

# StepOver Leitfaden zur e-Signatur

Step Over  
the next step in business

Step Over  
the next step in business

Leitfaden zur  
e-Signatur

Elektronische Signatur mit und ohne Zertifikat  
Elektronische Signatur mit eigenhändiger Unterschrift

In Zusammenarbeit mit

  
BUSINESS DEVELOPMENT INTERNATIONAL

und

  
SigLab®

Version 4.2  
Veröffentlichungsdatum 21. Oktober 2008

#### Kontakt:

StepOver GmbH  
Wollgrasweg 27  
D-70599 Stuttgart  
Tel.: 0700/StepOver  
[www.StepOver.de](http://www.StepOver.de)

### Inhalt

<b>1</b>	<b>Vorwort des Autors.....</b>	<b>6</b>
<b>2</b>	<b>Impressum.....</b>	<b>7</b>
<b>3</b>	<b>Einleitende Informationen.....</b>	<b>8</b>
3.1	Wer sollte diesen Leitfaden lesen?.....	8
3.2	Inhalt und Themen des Leitfadens.....	8
3.3	Elementare Kenntnisse - Womit sollte man beginnen.....	9
3.4	Neuigkeiten der Version 4.1.....	10
3.5	Neuigkeiten der Version 4.0.....	10
3.6	Neuigkeiten der Version 3.....	10
3.7	Begriffe - Unterzeichner statt Signaturschlüssel-Inhaber.....	11
3.8	Fortgeschrittene elektronische Signatur ohne Zertifikate möglich.....	12
3.9	Haftungsausschluß.....	12
<b>4</b>	<b>Grundlagen.....</b>	<b>13</b>
4.1	Differenzierung Elektronische Signatur – Geheime Dokumente.....	13
4.2	Was ist eine elektronische Signatur?.....	13
4.2.1	Beispiele für Willenserklärungen.....	14
4.2.2	Beispiele für Bestätigungen.....	14
4.3	Anforderungen an elektronische Signaturen.....	14
4.3.1	Identifizierungsmerkmal Public Key für zertifikatsbasierte Signaturen.....	15
4.3.2	Identifizierungsmerkmal Unterschrift für Signaturen ohne Zertifikat.....	15
4.4	Was sind Massensignaturen?.....	15
4.4.1	Beispiele für Massensignaturen.....	15
4.5	Was ist ein Zeitstempel?.....	15
4.5.1	Beispiele für Zeitstempel.....	16
<b>5</b>	<b>Anwendungsbeispiele für eine elektronische Signatur.....</b>	<b>16</b>
5.1	Massensignaturen zur elektronischen Übermittlung von Rechnungen.....	16
5.1.1	Hinweis für gescannte Rechnungen.....	17
5.2	Signaturen für gescannte Papierdokumente.....	17
5.3	Zeitstempel für elektronische Archivierung von Dokumenten.....	17
5.4	Zeitstempel als Ergänzung zu qualifizierten Signaturen.....	17
5.5	Individualsignaturen für Willenserklärungen, Verträge und Bestätigungen.....	18
5.5.1	Signieren ohne vorherige Registrierung des Unterzeichners.....	18
5.5.2	Signieren mit vorheriger Registrierung des Unterzeichners.....	18
<b>6</b>	<b>Gesetzliche Rahmenbedingungen.....</b>	<b>20</b>
6.1	Rechtliche Anforderungen an elektronische Signaturen.....	20
6.1.1	Gesetzliche Schriftform erfordert qualifizierte Signatur.....	20
6.1.1.1	Technische Anforderungen an die qualifizierte elektronische Signatur.....	21
6.1.1.2	Erstellungsdatum qualifizierter Signaturen nur mit Zeitstempel möglich.....	21
6.1.2	Formfreie Vereinbarungen ohne qualifizierte elektronische Signatur.....	22
6.1.2.1	Vereinbarte Schriftform.....	22
6.1.2.2	Nutzung nicht-qualifizierter Signaturen als Beweismittel.....	23
6.1.2.3	Fortgeschrittene Signaturen als Beweismittel.....	23
6.1.3	Einfache und fortgeschrittene elektronische Signatur ohne Zertifikat.....	24

