdiensteanbieter zur Erbringung der Signatur- und Zertifizierungsdienste einsetzt, auch für andere Tätigkeiten verwendet, so dürfen die Systemelemente für die Erbringung der Signatur- und Zertifizierungsdienste in ihrer Wirkung nicht beeinflusst werden.

(2) Zur Erstellung sicherer elektronischer Signaturen sind Hashverfahren, die im Anhang 2 Punkt 2. genannt sind, einzusetzen. Die Algorithmen zur Erzeugung des Hashwerts sind bis zu dem im Anhang 2 Punkt 2. genannten Zeitpunkt als sicher anzusehen. Zur Ergänzung des Hashwerts dürfen auch Pseudozufallszahlen verwendet werden. Zur Verschlüsselung des Hashwerts sind Algorithmen, die im Anhang 2 Punkt 3. genannt sind, einzusetzen. Die Algorithmen zur Signaturerstellung sind bis zu dem im Anhang 2 Punkt 3. genannten Zeitpunkt als sicher anzusehen. Bei der Anwendung von Signaturalgorithmen, die Zufallszahlen benötigen (z.B. DSA), dürfen auch Pseudozufallszahlen verwendet werden.

(3) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, muss in der Lage sein, elektronische Signaturen sicher zu prüfen. Die Verfahren und Algorithmen zur Signaturprüfung bilden mit den Verfahren und Algorithmen zur Signaturerstellung eine logische Einheit und sind gemeinsam zu dokumentieren.

Technische Komponenten und Verfahren der Anweder für sichere elektronische Signaturen

§ 7. (1) Die Signatoren dürfen für die Erstellung sicherer elektronischer Signaturen nur solche Hashverfahren und Verfahren zur Verschlüsselung des Hashwerts einsetzen, die im Anhang 2 Punkt 2. und 3. genannt sind.

(2) Die von den Signatoren eingesetzten technischen Komponenten und Verfahren zur Erstellung sicherer elektronischer Signaturen müssen die vollständige Anzeige der zu signierenden Daten ermöglichen. Für die zu signierenden Daten dürfen nur die vom Zertifizierungsdiensteanbieter empfohlenen Formate verwendet werden. Die Spezifikation dieser Formate muss allgemein verfügbar sein. Können in einem Format auch dynamische Veränderungen oder unsichtbare Daten codiert werden, so dürfen die betreffenden Codierungen nicht verwendet werden. Der Zertifizierungsdiensteanbieter hat die Anwender anzuweisen oder ihnen Methoden

bereitzustellen, um dynamische Veränderungen oder unsichtbare Daten auszuschließen.

(3) Die Signaturfunktion in der Signaturerstellungseinheit des Signators darf nur nach Verwendung von Autorisierungscodes (z.B. PIN-Eingabe, Fingerabdruck) auslösbar sein. Die Anzahl der Signaturen, die mit einer Autorisierung des Signators gegenüber seiner Signaturerstellungseinheit ausgelöst wird, muss dem Signator bekanntgegeben werden. Das unbefugte Erfahren der Autorisierungscodes muss durch dessen Gestaltung und durch wirksame Sperrmechanismen praktisch ausgeschlossen sein. Derselbe Autorisierungscode darf nicht für unterschiedliche Anwendungen (z.B. Signatur- und Bankomatfunktion) verwendbar sein. Signaturerstellungseinheiten, die mehrere Anwendungen zulassen, wie z.B. Multiapplikationskarten oder Multiapplikationsterminals, dürfen nur verwendet werden, wenn die Maßnahmen und Methoden, die das Auslösen unterschiedlicher Anwendungen mit denselben Autorisierungscodes verhindern, im Sicherheitskonzept beschrieben sind. Die eingegebenen Autorisierungscodes dürfen von den verwendeten Systemelementen nicht gespeichert werden. Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungscodes müssen ausgeschlossen sein. Zu besonderen Sicherheitszwecken können die Autorisierungscodes auf mehrere Systemelemente verteilt werden. Der Signator ist über die zur Auslösung der Signaturfunktion erforderlichen Maßnahmen zu unterrichten (§ 10 Abs. 7).

(4) Als Signaturformate sind insbesondere die im Anhang 2 Punkt 4. genannten Formate geeignet.

(5) Will der Empfänger einer elektronisch signierten Erklärung eine sichere Signaturprüfung vornehmen, so hat er dafür Signaturprüfeinheiten zu verwenden, die im Sicherheitskonzept des Zertifizierungsdiensteanbieters, der das Zertifikat ausgestellt hat, für die sichere Signaturprüfung als geeignet bezeichnet sind. Diese Signaturprüfeinheiten müssen den Anforderungen des § 18 Abs. 4 SigG entsprechen.

Schutz der technischen Komponenten für sichere eletronische Signaturen beim Zertifizierungdiensteanbieter

§ 8. Der Zertifizierungsdiensteanbieter hat geeignete Vorkehrungen zu treffen, die die Signaturerstellungsdaten sowie die zum Erstellen der Zertifikate und die zum Abrufbarhalten der Verzeichnis- und Widerrufsdienste eingesetzten technischen Komponenten vor Kompromittierung und unbefugtem Zugriff schützen. Unbefugte Zugriffe müssen erkennbar sein.

Prüfung der technischen Komponenten und Verfahren für qualifizierte Zertifikate und sichere elektronische Signaturen

§ 9. (1) Zur Prüfung der technischen Komponenten und Verfahren für qualifizierte Zertifikate und sichere elektronische Signaturen sind geeignete und von einer Bestätigungsstelle anerkannte Sicherheitsprofile (Protection Profiles) der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation, ISO 15408) anwendbar.

(2) Die Prüfung der technischen Komponenten und Verfahren nach § 7 Abs. 2, § 10 und § 18 SigG kann auch nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), soweit anwendbar auch nach den Security Requirements for Cryptographic Modules (FIPS 140-1, level 2) oder dem British Standard (BS) 7799, erfolgen. Bei der Anwendung von ITSEC muss für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer elektronischer Signaturen und gegebenenfalls für die sichere Signaturprüfung die Evaluationsstufe E 3 mit der Mindeststärke der Sicherheitsmechanismen „hoch" eingehalten sein; bei den übrigen technischen Komponenten und Verfahren muss die Evaluationsstufe E 2 mit der Mindeststärke der Sicherheitsmechanismen „hoch" eingehalten sein.

(3) In der Bescheinigung der Erfüllung der Sicherheitsanforderungen für technische Komponenten und Verfahren ist anzugeben, für welche Anwendungen, unter welchen Bedingungen und bis zu welchem Zeitpunkt diese gilt. Eine Ausfertigung des Prüfberichts und der Bescheinigung ist der Aufsichtsstelle zu übermitteln .

Erbringung von Signatur- und Zertifizierungsdiensten für qualifizierte Zertifikate und sichere elektronische Signaturen

§ 10. (1) Werden die Einrichtungen eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, organisatorisch oder technisch getrennt geführt, so ist durch Sicherheitsmaßnahmen sicherzustellen, dass die Übertragung der Daten zwischen den Teileinrichtungen nicht zu einer Kompromittierung der Signatur- oder Zertifizierungsdienste führt.

(2) Die technischen Einrichtungen eines Zertifizierungsdiensteanbieters sind so zu gestalten, dass deren Funktionen und Anwendungen, die zu

den bereitgestellten Signatur- und Zertifizierungsdiensten gehören, von anderen Funktionen und Anwendungen getrennt sind. Eine Beeinflussung der Signatur- und Zertifizierungsdienste durch andere Funktionen und Anwendungen muss ausgeschlossen sein. Dies muss sowohl für den regulären Betrieb als auch für besondere Betriebssituationen und außerhalb des Betriebs sichergestellt sein. Besondere Betriebssituationen (z.B. Wartung) sind zu dokumentieren.

(3) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, hat geeignete Vorkehrungen zu treffen, die seine Einrichtungen zur Erbringung von Signatur- und Zertifizierungsdiensten vor unbefugtem Zutritt schützen.

(4) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, darf im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste nicht Personen beschäftigen, die wegen einer mit Vorsatz begangenen strafbaren Handlung zu einer Freiheitsstrafe von mehr als einem Jahr oder wegen strafbarer Handlungen gegen das Vermögen oder gegen die Zuverlässigkeit von Urkunden und Beweiszeichen zu einer Freiheitsstrafe von mehr als drei Monaten verurteilt wurden. Verurteilungen, die nach den Bestimmungen des Tilgungsgesetzes 1972 getilgt sind oder der beschränkten Auskunft unterliegen, bleiben außer Betracht. Die Zuverlässigkeit des Personals ist vom Zertifizierungsdiensteanbieter in Abständen von zumindest zwei Jahren zu überprüfen.

