

JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN

Fachbereich Mathematik und Informatik, Physik und Geographie
Fachgebiet Mathematik, Schwerpunkt Informatik

Institut für Informatik

Professur für Software-Engineering

DIPLOMARBEIT

Rechtliche Anerkennung, kryptographische Algorithmen
und praktischer Einsatz
der elektronischen Signatur

gestellt von:

Prof. Dr. Dr. h.c. M. G. Zilahi-Szabó

vorgelegt von:

Christian Stach

Giessen, im Juni 2003

Inhaltsverzeichnis

Inhaltsverzeichnis	II
Abbildungsverzeichnis.....	V
Tabellenverzeichnis	VI
Abkürzungsverzeichnis	VII
1 Einleitung.....	1
1.1 Problemstellung	1
1.2 Vorgehensweise	1
2 Rechtliche Grundlagen der elektronischen Signatur	3
2.1 Das Signaturgesetz.....	3
2.1.1 Regulierungsbehörde für Post und Telekommunikation	4
2.1.2 Zertifizierungsstellen	5
2.1.3 Prüfstellen für Hard- und Software.....	6
2.1.4 Zertifikatsinhaber.....	6
2.1.5 Die Signaturverordnung.....	7
2.1.6 Maßnahmenkataloge.....	7
2.2 Die Signaturgesetzgebung in Europa.....	8
2.2.1 Die EU-Richtlinie 1999/93/E.....	9
2.3 Die Signaturgesetzgebung außerhalb der EU	11
2.4 Die Novellierung des Signaturgesetzes	12
2.4.1 Kritische Betrachtung des Signaturgesetzes	12
2.4.2 Das neue Signaturgesetz	13
2.4.3 Die neue Signaturverordnung	17
2.5 Weitere gesetzliche Regelungen zur elektronischen Signatur	18
2.5.1 Die elektronische Signatur im Bürgerlichen Gesetzbuch.....	18
2.5.2 Beweiswert elektronischer Signaturen.....	19
2.5.3 Verwaltungsverfahrensgesetz	20
2.5.4 Umsatzsteuergesetz.....	21
2.6 Fazit	23

3	Mathematische Grundlagen.....	25
3.1	Kryptologie	25
3.1.1	Die geschichtliche Entwicklung der Kryptologie.....	25
3.1.2	Ziele der Kryptographie.....	28
3.1.3	Grundlagen der Kryptologie	30
3.2	Verschlüsselungsverfahren	33
3.2.1	Symmetrische Verschlüsselung	33
3.2.2	Asymmetrische Verschlüsselung.....	40
3.2.3	Hybridverfahren.....	48
3.3	Signaturverfahren.....	49
4	Die elektronische Signatur in der praktischen Anwendung.....	57
4.1	Standards und Spezifikationen.....	61
4.1.1	ISIS-MTT.....	64
5	Anbieter elektronischer Signaturen.....	65
5.1	Zertifizierungsdiensteanbieter	65
5.2	Anbieter fortgeschrittener elektronischer Signaturen	67
5.3	Hardwareanbieter	68
6	Einsatzmöglichkeiten elektronischer Signaturen	70
6.1	Elektronischer Vertragsabschluss	70
6.2	Elektronische Archivierung	70
6.3	Elektronische Kommunikation	71
6.3.1	Das Pilotprojekt SPHINX.....	71
6.4	Das Home Banking Interface - HBCI.....	72
6.5	eGovernment.....	74
6.5.1	Die elektronische Steuererklärung - ELSTER.....	75
6.6	Die mobile elektronische Signatur.....	78
6.6.1	Das Pilotprojekt mSign.....	78
6.6.2	Das Pilotprojekt MoSign	80
6.6.3	Die Initiative Radicchio	81
6.6.4	Die Initiative Mobile electronic Transaction - MeT.....	81
6.7	Die elektronische Rechnung	82
7	Schlussbetrachtung.....	85
8	Literaturverzeichnis	89

Anhang	95
A 1 Gesetzestexte.....	95
A 2 Zahlentheorie	119
A 3 Zertifizierungsdiensteanbieter.....	125

Abbildungsverzeichnis

Abbildung 1: Die vier Säulen der digitalen Signatur.....	4
Abbildung 2: Die zweistufige Sicherheitsinfrastruktur des Signaturgesetzes 1997	4
Abbildung 3: Die Skytale von Sparta	26
Abbildung 4 : Kryptosystem.....	31
Abbildung 5 : Schema der symmetrischen Verschlüsselung.....	33
Abbildung 6 : Funktionsschema eines symmetrischen Verschlüsselungsalgorithmus...	34
Abbildung 7: Vigenere Quadrat.....	36
Abbildung 8 : Rundenschema des DES	38
Abbildung 9 : TripleDES Schema	39
Abbildung 10 : Schlüsselanzahl bei 6 Teilnehmern	40
Abbildung 11 : Schema der asymmetrischen Verschlüsselung	41
Abbildung 12 : Beispiel eines Public Key Konzeptes	41
Abbildung 13 : Schlüsselschema des Public Key Konzeptes	42
Abbildung 14: Wachstum der Schlüsselanzahl bei steigender Teilnehmerzahl	43
Abbildung 15 : Asymmetrische Verschlüsselung mit dem RSA Algorithmus	47
Abbildung 16 : Schema des Hybridverfahrens	49
Abbildung 17 : Signaturschema.....	50
Abbildung 18 : Kryptographische Hashfunktion.....	50
Abbildung 19 : Signatur erstellen	53
Abbildung 20 : Signatur überprüfen	54
Abbildung 21 : Klartext	55
Abbildung 22: Signieren einer Nachricht	58
Abbildung 23: Prüfung der Signatur mittels Zertifikat und Prüfsoftware	60
Abbildung 24: Der Aufbau einer HBCI-Nachricht.....	72
Abbildung 25: Der HBCI - Dialog	73
Abbildung 26: Aufbau des Projektes mSign.....	79

Tabellenverzeichnis

Tabelle 1: Verschlüsselung mit der Cäsarchiffre.....	26
Tabelle 2 : Polyalphabetische Verschlüsselung.....	35
Tabelle 3 : Beispiel einer Umwandlung in ASCII Werte	46
Tabelle 4: Hashwerte der Nachricht „a“	52
Tabelle 5: Hashwerte der Nachricht „A“	52
Tabelle 6 : Hashwerte der Nachricht „Die elektronische Signatur“	52
Tabelle 7 : Eigenschaften der Hashfunktionen	53
Tabelle 8: Vergleich der Schlüssellängen bei RSA und ECC	56
Tabelle 9: Preisübersicht der TeleSec.....	66
Tabelle 10: Preisübersicht der Signtrust	66
Tabelle 11: Preisliste der Kartenlesegeräte.....	69
Tabelle 12: Anzahl der abgegebenen elektronischen Steuererklärungen	76
Tabelle 13: Kostenvergleich Rechnungsübermittlung.....	82
Tabelle 14: Kostenvergleich Rechnungsbearbeitung	83
Tabelle 15 : ASCII Werte	123
Tabelle 16: Die akkreditierten Zertifizierungsdiensteanbieter laut RegTP	125
Tabelle 17: Die angezeigten Zertifizierungsdiensteanbieter laut RegTP	125

Abkürzungsverzeichnis

Abs	Absatz
BGB	Bürgerliches Gesetzbuch
BMI	Bundesministerium des Inneren
BSI	Bundesamt für Sicherheit
c` t	Magazin für Computer und Technik
DES	Data Encryption Standard
DSS	Digital Signature Standard
ECC	Eliptic Curves Cryptography
EGSRL	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen
eCommerce	Electronic Commerce
E-Mail	Electronic Mail
EU	Europäische Union
EWiR	Europäischer Wirtschaftsraum
ggT	größter gemeinsamer Teiler
GSM	Global System for Mobile Communication
HBCI	Home Banking Computer Interface
ISIS	Industrial Signature Interoperability Specification
ITSCC	Common Criteria for Information Technology Security
ITSEC	Information Technology Systems Evaluation Criteria
ITSEM	Information Security Evaluation Manual
ITU	International Telecommunication Union
IuKDG	Informations- und Telekommunikationsgesetz
M-Brokerage	Mobil-Brokerage
M-Business	Mobil-Business
M-Commerce	Mobil-Commerce
MD	Message Digest
MTT	Mail TrusT Standard
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCSP	Open Certificate Status Protocol

OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
PDA	personal digital assistant
PGP	Pretty Good Privacy
PKCS	Public Key Crypto System
PKI	Public Key Infrastruktur
RegTP	Regulierungsbehörde für Post und Telekommunikation
ROI	Return on Investment
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SigG97	Signaturgesetz in der Fassung vom 13. Juni 1997
SigG01	Signaturgesetz in der Fassung vom 16. Mai 2001
SigV97	Signaturverordnung in der Fassung vom 1. November 1997
SigV01	Signaturverordnung in der Fassung vom 16. November 2001
SIM-Karte	Subscriber Identification Module
StAndG	Steueränderungsgesetz
UstG	Umsatzsteuergesetz
Vgl	Vergleiche
WAP	Wireless application protocol
TÜV	Technischer Überwachungsverein
UNCITRAL	UN-Kommission für internationales Handelsrecht
ZKA	Zentraler Kreditausschuss
ZPO	Zivilprozessordnung

1 Einleitung

1.1 Problemstellung

Die handschriftliche Art des Unterschreibens existiert bereits seit vielen Jahrhunderten und ist typischer Weise an den materiellen Träger Papier gebunden. Sie garantiert den Ursprung eines Dokumentes und findet in zahlreichen Rechtsvorschriften Anwendung. In der heutigen modernen Informations- und Kommunikationsgesellschaft werden jedoch Daten immer häufiger elektronisch erzeugt. Die Etablierung des Internets im Privat- und Geschäftsverkehr fördert diese Entwicklung. Digitalisierte Dokumente und ihre Übermittlungswege haben neben den Vorteilen, wie die Archivierung auf kleinstem Raum und dem schnellen und kostengünstigen weltweiten Transport auch einige Nachteile. Die Identität des Erzeugers und die Integrität des Inhalts elektronischer Dokumente ist nicht immer gewährleistet. Der Versand von Daten über die Transportwege des Internets eröffnet unbefugten Dritten die Möglichkeit der Manipulation von Inhalt und Ursprung. Der Abschluss von Verträgen, der Kauf von Waren und Dienstleistungen, Bankgeschäfte per Mausclick oder die Kommunikation mit Behörden müssen jedoch dem Vergleich mit den bestehenden Gesetzen und Gepflogenheiten standhalten. Sie müssen authentisch, vertraulich und verbindlich sein. Um dies zu gewährleisten bedarf es im elektronischen Datenverkehr einer Art persönlicher Unterschrift, welche die Echtheit der Herkunft ebenso garantiert wie die Integrität der Inhalte. Dieser Herausforderung stellt sich die elektronische Signatur.

Ziel dieser Diplomarbeit ist es, die gesetzlichen Rahmenbedingungen der elektronischen Signatur zu erörtern, die mathematischen Grundlagen aufzuzeigen und Einsatzmöglichkeiten im Privat- und Geschäftsbereich vorzustellen.

1.2 Vorgehensweise

Im zweiten Kapitel werden die rechtlichen Aspekte der elektronischen Signatur erörtert. Ein Schwerpunkt liegt dabei auf der Darstellung des Signaturgesetzes. Anschließend wird die europäische Gesetzgebung durch die Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen verdeutlicht und auf die Entwicklung der Signaturmodelle außerhalb der EU eingegangen. Darauf folgend wird die Novellierung des Signaturgesetzes im Zuge der EU-Richtlinie dargestellt. Abschließend wird

die Änderung des Umsatzsteuergesetzes erläutert und der Beweiswert elektronischer Signaturen aufgezeigt.

Kapitel drei widmet sich den mathematischen Grundlagen der elektronischen Signaturen. Anfangs wird die geschichtliche Entwicklung der Kryptologie von den klassischen bis hin zu den modernen Verfahren erörtert. Ziele kryptographischer Algorithmen werden erläutert und die symmetrischen und asymmetrischen Verschlüsselungsverfahren beschrieben. Ein Schwerpunkt wird dabei auf die Darstellung des RSA Algorithmus gelegt, der sich zu einem Standard der Signaturerstellung entwickelt hat. Abschließend werden alternative Signaturverfahren dargestellt und ein Beispiel einer Signaturerstellung mittels RSA Algorithmus aufgezeigt.

Die praktische Umsetzung von elektronischen Signaturen wird im vierten Kapitel erörtert. Die Erstellung und Verifikation von qualifizierten elektronischen Signaturen wird detailliert aufgezeigt. Es werden Standards und Spezifikationen erläutert und deren Marktetablierung diskutiert.

Im fünften Kapitel wird ein Überblick der Anbieter elektronischer Signaturen gegeben und die Kosten qualifizierter elektronischer Signaturen dargelegt.

Kapitel sechs widmet sich den Anwendungen und Einsatzmöglichkeiten elektronischer Signaturen im Privat- und Unternehmensbereich.

Im abschließenden siebten Kapitel wird die gesetzliche Entwicklung und die aktuelle Gesetzeslage reflektiert. Die Sicherheit der eingesetzten kryptographischen Verfahren wird diskutiert und die Anwendungsmöglichkeiten auf den praktischen Einsatz untersucht. Der Ausblick geht auf eine mögliche weitere Entwicklung und Chancen eines Masseneinsatzes der elektronischen Signaturen ein.

Im Anhang ist das Signaturgesetz und die Rechtsverordnung in der aktuellen Fassung abgebildet. Des Weiteren sind zahlentheoretische Ergänzungen und eine Aufstellung der akkreditierten und angezeigten Zertifizierungsdiensteanbieter zu finden.

2 Rechtliche Grundlagen der elektronischen Signatur

2.1 Das Signaturgesetz

Die erste Fassung des Signaturgesetzes¹ (SigG97) wurde am 13. Juni 1997 als Artikel 3 des Informations- und Kommunikationsdienste Gesetz des Bundes (IuKDG) beschlossen und trat am 1. August 1997 in Kraft². Das deutsche Signaturgesetz ist das erste nationale Gesetz dieser Art, abgesehen von vereinzelt Regelungen auf bundesstaatlicher Ebene in den USA. Der Zweck des Signaturgesetzes ist es laut § 1:

„Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können.“³

Im Sinne des Signaturgesetzes ist

- eine **digitale Signatur** ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt.⁴
- ein **Zertifikat** eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person (Signaturschlüssel-Zertifikat).⁵

Um diese Rahmenbedingungen zu schaffen, baut die digitale Signatur auf vier Säulen auf. Diese stellen die Regulierungsbehörde für Post und Telekommunikation (RegTP), die Zertifizierungsstellen, Prüfstellen für Hard- und Software und die Zertifikatsinhaber dar.

¹ Vgl. BGBl (1997)

² Vgl. Artikel 11 IuKDG

³ Vgl. § 1 SigG97

⁴ Vgl. § 2 Abs. (1) SigG97

⁵ Vgl. § 2 Abs. (3) SigG97

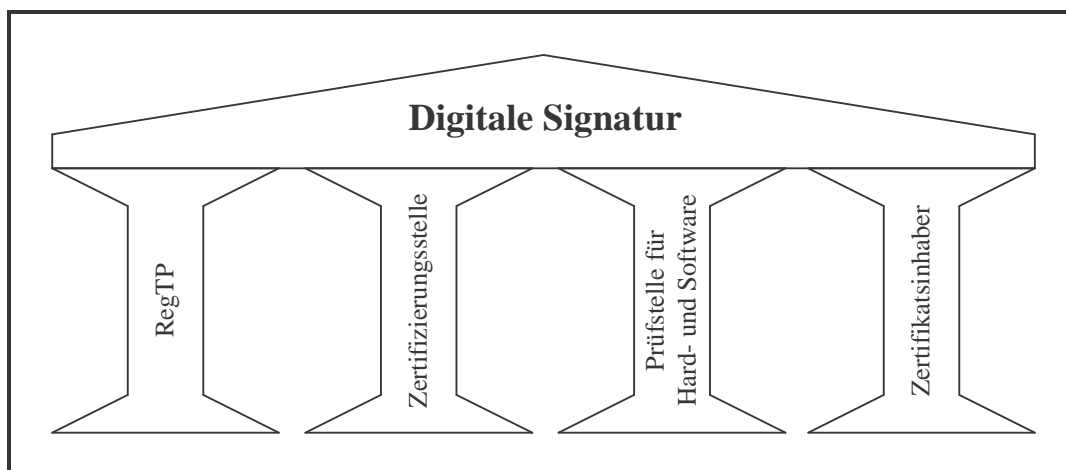


Abbildung 1: Die vier Säulen der digitalen Signatur

2.1.1 Regulierungsbehörde für Post und Telekommunikation

Als zuständige Behörde zur Erteilung der Genehmigungen von Zertifizierungsstellen, sowie die Überwachung der Einhaltung dieses Gesetzes und der Verordnung wird die **Regulierungsbehörde für Post und Telekommunikation (RegTP)** beauftragt⁶. Sie betreibt seit dem 1. Januar 1998 die oberste nationale Zertifizierungsinstanz⁷ (Wurzelinanz) und ist somit als alleinige Institution für das Ausstellen von Zertifikaten einer Zertifizierungsstelle verantwortlich⁸. Diese Zertifikate einer Zertifizierungsstelle werden zum Signieren der Teilnehmerzertifikate eingesetzt. Die zweistufige Hierarchie der Zertifizierungsstellen gewährleistet eine sichere Überprüfbarkeit der Zertifikate und eine authentische Zuordnung öffentlicher Signaturschlüssel zu natürlichen Personen⁹.

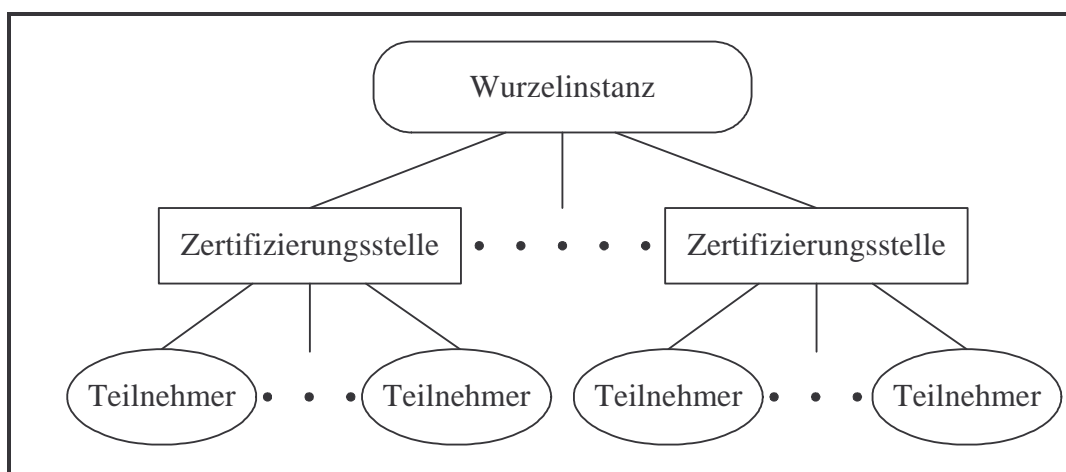


Abbildung 2: Die zweistufige Sicherheitsinfrastruktur des Signaturgesetzes 1997

⁶ Vgl. § 3 SigG97

⁷ Vgl. Webseite der Regulierungsbehörde. Online im Internet: [http:// www.regtp.de](http://www.regtp.de) FAQ (Stand 25.02.03)

⁸ Das öffentliche Zertifikatsverzeichnis der RegTP ist online im Internet unter [http:// www.nrca-ds.de](http://www.nrca-ds.de) abrufbar.

⁹ Vgl. REISEN, A. (1997), S. 2

2.1.2 Zertifizierungsstellen

Die **Zertifizierungsstellen** bilden das Herzstück der Sicherheitsinfrastruktur und müssen gemäß § 4 SigG97 vor Aufnahme der Tätigkeit durch die RegTP genehmigt werden. Ihre Aufgaben¹⁰ sind insbesondere:

- Die zuverlässige Identifizierung¹¹ einer Person, die ein Zertifikat beantragt.
- Die Generierung eines Schlüsselpaares bestehend aus öffentlichem und privatem Schlüssel.
- Die Signatur des Schlüssels und Teilnehmerdaten durch die Zertifizierungsstelle (Schlüsselzertifizierung).
- Das Übertragen des Zertifikates auf ein geeignetes Medium¹².
- Führung eines Verzeichnis- und Sperrdienstes zur Überprüfung und Sperrung von Zertifikaten.
- Das Anbieten eines Zeitstempeldienstes.

Eine Zertifizierungsstelle gibt folglich Zertifikate aus, welche eine eindeutige Zuordnung eines Schlüsselpaares zu einer bestimmten Person bestätigen. Diese Zertifikate werden in Verzeichnissen gespeichert, die jederzeit abrufbar sein müssen, um die Korrektheit von Signaturen zu überprüfen und die Sperrung von Zertifikaten zu ermöglichen.

Unter einem **Zeitstempel** wird eine signierte Bescheinigung einer Zertifizierungsstelle verstanden, die damit bestätigt, dass ihr bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Diese Leistung wird als Pflichtdienstleistung formuliert.

Ein **Zertifikat** ist vergleichbar mit einem digitalen Ausweis¹³, welches mindestens folgende Angaben¹⁴ enthalten muss:

- den Namen des Inhabers oder ein Pseudonym,
- eine laufende Zertifikatsnummer,
- den Namen der Zertifizierungsstelle,
- den öffentlichen Schlüssel und die Algorithmen, für welche der Schlüssel eingesetzt werden kann,
- gegebenenfalls Beschränkungen des Zertifikates,
- Beginn und Ende der Gültigkeit.

¹⁰ Vgl. § 5 SigG97

¹¹ Vgl. § 5 SigG97

¹² Dieses Medium wird meist durch eine Chipkarte verkörpert.

¹³ Vgl. HOCHMANN, S. (2001), S. 16

¹⁴ Vgl. § 7 SigG97

2.1.3 Prüfstellen für Hard- und Software

Die **Prüfstellen für Hard- und Software** werden durch die RegTP bestimmt. Diese Stellen prüfen gemäß § 14 SigG97 die technischen Komponenten, sowie das Sicherheitskonzept auf Gesetzeskonformität. Die Untersuchungen und Bestätigungen werden derzeit von folgenden drei anerkannten Stellen durchgeführt¹⁵.

- Das Bundesamt für Sicherheit in der Informationstechnik in Bonn.
(Veröffentlicht im Bundesanzeiger Nr. 31, S. 1787 vom 14. Februar 1998)
- T-Systems ISS GmbH in Bonn¹⁶.
(Veröffentlicht im Bundesanzeiger Nr. 52, S. 4142 vom 17. März 1999)
- TÜV Informationstechnik GmbH in Essen.
(Veröffentlicht im Bundesanzeiger Nr. 52, S. 4142 vom 17. März 1998)

Sie haben den Nachweis¹⁷ erbracht, dass sie

- die ausreichende Erfahrung in der Anwendung der Prüfkriterien,
- die notwendige Zuverlässigkeit sowie wirtschaftliche und finanzielle Unabhängigkeit,
- die Fachkunde zur ordnungsgemäßen Erfüllung der obliegenden Aufgaben besitzen.

Durch die Bestätigung einer erbrachten Sicherheit soll das Vertrauen und die Akzeptanz der Signaturen gefördert werden.

2.1.4 Zertifikatsinhaber

Das Signaturgesetz versteht unter einem **Zertifikatsinhaber** eine natürliche Person, die im Besitz eines Signaturzertifikates einer Zertifizierungsstelle ist. Diesem Vorgang geht gemäß § 5 SigG97 die Erstellung eines Antrages und eine zuverlässige Identifizierung des Antragstellers durch die Zertifizierungsstelle voraus. Die Aufnahme eines Pseudonyms und/oder berufsrechtlicher oder sonstiger Zulassungen steht dem Zertifikatsinhaber frei.

¹⁵ Eine aktuelle Liste der Prüfstellen ist online im Internet unter [http:// www.regtp.de](http://www.regtp.de) abrufbar.

¹⁶ Ehemals debis Systemhaus Information Security Services GmbH

¹⁷ Vgl. § 11 SigV01

2.1.5 Die Signaturverordnung

In § 16 SigG97 wird die Bundesregierung ermächtigt, durch Rechtsverordnung die erforderlichen Vorschriften zur digitalen Signatur zu erlassen. Diese Verordnung zur digitalen Signatur (SigV97)¹⁸ trat am 1. November 1997 in Kraft¹⁹. Sie regelt unter anderem das Genehmigungsverfahren der Zertifizierungsstellen²⁰ und deren Aufgaben, wie z.B. die Erstellung öffentlicher Verzeichnisse von Zertifikaten und die Unterrichtung der Antragsteller²¹ über die erforderlichen Maßnahmen zur Gewährleistung der Sicherheit von Signaturen. Zu diesen Maßnahmen gehört insbesondere der richtige Umgang mit dem privaten Signaturschlüssel und der Schutz technischer Komponenten vor unbefugtem Zugriff. Des Weiteren wird die Vergabe, Gültigkeitsdauer und Sperrung von Zertifikaten in der Verordnung festgelegt. So beträgt beispielsweise die Gültigkeitsdauer eines Zertifikates höchstens 5 Jahre²².

Das SigG97 und die SigV97 lassen Raum für innovative Lösungen und regeln grundsätzlich nur Zielvorgaben²³. Technische Standards und betriebliche Abläufe der Zertifizierungsstellen sind nicht Bestandteil des Gesetzes oder der Verordnung. Diese werden nach § 12 und § 16 SigV97 in zwei Maßnahmenkatalogen behandelt.

2.1.6 Maßnahmenkataloge

Für die Entwicklung eines Sicherheitskonzeptes für Zertifizierungsstellen und die Anforderungen an die technischen Komponenten wurde das Bundesamt für Sicherheit (BSI) beauftragt, das im Jahr 1998 zwei Maßnahmenkataloge²⁴ vorlegte. Die enthaltenen Maßnahmenbeschreibungen erheben den Anspruch grundsätzlich technikneutral zu sein, um den Raum für innovative Lösungen uneingeschränkt zu erhalten.

Der „**Maßnahmenkatalog für Zertifizierungsstellen nach dem Signaturgesetz**“ wurde gemäß § 12 SigV97 erstellt und richtet sich an die Betreiber der Zertifizierungsstellen, die einen gesetzeskonformen Aufbau des Zertifizierungsbetriebes erstreben. Der Katalog beinhaltet unter anderem Empfehlungen und Gesetzeserläuterungen zu den Vorgängen der Ausstellung von Zertifikaten, dem Aufbau von Verzeichnissen und der Antragstellung.

¹⁸ Vgl. BGBl (1997)

¹⁹ Vgl. § 19 SigV97

²⁰ Vgl. § 1 SigV97

²¹ Vgl. § 4 SigV97

²² Vgl. § 7 SigV97

²³ Vgl. HOCHMANN, S. (2001), S. 32

²⁴ Vgl. Webseite des BSI. Online im Internet unter <http://www.bsi.de>, Maßnahmenkataloge (Stand 26.02.03)

Der „**Maßnahmenkatalog für technische Komponenten nach dem Signaturgesetz**“ wurde gemäß § 16 SigV97 verfasst und richtet sich an die Hersteller der technischen Komponenten. Der Katalog umfasst unter anderem die Verfahren zur Erzeugung und Speicherung von Signaturschlüsseln, Zertifikat- und Signaturprüfung. Des Weiteren erarbeitete das BSI „Angaben zum Maßnahmenkatalog“ und einen „Anforderungskatalog zur Infrastruktur für Zertifizierungsstellen“. Diese Dokumente beinhalten beispielsweise bauliche Maßnahmen, Zutrittskontrollen, Kryptoalgorithmen und Lösungsvorschläge.

2.2 Die Signaturgesetzgebung in Europa

In den Mitgliedsstaaten der EU entwickelten sich ebenfalls gesetzliche Rahmenbedingungen zur digitalen Signatur. In Italien trat im Jahr 1997 eine Verordnung über Kriterien und Methoden der Anwendung und Versendung von elektronischen Dokumenten in Kraft. In Spanien können Signaturen aufgrund einer Entscheidung des höchsten Gerichtshofes vom 3. November 1997 eingesetzt werden und in Österreich wird sie durch ein Gesetz seit dem Jahr 1999 geregelt²⁵. Um eine heterogene Regulierung in den einzelnen Mitgliedstaaten zu vermeiden, forderte das EU-Parlament bereits im September 1996 die Kommission auf, „Regelungen über Vertraulichkeit und Sicherheit elektronischer Kommunikation zu entwickeln“²⁶. Ziel war es einen einheitlichen Rechtsrahmen für elektronische Signaturen zu schaffen, um die Interoperabilität von Produkten für elektronische Signaturen zu fördern und den freien Warenverkehr innerhalb der EU zu gewährleisten²⁷. Am 13. Dezember 1999 wurde die „**Richtlinie 1999/93/E des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen**“ (EGSRL)²⁸ verabschiedet. Diese Richtlinie trat am 19. Januar 2000 in Kraft und musste nach Artikel 13 bis zum 19. Juli 2001 von den Mitgliedsstaaten umgesetzt werden.

²⁵ Vgl.: HOCHMANN, S. (2001), S. 60

²⁶ Vgl. LUTZENBERGER, T. (2002), S. 57

²⁷ Vgl. Erwägungsgrund 5 EGSRL (1999)

²⁸ Vgl. AMTSBLATT DER EUROPÄISCHEN GEMEINSCHAFT (1999)

2.2.1 Die EU-Richtlinie 1999/93/E

„Diese Richtlinie soll die Verwendung elektronischer Signaturen erleichtern und zu ihrer rechtlichen Anerkennung beitragen.“²⁹ Die EU-Richtlinie regelt im Gegensatz zum SigG97 nicht ausschließlich digitale Signaturen, sondern elektronische Signaturen im Allgemeinen.

Aus der Richtlinie lässt sich folgende Definition ableiten:

1. Als **elektronische Signatur** werden alle Identifizierungsmittel, wie elektronische Zeichen oder Symbole, die zur Authentifizierung einer Nachricht oder eines Dokumentes dienen, bezeichnet.
2. Im Unterschied dazu ist eine **digitale Signatur** eine elektronische Signatur, die meist auf kryptographischen Funktionen basiert, um die Authentizität und Integrität einer Nachricht sicherzustellen.

Die Ausweitung des Regelungsbereiches auf die elektronischen Signaturen wurde bewusst vollzogen, um Anbietern von Zertifikaten die Möglichkeit zu bieten neben den digitalen Signaturen basierend auf einer Public Key Infrastruktur auch alternative Verfahren³⁰ einzusetzen.

Die Begriffsbestimmungen werden in Artikel 2 EGSRL wie folgt vollzogen:

1. Eine **elektronische Signatur** bezeichnet Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.
2. Eine **fortgeschrittene elektronische Signatur** bezeichnet eine elektronische Signatur, 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.
3. Ein **Zertifikat** bezeichnet eine elektronische Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und die Identität dieser Person bestätigt wird.

²⁹ Vgl. Erwägungsgrund 16 EGSRL (1999)

³⁰ Vgl.: Kapitel 2.3 „Die Gesetzgebung außerhalb der EU“

4. Ein **qualifiziertes Zertifikat** bezeichnet ein Zertifikat, das bestimmte Inhaltsangaben³¹ erfüllt und von einem Zertifizierungsdiensteanbieter bereitgestellt wird, der den Anforderungen nach Anhang II der Richtlinie nachkommt.
5. Ein **Zertifizierungsdiensteanbieter** bezeichnet eine Stelle oder eine juristische oder natürliche Person, die Zertifikate ausstellt oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellt.
6. Eine **sichere Signaturerstellungseinheit** ist eine konfigurierte Soft- oder Hardware, die zur Implementierung der Signaturerstellungsdaten verwendet wird.

Die EU-Richtlinie unterscheidet einfache und fortgeschrittene elektronische Signaturen. Während die einfachen elektronischen Signaturen nicht geregelt werden, sind die fortgeschrittenen technischen und organisatorischen Sicherheitsanforderungen unterworfen. Diese werden im Anhang der EU-Richtlinie aufgeführt und beziehen sich auf die qualifizierten Zertifikate, deren Anbieter und sichere Signaturerstellungseinheiten.

Das Betreiben eines Zertifizierungsdienstes ist nicht genehmigungspflichtig, es wird jedoch ein einzelstaatliches System zur Überwachung der Anbieter von qualifizierten Zertifikaten gefordert. Den Mitgliedsstaaten ist es freigestellt, ein freiwilliges Akkreditierungssystem einzuführen, um das Vertrauen und die Sicherheit der Signatur zu steigern.³²

Im Gegensatz zum SigG97 wird für fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und von einer sicheren Signaturerstellungseinheit erstellt wurden, gefordert³³, dass sie

- 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.
- in Gerichtsverfahren als Beweismittel zugelassen sind.

Eine Haftungsregelung³⁴ für Anbieter von qualifizierten Zertifikaten ist ebenfalls Bestandteil der Richtlinie und wurde als Mindestregelung formuliert. Weitere Haftungsbestimmungen unterliegen den einzelstaatlichen Gesetzen.

Ausländische Zertifikate müssen gleichgestellt behandelt werden, wenn sie

- die EU-Richtlinie erfüllen oder
- ein EU ansässiger Zertifizierungsdiensteanbieter für das Zertifikat einsteht oder

³¹ Vgl. Anhang I EGSRL (1999)

³² Vgl. Artikel 3 EGSRL (1999)

³³ Vgl. Artikel 5 EGSRL (1999)

³⁴ Vgl. Artikel 6 EGSRL (1999)

- sie durch Vereinbarungen zwischen der Gemeinschaft und Drittländern anerkannt sind³⁵.

2.3 Die Signaturgesetzgebung außerhalb der EU

Das PKI Modell, welches im SigG97 für die elektronische Signatur in Deutschland vorgeschrieben ist, ebnet den Weg für einen sicheren und weltweiten Datenaustausch. Die EU-Richtlinie fördert die Akzeptanz und die Interoperabilität der Signaturen, da sie gemeinschaftliche Rahmenbedingung für die 15 Mitgliedsstaaten bereitstellt. Es ist abzuwarten, ob diese zu einem einheitlichen technischen Standard und zu einer europaweiten interoperablen PKI führen.

Außerhalb der EU ist es notwendig einheitliche Standards zu etablieren und einzelstaatliche Sonderlösungen zu vermeiden³⁶. Weltweit haben sich vier Modelle³⁷ durchgesetzt, welche die elektronische Kommunikation regeln:

1. Das PKI Modell

Bei Anwendung des Public Key Modells³⁸ besitzt jeder Teilnehmer stets ein Schlüsselpaar, wobei die öffentlichen Schlüssel in einem allgemein zugänglichen Schlüsselverzeichnis geführt werden. Dieses Modell bietet bisher den höchsten Sicherheitsstandard, es ist jedoch in der Ausführung sehr kostenintensiv und begrenzt den Raum für die Entwicklung neuer Technologien.

2. Das Criteria based Modell

Das Criteria based Modell stellt bestimmte gesetzliche Anforderungen an eine elektronische Signatur. Es ist technologieunabhängig, erkennt aber nur Verfahren an, die einen bestimmten Sicherheitsstandard erfüllen und fördert verschiedene Systeme und unterschiedliche Preisstrukturen. Die EU-Richtlinie beispielsweise basiert auf diesem Modell.

3. Das Signature enabling Modell

Das Signature enabling Modell fordert die Beseitigung der Barrieren, die Schriftform und eigenhändige Unterschrift vorschreiben, um die Gleichstellung von elektronischer Signatur und handschriftlicher Unterschrift zu fördern. An eine Signatur werden keine technischen und organisatorischen Anforderungen

³⁵ Vgl. Artikel 7 EGSRL (1999)

³⁶ Vgl. HOCHMANN, S. (2001), S. 65

³⁷ Vgl. HOEREN, T., SCGÜNGEL, M. (1999) S. 385f

³⁸ Vgl. Kapitel 3.2.2 „Asymmetrische Verschlüsselung“

gestellt, so werden alle elektronischen Zeichen akzeptiert, welche zur Authentifizierung von Dokumenten dienen. Das Signature enabling Modell geht im Gegensatz zum PKI Modell einen konträren Weg, da es sehr offen gegenüber neuen Technologien ist. Es sieht jedoch keine Sicherheitsstandards vor und behindert somit eine allgemeine Anerkennung aller elektronischer Signaturen.

4. Das Hybrid Modell

Das Hybrid Modell vereint verschiedene Elemente der vorangegangenen Modelle, so werden digitale und elektronische Signaturen als gleichwertig anerkannt. Es ist folglich sehr flexibel und kann sich der gegebenen Marktlage anpassen. Die Public Key Infrastruktur einer Hybrid Lösung muss jedoch einer Kontrolle unterliegen, um die Sicherheit des Verfahrens zu gewährleisten.

2.4 Die Novellierung des Signaturgesetzes

2.4.1 Kritische Betrachtung des Signaturgesetzes

Deutschland hat mit der Gesetzgebung zur digitalen Signatur eine Vorreiterrolle innerhalb der EU übernommen. Wie aus der Darstellung bereits ersichtlich wurde, sind einige Bereiche stark reglementiert, andere Bereiche hingegen wurden vernachlässigt. Die Bundesregierung stieß damit auf Kritik von Anwendern und Anbietern von Sicherheitstechnologien.

Im Folgenden wird auf die wichtigsten Kritikpunkte³⁹ eingegangen:

1. Haftung

Das SigG97 sieht keine speziellen Haftungsregelungen für Zertifizierungsstellen vor, es gelten lediglich die allgemeingültigen Haftungsregelungen. Fraglich ist, ob und wie Zertifizierungsstellen für die ordnungsgemäße Durchführung der Pflichtdienstleistungen verantwortlich und im Schadensfalle haftbar zu machen sind.

2. Zertifizierungsstellen

Zertifizierungsstellen werden durch das Gesetz stark reglementiert. Die geforderten Sicherheitsmaßnahmen werden hoch eingestuft, sind schwer umzusetzen und mit hohen Kosten verbunden. Diese Tatsache begründet auch eine Warte-

³⁹ Vgl. HOCHMANN, S. (2001) S. 72f.

zeit von achtzehn Monaten zwischen der Einführung des Signaturgesetzes und der Marktreife der ersten Zertifizierungsstellen. Eine Gefahr stellt die flache zweistufige Zertifizierungshierarchie dar. So kann die Sicherheit des gesamten Systems durch das Brechen eines Privat Key der Wurzelinstanz in Frage gestellt werden.

3. Ausländische Zertifikate

Ausländische Zertifikate aus anderen Mitgliedsstaaten der EU oder des EWIR (Europäischer Wirtschaftsraum) sind laut § 15 SigG97 den inländischen Zertifikaten gleichgestellt, soweit sie eine gleichwertige Sicherheit aufweisen. Durch die Anerkennung sollte eine weltweite Verbreitung der digitalen Signatur gefördert werden. In der Anlage II des Maßnahmenkataloges für technische Komponenten wird die Evaluierungsstufe E4 für die Erzeugung von Signaturschlüsseln, der Speicherung und Anwendung des privaten Signaturschlüssels vorgesehen. Dieser hohe Maßstab⁴⁰ für die Signatur in Deutschland stellt die Gleichstellung ausländischer Zertifikate in Frage, da nicht jeder Staat diese Anforderungen an digitale Signaturen setzt.

2.4.2 Das neue Signaturgesetz

Die rechtlichen Ausführungen der EU-Richtlinie, sowie die Kritik am Signaturgesetz zeigen deutlich, dass ein Anpassungsbedarf des nationalen Rechtsrahmens bestand. Um den Erfahrungsvorsprung und die Vorreiterrolle der Bundesrepublik in Europa auszubauen und bereits vor Ablauf der geforderten Umsetzungsfrist⁴¹ vom 19. Juli 2001 verbesserte Bedingungen im elektronischen Geschäftsverkehr zu schaffen, musste der deutsche Gesetzgeber handeln. Am 16. Mai 2001 wurde das „**Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften**“ (SigG01)⁴² vom deutschen Bundestag verabschiedet und trat am 1. Juni als Substitut des Signaturgesetzes von 1997 in Kraft.

Zweck des Gesetzes ist es nach § 1

„Rahmenbedingungen für elektronische Signaturen zu schaffen“ und „ihre Verwendung freizustellen“.

⁴⁰ Zur Einordnung: Die Sicherheitsstufe E5 wird in den USA für die Kontrolle von Nuklearwaffen vorgeschrieben.

⁴¹ Vgl. § 13 EGSRL (1999)

⁴² Vgl. BGBl (2001)

Der Regelungsbereich wurde, wie es die Zweckbestimmung verdeutlicht, von den digitalen auf die elektronischen Signaturen ausgeweitet. Um einen einheitlichen europäischen Standard zu etablieren, wurden die Begriffsbestimmungen sowie die Regelung für ausländische elektronische Signaturen und Produkte unmittelbar oder sinngemäß der EU-Richtlinie übernommen.

Zertifizierungsdiensteanbieter sind nach § 2 SigG01 natürliche oder juristische Personen, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen. Der Zeitstempeldienst wird von einer Pflichtdienstleistung zu einer Wahldienstleistung herabgestuft. Dies ermöglicht den Anbietern den Zeitstempeldienst auszulagern und fördert Unternehmen, die ausschließlich eine isolierte Zeitstempelung anbieten. Der Betrieb eines Zertifizierungsdiensteanbieters wird von einem Genehmigungsverfahren befreit⁴³ und durch die Aufnahme von Bußgeldvorschriften⁴⁴ und Aufsichtsregelungen unter Überwachung gestellt.

Ein **qualifiziertes Zertifikat** muss gemäß § 7 folgende Angaben enthalten und eine qualifizierte elektronische Signatur tragen:

1. Den Namen des Signaturschlüssel-Inhabers gegebenenfalls mit einem Namenszusatz oder einem Pseudonym.
2. Den zugeordneten Signaturprüf Schlüssel.
3. Die Bezeichnung der Algorithmen, mit denen der Signaturprüf Schlüssel des Zertifizierungsdiensteanbieters benutzt werden kann.
4. Die laufende Nummer des Zertifikates.
5. Beginn und Ende der Gültigkeit des Zertifikates.
6. Den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist.
7. Angaben darüber, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist.
8. Angaben, dass es sich um ein qualifiziertes Zertifikat handelt.

Signaturschlüssel im Sinne des Gesetzes sind einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden.

Signaturprüf Schlüssel sind elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden.

⁴³ Vgl. § 4 SigG01

⁴⁴ Vgl. § 21 SigG01

In § 11 und § 12 werden umfassende Haftungsregelungen aufgenommen, welche die geforderte Mindesthaftung der Richtlinie übertreffen. So haftet ein Zertifizierungsdiensteanbieter nicht nur für seine Zertifikate, sondern auch für die technischen Sicherheitseinrichtungen. Um den gesetzlichen Schadensersatzpflichten nachkommen zu können, ist der Zertifizierungsdiensteanbieter verpflichtet eine Mindestdeckungssumme⁴⁵ von 250.000 € nachzuweisen.

Der Gesetzgeber nutzt die Möglichkeit durch die Schaffung eines freiwilligen Akkreditierungssystems⁴⁶ der Zertifizierungsdiensteanbieter die Sicherheit und das Vertrauen der Signaturen zu steigern. Um einen Zertifizierungsdienst anbieten zu können, muss

- die erforderliche Zuverlässigkeit durch die Einhaltung der Rechtsvorschriften nachgewiesen werden.
- das Personal über die erforderlichen Kenntnisse, Erfahrungen und Fertigkeiten⁴⁷ verfügen.
- eine Deckungsvorsorge nachgewiesen werden.

Die Regulierungsbehörde ist weiterhin die zuständige Behörde zur Überwachung und Akkreditierung der Zertifizierungsdiensteanbieter. Sie bildet die Wurzelinstanz der qualifizierten Zertifikate mit Anbieterakkreditierung und bestimmt die Prüfstellen für Hard- und Software.

Die Novellierung des Signaturgesetzes führt zu einer Vierteilung der elektronischen Signaturen, die hierarchisch von der elektronischen, über die fortgeschrittene elektronische und qualifizierte elektronische zur qualifizierten elektronischen Signatur mit Anbieterakkreditierung⁴⁸ führt, welche die höchste Sicherheitsstufe darstellt.