6.1.3.1	Fortgeschrittene Signaturen benötigen asymmetrische Verschlüsselung.....	24
6.1.3.2	Beweiskraft von nicht-qualifizierten Signaturen .....	25
6.1.3.3	Zuordnung der elektronischen Signatur zum Unterzeichner .....	26
6.2	Elektronische Urkunden .....	26
6.2.1	Elektronische Dokumente mit qualifizierter Signatur .....	26
6.2.2	Eigenhändig unterschriebene elektronische Dokumente .....	26
6.3	Anpassung von Vertragsbestimmungen .....	28
6.4	Betrachtungen angeblicher Erfordernisse einer qualifizierten Signatur .....	28
6.4.1	Bundesdatenschutzgesetz § 4a.....	28
6.4.2	Ermächtigung zum Lastschriftinzug .....	29
6.4.3	Gesundheitsfragen und Kundenbelehrung.....	29
<b>7</b>	<b>Abweichungen des SigG zur EG-Signaturrichtlinie.....</b>	<b>30</b>
7.1	Signaturschlüssel-Inhaber anstatt Unterzeichner .....	30
7.2	1. Gesetz zur Änderung des Signaturgesetzes.....	30
7.3	BMVA Stellungnahme zu fortgeschrittenen Signaturen.....	31
<b>8</b>	<b>Vorhaltung signierter Dokumente als Beweismittel.....</b>	<b>33</b>
8.1	Gültigkeit und Beweisfähigkeit von elektronischen Signaturen .....	33
8.1.1	Gültigkeit von Zertifikaten .....	33
8.1.2	Gültigkeit von Verschlüsselungsalgorithmen.....	33
8.1.3	Erhaltung der Beweisfähigkeit von Signaturen .....	34
8.2	Ablage oder Archivierung von signierten Dokumenten?.....	34
8.2.1	Nachsignierung / Übersignierung .....	34
8.2.2	Nachsignierung oder revisionssicheres Archiv? .....	35
8.2.3	Erhalt von Formerfordernissen durch revisionssichere Archive?.....	35
<b>9</b>	<b>Biometrie und Unterschrift .....</b>	<b>36</b>
9.1	Biometrische Authentifizierungsverfahren für qualifizierte Signaturen .....	36
9.2	Eigenhändige Unterschrift für Signaturen ohne Zertifikate .....	36
<b>10</b>	<b>Welche Dokumente sind zur Signierung geeignet? .....</b>	<b>37</b>
10.1	Erstellung des Hashwertes .....	37
10.1.1	Signierung von Verweisen.....	37
10.2	Betrachtungen verschiedener Dokument-Formate .....	37
10.2.1	MS-Office / Dokumente mit dynamischen Verknüpfungen .....	37
10.2.2	TIFF .....	38
10.2.3	XML .....	39
10.2.4	Adobe - PDF .....	39
10.2.5	PDF/A .....	40
10.2.6	PDF – Open Source.....	40
10.2.7	E-Mails .....	40
<b>11</b>	<b>Technische Aspekte .....</b>	<b>41</b>
11.1	Die grundsätzliche Struktur einer elektronischen Signatur.....	41
11.2	Beispiel einer symmetrischen Verschlüsselung .....	42
11.3	Symmetrische Verschlüsselung.....	42
11.4	Asymmetrisches Verschlüsselungsverfahren.....	44
11.5	Der Hash(-wert).....	45
11.5.1	Datei- / File-Signierung.....	45