(5) Das technische Personal eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, muss über ausreichendes Fachwissen in folgenden Bereichen verfügen:

1. allgemeine EDV-Ausbildung,
2. Sicherheitstechnologie, Kryptographie, elektronische Signatur und Public Key Infrastructure,
3. technische Normen, insbesondere Evaluierungsnormen, sowie
4. Hard- und Software.

Auf Verlangen der Aufsichtsstelle muss der Zertifizierungsdiensteanbieter darlegen, durch welche einschlägige Ausbildung an anerkannten Bildungseinrichtungen oder durch welche einschlägigen fachlichen Tätigkeiten das ausreichende Fachwissen des Personals gegeben ist. Die Ausbildung des technischen Personals in den einzelnen Bereichen muss zumindest ein Jahr gedaürt haben. Das ausreichende Fachwissen kann z.B. durch Absolvierung einer einschlägigen Höheren Technischen Lehranstalt (HTL), einer solchen Fachhochschule oder eines einschlägigen Studiums erworben werden. Diese Ausbildung kann durch eine fachlich einschlägige Tätigkeit in der Daür von zumindest drei Jahren ersetzt werden.

(6) Werden die Signaturerstellungsdaten beim Zertifizierungsdiensteanbieter erzeugt, so dürfen sie nur an den Signator ausgehändigt werden. Die Möglichkeit der Verwendung der Signaturerstellungsdaten vor der Aushändigung an den Signator muss ausgeschlossen sein. In jedem Fall hat sich der Zertifizierungsdiensteanbieter darüber zu vergewissern, dass die Signaturerstellungsdaten des Signators und die Signaturprüfdaten des entsprechenden Zertifikats in komplementärer Weise anwendbar sind.

(7) Ein Zertifizierungsdiensteanbieter hat den Signator vor der erstmaligen Verwendung der Signaturerstellungsdaten über alle sicherheitsrelevanten Maßnahmen bei deren Anwendung (z.B. Sicherheit der Autorisierungscodes, Prüfung des Ausschlusses fremder Verwendung, Inanspruchnahme der Verzeichnis- und Widerrufsdienste, Möglichkeit der Anzeige zu signierender Daten, Verwendung geeigneter Formate) schriftlich oder unter Verwendung eines daürhaften Datenträgers klar und allgemein verständlich zu unterrichten.

Antrag auf Ausstellung eines qualifizierten Zertifikats

§ 11. (1) Der Zertifizierungsdiensteanbieter hat die Identität des Zertifikatswerbers anhand eines gültigen amtlichen Lichtbildausweises festzustellen. Der Antrag auf Ausstellung eines qualifizierten Zertifikats muss vom Zertifikatswerber eigenhändig unterschrieben sein. Vom vorgelegten Lichtbildausweis ist eine Ablichtung herzustellen, die mit dem Antrag zu dokumentieren ist. Ist ein solcher Antrag mit der sicheren elektronischen Signatur des Zertifikatswerbers versehen, so kann von der erneuten Feststellung seiner Identität abgesehen werden.

(2) Der Antrag auf Ausstellung eines qualifizierten Zertifikats hat insbesondere zu enthalten:

1. Namen, Datum und Ort der Geburt sowie Adresse des Zertifikatswerbers, Datum der Ausstellung und Nummer des vorgelegten Lichtbildausweises sowie die Behörde, die diesen ausstellte;
2. gegebenenfalls Angaben, ob das Zertifikat eine Einschränkung des Anwendungsbereichs oder eine Begrenzung des Transaktionswerts enthalten soll,
3. gegebenenfalls Angaben darüber, ob eine Vertretungsmacht für Dritte, andere rechtlich erhebliche Eigenschaften des Zertifikatswerbers, wie etwa eine berufsrechtliche oder sonstige Zulassung, oder weitere Angaben in das qualifizierte Zertifikat aufgenommen werden sollen.

(3) Wenn in ein qualifiziertes Zertifikat Angaben über die Vertretungsmacht für einen Dritten aufgenommen werden sollen, muss die Ver-

tretungsmacht zuverlässig nachgewiesen sein und eine schriftliche oder mit einer sicheren elektronischen Signatur versehene Einwilligung des Dritten vorliegen. Dieser ist über den Inhalt des qualifizierten Zertifikats schriftlich oder unter Verwendung eines daürhaften Datenträgers zu unterrichten und auf die Möglichkeit des Widerrufs nach § 9 Abs. 1 Z 1 SigG hinzuweisen. Eine berufsrechtliche oder sonstige Zulassung muss vor deren Aufnahme in ein qualifiziertes Zertifikat ebenfalls zuverlässig nachgewiesen sein. Untersteht der Signator im Hinblick auf eine eingetragene berufsrechtliche Qualifikation einer öffentlich-rechtlichen Berufsaufsicht, so ist die Einrichtung, die die Berufsaufsicht ausübt, über den Inhalt des qualifizierten Zertifikats schriftlich oder unter Verwendung eines daürhaften Datenträgers zu unterrichten.

Qualifizierte Zertifikate

§ 12. (1) Stellt ein Zertifizierungsdiensteanbieter neben qualifizierten auch andere Zertifikate aus, so muss er für die Signatur der qualifizierten Zertifikate gesonderte Signaturerstellungsdaten verwenden.

(2) Als Formate für qualifizierte Zertifikate sind insbesondere die im Anhang 2 Punkt 5. genannten Formate geeignet. Das Gleiche gilt für die Codierungen in qualifizierten Zertifikaten.

(3) Die Gültigkeitsdaür eines qualifizierten Zertifikats darf höchstens drei Jahre betragen und den Zeitraum der Eignung der eingesetzten technischen Komponenten und Verfahren sowie der zugehörigen Parameter nach den Anhängen 1 und 2 nicht überschreiten.

(4) Bis zum Ablauf der Gültigkeit eines qualifizierten Zertifikats ist es zulässig, mit Ausnahme der Gültigkeitsdaür dieselben Inhalte samt denselben Signaturprüfdaten neu zu zertifizieren und auf diese Weise ein neüs Zertifikat auszustellen. In allen anderen Fällen bewirken Zertifikate mit denselben Signaturprüfdaten und unterschiedlichen Inhalten eine Kompromittierung der betroffenen Zertifikate.

(5) Ein Zertifizierungsdiensteanbieter ist berechtigt, mit Zustimmung eines anderen Zertifizierungsdiensteanbieters dessen Zertifikat oder die von diesem ausgestellten Zertifikate zu zertifizieren. Die Zertifikate, die er auf diese Weise ausstellt, dürfen keine Modifikationen aufweisen; er hat auch für die Erbringung der Verzeichnis- und Widerrufsdienste Sorge zu tragen und gegebenenfalls die Widerrufe des anderen Zertifizierungsdiensteanbieters unmittelbar nachzuvollziehen.

Verzeichnis- und Widerrufsdienste für qualifizierte Zertifikate

§ 13. (1) Als Formate für Verzeichnis- und Widerrufsdienste sind insbesondere die im Anhang 2 Punkt 6. genannten Formate geeignet. Die Verzeichnis- und Widerrufsdienste können auch in unterschiedlichen Formaten bereitgestellt werden. Der Zertifizierungsdiensteanbieter hat sicherzustellen, dass die Formate der Widerrufsdienste für deren Weiterführung durch die Aufsichtsstelle geeignet sind. Werden die Verzeichnis- und Widerrufsdienste von einem anderen Zertifizierungsdiensteanbieter übernommen, so müssen diese weiterhin in denselben Formaten bereitgestellt werden.

(2) Der Zertifizierungsdiensteanbieter hat den Signatoren sowie Dritten, für die Angaben über die Vertretungsmacht des Signators in ein qualifiziertes Zertifikat aufgenommen wurden, geeignete Kommunikationsmöglichkeiten bekanntzugeben, mit denen diese jederzeit einen unverzüglichen Widerruf des Zertifikats veranlassen können. Dafür muss ein Authentifizierungsverfahren vorgesehen werden. Der Widerruf eines qualifizierten Zertifikats muss jedenfalls auch in Papierform möglich sein.

(3) Die Verzeichnis- und Widerrufsdienste müssen vor Fälschung, Verfälschung und unbefugtem Abruf ausreichend geschützt sein. Es muss sichergestellt sein, dass nur befugte Personen Eintragungen und Veränderungen in den Verzeichnissen vornehmen können. Weiters muss sichergestellt sein, dass eine Sperre oder ein Widerruf nicht unbemerkt rückgängig gemacht werden kann.