2.4.2.1 Elektronische Signaturen

Eine elektronische Signatur gemäß § 2 SigG01 sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen. Beispielsweise ist eine handschriftliche Unterschrift, welche mit Hilfe eines Scanners digitalisiert und in ein elektronisches Dokument eingefügt wird, bereits eine elektronische Signatur. Mit dieser Form ist kein Sicherheitswert verbunden, da sie mit geringem Aufwand vervielfältigt und in weitere Dokumente eingebunden werden kann.

⁴⁵ Vgl. § 12 SigG01

⁴⁶ Vgl. § 15 SigG01

⁴⁷ Vgl. Anhang II (e) EGSRL (1999)

⁴⁸ Vgl. § 2 SigG01

2.4.2.2 Fortgeschrittene elektronische Signaturen

Fortgeschrittene elektronische Signaturen sind elektronische Signaturen, die

- ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
- die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
- mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann,
- mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Diese Voraussetzungen ermöglichen einem Anwender die Erstellung eines Schlüssel-paares (privater und öffentlicher Schlüssel) z.B. mit einem Softwareprogramm wie PGP⁴⁹. Der Anwender signiert die Daten mit dem privaten Schlüssel und stellt den öffentlichen Schlüssel in einem öffentlichen Verzeichnis bereit. Ein Empfänger ist somit in der Lage die Authentizität und Integrität eines signierten Dokumentes zu überprüfen. Fortgeschrittene elektronische Signaturen sind in Deutschland nicht als Substitut zur handschriftlichen Unterschrift einsetzbar und unterliegen lediglich der freien Beweiswürdigung⁵⁰.

2.4.2.3 Qualifizierte elektronische Signaturen

Eine qualifizierte elektronische Signatur erfüllt die Voraussetzungen einer fortgeschrittenen elektronischen Signatur und

- beruht zum Zeitpunkt ihrer Erzeugung auf einem gültigen qualifizierten Zertifikat.
- muss mit einer sicheren Signaturerstellungseinheit erzeugt werden.

Qualifizierte elektronische Signaturen sind gemäß Artikel 5 EGSRL der handschriftlichen Unterschrift gleichgestellt. Die rechtlich anerkannte äquivalente Anwendung qualifizierter elektronischer Signaturen und handschriftlicher Unterschrift ist jedoch nicht Bestandteil des Signaturgesetzes.

2.4.2.4 Qualifizierte elektronische Signaturen mit Anbieterakkreditierung

Qualifizierte elektronische Signaturen mit Anbieterakkreditierung sind qualifizierte elektronische Signaturen, welche auf einem qualifizierten Zertifikat eines akkreditierten

⁴⁹ Vgl. Kapitel 5.2 „Anbieter fortgeschrittener elektronischer Signaturen“

⁵⁰ Vgl. Kapitel 2.5.2 „Beweiswert elektronischer Signaturen“

Zertifizierungsdiensteanbieters beruhen. Diese Form der Signatur entspricht den digitalen Signaturen des Signaturgesetzes von 1997. Sie unterliegen gemäß § 15 SigG01 einer Sicherheitsvermutung und es ist zu erwarten⁵¹, dass ihnen ein hoher Beweiswert vor Gericht zukommt.

2.4.3 Die neue Signaturverordnung

Um den veränderten Ansprüchen gerecht zu werden, wurde die Signaturverordnung (SigV01)⁵² ebenfalls novelliert und trat am 16. November 2001 in Kraft. Diese erlässt gemäß § 24 SigG01 die erforderlichen Rechtsvorschriften zur elektronischen Signatur.

Die Anzeige eines Zertifizierungsdiensteanbieters muss nach § 1 neben Namensangabe, gesetzlichen Vertretern, aktuelle Führungszeugnisse und einer Deckungsvorsorge nach § 12 SigG01, eine genaue Darlegung des Sicherheitskonzeptes einschließen. Dieses beinhaltet unter anderem technische, bauliche und organisatorische Sicherheitsmaßnahmen, sowie eine Übersicht der eingesetzten Produkte.

Ein Antragsteller wird mittels Personalausweises oder Reisepass identifiziert⁵³. Die Gültigkeitsdauer eines qualifizierten Zertifikates darf höchstens fünf Jahre betragen und den Zeitraum der Eignung der eingesetzten und zugehörigen Parameter nicht überschreiten.

Das Verfahren zur langfristigen Datensicherung wird gemäß § 17 SigV01 wie folgt geregelt:

Daten mit einer qualifizierten elektronischen Signatur sind neu zu signieren, falls diese für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. Diese erneute Signatur muss frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.

Des Weiteren regelt die Verordnung neben der Führung eines Zertifikatsverzeichnisses und der Sperrung von qualifizierten Zertifikaten, die Deckungsvorsorge, Einstellung der Zertifizierungstätigkeit, die freiwillige Akkreditierung, sowie Kosten für Amtshandlungen, die in Anlage II detailliert aufgelistet⁵⁴ sind.

⁵¹ Vgl. HOCHMANN, S. (2001), S. 94

⁵² Vgl. BGBl (2001)

⁵³ Vgl. § 3 SigV01

⁵⁴ Vgl. Anhang II SigV01

2.5 Weitere gesetzliche Regelungen zur elektronischen Signatur

2.5.1 Die elektronische Signatur im Bürgerlichen Gesetzbuch

Das Signaturgesetz spart die Gleichstellung von handschriftlicher und elektronischer Unterschrift aus. Dieser zentralen Forderung der EU-Richtlinie kommt der deutsche Gesetzgeber durch das „**Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr**“⁵⁵ nach, welches am 13. Juli 2001 vom Bundestag beschlossen wurde und am 1. August in Kraft trat.

Artikel 1 beschäftigt sich mit der Änderung des Bürgerlichen Gesetzbuchs⁵⁶ (BGB). Das BGB geht vom Grundsatz der Vertrags- und Formfreiheit aus. Dies bedeutet, dass dem Einzelnen freisteht, mit wem ein Vertrag geschlossen wird und welchen Inhalt dieser besitzt. Die Formfreiheit überlässt dem Einzelnen die Wahl der Art und Weise, wie jemand den Geschäftswillen äußert. Für eine Reihe von Fällen schreibt der Gesetzgeber jedoch eine bestimmte Form vor. Dabei werden die Folgenden unterschieden:

1. Die **Schriftform** verlangt eine schriftliche Verkörperung mit eigenhändiger Namensunterschrift des Ausstellers.⁵⁷
2. Die **elektronische Form** besteht aus einem elektronischen Dokument, welches den Namen des Ausstellers beinhaltet und mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist.

Die Änderungen des BGB im Zuge des Formanpassungsgesetzes sehen die Einfügung des § 126 Absatz 3 vor, der wie folgt lautet:

„Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt“

Des Weiteren wird § 126a eingefügt.

- § 126a (1) Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.
- (2) Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren.

⁵⁵ BGBl (2001)

⁵⁶ BECK (2001)

⁵⁷ Vgl. § 126 BGB (2003)

Der Gesetzgeber hat die elektronische Form nur unter Ausnahmeregelungen der Schriftform gleichgestellt. So ist sie unter anderem ausgeschlossen⁵⁸ bei

1. der Auflösung, Kündigung und Befristung von Arbeitsverträgen.
2. der Erteilung des Zeugnisses.
3. der Erteilung des Leibrentenversprechens.
4. der Erteilung der Bürgschaftserklärung.
5. der Erteilung des Versprechens.
6. der Erteilung der Anerkennungserklärung.

Diese Ausnahmen werden wegfallen, wenn die elektronische Form einen vergleichbaren Grad der Verankerung in der Bevölkerung erreicht wie die schriftliche Form, die nach Meinung der Gesetzgebung vor übereilter Bindung besser schützt⁵⁹.

2.5.2 Beweiswert elektronischer Signaturen

Die in der EU-Richtlinie geforderte Zulassung elektronischer Signaturen als Beweismittel vor Gericht wird im Signaturgesetz nicht explizit vorgeschrieben. Die grundsätzliche Zulassung elektronisch signierter Dokumente ist nicht strittig, fraglich ist jedoch welcher Beweiswert diesen zukommt.

Die Zivilprozessordnung (ZPO)⁶⁰ soll diese Fragen klären. Die ZPO unterscheidet grundsätzlich die folgenden Beweismittel:

- Augenscheinbeweis⁶¹,
- Zeugenbeweis,
- Beweis durch Sachverständige,
- Urkundenbeweis⁶²,
- Parteivernehmung.

Zunächst kommt für elektronische Dokumente der Urkunden- und Augenscheinbeweis in Betracht. Gemäß der ZPO ergibt sich für eine Urkunde folgende Definition:

Eine **Urkunde** ist eine in der Schrift verkörperte Erklärung, die allgemein oder für Eingeweihte verständlich ist, die Aussteller erkennen lässt und die zum Beweis einer rechtlich erheblichen Tatsache bestimmt ist.

⁵⁸ Vgl. Artikel 1 Formanpassungsgesetz (2001)

⁵⁹ Vgl. LUTZENBERGER, S. (2001), S. 46

⁶⁰ Vgl. BECK (2001)

⁶¹ Vgl. §§ 371, 372 ZPO (2002)

⁶² Vgl. §§ 415-444 ZPO (2002)

Durch die fehlende Verkörperung kann ein elektronisches Dokument keinen Urkundenbeweis, sondern lediglich den Augenscheinbeweis durch Vorlegung oder Übermittlung der Datei antreten⁶³. Sie gelten somit als Objekte, die der freien richterlichen Beweismwürdigung unterliegen. Dateien mit einer einfachen oder fortgeschrittenen elektronischen Signatur fallen als elektronische Dokumente ebenfalls unter den Augenscheinbeweis. Der Gesetzgeber steigert jedoch laut ZPO § 292a die Beweiskraft der qualifizierten elektronischen Signaturen:

„Der Anschein der Echtheit einer qualifizierten elektronischen Signatur, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstlich Zweifel daran begründen, dass die Erklärung mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist.“⁶⁴

Durch diese Vermutungsregel⁶⁵ kann der Gegenbeweis vom Zertifikatinhaber nur angetreten werden, wenn er durch Tatsachen beweist, dass ein abweichender Geschehensablauf möglich ist. Dieser Schutz des Empfängers eines digital signierten Dokumentes geht über die rechtliche Bedeutung der Schriftform hinaus, da für diese keine Beweiserleichterung existiert.

2.5.3 **Verwaltungsverfahrensgesetz**

Am 21. August 2002 trat das Dritte Gesetz zur Änderung verwaltungsverfahrenrechtlicher Vorschriften⁶⁶ in Kraft. Im Verwaltungsverfahrensgesetz wird nach § 3 folgender eingefügt:

§ 3a „Elektronische Kommunikation“

1. Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.
2. Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronische Signatur nach dem Signaturgesetz zu versehen. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüssel-Inhabers nicht ermöglicht, ist nicht zulässig.

⁶³ Vgl. § 371 ZPO (2002)

⁶⁴ Vgl. § 292a ZPO (2002)

⁶⁵ Vgl. LUTZENBERGER, S. (2001), S. 58

⁶⁶ BGBl (2002)

3. Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, hat sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück zu übermitteln.

Mit dieser Gesetzesänderung wurde eine weitere rechtliche Hürde für den Einsatz elektronischer Signaturen beseitigt. Für Bürgerinnen und Bürger macht es im Verhältnis zu staatlichen Stellen keinen rechtlichen Unterschied mehr, ob sie behördliche Schreiben handschriftlich oder elektronisch unterzeichnen.

2.5.4 Umsatzsteuergesetz

2.5.4.1 Das ursprüngliche⁶⁷ Umsatzsteuergesetz

Die **Umsatzsteuer** ist eine Verbrauchersteuer und wird innerhalb einer Handelskette auf jeder Stufe an den Staat abgeführt und als Kosten auf den Warenwert⁶⁸ aufgeschlagen. So fordert der Produzent einer Ware beim Verkauf an den Großhändler Umsatzsteuer. Ebenso berechnet der Großhändler dem Einzelhändler und der Einzelhändler dem Endverbraucher Umsatzsteuer auf den Weiterveräußerungspreis. Im Gegensatz zum Endverbraucher können Unternehmen gemäß § 2 Umsatzsteuergesetz (UStG), die von ihnen gezahlte Umsatzsteuer auch als **Vorsteuer** bezeichnet mit ihrer Umsatzsteuerschuld verrechnen. Auf diese Weise wird lediglich die Umsatzsteuer auf den Mehrwert einer Ware an das Finanzamt abgeführt. Der Vorsteuerabzug ist jedoch an drei Bedingungen geknüpft:

1. Der Leistende muss ein Unternehmer sein und eine Leistung für das Unternehmen des Empfängers erbracht haben.
2. Der Empfänger muss die Leistung durch eine Rechnung gemäß § 14 UStG belegen, auf welcher die Umsatzsteuer ausgewiesen ist.
3. Der Vorsteuerabzug darf erst vollzogen werden, wenn der leistende Unternehmer die vereinbarte Leistung empfangen hat.

⁶⁷ In seiner Fassung bis 31. Dezember 2001

⁶⁸ Vgl. HOERETH, ROISCH, SCHIEGL (2001), S. 2

Damit eine Rechnung als solche im Sinne des UStG anerkannt wird, müssen folgende Angaben⁶⁹ enthalten sein:

- der Name und die Anschrift des leistenden Unternehmers,
- der Name und die Anschrift des Leistungsempfängers,
- die Menge und die handelsübliche Bezeichnung des Gegenstandes der Lieferung oder die Art und der Umfang der sonstigen Leistung,
- der Zeitpunkt der Lieferung oder der sonstigen Leistung,
- das Entgelt für die Lieferung oder sonstige Leistung und den auf das Entgelt entfallenden Steuerbetrag.

Eine Rechnung muss gemäß § 14 UStG eine Urkunde sein, also eine körperliche Form erfüllen. Wird eine Rechnung als Schriftstück versendet oder per Telefax übermittelt, ist diese Formerfordernis erfüllt. Eine elektronische Übermittlung der Rechnungsdaten per E-Mail oder Datenträgeraustausch wird aufgrund der fehlenden körperlichen Form nicht anerkannt, auch ein nachträgliches Ausdrucken der elektronischen Daten berechtigt nicht zum Vorsteuerabzug.

2.5.4.2 Das neue Umsatzsteuergesetz

Im Rahmen des Steueränderungsgesetz 2001 (StÄndG 2001) vom 20. Dezember 2001 wird auch das Umsatzsteuergesetz novelliert. Laut § 14 UStG gilt seit dem 1. Januar 2002 als Rechnung auch eine mit einer qualifizierten elektronischen Signatur mit Anbieterakkreditierung versehene elektronische Abrechnung. Die elektronische Rechnung ist somit eine Rechnung mit dem oben geforderten Inhalt, die anstatt in Papierform als Datei erstellt und digital signiert wird. Die Signatur dient in diesem Falle als Herkunftsbeleg und garantiert die Unverfälschtheit der Rechnungsdaten. Die Möglichkeit der Erstellung und Versendung elektronischer Rechnungen dient als Ergänzung zum Papierverkehr. Es ist den Unternehmen somit freigestellt ihre Rechnungen auf elektronischen oder auf dem herkömmlichen papiergebundenem Wege zu versenden.

In diesem Zusammenhang ist abschließend die europäische Richtlinie zur Vereinfachung, Modernisierung und Harmonisierung der mehrwertsteuerlichen Anforderungen an die Rechnungsstellung⁷⁰ zu erwähnen.

⁶⁹ Vgl. § 14 UstG (2002)

⁷⁰ Vgl. AMTSBLATT DER EUROPÄISCHEN GEMEINSCHAFT (2002)

Diese wurde am 20. Dezember 2001 beschlossen und ist von den Mitgliedsstaaten bis zum 1. Januar 2004 umzusetzen. Artikel 2 der Richtlinie fordert, dass elektronisch übermittelte Rechnungen von den Mitgliedsstaaten akzeptiert werden, falls die Echtheit der Herkunft und die Unversehrtheit des Inhalts gewährleistet werden kann. Dies ist durch den Einsatz einer fortgeschrittenen elektronischen Signatur zu garantieren. Die Mitgliedsstaaten können allerdings verlangen, dass qualifizierte elektronische Signaturen eingesetzt werden müssen.

Eine Stellungnahme der Bundesregierung zu dieser Richtlinie liegt zum jetzigen Zeitpunkt nicht vor. Es ist jedoch zu erwarten, dass an einem Einsatz qualifizierter elektronischer Signaturen im UStG festgehalten wird.

2.6 Fazit

Die Novellierung des Signaturgesetzes und der Verordnung erfüllt die erforderlichen Anpassung an die EU-Richtlinie. Durch die Einführung von Haftungsbestimmungen, der Gleichstellung ausländischer Zertifikate und die Aufhebung der Genehmigungspflicht von Zertifizierungsdiensteanbieter werden die wichtigsten Kritikpunkte des alten Signaturgesetzes beseitigt. Die Gleichstellung qualifizierter elektronischer Signaturen mit der handschriftlichen Unterschrift ist ebenso positiv zu sehen, wie die Zulassung und Beweismittelregelungen vor Gericht. Durch den deutschen Gesetzgeber werden die Rahmenbedingungen für elektronische Signaturen geschaffen. Die legislative Vereinheitlichung ebnet den Weg für eine interoperable Verbreitung innerhalb der EU und ist ein Vorbild für eine weltweite Anwendung.

Trotz dieser positiven Aspekte existieren weiterhin rechtliche Kritikpunkte. So geht das Signaturgesetz nicht auf einen exakten Sperrzeitpunkt eines Zertifikates ein. Gemäß § 7 SigG01 wird eine rückwirkende Sperrung zwar ausgeschlossen, eine Konkretisierung des Begriffs „Sperrzeitpunkt“ wird jedoch nicht getroffen. Dies ist wünschenswert, da ein Zertifizierungsdiensteanbieter ordnungswidrig⁷¹ handelt, wenn er vorsätzlich oder fahrlässig nicht dafür sorgt, dass ein qualifiziertes Zertifikat nicht oder nicht rechtzeitig gesperrt wird. Als möglicher Sperrzeitpunkt kann verstanden werden:

1. Zeitpunkt der Beantragung einer Sperrung durch den Antragsteller.
2. Zeitpunkt der Erstellung des Spereintrages beim Zertifizierungsdiensteanbieter.
3. Zeitpunkt der Veröffentlichung des Sperrvermerkes im Sperrverzeichnis.

⁷¹ Diese Ordnungswidrigkeit wird mit einer Geldbuße von bis zu 10.000 Euro geahndet.

Das BSI favorisiert in den Angaben zum Maßnahmenkatalog den Zeitpunkt der Erstellung, gesteht jedoch eine Bearbeitungszeit von ca. 10 Minuten ein.

Kritisch an der aktuellen Gesetzgebung ist ebenso die Tatsache zu sehen, dass Zertifikate nur an natürliche und nicht an juristische Personen vergeben werden können. Ein Arbeitgeber kann demnach lediglich durch seine Mitarbeiter handeln. Bei Ausscheiden oder Arbeitsplatzwechsel ist ein neues Zertifikat erforderlich. Dieses Problem besteht in gleichem Maße für Zertifizierungsstellen und bedeutet für Unternehmen einen finanziellen Mehraufwand. Eine Begründung dieser Vorgehensweise ist in der papiergebundenen Art des Unterschreibens verankert. Handschriftliche Unterschriften werden von dafür ermächtigten **natürlichen** Personen abgegeben.⁷²

⁷² Vgl. Webseite der Regulierungsbehörde. Online im Internet: [http:// www.regtp.de](http://www.regtp.de) FAQ (Stand 25.02.03)

3 Mathematische Grundlagen

3.1 Kryptologie

Die Grundlage der fortgeschrittenen elektronischen Signatur bilden kryptographische Verfahren. Die **Kryptologie** ist laut Definition die Lehre der Entwicklung, Anwendung und Analyse von Verschlüsselungsverfahren. Sie besteht aus den zwei Teilgebieten **Kryptographie** und **Kryptanalyse**. Diese Begriffe stammen aus dem Griechischen und setzen sich aus den Worten kryptos (verstecken) und logos (das Wort, der Sinn), bzw. graphein (schreiben) und analysein (auflösen, entziffern) zusammen. Während die Kryptographie die Entwicklung von Algorithmen zur Geheimhaltung von Nachrichten zum Ziel hat, ist die Kryptanalyse die komplementäre Wissenschaft. Diese beschäftigt sich mit den Methoden der Rücktransformation verschlüsselter Daten und den Angriffen auf die Verschlüsselungsverfahren zum Zweck der Bewertung kryptographischer Stärken bzw. Schwächen.⁷³

3.1.1 Die geschichtliche Entwicklung der Kryptologie

Seit es Menschen gibt existieren Geheimnisse, die an sicheren Orten verborgen wurden. Bestand die Notwendigkeit geheime Botschaften über unsicheres Gebiet zu transportieren, so wurden schon im Altertum kryptographische Verfahren eingesetzt. Bedeutende Persönlichkeiten der Geschichte sind mit ihr verknüpft, wie Cäsar, Karl der Große, Casanova und Maria Stuart.

3.1.1.1 Skytale von Sparta

Das älteste⁷⁴ bekannte Beispiel für eine Verschlüsselung ist die **Skytale von Sparta**⁷⁵. Sie wurde von der spartanischen Regierung genutzt, um geheime Nachrichten an ihre Generäle zu übermitteln. Bei der Skytale handelt es sich um einen Stab aus Holz, um den ein schmales Band aus Pergament spiralförmig gewickelt wurde.

⁷³ Vgl. BEUTELSPACHER, A. (1991), S. 10

⁷⁴ Erste Erwähnung durch den griechischen Historiker Plutarch ungefähr 500 vor Christus.

⁷⁵ Vgl. BEUTELSPACHER, A. (1991), S. 11

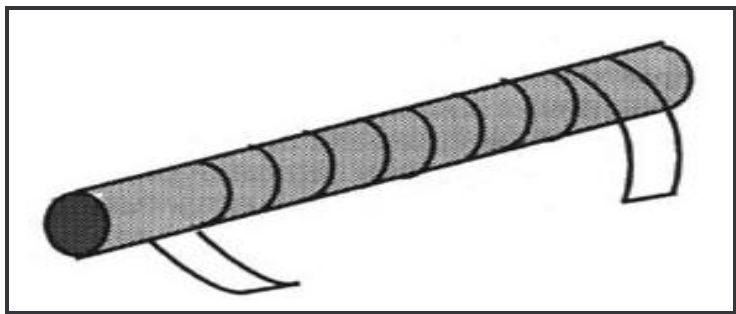


Abbildung 3: Die Skytale von Sparta

Die Botschaft wurde der Stablänge nach auf das Band geschrieben. War das Pergament abgewickelt, so konnte es nur von einer Person gelesen werden, die einen Stab genau desselben Umfangs besaß.

Beispielsweise wird eine verschlüsselte Nachricht mit der folgenden Buchstabenfolge

DFAIREAIMARUBMUAFEOENAGRNGMIGRYNEIKNNFLTG

von einer Skytale mit einem Durchmesser von fünf Buchstaben zu

Der Angriff auf Amyklai⁷⁶ beginnt im Morgengrauen.

entschlüsselt.

3.1.1.2 Cäsarchiffre

Eine einfache und daher sehr bekannte Verschlüsselungsmethode nutzte schon Gaius Julius Cäsar (101 - 44 v. Chr.), um geheime Nachrichten vor Feinden zu schützen. Bei dieser so genannten Cäsarchiffre⁷⁷ wird jeder Buchstabe der Nachricht um 3 Stellen im Alphabet verschoben.

a	b	c	d	e	f	g	h	i	j	k	l	m
D	E	F	G	H	I	J	K	L	M	N	O	P
n	o	p	q	r	s	t	u	v	w	x	y	z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C
Die Nachricht				„Alea jacta est.“ ⁷⁸								
wird so zum Geheimtext				DOHD MDFWD HVW								

Tabelle 1: Verschlüsselung mit der Cäsarchiffre⁷⁹

⁷⁶ Amyklai ist der Name eines Dorf, welches nahe Sparta gelegen war und von den Spartaner 700 v. Chr. erobert wurde.

⁷⁷ Vgl. NEUMANN, H. (2000), S. 12

⁷⁸ Lateinisch für „Der Würfel ist gefallen!“. Ein Ausspruch von Julius Cäsar als er am 10. Januar 49 v. Chr. den Rubikon überschritt, der Oberitalien von Italien trennte.

⁷⁹ Vgl. NEUMANN, H. (2000), S. 12

3.1.1.3 Die Chiffriermaschine Enigma

Die wohl bekannteste Anwendung einer Verschlüsselungstechnik ist die von der deut-



schon Wehrmacht im zweiten Weltkrieg eingesetzte **Enigma**⁸⁰. Diese elektronische Maschine, die vom Aussehen und der Bedienung einer Schreibmaschine ähnelt, wurde von Arthur Scherbius⁸¹ 1923 ursprünglich für den zivilen Einsatz entwickelt. Bis zum Ende des zweiten Weltkrieges wurde die Enigma mehrfach weiterentwickelt und mehr als 100.000fach hergestellt. Die Engländer versuchten in Bletchley Park von 1939 bis 1945 mit zeitweise bis zu 10.000 Mathematikern, Ingenieuren und Hilfskräften die Enigma zu entschlüsseln. Der prominenteste Mitarbeiter war Alan Turing, einer der

großen Informatikpioniere. Um die großen Datenmenge zu bewältigen, wurden die ersten Computer entwickelt. Bei diesen Entschlüsselungsversuchen, die mehrfach erfolgreich waren, kam auch Colossus, der erste programmierbare britische Computer zum Einsatz. Das Beispiel der Enigma verdeutlicht, wie die moderne Kryptographie die Entwicklung der Informatik und der Computer vorantrieb.

3.1.1.4 Die moderne Kryptologie

Seit Mitte der siebziger Jahre ist die Kryptologie mehr in das öffentliche Interesse der Forschung getreten. Von großer Bedeutung war die Entwicklung des **Data Encryption Standard DES**⁸² im Jahre 1977 und die Erfindung der **Public Key Kryptographie**⁸³ durch Diffie und Hellman im Jahre 1976⁸⁴, welche die Grundlage der fortgeschrittenen elektronischen Signatur bildet. Auf diese Meilensteine der modernen Kryptologie wird im Kapitel 3.2 „Verschlüsselungsverfahren“ detailliert eingegangen.

⁸⁰ Griechisch für Geheimnis

⁸¹ Vgl. ERTEL, W. (2001), S. 42

⁸² Siehe auch Kapitel 3.2.1 „Symmetrische Verschlüsselung“

⁸³ Siehe auch Kapitel 3.2.2 „Asymmetrische Verschlüsselung“

⁸⁴ Vgl. BEUTELSPACHER, A. (2001), Vorwort

3.1.2 Ziele der Kryptographie

Die Ziele moderner kryptographischer Verfahren werden im Wesentlichen in die Bereiche Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit unterteilt⁸⁵. Diese müssen nicht bei jeder Anwendung gleichzeitig erfüllt werden.

1. Vertraulichkeit und Geheimhaltung

Die Vertraulichkeit ist die Verschlüsselung von Daten zum Schutz vor Unbefugten. Kryptographisch wird die Geheimhaltung einer Nachricht erreicht, indem der Sender den Inhalt derart verändert, dass dieser für unbefugte Personen unlesbar ist. Der Empfänger kann jedoch durch eine geheime Zusatzinformation die ursprüngliche Nachricht zurückgewinnen. Die Geheimhaltung ist wohl der älteste Zweig der Kryptographie und findet besonders im militärischen Bereich häufig Anwendung. Aber auch im zivilen Bereich mehren sich die Einsatzmöglichkeiten kryptographischer Verfahren. Im Zeitalter der Globalisierung und des E-Business werden Rechnungen, Verträge und andere vertrauliche Daten auf Rechnern gespeichert und über das Internet ausgetauscht. Aufgrund der dezentralen Struktur des Internets werden Datenpakete von Router⁸⁶ zu Router bis zum eigentlichen Ziel weitergeleitet.⁸⁷ Auf diesem Weg können böswillige Angreifer an einem Router durchgereichten Datenpakete lesen und brisante Informationen fälschen.

2. Integrität

Die Integrität ist der Nachweis der Unversehrtheit einer empfangenen Nachricht. Während die Geheimhaltung versucht, die Nachricht vor unbefugtem Lesen zu bewahren, ist das Ziel der Integrität die Daten vor unberechtigter Änderung zu schützen. Die Integrität einer Nachricht ist also gewahrt, wenn sie nicht unmerklich verändert werden kann. Die Vertraulichkeit stellt einen Schutz vor passiven Mitlesern dar, die Integrität hingegen verlangt, dass der Empfänger erkennen kann, ob eine Nachricht durch einen aktiven Angreifer manipuliert wurde. Die Unversehrtheit von Botschaften hat in den letzten Jahren der reinen Geheimhaltung den Rang abgelaufen⁸⁸ und ist dafür verantwortlich, dass sich die Kryptographie nicht mehr auf den stark eingegrenzten Bereich der militärischen Anwendungen beschränkt, sondern auch in der freien Wirtschaft ihre Berechti-

⁸⁵ Vgl. NEUMANN, H. (2000), S. 4

⁸⁶ Ein Router ist ein Gerät, welches die Verbindung zwischen zwei oder mehr Netzwerken verwaltet.

⁸⁷ Vgl. LUITWIELER, J. (1998), Kapitel 3 „Kryptographie“

⁸⁸ Vgl. BEUTELSPACHER, A. (1991), S. 5

gung findet. Ein Beispiel für die Wichtigkeit der Datenintegrität ist im Bereich der elektronischen Überweisung zu finden. Könnte ein Unbefugter eine Überweisung einsehen, ist dies weniger schwer zu bewerten als die Manipulation der Daten eines Überweisungsträgers, wie Kontonummer oder Überweisungsbetrag.

3. **Authentizität**

Unter Authentizität wird zum einen die **Teilnehmerauthentizität** und zum anderen die **Nachrichtenaauthentizität** unterschieden. Die Teilnehmerauthentizität ist gegeben, wenn ein Teilnehmer seine Identität zweifelsfrei nachweisen kann. In der Praxis existieren viele Beispiele, bei denen dieser Nachweis eine Rolle spielt:

- Die meisten Computersysteme sind derart ausgelegt, dass prinzipiell viele Benutzer unabhängig voneinander mit einem Rechner arbeiten können. Diese Multiuser-Systeme müssen sich, meist durch Passwortverfahren, von der Identität der Benutzer überzeugen können.
- Ein weiteres typisches Beispiel ist die Eingabe einer Geheimzahl zur Benutzung eines Geldautomaten.
- Aber auch im Mobilfunk sind Authentifikationsverfahren wichtig. Ein Mobilfunknetzbetreiber muss die Identität eines Telefonierenden zweifelsfrei feststellen können, da dieser auch für die Gesprächskosten aufkommt.

Die Nachrichtenaauthentizität liegt vor, wenn sich der Empfänger einer Nachricht zweifelsfrei vom Ursprung dieser überzeugen kann. Diese Forderung richtet sich ebenfalls gegen aktive Angreifer und ist der Integrität sehr ähnlich. Der Unterschied zur Integrität ist die Frage, ob die Nachricht tatsächlich vom Sender stammt. Die Datenunversehrtheit ist auch dann gegeben, falls ein Angreifer eine Nachricht unter falschem Namen versendet. Der Empfänger muss also die Möglichkeit haben, die Herkunft einer Nachricht ermitteln zu können und somit ihre Authentizität zu prüfen. Im Bereich des Homebanking und Electronic cash ist die Nachrichtenaauthentizität von großer Bedeutung. Ein Angreifer hätte ansonsten die Möglichkeit durch Geldtransaktionen unter falschen Namen sein Konto stand aufzubessern.

4. Verbindlichkeit

Die Verbindlichkeit ist der zweifelsfreie Nachweis der Urheberschaft eines Dokumentes. Eine Person übermittelt einer zweiten Person eine Nachricht verbindlich, wenn der Empfänger anschließend Dritten gegenüber nachweisen kann, dass die Nachricht tatsächlich von dem Absender stammt. Dies ist mehr als nur die Nachrichtenauthentizität, da eine Nachricht auch dann authentisch wäre, wenn sich der Empfänger zwar überzeugen kann, dass sie vom Absender stammt, dies aber nicht selbst beweisen kann. Ein Sender hat bei einer verbindlichen Nachricht nicht die Möglichkeit eines Abstreitens der Übermittlung.

3.1.3 Grundlagen der Kryptologie

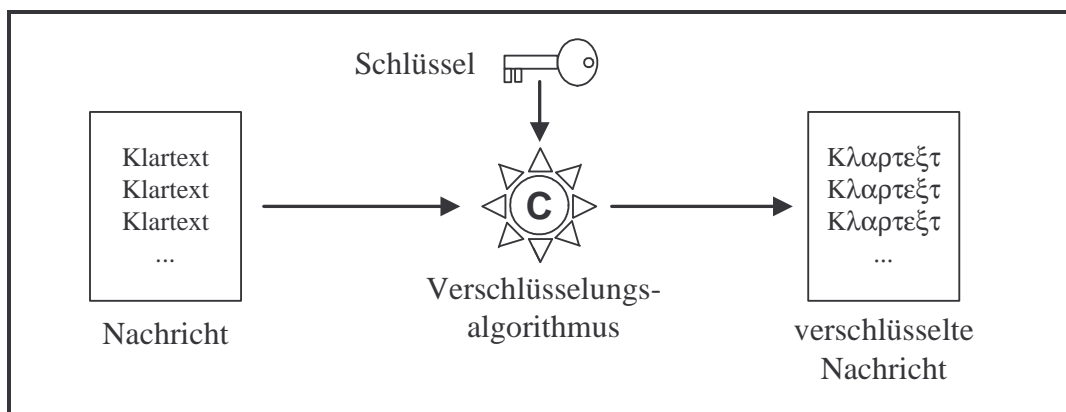
In diesem Abschnitt werden die grundlegenden Begriffe der Kryptographie und Kryptanalyse am Beispiel der Verschlüsselung erläutert. Obwohl die Geheimhaltung bei einer Signatur eine untergeordnete Rolle spielt, bilden die Verschlüsselungsverfahren die Grundbausteine für die Algorithmen der fortgeschrittenen elektronischen Signatur.

Das Ziel der Geheimhaltung ist es, eine vertrauliche Kommunikation zwischen zwei Personen zu sichern. Diese Personen werden in Sender und Empfänger eingeteilt. In der Literatur werden häufig die Synonyme Alice für den Sender und Bob stellvertretend für den Empfänger verwendet. Diese Bezeichnungen haben sich international durchgesetzt und werden im Folgenden ebenfalls zur Anwendung kommen.

Um eine Verschlüsselung tatsächlich anwenden zu können, müssen sich Alice und Bob auf ein bestimmtes Verfahren einigen, das sie verwenden wollen. Dieser **Verschlüsselungsalgorithmus** ist eine mathematische Transformation, welche die ursprüngliche Nachricht, den **Klartext** oder **Plaintext** in eine veränderte den **Chiffretext** oder **Geheimtext** umwandeln kann. Dieser Vorgang wird als **Verschlüsselung** (encryption) oder auch als **Chiffrierung** bezeichnet, während die Umkehrung **Entschlüsselung** (decryption) oder auch **Dechiffrierung** genannt wird.⁸⁹ Dem Verfahren wird des Weiteren ein variabler Parameter hinzugefügt, der so genannte **Schlüssel**. Auf diesen müssen sich die Beteiligten einigen, er bleibt jedoch ihr Geheimnis und ist innerhalb eines Algorithmus veränderlich. Die Vereinigung von Algorithmus, zugehörigen Schlüsseln und den verschlüsselten Nachrichten wird **Kryptosystem**⁹⁰ genannt.

⁸⁹ Vgl. LUTZENBERGER, T. (2002), S. 5

⁹⁰ Vgl. BEUTELSPACHER, A. (1991), S. 11

Abbildung 4 : Kryptosystem⁹¹

Ein Grundprinzip⁹² der modernen Kryptographie ist die Forderung, dass ein Angreifer stets die Ver- und Entschlüsselungsfunktion kennt und nur der Schlüssel geheim ist.

*Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus, sondern ausschließlich von der Geheimhaltung des Schlüssels abhängen.*⁹³

Dieses Prinzip wird in der Literatur als die Maxime von Kerckhoff⁹⁴ bezeichnet und ist dadurch begründet, dass bei jedem kommerziell eingesetzten Verschlüsselungsalgorithmus in der Entwicklung, Spezifizierung, Normung, Prüfung und Umsetzung derart viele Personen, wie z.B. Designer, Analytiker und Programmierer involviert sind, dass eine Geheimhaltung fast unmöglich ist. Ein weiterer Grund für diese Forderung ist die Tatsache, dass kryptographische Schlüssel verhältnismäßig kurze Zeichenketten sind, wohingegen die Beschreibung eines Algorithmus viele Seiten in Anspruch nehmen kann. Das Kerckhoffsche Prinzip formuliert auch die Tatsache, dass die Praxis der beste Test für einen Algorithmus ist. Die Veröffentlichung eines Verfahrens wird als die wichtigste Voraussetzung angesehen, um einen Algorithmus als sicher einschätzen zu können. Denn nur eine ausgiebige Kryptanalyse kann Schwächen eines Verfahrens zuverlässig aufdecken.

Die Sicherheit eines Verschlüsselungsalgorithmus lässt sich durch zwei charakteristische Merkmale beschreiben. Zum einen gegen welche Angriffe die Chiffre anfällig ist, und zum anderen wie viel Information ein Angreifer durch einen Angriff gewinnen kann.

⁹¹ Vgl. HOCHMANN, S. (2001), S. 11

⁹² Vgl. NEUMANN, H. (2000), S. 6

⁹³ Vgl. BEUTELSPACHER, A. (1991), S. 23

⁹⁴ A. Kerckhoff (1825-1903) war der erste Kryptologe der diese Forderung formulierte.

Folgende vier häufig verwendete Arten von Krypto-Angriffen⁹⁵ sind zu unterscheiden:

1. **Ciphertext-Only-Attack** oder Angriff mit bekanntem Geheimtext:
Der Angreifer verfügt lediglich über einen Chiffretext oder nur ein Teilstück desselben. In der Kryptographie gehört dies zu den grundsätzlichen Modellannahmen, dass es einem Angreifer möglich ist, den Geheimtext abzufangen.
2. **Known-Plaintext-Attack** oder Angriff mit bekanntem Klartext:
Der Angreifer kennt bei diesem Szenario neben dem Chiffretext auch den dazu gehörigen Klartext und versucht auf Basis dieses Wissens den Algorithmus zu entschlüsseln.
3. **Chosen-Plaintext-Attack** oder Angriff mit gewählttem Klartext:
Der Angreifer verfügt über den Zugriff auf die Verschlüsselung und ist somit in der Lage, gezielt Klartextblöcke seiner Wahl verschlüsseln zu lassen, um Rückschlüsse auf den Schlüssel oder den Algorithmus zu erhalten. Ziel dieses Angriffes ist es, durch speziell geformte Klartextnachrichten die Verschlüsselung zu dechiffrieren. Der Schlüssel ist jedoch nach wie vor geheim.
4. **Chosen-Ciphertext-Attack** oder Angriff mit gewählttem Geheimtext:
Der Angreifer hat nicht nur Zugriff auf die Verschlüsselung, sondern ist auch in der Lage einen Geheimtext seiner Wahl entschlüsseln zu lassen.

Die höchste Sicherheit gewährleistet ein Kryptosystem, welches bei einem beliebigen Angriff keinerlei Informationen preisgibt.

Eine einfache, aber meist sehr zeit- und rechenintensive Methode einen Geheimtext zu brechen, ist der so genannte **Brute-Force-Attack** oder Angriff mit Brachialgewalt. Ein Angreifer probiert systematisch alle möglichen Schlüssel aus, um einen sinnvollen Klartext zu ermitteln. Auf diese Weise lassen sich annähernd alle Kryptoalgorithmen überwinden. Um einen Brute-Force-Angriff auszuschließen, ist es notwendig einen ausreichend großen Schlüsselraum zu wählen.

Für die Beurteilung der benötigten Schlüsselraumgröße ist folgende Definition hilfreich.

Definition⁹⁶ : Ein Algorithmus gilt als **sicher**, wenn

- der zum Aufbrechen nötige Geldaufwand den Wert der verschlüsselten Daten übersteigt oder
- die zum Entschlüsseln erforderliche Zeit größer ist als die Zeit, welche die Daten geheim bleiben müssen oder

⁹⁵ Vgl. NEUMANN, H. (2000), S. 10

⁹⁶ Vgl. ERTEL, W. (2001), S. 24

- das mit einem bestimmten Schlüssel chiffrierte Datenvolumen kleiner ist als die zum Decodieren erforderliche Datenmenge.

3.2 Verschlüsselungsverfahren

3.2.1 Symmetrische Verschlüsselung

Im Allgemeinen werden in der Kryptographie zwei Arten von Verschlüsselungsalgorithmen unterschieden. Auf der einen Seite stehen die symmetrischen Verfahren zu denen beispielsweise die Cäsarchiffre und die Skytale von Sparta gehören. Auf der anderen Seite stehen die asymmetrischen oder auch modernen Verschlüsselungsverfahren. In den folgenden Abschnitten werden einige symmetrische und asymmetrische Algorithmen vorgestellt und auf die grundlegenden Unterschiede eingegangen.

Symmetrische Kryptographie ist gleichsam die Grundform der Verschlüsselung. Bei diesen Verfahren ist der Schlüssel für Chiffrieren und Dechiffrieren identisch. Aus diesem Grund muss dieser stets geheim bleiben und darf nur auf einem sicheren Kanal ausgetauscht werden.

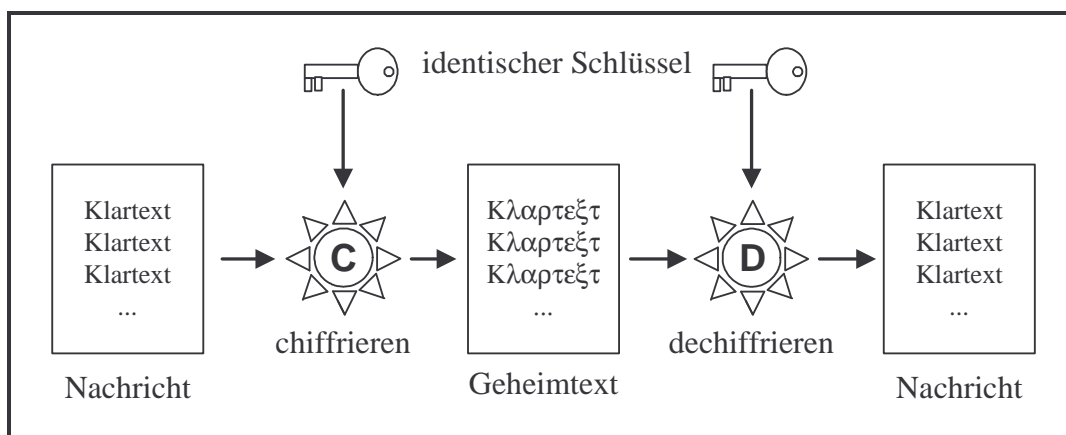


Abbildung 5 : Schema der symmetrischen Verschlüsselung⁹⁷

Formal besteht ein symmetrischer Algorithmus aus einer mathematischen Verschlüsselungsfunktion f mit zwei Eingabewerten, dem Schlüssel k und dem Klartext m , und einer Ausgabe, dem Geheimtext c , der sich aus k und m ergibt. Dies bedeutet, dass $c = f(m, k)$ gilt. Die Verschlüsselungsfunktion f muss eindeutig umkehrbar sein, damit später der berechtigte Empfänger aus dem Chiffretext und dem Schlüssel den Klartext bilden kann. Das bedeutet, es muss einen mathematischen Zusammenhang geben, der

⁹⁷ Vgl. HOCHMANN, S. (2001), S. 12

mit Hilfe der Umkehrfunktion f^* , dem Schlüssel k und Chiffretext c den Klartext m bildet. Dieser Zusammenhang wird durch die Formel $f^*(k, c) = m$ beschrieben.