11.5.2	Inhalt- / Content-Signierung.....	45
11.6	Das Zertifikat .....	46
11.7	Qualifizierte elektronische Signatur .....	46
11.7.1	Sicherheitsanforderungen .....	47
11.8	Erstellung zertifikatsbasierter Signaturen mit Signaturkarte .....	48
11.9	Graphische Darstellung der Signaturerstellung und deren Prüfung.....	50
11.10	Fortgeschrittene elektronische Signatur .....	51
11.11	Nicht-qualifizierte Signaturen mit eigenhändiger Unterschrift .....	51
11.11.1	Signaturerstellung mit Signaturdienst .....	52
11.11.2	Signaturerstellung ohne Signaturdienst .....	53
<b>12</b>	<b>Checkliste .....</b>	<b>54</b>
12.1	Zusammenstellung relevanter Aspekte.....	54
12.2	Beispiel für die Vorgehensweise bei der Analyse .....	55
<b>13</b>	<b>Politische Aspekte .....</b>	<b>56</b>
13.1	Warum hält man am PIN Verfahren fest.....	56
13.2	Kontroverse Positionen.....	57
<b>14</b>	<b>Links und Kontakte.....</b>	<b>59</b>
14.1	GDPdU .....	59
14.2	Unternehmen und Verbände .....	59
14.3	SigLab – Signaturlabor .....	59
14.4	Die StepOver GmbH.....	61
<b>15</b>	<b>Autoren .....</b>	<b>62</b>
<b>16</b>	<b>Kurz-Glossar und verwendete Abkürzungen.....</b>	<b>63</b>
<b>17</b>	<b>Deutsche Gesetze, Verordnungen und Vorschriften .....</b>	<b>65</b>
	AO § 87a Elektronische Kommunikation .....	65
	BDSG § 4a Einwilligung .....	67
	BGB § 125 Nichtigkeit wegen Formmangels.....	67
	BGB § 126 Schriftform .....	67
	BGB § 126a Elektronische Form.....	68
	BGB § 126b Textform .....	68
	BGB § 127 Vereinbarte Form.....	68
	BGB § 355 Widerrufsrecht bei Verbraucherverträgen.....	69
	BGB § 484 Schriftform bei Teilzeit-Wohnrechtverträgen .....	69
	BGB § 492 Schriftform, Vertragsinhalt .....	70
	SGB I § 36a Elektronische Kommunikation .....	71
	SGB 4 § 110d Beweiswirkung.....	71
	SigG § 1 Zweck und Anwendungsbereich .....	73
	SigG § 2 Begriffsbestimmungen .....	73
	SigV § 15 Anforderungen an Produkte für qualifizierte elektronische Signaturen.....	75
	SRVwV § 36- Allgemeine Verwaltungsvorschrift über das Rechnungswesen .....	77
	UStG § 14 Ausstellung von Rechnungen.....	78
	VVG § 3.....	80
	VVG § 5a.....	80
	VVG § 8.....	82
	VVG § 16 .....	82

	VwVfG § 3a Elektronische Kommunikation.....	84
	VwVfG § 33 Beglaubigung von Dokumenten .....	84
	VwVfG § 37 Bestimmtheit und Form des Verwaltungsaktes .....	85
	VwVfG § 69 Entscheidung .....	86
	ZPO § 292a Anscheinsbeweis bei qualifizierter elektronischer Signatur.....	87
	ZPO § 144 Augenschein; Sachverständige.....	87
	ZPO § 371 Beweis durch Augenschein.....	87
	ZPO § 371a Beweiskraft elektronischer Dokumente .....	87
	ZPO § 286 Freie Beweiswürdigung.....	89
	ZPO § 453 Beweiswürdigung bei Parteivernehmung.....	89
	ZPO § 416 Beweiskraft von Privaturkunden .....	89
	ZPO § 439 Erklärung über Echtheit von Privaturkunden .....	89
	ZPO § 440 Beweis der Echtheit von Privaturkunden.....	90
	ZPO § 441 Schriftvergleichung.....	90
	ZPO § 442 Würdigung der Schriftvergleichung.....	90
<b>18</b>	<b>Richtlinie 1999/93/EG EG-Signaturrechtlinie .....</b>	<b>91</b>
	Artikel 1 - Anwendungsbereich .....	96
	Artikel 2 - Begriffsbestimmungen .....	96
	Artikel 3 - Marktzugang .....	98
	Artikel 4 - Binnenmarktgrundsätze .....	98
	Artikel 5 - Rechtswirkung elektronischer Signaturen.....	100
	Artikel 6 - Haftung .....	100
	Artikel 7 - Internationale Aspekte.....	102
	Artikel 8 - Datenschutz.....	102
	Artikel 9 - Ausschuß .....	103
	Artikel 10 - Aufgaben des Ausschusses.....	104
	Artikel 11 - Notifizierung .....	104
	Artikel 12 - Überprüfung.....	104
	Artikel 13 - Durchführung.....	104
	Artikel 14 - Inkrafttreten .....	105
	Artikel 15 - Adressaten.....	105
	ANHANG I.....	106
	ANHANG II.....	108
	ANHANG III .....	110
	ANHANG IV .....	110

## I Vorwort des Autors

An meiner Aussage, dass alle technischen Neuerungen immer im Kontext zu ihrer Einsetzbarkeit stehen, hat sich nichts geändert. Elektronische Signaturen bieten enorme Einsparungspotentiale durch entsprechende Prozeßoptimierungen, doch man kommt auch bei elektronischen Signaturen nicht um eine differenzierte Betrachtung herum.