(4) Die Aktualisierung der Widerrufsdienste muss während der Geschäftszeiten spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgen. Die Geschäftszeiten müssen zumindest an Werktagen den Zeitraum von 9 bis 17 Uhr und an Samstagen den Zeitraum von 9 bis 12 Uhr umfassen. Außerhalb der Geschäftszeiten hat der Zertifizierungsdiensteanbieter jedenfalls dafür Sorge zu tragen, dass ein Verlangen auf Widerruf eines qualifizierten Zertifikats jederzeit automatisiert entgegengenommen wird und die Sperre auslöst.

(5) Die zeitliche Verfügbarkeit der Verzeichnisdienste muss im Sicherheitskonzept angegeben werden. Die Verzeichnisdienste müssen zumindest während der Geschäftszeiten nach Abs. 4 verfügbar sein. Die Widerrufsdienste müssen ständig verfügbar sein. Eine durchgehende Unterbrechung der Verzeichnis- oder der Widerrufsdienste von mehr als 30 Minuten während des Verfügbarkeitszeitraums ist als Störfall zu dokumentieren. Für Wartungs- und Ausfallsituationen des Widerrufsdienstes

ist ein Ersatzsystem bereitzustellen. Fällt auch das Ersatzsystem aus, so ist dies innerhalb eines Kalendertags der Aufsichtsstelle anzuzeigen. Diese hat innerhalb von drei Kalendertagen den Widerrufsdienst wiederherzustellen. Die Widerrufsdienste müssen allgemein frei zugänglich sein. Die Abfrage der Widerrufsdienste muss unentgeltlich und ohne Identifikation möglich sein.

(6) Ein Zertifizierungsdiensteanbieter hat die Verzeichnis- und Widerrufsdienste zumindest bis zum Zeitpunkt des erforderlichen Nachsignierens (§ 17) zu führen. Nach Ablauf dieser Frist hat der Zertifizierungsdiensteanbieter eine Überprüfung der qualifizierten Zertifikate bis zum Ablauf der in § 16 Abs. 2 genannten Frist im Einzelfall zu ermöglichen. Das Gleiche gilt für die Weiterführung der Widerrufsdienste durch die Aufsichtsstelle im Falle der Einstellung oder Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters.

(7) Der Zeitraum, während dessen eine Sperre wirksam sein kann, muss im Sicherheitskonzept angegeben werden. Dieser Zeitraum darf drei Werktage nicht übersteigen. Während dieses Zeitraums kann eine Sperre aufgehoben werden. Eine aufgehobene Sperre hat auf die Gültigkeit des Zertifikats keinen Einfluß. Wird eine Sperre während des genannten Zeitraums nicht aufgehoben, so ist das Zertifikat zu widerrufen. Erfolgt auf Grund einer Sperre der Widerruf eines Zertifikats, so gilt bereits die Sperre als Widerruf.

(8) Werden die Signaturerstellungsdaten des Signators bekannt oder kommen diese außer beim Signator als Signaturerstellungsdaten oder in anderer Form ein weiteres Mal vor, so liegt eine Kompromittierung der Signaturerstellungsdaten vor, die zum Widerruf des Zertifikats des Signators führen muss. Der Widerruf ist vom Signator zu verlangen (§ 9 Abs. 1 Z 1 SigG) oder vom Zertifizierungsdiensteanbieter aus eigenem vorzunehmen (§ 9 Abs. 1 Z 6 SigG), sobald er von der Kompromittierung Kenntnis erlangt.

Sichere Zeitstempeldienste

§ 14. (1) Für die Erbringung sicherer Zeitstempeldienste dürfen ausschließlich qualifizierte und nur für diesen Zweck ausgestellte Zertifikate verwendet werden. Dieser Verwendungszweck ist im Zertifikat zu bezeichnen.

(2) Die bescheinigte Zeitangabe (Datum und Uhrzeit) hat sich nach Mitteleuropäischer Zeit (MEZ) unter Beachtung der Sommerzeit zu richten; andere Zeitzonen sind ausdrücklich anzugeben. Die Abweichung von

der tatsächlichen Zeit darf beim Anbieter des Zeitstempeldienstes höchstens eine Minute betragen.

(3) Die zeitliche Verfügbarkeit sicherer Zeitstempeldienste muss im Sicherheitskonzept des Zertifizierungsdiensteanbieters, der solche Dienste bereitstellt, angegeben werden.

Sicherheits- und Zertifizierungskonzept für qualifizierte Zertifikate

§ 15. (1) Das Sicherheits- und Zertifizierungskonzept hat insbesondere folgenden Inhalt aufzuweisen:

1. Namen des Zertifizierungsdiensteanbieters,
2. Adresse des Zertifizierungsdiensteanbieters und Staat seiner Niederlassung,
3. Art, Anwendungsbereich und Erbringung der bereitgestellten Signatur- und Zertifizierungsdienste,
4. Verfahren zur Antragstellung,
5. gegebenenfalls Art und Weise der Aufnahme von Pseudonymen sowie von Angaben über eine Vertretungsmacht oder sonstige rechtlich erhebliche Eigenschaften des Signators in das Zertifikat,
6. Geschäftszeiten,
7. Erzeugung der Signaturerstellungsdaten des Zertifizierungsdiensteanbieters,
8. Format der Signaturerstellungsdaten des Zertifizierungsdiensteanbieters,
9. Signaturprüfdaten, gegebenenfalls das Zertifikat des Zertifizierungsdiensteanbieters,
10. Erzeugung der Signaturerstellungsdaten der Signatoren,
11. Format der Signaturerstellungsdaten der Signatoren,
12. eingesetzte Verfahren zur Erstellung der bereitgestellten Signaturen (Hashverfahren und Verfahren zur Verschlüsselung des Hashwerts),
13. Liste der eingesetzten, bereitgestellten und empfohlenen Signaturprodukte,
14. Sicherheit der Autorisierungscodes,
15. anwendbare Formate für zu signierende Dokumente und gegebenenfalls Methoden zur Verhinderung dynamischer Veränderungen,
16. Formate und Gültigkeitsdaür der Zertifikate,
17. technische Normen, Zugangsmodalitäten sowie Aktualisierungs- und Verfügbarkeitszeitraum für die bereitgestellten Verzeichnis- und Widerrufsdienste einschließlich des Zeitraums der Sperre,

18. gegebenenfalls Verfügbarkeitszeitraum bereitgestellter Zeitstempeldienste,
19. nachvollziehbare und allgemein verständliche Methode zur sicheren Signaturprüfung,
20. Format der Dokumentation von Sicherheitsvorkehrungen, Störfällen und besonderen Betriebssituationen,
21. Zeitraum und Verfahren des Nachsignierens,
22. Schutz der technischen Komponenten von unbefugtem Zugriff,
23. Schutz der Einrichtungen des Zertifizierungsdiensteanbieters vor unbefugtem Zutritt.

(2) Das Sicherheits- und Zertifizierungskonzept ist der Aufsichtsstelle in elektronischer Form im Format RTF, PDF, Ascii oder Postscript vorzulegen. Es muss mit der sicheren elektronischen Signatur des Zertifizierungsdiensteanbieters signiert sein. Der Zertifizierungsdiensteanbieter hat das Sicherheits- und Zertifizierungskonzept sowie eine Zusammenfassung klar und allgemein verständlich im Format RTF, PDF, Ascii oder Postscript elektronisch jederzeit allgemein abrufbar zu halten.

Dokumentation

§ 16. (1) Die Dokumentation nach § 11 SigG, einschließlich der Störfälle und der besonderen Betriebssituationen sowie der Unterrichtung der Zertifikatswerber nach § 20 SigG, muss jedenfalls in elektronischer Form erfolgen. Soweit die Erzeugung der Signaturerstellungsdaten außerhalb der Signaturerstellungseinheit des Signators erfolgt, gilt dies auch für den Zeitpunkt der Übertragung der Signaturerstellungsdaten auf die Signaturerstellungseinheit. Die in der Dokumentation eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, enthaltenen Daten müssen mit seiner sicheren elektronischen Signatur versehen sein und sichere Zeitstempel (§ 14) enthalten.

(2) Die Dokumentation nach Abs. 1 ist zumindest 33 Jahre ab der letzten Eintragung aufzubewahren und so zu sichern, dass sie innerhalb dieses Zeitraums lesbar und verfügbar bleibt.