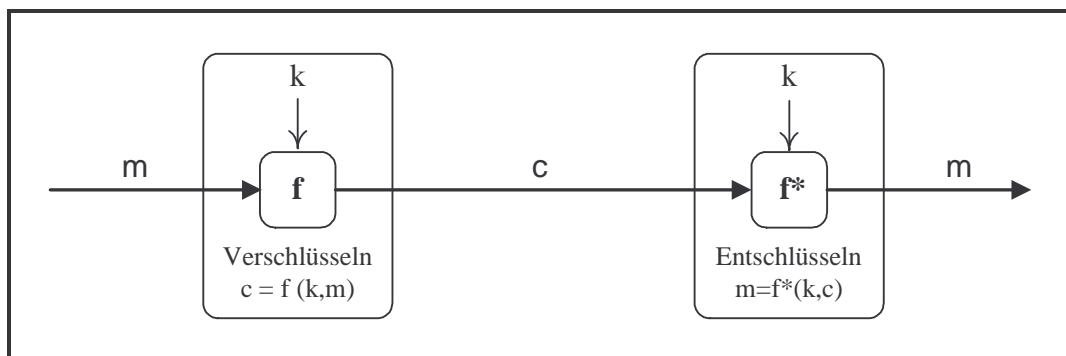


Abbildung 6 : Funktionsschema eines symmetrischen Verschlüsselungsalgorithmus⁹⁸

Es existieren verschiedene Verfahren, Klartexte symmetrisch zu verschlüsseln. Dabei werden so genannte **Transpositionschiffren** und **Substitutionschiffren** eingesetzt⁹⁹.

Definition: Ein Geheimtext, der durch Permutation¹⁰⁰ der Klartextzeichen erzeugt wird, wird als **Transpositionschiffre** oder **Permutationsschiffre** bezeichnet. Bei einer **Substitutionschiffre** wird jedes Zeichen des Klartextes durch ein anderes ersetzt, die Position bleibt jedoch gleich. Eine Substitutionsschiffre heißt **monoalphabetisch**, wenn jedes Klartextzeichen immer auf das gleiche Geheimtextzeichen abgebildet wird. Sie heißt **polyalphabetisch**, wenn sie nicht monoalphabetisch ist.

Die Skytale ist der Prototyp eines Transpositionsalgorithmus, während die Cäsarschiffre ein typisches Beispiel für einen monoalphabetischen Substitutionsalgorithmus ist.

Von der Art und Weise wie der Klartext abgearbeitet wird, werden **Stromchiffrier-** und **Blockchiffrierverfahren** unterschieden.

Definition: Ein Chiffrierverfahren heißt **Blockchiffrierverfahren**, falls der Klartext in Einheiten fester Länge aufgeteilt und jeder Block nach einem vorgegebenen Schema (z.B. Transposition) verarbeitet wird.

Ein Chiffrierverfahren heißt **Stromchiffrierverfahren**, falls die einzelnen Zeichen des Klartextes hintereinander mit einer in jedem Schritt variierenden Funktion verarbeitet werden.

⁹⁸ Vgl. BEUTELSPACHER, A. (2001), S. 7

⁹⁹ Vgl. BEUTELSPACHER, A. (1991), S. 12

¹⁰⁰ Eine Permutation ist eine bijektive Abbildung einer endlichen Menge in sich.

Exemplarisch sollen hier einige klassische Bausteine der symmetrischen Verschlüsselungsverfahren aufgezeigt werden. Diese Bausteine werden bei der fortgeschrittenen elektronischen Signatur in Kombination angewandt.

Ein klassischer Vertreter der polyalphabetischen Stromchiffre ist die **Vigenere Chiffre**¹⁰¹, die im 16. Jahrhundert von dem Franzosen Blaise de Vigenere erfunden wurde. Es handelt sich dabei um eine Verschiebechiffre ähnlich wie der von Julius Caesar. Der Unterschied zur Cäsarchiffre liegt in dem zusätzlichen **Schlüsselwort w**, welches zwischen Sender und Empfänger im Vorfeld vereinbart wird. Dieses Schlüsselwort wird wiederholt aneinander geschrieben, bis die Länge der Schlüsselworte die Länge des **Klartextes m** erreicht. Nun wird jedes Zeichen des Klartextes in Abhängigkeit vom Schlüsselwort verschlüsselt. Die Verschlüsselung wird mit Hilfe eines Vigenere Quadrates vorgenommen. Im folgenden Beispiel wird der Klartext „An Koenigin Maria Stuart“ mittels des nachfolgenden Vigenere Quadrates und dem Schlüsselwort KRYPTO verschlüsseln.

Schlüsselwort:	K	R	Y	P	T	O	K	R	Y	P	T	O	K	R	Y	P	T	O	K	R	Y
Klartext:	A	n	K	o	e	n	i	g	i	n	M	a	r	i	a	S	t	u	a	r	t
Chiffretext:	K	E	I	D	X	B	S	X	G	C	F	O	B	Z	Y	H	M	I	K	I	R

Tabelle 2 : Polyalphabetische Verschlüsselung

Während das Schlüsselwortzeichen die Zeile des Quadrates festlegt, gibt das Klartextzeichen die Spalte vor. Der Chiffrieralgorithmus ersetzt das erste Zeichen des Klartextes „A“ durch das Geheimtextzeichen „K“. Dies begründet sich in der Tatsache, dass in der a-ten Spalte in der Zeile, welche mit dem Schlüsselwortzeichen „K“ beginnt, das Geheimtextzeichen „K“ steht. Formal bedeutet dies, dass $f(K, A) = K$ gilt.

¹⁰¹ Vgl. BEUTELSPACHER, A. (1991), S. 35

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Abbildung 7: Vigenere Quadrat

In diesem Zusammenhang sei noch das so genannte **ONE-TIME-PAD** erwähnt. Es wurde 1917 von Major J. Mauborgne und G. Vernam von AT&T erfunden. Es handelt sich hierbei um ein Vigenere Chiffre mit einem unendlich langen Schlüsselwort. Dieses Verfahren ist das einzige bisher bekannte, welches eine perfekte Sicherheit garantieren kann.

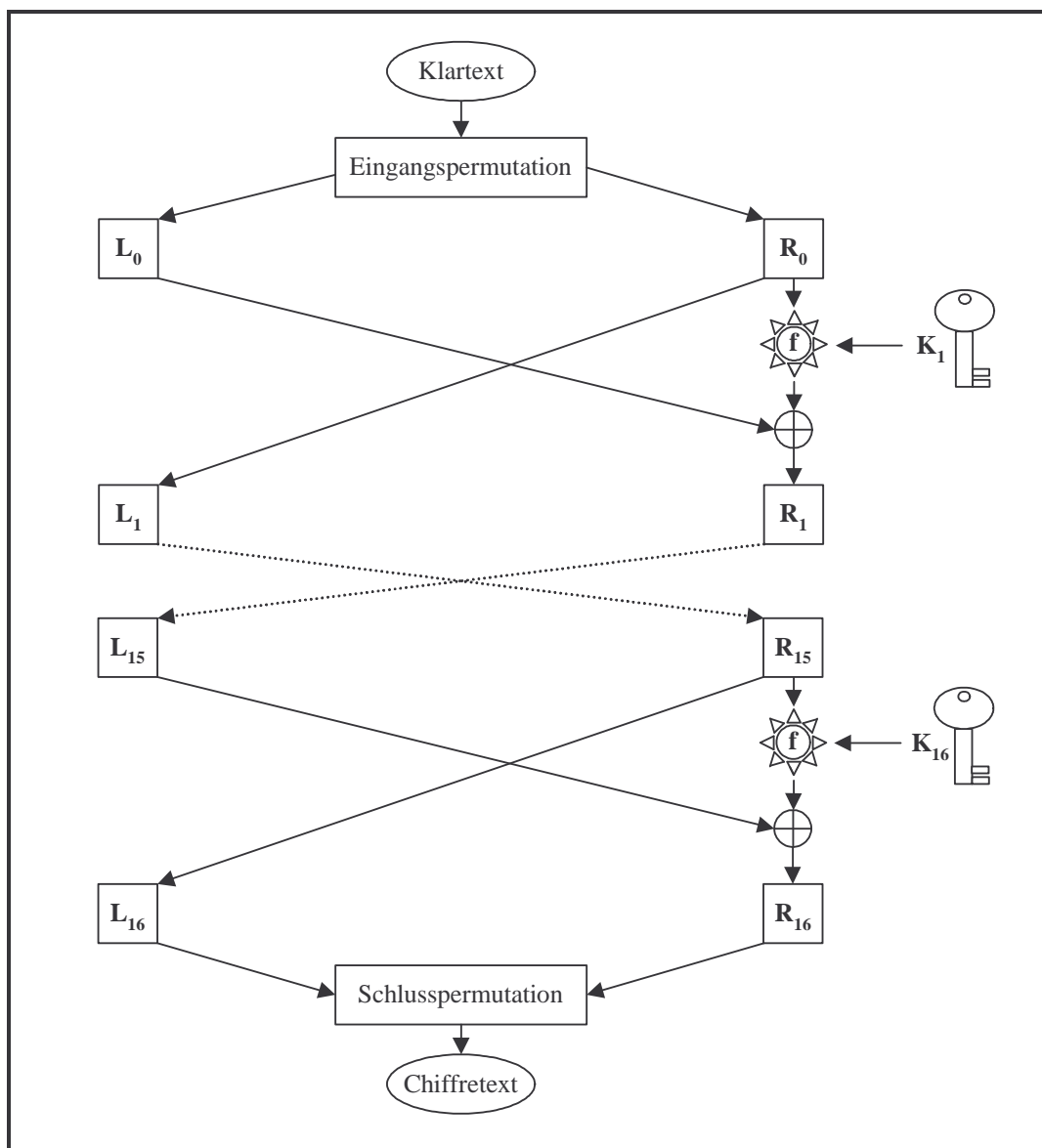
Definition: Ein Kryptosystem k wird als **perfekt** bezeichnet, wenn jeder Klartext mit einem zu k gehörigen Schlüssel auf jeden beliebigen Geheimtext abgebildet werden kann.¹⁰² Dies bedeutet, dass ein Angreifer aus einem Chiffretext nicht auf den Klartext schließen kann. Selbst ein Brute-Force Angriff auf ein perfektes Kryptosystem hat keinen Erfolg.

¹⁰² Vgl. NEUMANN, H. (2000), S. 18

Dieses Verfahren bietet eine hohe Sicherheit, es konnte sich jedoch in der freien Wirtschaft nicht durchsetzen. Dies ist hauptsächlich in der Länge des Schlüssels begründet. Dieser muss mindestens die Länge der eigentlichen Nachricht haben und auf einem sicheren Wege vom Sender zum Empfänger transportiert werden. Aus diesem Grund kommt es meist nur in militärischen und geheimdienstlichen Anwendungen zum Einsatz.

Der **DES (Data Encryption Standard)**¹⁰³ ist derzeit der am weitesten verbreitete Vertreter der symmetrischen Blockchiffren. Dieser Algorithmus wurde von Beginn an vollständig publiziert und war damit das erste Verfahren der Geschichte, bei dem das Kerckhoffsche Prinzip voll erfüllt wurde. Ursprünglich wurde es von Horst Feistel im Auftrag von IBM im Jahr 1973 unter dem Namen Lucifer vorgestellt. Lucifer arbeitete auf 64-Bit Blöcken mit einem 128-Bit Schlüssel und siegte bei einer öffentlichen Ausschreibung des NIST (National Institute of Standards and Technology, USA), welche die Entwicklung eines amerikanischen Verschlüsselungsstandards als Ziel hatte. Nachdem die Schlüssellänge auf 56-Bit herabgesetzt und Lucifer weiterentwickelt wurde, um eine einfache Implementierung in Hardware zu erreichen, wurde DES im Jahre 1977 in den USA offiziell eingeführt. Als Konsequenz der Veröffentlichung und der laufenden intensiven Schwachstellenanalyse ist die Sicherheit stets bekannt, wodurch das Vertrauen in DES wächst. Aus diesem Grund ist er im kommerziellen Bereich der am häufigsten verwendete Algorithmus und kommt vor allem im Bankenbereich erfolgreich zum Einsatz. DES verschlüsselt und entschlüsselt 64 Bit große Klartextblöcke mit einem 56 Bit Schlüssel. Dabei kommen keine komplizierten mathematischen Funktionen zum Tragen, es werden lediglich einzelne Bits, nach festen Regeln permutiert und substituiert. Der Klartext wird in 16 Runden durch Vertauschen und Ersetzen derart verändert, dass der Chiffretext nicht ohne Kenntnis des Schlüssels in einer annehmbaren Zeitspanne ermittelt werden kann.

¹⁰³ Vgl. ERTEL, W. (2001), S. 54

Abbildung 8 : Rundenschema des DES¹⁰⁴

Da DES auf 64 Bit Blöcke arbeitet, wird der Klartext zunächst in Blöcke dieser Größe eingeteilt. Nach der Eingangspemutation wird jeder 64 Bit Block in einen linken Teil L_0 und den rechten Teil R_0 mit je 32 Bit gesplittet. In jeder der 16 Runden wird die rechte Hälfte unverändert als linke Hälfte der nächsten Runde übernommen. Es gilt $L_1 = R_0$, $L_2 = R_1$, ..., $L_{16} = R_{15}$. Auf die rechte Hälfte wird nun die Funktion f mit dem Teilschlüssel K_1 angewendet. Das Ergebnis wird mit der linken Hälfte XOR-verknüpft und wird zur rechten Hälfte R_1 der nächsten Runde. Formal gilt für die 16 Runden:

$$L_i = R_{i-1} \quad \text{für } i = 1, \dots, 16$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \quad \text{für } i = 1, \dots, 16$$

¹⁰⁴ Vgl. ERTEL, W. (2001), S. 58

DES bietet einen ausreichenden Schutz gegen die meisten Angriffe. Ein Kritikpunkt ist jedoch die mit 56 Bit kurze Schlüssellänge, aus der sich eine mögliche Schlüsselanzahl von 2^{56} ergibt, womit eine Brute-Force Angriff bereits im Rahmen des möglichen liegt. Dies belegen folgende erfolgreiche Angriffe auf das Verfahren. Im Jahre 1994 wurde DES mit einem Rechenaufwand von 50 Tagen auf 12 HP-9735-Workstations erstmals entschlüsselt. Am 17.7.1998 überwindet die Electronic Frontier Foundation (EFF) mit einem Spezialchip den Algorithmus in weniger als drei Tagen und am 19.4.1999 decodieren 100.000 PCs von Distributed.net und der EFF Spezialrechner DES in 22 Stunden und 15 Minuten. Bei diesen beachtlichen Rekorden ist jedoch zu bedenken, dass die eingesetzten Rechner einen Wert in die Millionen Euro haben und meist nur von Industrieländern oder großen Organisationen eingesetzt werden können.

In Anbetracht der Anfälligkeit des DES auf Brute-Force Angriffe gibt es alternative Verfahren, wie **TripleDES**, **AES** und **IDEA**¹⁰⁵. Bei TripleDES wird der Klartext dreimal mit DES verschlüsselt. Die Schlüssellänge wird dabei beim Verwenden von zwei verschiedenen DES Schlüsseln auf 112 Bit erhöht.

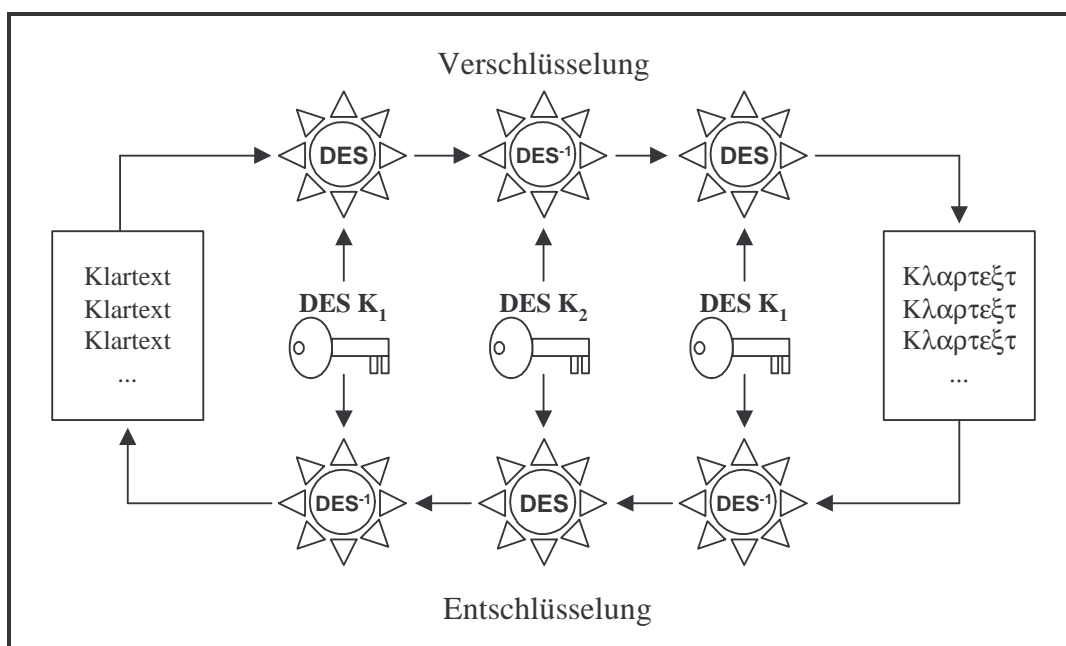


Abbildung 9 : TripleDES Schema¹⁰⁶

Die Vorteile der symmetrischen Algorithmen sind die relativ einfache Implementierung und hohe Geschwindigkeit. Auch die Vielfalt der bekannten Algorithmen ist sehr positiv zu sehen.

¹⁰⁵ Vgl. ERTEL, W. (2001), S. 64 und S. 71

¹⁰⁶ Vgl. LUITWIELER, J. (1998), Abbildung 3.15 „TripleDES“

Die bereits dargestellten symmetrischen Verfahren haben eine grundlegende Gemeinsamkeit. Bevor Sender und Empfänger miteinander vertraulich kommunizieren können, müssen sie sich auf einen gemeinsamen geheimen Schlüssel einigen und diesen über einen sicheren Kanal austauschen. Diese Prämisse des sicheren Kanals für den Schlüsseltransport ist ein großes Manko der symmetrischen Verschlüsselung, aber auch das Schlüsselmanagement stellt ein großes Problem dar. Will eine Person geschützte Daten nicht nur mit einer Person, sondern mit einem größeren Personenkreis von n Teilnehmern austauschen, so müsste sie mit jedem Kommunikationspartner einen geheimen Schlüssel vereinbaren. Wenn jeder Teilnehmer mit jedem einzelnen des Personenkreises in Kontakt treten will, so werden

$$\text{Anzahl} = \frac{n * (n - 1)}{2}$$

geheime Schlüssel benötigt.

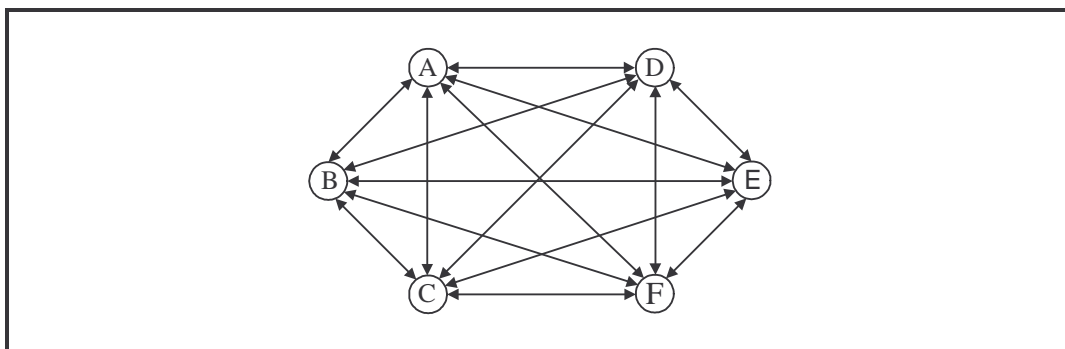


Abbildung 10 : Schlüsselanzahl bei 6 Teilnehmern¹⁰⁷

Aus der Abbildung ist leicht ersichtlich, dass für den normalen Geschäftsverkehr dieses Verfahren nicht geeignet ist. Es ist zu aufwändig, derart viele Schlüssel geheim zu verwalten und diese auf Aktualität zu prüfen. Es stellt sich die Frage, wie es möglich ist, das Schlüsselproblem zu umgehen.

3.2.2 Asymmetrische Verschlüsselung

Erst Mitte der siebziger Jahre wurde eine Lösung des Schlüsselproblems gefunden. Diese heißt **asymmetrische Verfahren** oder **Public Key Konzept** und wurde 1976 von den Mathematikern Withfield Diffie und Martin Hellmann entwickelt.

Bei dem Public Key Konzept besitzt jeder Teilnehmer stets ein Schlüsselpaar (E, D), wobei E als **öffentlicher Schlüssel (public key)** und D als **privater Schlüssel (privat**

¹⁰⁷ Vgl. LUITWIELER, J. (1998), Abbildung 3.3 „Schlüsselwachstum“

key) bezeichnet wird. Der öffentliche Schlüssel E (Encryption) dient zur Verschlüsselung, während der private Schlüssel D (Decryption) zur Entschlüsselung verwendet wird. Alle öffentlichen Schlüssel sind in einer allgemein zugänglichen Datei, einem Schlüsselverzeichnis nach dem Modell des Telefonbuchs aufgelistet. Im Gegensatz dazu werden die privaten Schlüssel geheim gehalten und sind ausschließlich ihrem Besitzer allein zugänglich.¹⁰⁸

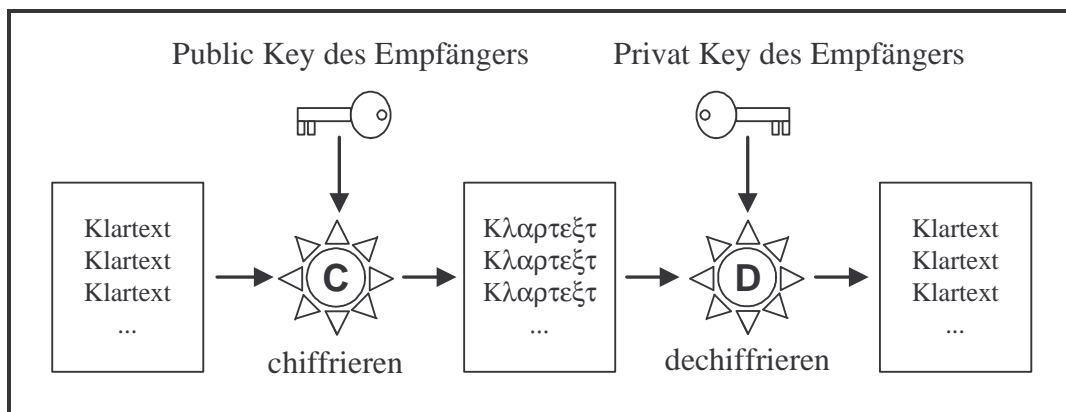


Abbildung 11 : Schema der asymmetrischen Verschlüsselung¹⁰⁹

Im Folgenden wird ein Beispiel aus dem Alltag angeführt, um das diffizile Prinzip der Public Key Kryptographie begreiflicher darzustellen und den Umgang mit der Terminologie zu erleichtern.

Briefkastenbeispiel:¹¹⁰

Jeder der n Teilnehmer hat einen Briefkasten mit Namensschild, Schloss und einen zugehörigen Schlüssel, dabei übernehmen die Briefkästen die Funktion der öffentlichen Schlüssel, die individuellen Briefkastenschlüssel entsprechen hingegen den private keys.

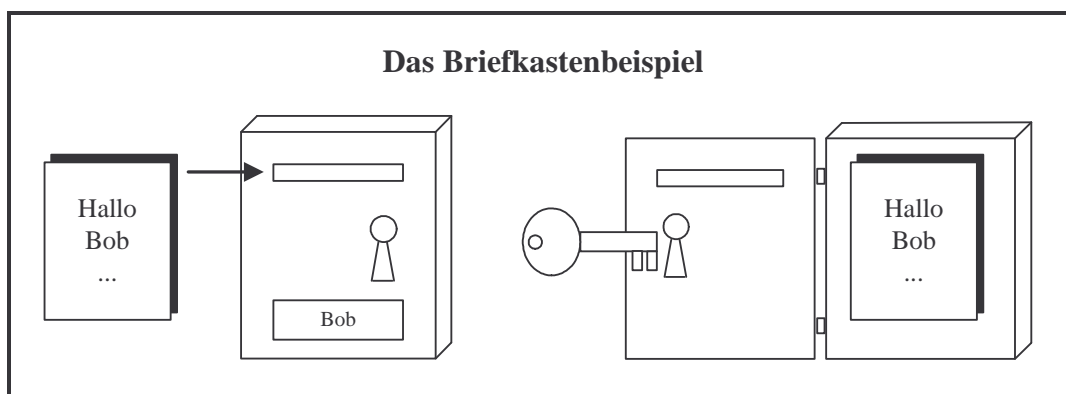


Abbildung 12 : Beispiel eines Public Key Konzeptes

¹⁰⁸ Vgl. BEUTELSPACHER, A. (1991), S. 112

¹⁰⁹ Vgl. HOCHMANN, S. (2001), S. 14

¹¹⁰ Vgl. BEUTELSPACHER, A. (1991), S. 114

Um Bob eine vertrauliche Nachricht zukommen zu lassen, muss Alice diese in seinen Briefkasten werfen. Dieser Vorgang entspricht der Verschlüsselung, denn die Nachricht ist nun nicht mehr lesbar. Das Leeren des Briefkastens ist nur durch den persönlichen Schlüssel möglich und entspricht der Entschlüsselung.

Formal muss ein sinnvolles asymmetrisches Verschlüsselungsverfahren folgende Forderungen¹¹¹ erfüllen:

1. Eindeutige Entschlüsselung:

Für alle Nachrichten m gilt $D_T(E_T(m)) = m$, wobei D_T den privaten, E_T den öffentlichen Schlüssel des Teilnehmers T und $E_T(m)$ den Geheimtext bezeichnet.

2. Public Key Eigenschaft:

Es ist unmöglich, aus der Kenntnis von E_T auf D_T zu schließen.

Im Briefkastenbeispiel entspricht die erste Forderung der Tatsache, dass jeder Teilnehmer T die Möglichkeit besitzt eine eingeworfene und damit unlesbare Botschaft $E_T(m)$ durch Öffnen des Briefkastens mit seinem Schlüssel D_T in die Nachricht m zu entschlüsseln. Die zweite Forderung entspricht hingegen dem Faktum, dass aus der Kenntnis des Briefkastens noch nicht die Möglichkeit entsteht, die eingeworfene Post lesen zu können.

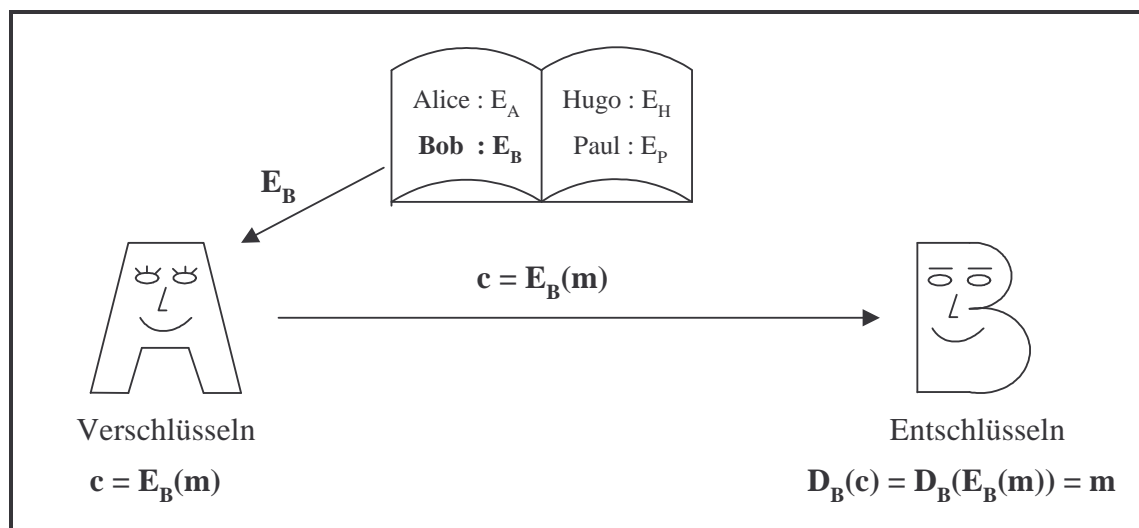


Abbildung 13 : Schlüsselschema des Public Key Konzeptes¹¹²

¹¹¹ Vgl. BEUTELSPACHER, A: (2001), S. 11

¹¹² Vgl. NEUMANN, H. (2001), S. 6

Die Anwendung einer asymmetrischen Verschlüsselung stellt sich wie folgt dar:

Will Alice an Bob eine Nachricht m senden, so sucht sie den öffentlichen Schlüssel E_B von Bob im Schlüsselverzeichnis heraus, verschlüsselt die Nachricht m mittels E_B und sendet $E_B(m)$ an Bob. Dieser kann den Geheimtext $E_B(m)$ durch $m = D_B(E_B(m))$ entschlüsseln, da er allein seinen geheimen Schlüssel D_B kennt.

Der größte Vorteil von asymmetrischen Verschlüsselungssystemen liegt im einfachen Schlüsselmanagement. Der Schlüsselaustausch ist nicht mehr notwendig und eine spontane Kommunikation ist jeder Zeit möglich. Bei einem symmetrischen System mit n Teilnehmern werden bekanntlich $n * (n - 1) / 2$ Schlüssel eingesetzt. Die Schlüsselanzahl steigt somit quadratisch mit der Zahl der Teilnehmer. Demgegenüber benötigt bei einem asymmetrischen Verfahren jeder Teilnehmer nur zwei Schlüssel, von denen lediglich einer geheim gehalten werden muss. Die Anzahl ist also gerade doppelt so groß wie die Anzahl der Teilnehmer. Beispielsweise werden in einem symmetrischen System bei 1.000 Teilnehmern 499.500 Schlüssel benötigt, in einem asymmetrischen System liegt die Zahl der Schlüssel lediglich bei 2.000.

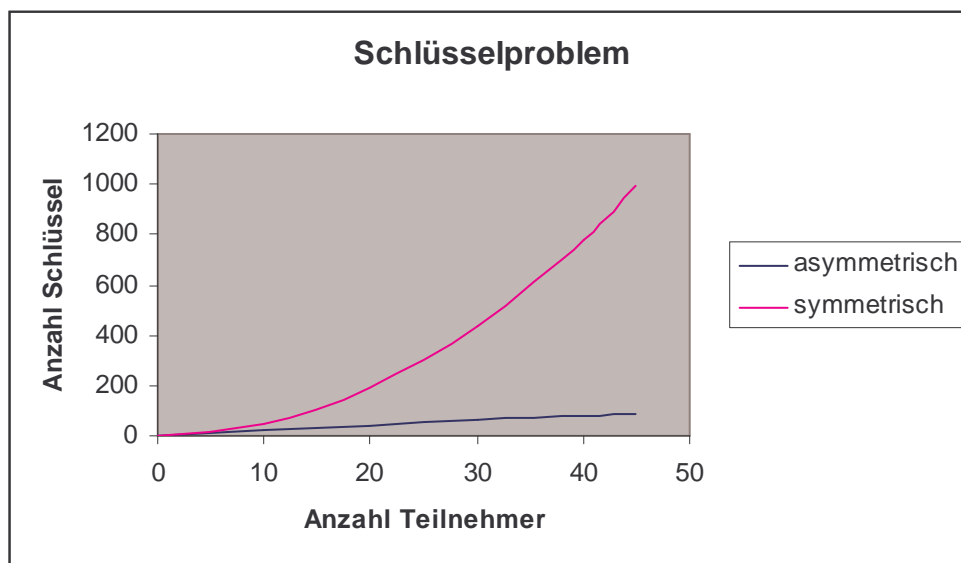


Abbildung 14: Wachstum der Schlüsselanzahl bei steigender Teilnehmerzahl

Ein weiterer Vorteil eines asymmetrischen Systems ist das problemlose Hinzufügen neuer Geschäftspartner, während bei einem symmetrischen jeder Teilnehmer mit einem Neuzugang einen weiteren Schlüssel austauschen muss.

Für die praktischen Umsetzung asymmetrischer Verfahren werden so genannte **Einwegfunktion**¹¹³ benötigt. Diese sind einfach auszuführen, aber schwer zu invertieren. Ein Telefonbuch ist ein Beispiel für eine Einwegfunktion. Dies ermöglicht ein einfaches Zuweisen einer Telefonnummer zu einer Person, wobei das Auffinden einer Person anhand der Telefonnummer bedeutend aufwändiger ist.

Definition: Eine Funktion $f : X \rightarrow Y$ heißt Einwegfunktion (one-way function), wenn gilt:

- (Einfache Berechenbarkeit) Es gibt ein effizientes Verfahren zur Berechnung von $y = f(x)$ für jedes $x \in X$.
- (Schwierig zu invertieren) Es gibt kein effizientes Verfahren zur Berechnung von $x = f^{-1}(y)$ für jedes $y \in Y$.

Eine Funktion $f : X \rightarrow Y$ heißt Trapdoor Einwegfunktion (trapdoor one-way function), wenn gilt:

- $y = f(x)$ ist „leicht“ mit einem effizienten Algorithmus E zu berechnen.
- $x = f^{-1}(y)$ ist „leicht“ mit einem effizienten Algorithmus D zu berechnen.

Die Bestimmung von D aus E ist jedoch ohne eine geheim zu haltende Zusatzinformation (Trapdoor) „schwer“.

Die Existenz dieser Funktionen konnte bisher nicht bewiesen werden. Nach dem heutigen Wissensstand wird jedoch davon ausgegangen, dass die diskrete Exponentialfunktion und das Quadrieren¹¹⁴ modulo n Einwegfunktionen darstellen¹¹⁵. Dieses Prinzip der Einwegfunktion wird ebenfalls für die kryptographische Hashfunktion genutzt, auf die im Kapitel 3.3 „Signaturverfahren“ näher eingegangen wird. Für die asymmetrischen Verfahren ist das Konzept der **Trapdoor Einwegfunktionen** von immenser Bedeutung. Hierbei handelt es sich um eine Einwegfunktion, also eine außerordentlich schwer zu invertierende Funktion, zu der es eine Geheiminformation gibt, mit der sie invertiert werden kann. Diese Geheiminformation wird als Geheimtür oder Trapdoor bezeichnet.

¹¹³ Vgl. BEUTELSPACHER, A. (2001), S. 12

¹¹⁴ Siehe Anhang A2 (Z15)

¹¹⁵ Vgl. BEUTELSPACHER, A. (1991), S. 13

3.2.2.1 Der RSA Algorithmus

Im Jahre 1978 entwickelten Ronald Rivest, Adi Shamir und Leonard Adleman den nach ihnen benannten RSA Algorithmus, als sie zu zeigen versuchten, dass Public Key Kryptographie unmöglich sei. Dieser Algorithmus ist einer der populärsten und wichtigsten Vertreter der asymmetrischen Verschlüsselungsverfahren und ermöglicht das Erstellen fortgeschrittener elektronischer Signaturen.

3.2.2.2 Die Schlüsselerzeugung des RSA Algorithmus¹¹⁶

Die Schlüsselerzeugungsstelle¹¹⁷ oder der Anwender wählt zwei Primzahlen¹¹⁸ p und q , deren Länge, je nach Sicherheit, zwischen 384 und 512 Bit liegen sollte.¹¹⁹

Aus diesen Zahlen wird

$$n = p * q \text{ und } \Phi(n) = \Phi(p * q) = (p - 1)(q - 1) \text{ }^{120}$$

berechnet, wobei n eine Länge von 512 bis 1024 Bit erreicht. Die Regulierungsbehörde für Post und Telekommunikation RegTP erachtet einen RSA Algorithmus mit einem n der Länge von 1024 Bit bis Ende 2006 als einen geeigneten und sicheren Kryptoalgorithmus im Sinne des Signaturgesetzes¹²¹. Im nächsten Schritt wird eine Zahl e gewählt, die zu $\Phi(n)$ relativ prim¹²² ist. Das bedeutet, dass der $ggT(e, \Phi(n)) = 1$ ist¹²³. e kann bis auf die relative Primität frei bestimmt werden, aus diesem Grund wird oft die vierte Fermat Zahl $F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65.537$ gewählt. Diese erleichtert durch ihre binäre Darstellung `1 0000 0000 0000 0001` ein Potenzieren z.B. mit dem Square-and-Multiply-Algorithmus¹²⁴. Als letzter Schritt wird eine Zahl d als Lösung der Gleichung $ed = 1 \text{ mod } \Phi(n)$ berechnet. d kann eindeutig mit dem erweiterten Euklidischen Algorithmus berechnet werden. Auf diese Weise erhält der Anwender das Zahlenpaar $P = (e, n)$ als öffentlichen Schlüssel und $S = (d, n)$ als privaten Schlüssel.

¹¹⁶ Siehe Anhang A2 (Z16)

¹¹⁷ Die Schlüsselerzeugungsstelle (z.B. ein Zertifizierungsdiensteanbieter) ist eine Institution, welche Schlüssel erzeugt und vergibt.

¹¹⁸ Siehe Anhang A2 (Z3)

¹¹⁹ Vgl. ERTEL, W. (2001), S. 76

¹²⁰ Siehe Anhang A2 (Z7)

¹²¹ Vgl. Geeignete Kryptoalgorithmen (2002), S. 3

¹²² Siehe Anhang A2 (Z6)

¹²³ Siehe Anhang A2 (Z5)

¹²⁴ Vgl. NEUMANN, H. (2001), S. 16

Der Anwender muss also folgende Schritte durchlaufen:

1. Wahl der Primzahlen p und q .
2. Berechnung des Modul $n = p * q$.
3. Berechnung von $\Phi(n) = \Phi(p * q) = (p - 1)(q - 1)$.
4. Wahl des Exponenten e mit der Bedingung, dass $\text{ggT}(e, \Phi(n)) = 1$.
5. Berechnung von d als Lösung der Gleichung $ed = 1 \text{ mod } \Phi(n)$.
6. $P = (e, n)$ öffentlicher Schlüssel.
 $S = (d, n)$ privater Schlüssel.

3.2.2.3 Die Anwendung des RSA Algorithmus

Um eine Nachricht m zu verschlüsseln, muss diese zunächst durch eine oder mehrere natürliche Zahlen m_1, \dots, m_k mit $m_i \leq n$ dargestellt werden, wobei n der Modul des RSA Schlüssel ist. Eine Möglichkeit dies zu erreichen, ist jedes einzelne Zeichen der Nachricht durch ihren ASCII Wert¹²⁵ zu ersetzen.

Aus dem Begriff „KLARTEXT“ wird so							
K	L	A	R	T	E	X	T
01001011	01001100	01000001	01010010	01010100	01000101	01011000	01010100

Tabelle 3 : Beispiel einer Umwandlung in ASCII Werte

Jedes Zeichen (einschließlich Satzzeichen und Zwischenräume) wird auf diese Weise als eine Folge von acht Bits dargestellt. Wenn n eine 1024 Bit Zahl ist, so werden 128 Zeichen zu Blöcken von $128 * 8 = 1024$ Bit zusammen gefasst. Ein solcher 1024 Bit Block wird nun als natürliche Zahl $M \in Z_n$ interpretiert und durch $E(M) = M^e \text{ mod } n = C$ **verschlüsselt**. Die Nachricht wird also mit e potenziert und mit dem RSA Modul n reduziert, wobei das Paar (e, n) der öffentliche Schlüssel des Empfängers ist.

Der Empfänger **entschlüsselt**, indem er mit seinem privaten Schlüsselpaar (d, n) $D(C) = C^d \text{ mod } n = M$ berechnet.

¹²⁵ Siehe Anhang A2 (Z19)

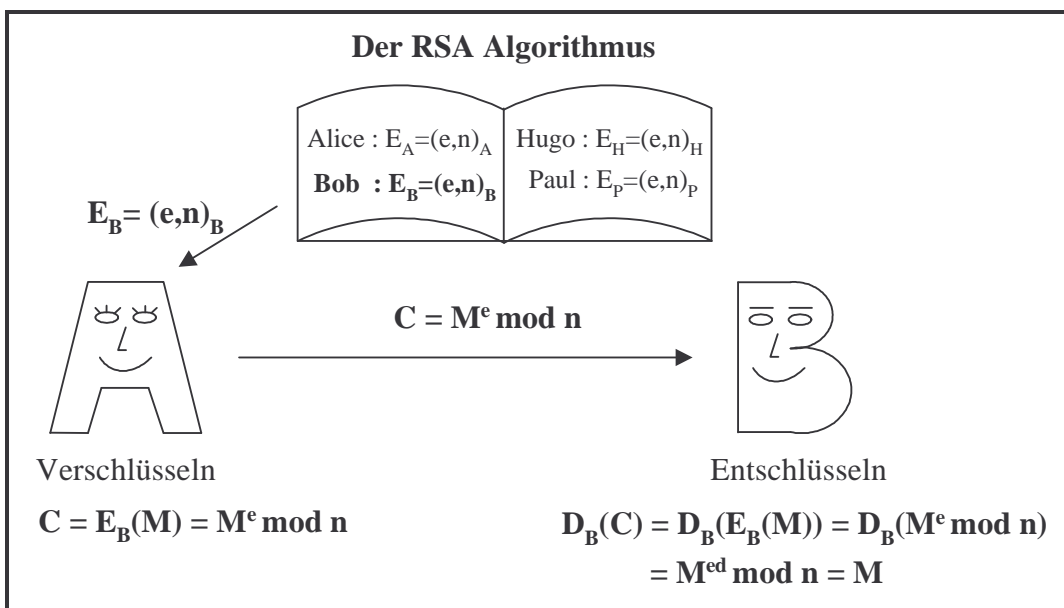


Abbildung 15 : Asymmetrische Verschlüsselung mit dem RSA Algorithmus

3.2.2.4 Die Korrektheit des RSA Algorithmus

Unter der Korrektheit des Algorithmus ist zu verstehen, dass die Verschlüsselungs- und die Entschlüsselungsfunktionen invers zueinander sind. Für eine beliebige Nachricht M muss gelten, dass $D(E(M)) = E(D(M)) = M$ ist.

Aus der Konstruktion der Funktionen folgt, dass

$$D(E(M)) = D(M^e \bmod n) = M^{ed} \bmod n = E(M^d \bmod n) = E(D(M))$$

gilt. Da $M^{ed} \bmod n = M$ gilt¹²⁶, arbeitet der RSA Algorithmus korrekt.