Es gibt unterschiedliche Signaturverfahren und unterschiedliche Einsatzszenarien. Es gilt deshalb, zunächst die eigenen Anforderungen und Anwendungsprozesse zu betrachten und erst daraus die sinnvollen Signaturverfahren und -techniken abzuleiten. Somit sollte auch bei der ersten Betrachtung nicht das Signaturverfahren im Vordergrund stehen, sondern der jeweilige Prozeß, der eventuell mit einem geeigneten Signaturverfahren zu optimieren ist.

Alle Signaturverfahren haben Vorteile und Nachteile. So sind einzeln abzugebende Willenserklärungen in einem anderen Umfeld zu betrachten als massenhaft zu signierende elektronische Rechnungen oder die Signierung gescannter Dokumente. Dazu kommen rechtliche Anforderungen für den jeweiligen Geschäftsvorfall aus den verschiedensten Gesetzen und Verordnungen.

Wie immer habe ich mich bemüht, diesen Leitfaden so objektiv wie möglich unter Einbezug der verschiedenen Signaturverfahren zu gestalten, wobei ich mir jedoch auch erlaube, auf bestehende Mißstände hinzuweisen. Mein besonderer Dank gilt natürlich Denjenigen, die mit ihrer Kritik, ihren Anregungen und Hinweisen diese Überarbeitung erneut möglich gemacht haben.

Frankfurt am Main, im Juli 2007



Rolf Schmoldt



# StepOver

## Leitfaden zur e-Signatur

Step Over  
the next step in business

## 2 Impressum

Herausgeber: StepOver GmbH  
Wollgrasweg 27  
70599 Stuttgart  
Tel.: +49 711 12026930  
Web <http://www.StepOver.de>

Mit freundlicher Genehmigung der

BDI Business Development International GmbH

Verantwortlich im Sinne des Presserechts und Redaktion: Rolf Schmoltdt

### 3 Einleitende Informationen

#### 3.1 Wer sollte diesen Leitfaden lesen?

Dieser Leitfaden wurde entwickelt, um insbesondere die Kommunikation zwischen Anbietern von Dokument Management Systemen (DMS) und Endkunden zu erleichtern. Er soll verstanden werden als Brücke zwischen Interessierten und Experten. Aus der DMS-Branche betrifft dies u.a. folgenden Personenkreis:

- Systemintegratoren und Anbieter von Dokument Management Systemen
- Personal aus Vertrieb und Marketing
- Projekt- und Produktmanager
- Consultants

Bei den Endkunden stehen vor allem diejenigen Personen im Fokus, die sich aufgrund notwendiger Prozeßoptimierungen mit dem Thema Elektronische Signatur erstmals inhaltlich auseinandersetzen müssen.

Natürlich ist dieser Leitfaden auch für jedermann geeignet, der sich in die Materie einarbeiten möchte, auch wenn bereits in den einführenden Kapitel mehrfach Begriffe verwendet werden, die erst später erklärt werden.

Soweit der Leser mit dieser Broschüre Neuland betritt, bitten wir das gelegentlich notwendige "Nachschlagen" in den jeweiligen Kapiteln zu entschuldigen. Die sich öfters wiederholenden Erläuterungen wurden bewußt eingearbeitet, um das Lesen dedizierter Kapitel ohne Nachlesen anderer Kapitel zu ermöglichen. Zur Erleichterung wurden die Kapitel klein gehalten und über das Inhaltsverzeichnis können erklärungsbedürftige Aspekte schnell gefunden werden. Es sei hier der Hinweis erlaubt, dass es sich um eine kostenfreie Publikation handelt.

#### 3.2 Inhalt und Themen des Leitfadens

Dieser Leitfaden bietet Informationen über elektronische Signaturen, mögliche Anwendungsszenarien für automatisierte Signaturen (Zeitstempel und Massensignaturen) und Individualsignaturen sowie weiterführende Fachinformationen und Gesetzesauszüge. Schwerpunkt sind Individualsignaturen.

Es werden vorrangig solche Signaturverfahren behandelt, für die asymmetrische Verschlüsselungsverfahren zur Verschlüsselung des Hashwertes (Prüfsumme über die signierten Daten) eingesetzt werden. Insbesondere wird die Einsatzmöglichkeit gesetzeskonformer Signaturtechnologien mit eigenhändigen Unterschriften ohne Verwendung von Signaturkarten oder qualifizierten Signaturen sowie die dazu notwendige technische und rechtliche Information vorgestellt.