Erneuerte elektronische Signatur (Nachsignieren)

§ 17. Der Zeitraum, nach dem eine neü sichere elektronische Signatur wegen drohender Verringerung des Sicherheitswerts angebracht werden sollte, muss im Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters angegeben werden. Dieses muss ein Nachsignieren jedenfalls vor Ablauf der in den Anhängen für die Sicherheit der eingesetzten Signaturerstellungsverfahren angegebenen Perioden vorsehen.

Beim Anbringen einer neün Signatur muss ein Zeitstempel verwendet werden.

Aufsicht und Akkreditierung

§ 18. (1) Die Anzeige der Aufnahme der Tätigkeit eines Zertifizierungsdiensteanbieters nach § 6 Abs. 2 SigG muss in elektronischer Form erfolgen. Soweit spezielle Inhalte der Anzeige nicht ein anderes Format erfordern, ist das Format RTF, PDF, Ascii oder Postscript zu verwenden. Die Anzeige muss elektronisch signiert sein. Die Aufsichtsstelle muss in der Lage sein, sich von der Echtheit der Daten zu überzeugen. Zu diesem Zweck kann sie auch das persönliche Erscheinen des Zertifizierungsdiensteanbieters oder eines vertretungsbefugten Organs anordnen. Stellt der Zertifizierungsdiensteanbieter qualifizierte Zertifikate aus, so hat sich die Aufsichtsstelle darüber zu vergewissern, dass die Signaturerstellungsdaten des Zertifizierungsdiensteanbieters und die Signaturprüfdaten des entsprechenden Zertifikats in komplementärer Weise anwendbar sind.

(2) Der Anzeige sind insbesondere anzuschließen:

1. Sicherheits- und Zertifizierungskonzept,
2. Darstellung der spezifischen sicherheitsrelevanten Bedrohungen und Risiken beim Zertifizierungsdiensteanbieter,
3. Nachweis der finanziellen Ausstattung sowie der erforderlichen Haftpflichtversicherung und
4. Nachweis des Fachwissens des technischen Personals.

(3) Die Anordnungen des Abs. 1 gelten für die Anzeige weiterer Sicherheits- und Zertifizierungskonzepte sowie für die Anzeige sicherheitsrelevanter Veränderungen bestehender Sicherheits- und Zertifizierungskonzepte sinngemäß.

(4) Die Aufsichtsstelle hat Zertifizierungsdiensteanbieter zumindest in regelmäßigen Abständen von zwei Jahren sowie bei sicherheitsrelevanten Veränderungen des Sicherheits- und Zertifizierungskonzepts zu überprüfen. Darüber hinaus ist die Aufsichtsstelle berechtigt, jederzeit stichprobenartige Überprüfungen der Zertifizierungsdiensteanbieter vorzunehmen. Die Aufsichtsstelle hat eine solche zusätzliche Überprüfung vorzunehmen, wenn ein begründeter Verdacht des Vorliegens sicherheitsrelevanter Mängel besteht.

(5) Die Aufsichtsstelle, ihre Organe sowie die für sie tätigen Personen und Einrichtungen unterliegen der Amtsverschwiegenheit im Sinn des Art. 20 Abs. 3 B-VG.

(6) In die bei der Aufsichtsstelle geführten Verzeichnisse dürfen nur solche Umstände aufgenommen werden, die auf ihre Richtigkeit hin

überprüft wurden. Für diese Verzeichnisse muss eines der im Anhang 2 Punkt 6. genannten Formate verwendet werden. Die Aufsichtsstelle muss eine allgemein zugängliche Homepage führen, in der ihre Adresse, ihre Signaturprüfdaten sowie die Formate der bei ihr geführten Verzeichnisse und die Zugangsmodalitäten zu diesen angegeben sind.

(7) Im Fall einer freiwilligen Akkreditierung nach § 17 SigG tritt der Antrag auf Akkreditierung an die Stelle der Anzeige der Aufnahme der Tätigkeit des Zertifizierungsdiensteanbieters.

(8) Die Kennzeichnung akkreditierter Zertifizierungsdiensteanbieter nach § 17 SigG hat die Wortfolge „Akkreditierter Zertifizierungsdiensteanbieter" zu enthalten. Akkreditierte Zertifizierungsdiensteanbieter sind berechtigt, das Bundeswappen mit dem Schriftzug „Akkreditierter Zertifizierungsdiensteanbieter" zu führen.

Hinweis auf die Notifikation

§ 19. Diese Verordnung wurde unter Einhaltung der Bestimmungen der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften in der Fassung der Richtlinie 98/48/EG der Europäischen Kommission notifiziert (Notifikationsnummer 99/0448/A).

Anhang 1
Parameter für technischen Komponenten und Verfahren für sichere elektronische Signaturen

1. Signaturerstellungsdaten der Aufsichtsstelle

Die Signaturerstellungsdaten der Aufsichtsstelle müssen dem Verfahren RSA (zur Verschlüsselung des Hashwerts) entsprechen (Hauptsystem).

Werden von der Aufsichtsstelle zusätzlich andere Signaturerstellungsdaten eingesetzt (§ 3 Abs. 1 vorletzter Satz), so muss es sich dabei um Signaturerstellungsdaten für sichere elektronische Signaturen handeln.

2. Signaturerstellungsdaten für sichere elektronische Signaturen

Die Schlüssellänge der Signaturerstellungsdaten für sichere elektronische Signaturen muss zumindest betragen:

- beim Verfahren RSA 1023 Bit,
- beim Verfahren DSA 1023 Bit,

– bei DSA-Varianten, die auf elliptischen Kurven basieren, 160 Bit.

Führende Nullbit sind in die Schlüssellänge nicht einzurechnen. Die Schlüssellänge ist jedenfalls für den geheimen Teil der Signaturerstellungsdaten maßgeblich.

3. Zufälle für Signaturerstellungsdaten für sichere elektronische Signaturen

Die Signaturerstellungsdaten für sichere elektronische Signaturen müssen zumindest in folgender Anzahl von Bitstellen durch tatsächliche Zufallselemente beeinflußt sein:

– bei den Verfahren RSA und DSA 1023 Bit,
– bei DSA-Varianten, die auf elliptischen Kurven basieren, 160 Bit.

In diesen Fällen liegt ein qualitätsvoller Zufall vor. Werden zur Sicherstellung der Einzigartigkeit von Signaturerstellungsdaten bei deren Erzeugung weitere Schlüsselelemente, z.B. führende oder nachlaufende Bit, in festgelegter oder in zufälliger Form eingebunden, so darf die Anzahl der durch einen qualitätsvollen Zufall beeinflussten Bitstellen dadurch nicht verringert werden.

4. Sicherheitsperiode

Die unter Punkt 1. bis 3. aufgezählten Schlüssellängen der Signaturerstellungsdaten sind unter Verwendung der genannten Algorithmen bis 31.12.2005 für den Einsatz bei sicheren elektronischen Signaturen als sicher anzusehen.

Anhang 2
Technische Verfahren und Formate

1. Technische Verfahren der Aufsichtsstelle

Bei der Aufsichtsstelle ist als Hashverfahren das Verfahren SHA-1 und zur Verschlüsselung des Hashwerts das Verfahren RSA einzusetzen (Hauptsystem). Die Verwendung des Chinese Remainder Theorem (CRT) ist nicht zulässig.

Werden von der Aufsichtsstelle zusätzlich andere Signaturerstellungsdaten eingesetzt (§ 3 Abs. 1 vorletzter Satz), so muss es sich bei den entsprechenden Verfahren zur Verschlüsselung des Hashwerts um solche für sichere elektronische Signaturen handeln.

2. Hashverfahren für sichere elektronische Signaturen

Folgende Hashverfahren werden als sicher anerkannt:

a) RIPEMD-160,

b) Funktion SHA-1.

Diese Hashverfahren sind bis 31.12.2005 für den Einsatz bei elektronischen Signaturen als sicher anzusehen.

Diesen Hashverfahren sind andere Verfahren gleichgestellt, die zumindest die gleiche Sicherheit aufweisen und von einer Bestätigungsstelle als solche anerkannt und veröffentlicht wurden.

3. Verfahren zur Signaturerstellung (Verschlüsselung des Hashwerts) für sichere elektronische Signaturen

Folgende Verfahren zur Signaturerstellung werden als sicher anerkannt:

a) RSA,

b) DSA,

c) DSA-Varianten, die auf elliptischen Kurven basieren:

- ISO/IEC 14883-3, Annex A.2.2 („Agnew-Mullin-Vanstone analogü"),
- IEEE-Standard P1363, Abschnitt 5.3.3 („Nyberg-Rüppel version"),
- IEEE-Standard P1363 [5], Abschnitt 5.3.4 („DSA version").

Für die Umsetzung sind nach Möglichkeit international anerkannte Methoden zu verwenden.