3.2.2.5 Sicherheit des RSA Algorithmus

Die Public Key Eigenschaft des RSA Algorithmus besteht darin, dass aus der Kenntnis des öffentlichen Schlüssels (e, n) der private Schlüssel d nicht zu berechnen ist. Es ist jedoch unproblematisch mit Hilfe des erweiterten Euklidischen Algorithmus und mit der Kenntnis von p und q den geheimen Schlüssel d aus der Gleichung $ed = 1 \bmod \Phi(n)$ zu bestimmen. Der RSA Algorithmus ist eine Trapdoor Einwegfunktion, da das Potenzieren mit e modulo n leicht zu berechnen ist, die Umkehrfunktion jedoch ohne die Trapdoorinformation d nicht effizient möglich ist. Die Sicherheit des RSA Algorithmus basiert auf der Tatsache, dass es sehr zeitaufwendig ist, große Zahlen n in ihre Primfaktoren p und q zu zerlegen. Durch einen seit 1991 laufenden Wettbewerb der Firma RSA

¹²⁶ Vgl. ERTEL, W. (2001), S. 77

Security, dessen Ziel die Zerlegung großer RSA Zahlen ist, wird eine weltweite Überprüfung des Faktorisierungsfortschrittes erreicht. Im August 1999 wurde RSA-155 mit 155 Dezimalstellen¹²⁷ faktorisiert und hält damit den Faktorisierungsrekord. Für diesen Erfolg wurde eine Rechenzeit von 4 Monaten an 292 PCs und Workstations mit etwa 400 MHz Taktfrequenzen benötigt. 5 Jahre zuvor wurde mit vergleichbarem Aufwand RSA-129 entschlüsselt, dies zeigt eine Steigerung von 26 Dezimalstellen in 5 Jahren. Aus diesen Rekorden ist ersichtlich, dass ein 1024 Bit RSA Modul¹²⁸ derzeit als sicher einzustufen ist. Der erste RSA-308 Faktorisierungsrekord wird im Jahre 2037 erwartet. Trotz dieser hohen Sicherheit muss bedacht werden, dass die Faktorisierung von großen Zahlen ein sehr schwieriges Problem darstellt. Experten vermuten, dass kein effizientes Verfahren zur Faktorisierung existiert, dies ist jedoch nicht bewiesen.¹²⁹

Für die Sicherheit des RSA Algorithmus ist die Wahl der Primzahlen p und q von immenser Bedeutung. Diese Zahlen müssen effizient und zufällig aus einer möglichst großen Menge von Primzahlen gewählt werden, um einem Angreifer die Möglichkeit eines Brute-Force Angriffes auf die Faktorisierung des Modul n zu nehmen. Zum zufälligen Erzeugen einer Primzahl werden Zufallszahlen generiert und getestet, ob diese prim sind. Ein effizienter Test ist beispielsweise der Primzahltest von Miller und Rabin¹³⁰. Die Anzahl der Primzahlen mit 512 Bit Länge liegt bei¹³¹ $\approx 1.9 \cdot 10^{151}$. Diese große Menge von Primzahlen schließt die Möglichkeit des Abspeichern und Testen aller Primzahlen aus. Der Modul n kann demnach nicht durch Multiplizieren beliebiger 512 Bit Primzahlen effizient berechnet werden.

3.2.3 Hybridverfahren

Trotz der vielen Vorteile der asymmetrischen Algorithmen werden diese in der Praxis nur selten für die Verschlüsselung verwendet. Dies ist darin begründet, dass bislang kein Kryptosystem bekannt ist, das sowohl sicher als auch schnell ist. Um die Geschwindigkeitsvorteile von symmetrischen und das Schlüsselmanagement asymmetrischen Techniken gemeinsam nutzen zu können, werden zur Verschlüsselung in der Praxis meist Mischverfahren (**Hybridverfahren**¹³²) verwendet.

¹²⁷ 155 Dezimalstellen entsprechen einer 512 Bit Zahl.

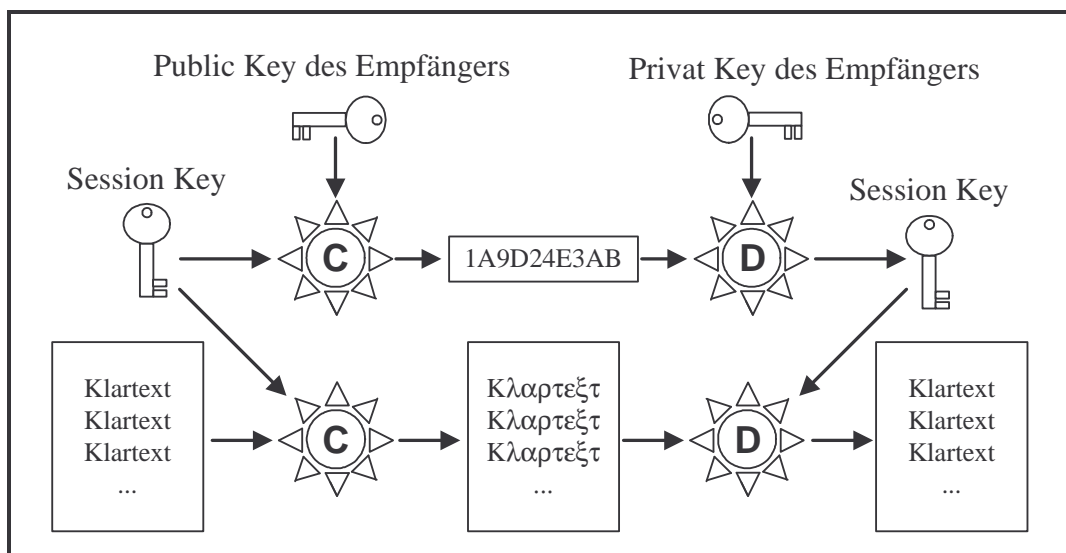
¹²⁸ 1024 Bit Zahl entspricht 308 Dezimalstellen

¹²⁹ Vgl. ERTEL, W. (2001), S. 79

¹³⁰ Vgl. ERTEL, W. (2001), S. 79

¹³¹ Siehe Anhang A2 (Z4)

¹³² Vgl. CrypTool (2002), S. 9

Abbildung 16 : Schema des Hybridverfahrens¹³³

Hier werden die Daten mittels symmetrischer Verfahren verschlüsselt. Der Schlüssel ist ein vom Absender zufällig generierter **Sitzungsschlüssel** (session key), der nur für diese Nachricht verwendet wird. Anschließend wird dieser Sitzungsschlüssel mit Hilfe des asymmetrischen Verfahrens verschlüsselt und zusammen mit der Nachricht an den Empfänger übertragen. Der Empfänger kann den Sitzungsschlüssel mit Hilfe seines geheimen Schlüssels bestimmen und mit diesem die Nachricht entschlüsseln. Auf diese Weise nutzt der Anwender das einfache Schlüsselmanagement asymmetrischer Verfahren und kann dennoch große Datenmengen schnell und effektiv mit symmetrischen Verfahren verschlüsseln.

3.3 Signaturverfahren

Die elektronische Signatur stellt ein elektronisches Äquivalent zur handschriftlichen Unterschrift dar. Der allgemeine Aufbau eines **Signaturschemas** beinhaltet eine **Signaturfunktion**, die geheim gehalten wird, und eine **Verifikationsfunktion**, die öffentlich bekannt ist. Bei dieser Modellannahme ist es nicht möglich, von der Verifikationsfunktion auf die Signaturfunktion zu schließen.¹³⁴

Ein Teilnehmer T signiert eine Nachricht m , indem er seine Signaturfunktion s_T anwendet und so die Signatur $sig = s_T(m)$ erhält. Die Nachricht und die Signatur werden

¹³³ Vgl. HOCHMANN, S. (2001), S. 26

¹³⁴ Vgl. BEUTELSPACHER, A. (2001), S. 17

zum Empfänger gesendet, der mit der öffentlichen Verifikationsfunktion die Signatur auf Korrektheit prüft.

Jedes asymmetrische Verschlüsselungsverfahren kann zum Signieren genutzt werden. Bei diesen Verfahren ist die Verifikationsfunktion die Umkehrung der Signaturfunktion.

Es gilt $v_T(\text{sig}) = m$.

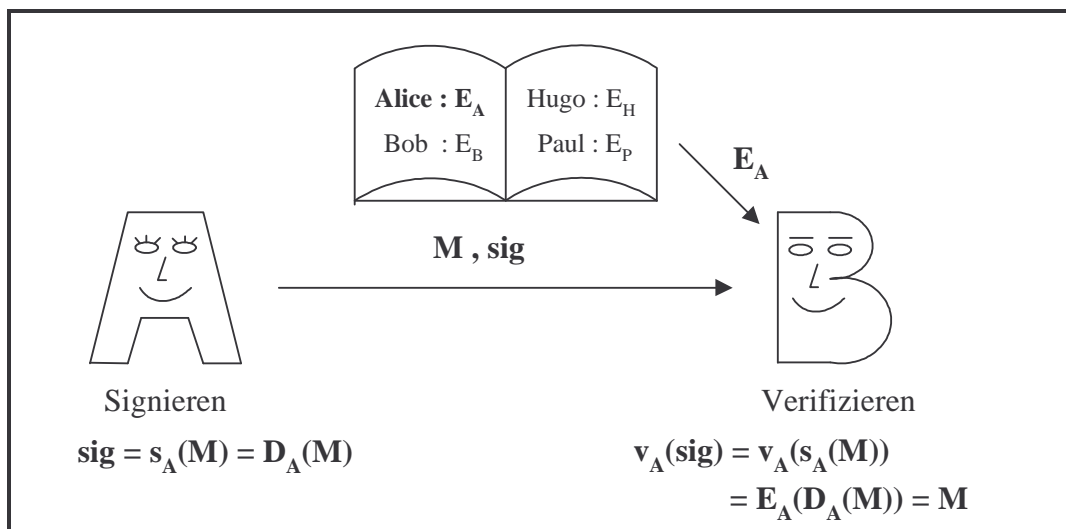


Abbildung 17 : Signaturschema

Wie bereits im Kapitel 3.2.2 „Asymmetrische Verschlüsselung“ verdeutlicht wurde, sind asymmetrische Signaturverfahren sehr rechenintensiv und nehmen daher bei langen Klartexten viel Zeit in Anspruch. Um den Datenverkehr nicht unnötig anwachsen zu lassen, wird nicht der gesamte Klartext signiert. An dieser Stelle kommen **kryptographische Hashfunktionen**¹³⁵ zum Einsatz. Bei einer Hashfunktion handelt es sich um eine mathematische Einwegfunktion, die eine Nachricht beliebiger Länge auf eine Zeichenfolge fester Größe abbildet. Diese Zeichenfolge wird als Hashwert bezeichnet und hat bei modernen Verfahren meist eine Länge von 128 oder 160 Bit.

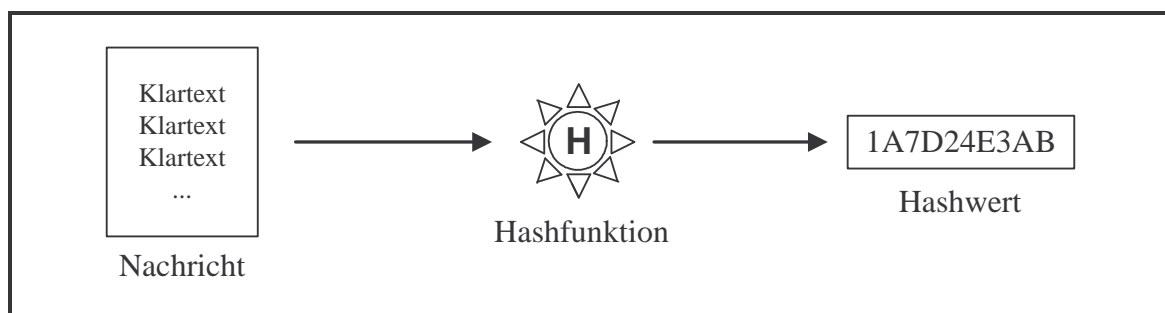


Abbildung 18 : Kryptographische Hashfunktion¹³⁶

¹³⁵ Vgl. CrypTool (2002), S. 108

¹³⁶ Vgl. HOCHMANN, S. (2001), S. 20

Das Signieren des Hashwertes anstelle des gesamten Dokumentes bringt jedoch ein nicht abschätzbares Sicherheitsrisiko mit. So stehen einer endlichen Anzahl möglicher Hashwerte eine unendliche Zahl möglicher Texte gegenüber. Es besteht theoretisch die Möglichkeit zu einem bereits signierten Hashwert einen zweiten Klartext zu finden, der auf denselben Hashwert abgebildet wird. Dieses Verfahren wird auch als Substitutions-attacke bezeichnet. Das Risiko der Substitution wird jedoch durch die Redundanz der natürlichen Sprache abgeschwächt. Dies bedeutet, dass zwar unendlich viele Möglichkeiten existieren Zeichen zu kombinieren, aber nicht alle Zeichenkombinationen ergeben einen sprachlichen Zusammenhang. Die Suche eines Klartextes mit bestimmter Bedeutung zu einer gegebenen Hashfunktion ist nahezu aussichtslos.

Moderne Hashfunktionen sollten den folgenden Anforderungen¹³⁷ genügen:

- Jeder Hashwert sollte etwa gleich oft vorkommen.
- Kleine Änderungen des Klartextes müssen den Hashwert verändern.
- Es darf nicht möglich sein, in realistischer Zeit einen zweiten sinnvollen Klartext zu finden, der denselben Hashwert besitzt.

Die letzte Forderung wird als **Kollisionssicherheit** bezeichnet. In der Literatur wird die starke und die schwache Kollisionssicherheit unterschieden. Ein Verfahren hat eine starke Kollisionssicherheit, wenn es nur schwer möglich ist, freie Kollisionen zu finden, d.h. es wird ein zweiter Klartext zu einem Hashwert gesucht, wobei der Klartext keinerlei Vorgaben hat. Bei der schwachen Kollisionssicherheit wird eine gebundene Kollision gesucht, d.h. der gesuchte Klartext zum gegebenen Hashwert hat bestimmte Vorgaben.

Es existieren eine Reihe von Hashverfahren, die folgenden kommen in der Praxis häufig zur Anwendung:

1. **MD 4** (Message Digest) und **MD 5** wurden von Ron Rivest entwickelt und erzeugen Hashwerte von 128 Bit Länge. Während MD4 leicht zu brechen ist, gilt MD5 als sehr sicher und findet unter anderem in PGP¹³⁸ Anwendung.
2. **RipeMD** wurde im Rahmen des RIPE-Projektes der EU entwickelt. Es existieren Versionen mit 128, 160, 256 und 320 Bit Hashwerten.
3. **SHA** (Secure Hash Algorithm) wurde vom National Institute of Standards and Technology (NIST) in Zusammenarbeit mit der NSA im Rahmen des Digital Signature Standard (DSS) entwickelt. Der dazugehörige Hash-Standard, Secure

¹³⁷ Vgl. LUTZENBERGER, T. (2002), S. 17

¹³⁸ Vgl. Kapitel 5.2 „Anbieter fortgeschrittener elektronischer Signaturen“

Hash Standard (SHS), spezifiziert SHA mit einer Hashwertlänge von 160 Bit. **SHA-1** korrigiert einen Fehler, der die Sicherheit von SHA beeinträchtigt. Dieses Verfahren ist sicherer als MD5, arbeitet jedoch langsamer.

Es ist empfehlenswert, ein Verfahren mit 160 Bit Länge zu wählen, um die Sicherheit des Verfahrens zu steigern. Bisher konnte die Existenz von perfekt sicheren kryptographischen Hashfunktionen nicht formal bewiesen werden. Die RegTP erachtet SHA-1 und RIPEMD-160 als geeignete und sichere Hashfunktionen im Sinne des Signaturgesetzes.¹³⁹

Nachricht : „a“	
Hashfunktion	Hashwert
MD 4	BDE52CB31DE33E46245E05FBDBD6FB24
MD 5	0CC175B9C0F1B6A831C399E269772661
SHA-1	86F7E437FAA5A7FCE15D1DDCB9EAEAEA377667B8
RipeMD-160	0BDC9D2D256B3EE9DAAE347BE6F4DC835A467FFE

Tabelle 4: Hashwerte der Nachricht „a“¹⁴⁰

Nachricht : „A“	
Hashfunktion	Hashwert
MD 4	D5EF20EEB3F75679F86CF57F93ED0FFE
MD 5	7FC56270E7A70FA81A5935B72EACBE29
SHA-1	6DCD4CE23D88E2EE9568BA546C007C63D9131C1B
RipeMD-160	DDADEF707BA62C166051B9E3CD0294C27515F2BC

Tabelle 5: Hashwerte der Nachricht „A“

Nachricht : „Die elektronische Signatur“	
Hashfunktion	Hashwert
MD 4	B7E3879D02427CDFC7D6C2892C9BE43B
MD 5	1C4FFAF2F75DFCA9531C38303A14A4A5
SHA-1	82AC6CAF61A660C4E6A4E844B6565285D650814D
RipeMD-160	B649AC74BCC97D703A4986707974C0E6941AEE21

Tabelle 6 : Hashwerte der Nachricht „Die elektronische Signatur“

¹³⁹ Vgl. Geeignete Kryptoalgorithmen (2002), S. 2

¹⁴⁰ Die Berechnung der Hashwerte wurde mit CrypTool 1.3.00 durchgeführt.

Die folgende Tabelle gibt einen Anhaltspunkt über die Geschwindigkeit der Hashfunktionen:

Hashfunktion	Blocklänge	Runden	Mbit / Sek	MByte / sek	Relative Geschwindigkeit
MD 4	128	241	191,2	23,90	1,00
MD 5	128	337	136,7	17,09	0,72
RipeMD-128	128	592	77,8	12,00	0,50
SHA-1	160	837	55,1	6,88	0,29
RipeMD-160	160	1013	45,5	5,68	0,24

Tabelle 7 : Eigenschaften der Hashfunktionen¹⁴¹

Der Ablauf einer Signaturerstellung mit Hilfe einer kryptographischen Hashfunktion und einem asymmetrischen Verschlüsselungsverfahren wird im Folgenden verdeutlicht.

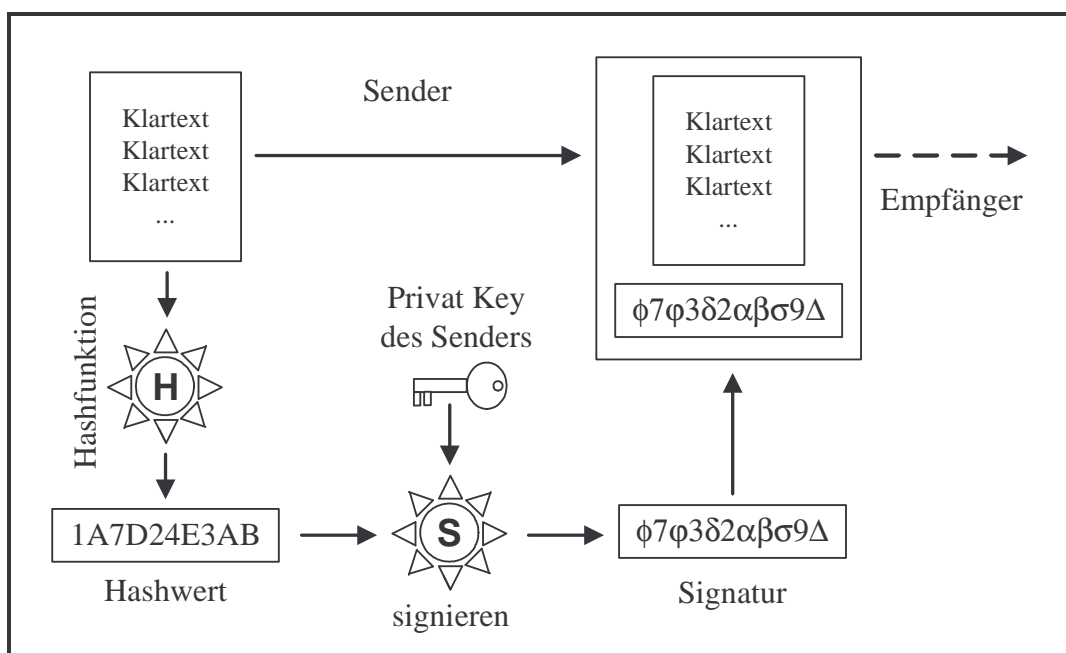
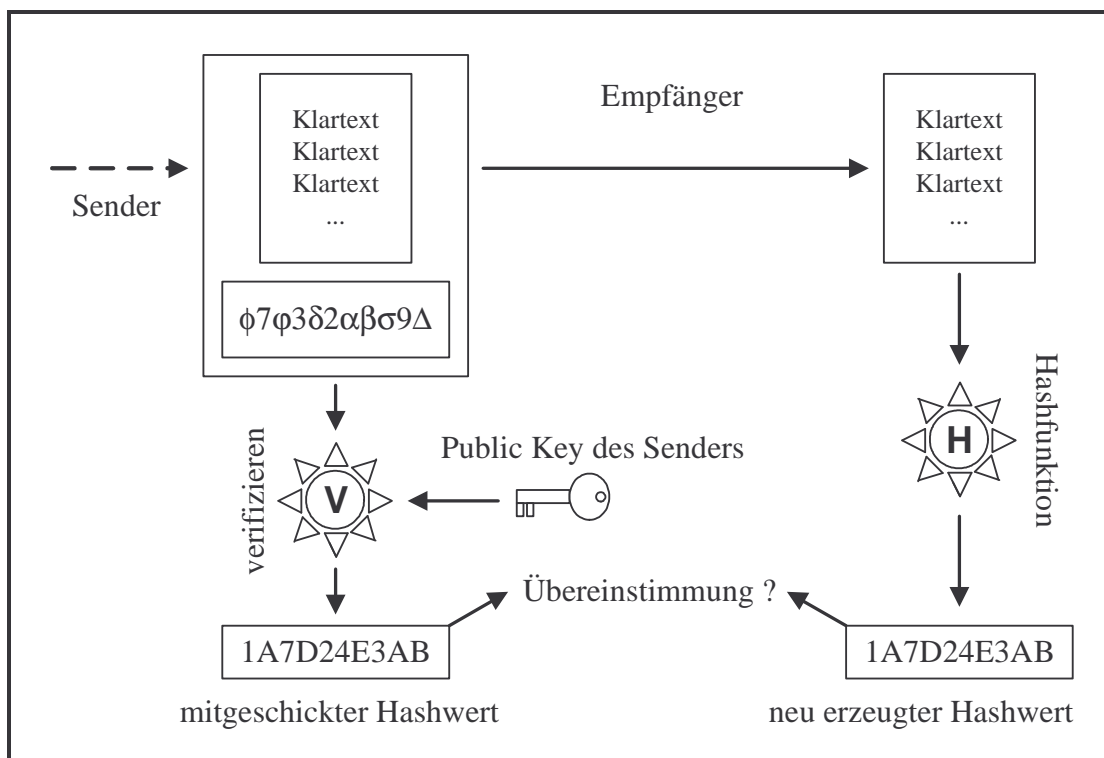


Abbildung 19 : Signatur erstellen¹⁴²

Der Absender einer Nachricht berechnet mit Hilfe der Hashfunktion den Hashwert über die zu signierenden Daten und verschlüsselt diesen mit seinem privaten Schlüssel. Das Ergebnis dieser Berechnung stellt die fortgeschrittene elektronische Signatur dar. Diese wird mit der Nachricht verknüpft und an den Empfänger übermittelt.

¹⁴¹ Vgl. The Hash Function (1999), How fast is RipeMD-160

¹⁴² Vgl. HOCHMANN, S. (2001), S. 22

Abbildung 20 : Signatur überprüfen¹⁴³

Der Empfänger kann die Signatur verifizieren, indem er mit Hilfe des Public Key des Senders die Signatur entschlüsselt. Dieser erhaltene Wert wird mit dem Hashwert des Klartextes verglichen, welchen der Empfänger durch Anwenden der Hashfunktion auf den Klartext neu erzeugt. Stimmen diese Hashwerte überein, ist die Signatur korrekt und das Dokument wurde ordnungsgemäß unterschrieben. Bei diesem Vorgang ist es nicht erforderlich, dass der Empfänger selbst ein Schlüsselpaar besitzt, denn es werden ausschließlich Schlüssel des Absenders genutzt. Auf diese Weise kann jeder, der im Besitz der Nachricht und der Signatur ist, diese verifizieren.

Im Folgenden wird zur Veranschaulichung des Signaturschemas ein Klartext unter Verwendung des RipeMD-160 gehasht und mittels eines RSA mit 512 Bit Schlüssel als Verschlüsselungsfunktion elektronisch signiert. In der Praxis werden Schlüssel und Signaturen im Hexadezimalsystem dargestellt, diese Verfahrensweise wird im folgenden Beispiel Verwendung finden.

¹⁴³ Vgl. HOCHMANN, S. (2001), S. 23

Sehr geehrter Bob,
 bitte überweisen Sie 1000 Euro auf folgendes Konto
 Kontonummer 1234
 Sparkasse Musterstadt

Mit freundlichen Grüßen
 Alice

Abbildung 21 : Klartext

Die Anwendung der Hashfunktion RipeMD-160 auf den Klartext führt zu dem Hashwert:

Hashwert M: 4EE7A7F0569028833D46EDE3A6DA942EFB330EF7

Dieser Hashwert M wird mit einem RSA Schlüssel (512 Bit) chiffriert. Die Signatur berechnet sich aus $sig = M^d \bmod n$ und stellt sich folgendermaßen dar¹⁴⁴:

Signatur sig 9E12B303C270D6C7FB04F895DED320DD
 4E48E32FCEE44412C4D7E8B665E3CE70
 A7B5E2CDC640D626FED0305F8DABD05C
 012D49898DA0ED33C7293CDAA64FE605

Der Empfänger verifiziert die Signatur mit dem öffentlichen Schlüssel (e, n) :

Exponent e : 10001

Modul n : FE653B2AB95AEDF110696CB509FB0A21C8AD0AEE7
 579453BC14E4DEAFEBBD0E6C17DBA7625CBD5A99E
 6DFE174D9220919C62996F966CA672DC73A76A734
 0374B

Der Hashwert M ergibt sich dabei aus $M = M^{de} \bmod n$. Falls dieser berechnete Wert mit dem mitgeschickten Hashwert übereinstimmt, wurde die Nachricht erfolgreich verifiziert.

¹⁴⁴ Die Berechnungen im Folgenden wurden mit CrypTool 1.3.00 durchgeführt.

Der RSA Algorithmus wird in der Praxis am häufigsten eingesetzt, um fortgeschrittene elektronische Signaturen zu erstellen. Es existieren jedoch einige Alternativen zu RSA-basierten Verfahren:

1. Die Sicherheit des **ElGamal** Signaturverfahren¹⁴⁵ beruht auf dem Problem der Berechnung diskreter Logarithmen. Eine effizientere Variante des ElGamal Verfahrens ist der Digital Signature Algorithm¹⁴⁶ **DSA**, der 1991 vom US-amerikanischen National Institute of Standards NIST vorgeschlagen und später zum amerikanischen Signaturstandard erklärt wurde. Im Gegensatz zum RSA Algorithmus und ElGamal ist das Chiffrieren mit DSA nicht möglich. Dieses Verfahren kommt in Frankreich zur Anwendung, da das französische Recht das Signieren von elektronischen Daten zwar gestattet, jedoch ist das Verschlüsseln von Daten ohne Genehmigung verboten.
2. Die wichtigste und bekannteste Alternative zu RSA-basierten Verfahren ist die Verwendung elliptischer Kurven¹⁴⁷, so genannte ECC Verfahren (Eliptic Curves Cryptography). Diese sind von besonderem Interesse, da sie im Vergleich mit RSA-basierten Verfahren bei gleicher Sicherheit mit kürzeren Schlüssellängen auskommen.

Verfahren	Vergleichbare Schlüssellängen in Bit		
RSA	512	1024	2048
ECC	108 ¹⁴⁸	160	210

Tabelle 8: Vergleich der Schlüssellängen bei RSA und ECC¹⁴⁹

¹⁴⁵ Vgl. BUCHMANN, J. (2001), S. 182

¹⁴⁶ Vgl. BUCHMANN, J. (2001), S. 187

¹⁴⁷ Vgl. BUCHMANN, J. (2001), S. 196

¹⁴⁸ Ein 108 Bit ECC Schlüssel wurde im Mai 2000 auf 9500 Rechnern in vier Monaten entschlüsselt.

¹⁴⁹ Vgl. KOY, H. (2001), S. 9

4 Die elektronische Signatur in der praktischen Anwendung

Im vorangegangenen Kapitel wurden die theoretischen Grundlagen der elektronischen Signatur dargelegt. Im Folgenden wird die praktische Anwendung am Beispiel der qualifizierten elektronischen Signaturen gemäß SigG01 erläutert. Diese Vorgehensweise wurde gewählt, da ausschließlich diese Form gemäß der deutschen Gesetzgebung der handschriftlichen Unterschrift gleichgestellt ist.

Zum Ausstellen einer qualifizierten elektronischen Signatur benötigt der Anwender laut Signaturgesetz¹⁵⁰ ein qualifiziertes Zertifikat und eine sichere Signaturerstellungseinheit. In der Praxis werden meist SmartCards als sichere Signaturerstellungseinheit verwendet, die mittels Kartenleser Daten aufnehmen und durch den Einsatz eines implementierten Prozessorchips Berechnungen durchführen können. Der Ablauf einer Signaturerstellung ist abhängig von der eingesetzten Software, die sich in der text- und dateibasierten Arbeitsweise unterscheidet. Bei einem textbasierten Verfahren wird ein Dokument mittels eines Textverarbeitungsprogramms oder eines E-Mail Clients verfasst und anschließend die Signatur anhand der Zeichen des Dokumentes berechnet. Viele Hersteller von textbasierten Signaturprogrammen bieten PlugIns für die weit verbreiteten Kommunikationsprogramme wie z.B. Microsoft Outlook oder Lotus Notes an, die das Signieren direkt aus dem jeweiligen E-Mail Programm ermöglichen.

Dateibasierte Verfahren sind unabhängig vom Format des zu signierenden Dokumentes. Bei dieser Arbeitsweise wird eine Datei ausgewählt und in ein spezielles Signaturformat umgewandelt. Diese signierte Datei ermöglicht eine spätere Verifikation und ein Exportieren des ursprünglichen Dokumentes durch den Empfänger. Bei diesem Vorgang bleibt die signierte Datei unbeschädigt und kann jederzeit erneut auf Integrität und Authentizität geprüft werden.

Eine Signaturerstellung setzt eine vorherige Authentifizierung des Zertifikatsinhabers gegenüber der SmartCard voraus. Dies soll gewährleisten, dass qualifizierte elektronische Signaturen ausschließlich durch die hierfür berechtigte Person erstellt wird. Die Authentifizierung wird mittels Eingabe einer PIN oder durch biometrische Daten (persönliche Merkmale) vollzogen. Derzeit beschäftigt sich die Biometrie mit unterschiedlichen Methoden, wie z.B. Fingerabdruck, Stimmerkennung, Irisscan, Hand- und Gesichtserkennung. Sowohl das PIN-Verfahren als auch der Einsatz biometrischer Daten besitzen Vor- und Nachteile. So können biometrische Merkmale nicht von Unbefugten

¹⁵⁰ Vgl. § 2 Abs. (3) SigG01

verwendet werden und bergen nicht die Gefahr des Vergessens, wie z.B. einer PIN. Ein Nachteil stellt hingegen die Toleranzbreite der eingesetzten Methoden dar. Jedes biometrische Verfahren muss zwischen Original und Fälschung unterscheiden und gewisse Toleranzen akzeptieren. Dies führt zwangsläufig zu einer Fehleranfälligkeit. Ein weiterer Nachteil sind die im Vergleich zum PIN-Verfahren hohen Anschaffungskosten.¹⁵¹

Im Allgemeinen verläuft eine **Signaturerstellung**¹⁵² in folgenden Schritten:

1. Die Signatursoftware wird aufgerufen und das zu signierende Dokument ausgewählt.
2. Es erfolgt eine Aufforderung, die Signaturkarte in den Kartenleser einzulegen. Anschließend wird der Text, auf welchen sich die Signatur bezieht, dem Unterzeichnenden angezeigt und es erfolgt der Hinweis, dass er eine rechtsverbindliche Unterschrift leistet.

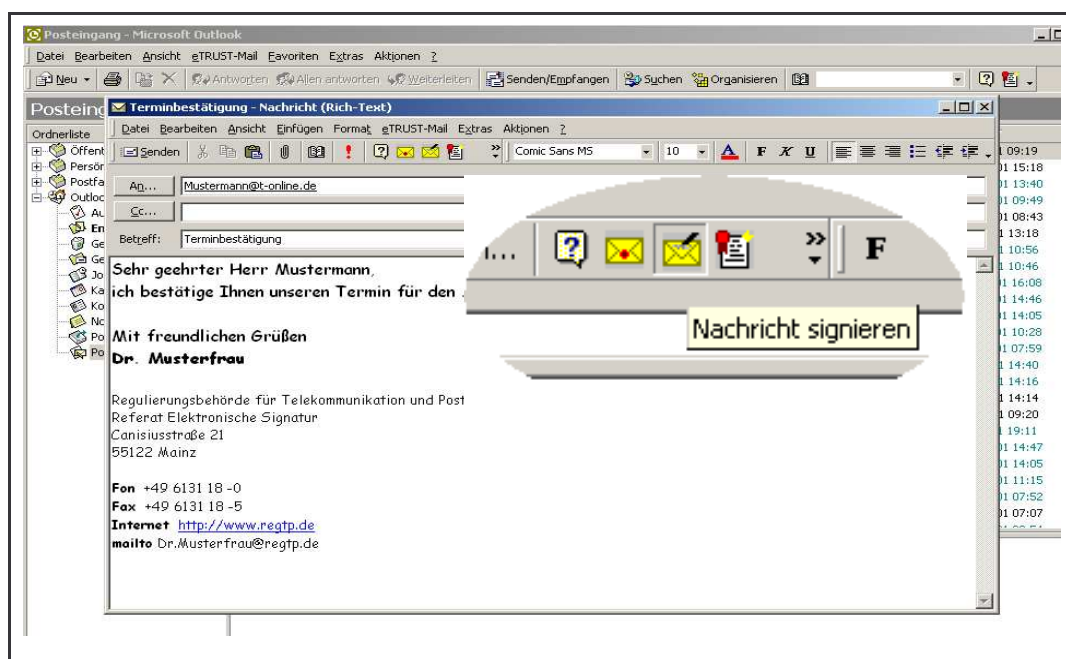


Abbildung 22: Signieren einer Nachricht¹⁵³

3. Der Anwender muss sich als rechtmäßiger Zertifikatsinhaber durch ein geeignetes Verfahren authentifizieren.
4. Nach einer erfolgreichen Authentifizierung wird der Hashwert berechnet und mittels des privaten Schlüssels chiffriert, der auf der SmartCard gespeichert ist.

¹⁵¹ Vgl. HOCHMANN, S. (2001), S. 136

¹⁵² Vgl. Webseite der Signtrust. Online im Internet unter <http://www.signtrust.de>

¹⁵³ Beispiel einer Signaturerstellung mit einem PlugIn für Microsoft Outlook des Zertifizierungsdiensteanbieters Deutsche Post Signtrust.

Das Resultat stellt die qualifizierte elektronische Signatur dar, die an das Programm übermittelt wird.

5. Es wird eine Signaturdatei bestehend aus Dokument, qualifizierter elektronischer Signatur und dem qualifizierten Zertifikat erstellt. Das Zertifikat dient der späteren Verifikation, da es neben dem Namen des Inhabers insbesondere dessen öffentlichen Schlüssel enthält.
6. Abschließend informiert das Programm über den erfolgreichen Signaturvorgang und die Signaturdatei kann übermittelt werden. Optional ist es möglich die Datei zu verschlüsseln und/oder sie mit einem qualifizierten Zeitstempel zu versehen. Die Verschlüsselung wird mit einem Hybridverfahren vollzogen, welches meist aus dem symmetrischen TripleDES Verfahren mit einer Schlüssellänge von 112 Bit und dem asymmetrischen RSA Algorithmus mit einem 1024 Bit Schlüssel besteht.

Die Verifikation einer qualifizierten elektronischen Signatur wird mittels einer geeigneten Prüfsoftware durchgeführt, die von einigen Zertifizierungsdiensteanbietern kostenlos zur Verfügung gestellt wird. Durch diese Vorgehensweise ist garantiert, dass jeder Empfänger einer signierten Nachricht diese verifizieren kann. Es ist dazu nicht erforderlich, dass er die technischen Voraussetzungen für die Erstellung von Signaturen erfüllt.

Die **Prüfung einer Signatur**¹⁵⁴ verläuft im Allgemeinen in folgenden Schritten:

1. Die Prüfsoftware wird aufgerufen und die Signaturdatei ausgewählt. Es findet eine lokale Prüfung auf Basis des angehängten Zertifikates statt. Dazu wird die Signatur mit Hilfe des öffentlichen Schlüssels dechiffriert und der so erhaltene Wert mit dem Hashwert über das ursprüngliche Dokument verglichen. Das Ergebnis, der Prüfungszeitpunkt und die Zertifikatsangaben werden dem Empfänger angezeigt.
2. Das angehängte Zertifikat wird auf Gültigkeit und eventuelle Sperrung zum Ausstellungszeitpunkt geprüft. Dies geschieht durch eine Abfrage bei dem Verzeichnisdienst des ausstellenden Zertifizierungsdiensteanbieters. Abschließend wird die Signatur des Zertifikates anhand des öffentlichen Schlüssels des Zertifizierungsdiensteanbieters verifiziert, um die Zertifikatsangaben zu bestätigen.
3. Im letzten Schritt wird die Zertifikatssignatur des Zertifizierungsdiensteanbieters mittels des öffentlichen Schlüssels der Wurzelinstanz auf Korrektheit geprüft.

¹⁵⁴ Vgl. Webseite der Signtrust. Online im Internet unter <http://www.signtrust.de>



Abbildung 23: Prüfung der Signatur mittels Zertifikat und Prüfsoftware

Sowohl die Erstellung als auch die Verifikation der qualifizierten elektronischen Signaturen verläuft weitgehend automatisiert und ist abgesehen von der graphischen Darstellung, anbieterübergreifend vergleichbar. In der praktischen Anwendung bestehen jedoch weiterhin Unwägbarkeiten. So ist es den Zertifizierungsdiensteanbietern bis zum heutigen Zeitpunkt nicht gelungen, eine Prüfsoftware zu entwickeln, die beliebige qualifizierte elektronische Signaturen verifiziert. Ebenso ist es derzeit nicht möglich eine bestimmte SmartCard mit einer beliebigen Signatursoftware zu nutzen. Für eine einheitliche und interoperable Anwendung elektronischer Signaturen ist es daher unabdingbar, dass Standards erarbeitet werden, die internationale Anerkennung erlangen können.

4.1 Standards und Spezifikationen

Auf internationaler Ebene befasst sich die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) und die Welthandelsorganisation mit diesem Thema.¹⁵⁵ Eine Modellgesetzgebung zum eCommerce, die Regelungen für elektronische Signaturen vorsieht, wurde durch die UN-Kommission für internationales Handelsrecht (UNCITRAL) erarbeitet. 1991 entwickelte Deutschland, Frankreich, die Niederlande und Großbritannien die Information Technology Systems Evaluation Criteria (ITSEC). Diese Kriterien stellen einen Maßstab für die Bewertung der Sicherheit von technischen Komponenten dar und werden durch das Information Security Evaluation Manual (ITSEM) ergänzt. Des Weiteren wurden die Common Criteria for Information Technology Security (ITSCC) von den ITSEC Ländern im Zusammenschluss mit Kanada und den USA erarbeitet. Diese beinhalten Prüfungskriterien der Sicherheit von Informationstechnik und werden als Vorgaben für die Prüfung von Produkten für qualifizierte elektronische Signaturen eingesetzt¹⁵⁶.

Für die Schaffung einer einheitlichen Infrastruktur ist es von zentraler Bedeutung, dass eine Vereinheitlichung folgender Punkte vorangetrieben wird:

- Format und Inhalt eines Schlüsselzertifikats, insbesondere der Attribute und Pseudonyme.
- Verfahren bei Abruf und Sperrung von Zertifikaten.
- Die verwendeten Signaturalgorithmen, insbesondere der Schlüssellängen.
- Verfahren für die Ausstellung von Wurzelzertifikaten für die Zertifizierungsdiensteanbieter.

Im folgenden werden einige Standards, die sich bereits etabliert haben oder eine große Marktakzeptanz besitzen vorgestellt:

1. Die Gültigkeitsabfrage von Zertifikaten wird zunehmend durch das **Open Certificate Status Protocol (OCSP)** realisiert.
2. Bei den asymmetrischen Kryptoalgorithmen hat sich das **RSA Verfahren** mit einer Schlüssellänge von 1024 Bit durchgesetzt.
3. Die Kommunikation zwischen Chipkarte und Anwendung wird durch **Public Key Crypto System (PKCS)** geregelt. Dieser Standard wurde von der amerikanischen Firma RSA Inc. entwickelt.

¹⁵⁵ Vgl. HOCHMANN, S. (2001), S. 69f

¹⁵⁶ Vgl. Anlage 1 SigV01

4. Als Format für Zertifikate konnte sich der ITU (International Telecommunication Union) Standard **X.509** durchsetzen.¹⁵⁷ Gemäß der aktuellen Version muss ein digitales Zertifikat folgende Angaben enthalten:

- Version: Die Versionsnummer des Standards zur Zeit v3.
- Seriennummer: Durch diese Nummer und den Herausgeber ist ein Zertifikat eindeutig bestimmt.
- Signatur: Bezeichnung des Algorithmus, mit dem der Herausgeber das Zertifikat signiert.
- Herausgeber: Der eindeutige Name des Herausgebers.
- Gültigkeit: Der Gültigkeitszeitraum des Zertifikates.
- Inhaber: Der Eindeutige Name des Zertifikatsinhabers.
- Öffentlicher Schlüssel: Den öffentlichen Schlüssel des Inhabers und die Bezeichnung des Algorithmus, mit dem dieser verwendet wird.

Optional kann ein Zertifikat folgende Erweiterungen beinhalten:

- Verwendungszweck: Dieser gibt an, ob ein Schlüsselpaar für das Signieren, Verschlüsseln oder Signieren von Zertifikaten genutzt wird.
- Pfadlänge: Gibt die maximal erlaubte Tiefe einer Zertifizierungshierarchie an.
- CRL Distribution Point: Enthält den Verweis auf die verfügbare Sperrliste.
- Certificate Policies: Gibt die Adresse an, unter welcher die Richtlinien für die Generierung und Verwaltung dieser Zertifikate schriftlich festgehalten sind.

5. Der vorherrschende Standard im Bereich der fortgeschrittenen elektronischen Signaturen wurde von der Software PGP (Pretty Good Privacy) gesetzt und trägt den Namen **OpenPGP**. OpenPGP sieht Zertifikate vor, die mehrere elektronische Signaturen enthalten können. Diese Signaturen werden von Personen erstellt, die die Echtheit des Schlüssels und die Identität des Inhabers bestätigen.¹⁵⁸ Ein Anwender hat folglich die Möglichkeit durch das Signieren seines Zertifikates durch Behörden, Privatpersonen und Unternehmen, das Vertrauen in seine Signaturen zu steigern. Es existieren des Weiteren Zertifikatsfelder, die den

¹⁵⁷ Vgl. Webseite der International Telecommunication Union. Online im Internet unter <http://www.itu.int/home/index.html>

¹⁵⁸ Vgl. GARFINKEL, S. (1996), S. 14

Grad des Vertrauens angeben, welches eine dritte Person oder Stelle dem Zertifikatsinhaber entgegen bringt.

6. Im April 1999 wurde Identrus¹⁵⁹ von acht der weltweit größten Finanzinstitutionen mit dem Ziel gegründet, eine globale Infrastruktur auf Basis einer PKI für den Handel im Unternehmensbereich zu schaffen. Die Identrus-PKI sieht drei Stufen von Zertifizierungsinstanzen vor und ist strikt hierarchisch aufgebaut. Als Wurzelzertifizierungsinstanz agiert ein von Identrus betriebene Zertifizierungsstelle, die in mehreren auf militärischem Niveau gesicherten Datenzentren in Kanada und den Niederlanden angesiedelt ist. Die an Identrus beteiligten Banken betreiben eine Hierarchie-Ebene tiefer Zertifizierungsinstanzen, die digitale Zertifikate für Zertifizierungsinstanzen ihrer Firmenkunden ausstellen. Endanwender sind autorisierte Mitarbeiter der Firmenkunden oder von den Banken direkt zertifizierte Personen.

Um eine uneingeschränkte Interoperabilität verschiedener Signaturanwendungen gewährleisten zu können, ist es notwendig diese nationalen und internationalen Standards zu einer einheitlichen Spezifikation für elektronische Signaturen zu vereinen.

Die erste Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG97 und SigV97 (SigI) wurde 1999 vom BSI¹⁶⁰ entwickelt. Sie richtet sich an die Betreiber von Zertifizierungsstellen und stellt lediglich eine Empfehlung dar. Die **SigI** umfasst unter anderem Abschnitte zu den Themen Zertifikate, Signatur, Anwenderinfrastruktur, Zeitstempel, Verzeichnisdienst, Gültigkeitsmodell, Signierkomponenten, Positivlisten, Normen und Standards.

Aufbauend auf der SigI entwickelte die Arbeitsgemeinschaft der Trustcenter T7 im Jahre 2000 die **Industrial Signature Interoperability Specification (ISIS)** für den Zertifikatsaustausch und der TeleTrust Verein schuf mit **MailTrust (MTT)** eine offene Schnittstelle für den Zugriff von Softwareanwendungen auf die Signaturkarte.