### 3.3 Elementare Kenntnisse - Womit sollte man beginnen

Ich empfehle Personen, die sich erstmals dem Thema Elektronische Signatur widmen, sich zuerst die technischen Erläuterungen (Kap. 11) über Hashwert und asymmetrischer Verschlüsselung sowie den Gesetzestext zum [SigG § 2 Begriffsbestimmungen](#) durchzulesen. Diese bilden die Basis zum Verständnis der in diesem Leitfaden gemachten Aussagen.

### 3.4 Neuigkeiten der Version 4.1

#### **Angebliches Erfordernis für qualifizierte elektronisch Signatur**

Neu ist die exemplarische Betrachtung verschiedener Anforderungen wie z.B. der Datenschutzerklärung bei Versicherungs- und Kontoeröffnungsanträgen, der Bestätigung über den schriftlichen Erhalt der Fragen zur Gesundheit und der Kundenbelehrung sowie des Auftrages zum Einzug per Lastschrift.

#### **Korrektur Aussage PDF / A - Signaturfelder**

Die in der Version 4.0 gemachte Aussage, PDF / A – Dokumente könnten nicht mit Signaturfeldern genutzt werden, muß ich hier korrigieren. Darüber bin ich selbst erfreut, bietet diese Möglichkeit nämlich eine Weiterführung der bisherigen Ansätze zur Verwendung von PDF Dokumenten mit fortgeschrittener Signaturen in Verbindung mit eigenhändigen Unterschriften (siehe Kapitel 10.2.5).

### 3.5 Neuigkeiten der Version 4.0

#### **GDPdU – Auslagerung der Signaturprüfung bei Rechnungen**

Die Zertifizierungsdiensteanbieter bieten mit ihren Signaturdiensten für elektronische Rechnungen nun auch die gleichzeitige Prüfung der von Ihnen erstellten Signaturen an. Damit wird dem Rechnungsempfänger nun die Rechnung selbst, die qualifizierte Signatur sowie das Prüfprotokoll zugestellt.

#### **Laut BSI fortgeschrittene Signaturen ohne Zertifikate möglich**

Das BSI hat in seiner Broschüre *Grundlagen der elektronischen Signatur* von 2006 in seinem Glossar unter *Fortgeschrittene elektronische Signatur* eingeräumt, dass fortgeschrittene Signaturen ohne Zertifikate möglich sind.

### 3.6 Neuigkeiten der Version 3

#### **Unterschied Content- und File - Signierung**

Neu ist der Aspekt zur Content - Signierung innerhalb von Textverarbeitungssystemen und von PDF - Dokumenten im Kapitel *Welche Dokumente sind zur Signierung geeignet*.

#### **Keine Zertifikat für fortgeschrittene elektronische Signatur erforderlich**

Als wichtiges Ereignis – vor allem für zertifikatsfreie Signaturverfahren – ist das am 11. Januar 2005 in Deutschland in Kraft getretene 1. Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) anzusehen.

Entscheidend ist dabei vor allem die Korrektur des §2 Abs. 9 SigG, wodurch nun in Deutschland für die fortgeschrittene elektronische Signatur eine Identifizierung des Unterzeichners nicht mehr von einem Zertifikat (Zuordnung eines Public Keys zu einer

Person und deren Registrierung) abhängig ist und damit entsprechend der EG-Signaturrichtlinie nun auch andere Identifizierungsverfahren wie eigenhändige Unterschriften möglich sind (siehe Kapitel 7.2).

### **Urkundenbeweis für qualifizierte Signaturen**

Für elektronische Privaturkunden, die mit einer qualifizierten elektronischen Signatur versehen sind, gilt ab seit dem 1. April 2005 der neue §371a ZPO. Der § 292a ZPO wurde ersatzlos gestrichen. Es stellt sich allerdings die Frage, ob gemäß § 440 ZPO eigenhändig unterschriebene elektronische Dokumente schon alleine wegen der eigenhändigen Unterschrift als Privaturkunden anzusehen sind.