Die genannten Algorithmen sind bis 31.12.2005 für den Einsatz bei elektronischen Signaturen als sicher anzusehen.

Diesen Verfahren zur Signaturerstellung sind andere Verfahren gleichgestellt, die zumindest die gleiche Sicherheit aufweisen und von einer Bestätigungsstelle als solche anerkannt und veröffentlicht wurden.

4. Formate für sichere elektronische Signaturen

Die für sichere elektronische Signaturen eingesetzten Formate sollten einem international anerkannten Standard oder einer anerkannten Empfehlung (z.B. PKCS#7 Cryptographic Message Syntax Standard) entsprechen.

5. Formate für qualifizierte Zertifikate

Die European Electronic Signatures Standardization Initiative (EESSI) ist derzeit damit beschäftigt, Formate und Normen für die Darstellung qualifizierter Zertifikate sowie für deren Inhalte auszuarbeiten. Vorläufig wird empfohlen, international anerkannte Normungsvorschläge (z.B. X.509 v3 certificate oder X.509 v2 CRL for use in the Internet) anzuwenden. Die detaillierte Ausprägung des Formats ist im Sicherheits- und Zertifizierungskonzept darzustellen. Zur Beschreibung ist eine Formale Notation (z.B. CCITT bzw. ITU-T Recommendation X.208: Specification of Abstract Syntax Notation One - ASN.1 - 1988) zu verwenden. Dies gilt auch für die Codierung der Kennzeichnung „qualifiziert" in einem qualifizierten Zertifikat.

6. Formate für Verzeichnis- und Widerrufsdienste für qualifizierte Zertifikate

Die Verzeichnis- und Widerrufsdienste sollten in einem international anerkannten Format geführt werden. Für den Zugang zu den Verzeichnis- und Widerrufsdiensten werden insbesondere folgende internationale Normen empfohlen:

a) 1988 CCITT (ITU-T) X.500 / ISO IS9594,

b) RFC 2587 Internet X.509 Public Key Infrastructure LDAPv2 Schema,

c) RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile,

d) RFC 2589 Lightweight Directory Access Protocol (LDAPv3) Extensions for Dynamic Directory Services.

Literaturverzeichnis

Aichholzer/Schmutzer, Bericht/Information E-Government – Elektronische Informationsdienste auf Bundesebene in Österreich, Studie im Auftrag des Bundeskanzleramtes, 1999.

American Bar Association, Digital Signature Guidelines, 1996.

Angel, Why use Digital Signatures for Electronic Commerce, The Journal of Information, Law and Technology, JILT Commentary 2 (1999), http://www.law.warwick.ac.uk/jilt/99-2/angel.html.

Bahr, Signaturgesetze in Österreich, Deutschland und Italien, Zeitschrift des österreichischen Juristenverbandes, Nova & Varia 3 (1999), S. 71.

Baum, Die elektronische Identität? Datenschutz und Datensicherheit (1999), S. 511.

Baum, Gültigkeitsmodell des SigG, Die Gültigkeit der Signatur als Voraussetzung für die Sicherheitsvermutung nach § 11 SigG, Datenschutz und Datensicherheit (1999), S. 291.

Bauspieß/Scheerhorn, Zertifikatswechsel und Schlüsselgültigkeiten, Datenschutz und Datensicherheit (1997), S. 334.

Bellovin, Packets found on an Internet, 1993, http://www.research.att.com/~smb/papers/packets.pdf.

Bellovin, There Be Dragons, 1992, http://www.research.att.com/~smb/papers/dragon.pdf.

Berger, Signatur-Interoperabilitätsspezifikationen: Zertifikate und Dokumentenformate, Datenschutz und Datensicherheit (1999), S. 206.

Berleur, Self-Regulation and Democracy: Choice and Limits? Proceedings of the Joint IFIP WG 8.5 and WG 9.6 Working Conference 1999, S. 161, ISBN 91-7153-909-3, Kista Schweden.

Bertsch/Pordesch, Zur Problematik von Prozeßlaufzeiten bei der Sperrung von Zertifikaten, Datenschutz und Datensicherheit (1999), S. 514.

Bertsch/Rannenberg, Lean Infrastructures for Sustainable Digital Signatures, , Proceedings of the Joint IFIP WG 8.5 and WG 9.6 Working Conference 1999, S. 161, ISBN 91-7153-909-3, Kista Schweden.

Bichler/Kaukal/Werthner, Elektronische Märkte – Ein neuer Trend in der betrieblichen Beschaffung, in: *Schweighofer/Menzel* (Hg.), E-Commerce und E-Government, aktuelle Fragestellungen der Rechtsinformatik, Verlag Österreich (2000), S. 13.

Bizer, Das Schriftformprinzip im Rahmen rechtsverbindlicher Telekooperation, Datenschutz und Datensicherheit (1992), S. 169.

Bizer, Der gesetzliche Regelungsbedarf digitaler Signaturverfahren, Datenschutz und Datensicherheit (1995), S. 459.

Bizer, Gateway: Schriftform, Datenschutz und Datensicherheit (1992), S. 199.

Bizer/Hammer, Elektronisch signierte Dokumente als Beweismittel, Datenschutz und Datensicherheit (1993), S. 619.

Blattner-Zimmermann, Warum (BSI-) Zertifikate? Datenschutz und Datensicherheit (1998), S. 222.

Bleumer, Biometrische Ausweise, Schutz von Personenidentitäten trotz biometrischer Erkennung, Datenschutz und Datensicherheit (1999), S. 155.

Boriths Müller/Roessler, Zur rechtlichen Anerkennung elektronischer Signaturen in Europa, Datenschutz und Datensicherheit (1999), S. 497.

Borzo, InfoWorld Electric, Mai 1998, http://www.infoworld.com/cgi-bin/displayStory.pl?980511.eiecomm.htm.

Brenn, Das österreichische Signaturgesetz, ÖJZ (1999), S. 587.

Brenn, Haftet ein Internet-Service-Provider für die von ihm verbreiteten Informationen? ecolex (1999), S. 249.

Brenn, Signaturgesetz, Manz (1999).

Brenn, Verbürgung durch mouse-click? ecolex (1999), S. 243.

Brenn, Zivilrechtliche Rahmenbedingungen für den rechtsgeschäftlichen Verkehr im Internet, ÖJZ (1997), S. 641.

Brisch, EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr, Computer und Recht (1999), S. 235.

Brisch, Gemeinsame Rahmenbedingungen für elektronische Signaturen – Richtlinienvorschlag der Europäischen Kommission, Computer und Recht (1998), S. 492.

Britz, Urkundenbeweisrecht und Elektroniktechnologie, C.H. Beck (1996).

Brooks, Cypherpunks „brute" key cracking ring, http://www.brute.cl.cam.ac.uk/brute/, *Rescorla/Schiffman,* Internet-Draft, The Secure HyperText Transfer Protocol, ftp://ftp.isi.edu/in-notes/rfc2660.txt.

Brown, Techniques for Implementing the RSA Public Key Cryptosystem, Computer Science Department Report, University of New South Wales, Australian Defence Force Academy, Canberra: http://www.uni-siegen.de/security/krypto/rsa-tr-cs87-7.txt.

Brunner, Das elektronisch gespeicherte Dokument und dessen Beweischarakter, NZ (1996), S. 161.

Burkert, Ein Informationszugangsgesetz – auch für Deutschland, Datenschutz und Datensicherheit (1998), S. 430.

Bydlinski P., Die Notariatsaktpflicht 1850 und heute, NZ (1990), S. 289.

Bydlinski P., Telefaxbürgschaft: OGH folgt BGH, Recht der Wirtschaft (1996), S. 196.

Camphausen, Schlüsselzertifizierung mit PGP, Datenschutz und Datensicherheit (1998), S. 382.

Colleran, Standardisation issues for the European Trust Services (ETS), Quercus Information Ltd, UK (1997).

Coppersmith, The Data Encryption Standard and its Strength Against Attacks, IBM Research Report RC 18613 (81421), 1992.

Damker/Müller, Verbraucherschutz im Internet, Datenschutz und Datensicherheit (1997), S. 24.

Diffie/Hellman, Multiuser Cryptographic Techniques, AFIPS National Computer Conference 1976.

Diffie/Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory 1976.

Diregger, Kryptographie und Menschenrechte, Datenschutz und Datensicherheit (1998), S. 28.

Dobbertin, Digitale Fingerabdrücke, sichere Hashfunktionen für digitale Signaturen, Datenschutz und Datensicherheit (1997), S. 82.