¹⁵⁹ Vgl. Webseite der Identrus Organisation. Online im Internet unter <http://www.identrus.com/>

¹⁶⁰ Vgl. Webseite des BSI. Online im Internet unter <http://www.bsi.de>

4.1.1 ISIS-MTT

Weder ISIS noch MTT hatte eine Markt- oder Normungsrelevanz¹⁶¹. Ein Hauptgrund dafür war die Konkurrerung aufgrund der teilweisen Inkompatibilität der Spezifikationen. Aus diesem Grund beauftragte das Bundeswirtschaftsministerium den TeleTrust Verein im Juli 2001 durch eine Zusammenführung eine einheitliche Interoperabilitätsspezifikation zu erarbeiten¹⁶². Eine erste Fassung von **ISIS-MTT** wurde im Oktober 2001 vorgelegt. Zur Steigerung der Akzeptanz basiert diese weitgehend auf etablierte Standards wie X.509 und PKCS und umfasst die Aspekte Zertifikat- und Nachrichtenformat, PKI Infrastruktur, Sperrlisten, Zugriffsprotokolle und kryptographische Algorithmen. Qualifizierte Signaturen nach dem Signaturgesetz wurden ebenso berücksichtigt, wie die Spezifikation von Sicherheitsfunktionen mit unterschiedlichen Sicherheitsniveaus. Eine Testspezifikation, die alle definierten Schnittstellen enthält, liegt seit April 2002 vor. Herstellern wird somit die Möglichkeit eröffnet, Produkte auf ISIS-MTT Kompatibilität zu prüfen und von einer unabhängigen Prüfstelle abnehmen zu lassen. Durch ISIS-MTT soll die Akzeptanz von Signatur-, Verschlüsselungs- und Authentifizierungsprodukten bei eGovernment und eCommerce, sowie die Investitionsbereitschaft der Anwendungsentwickler erhöht werden. In wieweit sich ISIS-MTT auf nationaler und internationaler Ebene durchsetzen kann, ist zum heutigen Zeitpunkt noch offen. Durch die Beteiligung von Regierung, Zertifizierungsstellen und den über 100 Firmen des TeleTrust eV wird der Spezifikation auf nationaler Ebene ein hohes Markt- und Normierungspotential zukommen.¹⁶³

¹⁶¹ Vgl. SIETMANN, R. (2001)

¹⁶² Vgl. Webseite der ISIS-MTT Organisation. Online im Internet unter <http://www.t7-isis.de/>

¹⁶³ Vgl. REIMER, H. (2002)

5 Anbieter elektronischer Signaturen

5.1 Zertifizierungsdiensteanbieter

Im Bereich der elektronischen Signatur existieren eine Reihe von Unternehmen, die elektronische Signaturen und technische Komponenten vertreiben. Im Folgenden werden Anbieter von qualifizierten und fortgeschrittenen elektronischen Signaturen vorgestellt. Des Weiteren werden Hardwareanbieter und ihre Produkte exemplarisch dargestellt.

Ein Zertifizierungsdiensteanbieter im Sinne des SigG01¹⁶⁴ bietet qualifizierte Zertifikate oder qualifizierte Zeitstempel an. Die RegTP¹⁶⁵ führt stets eine aktuelle Liste aller angezeigten und akkreditierten Anbieter¹⁶⁶.

Das Produktzentrum TeleSec¹⁶⁷ der Deutschen Telekom AG wurde am 22. Dezember 1998 als erste Zertifizierungsstelle genehmigt und bietet Dienstleistungen im Bereich der elektronischen Signatur für Privat- und Geschäftskunden an. Die Produktpalette umfasst neben qualifizierten elektronischen Signaturen auch Servicelösungen im Bereich Einrichtung, Betreuung und Beratung. Einer Zertifikatsvergabe geht das Ausfüllen eines Antragformulars voraus. Dieser Vorgang kann beispielsweise in einem T-Punkt im Beisein eines zertifizierten Mitarbeiters vollzogen werden, der die Identität des Antragstellers anhand des Personalausweises oder Reisepass bestätigt. Das Startpaket umfasst eine personalisierte Chipkarte einschließlich eines Attribut-Zertifikats. Ein Chipkartenleser ist nicht im Lieferumfang enthalten und muss auf dem freien Markt¹⁶⁸ erstanden werden. Die Signatursoftware PKS Crypt und SecuBusiness arbeiten dateibasiert und sind kostenlos als Download auf der Homepage¹⁶⁹ erhältlich. Für die elektronische Signatur wird ein RSA Algorithmus mit einer Schlüssellänge von 1024 Bit und die Hashfunktion RipeMD 160 verwendet, während die Verschlüsselung als Hybridverfahren mit dem asymmetrischen RSA Algorithmus mit 1024 Bit und dem symmetrischen Verschlüsselungsverfahren TripleDES oder IDEA geleistet wird.

¹⁶⁴ Vgl. § 2 SigG01

¹⁶⁵ Nähere Informationen unter <http://www.regtp.de>

¹⁶⁶ Vgl. Anhang A 3 „Liste der angezeigten und akkreditierten Zertifizierungsdiensteanbieter“

¹⁶⁷ Vgl. Webseite der Telesec. Online im Internet unter <http://www.telesec.de>

¹⁶⁸ Vgl. Kapitel 5.3 „Hardwareanbieter“

¹⁶⁹ Nähere Informationen unter <http://www.telesec.de>, Stand April 2003

Leistung	Preis
Personifizierte Chipkarte einschließlich Attribut-Zertifikat	27,35 €
Public Key Service ¹⁷⁰	jährlich ¹⁷¹ 49,83 €
Kartenleser	derzeit nicht im Angebot
Software	kostenlos

Tabelle 9: Preisübersicht der TeleSec¹⁷²

Die Deutsche Post Signtrust¹⁷³ ist seit dem Jahr 2000 ein genehmigter Zertifizierungsdiensteanbieter und bietet Privat- und Geschäftskunden qualifizierte elektronische Zertifikate mit Anbieterakkreditierung. Ein Startpaket umfasst eine personifizierte Signaturkarte, einen Kartenleser und die Signtrust Mail Software als PlugIn für Microsoft Outlook bzw. Lotus Notes. Die Identifizierung wird in einer Postfiliale mit Hilfe des PostIdent Verfahren festgestellt. Dieses zertifizierte Verfahren bestätigt durch Vorlage des Personalausweises oder Reisepass gegenüber Dritten die Identität des Antragstellers. Für die Signaturerstellung und Verschlüsselung werden ebenfalls die Algorithmen RSA 1024 Bit und TripleDes verwendet.

Leistung	Preis
Personifizierte Chipkarte einschließlich Attribut-Zertifikat und Kartenleser	58 €
Public Key Service ¹⁷⁴	jährlich 45,24 €
Software	kostenlos

Tabelle 10: Preisübersicht der Signtrust¹⁷⁵

Einige Zertifizierungsdiensteanbieter haben sich spezialisiert. So bietet **Medizon** Lösungen im elektronischen Gesundheitswesen¹⁷⁶ an. Das Kundenklientel umfasst Krankenhäuser, Ärzte und Firmen aus dem pharmazeutischen Bereich. Die **Bundesnotarkammer** betreibt kein eigenes Trustcenter, sondern nutzt die Kompetenzen von Signtrust. Derzeit richtet sich das Angebot nur an Notare, deren Mitarbeiter und verwandte Berufsgruppen, nicht an Privatanwender. Die **Datev eG** wendet sich mit ihren Produkten vor allem an die Genossenschaft "DATEV eG", zu denen Steuerberater,

¹⁷⁰ Der Public Key Service umfasst sowohl Verzeichnis- als auch Sperrdienst.

¹⁷¹ Preis inklusive Umsatzsteuer.

¹⁷² Vgl. Preisliste der deutschen Telekom AG, Public Key Service. Online im Internet unter <http://www.telekom.de>

¹⁷³ Vgl. Webseite der Deutschen Post Signtrust. Online im Internet unter <http://www.signtrust.de>

¹⁷⁴ Der Public Key Service umfasst sowohl Verzeichnis- als auch Sperrdienst.

¹⁷⁵ Nähere Informationen unter <http://www.signtrust.de>, Stand April 2003

¹⁷⁶ Dieser Bereich wird auch als eHealth bezeichnet.

Rechtsanwälte, Wirtschaftsprüfer, Buchprüfer und deren Mandanten zählen, sowie im Bereich elektronische Signaturen auch an Behörden und Institutionen. Die Steuerberaterkammern nutzen die Datev eG als Zertifizierungsdiensteanbieter und betreiben somit kein eigenständiges Trustcenter.

5.2 Anbieter fortgeschrittener elektronischer Signaturen

Neben den Anbietern von qualifizierten elektronischen Zertifikaten werden von verschiedenen Unternehmen Software für fortgeschrittene elektronische Signaturen meist kostenlos angeboten. Zu den bekanntesten Produkten gehören PGP (Pretty Good Privacy) und PEM (Privacy Enhanced Mail).

PGP wurde bereits 1995 von dem amerikanischen Kryptologen Phillip Zimmermann entwickelt¹⁷⁷ und ist seitdem als Sharewareprogramm weit verbreitet. Die Vorteile von PGP liegen in der einfachen Bedienung dank der grafischen Oberfläche und in der Möglichkeit mittels PlugIns, direkt in den gewohnten Programmen Signaturen zu erstellen und Dokumente zu verschlüsseln. Es gilt als Standard der Kryptographie¹⁷⁸ und ist für Privatpersonen und gemeinnützige Organisationen kostenlos¹⁷⁹. Für Unternehmen beträgt der Preis einer Lizenz ca. 45 €. Die Verschlüsselung wird mit einem Hybridverfahren bestehend aus RSA und IDEA Verfahren realisiert. Die Public Key Infrastruktur basiert auf dem RSA Algorithmus mit MD 5 als Hashfunktion. Der private Schlüssel wird auf dem jeweiligen PC und nicht auf einer SmartCard gespeichert. Dieses Verfahren ist kostengünstig stellt jedoch ein Sicherheitsrisiko dar. So ist es durch fehlende Sicherheitsmechanismen, wie z.B. Virenschutzprogramme möglich mittels trojanischen Pferden¹⁸⁰ Schlüsseldaten auszuspionieren. Zertifizierungsdienste für PGP¹⁸¹ bietet unter anderem der Heise Verlag, der Verein zur Förderung eines Deutschen Forschungsnetzes eV (DFN - Verein) und TC Trustcenter. Ein Anwender generiert sich mit PGP sein Schlüsselpaar und lässt den öffentlichen Schlüssel durch einen Anbieter mit dessen Signatur versehen. Eine persönliche Kontaktaufnahme zwischen Zertifizierungsdiensteanbieter und Antragsteller zur Identifikation ist notwendig.

¹⁷⁷ Vgl. GARFINKEL, S. (1996), S.11

¹⁷⁸ Vgl.: www.Helmhold.de/pgp

¹⁷⁹ Downloadmöglichkeiten gibt es beim "International PGP Home" unter <http://www.pgpi.org/>.

¹⁸⁰ Ein trojanisches Pferd ist ein selbstständiges Programm, welches sich häufig unbemerkt entfaltet und wichtige Daten zerstören oder Informationen an eine fremde Adresse weiterleiten.

¹⁸¹ Vgl. HOCHMANN, S. (2001), S.128

Des Weiteren werden von Unternehmen auch eigene Zertifikate vergeben, so bietet die Web.de AG ein kostenloses Zertifikat für den sicheren E-Mail Versand an. Der Zertifizierungsdiensteanbieter D-Trust vertreibt für unterschiedliche Preise und Anwendungen, wie Secure E-Mail, Secure Web oder E-Commerce eigene Zertifikate¹⁸².

5.3 Hardwareanbieter

Im Bereich der Entwicklung von Hardware sind verschiedene Richtungen erkennbar. So beschäftigen sich verschiedene Unternehmen mit der technischen Umsetzung von Signaturkarten oder Chipkartenlesegeräten. Einige Hersteller arbeiten im Themengebiet der Zeitstempelung oder gehen neue Wege und entwickeln biometrische Systeme, die den Richtlinien der elektronischen Signatur entsprechen.

Signaturkarten, die als Produkte für qualifizierte elektronische Signaturen bereits bestätigt¹⁸³ wurden, werden von folgenden Unternehmen¹⁸⁴ angeboten:

- Datev eG
- Deutsche Post AG Signtrust
- Deutsche Telekom AG
- D-Trust GmbH
- ORGA Kartensysteme GmbH

Bestätigte Chipkartenlesegeräte werden vertrieben¹⁸⁵ von:

- Cherry GmbH
- KOBIL SYSTEMS GmbH
- ORGA Kartensysteme GmbH
- Reiner Kartengeräte GmbH & Co. KG
- SCM Microsystems GmbH

¹⁸² Vgl. Anhang A 3

¹⁸³ Vgl. Liste der erteilten Bestätigungen unter <http://www.tuvt.de>

¹⁸⁴ Stand April 2003

¹⁸⁵ Stand April 2003

Die folgende Tabelle¹⁸⁶ vermittelt einen Eindruck über die Preisstrukturen im Bereich der Chipkartenleser:

Anbieter	Leistung	Preis
Cherry GmbH	Tastatur mit Chipkartenleser	ca. 185 €
KOBIL SYSTEMS GmbH	Chipkartenleser	ca. 145 €
ORGA Kartensysteme GmbH	Chipkartenleser	ca. 200 €
Reiner Kartengeräte GmbH & Co. KG	Chipkartenleser	ca. 100 €
SCM Microsystems GmbH	Chipkartenleser	ca. 80 €

Tabelle 11: Preisliste der Kartenlesegeräte¹⁸⁷

¹⁸⁶ Die Auswahl der angegebenen Produkte ist frei gewählt und besitzt nicht den Anspruch auf Vollständigkeit

¹⁸⁷ Stand Mai 2003

6 Einsatzmöglichkeiten elektronischer Signaturen

Elektronische Signaturen können in allen Bereichen eingesetzt werden, in denen Verbindlichkeit, Integrität und Authentizität eine elementare Rolle spielen. In fast jedem Unternehmen ist es möglich durch digitalisierte Geschäftsabläufe Kosten zu senken, die Effizienz zu steigern und einen schnellen ROI (Return on Investment) zu liefern. Unternehmen aus den unterschiedlichsten Branchen beschäftigen sich mit dem Leistungspotential elektronischer Signaturen. Für den Schutz sensibler Daten und die Digitalisierung von Geschäftsprozessen werden diese bereits im Sozial- und Gesundheitswesen (eHealth), dem Rechts- und Versicherungsbereich, dem Steuerwesen und im Privatbereich angewendet. Im Folgenden werden Pilotprojekte und Praxisbeispiele elektronischer Signaturen aufgezeigt.

6.1 Elektronischer Vertragsabschluss

Der Abschluss von Verträgen im globalen Handel wird immer häufiger auf weite Entfernung mit Personen geschlossen, die nicht näher bekannt sind. Der Versand papierbasierter Verträge ist im Vergleich mit den elektronischen Transportmöglichkeiten via Internet sehr zeitintensiv. Durch einen ständigen Wechsel der Vertragspartner ist es oft nicht möglich, die Echtheit einer handschriftlichen Unterschrift aufgrund fehlender Vergleiche zu prüfen. Eine Lösung bietet der Einsatz elektronischer Signaturen, der die Verbindlichkeit und Authentizität handschriftlich unterschriebener Verträge mit den schnellen und kostengünstigen Versandmöglichkeiten digitaler Dokumente verbindet.

6.2 Elektronische Archivierung

In fast allen Bereichen der Wirtschaft und Verwaltung werden heute Papierbelege zur besseren und schnelleren Bearbeitung mittels Scannereinsatzes digitalisiert. Die Papier-Originalbelege können jedoch nicht vernichtet werden, da im Streitfall ein Nachweis der Originaldaten geführt werden muss. Dies führt zu erheblichen Aufbewahrungskosten. Durch das Signieren mit qualifizierten elektronischen Signaturen und den Einsatz von qualifizierten Zeitstempeln¹⁸⁸ wird der rechtssichere¹⁸⁹ Medienübergang zwischen Papierdokumenten und deren Digitalisierung ermöglicht. Auf diese Weise können auch

¹⁸⁸ Ein Zeitstempel ist eine elektronische Bescheinigung eines Zertifizierungsdiensteanbieters, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben.

¹⁸⁹ Vgl. § 17 SigV01

hochvolumige Papier und Datenbestände schnell und sicher in papierlose Archive überführt werden.

6.3 Elektronische Kommunikation

E-Mail stellt bereits heute die am häufigsten genutzte Internet-Kommunikation dar. Zur Absicherung von elektronischen Nachrichten sollten kryptographische Verfahren eingesetzt werden. Sie schützen die Vertraulichkeit der Nachricht durch Verschlüsselung, sowie deren Integrität und Authentizität durch eine elektronische Signatur. Auf diese Weise können Unternehmen mit Mitarbeitern und Geschäftspartnern auf der ganzen Welt vertrauliche Informationen austauschen.

6.3.1 Das Pilotprojekt SPHINX

Für eine weltweite sichere Kommunikation ist es notwendig, einen E-Mail Standard zu etablieren. Zu diesem Zweck führte das BSI von 1998 bis 2000 in enger Zusammenarbeit mit Herstellern, Zertifizierungsstellen und Anwendern das Pilotprojekt **SPHINX**¹⁹⁰ durch. Es galt Ende-zu-Ende-Sicherheit und elektronische Signaturen nach dem SigG01 auf der Basis internationaler Standards zu realisieren. An diesem Projekt beteiligten sich insgesamt über 80 Behörden und Firmen. Ziel war es,

- die produktübergreifende Interoperabilität der Lösungen verschiedener Anbieter zu erproben,
- die Akzeptanz der Produkte bei den Anwendern zu erfahren und
- die Aufwände für eine Einführung von in SPHINX getesteten Produkten in der öffentlichen Verwaltung zu ermitteln.

Es sollte eine Basis zur breiten Einführung von Produkten geschaffen werden, die konform zum deutschen Signaturgesetz sind. Seit dem Abschluss des Pilotprojektes im Jahr 2000 werden je einmal pro Quartal vom Testlabor der Firma SchlumbergerSema Competence Center Informatik im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik Tests auf Interoperabilität durchgeführt. Die Basis der Tests bildet die „Testspezifikation Client-Produkte: Interoperabilität und Funktionalität“. Das BMI (Bundesinnenministerium) fordert, dass ausschließlich erfolgreich geprüfte Produkte in der Bundesverwaltung eingesetzt werden.

¹⁹⁰ Vgl. Projekt Sphinx. Online im Internet unter <http://www.bsi.de/aufgaben/projekte/sphinx/index.htm>

6.4 Das Home Banking Interface - HBCI

Unter **HBCI**¹⁹¹ (Home Banking Computer Interface) ist ein Standard zu verstehen, der von den deutschen Kreditinstituten gemeinsam erarbeitet und 1997 vom Zentralen Kreditausschuss (ZKA) verabschiedet wurde. Dieser regelt die Kommunikation zwischen Kunden und der entsprechenden Bank, um Homebanking-Transaktionen sicher und benutzerfreundlich abzuwickeln. Im Online Bereich dominiert bis heute das PIN- und TAN-Verfahren. Bei diesem identifiziert sich der Anwender gegenüber dem Bankrechner mit einer persönlichen Identifikationsnummer (PIN) und autorisiert Transaktionen mittels einer einmal gültigen Transaktionsnummer (TAN). Die Nachteile des Verfahrens, wie die aufwendige Pflege der TAN-Listen für die Geldinstitute und die notwendige Geheimhaltung dieser auf der Kundenseite werden durch einen Wechsel zu HBCI Verfahren beseitigt. Der HBCI Standard regelt sowohl die Transportprotokolle und Zeichensätze als auch die Datendarstellung, welche eine Trennzeichensyntax verwendet, die an das komplexe UN/EDIFACT¹⁹² angelehnt ist.

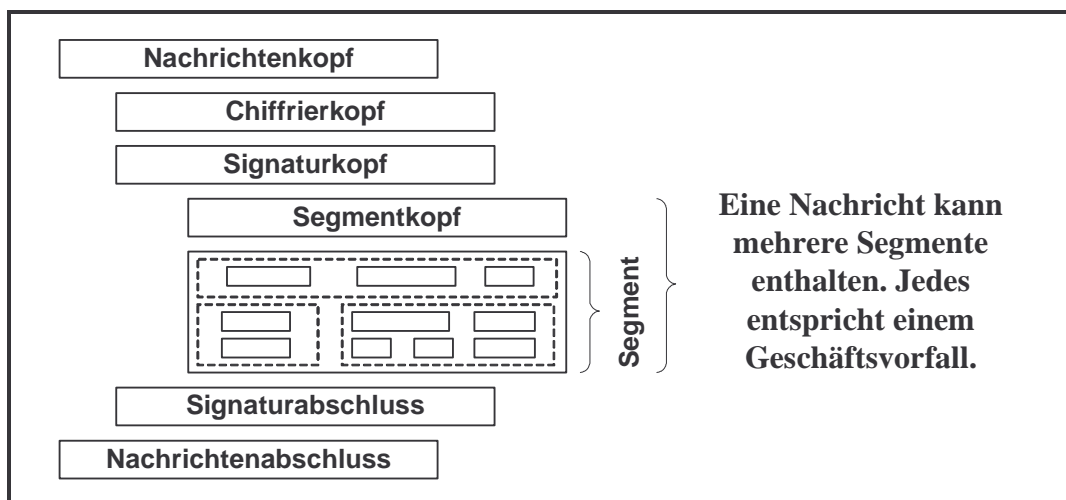


Abbildung 24: Der Aufbau einer HBCI-Nachricht¹⁹³

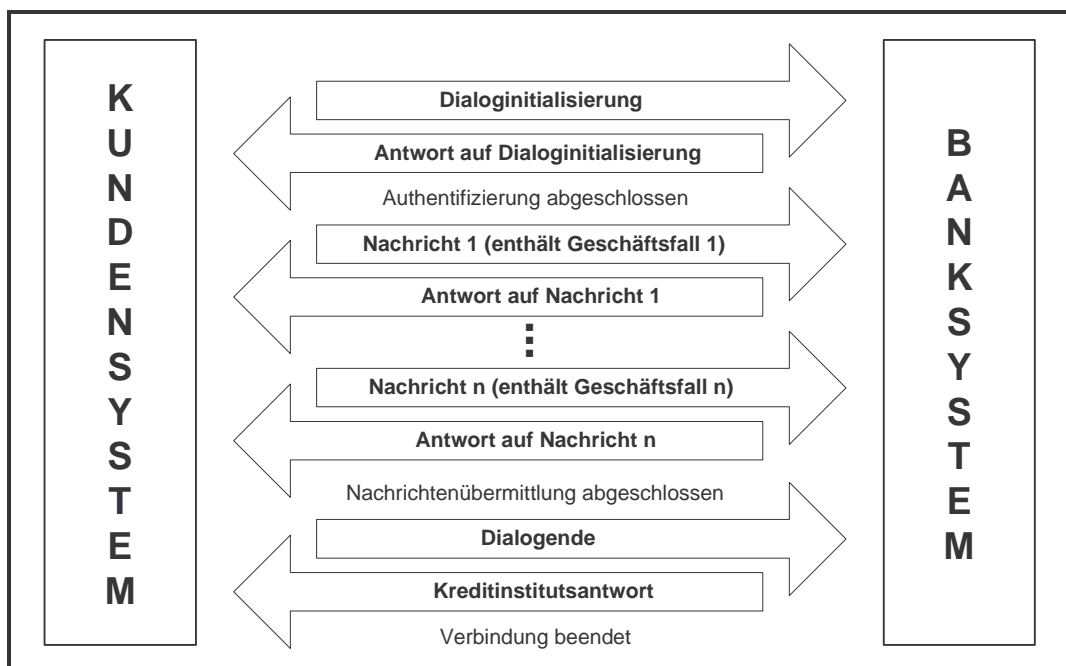
Der Segmentkopf gibt die Art des Geschäftsvorfalles an, während der Chiffrierkopf zur Verschlüsselung der Daten benötigt wird. Im Signaturkopf sind Informationen über das anzuwendende Sicherheitsverfahren gespeichert. Die elektronische Unterschrift ist im Signaturabschluss enthalten.

Die Nachrichten werden über den HBCI Dialog gesendet, der die Kommunikation zwischen Kunden- und Banksystem festlegt.

¹⁹¹ Vgl.: <http://www.hbci.de>

¹⁹² Vgl. Erkel, S. (2003), Kapitel 7.3 „Die EDIFACT-Nachricht“

¹⁹³ Vgl. WINDISCH, D. (2002), S. 13

Abbildung 25: Der HBCI - Dialog¹⁹⁴

Jede Nachricht wird mit dem TripleDES Algorithmus symmetrisch verschlüsselt und zur Sicherstellung der Datenintegrität und Authentifizierung vom Kunden elektronisch signiert. Die Signatur wird mit der Hashfunktion RipeMD oder SHA-1 und dem RSA Algorithmus als Signaturverfahren erzeugt.

HBCI Produkte¹⁹⁵ werden mittlerweile von über 2.000 Banken vertrieben. Das Startpaket umfasst ein Software Programm, welches einen Online und Offline Betrieb erlaubt. Der Signaturschlüssel ist entweder auf einer Diskette oder einer SmartCard gespeichert. Ein Kartenleser¹⁹⁶ ist meist nicht im Lieferumfang enthalten.

Anwendungsbereiche von HBCI Verfahren im inländischen Zahlungsverkehr sind

- Erstellung von Einzel- und Sammelaufträgen
- Abruf von Kontoumsätzen
- Wertpapiergeschäfte
- Depotverwaltung

sowie im ausländischen Zahlungsverkehr

- Zahlungsaufträge
- Anzeige von Kartendaten
- Online Sperrung von Bankkarten

¹⁹⁴ Vgl. WINDISCH, D. (2002), S. 13

¹⁹⁵ Eine Liste von HBCI Produkten befindet sich online im Internet unter <http://www.hbci.de>.

¹⁹⁶ HBCI fähige Kartenleser sind auf dem freien Markt für ca. 50 Euro erhältlich. Vgl. auch Kapitel 5.3 „Hardwareanbieter“

- Devisenanzeige
- Bestellung von Sorten und Reisechecks

Das Thema Homebanking gewinnt zunehmend an Bedeutung, da es dem Anwender einen flexiblen zeitunabhängigen Zugriff auf Geld- und Wertanlagen bietet. Im Bankwesen ist ein Trend zu kartenbasierten Lösungen unter der Verwendung elektronischer Signaturen erkennbar.

6.5 eGovernment

Electronic Government (eGovernment) bezeichnet die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien.¹⁹⁷

Die Bundesregierung hat die Bedeutung und Möglichkeiten elektronischer Medien für den Bürger und die Wirtschaft bereits frühzeitig erkannt. So startete Bundeskanzler Gerhard Schröder im Sommer 2000 die Initiative¹⁹⁸ Bund Online 2005. Mit ihr hat sich die Bundesregierung verpflichtet, die etwa 400 internetfähigen Dienstleistungen der Bundesverwaltung bis zum Jahr 2005 online bereit zu stellen. Ziel ist es, durch den Einsatz moderner Kommunikationsmittel die Bearbeitung zu beschleunigen, einen zentralen Beitrag zur Verwaltungsmodernisierung zu leisten und die Dienstleistungen des Bundes für Bürger und Unternehmen kostengünstiger, schneller und einfacher anbieten zu können. Für die Umsetzung dieses Vorhabens ist ein Gesamtfinanzbedarf von 1,4 Mrd. Euro im Zeitraum 2002 bis 2005 eingeplant. Die Regierung kalkuliert ab 2006 mit jährlichen Einsparungen von 400 Mio. Euro¹⁹⁹. Die Einsatzmöglichkeiten von elektronischen Signaturen im eGovernment sind vielfältig:

- Die Beantragung von staatlichen Leistungen, wie BAföG, Rente, Arbeitslosen- oder Kindergeld,
- Verlängerung von Dokumenten, wie Reisepass oder Personalausweis,
- An- und Ummeldungen von Kfz oder Wohnsitzen,
- Stellen von Bauanträgen,
- Eheschließungen,
- Wahlen oder Volksabstimmungen

¹⁹⁷ Vgl. REINERMANN, H. (2002), S. 1

¹⁹⁸ Vgl. Bund Online 2005. Online im Internet unter <http://www.bundonline2005.de>

¹⁹⁹ Vgl. „Projekt Bund Online 2005 wird fortgesetzt“ (2003). Online im Internet unter <http://www.golem.de>

sind typische Kommunikationsvorgänge zwischen Bürgern und Behörden bei denen Unterschriften benötigt werden. Der Einsatz elektronischer Signaturen in diesen Bereichen bietet Vorteile für Bürger und Regierung. Durch die Digitalisierung der Daten und die schnellen Versandwege werden Bearbeitungszeiten verkürzt. Anwender können Behördengänge vom heimischen PC aus rund um die Uhr erledigen.

Zu den bereits realisierten Online Dienstleistungen²⁰⁰ gehören unter anderem:

1. Vergabe von öffentlichen Aufträgen

Diese Dienstleistung deckt die elektronische Vergabe von Aufträgen der Bundesverwaltung ab. Es erfolgt die vollständige, rechtsverbindliche und medienbruchfreie Kommunikation zwischen der Vergabestelle und den potenziellen Bietern. Diese erstreckt sich von der Bekanntmachung über die elektronische Angebotsabgabe bis hin zur Zuschlagserteilung über die Vergabepattform unter Verwendung des pdf-Formats sowie der gesetzeskonformen elektronischen Signatur. Nutzer des Systems sind die Bieter (Unternehmen), Vergabestellen des Bundes, der Länder und Kommunen.

2. Dienstleistung „eService“ der Bundesversicherungsanstalt für Angestellte (BfA)

Neben einem umfangreichen Informationsangebot zu ihren Aufgaben und Leistungen bietet die BfA seit der CeBIT im März 2002 Inhabern einer sicheren Signaturchipkarte den „eService“ an. Dieser Service bietet den Versicherten zunächst die Möglichkeit, ihren persönlichen Versicherungsverlauf, eine Auskunft über die bisher erreichte Rentenhöhe sowie eine Prognoseberechnung über die zukünftige Altersrente online abzurufen. Die Auskunft erscheint dann nach wenigen Sekunden als pdf-Datei am Bildschirm.

6.5.1 Die elektronische Steuererklärung - ELSTER

Ein weiteres Einsatzgebiet elektronischer Signaturen im eGovernment ist die elektronische Steuererklärung²⁰¹ (ELSTER). Diese ist Teil des Aktionsprogramms „Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts“ und der Förderung des eGovernment durch die Bundesregierung²⁰². Sie bietet den Bürgerinnen und Bürgern die Möglichkeit, ihre Steuererklärung am heimischen PC zu bearbeiten. Die

²⁰⁰ Vgl. Umsetzungsplan 2002. Online im Internet unter <http://www.bund.de/BundOnline-2005/Umsetzungsplan-.7193.htm>

²⁰¹ Vgl. Webseite Elster. Online im Internet unter <http://www.elster.de>

²⁰² Vgl. Monatsbericht des BMF April 2003

Datensicherheit auf dem Kommunikationsweg zwischen Bürger und Finanzbehörde wird durch den Einsatz eines Verschlüsselungsverfahrens gewährleistet. Es handelt sich hierbei um ein Hybridverfahren unter Verwendung von TripleDES 112 Bit und RSA 2048 Bit. Von den Finanzbehörden wird ELSTER als Standard für die Übertragung elektronischer Steuererklärungen genutzt und steht den Bürgern seit dem Jahr 2000 kostenlos²⁰³ zur Verfügung. Durch integrierte Plausibilitätsprüfungen wird die Konsistenz der Daten gewährleistet und folglich die Erstellung einer Steuererklärung erleichtert. Die Benutzerfreundlichkeit und der Funktionsumfang wird mit jedem Release verbessert. So ist es seit März 2002 möglich, eine Steuererklärung mit einer elektronischen Signatur zu versehen. Im Rahmen eines Pilotprojektes wird seit Juni 2002 die Einführung elektronischer Signaturen in den Ländern Bayern, Niedersachsen, Nordrhein-Westfalen, Saarland, Sachsen und Sachsen-Anhalt erprobt. Es werden derzeit die Signaturkarten²⁰⁴ der TeleSec, der Signtrust, der Deutschen Bank, der Hypovereinsbank und der Steuerberaterorganisation DATEV e.G. unterstützt. Durch den Einsatz elektronischer Signaturen ist die papierlose Abgabe einer Steuererklärung ohne Medienbruch realisierbar.

Die Finanzverwaltung verzeichnet einen stetigen Anstieg der ELSTER-Anwender, wie folgende Tabelle belegt. Die aktuelle Version²⁰⁵ wurde seit 1. Januar 2003 bereits 172.164 mal heruntergeladen.

Jahr	Anzahl der abgegebenen elektronischen Steuererklärungen
1999	25.000
2000	145.000
2001	322.000
2002	über 500.000

Tabelle 12: Anzahl der abgegebenen elektronischen Steuererklärungen²⁰⁶

Der Gesetzgeber regelt den rechtlichen Rahmen der Abgabe für die elektronische Übermittlung von Steuerdaten durch die „Verordnung zur elektronischen Übermittlung von Steuererklärungen²⁰⁷ und sonstigen für das Besteuerungsverfahren erforderlichen Daten“. Diese Verordnung wurde am 28. Januar 2003 novelliert. Danach gelten für die

²⁰³ Downloadmöglichkeit auf der Elster Webseite unter <http://www.elsterformular.de>

²⁰⁴ Vgl. Webseite ELSTER. Online im Internet unter <http://www.elster.de>

²⁰⁵ Elsterformular 2002

²⁰⁶ Vgl. Monatsbericht des BMF April 2003

²⁰⁷ Vgl. BGGI (2003)

elektronische Signatur im Steuerrecht erleichterte Anforderungen. Gemäß § 7 dieser Verordnung werden fortgeschrittene elektronische Signaturen von den Finanzbehörden akzeptiert, die

- mit einer Signaturerstellungseinheit erzeugt werden, welche die wesentlichen Anforderungen an eine sichere Signaturerstellungseinheit erfüllt, und
- auf einem zum Zeitpunkt ihrer Erzeugung gültigen Zertifikat beruhen, das den wesentlichen Anforderungen an ein qualifiziertes Zertifikat entspricht.

Der Ablauf einer elektronischen Steuererklärung ohne den Einsatz elektronischer Signaturen stellt sich im Allgemeinen wie folgt dar:

1. Der Anwender füllt das ELSTER Formular am heimischen PC aus.
2. Die elektronischen Steuerdaten werden verschlüsselt und an die Finanzbehörde übermittelt.
3. Zum Zwecke des rechtsgültigen Unterschreibens müssen die Steuerdaten auf ein behördliches Steuerformular ausgedruckt werden.
4. Die papierbasierten Steuerdaten müssen kuvertiert und auf dem Postweg an die Finanzbehörde übermittelt werden.
5. Die Finanzbehörde bearbeitet die papierbasierten und elektronischen Daten des Steuerpflichtigen.
6. Die Steuerbenachrichtigung wird auf dem Postweg von der Finanzbehörde an den Steuerpflichtigen gesendet.

Der Ablauf einer elektronischen Steuererklärung mit elektronischer Signaturen verläuft im Allgemeinen wie folgt:

1. Der Anwender füllt das ELSTER Formular am heimischen PC aus.
2. Die elektronischen Steuerdaten werden verschlüsselt, signiert und an die Finanzbehörde übermittelt.
3. Die Finanzbehörde bearbeitet die elektronischen Daten des Steuerpflichtigen.
4. Die Steuerbenachrichtigung wird von der Finanzbehörde per E-Mail an den Steuerpflichtigen gesendet.

Es ist aus steuerrechtlichen Gründen notwendig, die Daten handschriftlich zu unterschreiben. Diese Vorschrift macht ein Ausdrucken und Versenden auf dem herkömmlichen Postweg erforderlich. Durch den Einsatz elektronischer Signaturen können effizient Kosten eingespart werden. Auf der staatlichen Seite wird dies verwirklicht durch den Wegfall der Verwaltung papierbasierter Formulare und einen beschleunigten Bear-

beitungsvorgang. Auf der Anwenderseite lassen sich Kosten senken durch das Ausbleiben von Druck- und Versandkosten.

6.6 Die mobile elektronische Signatur

Dem Geschäftsfeld des M-Business wird ein starkes Wachstumspotential vorausgesagt. Prognosen gehen davon aus, dass das Transaktionsvolumen über elektronische Netze mittels mobiler Endgeräte wie Handy und PDA (Personal Digital Assistant) bereits in naher Zukunft den Bereich des klassischen E-Commerce überbieten wird.²⁰⁸ Die breite Marktakzeptanz, die Anzahl der Nutzer mobiler Geräte²⁰⁹, sowie die mannigfachen Funktionalitäten sprechen ebenfalls für diese Prognose. Seit Einzug des WAP (Wireless application protocol) in die GSM-Telefone²¹⁰ ist der Zugang zu Informationen und Dienstleistungen des Internets Stand der Technik. Beispielsweise ist das Abfragen von Aktienkursen mittels dieses Dienstes möglich. Der Bereich des M-Brokerage ist jedoch ungleich interessanter, wenn nicht nur das Abfragen, sondern ebenso der Handel über das Handy abgewickelt werden kann. Die Akzeptanz des M-Commerce ist mit der Gewährleistung der Sicherheit kommerzieller Transaktionen eng verbunden. Neben den hohen Anschaffungskosten, den niedrigen Übertragungsraten stehen die Sicherheitsbedenken als Hauptgrund für die schleppende Durchsetzung des M-Commerce. Der Einsatz elektronischer Signaturen in mobilen Endgeräten ist prädestiniert für die Gewährleistung der Datenintegrität und Authentizität. Eine unbedingte Voraussetzung eines breiten Einsatzes ist ein allgemein akzeptierter Standard im mobilen Internet.

Im Jahr 2000 sind die Standardisierungsaktivitäten auf dem Gebiet der mobilen elektronischen Signatur vorangetrieben worden.

6.6.1 Das Pilotprojekt mSign

Das **mSign** Konsortium²¹¹ besteht aus über 50 Unternehmen der Internet-Branche und des mobilen Telekommunikationssektors. Zu den Gründungsmitgliedern gehören Siemens, Deutsche Telekom, E-Plus Mobilfunk, D2-Vodafone, T-Mobil und O2. Initiiert wurde es von der Brokat AG mit dem Ziel der Standardisierung betriebswirtschaftlicher Abläufe und technischer Einsätze mobiler Signaturen. GSM-Telefone besitzen eine SIM-Karte (Subscriber Identification Module), welche benutzerbezogene Daten und

²⁰⁸ Vgl. Funkschau (2001)

²⁰⁹ Seit Dezember 2000 liegt die Anzahl mobiler Telefone in Deutschland mit 50 Mio. über der Zahl der Festnetztelefone.

²¹⁰ Telefone basierend auf dem technischen Standard GSM (Global System of Mobil Communication)

Informationen ausgeben und speichern kann. Diese Karten basieren auf speziellen Chipkarten (Smart Card), die ähnlich den Signaturkarten operieren. Der mSign Ansatz sieht die Erweiterung der SIM-Karte um eine Signaturfunktion vor. Dieser Lösungsansatz nutzt die GSM-Infrastruktur, die einheitlichen Übertragungsstandards und kommt andererseits ohne zusätzliche Kartenleser und externe Signaturkomponenten aus. Dabei übernimmt der Netzbetreiber gegenüber den Anbietern und Kunden im M-Commerce die Rolle des Transaktions- und Paymentproviders, der sichere Verfahren für Bezahl- und Signiervorgänge anbietet. Ein Protokoll zur Spezifikation der Schnittstelle zwischen Mobilfunkbetreiber und den Diensteanbietern wurde im Jahr 2000 veröffentlicht. mSign sieht im Micro-Payment die Autorisierung von Bezahlvorgängen mittels PIN oder Passwort vor, welche durch SMS oder Spracheingabe übermittelt wird. Kryptographische Verfahren bleiben dem Bereich des Macro-Payment vorbehalten. Denkbar in diesem Bereich ist eine Abstufung der Sicherheit durch die verwendeten Signaturverfahren und die Art der Signaturerstellung, die entweder nicht unmittelbar oder direkt auf der SIM-Signaturkarte erzeugt werden. Die letzte Variante erlangt die höchste Sicherheitsstufe und ist signaturgesetzkonform. Der Vorteil der Verschmelzung von SIM-Karte und Signaturkarte liegt eindeutig auf der Anwenderseite, da es nicht nötig ist weitere Geräte an das Mobilfunktelefon anzuschließen. Dies führt zu einer einfachen und flexiblen Handhabung.

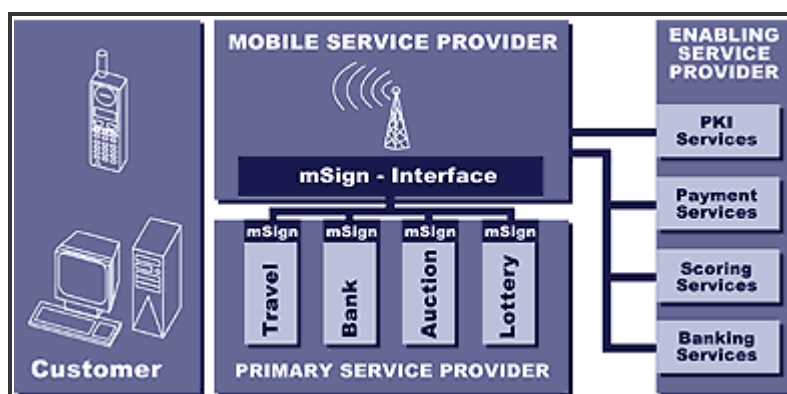


Abbildung 26: Aufbau des Projektes mSign²¹²

Durch den Eingriff in mehrere Standards ist jedoch das Investment zur Entwicklung ungleich höher als bei einer Variante mit separatem Kartenleser²¹³. Die SIM-Karte muss den Erfordernissen der elektronischen Signatur angepasst werden. Des Weiteren bedarf

²¹¹ Vgl. Webseite des Projekt mSign. Online im Internet unter <http://www.msign.de>

²¹² Vgl. Webseite des Projekt mSign. Online im Internet unter <http://www.msign.de>

es einer Veränderung der Infrastruktur zur technischen Personalisierung, um eine signaturgesetzkonforme Registrierung und Identifizierung zu ermöglichen. Auf der organisatorischen Seite müssen Regelungen getroffen werden zwischen Anwender auf der einen Seite und Mobilfunknetzbetreiber und Signaturanbieter auf der anderen.

6.6.2 Das Pilotprojekt MoSign

Das Projekt **MoSign**²¹⁴ verfolgt die Variante Mobiltelefon mit separatem Kartenleser und Signaturkarte. Die modernen SIM-Karten Geräte sind in der Lage Daten zu empfangen, zu speichern, anzuzeigen, zu verändern und zu senden. Wichtige Eigenschaften, die bei einem internetfähigen PC vorausgesetzt und zum Erstellen oder Prüfen von Signaturen benötigt werden. MoSign setzt somit auf bereits etablierte PKI-Standards und verwendet eine universell einsetzbare, endgeräteunabhängige SmartCard mit Zertifikaten, die den Anforderungen von Identrus²¹⁵ entsprechen. Dem Konsortium MoSign gehören neben Emagine, Ericsson, Materna, Microsoft, SemaGroup, Siemens und TC Trustcenter auch die vier deutschen Privatbanken Commerzbank, Deutsche Bank, Dresdner Bank und Hypo Vereinsbank an. Ziel ist nicht die Entwicklung neuer Standards, sondern das Sammeln konkreter Erfahrungen bei der Umsetzung bestehender Standards. Herzstück für sichere Onlinetransaktionen bildet eine personengebundene Chipkarte des akkreditierten Zertifizierungsdiensteanbieters TC Trustcenter. Mit dieser kann der Karteninhaber elektronische Unterschriften erzeugen und mobile sichere Transaktionen durchführen. Die Prüfung der Zertifikate sowie die Berechtigung der Transaktion wird durch den Legitimation Server von Emagine geleistet. Anstelle reiner Signaturkarten sieht das Konsortium auch die millionenfach eingesetzten EC-Karten²¹⁶ vor, deren Geldkarten-Chip um eine Signaturfunktionalität erweitert werden muss. Aus diesem Grund wird auch das MoSign Projekt mit dem Begriff „**Banken-Signaturkarte**“ charakterisiert. Ziel der Banken-Signaturkarte ist die Bindung des Zertifikatsinhabers an das Geldinstitut und der Einsatz bei dem etablierten Online Banking, der zu einem Verzicht der organisatorischen Pflege von TAN-Listen (Transaktionsnummer) führen kann. Die Substitution des PIN und TAN Verfahrens durch die Signaturkarte bietet dem Geldinstitut ein Einsparpotential und dem Kunden eine höhere Sicherheit und einfache Handhabung.