### **Qualifizierte Signaturen ohne Zeitstempel auf Dauer ohne Beweiskraft**

Nachdem der Gültigkeitszeitraum eines Zertifikats abgelaufen ist, können mit dem Signaturschlüssel (Private Key) dennoch weiter qualifizierte elektronische Signaturen erstellt werden. Ohne entsprechendem Zeitstempel ist somit die qualifizierte elektronische Signatur dem Vorwurf ausgesetzt, dass diese erst nach Ablauf des Zertifikats erstellt wurde und somit nichtig sei.

Ein solcher Zeitstempel mit korrektem Datum und korrekter Uhrzeit kann natürlich nicht auf einem PC, Notebook oder Tablet-PC mit veränderbarer Zeit erstellt werden, sondern nur durch geeichte Zeitstempel-Server. Die dadurch notwendige Intranet oder Internetverbindung hebt damit letzt endlich den dezentralen Ansatz der zertifikatsbasierten Signaturen auf.

## **3.7 Begriffe - Unterzeichner statt Signaturschlüssel-Inhaber**

Das deutsche Signaturgesetz (SigG) weicht mit dem in §2 definierten Begriff „Signaturschlüssel-Inhaber“ von der Definition „Unterzeichner / Signatory“ der EG-Signaturrichtlinie (EGSRL) ab. Dies sei nach Aussage des Bundesministeriums für Wirtschaft historisch durch das Signaturgesetz von 1997 bedingt. Der Begriff Signaturschlüssel-Inhaber führt jedoch leider immer wieder selbst bei Spezialisten zu Verwirrungen. So impliziert der Begriff Inhaber fälschlich bei vielen Personen die Vorstellung, dass dem Signierenden ein Signaturschlüssel gehören müsse, bzw. der Signaturschlüssel der Person zugeordnet sein müsse.

In der EG-Signaturrichtlinie wird jedoch lediglich von einem Unterzeichner gesprochen, der eine Signaturerstellungseinheit besitzt. Inhaberschaft ist jedoch weder als Eigentum noch als Zuordnung, sondern adäquat zum Begriff Besitz zu verstehen. Die Inhaberschaft eines Signaturschlüssels – gemeint ist damit die kontrollierte Verwendungsmöglichkeit eines Signaturschlüssels – kann somit auch als temporärer Besitz verstanden werden, d.h. es können auch Signaturschlüssel verwendet werden, die dem Signierenden weder gehören noch zugeordnet sind.

Um Sie beim Lesen nicht mit solchen notwendigen Differenzierungen zu belasten, wird in diesem Leitfaden für eine Person, die eine Signaturerstellung auslöst, entweder gemäß

der EG-Signaturrechtlinie der Begriff „Untersigner“ oder der Begriff „Signaturersteller“ verwendet.

### 3.8 Fortgeschrittene elektronische Signatur ohne Zertifikate möglich

2005 hat das Bundesministerium für Wirtschaft mit dem I. SigÄndG bezüglich des §2 Abs. 9 Signaturgesetz klargestellt, dass nur für eine qualifizierte elektronische Signatur der Signaturprüf Schlüssel (und damit auch der korrespondierende Signaturschlüssel) per Zertifikat dem Signierenden zugewiesen sein muß.

Ohne die neue Angabe „für qualifizierte elektronische Signaturen“ waren bis zum Inkrafttreten des I. SigÄndG am 11. Januar 2005 die meisten Personen fälschlich davon ausgegangen, dass auch für eine fortgeschrittene elektronische Signatur, für die ebenfalls der Begriff Signaturschlüssel-Inhaber verwendet wird, der Signaturprüf Schlüssel per Zertifikat zugewiesen sein müßte.

Inzwischen schreibt selbst das BSI in seiner mit secunet erstellten Broschüre, dass fortgeschrittene Signaturen „meist“ mit zertifikatsbasierten Signaturen erstellt werden, was im Umkehrschluß heißt: Eine fortgeschrittene elektronische Signatur kann einerseits auf einem Zertifikat, also einem zugeordneten Signaturprüf Schlüssel, basieren, kann aber auch auf einem nicht-zugeordneten Signaturprüf Schlüssel beruhen.

### 3.9 Haftungsausschluß

Für die korrekte Wiedergabe Texte deutscher Gesetze, Verordnungen und Vorschriften sowie die Wiedergabe der EG-Signaturrechtlinie kann keine Haftung oder Gewährleistung übernommen werden. Auch weisen wir darauf hin, dass Gesetze jederzeit durch den Gesetzgeber und Verordnungen durch die jeweiligen Institutionen geändert werden können.