Dumortier/Van Eecke/European Commission, The Legal Aspects of Digital Signatures, Mys & Bresch publishers (1999).

Ebbing, Schriftform und E-Mail, Computer und Recht (1995), S. 278.

Egan, ISO OSI 7 Layer Model forced with TCP/IP (2000), http://libweb.sonoma.edu/mike/networking/netmodels/isoosi7layermodel.html.

Eisele, Sicherheit und Elektronische Unterschriften – Smart Disk, Datenschutz und Datensicherheit (1995), S. 401.

Emmert, Haftung der Zertifizierungsstellen, Computer und Recht (1999), S. 244.

Engel-Flechsig, IuKDG vom Bundestag verabschiedet, Datenschutz und Datensicherheit (1997), S. 474.

Esslinger/Müller, Secure Sockets Layer (SSL) Protokoll, Datenschutz und Datensicherheit (1997), S. 691.

ETSI, Draft on Electronic Signature Standardization for Business Transactions, Draft ETSI ES 201 733, V1.1.3 (1999-09).

Europäische Kommission, Grünbuch über die Information des öffentlichen Sektors in der Informationsgesellschaft, KOM (1998) 585.

Europäische Kommission, Towards A European Framework for Digital Signatures and Encryption, Brüssel, 1997 verfügbar unter: http://www.ispo.cec.be/eif/policy/97503.html.

Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt (E-Commerce Richtlinie), KOM (1998) 586.

Europäisches Parlament und Rat, Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Amtsblatt Nr. L 013 vom 19. 1. 2000, S. 0012 – 0020, CELEX Nr. 31999L0093.

Fasching, Die Form der Schiedsvereinbarung – Schriftform und neu zugelassene technisch bedingte Übermittlungsformen (§ 577 Abs 3 ZPO), ÖJZ (1989), S. 289.

Fasching, Kommentar zu den Zivilprozeßgesetzen, Manz (1966).

Fasching, Lehrbuch des österreichischen Zivilprozeßrechts[10], Manz (1990).

Federrath, Schlüsselgenerierung in Trust Centern? Datenschutz und Datensicherheit (1997), S. 98.

Finocchiaro, A brief summary of Italian legislation on digital signature (1999), http://cwis.kub.nl/~frw/people/hof/ds-italy.htm.

Forgó, Was sind und wozu dienen digitale Signaturen? ecolex (1999), S. 235.

Fox, Datenschutz und Datensicherheit Report: 15 Kandidaten für den DES-Nachfolger „Advanced Encryption Standard", Datenschutz und Datensicherheit (1998), S. 606.

Fox, Eine kritische Würdigung des SigG, Datenschutz und Datensicherheit (1999), S. 508.

Fox, Fälschungssicherheit digitaler Signaturen, eine Übersicht, Datenschutz und Datensicherheit (1997), S. 69.

Fox, Gateway: Chaffing and Winnowing, Datenschutz und Datensicherheit (1998), S. 409.

Fox, Schlüsseltechnologie Kryptographie, Datenschutz und Datensicherheit (1998), S. 492.

Fox, Zu einem prinzipiellen Problem digitaler Signaturen, Datenschutz und Datensicherheit (1998), S. 386.

Freier/Karlton/Kocher, Internet-Draft The SSL Protocol 3, http://www.alternic.com/drafts/.

Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution (1995), http://www.law.miami.edu/~froomkin/articles/clipper.htm.

Geiger, Europäische Grundlagen des Informationsrechts, Proceedings zu der Jahrestagung der Deutschen Gesellschaft für Recht und Informatik E.V. 1999.

Gerscha, Beiträge zu ausgewählten gewerberechtlichen Fragen, WEKA-Verlag (1998).

Glade/Reimer/Struiff, Digitale Signaturen & Sicherheitssensitive Anwendungen, Datenschutz und Datensicherheit Fachbeiträge, Vieweg Verlag (1995).

Graf, Wer haftet beim Telebanking? ecolex (1999), S. 239.

Grant, Understanding Digital Signatures, Commerce Net Press (1997).

Gravesen/Dumortier/Van Eecke, Die europäische Signaturrichtlinie – Regulative Funktion und Bedeutung der Rechtswirkung, Mulimedia und Recht (1999), S. 577.

Grimm, Gateway: Electronic Commerce, Datenschutz und Datensicherheit (1997), S. 420.

Grimm, Wir brauchen das digitale Signaturgesetz, Datenschutz und Datensicherheit (1997), S. 286.

Grimm/Fox, Entwurf einer EU-Richtlinie zu Rahmenbedingungen „elektronischer Signaturen", Datenschutz und Datensicherheit (1998), S. 407.

Gruschitz, TÜViT – der Informatik – TÜV, Datenschutz und Datensicherheit (1998), S. 225.

Gschnitzer, Allgemeiner Teil des Bürgerlichen Rechts, Springer (1992).

Gundermann/Köhntopp, Biometrie zwischen Bond und Big Brother, Technische Möglichkeiten und rechtliche Grenzen, Datenschutz und Datensicherheit (1999), S. 143.

Hagemann/Schaup/Schneider, Sicherheit und Perspektiven elektronischer Zahlungssysteme, Datenschutz und Datensicherheit (1999), S. 5.

Hammer, Gateway: Infrastruktur, Datenschutz und Datensicherheit (1995), S. 293.

Hammer, Sicherungsinfrastrukturen und rechtliche Rahmenbedingungen, Datenschutz und Datensicherheit (1996), S. 147.

Hammer, TeleTrust: Verletzlichkeit und Verfassungsverträglichkeit eines Konzeptes für rechtssichere Transaktion in der Informationsgesellschaft, Datenschutz und Datensicherheit (1988), S. 391.

Hammer/Bizer, Beweiswert elektronisch signierter Dokumente, Datenschutz und Datensicherheit (1993), S. 689.

Hansen, Klare Sicht am Info-Highway, Geschäfte via Internet & Co., Orac (1996).

Heiler, Unbürokratische Zertifizierung? Private Zertifizierstellen für IT-Produkte und -Systeme, Datenschutz und Datensicherheit (1998), S. 224.

Hein/Rieder, Digitale Signaturen in den USA, Stand der Gesetzgebung und Praxis, Datenschutz und Datensicherheit (1997), S. 469.

Heun, Elektronisch erstellte oder übermittelte Dokumente und Schriftform, Computer und Recht (1995), S. 2.

Heuser, Verschlüsselung in der öffentlichen Verwaltung, Datenschutz und Datensicherheit (1996), S. 659.

Hillebrand, Sicherheit im Internet aus Sicht der Nutzer, Datenschutz und Datensicherheit (1998), S. 218.

Hinden von, Persönlichkeitsverletzungen im Internet: das anwendbare Recht, Mohr Siebeck (1999).

Hirsch, E-Cash – zivilrechtliche Einordnung, Haftungsfragen und europarechtliche Initiativen, Dissertation an der Universität Wien (1999).

Hirsch, Rechtliche Untersuchung des virtuellen Zahlungsmediums E-Cash, in: *Schweighofer/Menzel* (Hg.), E-Commerce und E-Government, Fragestellungen der Rechtsinformatik, Verlag Österreich (2000), S. 29.

Horster/Portz, Privacy Enhanced Mail (PEM), Ein Standard zur Sicherung des elektronischen Nachrichtenverkehrs im Internet, Datenschutz und Datensicherheit (1994), S. 434.

Horster/Schartner/Wohlmacher, Keymanagment, S. 40, Proceedings of the XV. IFIP World Computer Congress, Papp/Posch, Global IT Security, OCG Schriftenreihe (1998).

Hortmann, Wie sicher ist die PIN? (Scheckkarten Urteil des OLG Hamm), Datenschutz und Datensicherheit (1997), S. 532.

Hytha, Schlichten statt streiten? Vor- und Nachteile von EDV-Schiedsgerichten, EDV und Recht (1988), S. H 3, 2.

ICC, General Usage for International Digitally Ensured Commerce (GUIDEC), 1997 verfügbar unter: http://www.iccwbo.org/home/guidec/guidec.asp.

Informations- und Kommunikationsdienste-Gesetz – IuKDG, Beschlusses des Deutschen Bundestages vom 13. Juni 1997, BT-Drs. 13/7934 vom 11.06.1997.

ISTEV, Legal and Regulatory Issues for the European Trusted Services Infrastructure, European Commission, 1997.

*Jaburek/*Wölfl, Cyber-Recht: Marktplatz Internet – schrankenlose Geschäfte, Ueberreuter (1997).

Jud/Högler-Pracher, Die Gleichsetzung elektronischer Signaturen mit der eigenhändigen Unterschrift, ecolex (1999), S. 610.