²¹³ Vgl. TÜViT Arbeitspapier (2001), S. 2

²¹⁴ Vgl. Webseite des Projekt MoSign. Online im Internet unter <http://www.mosign.de>

²¹⁵ Vgl. Kapitel 4.1 „Standards und Spezifikationen“

6.6.3 Die Initiative Radicchio

Eine weitere Organisation im Bereich M-Business ist **Radicchio**²¹⁷. Bestehend aus über 50 Unternehmen des M-Commerce und der Sicherheitsindustrie handelt es sich nicht um ein Standardisierungsforum. Radicchio hat zum Ziel, industrieübergreifende Plattformen für vertrauenswürdige Transaktionen zu schaffen. Verfahren der Registrierung, Zertifizierung und Interoperabilität werden geklärt und einer breiten Öffentlichkeit zugänglich gemacht. Die Guidelines for Secure M-Commerce (radicchio guide) empfiehlt den Aufbau auf nationalen Signaturgesetzen, unter Beachtung der EU-Richtlinie²¹⁸ über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. Als Signaturalgorithmen werden der RSA Algorithmus mit einer Schlüssellänge von 1024 Bit, sowie der ECC mit einem 163 Bit Schlüssel empfohlen.

6.6.4 Die Initiative Mobile electronic Transaction - MeT

In der **Mobile electronic Transaction**²¹⁹ Initiative (**MeT**) haben sich seit April 2000 die Hersteller von Mobilfunk-Endgeräten Ericsson, Motorola, Nokia, Panasonic und Siemens zusammengeschlossen. Ziel ist es hersteller- und endgeräteübergreifende Lösungen für Signatur- und Zahlungsvorgänge zu definieren. Des Weiteren verfolgt die Initiative eine möglichst einfache und unabhängig von den Gerätetypen einheitliche Oberflächen und Anwendungen mit universeller Operabilität. Dabei werden keine speziellen Paymentverfahren favorisiert und ein zusätzlicher Installationsaufwand für den Benutzer vermieden. MeT hat sich zur Aufgabe gemacht, einen verbindlichen Rahmen für die Entwicklung von M-Commerce Anwendungen aufzustellen. Richtlinien sollen vorgeben, wie mobile elektronische Transaktionen unter Verwendung der durch MeT initiierten Standards vom Mobilgerät auszuführen sind.

²¹⁶ In Deutschland existieren ca. 50 Mio ec-Karten.

²¹⁷ Vgl. Webseite des Projekt Radicchio. Online im Internet unter <http://www.radicchio.org>

²¹⁸ Vgl. Kapitel 2.2.1 „Die EU-Richtlinie 1999/93/E“

²¹⁹ Vgl. Webseite des Projekt MET. Online im Internet unter <http://www.mobiletransaction.org>

6.7 Die elektronische Rechnung

Ein interessantes und lukratives Einsatzgebiet elektronischer Signaturen ist die elektronische Rechnungsstellung (eBilling). Diese Anwendung kann in die zwei Ausprägungen Web- und E-Mail-Billing eingeteilt werden.

Beim Web-Billing stellen Unternehmen digitale Rechnungen auf einer Webseite bereit und bieten ihren Kunden die Möglichkeit die Rechnungsdaten abzurufen.

Das E-Mail-Billing wird im Folgenden kurz dargestellt und auf den Einsatz elektronischer Signaturen untersucht. Seit längerem setzen viele Unternehmen E-Mails zur Rechnungsstellung ein. Diese hatten jedoch nur informativen Charakter, da für einen Vorsteuerabzug eine Rechnung in Schriftform vorzulegen war. Mit Inkrafttreten des Umsatzsteueränderungsgesetzes²²⁰ ist es seit dem 1. Januar 2002 möglich, dass elektronische Rechnungen für den Vorsteuerabzug anerkannt werden, sofern sie die allgemeinen Anforderungen an eine Rechnung erfüllen und außerdem mit einer qualifizierten elektronischen Signatur mit Anbieterakkreditierung versehen sind. Unternehmen haben somit die Möglichkeit eine durchgängig medienbruchfreie elektronische Rechnungsstellung aufzubauen. Dies führt zu einem Einsparpotential sowohl auf Seiten des Rechnungsstellers als auch bei einem Rechnungsempfänger.

Kostenvergleich: Rechnungsübermittlung durch Rechnungssteller		
Durchschnitt pro Rechnung	Papierrechnung	E-Mail-Billing
Zeitbedarf (in Minuten)	11	8
Kalkulatorischer Stundensatz ²²¹	30,00 €	30,00 €
Bearbeitungskosten (= Bearbeitungszeit /60 * Stundensatz)	5,50 €	4,00 €
Sachkosten	1,55 €	0,30 €
Gesamtkosten (= Bearbeitungskosten + Sachkosten)	7,05 €	4,30 €
Kosteneinsparung	-	2,75 €

Tabelle 13: Kostenvergleich Rechnungsübermittlung²²²

²²⁰ Vgl. Kapitel 2.5.4 „Umsatzsteuergesetz“

²²¹ Ausgerichtet an dem durchschnittlichen Stundensatz einer Sekretärin. Vgl. Fiebich & PartnerInnen Steuerberatungskanzlei. Online im Internet unter http://www.fiebich.com/fiebich_folder.pdf

²²² Vgl. ERKEL, S. (2003), Kapitel 10.2.4 „Kostenvergleich IST/SOLL-Modell“

Kostenvergleich: Rechnungsbearbeitung durch Rechnungsempfänger		
Durchschnitt pro Rechnung	Papierrechnung	E-Mail-Billing
Zeitbedarf (in min)	24	9
kalkulatorischer Stundensatz	30,00 €	30,00 €
Bearbeitungskosten	12,00 €	4,50 €
Gesamtkosten	12,00 €	4,50 €
Kosteneinsparung	-	7,50 €

Tabelle 14: Kostenvergleich Rechnungsbearbeitung²²³

Die Aufstellung zeigt ein Einsparpotential durch den Einsatz von E-Mail-Billing auf Seiten des Rechnungssteller von 30% gegenüber einer Papierrechnung. Dies ist zum Großteil auf den Wegfall von Druck-, Kuvertierungs- und Portokosten zurückzuführen. Die Kosteneinsparung von 60% auf Seiten des Rechnungsempfängers wird vor allem durch die stark verkürzte Bearbeitungszeit erreicht, die hauptsächlich aus der automatisierten Datenerfassung resultiert.

Auf Seiten des Rechnungsstellers sind durch den Versand per E-Mail-Billing folgende Vorteile²²⁴ zu erkennen:

- Einsparungen durch den Wegfall von Druck-, Kuvertierungs- und Portokosten.
- Kostenreduktion durch verkürzte Bearbeitungszeit.
- Rechnungsdaten lassen sich durch den Wegfall der Postlaufzeit zeitnah übertragen. Dies führt zu einem beschleunigten Rechnungsversand, so dass die geforderten Zahlungen früher ausgelöst werden und Zinsgewinne erzielen können.
- Durch eine automatisch erzeugte E-Mail, die als Empfangsbestätigung fungiert, wird die Nachweisbarkeit der Zustellung günstig und komfortabel vollzogen.
- Die Anwendung von Verschlüsselungsverfahren führt zu einem effektiven Datenschutz.
- Die Marketingfunktion der Rechnung kann kostengünstig und kundenfreundlich gestaltet werden. Dies kann beispielsweise durch das Anhängen von Werbeinformationen realisiert werden.

²²³ Vgl. ERKEL, S. (2003), Kapitel 10.4 „Kostenvergleich IST/SOLL-Modell“

²²⁴ Vgl. ERKEL, S. (2003), Kapitel 10.3 „Ergebnis der Optimierung“

Auf Seiten des Rechnungsempfängers werden folgende Vorteile²²⁵ erzielt:

- Rechnungsdaten können firmenintern ohne Zeitverlust weitergeleitet werden.
- Eventuell auftretende Klärungsfälle können zeitnah per E-Mail ablaufen.
- Die Rechnungsdaten können ohne Medienbruch in das hauseigene EDV-System übernommen werden. Dadurch lassen sich Fehler vermeiden und die Bearbeitungszeit verkürzen, so dass Bearbeitungskosten erheblich gesenkt werden können.
- Die beschleunigte Rechnungsübertragung und –bearbeitung erleichtert das Einhalten von Skontofristen.
- Die Rechnung kann unmittelbar zu einem Vorsteuerabzug gegenüber den Finanzbehörden geltend gemacht werden. Dadurch wird der Vorsteuergewinn beschleunigt.
- Durch eine direkte elektronische Archivierung der Rechnung entfallen aufwändige Scan-Verfahren, um Daten auf Papier in eine elektronische Form zu überführen. Des Weiteren werden die Aufbewahrungskosten durch die Archivierung auf kleinerem Raum gesenkt. Vor allem in Unternehmen mit einem hohen Rechnungsvolumen stellt dies aufgrund der langen Aufbewahrungsfrist von 10 Jahren einen bedeutenden Vorteil dar.

Der Rechnungsempfänger kann die Vorteile der elektronischen Rechnungsstellung ohne eigenen finanziellen Aufwand nutzen. Auf diese Weise wird die Bindung zu dem rechnungsstellenden Unternehmen gestärkt und die Kundenzufriedenheit gesteigert. Die geschaffene Rechtssicherheit sorgt für einen Investitionsschutz für Unternehmen und ermöglicht einen effektiven ROI.

Die Umstellung vom papierbasierten Rechnungsaustausch auf einen elektronischen Rechnungsprozess unter Verwendung qualifizierter elektronischer Signaturen mit Anbieterakkreditierung eröffnet Unternehmen ein hohes Einsparpotential. Vor dem Hintergrund der angespannten wirtschaftlichen Lage und dem steigenden Kosten- und Konkurrenzdruck führen innerbetriebliche Kostensenkungen zu einer nachhaltigen Steigerung des Gewinns und der Wettbewerbsfähigkeit eines Unternehmens.²²⁶

²²⁵ Vgl. ERKEL, S. (2003), Kapitel 10.3 „Ergebnis der Optimierung“

²²⁶ Nähere Informationen siehe ERKEL, S. (2003)

7 Schlussbetrachtung

Das Ziel der vorliegenden Diplomarbeit war es, die gesetzlichen Rahmenbedingungen der elektronischen Signatur zu erörtern, die mathematischen Grundlagen aufzuzeigen und Einsatzmöglichkeiten im Privat- und Geschäftsbereich vorzustellen.

Es wurde detailliert auf die rechtliche Seite der elektronischen Signaturen eingegangen und die Entwicklung der letzten sechs Jahre aufgezeigt. Die Darstellung des SigG97 und der SigV97 verdeutlicht ihren Experimentiercharakter und weist, bedingt durch die fehlende Erfahrung, deren Schwächen auf. Die Zielsetzung des Gesetzgebers war die Schaffung eines rechtlichen Rahmens für digitale Signaturen, der eine höchstmögliche Sicherheit bietet. Um dies zu erreichen wurden einige Bereiche, wie z.B. das Betreiben einer Zertifizierungsstelle sehr strikt geregelt und führte zu hohen Investitionen. Die Ausparung von Haftungsregelungen war ebenso kritisch zu sehen, wie die fehlende Gleichstellung der handschriftlichen und elektronischen Unterschrift, welche die möglichen Anwendungsbereiche stark einschränkte.

Die dreijährige Entwicklungsphase der EU-Richtlinie wurde genutzt, um eine Vereinheitlichung auf europäischer Ebene zu erreichen und die Unzulänglichkeiten des SigG97 zu beseitigen. Durch die Aufnahme von Haftungsregelungen und die Gleichstellung der elektronischen und schriftlichen Form wurde dies weitestgehend erreicht. Die EU-Richtlinie legt jedoch Rahmenbedingungen fest, welche von den einzelnen Mitgliedsstaaten ausgefüllt werden müssen und ist lediglich hinsichtlich ihrer Ziele verbindlich. Der gesetzliche Spielraum kann zu heterogenen Lösungen führen und die Entwicklung einer interoperablen europäischen Umgebung elektronischer Signaturen verlangsamen. Aus diesem Grund ist es besonders wichtig, die einzelstaatlichen Umsetzungen der EU-Richtlinie in nationales Recht zu beobachten.

Im aktuellen deutschen Signaturgesetz wurde vor allem auf eine möglichst konforme Umsetzung der EU-Richtlinie geachtet, dies spiegelt sich in der Übernahme der Legaldefinitionen und der Genehmigungsfreiheit von Zertifizierungsdiensteanbietern wieder. Das Festhalten an der Zertifizierungsstruktur, welche sich im Laufe des ersten Signaturgesetzes gebildet hat, durch die Einführung eines freiwilligen Akkreditierungssystem ist nicht verwunderlich. Auch die Ausnutzung des Spielraumes, Signaturen im öffentlichen Bereich höheren Anforderungen zu unterwerfen, war zu erwarten. Dieser Weg wurde gewählt, um die hohen Investitionen der Zertifizierungsdiensteanbieter zu rechtfertigen

und die bestehende hohe Sicherheit der Infrastruktur beizubehalten. Die Aufnahme von Haftungsregelungen und Bußgeldvorschriften bei Ordnungswidrigkeiten gehen über das geforderte Maß der EU-Richtlinie hinaus, dies stellt eine Überregulierung und eine finanzielle Mehrbelastung der Anbieter dar. Dennoch könnte ein positiver Effekt dieser Regelung sein, dass Anbieter angehalten werden, sachgerechte und ordnungsgemäße Dienste zu verrichten. Gleichzeitig werden potentielle Anbieter mit geringer Kapitaldecke und/oder unzureichender Erfahrung abgehalten, als Zertifizierungsdiensteanbieter am Markt aufzutreten. Abschließend ist zu erwähnen, dass das Signaturgesetz und die Verordnung in der gültigen Fassung ausgereift scheint und nur in Details kritisiert wird. Die geforderte Gleichstellung der elektronischen und schriftlichen Form durch das Formanpassungsgesetz ist sehr positiv zu sehen und führt zu einer Rechtssicherheit im Einsatz qualifizierter elektronischer Signaturen. Durch die Änderungen im Umsatzsteuergesetz und im Verfahrensverwaltungsgesetz werden neue Einsatzgebiete geschaffen, die eine Verbreitung und die Akzeptanz elektronischer Signaturen fördern.

Die aufgezeigten kryptologischen Verfahren sind als ausreichend sicher zu erachten. Nach dem heutigen Stand der Technik und den momentan verfügbaren Methoden der Kryptanalyse ist das Fälschen von Signaturen ohne Kenntnis des privaten Schlüssels nahezu unmöglich. Es ist jedoch zu beachten, dass die eingesetzten Algorithmen auf mathematischen Vermutungen beruhen. So beruht die Sicherheit des RSA Algorithmus²²⁷ auf dem Faktorisierungsproblem großer Zahlen. Es besteht somit die Gefahr, dass durch die Entwicklung von neuen mathematischen Methoden das Entschlüsseln eingesetzter Verfahren ermöglicht werden kann. Eine solche Schwachstelle würde jedoch bekannt werden, da alle kommerziellen Signaturverfahren das Prinzip von Kerckhoff erfüllen.

Das Gefahrenpotential einer Verfälschung von Signaturen bei einem Zertifizierungsdiensteanbieter ist durch hohen Sicherheitsanforderungen gemäß Signaturgesetz an die eingesetzten Produkte gering. Besonders bei einem akkreditierten Zertifizierungsdiensteanbieter ist eine Manipulation nahezu ausgeschlossen. Durch die Prüfstellen werden gemäß SigV01 Zuverlässigkeit, Fachkompetenz und die Infrastruktur im Rahmen einer akkreditierten Tätigkeit in regelmäßigen Abständen kontrolliert. Die Infrastruktur stellt sicher, dass unbefugten der Zutritt auf sicherheitsrelevante Bereiche un-

²²⁷ Vgl. Kapitel 3.2.2.5 „Sicherheit des RSA Algorithmus“

tersagt wird. Des Weiteren wird durch die Aufgabentrennung garantiert, dass dieselbe Person nicht mehrere sicherheitsrelevante Tätigkeiten wahrnimmt.

Das größte Gefahrenpotential für die Sicherheit elektronischer Signaturen liegt auf der Anwenderseite. Durch die finanziellen Beschränkungen ist es dem durchschnittlichen Anwender nicht möglich den Sicherheitsstandard eines Zertifizierungsdiensteanbieters zu erlangen. Durch fehlende Schutzmechanismen sind PCs oft Angriffen von trojanischen Pferden²²⁸ oder Computer Viren ausgesetzt. Diese können Informationen, wie eine PIN ausspionieren. So ist es im September 2000 einem Team von Informatikern der Universität Bonn mit Hilfe eines Trojaners gelungen, die PIN der SignTrust Software eTrust Mail 1.01 für MS Outlook auszulesen.²²⁹ Es ist jedoch zu bedenken, dass der Signaturvorgang ausschließlich auf einer Chipkarte vollzogen wird. Diese Vorgehensweise stellt sicher, dass ein Angreifer trotz abgefangener PIN nicht in der Lage ist, Signaturen zu fälschen. Der Gesetzgeber hat die „Schwachstelle Anwender“ frühzeitig erkannt und eine Unterrichtungspflicht in das Signaturgesetz²³⁰ aufgenommen. Ein Zertifizierungsdiensteanbieter muss demnach den Antragsteller über die Maßnahmen unterrichten, die erforderlich sind, um zur Sicherheit von qualifizierten elektronischen Signaturen beizutragen.

Die Einsatzmöglichkeiten elektronischer Signaturen erweisen sich als vielfältig und die angeführten Pilotprojekte zeigen, dass Unternehmen das Potential erkannt haben und bereit sind in neue Bereiche zu investieren. Am Beispiel der elektronischen Rechnungsstellung wird deutlich, dass sich durch den Einsatz elektronischer Signaturen betriebliche Geschäftsprozesse effizient gestalten lassen und Kosteneinsparungen erzielt werden können. Dies gilt auch für die behördliche Kommunikation, die insbesondere durch die Initiative Bund Online 2005 gefördert wird. Das aufgeführte Nutzenpotential lässt den Schluss zu, dass sich elektronische Signaturen im Unternehmensbereich durchsetzen werden. Wie umfassend dies geschehen wird, hängt von verschiedenen Faktoren ab. Ein wichtiger Punkt sind die anfallenden Investitionskosten, die aufgebracht werden müssen, um eine Signaturlösung zu realisieren. Diese sind gerade für einen Masseneinsatz nicht zu unterschätzen. Um das Investitionsrisiko zu minimieren ist es notwendig, langfristig interoperable Systeme einzusetzen. In diesem Zusammenhang sind Hard- und

²²⁸ Ein trojanisches Pferd ist ein selbstständiges Programm, welches sich häufig unbemerkt entfaltet und wichtige Daten zerstören oder Informationen an eine fremde Adresse weiterleiten.

²²⁹ Vgl. Artikel des Heise Verlags (2001)

²³⁰ Vgl. § 6 SigG01

Software-Hersteller gefordert, bei der Entwicklung von Signatur-Produkten die ISIS-MTT-Spezifikation umzusetzen.

Im Privatbereich werden sich speziell die fortgeschrittenen elektronischen Signaturen aufgrund der kostengünstigen und einfachen Anwendung, beispielsweise in der E-Mail Kommunikation durchsetzen. Die qualifizierten elektronischen Signaturen werden in diesem Bereich derzeit nur vereinzelt genutzt. Eine Hauptursache dafür besteht in den verhältnismäßig hohen Anschaffungskosten und den noch eingeschränkten Einsatzmöglichkeiten. Neue Anwendungsbereiche erschließen sich zwar im Bereich des eGovernments, aber auch hierbei ist es fraglich, ob die Verwaltungsanwendungen alleine einen ausreichenden Anreiz für die Verbreitung qualifizierter elektronischer Signaturen bietet. Der Datenaustausch zwischen einer Privatperson und staatlichen Behörden ist meist zu gering, um einen positiven Kosten-Nutzen-Effekt zu erzielen.

Abschließend kann festgestellt werden, dass die elektronische Signatur zwar eingesetzt wird, aber von einer Massenapplication, wie sie die Bundesbehörden anstreben, noch weit entfernt ist. Um diese realisieren zu können, ist es erforderlich die technische Umsetzung an ein verbreitetes und akzeptiertes Medium zu binden. Ein erfolgversprechender Ansatz für eine praktikable signaturgesetzkonforme Massenapplication in Deutschland besteht in der Ausgabe von EC-Karten mit einem signaturfähigen Chip. EC-Karten besitzen einen hohen Verbreitungsgrad. Sie bieten durch die Ausstattung mit einem Geldkartenchip eine geeignete Möglichkeit Signaturfunktionalitäten zu integrieren. Diese können sowohl das Erstellen fortgeschrittene als auch qualifizierte elektronische Signaturen enthalten. Bereits umgesetzt wird dieser Ansatz in Österreich. Dabei ist vorgesehen, dass im Jahr 2004 alle EC-Karten signaturfähig sind. Das österreichische Geschäftsmodell sieht einen Betrag von 10 Cent für jede Signatur- und Verschlüsselungsapplication vor. In wie weit sich die EC-Karten basierte Lösung in Deutschland durchsetzen wird ist zum jetzigen Zeitpunkt nicht abzusehen. Es sind jedoch positive Ansätze zu erkennen, so vergibt die Deutsche Bank in diesem Jahr 10.000 signaturfähige EC-Karten an ihre Kunden.

Gelingt es, staatliche Initiativen mit den privaten und wirtschaftlichen Interessen in Einklang zu bringen, so ist die elektronische Signatur eine Technik mit Zukunft.

8 Literaturverzeichnis

Allgemeine Literatur:

ANDRES, J., HUSS, B., „*Die elektronische Rechnung im deutschen Umsatzsteuerrecht*“, Stand 23. April 2002. Download am 10. Dezember 2002 unter <http://www.jurpc.de/aufsatz/20020099.htm>

BEUTELSPACHER, A., „*Kryptologie*“, Vieweg Verlag, 2.Auflage Braunschweig 1991

BEUTELSPACHER, A., SCHWENK, J., WOLFENSTETTER, K.D., *Moderne Verfahren der Kryptographie*, Vieweg Verlag, 4. Auflage Braunschweig 2001

BUCHMANN, J., *Einführung in die Kryptographie*, Springer Verlag, 2. Auflage Berlin 2001

DEUTSCH, T., „*Die Beweiskraft elektronischer Dokumente*“, Stand 28.09.2000. Download am 10. Dezember 2002 unter <http://www.jurpc.de/aufsatz/20000188.htm>

DIERING, M., SCHMEH, K., „*Zertifizierter Paragrafenschwengel, Signaturgesetze in Europa*“, Artikel der Zeitschrift c't Ausgabe 13/01 Seite 182

ERTEL, W., „*Angewandte Kryptographie*“, Fachbuchverlag Leipzig, München 2001

GARFINKEL, S., „*PGP: Pretty Good Privacy, Verschlüsselung von E-Mail*“, O'Reilly International Thomson Verlag GmbH & Co KG, 1. Auflage Bonn 1996

HOCHMANN, S., „*Elektronische Signatur*“, BoD Books on Demand, Norderstedt 2001

HOEREN, T., SCHÜNGEL, M. „*Rechtsfragen der digitalen Signatur*“, Erich Schmidt Verlag, Berlin 1999

HOERETH, U., ROBISCH, M., SCHIEGL, B., „*Die elektronische Rechnung*“, Stand 29. November 2001. Download am 27. November 2002 unter [http://www.ey.com/global/download.nsf/Germany/Die_elektronische_Rechnung/\\$file/Die_elektronische_Rechnung.pdf](http://www.ey.com/global/download.nsf/Germany/Die_elektronische_Rechnung/$file/Die_elektronische_Rechnung.pdf)

KOY, H., SCHNEIDER, J., „*Selbst geknackt Spielerisches Erforschen der Kryptographie*“, Artikel der Zeitschrift c't Ausgabe 14/01 Seite 204

LUITWIELER, J., „*Digitale Signaturen und Verschlüsselung*“. Download am 10. Dezember 2002 unter <http://home.t-online.de/home/jerry.luitwieler/>

LUTZENBERGER, T., „*Technische und rechtliche Aspekte der digitalen Signatur*“, Diplomarbeit der TU München. Download am 10. Dezember 2002 unter <http://www.sicherheit-im-internet.de/download/DiplomarbeitLutzenberger.pdf>

MANHART, K. „*Mobile digitale Signatur*“ Artikel der Funkschau 13/2001. Download am 10. Mai 2003 unter <http://funkschau.de/heftarchiv/pdf/2001/fs1301/fs0113060.pdf>

NEUMANN, H., Skript zur Vorlesung „*Kryptographie I*“, Sommersemester 2000, Justus-Liebig-Universität Giessen

NEUMANN, H., Skript zur Vorlesung „*Kryptographie II*“, Wintersemester 2000/2001 Justus-Liebig-Universität Giessen

REIMER, H., „*ISIS-MTT - Interoperable PKI Anwendungen*“. Stand 22. Juni 2002. Download am 13. Mai 2003 unter <http://www.regtp.de/signatur-tage/reimer.pdf>

REINERMANN, HEINRICH, „*Electronic Government in Deutschland*“, Speyerer Forschungsberichte 226, Speyer 2002

REISEN, A., „*Signaturgesetz und Verordnung Die ersten Schritte*“, 1997. Download am 3. Februar 2003 unter <http://www.bsi.de/esig/lit/siswv.pdf>

REISEN, A., „*Digitale Signaturen*“. Download am 3. Februar 2003 unter <http://www.bsi.de/esig/lit/ds.pdf>

SCHREIBER, L., „*Elektronisches Verwalten, zum Einsatz der elektronischen Signatur in der öffentlichen Verwaltung*“, Nomos Verlagsgesellschaft, Baden Baden 2003.

SCHICKER, S., „*Die elektronische Signatur*“, Stand 11. Juni 2001. Download am 10. Dezember 2002 unter <http://www.jurpc.de/aufsatz/20010139.htm>

SIETMANN, R., „*Eine Hürde weniger ISIS-MTT soll die digitale Signatur massentauglich machen*“ Artikel der Zeitschrift c't Ausgabe 20/01 Seite 59

WINDISCH, D., „*Bezahlen im Internet*“, Stand 5. Februar 2003. Download am 10. April 2003 unter <http://goethe.ira.uka.de/seminare/internet/bezahlung>

Gesetzestexte:

„*Bürgerliches Gesetzbuch (BGB)*“, Beck Texte im dtv, 50. Auflage, 2002

„*Drittes Gesetz zur Änderung verwaltungsverfahrenrechtlicher Vorschriften*“ vom 21. August 2002. Bundesgesetzblatt Jahrgang 2002 Teil I Nr. 60, S. 3322 vom 27. August 2002

„*Gesetz zur Änderung steuerlicher Vorschriften (Steueränderungsgesetz 2001 - StÄndG 2001)*“. Bundesgesetzblatt Jahrgang 2001 Teil I Nr.72, S. 3793 vom 22. Dezember 2001.

„*Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften*“, vom 16. Mai 2001. Bundesgesetzblatt Jahrgang 2001 Teil I Nr.22, S. 876 vom 21. Mai 2001.

„*Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr*“, vom 13. Juli 2001. Bundesgesetzblatt Jahrgang 2001 Teil I Nr.35, S. 1542 vom 18. Juli 2001.

„Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste“, Artikel 3 „Gesetz zur digitalen Signatur“, vom 13. Juni 1997. Bundesgesetzblatt Jahrgang 1997 Teil I S. 1870.

„Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“, Amtsblatt der Europäischen Gemeinschaften vom 19. Januar 2000.

„Richtlinie 2001/115/EG des RATES vom 20. Dezember 2001 zur Änderung der Richtlinie 77/388/EWG mit dem Ziel der Vereinfachung, Modernisierung und Harmonisierung der mehrwertsteuerlichen Anforderungen an die Rechnungstellung“, Amtsblatt der Europäischen Gemeinschaften vom 17. Januar 2002.

„Umsatzsteuergesetz § 14 und § 15“. Stand 19. Dezember 2001. Bundesgesetzblatt Teil I Jahrgang 1999, S. 1270. Zuletzt geändert am 19. Dezember 2001 im Bundesgesetzblatt Teil I Jahrgang 2001, S. 3922.

„Verordnung zur digitalen Signatur“, vom 1. November 1997. Bundesgesetzblatt Jahrgang 1997 Teil I, S. 2498

„Verordnung zur elektronischen Signatur (Signaturverordnung - SigV)“, vom 16. November 2001. Bundesgesetzblatt Jahrgang 2001 Teil I Nr.59, S. 3074 vom 21. November 2001.

„Zivilprozessordnung (ZPO)“, Beck Texte im dtv, 33. Auflage, 2001

Literatur ohne angegebenen Verfasser:

„BundOnline 2005 Projekt wird fortgesetzt“. Stand 20. Februar 2003. Download am 13. Mai 2003 unter <http://www.golem.de/0302/24076.html>

„BSI-Interoperabilitätsspezifikationen“. Stand 1999. Download am 13. Mai 2003 unter <http://www.bsi.de/esig/basics/techbas/interop/bsi/index.htm>

„*Digitales Signieren unsicher*“, Artikel des Heise Verlags vom 11. Juni 2001. Download am 11. Mai 2003 unter <http://www.heise.de/newsticker/data/js-11.06.01-000/>

„*ELSTER Die Kommunikationssoftware der Finanzverwaltung*“. Monatsbericht April 2003 des Bundesministeriums der Finanzen. Download am 29. Mai 2003 unter <http://www.bundesfinanzministerium.de/BMF-.336.18195/Monatsbericht/.htm>.

„*FAQ des Zertifizierungsdiensteanbieters Signtrust. Zum Thema: Erstellung und Prüfung qualifizierter elektronischer Signaturen*“. Download am 17. Mai 2003 unter <http://www.signtrust.de/index.php?menu=service&menu2=faq#>

„*Geeignete Kryptoalgorithmen*“. Veröffentlicht im Bundesanzeiger Nr. 48, S. 4202-4203 vom 11. März 2003. Download am 10. Dezember 2002 unter <http://www.regtp.de>

„*Maßnahmenkatalog für technische Komponenten nach dem Signaturgesetz*“, Stand: 15. Juli 1998. Download am 3. Februar 2003 unter http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/7.pdf

„*Maßnahmenkatalog für Zertifizierungsstellen nach dem Signaturgesetz*“, Stand: 15. Juli 1998. Download am 3. Februar 2003 unter http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/6.pdf

„*Mobile elektronische Signatur*“, TÜViT Arbeitspapier, Stand Dezember 2002. Download am 10. April 2003 unter <http://www.mediakomm.net/documents/forschung/mobile--signatur.pdf>

„*Preisliste der deutschen Telekom AG Public Key Service*“, Stand Januar 2000. Download am 14. Mai 2003 unter http://www.telekom.de/dtag/t-telesec/telesec_showdatei/1,2626,12,00.pdf

„*Skript zu CrypTool Version 1.3.03*“. Download am 11. Dezember 2002 unter <http://www.cryptool.de>

„*The hash function RIPEMD-160*“. Download am 12. Dezember 2003 unter <http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html>

„*Wie signiert der Anwender*“, Anleitung zur Signatur elektronischer Dokumente. Download am 13. Dezember 2002 unter <http://www.regtp.de> Veröffentlichungen.

„*FAQ der elektronischen Signatur*“, Webseite der Regulierungsbehörde. Download am 14. Januar 2003 unter <http://www.regtp.de>

Unveröffentlichte Texte:

ERKEL, S., „*Anforderungen, Potentiale und technische Umsetzungsmöglichkeiten der elektronischen Rechnungsstellung über das Internet unter Einsatz elektronischer Signaturen gemäß § 14 Umsatzsteuergesetz*“, unveröffentlichte Diplomarbeit am Institut für Informatik, Justus-Liebig-Universität Giessen Juni 2003

Anhang

A 1 Gesetzestexte

Gesetz über Rahmenbedingungen für elektronische Signaturen vom 16. Mai 2001 (Signaturgesetz 2001)

Inhaltsübersicht

Erster Abschnitt: Allgemeine Bestimmungen

§ 1 Zweck und Anwendungsbereich

§ 2 Begriffsbestimmungen

§ 3 Zuständige Behörde

Zweiter Abschnitt: Zertifizierungsdiensteanbieter

§ 4 Allgemeine Anforderungen

§ 5 Vergabe von qualifizierten Zertifikaten

§ 6 Unterrichtungspflicht

§ 7 Inhalt von qualifizierten Zertifikaten

§ 8 Sperrung von qualifizierten Zertifikaten

§ 9 Qualifizierte Zeitstempel

§ 10 Dokumentation

§ 11 Haftung

§ 12 Deckungsvorsorge

§ 13 Einstellung der Tätigkeit

§ 14 Datenschutz

Dritter Abschnitt: Freiwillige Akkreditierung

§ 15 Freiwillige Akkreditierung von Zertifizierungsdiensteanbietern

§ 16 Zertifikate der zuständigen Behörde

Vierter Abschnitt: Technische Sicherheit

§ 17 Produkte für qualifizierte elektronische Signaturen

§ 18 Anerkennung von Prüf- und Bestätigungsstellen

Fünfter Abschnitt: Aufsicht

§ 19 Aufsichtsmaßnahmen

§ 20 Mitwirkungspflicht

Sechster Abschnitt: Schlussbestimmungen

§ 21 Bußgeldvorschriften

§ 22 Kosten und Beiträge

§ 23 Ausländische elektronische Signaturen und Produkte für elektronische Signaturen

§ 24 Rechtsverordnung

§ 25 Übergangsvorschriften

Erster Abschnitt: Allgemeine Bestimmungen

§ 1 Zweck und Anwendungsbereich

- (1) Zweck des Gesetzes ist es, Rahmenbedingungen für elektronische Signaturen zu schaffen.
- (2) Soweit nicht bestimmte elektronische Signaturen durch Rechtsvorschrift vorgeschrieben sind, ist ihre Verwendung freigestellt.
- (3) Rechtsvorschriften können für die öffentlich-rechtliche Verwaltungstätigkeit bestimmen, dass der Einsatz qualifizierter elektronischer Signaturen zusätzlichen Anforderungen unterworfen wird. Diese Anforderungen müssen objektiv, verhältnismäßig und nichtdiskriminierend sein und dürfen sich nur auf die spezifischen Merkmale der betreffenden Anwendung beziehen.

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

1. „elektronische Signaturen“ Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,
2. „fortgeschrittene elektronische Signaturen“ elektronische Signaturen nach Nummer 1, die
 - a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
 - b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
 - c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
 - d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,
3. „qualifizierte elektronische Signaturen“ elektronische Signaturen nach Nummer 2, die
 - a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
 - b) mit einer sicheren Signaturerstellungseinheit erzeugt werden,
4. „Signaturschlüssel“ einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden,
5. „Signaturprüfchlüssel“ elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden,
6. „Zertifikate“ elektronische Bescheinigungen, mit denen Signaturprüfchlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigt wird,
7. „qualifizierte Zertifikate“ elektronische Bescheinigungen nach Nummer 6 für natürliche Personen, die die Voraussetzungen des § 7 erfüllen und von Zertifizierungsdiensteanbietern ausgestellt werden, die mindestens die Anforderungen nach den §§ 4 bis 14 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen,
8. „Zertifizierungsdiensteanbieter“ natürliche oder juristische Personen, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen,
9. „Signaturschlüssel-Inhaber“ natürliche Personen, die Signaturschlüssel besitzen und denen die zugehörigen Signaturprüfchlüssel durch qualifizierte Zertifikate zugeordnet sind,
10. „sichere Signaturerstellungseinheiten“ Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die mindestens die Anforderungen nach § 17 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen und die für qualifizierte elektronische Signaturen bestimmt sind,
11. „Signaturanwendungskomponenten“ Software- und Hardwareprodukte, die dazu bestimmt sind,
 - a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder
 - b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen,
12. „technische Komponenten für Zertifizierungsdienste“ Software- oder Hardwareprodukte, die dazu bestimmt sind,
 - a) Signaturschlüssel zu erzeugen und in eine sichere Signaturerstellungseinheit zu übertragen,
 - b) qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar zu

- halten oder
- c) qualifizierte Zeitstempel zu erzeugen,
13. „Produkte für qualifizierte elektronische Signaturen“ sichere Signaturerstellungseinheiten, Signaturanwendungskomponenten und technische Komponenten für Zertifizierungsdienste,
 14. „qualifizierte Zeitstempel“ elektronische Bescheinigungen eines Zertifizierungsdiensteanbieters, der mindestens die Anforderungen nach den §§ 4 bis 14 sowie § 17 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllt, darüber, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben,
 15. „freiwillige Akkreditierung“ Verfahren zur Erteilung einer Erlaubnis für den Betrieb eines Zertifizierungsdienstes, mit der besondere Rechte und Pflichten verbunden sind.

§ 3 Zuständige Behörde

Die Aufgaben der zuständigen Behörde nach diesem Gesetz und der Rechtsverordnung nach § 24 obliegen der Behörde nach § 66 des Telekommunikationsgesetzes.

Zweiter Abschnitt: Zertifizierungsdiensteanbieter

§ 4 Allgemeine Anforderungen

- (1) Der Betrieb eines Zertifizierungsdienstes ist im Rahmen der Gesetze genehmigungsfrei.
- (2) Einen Zertifizierungsdienst darf nur betreiben, wer die für den Betrieb erforderliche Zuverlässigkeit und Fachkunde sowie eine Deckungsvorsorge nach § 12 nachweist und die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 Nr. 1, 3 und 4 gewährleistet. Die erforderliche Zuverlässigkeit besitzt, wer die Gewähr dafür bietet, als Zertifizierungsdiensteanbieter die für den Betrieb maßgeblichen Rechtsvorschriften einzuhalten. Die erforderliche Fachkunde liegt vor, wenn die im Betrieb eines Zertifizierungsdienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen. Die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes liegen vor, wenn die Maßnahmen zur Erfüllung der Sicherheitsanforderungen nach diesem Gesetz und der Rechtsverordnung nach § 24 Nr. 1, 3 und 4 der zuständigen Behörde in einem Sicherheitskonzept aufgezeigt und geeignet und praktisch umgesetzt sind.
- (3) Wer den Betrieb eines Zertifizierungsdienstes aufnimmt, hat dies der zuständigen Behörde spätestens mit der Betriebsaufnahme anzuzeigen. Mit der Anzeige ist in geeigneter Form darzulegen, dass die Voraussetzungen nach Absatz 2 vorliegen.
- (4) Die Erfüllung der Voraussetzungen nach Absatz 2 ist über die gesamte Zeitdauer der Tätigkeit des Zertifizierungsdienstes sicherzustellen. Umstände, die dies nicht mehr ermöglichen, sind der zuständigen Behörde unverzüglich anzuzeigen.
- (5) Der Zertifizierungsdiensteanbieter kann unter Einbeziehung in sein Sicherheitskonzept nach Absatz 2 Satz 4 Aufgaben nach diesem Gesetz und der Rechtsverordnung nach § 24 an Dritte übertragen.

§ 5 Vergabe von qualifizierten Zertifikaten

- (1) Der Zertifizierungsdiensteanbieter hat Personen, die ein qualifiziertes Zertifikat beantragen, zuverlässig zu identifizieren. Er hat die Zuordnung eines Signaturprüfchlüssels zu einer identifizierten Person durch ein qualifiziertes Zertifikat zu bestätigen und dieses jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten. Ein qualifiziertes Zertifikat darf nur mit Zustimmung des Signaturschlüssel-Inhabers abrufbar gehalten werden.
- (2) Ein qualifiziertes Zertifikat kann auf Verlangen eines Antragstellers Angaben über seine Vertretungsmacht für eine dritte Person sowie berufsbezogene oder sonstige Angaben zu seiner Person (Attribute) enthalten. Hinsichtlich der Angaben über die Vertretungsmacht ist die Einwilligung der dritten Person nachzuweisen; berufsbezogene oder sonstige Angaben zur Person sind durch die für die berufsbezogenen oder sonstigen Angaben zuständige Stelle zu bestätigen. Angaben über die Vertretungsmacht für eine dritte Person dürfen nur bei Nachweis der Einwilligung nach Satz 2, berufsbezogene oder sonstige Angaben des Antragstellers zur Person nur bei Vorlage der Bestätigung nach Satz 2 in ein qualifiziertes Zertifikat aufgenommen werden. Weitere personenbezogene Angaben dürfen in ein qualifizier-

- tes Zertifikat nur mit Einwilligung des Betroffenen aufgenommen werden.
- (3) Der Zertifizierungsdiensteanbieter hat auf Verlangen eines Antragstellers in einem qualifizierten Zertifikat an Stelle seines Namens ein Pseudonym aufzuführen. Enthält ein qualifiziertes Zertifikat Angaben über eine Vertretungsmacht für eine dritte Person oder berufsbezogene oder sonstige Angaben zur Person, ist eine Einwilligung der dritten Person oder der für die berufsbezogenen oder sonstigen Angaben zuständigen Stelle zur Verwendung des Pseudonyms erforderlich.
 - (4) Der Zertifizierungsdiensteanbieter hat Vorkehrungen zu treffen, damit Daten für qualifizierte Zertifikate nicht unbemerkt gefälscht oder verfälscht werden können. Er hat weitere Vorkehrungen zu treffen, um die Geheimhaltung der Signaturschlüssel zu gewährleisten. Eine Speicherung von Signaturschlüsseln außerhalb der sicheren Signaturerstellungseinheit ist unzulässig.
 - (5) Der Zertifizierungsdiensteanbieter hat für die Ausübung der Zertifizierungstätigkeit zuverlässiges Personal und Produkte für qualifizierte elektronische Signaturen, die mindestens die Anforderungen nach den §§ 4 bis 14 sowie § 17 oder § 23 dieses Gesetzes und der Rechtsverordnung nach § 24 erfüllen, einzusetzen.
 - (6) Der Zertifizierungsdiensteanbieter hat sich in geeigneter Weise zu überzeugen, dass der Antragsteller die zugehörige sichere Signaturerstellungseinheit besitzt.

§ 6 Unterrichtungspflicht

- (1) Der Zertifizierungsdiensteanbieter hat den Antragsteller nach § 5 Abs. 1 über die Maßnahmen zu unterrichten, die erforderlich sind, um zur Sicherheit von qualifizierten elektronischen Signaturen und zu deren zuverlässiger Prüfung beizutragen. Er hat den Antragsteller darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.
- (2) Der Zertifizierungsdiensteanbieter hat den Antragsteller darüber zu unterrichten, dass eine qualifizierte elektronische Signatur im Rechtsverkehr die gleiche Wirkung hat wie eine eigenhändige Unterschrift, wenn durch Gesetz nicht ein anderes bestimmt ist.
- (3) Zur Unterrichtung nach Absatz 1 und 2 ist dem Antragsteller eine schriftliche Belehrung auszuhändigen, deren Kenntnisnahme dieser durch gesonderte Unterschrift zu bestätigen hat. Soweit ein Antragsteller bereits zu einem früheren Zeitpunkt nach den Absätzen 1 und 2 unterrichtet worden ist, kann eine erneute Unterrichtung unterbleiben.