Alle in diesem Leitfaden zu Gesetzen, Verordnungen, Vorschriften oder Richtlinien gemachten Aussagen stellen unverbindliche Interpretationen dar. Aus diesen Interpretationen kann vom Leser keine in irgendeiner Art und Weise durchgeführte Rechtsberatung und daraus resultierende Haftung her- bzw. abgeleitet werden. Rechtsberatungen können nur von Rechtsanwälten durchgeführt werden. Wir empfehlen Ihnen daher zur Überprüfung jedweder Rechtsinterpretationen die Hinzuziehung eines Anwalts Ihres Vertrauens.

## 4 Grundlagen

### 4.1 Differenzierung Elektronische Signatur – Geheime Dokumente

Die Verschlüsselung von Dokumenten für den geheimen elektronischen Datenaustausch ist kein Bestandteil von elektronischen Signaturen. Leider werden diese beiden Komplexe oft verwechselt, manchmal sogar fälschlich gleichgesetzt. Eine elektronische Signatur dient nicht zur Geheimhaltung von Informationen und somit nicht der Verschlüsselung von Dokumenteninhalten und bietet auch keinen Schutz gegen Veränderungen am signierten Dokument.

Für elektronische Signaturen sowie geheime elektronische Dokumente werden gleichermaßen asymmetrische Schlüssel (siehe Kap. 11.4) verwendet, jedoch in unterschiedlicher Anwendungsweise:

- Bei der Erstellung einer fortgeschrittenen oder qualifizierten elektronischen Signatur wird mit Hilfe eines geheimen Schlüssels (Private Key) lediglich die digitale Prüfsumme (Hashwert) der signierten Daten verschlüsselt. Die Prüfsumme kann mit Hilfe des in der Signatur mitgeführten und zum Private Key korrespondierenden öffentlichen Schlüssels (Public Key) zu einem beliebigen Zeitpunkt entschlüsselt und gegen eine erneut erstellte Prüfsumme verglichen werden.
- Der Inhalt geheimer Dokumente wird dagegen mit einem symmetrischen Schlüssel verschlüsselt, der wiederum mit dem Public Key des Empfängers verschlüsselt wird. Der symmetrische Schlüssel kann nur vom Empfänger mit dessen Private Key entschlüsselt werden und dann zur Entschlüsselung des Dokuments genutzt werden.

### 4.2 Was ist eine elektronische Signatur?

Eine elektronische Signatur ist eine von einer Person elektronisch erstellte Willenserklärung oder Bestätigung. Eine elektronische Signatur kann im eigenen Namen oder im Auftrag erfolgen, ist jedoch immer personengebunden.

Der Kern einer elektronischen Signatur ist aus technischer Sicht gesehen ein verschlüsselter Hashwert (Prüfsumme). Durch erneute Erstellung des Hashwertes und dessen Vergleich gegen den ursprünglichen Hashwert kann die Integrität von signierten Daten ermittelt werden und somit erkannt werden, ob Veränderungen an den Daten bzw. dem Dokument nach der Signaturerstellung vorgenommen wurden. Es kann jedoch nicht erkannt werden, welche Veränderungen vorgenommen wurden.

Anhand von persönlichen Merkmalen wie elektronischen Zertifikaten oder bei der Signaturerstellung biometrisch erfaßter eigenhändiger Unterschriften können Unterzeichner bzw. Signaturersteller bei Bedarf identifiziert werden.

### 4.2.1 Beispiele für Willenserklärungen

- Bestellungen
- Verträge
- Anträge
- Aufträge

### 4.2.2 Beispiele für Bestätigungen

- Empfangsbescheinigungen
- Quittungen
- Dokumentationen
- Protokolle
- Bescheide
- Status und Beglaubigung
- Aktion und Ergebnisse

### 4.3 Anforderungen an elektronische Signaturen

Aus den Anforderungen an ein zu signierendes elektronisches Dokument ergeben sich die Anforderungen an elektronische Signaturen.