Jud/Högler-Pracher, Schiedsverfahren mit modernen Kommunikationstechniken, ecolex (1999), S. 601.

Kelm, Signed in Germany, Datenschutz und Datensicherheit (1999), S. 526.

Kersten, debisZERT, Datenschutz und Datensicherheit (1998), S. 223.

Kilian, Möglichkeiten und zivilrechtliche Probleme eines rechtswirksamen elektronischen Datenaustauschs (EDI), Datenschutz und Datensicherheit (1993), S. 606.

Klauser, EuGVÜ und EVÜ, ecolex spezial, Manz (1999).

Kleinrock, Information Flow in Large Communication Nets, RLE, Quarterly Progress Report, Massachusets 1961.

Köhler, Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen (Teil 2), Datenschutz und Datensicherheit (1987), S. 7.

Köhler, Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen (Teil 3), Datenschutz und Datensicherheit (1987), S. 61.

Köhler, Die Problematik automatisierter Rechtsvorgänge, insbesondere Willenserklärungen, Archiv für zivilistische Praxis (1982), S. 126.

Köhler, Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen (Teil 1), Datenschutz und Datensicherheit (1986), S. 337.

Konf. d. Datenschutzbeauftragten des Bundes und der Länder (Deutschland), Anforderungen zur informationstechnischen Sicherheit von Chipkarten, Datenschutz und Datensicherheit (1997), S. 254.

Koziol, Bürgerliches Recht^{10}, Manz (1995).

Koziol, Österreichisches Haftpflichtrecht II^{2}, Manz (1984).

Kumbruck, Der „unsichere Anwender" – vom Umgang mit Signaturverfahren, Datenschutz und Datensicherheit (1994), S. 21.

Laga, Internet – Rechtsfreier Raum? Dissertation an der Universität Wien (1998).

Laga, Rechtsprobleme im Internet, Schriftenreihe Wissenschaft und Wirtschaftspraxis, Wirtschaftskammer Österreich (1998).

Laßmann, Bewertungskriterien zum Vergleich biometrischer Verfahren, Kriterienkatalog der Arbeitsgruppe 6 „Biometrische Identifikationsverfahren" von Tele TrusT Deutschland e. V., Datenschutz und Datensicherheit (1999), S. 135.

Lei/Massey, A Proposal for a new Block Encryption Standard, Proceedings zu EUROCRYPT 1990, Springer.

Lei/Massey, Markov Ciphers and Differential Cryptoanalysis, Proceedings zu EUROCRYPT 1991, Springer.

Lloyd, Information Technology Law (2nd Edition), Butterwoths (1997).

Lopez/Mana/Ortega, A Public Key Infrastructure for User Identification, Proceedings of the Joint IFIP WG 8.5 and WG 9.6 Working Conference 1999, S. 161, ISBN 91-7153-909-3, Kista Schweden.

Madl, Vertragsabschluß im Internet, ecolex (1996), S. 79[1]. *Eisenberger/Zuser*, Behörden und Zuständigkeiten nach dem Telekommunikationsgesetz 1997 unter besonderer Berücksichtigung der neu geschaffenen Regulierungsbehörde, Medien und Recht (1998), S. 90.

Martis, Verbraucherschutz, Beck, (1998).

Mayer-Schönberger, Das Recht am Info-Highway, Orac (1997).

Mayer-Schönberger/Pilz/Reiser/Schmölzer, Sicher und Echt: Der Entwurf eines SigG, Medien und Recht 3 (1998), S. 107 ff.

Mayer-Schönberger/Pilz/Reiser/Schmölzer, Signaturgesetz, Orac (1999).

Mayson, French and Ryan on Company Law, Blackstone Press (1996-97 edition).

Meents, Verbraucherschutz bei Rechtsgeschäften im Internet : Anwendung und Wirkung klassischer Instrumentarien des Verbraucherschutzrechts und der europäischen Fernabsatzrichtlinie, Schmidt (1998).

Menzel/Schweighofer, Das österreichische Signaturgesetz, Datenschutz und Datensicherheit (1999), S. 503.

Menzel/Schweighofer, Liability of Certification Authorities, Proceedings of the Joint IFIP WG 8.5 and WG 9.6 Working Conference 1999, S. 161, ISBN 91-7153-909-3, Kista Schweden.

Menzel/Schweighofer, Securing Electronic Commerce with Digital Signatures, Proceedings zur BILETA Konferenz: Cyberspace 1999, http://www.bileta.ac.uk/99papers/menzel.htm

Meyer, Der Schiedsgutachtervertrag, V. Florentz GmbH (1995).

Miedbrodt, Anwendungserfahrung ausgewählter US-amerikanischer Signaturgesetze, Datenschutz und Datensicherheit (1999), S. 194.

Miedbrodt, Regelungsansätze und -strukturen US-amerikanischer Signaturgesetzgebung, Datenschutz und Datensicherheit (1998), S. 389.

Mohr, Elektronischer Kauf – Verbraucherschutz im Fernabsatz, ecolex (1999), S. 247.

Möller/Pfitzmann/Stierand, Rechnergestützte Steganographie: Wie sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist, Datenschutz und Datensicherheit (1994), S. 318.

Müller/Paulus, Elliptische Kurven und Public Key Kryptographie, Datenschutz und Datensicherheit (1998), S. 496.

Müller/Pfau, Biometrische Verfahren zur Verifikation der Personenidentität, Datenschutz und Datensicherheit (1992), S. 346.

Müller/Wächter, Zur Aufnahme einer verschuldens-unabhängigen Schadenersatzregelung in das BDSG, Datenschutz und Datensicherheit (1989), S. 239.

Müller-Berg, EDI und Sicherheit, Datenschutz und Datensicherheit (1991), S. 514.

Nechvatal, Public Key Cryptography, in: *Simmons* (Hg.), Contemporary Cryptology: The Science of Information Integrety, IEEE Press (1992).

Nehl, Schlüsselgenerierung in Trust Centern? Datenschutz und Datensicherheit (1997), S. 100.

Nilson, Consolidation of the results of previous TTP work in INFOSEC programmes, Europäische Kommission (1997).

OECD, Guidelines for Cryptography Policy (1995).

Opplinger, Sicherheitsprotokolle für das Internet, Datenschutz und Datensicherheit (1997), S. 686.

Patel (et. al.), Support for Legal Framework and Anonymity in the KEYSTONE Public Key Infrastructure Architecture, Proceedings of the Joint IFIP WG 8.5 and WG 9.6 Working Conference 1999, S. 161, ISBN 91-7153-909-3, Kista Schweden.

Paulus/Müller, Zur Erzeugung kryptographisch starker elliptischer Kurven, Datenschutz und Datensicherheit (1998), S. 500.

Petersen, Privilege Managment Infrastruktur – PMI, Datenschutz und Datensicherheit (1999), S. 222.

Peterson, Faires elektronisches Geld, Datenschutz und Datensicherheit (1997), S. 647.

Pohl, Guidelines for the use of names and keys in a global TTP infrastructure (1997).

Polemi, Review and evaluation of Biometric Techniques for Identification and Authentication – Final Report, S. 8, DG Informationsgesellschaft – Infosec, April 1997, http://www.cordis.lu/infosec/src/stud5fr.htm.

Pordesch, Risiken elektronischer Signaturverfahren, Datenschutz und Datensicherheit (1993), S. 561.

Pordesch/Nissen, Fälschungsrisiken elektronisch signierter Dokumente, Computer und Recht (1995), S. 562.

Pordesch/Roßnagel/Schneider, Erprobung sicherheits- und datenschutzrelevanter Informationstechniken mit Simulationsstudien, Datenschutz und Datensicherheit (1993), S. 491.

Raab/Williams, Privacy in the GII: Issues, processes and solutions, Proceedings of the Joint IFIP WG 8.5 and WG 9.6 Working Conference 1999, S. 161, ISBN 91-7153-909-3, Kista Schweden.

Rannenberg, Sicherheitszertifizierung, Probleme, Trends und Chancen, Datenschutz und Datensicherheit (1998), S. 190.

Raßmann, Elektronische Unterschrift im Zahlungsverkehr, Computer und Recht (1998), S. 36.

Rechberger, Kommentar zur ZPO, Springer (1994).

Rechberger/Simotta, Grundriß des österreichischen Zivilprozeßrechts[5], Manz (1999).

Regulierungsbehörde für Telekommunikation und Post, Maßnahmenkatalog für digitale Signaturen – auf Grundlage von SigG und SigVO (1999).

Reimer, BioTrusT: Biometrie im Bankenbereich, Datenschutz und Datensicherheit (1999), S. 162.