§ 7 Inhalt von qualifizierten Zertifikaten

- (1) Ein qualifiziertes Zertifikat muss folgende Angaben enthalten und eine qualifizierte elektronische Signatur tragen:
 1. den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muss,
 2. den zugeordneten Signaturprüfschlüssel,
 3. die Bezeichnung der Algorithmen, mit denen der Signaturprüfschlüssel des Signaturschlüssel-Inhabers sowie der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann,
 4. die laufende Nummer des Zertifikates,
 5. Beginn und Ende der Gültigkeit des Zertifikates,
 6. den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist,
 7. Angaben darüber, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt ist,
 8. Angaben, dass es sich um ein qualifiziertes Zertifikat handelt, und
 9. nach Bedarf Attribute des Signaturschlüssel-Inhabers.
- (2) Attribute können auch in ein gesondertes qualifiziertes Zertifikat (qualifiziertes Attribut-Zertifikat) aufgenommen werden. Bei einem qualifizierten Attribut-Zertifikat können die Angaben nach Absatz 1 durch eindeutige Referenzdaten des qualifizierten Zertifikates, auf das sie Bezug nehmen, ersetzt werden, soweit sie nicht für die Nutzung des qualifizierten Attribut-Zertifikates benötigt werden.

§ 8 Sperrung von qualifizierten Zertifikaten

- (1) Der Zertifizierungsdiensteanbieter hat ein qualifiziertes Zertifikat unverzüglich zu sperren, wenn ein Signaturschlüssel-Inhaber oder sein Vertreter es verlangt, das Zertifikat auf Grund falscher Angaben zu § 7 ausgestellt wurde, der Zertifizierungsdiensteanbieter seine Tätigkeit beendet und diese nicht von einem anderen Zertifizierungsdiensteanbieter fortgeführt wird oder die zuständige Behörde gemäß § 19 Abs. 4 eine Sperrung anordnet. Die Sperrung muss den Zeitpunkt enthalten, von dem an sie gilt. Eine rückwirkende Sperrung ist unzulässig. Wurde ein qualifiziertes Zertifikat mit falschen Angaben ausgestellt, kann der Zertifizierungsdiensteanbieter dies zusätzlich kenntlich machen.
- (2) Enthält ein qualifiziertes Zertifikat Angaben nach § 5 Abs. 2, so kann auch die dritte Person oder die für die berufsbezogenen oder sonstigen Angaben zur Person zuständige Stelle, wenn die Voraussetzungen für die berufsbezogenen oder sonstigen Angaben zur Person nach Aufnahme in das qualifizierte Zertifikat entfallen, eine Sperrung des betreffenden Zertifikates nach Absatz 1 verlangen.

§ 9 Qualifizierte Zeitstempel

Stellt ein Zertifizierungsdiensteanbieter qualifizierte Zeitstempel aus, so gilt § 5 Abs. 5 entsprechend.

§ 10 Dokumentation

- (1) Der Zertifizierungsdiensteanbieter hat die Sicherheitsmaßnahmen zur Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 Nr. 1, 3 und 4 sowie die ausgestellten qualifizierten Zertifikate nach Maßgabe des Satzes 2 so zu dokumentieren, dass die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind. Die Dokumentation muss unverzüglich so erfolgen, dass sie nachträglich nicht unbemerkt verändert werden kann. Dies gilt insbesondere für die Ausstellung und Sperrung von qualifizierten Zertifikaten.
- (2) Dem Signaturschlüssel-Inhaber ist auf Verlangen Einsicht in die ihn betreffenden Daten und Verfahrensschritte zu gewähren.

§ 11 Haftung

- (1) Verletzt ein Zertifizierungsdiensteanbieter die Anforderungen dieses Gesetzes oder der Rechtsverordnung nach § 24 oder versagen seine Produkte für qualifizierte elektronische Signaturen oder sonstige technische Sicherungseinrichtungen, so hat er einem Dritten den Schaden zu ersetzen, den dieser dadurch erleidet, dass er auf die Angaben in einem qualifizierten Zertifikat, einem qualifizierten Zeitstempel oder einer Auskunft nach § 5 Abs. 1 Satz 2 vertraut. Die Ersatzpflicht tritt nicht ein, wenn der Dritte die Fehlerhaftigkeit der Angabe kannte oder kennen musste.
- (2) Die Ersatzpflicht tritt nicht ein, wenn der Zertifizierungsdiensteanbieter nicht schuldhaft gehandelt hat.
- (3) Wenn ein qualifiziertes Zertifikat die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt, tritt die Ersatzpflicht nur im Rahmen dieser Beschränkungen ein.
- (4) Der Zertifizierungsdiensteanbieter haftet für beauftragte Dritte nach § 4 Abs. 5 und beim Entstehen für ausländische Zertifikate nach § 23 Abs. 1 Nr. 2 wie für eigenes Handeln. § 831 Abs. 1 Satz 2 des Bürgerlichen Gesetzbuchs findet keine Anwendung.

§ 12 Deckungsvorsorge

Der Zertifizierungsdiensteanbieter ist verpflichtet, eine geeignete Deckungsvorsorge zu treffen, damit er seinen gesetzlichen Verpflichtungen zum Ersatz von Schäden nachkommen kann, die dadurch entstehen, dass er die Anforderungen dieses Gesetzes oder der Rechtsverordnung nach § 24 verletzt oder seine Produkte für qualifizierte elektronische Signaturen oder sonstige technische Sicherungseinrichtungen versagen. Die Mindestsumme beträgt jeweils 500 000 Deutsche Mark für einen durch ein haftungsauslösendes Ereignis der in Satz 1 bezeichneten Art verursachten Schaden.

§ 13 Einstellung der Tätigkeit

- (1) Der Zertifizierungsdiensteanbieter hat die Einstellung seiner Tätigkeit unverzüglich der zuständigen Behörde anzuzeigen. Er hat dafür zu sorgen, dass die bei Einstellung der Tätigkeit gültigen qualifizierten Zertifikate von einem anderen Zertifizierungsdiensteanbieter ü-

bernommen werden, oder diese zu sperren. Er hat die betroffenen Signaturschlüssel-Inhaber über die Einstellung seiner Tätigkeit und die Übernahme der qualifizierten Zertifikate durch einen anderen Zertifizierungsdiensteanbieter zu benachrichtigen.

- (2) Der Zertifizierungsdiensteanbieter hat die Dokumentation nach § 10 an den Zertifizierungsdiensteanbieter, welcher die Zertifikate nach Absatz 1 übernimmt, zu übergeben. Übernimmt kein anderer Zertifizierungsdiensteanbieter die Dokumentation, so hat die zuständige Behörde diese zu übernehmen. Die zuständige Behörde erteilt bei Vorliegen eines berechtigten Interesses Auskunft zur Dokumentation nach Satz 2, soweit dies technisch ohne unverhältnismäßig großen Aufwand möglich ist.
- (3) Der Zertifizierungsdiensteanbieter hat einen Antrag auf Eröffnung eines Insolvenzverfahrens der zuständigen Behörde unverzüglich anzuzeigen.

§ 14 Datenschutz

- (1) Der Zertifizierungsdiensteanbieter darf personenbezogene Daten nur unmittelbar beim Betroffenen selbst und nur insoweit erheben, als dies für Zwecke eines qualifizierten Zertifikates erforderlich ist. Eine Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zulässig. Für andere als die in Satz 1 genannten Zwecke dürfen die Daten nur verwendet werden, wenn dieses Gesetz es erlaubt oder der Betroffene eingewilligt hat.
- (2) Bei einem Signaturschlüssel-Inhaber mit Pseudonym hat der Zertifizierungsdiensteanbieter die Daten über dessen Identität auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich ist oder soweit Gerichte dies im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen. Die Auskünfte sind zu dokumentieren. Die ersuchende Behörde hat den Signaturschlüssel-Inhaber über die Aufdeckung des Pseudonyms zu unterrichten, sobald dadurch die Wahrnehmung der gesetzlichen Aufgaben nicht mehr beeinträchtigt wird oder wenn das Interesse des Signaturschlüssel-Inhabers an der Unterrichtung überwiegt.
- (3) Soweit andere als die in § 2 Nr. 8 genannten Zertifizierungsdiensteanbieter Zertifikate für elektronische Signaturen ausstellen, gelten die Absätze 1 und 2 entsprechend.

Dritter Abschnitt: Freiwillige Akkreditierung

§ 15 Freiwillige Akkreditierung von Zertifizierungsdiensteanbietern

- (1) Zertifizierungsdiensteanbieter können sich auf Antrag von der zuständigen Behörde akkreditieren lassen; die zuständige Behörde kann sich bei der Akkreditierung privater Stellen bedienen. Die Akkreditierung ist zu erteilen, wenn der Zertifizierungsdiensteanbieter nachweist, dass die Vorschriften nach diesem Gesetz und der Rechtsverordnung nach § 24 erfüllt sind. Akkreditierte Zertifizierungsdiensteanbieter erhalten ein Gütezeichen der zuständigen Behörde. Mit diesem wird der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen (qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung) zum Ausdruck gebracht. Sie dürfen sich als akkreditierte Zertifizierungsdiensteanbieter bezeichnen und sich im Rechts- und Geschäftsverkehr auf die nachgewiesene Sicherheit berufen.
- (2) Zur Erfüllung der Voraussetzungen nach Absatz 1 muss das Sicherheitskonzept nach § 4 Abs. 2 Satz 4 durch eine Stelle nach § 18 umfassend auf seine Eignung und praktische Umsetzung geprüft und bestätigt sein. Die Prüfung und Bestätigung ist nach sicherheitserheblichen Veränderungen sowie in regelmäßigen Zeitabständen zu wiederholen.
- (3) Die Akkreditierung kann mit Nebenbestimmungen versehen werden, soweit dies erforderlich ist, um die Erfüllung der Voraussetzungen nach diesem Gesetz und der Rechtsverordnung nach § 24 bei Aufnahme und während des Betriebes sicherzustellen.
- (4) Die Akkreditierung ist zu versagen, wenn die Voraussetzungen nach diesem Gesetz und der Rechtsverordnung nach § 24 nicht erfüllt sind; § 19 findet entsprechend Anwendung.
- (5) Bei Nichterfüllung der Pflichten aus diesem Gesetz oder der Rechtsverordnung nach § 24 oder bei Vorliegen eines Versagungsgrundes nach Absatz 4 hat die zuständige Behörde die

Akkreditierung zu widerrufen oder diese, soweit die Gründe bereits zum Zeitpunkt der Akkreditierung vorlagen, zurückzunehmen, wenn Maßnahmen nach § 19 Abs. 2 keinen Erfolg versprechen.

- (6) Im Falle des Widerrufs oder der Rücknahme einer Akkreditierung oder im Falle der Einstellung der Tätigkeit eines akkreditierten Zertifizierungsdiensteanbieters hat die zuständige Behörde eine Übernahme der Tätigkeit durch einen anderen akkreditierten Zertifizierungsdiensteanbieter oder die Abwicklung der Verträge mit den Signaturschlüssel-Inhabern sicherzustellen. Dies gilt auch bei Antrag auf Eröffnung eines Insolvenzverfahrens, wenn die Tätigkeit nicht fortgesetzt wird. Übernimmt kein anderer akkreditierter Zertifizierungsdiensteanbieter die Dokumentation gemäß § 13 Abs. 2, so hat die zuständige Behörde diese zu übernehmen; § 10 Abs. 1 Satz 1 gilt entsprechend.
- (7) Bei Produkten für qualifizierte elektronische Signaturen muss die Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 und der Rechtsverordnung nach § 24 nach dem Stand von Wissenschaft und Technik hinreichend geprüft und durch eine Stelle nach § 18 bestätigt worden sein; Absatz 1 Satz 3 findet entsprechende Anwendung. Der akkreditierte Zertifizierungsdiensteanbieter hat
 1. für seine Zertifizierungstätigkeit nur nach Satz 1 geprüfte und bestätigte Produkte für qualifizierte elektronische Signaturen einzusetzen,
 2. qualifizierte Zertifikate nur für Personen auszustellen, die nachweislich nach Satz 1 geprüfte und bestätigte sichere Signaturerstellungseinheiten besitzen, und
 3. die Signaturschlüssel-Inhaber im Rahmen des § 6 Abs. 1 über nach Satz 1 geprüfte und bestätigte Signaturanwendungskomponenten zu unterrichten.

§ 16 Zertifikate der zuständigen Behörde

- (1) Die zuständige Behörde stellt den akkreditierten Zertifizierungsdiensteanbietern die für ihre Tätigkeit benötigten qualifizierten Zertifikate aus. Die Vorschriften für die Vergabe von qualifizierten Zertifikaten durch akkreditierte Zertifizierungsdiensteanbieter gelten für die zuständige Behörde entsprechend. Sie sperrt von ihr ausgestellte qualifizierte Zertifikate, wenn ein akkreditierter Zertifizierungsdiensteanbieter seine Tätigkeit einstellt oder wenn eine Akkreditierung zurückgenommen oder widerrufen wird.
- (2) Die zuständige Behörde hat
 1. die Namen, Anschriften und Kommunikationsverbindungen der akkreditierten Zertifizierungsdiensteanbieter,
 2. den Widerruf oder die Rücknahme einer Akkreditierung,
 3. die von ihr ausgestellten qualifizierten Zertifikate und deren Sperrung und
 4. die Beendigung und die Untersagung des Betriebes eines akkreditierten Zertifizierungsdiensteanbieters jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten.
- (3) Bei Bedarf stellt die zuständige Behörde auch die von den Zertifizierungsdiensteanbietern oder Herstellern benötigten elektronischen Bescheinigungen für die automatische Authentifizierung von Produkten nach § 15 Abs. 7 aus.

Vierter Abschnitt: Technische Sicherheit

§ 17 Produkte für qualifizierte elektronische Signaturen

- (1) Für die Speicherung von Signaturschlüsseln sowie für die Erzeugung qualifizierter elektronischer Signaturen sind sichere Signaturerstellungseinheiten einzusetzen, die Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung der Signaturschlüssel schützen. Werden die Signaturschlüssel auf einer sicheren Signaturerstellungseinheit selbst erzeugt, so gilt Absatz 3 Nr. 1 entsprechend.
- (2) Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht. Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,
 1. auf welche Daten sich die Signatur bezieht,
 2. ob die signierten Daten unverändert sind,
 3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,

4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und
 5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 2 geführt hat. Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Die Signaturschlüssel-Inhaber sollen solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.
- (3) Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um
1. bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel zu gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit auszuschließen,
 2. qualifizierte Zertifikate, die gemäß § 5 Abs. 1 Satz 2 nachprüfbar oder abrufbar gehalten werden, vor unbefugter Veränderung und unbefugtem Abruf zu schützen sowie
 3. bei Erzeugung qualifizierter Zeitstempel Fälschungen und Verfälschungen auszuschließen.
- (4) Die Erfüllung der Anforderungen nach den Absätzen 1 und 3 Nr. 1 sowie der Rechtsverordnung nach § 24 ist durch eine Stelle nach § 18 zu bestätigen. Zur Erfüllung der Anforderungen nach den Absätzen 2 und 3 Nr. 2 und 3 genügt eine Erklärung durch den Hersteller des Produkts für qualifizierte elektronische Signaturen.

§ 18 Anerkennung von Prüf- und Bestätigungsstellen

- (1) Die zuständige Behörde erkennt eine natürliche oder juristische Person auf Antrag als Bestätigungsstelle nach § 17 Abs. 4 oder § 15 Abs. 7 Satz 1 oder als Prüf- und Bestätigungsstelle nach § 15 Abs. 2 an, wenn diese die für die Tätigkeit erforderliche Zuverlässigkeit, Unabhängigkeit und Fachkunde nachweist. Die Anerkennung kann inhaltlich beschränkt, vorläufig oder mit einer Befristung versehen erteilt werden und mit Auflagen verbunden sein.
- (2) Die nach Absatz 1 anerkannten Stellen haben ihre Aufgaben unparteiisch, weisungsfrei und gewissenhaft zu erfüllen. Sie haben die Prüfungen und Bestätigungen zu dokumentieren und die Dokumentation im Falle der Einstellung ihrer Tätigkeit an die zuständige Behörde zu übergeben.

Fünfter Abschnitt: Aufsicht

§ 19 Aufsichtsmaßnahmen

- (1) Die Aufsicht über die Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 obliegt der zuständigen Behörde; diese kann sich bei der Durchführung der Aufsicht privater Stellen bedienen. Mit der Aufnahme des Betriebes unterliegt ein Zertifizierungsdiensteanbieter der Aufsicht der zuständigen Behörde.
- (2) Die zuständige Behörde kann gegenüber Zertifizierungsdiensteanbietern Maßnahmen zur Sicherstellung der Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 treffen.
- (3) Die zuständige Behörde hat einem Zertifizierungsdiensteanbieter den Betrieb vorübergehend, teilweise oder ganz zu untersagen, wenn Tatsachen die Annahme rechtfertigen, dass er
 1. nicht die für den Betrieb eines Zertifizierungsdienstes erforderliche Zuverlässigkeit besitzt,
 2. nicht nachweist, dass die für den Betrieb erforderliche Fachkunde vorliegt,
 3. nicht über die erforderliche Deckungsvorsorge verfügt,
 4. ungeeignete Produkte für qualifizierte elektronische Signaturen verwendet oder
 5. die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 nicht erfüllt und Maßnahmen nach Absatz 2 keinen Erfolg versprechen.
- (4) Die zuständige Behörde kann eine Sperrung von qualifizierten Zertifikaten anordnen, wenn Tatsachen die Annahme rechtfertigen, dass qualifizierte Zertifikate gefälscht oder nicht hinreichend fälschungssicher sind oder dass sichere Signaturerstellungseinheiten Sicherheitsmängel aufweisen, die eine unbemerkte Fälschung qualifizierter elektronischer Signaturen oder eine unbemerkte Verfälschung damit signierter Daten zulassen.

- (5) Die Gültigkeit der von einem Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikate bleibt von der Untersagung des Betriebes und der Einstellung der Tätigkeit sowie der Rücknahme und dem Widerruf einer Akkreditierung unberührt.
- (6) Die zuständige Behörde hat die Namen der bei ihr angezeigten Zertifizierungsdiensteanbieter sowie der Zertifizierungsdiensteanbieter, die ihre Tätigkeit nach § 13 eingestellt haben oder deren Betrieb nach § 19 Abs. 3 untersagt wurde, für jeden über öffentlich erreichbare Kommunikationsverbindungen abrufbar zu halten.

§ 20 Mitwirkungspflicht

- (1) Die Zertifizierungsdiensteanbieter und die für diese nach § 4 Abs. 5 tätigen Dritten haben der zuständigen Behörde und den in ihrem Auftrag handelnden Personen das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten, auf Verlangen die in Betracht kommenden Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstigen Unterlagen in geeigneter Weise zur Einsicht vorzulegen, auch soweit sie in elektronischer Form geführt werden, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren.
- (2) Der zur Erteilung einer Auskunft Verpflichtete kann die Auskunft verweigern, wenn er sich damit selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr der Verfolgung wegen einer Straftat oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Er ist auf dieses Recht hinzuweisen.

Sechster Abschnitt: Schlussbestimmungen

§ 21 Bußgeldvorschriften

- (1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
 1. entgegen § 4 Abs. 2 Satz 1, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, 3 und 4, einen Zertifizierungsdienst betreibt,
 2. entgegen § 4 Abs. 3 Satz 1 oder § 13 Abs. 1 Satz 1 eine Anzeige nicht, nicht richtig oder nicht rechtzeitig erstattet,
 3. entgegen § 5 Abs. 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1 eine Person nicht, nicht richtig oder nicht rechtzeitig identifiziert,
 4. entgegen § 5 Abs. 1 Satz 2, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, ein qualifiziertes Zertifikat nicht nachprüfbar hält,
 5. entgegen § 5 Abs. 1 Satz 3 ein qualifiziertes Zertifikat abrufbar hält,
 6. entgegen § 5 Abs. 2 Satz 3 oder 4 eine Angabe in ein qualifiziertes Zertifikat aufnimmt,
 7. entgegen § 5 Abs. 4 Satz 2, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, eine Vorkehrung nicht oder nicht richtig trifft,
 8. entgegen § 5 Abs. 4 Satz 3 einen Signaturschlüssel speichert,
 9. entgegen § 10 Abs. 1 Satz 1, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, eine Sicherheitsmaßnahme oder ein qualifiziertes Zertifikat nicht, nicht richtig oder nicht rechtzeitig dokumentiert,
 10. entgegen § 13 Abs. 1 Satz 2, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, nicht dafür sorgt, dass ein qualifiziertes Zertifikat von einem anderen Zertifizierungsdiensteanbieter übernommen wird und ein qualifiziertes Zertifikat nicht oder nicht rechtzeitig sperrt oder
 11. entgegen § 13 Abs. 1 Satz 3 in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1 einen Signaturschlüssel-Inhaber nicht, nicht richtig oder nicht rechtzeitig benachrichtigt.
- (2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nr. 1, 7 und 8 mit einer Geldbuße bis zu hunderttausend Deutsche Mark, in den übrigen Fällen mit einer Geldbuße bis zu zwanzigtausend Deutsche Mark geahndet werden.
- (3) Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist die Regulierungsbehörde für Telekommunikation und Post.

§ 22 Kosten und Beiträge

- (1) Die zuständige Behörde erhebt für ihre folgenden Amtshandlungen Kosten (Gebühren und

Auslagen):

1. Maßnahmen im Rahmen der freiwilligen Akkreditierung von Zertifizierungsdiensteanbietern nach § 15 und der Rechtsverordnung nach § 24,
2. Maßnahmen im Rahmen der Ausstellung der qualifizierten Zertifikate nach § 16 Abs. 1 sowie der Ausstellung von Bescheinigungen nach § 16 Abs. 3,
3. Maßnahmen im Rahmen der Anerkennung von Prüf- und Bestätigungsstellen nach § 18 und der Rechtsverordnung nach § 24,
4. Maßnahmen im Rahmen der Aufsicht nach § 19 Abs. 1 bis 4 in Verbindung mit § 4 Abs. 2 bis 4 und der Rechtsverordnung nach § 24.

Kosten werden auch für den Verwaltungsaufwand erhoben, der dadurch entsteht, dass sich die Behörde bei der Durchführung der Aufsicht privater Stellen bedient. Das Verwaltungskostengesetz findet Anwendung.

- (2) Zertifizierungsdiensteanbieter, die den Betrieb nach § 4 Abs. 3 angezeigt haben, haben zur Abgeltung des Verwaltungsaufwands für die ständige Erfüllung der Voraussetzungen nach § 19 Abs. 6 eine Abgabe an die zuständige Behörde zu entrichten, die als Jahresbeitrag erhoben wird. Zertifizierungsdiensteanbieter, die nach § 15 Abs. 1 akkreditiert sind, haben zur Abgeltung des Verwaltungsaufwands für die ständige Erfüllung der Voraussetzungen nach § 16 Abs. 2 eine Abgabe an die zuständige Behörde zu entrichten, die als Jahresbeitrag erhoben wird.

§ 23 Ausländische elektronische Signaturen und Produkte für elektronische Signaturen

- (1) Elektronische Signaturen, für die ein ausländisches qualifiziertes Zertifikat aus einem anderen Mitgliedstaat der Europäischen Union oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum vorliegt, sind, soweit sie Artikel 5 Abs. 1 der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. EG 2000 Nr. L 13 S. 2) in der jeweils geltenden Fassung entsprechen, qualifizierten elektronischen Signaturen gleichgestellt. Elektronische Signaturen aus Drittstaaten sind qualifizierten elektronischen Signaturen gleichgestellt, wenn das Zertifikat von einem dortigen Zertifizierungsdiensteanbieter öffentlich als qualifiziertes Zertifikat ausgestellt und für eine elektronische Signatur im Sinne von Artikel 5 Abs. 1 der Richtlinie 1999/93/EG bestimmt ist und wenn
1. der Zertifizierungsdiensteanbieter die Anforderungen der Richtlinie erfüllt und in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum akkreditiert ist oder
 2. ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, welcher die Anforderungen der Richtlinie erfüllt, für das Zertifikat einsteht oder
 3. das Zertifikat oder der Zertifizierungsdiensteanbieter im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Europäischen Union und Drittstaaten oder internationalen Organisationen anerkannt ist.
- (2) Elektronische Signaturen nach Absatz 1 sind qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung nach § 15 Abs. 1 gleichgestellt, wenn sie nachweislich gleichwertige Sicherheit aufweisen.
- (3) Produkte für elektronische Signaturen, bei denen in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum festgestellt wurde, dass sie den Anforderungen der Richtlinie 1999/93/EG in der jeweils geltenden Fassung entsprechen, werden anerkannt. Den nach § 15 Abs. 7 geprüften Produkten für qualifizierte elektronische Signaturen werden Produkte für elektronische Signaturen aus einem in Satz 1 genannten Staat oder aus einem Drittstaat gleichgestellt, wenn sie nachweislich gleichwertige Sicherheit aufweisen.

§ 24 Rechtsverordnung

Die Bundesregierung wird ermächtigt, durch Rechtsverordnung die zur Durchführung der §§ 3 bis 23 erforderlichen Rechtsvorschriften zu erlassen über

1. die Ausgestaltung der Pflichten der Zertifizierungsdiensteanbieter in Bezug auf die Betriebsaufnahme und während des Betriebes sowie bei Einstellung des Betriebes nach § 4 Abs. 2 und 3, §§ 5, 6 Abs. 1, §§ 8, 10, 13 und 15,

2. die gebührenpflichtigen Tatbestände und die Gebührensätze sowie die Höhe der Beiträge und das Verfahren der Beitragserhebung durch die zuständige Behörde; bei der Bemessung der Beiträge ist der Verwaltungsaufwand (Personal- und Sachaufwand) sowie Investitionsaufwand zugrunde zu legen soweit er nicht bereits durch eine Gebühr abgegolten wird,
3. die Ausgestaltung des Inhalts und die Gültigkeitsdauer von qualifizierten Zertifikaten nach § 7,
4. die zur Erfüllung der Verpflichtung zur Deckungsvorsorge nach § 12 zulässigen Sicherheitsleistungen sowie deren Umfang, Höhe und inhaltliche Ausgestaltung,
5. die näheren Anforderungen an Produkte für qualifizierte elektronische Signaturen nach § 17 Abs. 1 bis 3 sowie die Prüfung dieser Produkte und die Bestätigung, dass die Anforderungen erfüllt sind, nach § 17 Abs. 4 und § 15 Abs. 7,
6. die Einzelheiten des Verfahrens der Anerkennung sowie der Tätigkeit von Prüf- und Bestätigungsstellen nach § 18,
7. den Zeitraum sowie das Verfahren, nach dem Daten mit einer qualifizierten elektronischen Signatur nach § 6 Abs. 1 Satz 2 neu signiert werden sollten,
8. das Verfahren zur Feststellung der gleichwertigen Sicherheit von ausländischen elektronischen Signaturen und ausländischen Produkten für elektronische Signaturen nach § 23.

§ 25 Übergangsvorschriften

- (1) Die nach dem Signaturgesetz vom 22. Juli 1997 (BGBl. I S. 1870, 1872), geändert durch Artikel 5 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3836), genehmigten Zertifizierungsstellen gelten als akkreditiert im Sinne von § 15. Diese haben der zuständigen Behörde innerhalb von drei Monaten nach Inkrafttreten dieses Gesetzes einen Deckungsnachweis nach § 12 vorzulegen.
- (2) Die von den Zertifizierungsstellen nach Absatz 1 bis zum Zeitpunkt des Inkrafttretens dieses Gesetzes nach § 5 des Signaturgesetzes vom 22. Juli 1997 (BGBl. I S. 1870, 1872), geändert durch Artikel 5 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3836), ausgestellten Zertifikate sind qualifizierten Zertifikaten gleichgestellt. Inhaber von Zertifikaten nach Satz 1 sind innerhalb von sechs Monaten nach Inkrafttreten dieses Gesetzes durch die Zertifizierungsstelle nach § 6 Abs. 2 in geeigneter Weise zu unterrichten.
- (3) Die von der zuständigen Behörde erfolgten Anerkennungen von Prüf- und Bestätigungsstellen nach § 4 Abs. 3 Satz 3 und § 14 Abs. 4 des Signaturgesetzes vom 22. Juli 1997 (BGBl. I S. 1870, 1872), geändert durch Artikel 5 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3836), behalten ihre Gültigkeit, soweit sie in Übereinstimmung mit § 18 dieses Gesetzes stehen.
- (4) Technische Komponenten, bei denen die Erfüllung der Anforderungen nach § 14 Abs. 4 des Signaturgesetzes vom 22. Juli 1997 (BGBl. I S. 1870, 1872) geprüft und bestätigt wurde, sind Produkten für qualifizierte elektronische Signaturen nach § 15 Abs. 7 dieses Gesetzes gleichgestellt.

Die verfassungsmäßigen Rechte des Bundesrates sind gewahrt.

Das vorstehende Gesetz wird hiermit ausgefertigt und wird im Bundesgesetzblatt verkündet.

Berlin, den 16. Mai 2001

Der Bundespräsident
Johannes Rau

Der Bundeskanzler
Gerhard Schröder

Der Bundesminister
für Wirtschaft und Technologie
Müller

Verordnung zur elektronischen Signatur vom 16. November 2001**(Signaturverordnung 2001)**

Auf Grund des § 24 des Signaturgesetzes vom 16. Mai 2001 (BGBl. I S. 876) in Verbindung mit dem 2. Abschnitt des Verwaltungskostengesetzes vom 23. Juni 1970 (BGBl. I S. 821) verordnet die Bundesregierung:

Inhaltsübersicht

- § 1 Form, Inhalt und Änderung der Anzeige
- § 2 Inhalt des Sicherheitskonzepts
- § 3 Identitätsprüfung und Attributsnachweise
- § 4 Führung eines Zertifikatsverzeichnisses
- § 5 Einzelne Sicherheitsvorkehrungen des Zertifizierungsdiensteanbieters
- § 6 Ausgestaltung der Unterrichtung
- § 7 Sperrung von qualifizierten Zertifikaten
- § 8 Umfang der Dokumentation
- § 9 Ausgestaltung der Deckungsvorsorge
- § 10 Einstellen der Tätigkeit
- § 11 Freiwillige Akkreditierung
- § 12 Festsetzung und Erhebung von Kosten
- § 13 Festsetzung und Erhebung von Beiträgen
- § 14 Inhalt und Gültigkeitsdauer von qualifizierten Zertifikaten
- § 15 Anforderungen an Produkte für qualifizierte elektronische Signaturen
- § 16 Verfahren der Anerkennung sowie der Tätigkeit von Prüf- und Bestätigungsstellen
- § 17 Zeitraum und Verfahren zur langfristigen Datensicherung
- § 18 Verfahren zur Feststellung der gleichwertigen Sicherheit von ausländischen elektronischen Signaturen und Produkten
- § 19 Inkrafttreten, Außerkrafttreten
- Anlage 1 (zu § 11 Abs.3 und zu § 15 Abs. 5): Vorgaben für die Prüfung von Produkten für qualifizierte elektronische Signaturen
- Anlage 2 (zu § 12): Kosten

§ 1 Form, Inhalt und Änderung der Anzeige

- (1) Eine Anzeige nach § 4 Abs. 3 des Signaturgesetzes ist schriftlich oder mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen bei der zuständigen Behörde vorzunehmen.
- (2) Die Anzeige muss folgende Angaben und Unterlagen umfassen:
 1. den Namen und die Anschrift des Zertifizierungsdiensteanbieters,
 2. die Namen der gesetzlichen Vertreter,
 3. aktuelle Führungszeugnisse nach § 30 Abs. 5 des Bundeszentralregistergesetzes für den Zertifizierungsdiensteanbieter und seine gesetzlichen Vertreter,
 4. einen aktuellen Handelsregisterauszug oder eine vergleichbare Unterlage,
 5. Belege zum Nachweis der erforderlichen technischen, administrativen und juristischen Fachkunde nach § 4 Abs. 2 Satz 3 des Signaturgesetzes,
 6. ein Sicherheitskonzept mit einer genauen Darlegung, wie dieses umgesetzt ist, ein-

- schließlich der Übertragung von Aufgaben an Dritte nach § 4 Abs. 5 des Signaturgesetzes, und
7. einen Nachweis der Deckungsvorsorge nach § 12 des Signaturgesetzes. Ändern sich die Umstände nach Satz 1 Nr. 1 oder Nr. 2 oder sicherheitserhebliche Umstände nach Satz 1 Nr. 6, ist die zuständige Behörde schriftlich oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments zu informieren. § 2 bleibt unberührt.
- (3) Soweit Teile des Zertifizierungsdienstes in einem Staat nach § 23 Abs. 1 Satz 1 des Signaturgesetzes oder unter den Bedingungen des § 23 Abs. 1 Satz 2 Nr. 3 des Signaturgesetzes in einem Drittstaat betrieben werden, sind zusätzlich Nachweise darüber vorzulegen, dass der Betrieb einer gleichwertigen Aufsicht unterliegt. Der Betrieb von Teilen des Zertifizierungsdienstes in einem anderen als in Satz 1 genannten Staat ist nur im Rahmen einer freiwilligen Akkreditierung zulässig, soweit die Sicherstellung der Aufsicht nachgewiesen wird.

§ 2 Inhalt des Sicherheitskonzepts

Das Sicherheitskonzept nach § 4 Abs. 2 Satz 4 des Signaturgesetzes hat Folgendes zu enthalten:

1. eine Beschreibung aller erforderlichen technischen, baulichen und organisatorischen Sicherheitsmaßnahmen und deren Eignung,
2. eine Übersicht über die eingesetzten Produkte für qualifizierte elektronische Signaturen mit Herstellererklärungen nach § 17 Abs. 4 Satz 2 oder Bestätigungen nach § 17 Abs. 4 Satz 1 oder nach § 15 Abs. 7 Satz 1 des Signaturgesetzes,
3. eine Übersicht über die Aufbau- und Ablauforganisation sowie die Zertifizierungstätigkeit,
4. die Vorkehrungen und Maßnahmen zur Sicherstellung und Aufrechterhaltung des Betriebes, insbesondere bei Notfällen,
5. die Verfahren zur Beurteilung und Sicherstellung der Zuverlässigkeit des eingesetzten Personals und
6. eine Abschätzung und Bewertung verbleibender Sicherheitsrisiken.

§ 3 Identitätsprüfung und Attributsnachweise

- (1) Der Zertifizierungsdiensteanbieter hat die Identifizierung des Antragstellers nach § 5 Abs. 1 des Signaturgesetzes anhand des Personalausweises oder eines Reisepasses, der auf eine Person mit Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union oder eines Staates des Europäischen Wirtschaftsraumes ausgestellt worden ist, oder anhand von Dokumenten mit gleichwertiger Sicherheit vorzunehmen. Soweit ein Antrag auf ein qualifiziertes Zertifikat mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments des Antragstellers gestellt wird, kann der Zertifizierungsdiensteanbieter von einer erneuten Identifizierung absehen. Die Identifizierung ist vor Übergabe des qualifizierten Zertifikats und vor Einstellung in das Zertifikatsverzeichnis gemäß § 4 Abs. 1 vorzunehmen.
- (2) Sollen nach § 5 Abs. 2 des Signaturgesetzes in ein qualifiziertes Zertifikat Attribute aufgenommen werden, muss die nach § 5 Abs. 2 Satz 2 oder Satz 4 oder Abs. 3 Satz 2 des Signaturgesetzes erforderliche Einwilligung oder Bestätigung mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments oder schriftlich vorliegen. Die dritte Person oder die für die berufsbezogenen oder sonstigen Angaben zur Person zuständige Stelle ist mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments oder schriftlich über den Inhalt des qualifizierten Zertifikates zu unterrichten und auf die Möglichkeit der Sperrung hinzuweisen.

§ 4 Führung eines Zertifikatsverzeichnisses

- (1) Der Zertifizierungsdiensteanbieter hat die von ihm ausgestellten qualifizierten Zertifikate, vorbehaltlich eines späteren Zeitpunktes nach § 5 Abs. 2 Satz 2, ab dem Zeitpunkt ihrer Ausstellung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens fünf weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates endet, in einem Verzeichnis gemäß den Vorgaben nach § 5 Abs. 1 Satz 2 des Signaturgesetzes zu führen.

- (2) Ein akkreditierter Zertifizierungsdiensteanbieter hat die von ihm ausgestellten qualifizierten Zertifikate, vorbehaltlich eines späteren Zeitpunktes nach § 5 Abs. 2 Satz 2, ab dem Zeitpunkt ihrer Ausstellung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens 30 weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates endet, in einem Verzeichnis gemäß den Vorgaben nach § 5 Abs. 1 Satz 2 des Signaturgesetzes zu führen.
- (3) Im Falle der Übernahme von qualifizierten Zertifikaten nach § 13 Abs. 1 Satz 2 des Signaturgesetzes gelten die Absätze 1 und 2 entsprechend.

§ 5 Einzelne Sicherheitsvorkehrungen des Zertifizierungsdiensteanbieters

- (1) Der Zertifizierungsdiensteanbieter hat durch geeignete Maßnahmen sicherzustellen, dass Signaturschlüssel nur auf der jeweiligen sicheren Signaturerstellungseinheit oder bei ihm oder einem anderen Zertifizierungsdiensteanbieter unter Nutzung von technischen Komponenten nach § 17 Abs. 3 Nr. 1 des Signaturgesetzes erzeugt und auf sichere Signaturerstellungseinheiten übertragen werden. Soweit er auch Wissensdaten zur Identifikation des Signaturschlüssel-Inhabers gegenüber einer sicheren Signaturerstellungseinheit oder technische Komponenten zur Erfassung biometrischer Merkmale und Übertragung von Referenzdaten auf die sichere Signaturerstellungseinheit bereitstellt, hat er auch Vorkehrungen zu treffen, um die Geheimhaltung der Identifikationsdaten zu gewährleisten und deren Speicherung außerhalb der jeweiligen sicheren Signaturerstellungseinheit nach Einbringen in dieselbe auszuschließen.
- (2) Der Zertifizierungsdiensteanbieter hat von ihm bereitgestellte Signaturschlüssel und Identifikationsdaten dem Signaturschlüssel-Inhaber auf der sicheren Signaturerstellungseinheit persönlich zu übergeben und die Übergabe von diesem schriftlich oder als mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenes elektronisches Dokument bestätigen zu lassen, es sei denn, es wird schriftlich oder mittels einer qualifizierten elektronischen Signatur nach dem Signaturgesetz eine andere Übergabe vereinbart. Erst nachdem der Signaturschlüssel-Inhaber den Erhalt der sicheren Signaturerstellungseinheit gegenüber dem Zertifizierungsdiensteanbieter bestätigt hat, darf das zugehörige qualifizierte Zertifikat nach § 5 Abs. 1 Satz 2 und 3 des Signaturgesetzes nachprüfbar und, soweit vereinbart, abrufbar gehalten werden.
- (3) Der Zertifizierungsdiensteanbieter hat sich zur Erfüllung der Voraussetzungen nach § 5 Abs. 5 des Signaturgesetzes von der Zuverlässigkeit von Personen, die am Zertifizierungsverfahren mitwirken, auf geeignete Weise zu überzeugen. Er kann hierzu insbesondere die Vorlage eines Führungszeugnisses nach § 30 Abs. 1 des Bundeszentralregistergesetzes verlangen. Unzuverlässige Personen sind vom Zertifizierungsverfahren auszuschließen. Der Zertifizierungsdiensteanbieter hat sich darüber hinaus anhand der Herstellerangaben oder in anderer geeigneter Weise von der Eignung der von ihm eingesetzten Produkte für qualifizierte elektronische Signaturen zu überzeugen und Vorkehrungen zu treffen, um diese vor unbefugtem Zugriff zu schützen.

§ 6 Ausgestaltung der Unterrichtung

Die Unterrichtung des Antragstellers nach § 6 Abs. 1 des Signaturgesetzes hat in allgemein verständlicher Sprache zu erfolgen und sich mindestens auf Folgendes zu erstrecken:

1. die Aufbewahrung und Anwendung der sicheren Signaturerstellungseinheit und geeignete Maßnahmen im Verlustfalle oder bei Verdacht des Mißbrauchs,
2. die Geheimhaltung von persönlichen Identifikationsnummern oder anderen Daten zur Identifikation des Signaturschlüssel-Inhabers gegenüber der sicheren Signaturerstellungseinheit,
3. die erforderlichen Sicherheitsmaßnahmen bei Erzeugung und Prüfung einer qualifizierten elektronischen Signatur,
4. die Möglichkeit von Beschränkungen in qualifizierten Zertifikaten nach § 7 Abs. 1 Nr. 7 des Signaturgesetzes,
5. die Notwendigkeit, Daten mit einer qualifizierten elektronischen Signatur neu zu signieren, falls die Signatur durch Zeitablauf ihren Sicherheitswert verliert,
6. die Existenz eines freiwilligen Akkreditierungssystems,
7. die dem Antragsteller zur Verfügung stehenden Beschwerde- und Schlichtungsmög-

- lichkeiten sowie die Einzelheiten der Inanspruchnahme solcher Verfahren und
8. das Verfahren der Sperrung nach § 7. Die Informationen sind auf Antrag auch Dritten zur Verfügung zu stellen.

§ 7 Sperrung von qualifizierten Zertifikaten

- (1) Der Zertifizierungsdiensteanbieter hat den nach § 8 des Signaturgesetzes zur Sperrung Berechtigten eine Rufnummer bekannt zu geben, unter der diese unverzüglich eine Sperrung der qualifizierten Zertifikate veranlassen können.
- (2) Der Zertifizierungsdiensteanbieter hat sich vor Sperrung auf geeignete Weise von der Identität des zur Sperrung Berechtigten zu überzeugen. Die Sperrung von qualifizierten Zertifikaten ist mit Angabe des Datums und der zu diesem Zeitpunkt gültigen gesetzlichen Zeit im Zertifikatsverzeichnis nach § 4 eindeutig kenntlich zu machen.

§ 8 Umfang der Dokumentation

- (1) Die Dokumentation nach § 10 des Signaturgesetzes hat sich auf das Sicherheitskonzept, einschließlich aller Änderungen, die Unterlagen zur Fachkunde der im Betrieb tätigen Personen und die vertraglichen Vereinbarungen mit den Antragstellern zu erstrecken.
- (2) Zum jeweiligen Antragsteller sind mindestens folgende Angaben und Unterlagen zu dokumentieren:
 1. eine Ablichtung des vorgelegten Ausweises oder andere Identitätsnachweise,
 2. ein vergebenes Pseudonym,
 3. der Nachweis über die Unterrichtung des Antragstellers nach § 6 des Signaturgesetzes,
 4. die Nachweise über die Einwilligungen der Berechtigten nach § 5 Abs. 2 Satz 2 und 4 und Abs. 3 Satz 2 des Signaturgesetzes,
 5. die Bestätigungen der zuständigen Stellen nach § 5 Abs. 2 Satz 2 des Signaturgesetzes,
 6. die ausgestellten qualifizierten Zertifikate mit dem jeweiligen Zeitpunkt der Ausstellung und der Übergabe sowie der Zeitpunkt der Einstellung in das Zertifikatsverzeichnis,
 7. die Sperrung von qualifizierten Zertifikaten,
 8. Auskünfte nach § 14 Abs. 2 Satz 2 des Signaturgesetzes und
 9. die Übergabebestätigungen für Signaturschlüssel und Identifikationsdaten nach § 5 Abs. 2 Satz 1 oder die Erklärung des Signaturschlüssel-Inhabers, wenn er eine andere Übergabe verlangt hat, und gegebenenfalls einen anderen Nachweis.
- (3) Die Dokumentation ist vorbehaltlich des Satzes 3 mindestens für den nach § 4 Abs. 1 genannten Zeitraum und bei akkreditierten Zertifizierungsdiensteanbietern mindestens für den nach § 4 Abs. 2 genannten Zeitraum aufzubewahren. Im Falle eines Gerichtsverfahrens, in dem der Nachweis der Zertifizierung von Belang ist, ist unbeschadet des Satzes 1 die Dokumentation mindestens bis zum rechtskräftigen Abschluss des Verfahrens aufzubewahren. Die Dokumentation von Auskünften nach § 14 Abs. 2 Satz 2 des Signaturgesetzes ist zwölf Monate aufzubewahren.