Reimer, Datenschutz und Datensicherheit Report: Argentinien: Digitale Signaturen in der öffentlichen Verwaltung, Datenschutz und Datensicherheit (1998), S. 544.

Reimer, Datenschutz und Datensicherheit Report: Sonera Smart Trust: SIM-Karten für digitale Signatur, Datenschutz und Datensicherheit (1999), S. 244.

Reimer, Datenschutz und Datensicherheit Report: USA: Rekord bei Angriffen auf Kryptoalgorithmen, Datenschutz und Datensicherheit (1999), S. 182.

Reiser, Internet – die Sicherheitsfragen, Ueberreuter (1998).

Remotti, Legal and Regulatory Issues concerning the TTPs and Digital Signatures, ISTEV (1997).

Rescorla/Schiffman, SHTTP Draft, http://www.terisa.com/shttp/current.txt.

Rhein, Digitale Signatur mittels Smart Cards, Diplomarbeit an der Technischen Universität Wien (1997).

Riedl, Auch die UNCITRAL mengt sich in den elektronischen Geschäftsverkehr ein, ecolex (1999), S. 241.

Rihaczek, Das elektronische Unterschriftssurrogat, Datenschutz und Datensicherheit (1991), S. 568.

Rihaczek, Das elektronische Unterschriftssurrogat, Nachtrag, Datenschutz und Datensicherheit (1992), S. 14.

Rihaczek, Der elektronische Beweis – Die Lücke bei der Umsetzung zum Rechtsgebrauch, Datenschutz und Datensicherheit (1994), S. 127.

Roessler, PGP – „Kryptographie fürs Volk", Datenschutz und Datensicherheit (1998), S. 377.

Rohde/Witzel, Akkreditierung von Prüflaboratorien, Datenschutz und Datensicherheit (1998), S. 203.

Roßnagel, Anerkennung von Prüf- und Bestätigungsstellen nach dem Signaturgesetz, Multimedia und Recht (1999), S. 342.

Roßnagel, Das Signaturgesetz jetzt verbessern und verabschieden, Datenschutz und Datensicherheit (1997), S. 287.

Roßnagel, Das Signaturgesetz, eine kritische Bewertung des Gesetzesentwurfs der Bundesregierung, Datenschutz und Datensicherheit (1997), S. 75.

Roßnagel, Europäische Signaturrichtlinie und Optionen ihrer Umsetzung, Multimedia und Recht (1999), S. 261.

Roßnagel, Institutionell-organisatorische Gestaltung informationstechnischer Sicherungsinfrastrukturen, Datenschutz und Datensicherheit (1995), S. 259.

Roßnagel/Wedde/Hammer/Pordesch, Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, Westdeutscher Verlag (1990).

Rummel, Kommentar zum ABGB^2, Manz (1990).

Sacher, Report of the Group of High-Level Private Sector Experts on Electronic Commerce, OECD.

Schmelz/Stratil, Das neue Telekommunikationsgesetz, ecolex (1998), S. 267.

Schmittmann, Geschäfte und Werbung im Internet, Datenschutz und Datensicherheit (1997), S. 636.

Schneider, Gateway: Rechtsverbindliche Telekooperation, Datenschutz und Datensicherheit (1993), S. 524.

Schneider/Andre, ICE-TEL, Datenschutz und Datensicherheit (1997), S. 419.

Schützig, Prüfung und Zertifizierung von IT-Installationen, Datenschutz und Datensicherheit (1998), S. 207.

Schweighofer, Rechtsvorschriften gelten auch für das Internet, Computer Kommunikativ 6 (1998).

Schwimann, Praxiskommentar zum ABGB^2, Orac (1997).

Segal, A Short History of Internet Protocols at CERN, http://home.cern.ch/~ben/TCPHIST.html

Seidel, Dokumentenschutz im elektronischen Rechtsverkehr (I), Computer und Recht (1993), S. 409.

Seidel, Dokumentenschutz im elektronischen Rechtsverkehr (II), Computer und Recht (1993), S. 484.

Smeddinghoff, (Ed.), Online Law – The SPA's Legal Guide to Doing Business on the Internet, Addison-Wesley Developers Press (1996).

Smith/Clarke, Identification, Authentication and Anonymity in a Legal Context, Proceedings of the Joint IFIP WG 8.5 and WG 9.6 Working Conference 1999, S. 161, ISBN 91-7153-909-3, Kista Schweden.

Spiegel, Gesicherter Umschlagplatz, S/MIME-fähige E-Mail-Programme und -Plugins, c't 26 (1999), S. 160.

Stahr, Die Unterschrift, Allgemeine Richtlinien, Steuer- und Wirtschaftskartei (1981).

Stallings, Sicherheit im Datennetz, Prentice Hall (1995).

Stiegler, Alternativen zur heutigen Evaluations- und Zertifizierungspraxis, Datenschutz und Datensicherheit (1998), S. 211.

Telekom-Control-GmbH, Wie funktionieren elektronische Signaturen? 1999, http://www.tkc.at/WWW/Signatur.nsf/pages/funktion

Telekom-Control-Kommission, Konsultation zu den Anforderungen des Signaturgesetzes an die Geräte der Endbenutzer (2000), S. 12, http://www.tkc.at.

Thomsen/Wheble, Trading with EDI, The legal issues, IBC Financial Books (1989).

Timm, Signatur und Haftungsrecht, Datenschutz und Datensicherheit (1997), S. 525.

UNCITRAL, Working Group on Electronic Commerce, A/CN.9/WG.IV/WP.82-Draft Uniform Rules on Electronic Signatures, 1999.

UNCITRAL, Working Group on Electronic Commerce, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, General Assembly Resolution 51/162 of 16 December 1996.

Utah Parliament, Commentary to the Utah Digital Signature Act, 1996, http://www.commerce.state.ut.us/web/commerce/digsig/commact.htm.

Utah Parliament, Utah Digital Signature Act, 1996, http://www.commerce.state.ut.us/web/commerce/digsig/act.htm.

V*an der Hof* Digital Signature Law Survey, http://cwis.kub.nl/~frw/people/hof/DS-lawsu.htm.

Wagner, Notariatsordnung[4], Manz (1995).

Weichert, Datenschutzrechtliche Anforderungen an Chipkarten, Datenschutz und Datensicherheit (1997), S. 266.

Weis, Gateway: SkipJack, Datenschutz und Datensicherheit (1998), S. 530.

Weis/Lucks, KEA, Datenschutz und Datensicherheit (1998), S. 593.

Welsch, Stufenweise skalierbare Sicherheit für digitale Signaturen, Datenschutz und Datensicherheit (1999), S. 520.

Wiener, „Efficient DES Key Search", Proceedings zur Crypto 1993, Springer (1993).

Wilhelm, Telefax: Zugang, Übermittlungsfehler und Formfragen, ecolex (19909, S. 208.

Wirtz, Automatische Unterschriftsverifikation, Datenschutz und Datensicherheit (1994), S. 385.

Witzel, Gateway: Akkreditierung, Datenschutz und Datensicherheit (1998), S. 226.

World Trade Organisations, Electronic Commerce and the Role of WTO, WTO Special Studies, WTO Publications, 1998.

Wright, The Law of Electronic Commerce (EDI, E-Mail and Internet: Technology, Proof, and Liability, Little Brown and Company (1996).

Zarkon, Hobbes Internet Timeline, verfügbar unter: http://info.isoc.org/guest/zakon/Internet/History/HIT.html, A Brief History of the Internet, http://info.isoc.org/internet/history/brief.html.

Zepf, Beweissichere Archivierung elektronisch ausgetauschter Geschäftsdaten, Datenschutz und Datensicherheit (1991), S. 180.

Zib, Electronic Commerce und Risikozurechnung im rechtsgeschäftlichen Bereich, ecolex (1999), S. 230.

Zieschang, Sicherheitsrisiken bei der Schlüsselzertifizierung, Datenschutz und Datensicherheit (1997), S. 341.

Zimmermann, Interview mit *Phil Zimmermann*, Datenschutz und Datensicherheit (1998), S. 36.

Zuccato, Legislation and economical aspects of Electronic Money with special viewpoint on Europe, Proceedings of the Joint IFIP WG 8.5 and WG 9.6 Working Conference 1999, S. 161, ISBN 91-7153-909-3, Kista Schweden.

Zwißler, Gateway: Homebanking Computer Interface (HBCI), Datenschutz und Datensicherheit (1999), S. 45.

Zwißler, Secure Electronic Transaction – SET, Datenschutz und Datensicherheit (1998), S. 711.

Index