§ 9 Ausgestaltung der Deckungsvorsorge

- (1) Die Deckungsvorsorge nach § 12 des Signaturgesetzes kann erbracht werden
 1. durch eine Haftpflichtversicherung bei einem im Geltungsbereich dieses Gesetzes zum Geschäftsbetrieb befugten Versicherungsunternehmen oder
 2. durch eine Freistellungs- oder Gewährleistungsverpflichtung eines im Geltungsbereich dieses Gesetzes zum Geschäftsbetrieb befugten Kreditinstituts, wenn gewährleistet ist, dass sie einer Haftpflichtversicherung vergleichbare Sicherheit bietet.
- (2) Soweit die Deckungsvorsorge durch eine Versicherung nach Absatz 1 Nr. 1 erbracht wird, gelten die folgenden Bestimmungen:
 1. Auf diese Versicherung finden § 158b Abs. 2 und die §§ 158c bis 158k des Gesetzes über den Versicherungsvertrag Anwendung. Zuständige Behörde nach § 158c Abs. 2 des Gesetzes über den Versicherungsvertrag ist die Behörde nach § 66 des Telekommunikationsgesetzes.
 2. Die Mindestversicherungssumme muss 2,5 Millionen Euro für den einzelnen Versicherungsfall betragen. Versicherungsfall ist jedes auf den Einzelfall bezogene haftungsaus-

lösende Ereignis im Sinne des § 12 Satz 1 des Signaturgesetzes, unabhängig von der Anzahl der dadurch ausgelösten Schadensfälle. Eine Vereinbarung, wonach ein Fehler, der sich in mehreren Zertifikaten, Zeitstempeln oder in der Auskunft nach § 5 Abs. 1 Satz 2 des Signaturgesetzes auswirkt, als ein Versicherungsfall gilt, ist nicht zulässig. Wird eine Jahreshöchstleistung für alle in einem Versicherungsjahr verursachten Schäden vereinbart, muss sie mindestens das Vierfache der Mindestversicherungssumme betragen.

3. Der räumliche Geltungsbereich des Versicherungsschutzes kann auf den Geltungsbereich der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. EG 2000, Nr. L 13 S. 2) beschränkt werden.
4. Von der Versicherung kann die Leistung nur ausgeschlossen werden für Ersatzansprüche aus vorsätzlich begangener Pflichtverletzung des Zertifizierungsdiensteanbieters oder der Personen, für die er einzustehen hat.
5. Die Vereinbarung eines Selbstbehaltes bis zu 1 Prozent der Mindestversicherungssumme ist zulässig.

§ 10 Einstellen der Tätigkeit

- (1) Der Zertifizierungsdiensteanbieter soll die Unterrichtung der zuständigen Behörde nach § 13 Abs. 1 Satz 1 des Signaturgesetzes spätestens zwei Monate vor Einstellung des Betriebes vornehmen.
- (2) Der Zertifizierungsdiensteanbieter soll die Unterrichtung der Signaturschlüssel-Inhaber nach § 13 Abs. 1 Satz 3 des Signaturgesetzes mindestens zwei Monate vor Betriebsaufgabe vornehmen. Er hat den Signaturschlüssel-Inhabern mitzuteilen, ob ein anderer Zertifizierungsdiensteanbieter die Zertifikate übernimmt, und diesen zu benennen.

§ 11 Freiwillige Akkreditierung

- (1) Der Antrag auf Akkreditierung nach § 15 Abs. 1 des Signaturgesetzes ist schriftlich oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments zu stellen. Der Antrag auf freiwillige Akkreditierung gilt als Anzeige nach § 1, wenn die dort genannten Voraussetzungen erfüllt sind.
- (2) Die Nachweise nach § 15 Abs. 1 Satz 2, Abs. 2 Satz 2 und Abs. 7 des Signaturgesetzes sind durch Vorlage der Ergebnisse der Prüf- und Bestätigungsstelle in schriftlicher Form oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments zu erbringen. Die regelmäßigen Prüfungen nach § 15 Abs. 2 Satz 2 des Signaturgesetzes sind im Abstand von drei Jahren durchzuführen. Der Prüfbericht und die Bestätigung darüber, dass die Anforderungen des Signaturgesetzes und dieser Verordnung weiterhin in vollem Umfang erfüllt werden, ist der zuständigen Behörde unaufgefordert vorzulegen.
- (3) Bei der Prüfung und Bestätigung der Sicherheit von Produkten für qualifizierte elektronische Signaturen nach § 15 Abs. 7 Satz 1 des Signaturgesetzes sind die Vorgaben des Abschnitts I der Anlage 1 zu dieser Verordnung zu beachten.

§ 12 Festsetzung und Erhebung von Kosten

- (1) Die gebührenpflichtigen Tatbestände für Amtshandlungen nach § 22 des Signaturgesetzes ergeben sich aus der Anlage 2 zu dieser Verordnung. Auslagen werden nach § 10 des Verwaltungskostengesetzes erhoben. Für den Widerruf oder die Rücknahme oder die Ablehnung eines Antrags oder einer Verwaltungshandlung werden Gebühren nach Maßgabe des § 15 des Verwaltungskostengesetzes erhoben.
- (2) Für die Stundensätze nach Nummer 2 der Anlage 2 zu dieser Verordnung ist für jede angefangene Viertelstunde ein Viertel dieser Stundensätze zu berechnen. Werden öffentliche Leistungen durch Angehörige der zuständigen Behörde außerhalb der Behörde erbracht, so sind Gebühren ferner zu berechnen, die innerhalb der üblichen Arbeitszeit liegen oder von der zuständigen Behörde besonders abgegolten werden, sowie für Wartezeiten, die der Kostenschuldner verursacht hat.

§ 13 Festsetzung und Erhebung von Beiträgen

- (1) Die Beiträge nach § 22 Abs. 2 Satz 1 des Signaturgesetzes berechnen sich nach dem hierfür erforderlichen Personal- und Sachaufwand der zuständigen Behörde unter Einschluss des

Aufwandes für Investitionen. Der Beitragssatz beträgt 0,48 Euro für jedes vom Beitragspflichtigen ausgestellte qualifizierte Zertifikat. Der auf das Allgemeininteresse entfallende Kostenanteil wurde beitragsmindernd berücksichtigt. Die Anteile am verbleibenden Aufwand werden den Beitragspflichtigen entsprechend der Zahl der von ihnen ausgestellten qualifizierten Zertifikate, die nach § 4 Abs. 1 im Zertifikatsverzeichnis zu führen sind, zugeordnet. Die Beitragspflichtigen haben der zuständigen Behörde die Zahl der Zertifikate nach Satz 2 jährlich, spätestens am 31. Januar des Folgejahres mitzuteilen. Kommt ein Beitragspflichtiger der Verpflichtung nach Satz 5 nicht nach, kann die zuständige Behörde eine Schätzung der ausgestellten qualifizierten Zertifikate eines Beitragspflichtigen vornehmen.

- (2) Die Kosten des Investitionsaufwandes werden entsprechend den jeweils gültigen steuerlichen Regelungen zur Abschreibung von Investitionsgütern festgelegt.
- (3) Für die Beiträge nach § 22 Abs. 2 Satz 2 des Signaturgesetzes gelten die Regelungen der Absätze 1 und 2, mit Ausnahme des Absatzes 1 Satz 4, entsprechend. Die Anteile am verbleibenden Aufwand nach Absatz 1 Satz 1 werden den Beitragspflichtigen entsprechend der Zahl der von ihnen ausgestellten qualifizierten Zertifikate, die nach § 4 Abs. 2 im Zertifikatsverzeichnis zu führen sind, zugeordnet.
- (4) Die Beitragspflicht nach § 22 Abs. 2 Satz 1 des Signaturgesetzes beginnt mit dem Monat der Anzeige nach § 4 Abs. 3 des Signaturgesetzes, die Beitragspflicht nach § 22 Abs. 2 Satz 2 des Signaturgesetzes mit dem Monat der Akkreditierung. Die Beitragspflicht endet mit Ablauf des Monats der Einstellung der Tätigkeit nach § 13 Abs. 1 des Signaturgesetzes sowie bei freiwilliger Akkreditierung auch mit Ablauf des Monats des Widerrufs oder der Rücknahme einer Akkreditierung nach § 15 Abs. 5 des Signaturgesetzes. Der Beitrag wird jährlich erhoben. Maßgeblich ist das Kalenderjahr. Besteht die Beitragspflicht nicht das volle Kalenderjahr, so ist der Beitrag anteilig zu berechnen; die Sätze 1 und 2 gelten entsprechend. Die Beiträge werden nach den Vorschriften des Verwaltungsvollstreckungsgesetzes beigetrieben.

§ 14 Inhalt und Gültigkeitsdauer von qualifizierten Zertifikaten

- (1) Die Angaben nach § 7 Abs. 1 des Signaturgesetzes in einem qualifizierten Zertifikat müssen eindeutig sein.
- (2) Ein qualifiziertes Attribut-Zertifikat nach § 7 Abs. 2 des Signaturgesetzes muss außer einer eindeutigen Referenz auf das zugrunde liegende qualifizierte Zertifikat mindestens folgende Angaben enthalten und eine qualifizierte elektronische Signatur des Zertifizierungsdiensteanbieters tragen:
 1. die Bezeichnung der Algorithmen, mit denen der Signaturprüfchlüssel des Zertifizierungsdiensteanbieters benutzt werden kann,
 2. die Nummer des Attribut-Zertifikates,
 3. den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist,
 4. Angaben, dass es sich um ein qualifiziertes Zertifikat handelt, und
 5. ein oder mehrere Attribute nach § 5 Abs. 2 des Signaturgesetzes.
- (3) Die Gültigkeitsdauer eines qualifizierten Zertifikates darf höchstens fünf Jahre betragen und den Zeitraum der Eignung der eingesetzten Algorithmen und zugehörigen Parameter nicht überschreiten. Die Gültigkeit eines qualifizierten Attribut-Zertifikates endet spätestens mit der Gültigkeit des qualifizierten Zertifikates, auf das es Bezug nimmt.

§ 15 Anforderungen an Produkte für qualifizierte elektronische Signaturen

- (1) Sichere Signaturerstellungseinheiten nach § 17 Abs. 1 Satz 1 des Signaturgesetzes müssen gewährleisten, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann. Der Signaturschlüssel darf nicht preisgegeben werden. Bei Nutzung biometrischer Merkmale muss hinreichend sichergestellt sein, dass eine unbefugte Nutzung des Signaturschlüssels ausgeschlossen ist und eine dem wissensbasierten Verfahren gleichwertige Sicherheit gegeben sein. Die zur Erzeugung und Übertragung von Signaturschlüsseln erforderlichen technischen Komponenten nach § 17 Abs. 1 Satz 2 oder Abs. 3 Nr. 1 des Signaturgesetzes müssen gewährleisten, dass aus einem Signaturprüfchlüssel oder einer Signatur nicht der Signaturschlüssel errechnet werden kann und die Signaturschlüssel nicht dupliziert

werden können.

- (2) Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass
 1. bei der Erzeugung einer qualifizierten elektronischen Signatur
 - a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,
 - b) eine Signatur nur durch die berechtigt signierende Person erfolgt,
 - c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird und
 2. bei der Prüfung einer qualifizierten elektronischen Signatur
 - a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und
 - b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.
- (3) Technische Komponenten nach § 17 Abs. 3 des Signaturgesetzes müssen gewährleisten, dass die Sperrung eines qualifizierten Zertifikates nicht unbemerkt rückgängig gemacht werden kann und die Auskünfte auf ihre Echtheit überprüft werden können. Die Auskünfte nach Satz 1 müssen beinhalten, ob die nachgeprüften qualifizierten Zertifikate im Verzeichnis der qualifizierten Zertifikate zum angegebenen Zeitpunkt vorhanden und ob sie nicht gesperrt waren. Nur nachprüfbar gehaltene qualifizierte Zertifikate dürfen nicht öffentlich abrufbar sein. Im Falle des § 17 Abs. 3 Nr. 3 des Signaturgesetzes muss gewährleistet sein, dass die zum Zeitpunkt der Erzeugung des qualifizierten Zeitstempels gültige gesetzliche Zeit unverfälscht in diesen aufgenommen wird.
- (4) Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.
- (5) Eine Herstellererklärung nach § 17 Abs. 4 des Signaturgesetzes muss
 1. den Aussteller und das Produkt genau bezeichnen und
 2. genaue Angaben darüber enthalten, welche Anforderungen des Signaturgesetzes und dieser Verordnung im Einzelnen erfüllt sind.

Bei der Prüfung und Bestätigung der Sicherheit von Produkten nach § 17 Abs. 1 und 3 Nr. 1 des Signaturgesetzes sind die Vorgaben des Abschnitts II der Anlage 1 zu dieser Verordnung zu beachten.

- (6) Soweit im Rahmen des Verfahrens nach Artikel 3 Abs. 5 und Artikel 9 der Richtlinie 1999/93/EG in der jeweils geltenden Fassung Referenznummern für allgemein anerkannte Normen für Produkte für qualifizierte elektronische Signaturen festgelegt und im Amtsblatt der Europäischen Gemeinschaften veröffentlicht werden, haben diese abweichend von den Absätzen 1 bis 5 Geltung, mit Ausnahme der Produkte nach § 15 Abs. 7 des Signaturgesetzes. Die zuständige Behörde veröffentlicht im Bundesanzeiger die aktuell gültigen Anforderungen auf Grund der Festlegungen nach Satz 1.

§ 16 Verfahren der Anerkennung sowie der Tätigkeit von Prüf- und Bestätigungsstellen

- (1) Ein Antrag einer Prüf- und Bestätigungsstelle nach § 18 Abs. 1 des Signaturgesetzes muss Folgendes umfassen:
 1. Namen und Anschrift des Antragstellers und seiner gesetzlichen Vertreter,
 2. aktuelle Führungszeugnisse nach § 30 Abs. 5 des Bundeszentralregistergesetzes des Antragstellers nach Nummer 1 und seiner gesetzlichen Vertreter,
 3. einen aktuellen Handelsregisterauszug oder eine vergleichbare Unterlage,
 4. Belege zum Nachweis der finanziellen Unabhängigkeit, insbesondere über Mindestkapital und vergleichbare Sicherheiten,
 5. Belege zum Nachweis der erforderlichen technischen, administrativen und juristischen Fachkunde nach § 18 Abs. 1 Satz 1 des Signaturgesetzes und
 6. eine Erklärung, auf welche gesetzliche Tätigkeiten des Signaturgesetzes sich der Antrag bezieht.
- (2) Für eine Anerkennung als Bestätigungsstelle für Tätigkeiten nach § 15 Abs. 7 und § 17 Abs. 4 Satz 1 des Signaturgesetzes muss der Antragsteller nachweisen, dass er über ausreichende Erfahrungen in der Anwendung der Prüfkriterien nach Anlage 1 zu dieser Verordnung ver-

- fügt. Er muss außerdem darlegen, wie er eine geeignete Überwachung der Prüftätigkeit sicherstellen wird.
- (3) Die für die Tätigkeit als Bestätigungsstelle oder Prüf- und Bestätigungsstelle nach § 18 Abs. 1 des Signaturgesetzes und der Entscheidung der Kommission 2000/709/EG vom 6. November 2000 (ABl. EG Nr. L 289 S. 42) über die Mindestkriterien gemäß Artikel 3 Abs. 4 der Richtlinie 1999/93/EG erforderliche
 1. Zuverlässigkeit besitzt, wer auf Grund seiner persönlichen Eigenschaften, seines Verhaltens und seiner Fähigkeiten zur ordnungsgemäßen Erfüllung der ihm obliegenden Aufgaben geeignet ist,
 2. Unabhängigkeit besitzt, wer keinem wirtschaftlichen, finanziellen oder sonstigen Druck unterliegt, der sein Urteil beeinflussen oder das Vertrauen in die unparteiische Aufgabewahrnehmung in Frage stellen kann,
 3. Fachkunde besitzt, wer auf Grund seiner Ausbildung, beruflichen Bildung und praktischen Erfahrung zur ordnungsgemäßen Erfüllung der ihm obliegenden Aufgaben geeignet ist.
 - (4) Der Betreiber einer Bestätigungsstelle oder Prüf- und Bestätigungsstelle nach § 18 des Signaturgesetzes hat sich von der Zuverlässigkeit und Fachkunde von Personen, die an der Prüfung oder Bestätigung mitwirken, auf geeignete Weise zu überzeugen. Er kann von diesen Personen die Vorlage eines Führungszeugnisses nach § 30 Abs. 1 des Bundeszentralregistergesetzes verlangen.
 - (5) Die zuständige Behörde veröffentlicht im Bundesanzeiger die Einzelheiten zu den Anforderungen nach den Absätzen 1 bis 4 und den Mindestkriterien nach Artikel 3 Abs. 4 der Richtlinie 1999/93/EG.

§ 17 Zeitraum und Verfahren zur langfristigen Datensicherung

Daten mit einer qualifizierten elektronischen Signatur sind nach § 6 Abs. 1 Satz 2 des Signaturgesetzes neu zu signieren, wenn diese für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Falle sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.

§ 18 Verfahren zur Feststellung der gleichwertigen Sicherheit von ausländischen elektronischen Signaturen und Produkten

- (1) Ein Zertifizierungsdiensteanbieter, der nach § 23 Abs. 1 Satz 2 Nr. 2 des Signaturgesetzes für qualifizierte Zertifikate mit Rechtswirkung nach Artikel 5 Abs. 1 der Richtlinie 1999/93/EG eines außerhalb des Europäischen Wirtschaftsraumes (Drittstaat) niedergelassenen Zertifizierungsdiensteanbieters entsteht, hat dies der zuständigen Behörde spätestens zu dem Zeitpunkt, zu dem diese Zertifikate im Geltungsbereich des Signaturgesetzes rechtswirksam werden sollen, schriftlich oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments anzuzeigen. Er hat dafür Sorge zu tragen, dass die qualifizierten Zertifikate des ausländischen Zertifizierungsdiensteanbieters und die darauf basierenden qualifizierten elektronischen Signaturen die Anforderungen des Signaturgesetzes und dieser Verordnung erfüllen und zu dem ausländischen Zertifizierungsdiensteanbieter die Unterlagen entsprechend § 1 Abs. 2 vorzulegen. § 2 gilt für die Angaben zu dem ausländischen Zertifizierungsdiensteanbieter entsprechend. Die zuständige Behörde hat den Namen des ausländischen Zertifizierungsdiensteanbieters unter Angabe des Zertifizierungsdiensteanbieters, der für seine qualifizierten Zertifikate eintritt, nach § 19 Abs. 6 des Signaturgesetzes abrufbar zu halten.
- (2) Die gleichwertige Sicherheit ausländischer elektronischer Signaturen nach § 23 Abs. 2 des Signaturgesetzes ist gegeben, wenn die zuständige Behörde festgestellt hat, dass
 1. die Sicherheitsanforderungen an Zertifizierungsdiensteanbieter und Produkte für qualifizierte elektronische Signaturen,
 2. die Prüfungsmodalitäten für Zertifizierungsdiensteanbieter und Produkte für qualifizierte elektronische Signaturen sowie die Anforderungen an die Prüf- und Bestäti-

- gungsstellen und
3. das Akkreditierungs- und Aufsichtssystem eine gleichwertige Sicherheit bieten. Zur Feststellung der gleichwertigen Sicherheit kann die zuständige Behörde mit der zuständigen ausländischen Stelle die Verfahren zur Anerkennung vereinbaren, soweit nicht entsprechende überstaatliche oder zwischenstaatliche Vereinbarungen getroffen sind.
- (3) Die Gleichwertigkeit von Produkten nach § 23 Abs. 3 Satz 2 des Signaturgesetzes ist gegeben, wenn die zuständige Behörde diese nach entsprechender Anwendung der Vorgaben nach Absatz 2 festgestellt hat.
- (4) Die zuständige Behörde hat in ihr Verzeichnis nach § 16 Abs. 2 des Signaturgesetzes auch die qualifizierten Zertifikate für Signaturprüfchlüssel oberster ausländischer Zertifizierungsdiensteanbieter, die nach § 23 Abs. 2 des Signaturgesetzes als gleichwertig anerkannt sind, aufzunehmen. Sie hat die Anerkennung durch eine qualifizierte elektronische Signatur mit Anbieterakkreditierung nach § 15 des Signaturgesetzes zu bestätigen.

§ 19 Inkrafttreten, Außerkrafttreten

Diese Verordnung tritt am Tage nach der Verkündung in Kraft; gleichzeitig tritt die Signaturverordnung vom 22. Oktober 1997 (BGBl. I S. 2498), geändert durch die Verordnung vom 22. Juni 2000 (BGBl. I S. 981), außer Kraft.

Berlin, den 16. November 2001

Der Bundeskanzler
Gerhard Schröder

Der Bundesminister
für Wirtschaft und Technologie
Müller

Anlage 1

(zu § 11 Abs. 3, § 15 Abs. 5 und § 16 Abs. 2)

Vorgaben für die Prüfung von Produkten für qualifizierte elektronische Signaturen

- I. Zu § 11 Abs. 3 dieser Verordnung und nach § 15 Abs. 7 des Signaturgesetzes (freiwillige Akkreditierung)

1. Prüfungsvorgaben**1.1 Anforderungen an Prüftiefen**

Die Prüfung der Produkte für qualifizierte elektronische Signaturen nach Maßgabe des § 15 Abs. 7 und des § 17 Abs. 4 des Signaturgesetzes hat nach den „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ (Common Criteria for Information Technology Security Evaluation, BAnz. 1999 S. 1945, – ISO/IEC 15408) oder nach den „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik“ (ITSEC – GMBI vom 8. August 1992, S. 545) in der jeweils geltenden Fassung zu erfolgen.

Die Prüfung muss

- a) bei technischen Komponenten nach § 2 Nr. 12 Buchstabe a des Signaturgesetzes mindestens die Prüftiefe EAL 4 oder E 3 umfassen,
- b) bei sicheren Signaturerstellungseinheiten nach § 2 Nr. 10 des Signaturgesetzes mindestens die Prüftiefe EAL 4 oder E 3 umfassen,
- c)
 - i) bei technischen Komponenten für Zertifizierungsdienste nach § 2 Nr. 12 Buchstabe b und c des Signaturgesetzes, die außerhalb eines besonders gesicherten Bereichs („Trust-center“) eingesetzt werden, mindestens die Prüfstufe „EAL 4“ oder „E3“ umfassen,
 - ii) bei technischen Komponenten für Zertifizierungsdienste nach § 2 Nr. 12 Buchstabe b und c des Signaturgesetzes, die innerhalb eines besonders gesicherten Bereichs eingesetzt werden, mindestens die Prüfstufe „EAL 3“ oder „E 2“ umfassen,
- d) bei Signaturanwendungskomponenten nach § 2 Nr. 11 des Signaturgesetzes mindestens die Prüfstufe „EAL 3“ oder „E 2“ umfassen.

1.2 Anforderungen an Schwachstellenbewertung/Mechanismenstärke

Bei den Prüfstufen „EAL 4“ und bei „EAL 3“ gemäß Abschnitt I Nr. 1.1 Buchstabe a bis c i) und Buchstabe d ist ergänzend zu den bei dieser Prüfstufe vorgeschriebenen Maßnahmen gegen ein hohes Angriffspotenzial zu prüfen und eine vollständige Missbrauchsanalyse durchzuführen. Die Stärke der Sicherheitsmechanismen muss bei allen Produkten gemäß Abschnitt I Nr. 1.1 Buchstabe a bis d im Fall „E 3“ und „E 2“ mit „hoch“ bewertet werden.

Abweichend hiervon genügt für den Mechanismus zur Identifikation durch biometrische Merkmale eine Bewertung der Sicherheitsmechanismen mit „mittel“, wenn diese zusätzlich zur Identifikation durch Wissensdaten genutzt werden.

1.3 Anforderungen an Algorithmen

Die Algorithmen und zugehörigen Parameter müssen nach Abschnitt I Nr. 1.2 dieser Anlage als geeignet beurteilt sein.

2. Algorithmen – Veröffentlichung und Neubestimmung der Eignung

Die zuständige Behörde veröffentlicht im Bundesanzeiger eine Übersicht über die Algorithmen und zugehörigen Parameter, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die

Eignung jeweils gilt. Der Zeitpunkt soll mindestens sechs Jahre nach dem Zeitpunkt der Bewertung und Veröffentlichung liegen. Die Eignung ist jährlich sowie bei Bedarf neu zu bestimmen. Die Eignung ist gegeben, wenn innerhalb des bestimmten Zeitraumes nach dem Stand von Wissenschaft und Technik eine nicht feststellbare Fälschung von qualifizierten elektronischen Signaturen oder Verfälschung von signierten Daten mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann. Die Eignung wird nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik unter Berücksichtigung internationaler Standards festgestellt. Experten aus Wirtschaft und Wissenschaft sind zu beteiligen.

3. Sicherheitsbestätigungen für Signaturprodukte

In der Bestätigung der Erfüllung der Anforderungen für Produkte für qualifizierte elektronische Signaturen ist anzugeben,

- a) für welche Anforderungen nach § 17 des Signaturgesetzes und nach § 15 dieser Verordnung die Bestätigung gilt und unter welchen Einsatzbedingungen,
- b) welche Algorithmen und zugehörigen Parameter nach Abschnitt I Nr. 2 eingesetzt und bis zu welchem Zeitpunkt diese mindestens geeignet sind sowie
- c) nach welcher Stufe die Produkte geprüft wurden und welche Mechanismenstärke erreicht wurde.

Eine Ausfertigung des Prüfberichtes, der Bewertung durch die Bestätigungsstelle und der Bestätigung ist bei der zuständigen Behörde zu hinterlegen. Auf Anforderung sind dieser auch alle weiteren Prüfunterlagen vorzulegen. Sie kann bei Anhaltspunkten für Mängel bei Prüfungen oder bei bestätigten Produkten sowie stichprobenweise Gutachten eines unabhängigen Dritten darüber einholen, ob die Produkte gemäß dieser Anlage geprüft wurden und ob diese die Anforderungen des Signaturgesetzes und der Signaturverordnung erfüllen. Betroffene Hersteller,

Vertreiber und Prüfstellen haben die dafür erforderliche Unterstützung zu gewähren. Wird diese nicht gewährt oder stellt sich heraus, dass bestätigte Produkte nicht ausreichend geprüft wurden oder Anforderungen nicht erfüllen, so kann die zuständige Behörde erteilte Bestätigungen für ungültig erklären.

4. Veröffentlichung der Sicherheitsbestätigung für Produkte

Die zuständige Behörde hat Produkte für qualifizierte elektronische Signaturen, die von einer nach § 18 des Signaturgesetzes anerkannten Stelle eine Bestätigung gemäß Abschnitt I Nr. 3 erhalten haben, im Bundesanzeiger zu veröffentlichen. Dabei ist anzugeben, bis zu welchem Zeitpunkt die Bestätigung mindestens gilt. Wird eine Bestätigung für ungültig erklärt, so hat die zuständige Behörde dies unter Angabe des Zeitpunktes, ab dem diese Maßnahme gilt, ebenfalls im Bundesanzeiger zu veröffentlichen.

- II. Zu § 15 Abs. 5 dieser Verordnung und nach § 17 Abs. 1 und 3 Nr. 1 des Signaturgesetzes (nach § 4 Abs. 3 des Signaturgesetzes angezeigte Zertifizierungsdiensteanbieter ohne freiwillige Akkreditierung)

Für die Prüfung von Produkten nach § 15 Abs. 5 gelten die Anforderungen nach Abschnitt I entsprechend.

Abweichend hiervon können

- Produkte zum Einsatz kommen, die den Normen nach § 15 Abs. 6 entsprechen,
- Produkte nach § 17 Abs. 2 und 3 Nr. 2 und 3 des Signaturgesetzes (bzw. nach Abschnitt I Nr. 1.1 Buchstabe c und d) zum Einsatz kommen, bei denen anstelle der Bestätigung eine Herstellererklärung nach § 17 Abs. 4 des Signaturgesetzes vorliegt.

Anlage 2

(zu § 12)

Kosten für Amtshandlungen nach § 22 Abs. 1 des Signaturgesetzes

1.1. Kosten nach § 22 Abs. 1 Nr. 1 des Signaturgesetzes

Kostennummer	Amtshandlung	Euro
1	Prüfung und Erteilung einer Akkreditierung nach § 15 Abs. 1 des Signaturgesetzes	Gebühr nach Zeitaufwand
2	Ablehnung eines Antrages auf Akkreditierung nach § 15 Abs. 4 des Signaturgesetzes oder Rücknahme oder Widerruf einer Akkreditierung nach § 15 Abs. 5 des Signaturgesetzes	Gebühr nach Zeitaufwand
3	Vollständige oder teilweise Zurückweisung eines Widerspruchs im Rahmen des Verfahrens nach § 15 Abs. 1 bis 6 des Signaturgesetzes	2 500
4	Überprüfung von Prüfberichten und Bestätigungen nach § 15 Abs. 2 des Signaturgesetzes	3 500
5	Maßnahmen im Falle des Widerrufs oder der Rücknahme einer Akkreditierung oder im Falle der Einstellung der Tätigkeit eines akkreditierten Zertifizierungsdiensteanbieters nach § 15 Abs. des Signaturgesetzes	Gebühr nach Zeitaufwand
6	Prüfungen und andere Maßnahmen nach § 19 des Signaturgesetzes	Gebühr nach Zeitaufwand

1.2. Kosten nach § 22 Abs. 1 Nr. 2 des Signaturgesetzes

Kostennummer	Amtshandlung	Euro
7	Ausstellung eines qualifizierten Zertifikates sowie dessen Sperrung nach § 16 Abs. 1 des Signaturgesetzes	500
8	Ausstellung einer Bescheinigung nach § 16 Abs. 3 des Signaturgesetzes	500

1.3. Kosten nach § 22 Abs. 1 Nr. 3 des Signaturgesetzes

Kostennummer	Amtshandlung	Euro
9	Erteilung einer Anerkennung als Bestätigungsstelle oder Prüf- und Bestätigungsstelle nach § 18 Abs. 1 des Signaturgesetzes nach a) § 15 Abs. 2 des Signaturgesetzes	2 500
10	b) § 15 Abs. 7 des Signaturgesetzes	2 500
11	c) § 17 Abs. 3 des Signaturgesetzes	1 000
12	Ablehnung eines Antrages auf Anerkennung oder Rücknahme oder Widerruf einer Anerkennung für Tätigkeiten nach a) § 15 Abs. 2 des Signaturgesetzes	2 500
13	b) § 15 Abs. 7 des Signaturgesetzes	2 500
14	c) § 17 Abs. 4 des Signaturgesetzes	1 000
15	Vollständige oder teilweise Zurückweisung eines Widerspruchs im Rahmen des Verfahrens nach § 18 Abs. 1 des Signaturgesetzes	1 000

1.4. Kosten nach § 22 Abs. 1 Nr. 4 des Signaturgesetzes

Kostennummer	Amtshandlung	Euro
16	Bearbeitung einer Anzeige nach § 4 Abs. 2 und 3 des Signaturgesetzes und erstmalige Überprüfung der Einhaltung des Signaturgesetzes und dieser Verordnung nach § 19 des Signaturgesetzes	Gebühr nach Zeitaufwand
17	Stichprobenartige Prüfungen im Rahmen der Aufsicht nach § 19 Abs. 1 des Signaturgesetzes im Falle der Feststellung eines Verstoßes gegen die für den Betrieb eines Zertifizierungsdienstes maßgeblichen Vorschriften des Signaturgesetzes oder dieser Verordnung	Gebühr nach Zeitaufwand
18	Anlassbezogene Prüfungen und andere Maßnahmen nach § 19 Abs. 1 des Signaturgesetzes im Falle eines Verstoßes gegen die für den Betrieb eines Zertifizierungsdienstes maßgeblichen Vorschriften des Signaturgesetzes oder dieser Verordnung	Gebühr nach Zeitaufwand

1.5. Kosten nach § 23 Abs. 1 des Signaturgesetzes

Kostennummer	Amtshandlung	Euro
19	Bearbeitung einer Anzeige nach § 18 Abs. 1 Satz 1 dieser Verordnung einschließlich der Aufnahme in das Zertifikatsverzeichnis nach § 18 Abs. 1 Satz 4 dieser Verordnung	Gebühr nach Zeitaufwand

2. Stundensätze und Km-Pauschale für Kfz-Einsatz

Kostennummer	Stundensatz/Km-Pauschale	Euro
20	Beamte des höheren Dienstes oder vergleichbare Angestellte	125
21	Beamte des gehobenen Dienstes oder vergleichbare Angestellte	95
22	Beamte des mittleren Dienstes oder vergleichbare Angestellte	69
23	Kraftfahrzeugeinsatz	0,70 Euro/km

A 2 Zahlentheorie

(Z1) Bezeichnung:

Mit N wird die Menge der **natürlichen Zahlen** $N = \{1, 2, 3, \dots\}$ bezeichnet.

Mit Z wird die Menge der **ganzen Zahlen** $Z = \{\dots -2, -1, 0, 1, 2, \dots\}$ bezeichnet.

(Z2) Definition:

Seien $a, b \in Z$ ganze Zahlen. a heißt ein **Teiler** von b , wenn ein $c \in Z$ existiert, so dass $a * c = b$ gilt.

(Z3) Definition:

Eine natürliche Zahl $p \in N$ mit $p \geq 2$ wird eine **Primzahl** genannt, wenn sie nur 1 und p als Teiler besitzt.

(Z4) Satz:

Die Zahl $\pi(n)$ der Primzahlen unterhalb n ist für große n näherungsweise durch

$$\pi(n) \approx \frac{n}{\ln(n)} \quad \text{gegeben.}$$

(Z5) Definition:

Der größte gemeinsame Teiler **ggT** zweier Zahlen a und b ist die größte natürliche Zahl, die a und b teilt.

(Z6) Definition:

Seien $a, b \in Z$ ganze Zahlen. a und b heißen **teilerfremd** oder prim zueinander, wenn $\text{ggT}(a, b) = 1$ ist.

(Z7) Definition:

Für eine natürliche Zahl n definieren wir $\Phi(n)$ als die Anzahl der zu n teilerfremden Zahlen, die nicht größer als n sind.

(Z8) Beispiel:

$\Phi(20) = 8$, da die zu 20 teilerfremden Zahlen ≤ 20 folgende 8 Zahlen sind: 1, 3, 7, 9, 11, 13, 17, 19.

(Z9) Bemerkung:

Ist p eine Primzahl, dann gilt $\Phi(p) = p - 1$, denn jede der $p - 1$ Zahlen $1, 2, \dots, p - 1$ sind teilerfremd zu p .

(Z10) Bemerkung:

Sind p und q zwei verschiedene Primzahlen, so ist $\Phi(pq) = (p - 1)(q - 1)$, denn es gibt $pq - 1$ Zahlen kleiner als pq , von denen nur die $q - 1$ Vielfachen von p und die $p - 1$ Vielfachen von q nicht teilerfremd zu pq sind. Da alle anderen Zahlen teilerfremd zu pq sind gilt $\Phi(pq) = pq - 1 - (q - 1) - (p - 1) = pq - q - p + 1 = (p - 1)(q - 1)$.

(Z11) Der Euklidische Algorithmus

Seien $a, b \in \mathbb{Z}$ ganze Zahlen mit $b > 0$. Dann gibt es eindeutig bestimmte ganze Zahlen q und r mit:

$$a = qb + r \quad \text{und} \quad 0 \leq r < b.$$

Es gilt weiterhin $\text{ggT}(a, b) = \text{ggT}(b, r)$.

Aus dieser Bemerkung folgt ein allgemeines Verfahren zur Berechnung des ggT zweier ganzer Zahlen a und b , der Euklidische Algorithmus..

Mit $a = r_0$ und $b = r_1$ folgt:

$$r_0 = q_1 r_1 + r_2 \quad \text{mit } 0 < r_2 < r_1 \quad \text{und } \text{ggT}(r_0, r_1) = \text{ggT}(r_1, r_2)$$

$$r_1 = q_2 r_2 + r_3 \quad \text{mit } 0 < r_3 < r_2 \quad \text{und } \text{ggT}(r_1, r_2) = \text{ggT}(r_2, r_3)$$

...

$$r_{n-2} = q_{n-1} r_{n-1} + r_n \quad \text{mit } 0 < r_n < r_{n-1} \quad \text{und } \text{ggT}(r_{n-2}, r_{n-1}) = \text{ggT}(r_{n-1}, r_n)$$

$$r_{n-1} = q_n r_n \quad \text{mit } \text{ggT}(r_{n-1}, r_n) = r_n$$

(Z12) Beispiel:

Sei $a = 792$ und $b = 75$.

$$792 = 10 * 75 + 42$$

$$75 = 1 * 42 + 33$$

$$42 = 1 * 33 + 9$$

$$33 = 3 * 9 + 6$$

$$9 = 1 * 6 + 3$$

$$6 = 2 * 3$$

Folgt $ggT(792,75) = 3$.

(Z13) Der erweiterte Euklidische Algorithmus

Sei $d = ggT(a,b)$. Dann existieren ganze Zahlen $x, y \in \mathbb{Z}$ mit

$$d = xa + yb.$$

(Z14) Eine solche Darstellung nennt man **Vielfachsummendarstellung** der Zahl $d = ggT(a,b)$. Diese wird mit Hilfe des Euklidischen Algorithmus berechnet.

$$\begin{aligned} d = r_n &= r_{n-2} - q_{n-1}r_{n-1} = r_{n-2} + (-q_{n-1})r_{n-1} \\ &= r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2}r_{n-2}) = (-q_{n-1})r_{n-3} + [1 - q_{n-2}q_{n-1}]r_{n-2} \\ &= [1 - q_{n-2}q_{n-1}](r_{n-4} - q_{n-3}r_{n-3}) - q_{n-1}r_{n-3} \\ &= [\dots]r_{n-4} + [\dots]r_{n-3} \\ &= \dots \\ &= xr_0 + yr_1 = xa + yb \end{aligned}$$

(Z15) Definition:

Der Modulo Operator gibt den Rest einer Division zweier ganzer Zahlen an,

z.B.: ist $8 \bmod 3 = 2$.

(Z16) Berechnung des geheimen Schlüssels des RSA Algorithmus

Sind a und b teilerfremde Zahlen $\text{ggT}(a,b) = 1$ so gibt es eine ganze Zahl $c \in \mathbb{Z}$ mit $bc \text{ MOD } a = 1$.

Dies folgt aus dem erweiterten Euklidischen Algorithmus:

$$\text{ggT}(a,b) = 1 = xa + yb$$

$$1 = (xa + yb) \text{ MOD } a = xa \text{ MOD } a + yb \text{ MOD } a = yb \text{ MOD } a$$

Mit $c = y$ folgt $bc \text{ MOD } a = 1$. c kann also mit Hilfe des erweiterten Euklidischen Algorithmus berechnet werden.

Der geheime Schlüssel d des RSA Algorithmus wird aus der Gleichung

$$ed \text{ MOD } \Phi(n) = 1 \text{ berechnet wobei } \text{ggT}(e, \Phi(n)) = 1.$$

Die Berechnung von d ist somit identisch mit der Berechnung von c .

(Z17) Bemerkung:

Die Implementierung und Berechnung des Euklidischen Algorithmus ist sehr einfach und effizient möglich. Dies gilt ebenso für den erweiterten Algorithmus. Somit ist die Berechnung des geheimen Schlüssels des RSA Algorithmus mit Computerunterstützung schnell und effizient lösbar.

(Z18) Definition:

Das **Hexadezimalsystem** oder Sechzehnersystem ist eine mathematische Methode zur Darstellung von beliebigen Zahlenwerten mit 16 Ziffern. Es werden die Ziffern 0 bis 9 und A bis F verwendet. Im Dezimalsystem entsprechen die Werte A bis F den Zahlenwerten 11 bis 16. Die Werte der Stellen entsprechen dabei 256, 16, 1 usw. Der Hexadezimalwert "1B" entspricht zum Beispiel im Dezimalsystem der 27.

Das Hexadezimalsystem wird meist zur übersichtlichen Darstellung von digitalisierten Informationen verwendet.

(Z19) ASCII Tabelle:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	TAB	LF	VT	FF	CR	SO	SI
1	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2		!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	

Tabelle 15 : ASCII Werte

Die Tabelle zeigt die ASCII Werte der 256 Zeichen im Hexadezimalsystem. Dabei repräsentiert die Reihe die erste Ziffer und die Spalte die Zweite. Das „Z“ befindet sich zum Beispiel in der Reihe 5 und in der Spalte A, dies ergibt den Hexadezimalwert 5A für „Z“. Im Binärsystem entspricht dies 01011011, da $BIN(5) = 0101$ und $BIN(A) = 1011$ ist.

Die ersten beiden Zeilen repräsentieren die **Control Codes**.

NUL (null)

SOH (start of heading)

STX (start of text)

ETX (end of text)

EOT (end of transmission) - Not the same as ETB

ENQ (enquiry)

ACK (acknowledge)

BEL (bell) Caused teletype machines to ring a bell. Causes a beep in many common terminals and terminal emulation programs.

BS (backspace) Moves the cursor (or print head) move backwards (left) one space.

TAB (horizontal tab) Moves the cursor (or print head) right to the next tab stop. The spacing of tab stops is dependent on the output device, but is often either 8 or 10.

LF (NL line feed, new line) Moves the cursor (or print head) to a new line. On Unix systems, moves to a new line

AND all the way to the left.

VT (vertical tab)

FF (form feed) Advances paper to the top of the next page (if the output device is a printer).

CR (carriage return) - Moves the cursor all the way to the left, but does not advance to the next line.

SO (shift out) - Switches output device to alternate character set.

SI (shift in) - Switches output device back to default character set.

DLE (data link escape)

DC2 (device control 2)

DC4 (device control 4)

SYN (synchronous idle)

ETB (end of transmission block) - Not the same as EOT

CAN (cancel)

SUB (substitute)

FS (file separator)

RS (record separator)

DC1 (device control 1)

DC3 (device control 3)

NAK (negative acknowledge)

EM (end of medium)

ESC (escape)

GS (group separator)

US (unit separator)

A 3 Zertifizierungsdiensteanbieter

Akkreditierte Zertifizierungsdiensteanbieter	RegTp Nr.	Genehmigung
Produktzentrum TeleSec der Deutschen Telekom AG	Z0001	22. Dezember 1998
Deutsche Post Signtrust	Z0002	23. Februar 2000
DATEV eG	Z0004	9. März 2001
Steuerberaterkammer Nürnberg	Z0005	9. März 2001
Medizon AG	Z0006	20. März 2001
Hanseatische Steuerberaterkammer Bremen	Z0007	21. Mai 2001
Steuerberaterkammer Saarland	Z0008	21. Mai 2001
Rechtsanwaltskammer Bamberg	Z0009	20. August 2001
Rechtsanwaltskammer Koblenz	Z0010	20. August 2001
Steuerberaterkammer Stuttgart	Z0011	20. August 2001
Steuerberaterkammer München	Z0012	20. August 2001
Steuerberaterkammer Berlin	Z0014	20. August 2001
AuthentiDate International AG	Z0015	09. November 2001
TC TrustCenter AG	Z0016	19. Dezember 2001
D-Trust GmbH	Z0017	08. März 2002
Steuerberaterkammer Niedersachsen	Z0018	02. September 2002
Hanseatische Rechtsanwaltskammer Hamburg	Z0019	02. September 2002
Rechtsanwaltskammer München	Z0020	05. November 2002
Steuerberaterkammer Brandenburg	Z0021	05. November 2002
Wirtschaftsprüferkammer	Z0022	21. November 2002
Rechtsanwaltskammer Berlin	Z0023	21. November 2002

Tabelle 16: Die akkreditierten Zertifizierungsdiensteanbieter laut RegTP²³¹

Angezeigte Zertifizierungsdiensteanbieter	Anzeige
D-Trust GmbH ²³²	22. Oktober 2001

Tabelle 17: Die angezeigten Zertifizierungsdiensteanbieter laut RegTP²³³

²³¹ Vgl. Webseite der Regulierungsbehörde. Online im Internet unter <http://www.regtp.de> Stand April 2003

²³² Veröffentlicht im Amtsblatt der RegTP Nr. 23 vom 28.11.2001, Seite 3484

²³³ Vgl. Webseite der Regulierungsbehörde. Online im Internet unter <http://www.regtp.de> Stand April 2003

Erklärung

Hiermit versichere ich, dass ich die Arbeit selbstständig verfasst und keine anderen als die angegebenen Hilfsmittel verwandt und die Stellen, die anderen Werken im Wortlaut oder dem Sinne nach entnommen sind, mit Quellenangaben kenntlich gemacht habe.

Giessen, im Juni 2003