1. Für einen unternehmensinternen Nachweis einer elektronischen Signierung könnte bei entsprechender Vorgabe durch die Geschäftsführung z.B. das manuelle oder automatische Einfügen einer gescannten Unterschrift als Bild in das Dokument oder eine Systemprotokollierung völlig genügen. Dies entspricht der sogenannten „einfachen“ elektronischen Signatur.
2. Im Geschäftsverkehr zwischen Unternehmen, aber auch zwischen Privatpersonen und Unternehmen oder zwischen Privatpersonen und Behörden etc., sind vom Papier abgeleitet beim Einsatz von elektronischen Signaturen jedoch bestimmte Anforderungen an Signaturen zu beachten:
  - Der Unterzeichner muß identifizierbar sein
  - Der Inhalt des Dokuments und das Identifizierungsmerkmal des Unterzeichners gehören zusammen
  - Nachträgliche Veränderungen am Dokument müssen erkennbar sein
  - Der Unterzeichner muß den Signaturprozeß kontrollieren können

Elektronische Signaturen werden als Datenstruktur entweder in die elektronischen Dokumente eingefügt oder den Dokumenten angehängt oder separat gehalten, was im letzteren Fall eine entsprechende Verwaltung erforderlich macht.

### 4.3.1 Identifizierungsmerkmal Public Key für zertifikatsbasierte Signaturen

Die Datenstruktur von elektronischen Signaturen, bei denen die Identifizierung eines Unterzeichners durch die Ermittlung der bereits früher festgestellten und in einem Zertifikat bestätigten Identität erfolgt, enthält die wesentlichen Elemente:

- Public Key zum Entschlüsseln des Hashwertes und zur Prüfung des Zertifikats
- Hashwert (Prüfsumme des signierten Dokumenteninhalts)

### 4.3.2 Identifizierungsmerkmal Unterschrift für Signaturen ohne Zertifikat

Bei elektronischen Signaturen, die von nicht-registrierten Unterzeichnern erstellt werden, wird die beim Signieren erfaßte eigenhändige Unterschrift als Identifizierungsmerkmal verschlüsselt im Dokument abgelegt. Das digitale Profil der Unterschrift wird in den Hashwert der elektronischen Signatur einbezogen.

### 4.4 Was sind Massensignaturen?

Eine elektronische Signatur ist per Gesetz an eine Person gebunden und muß daher einzeln erstellt werden. Allerdings können Ausnahmegenehmigungen erteilt werden, damit elektronische Signaturen auch im Batchverfahren (Stapel) automatisiert erstellt werden können. Dabei ist die Auslösung eines automatisierten Signiervorgangs an die signierende Person gebunden.

Praktisch werden Massensignaturen erstellt, indem der Inhaber einer Signaturkarte diese in das Lesegerät eines Signaturservers einsteckt und einen Signaturprozeß durch die Eingabe seiner PIN freischaltet. Solange die Karte nun in dem Lesegerät verbleibt, können auf dem Chip der Signaturkarte die elektronischen Signaturen erstellt werden.

#### 4.4.1 Beispiele für Massensignaturen

- Signierung elektronischer Rechnungen
- Scannen bzw. Umwandlung von Papierdokumenten mit abrechnungsrelevanten Daten in elektronische Dokumente (elektronische Bilder)

Mit einer elektronischen Signatur wird die Ausführung eines Prozesses bestätigt, z.B. die Umwandlung von Papierdokumenten in elektronische Dokumente.

### 4.5 Was ist ein Zeitstempel?

Ein Zeitstempel wird technisch wie eine elektronische Signatur erstellt, ist jedoch keine personengebundene Signatur (z.B. Willenserklärung), sondern wird lediglich für den Nachweis genutzt, dass der Inhalt eines elektronischen Dokuments zu einem bestimmten Zeitpunkt vorlag. Zeitstempel werden entweder online von Zeitstempeldiensten oder von entsprechenden Servern, die im Sinne einer Black Box ins Netz gestellt werden, erstellt. Die Datenstruktur eines Zeitstempels beinhaltet u.a. folgende wesentliche Inhalte:

- Erstellungsdatum und Uhrzeit des Zeitstempels
- Hashwert (Prüfsumme des „gestempelten“ Dokumenteninhalts)

Zeitstempel werden im allgemeinen durch entsprechende Dienste angeboten, die die aktuelle Uhrzeit gewährleisten. Zeitstempel werden vorrangig automatisiert wie Massensignaturen erstellt. Qualifizierte Zeitstempel können durch zertifizierte Unternehmen, z.B. Trust Center, oder durch entsprechende zertifizierte Geräte erstellt werden.

#### 4.5.1 Beispiele für Zeitstempel

- Konstruktionszeichnungen
- Ablage von Dokumenten in einem elektronischen Archiv

### 5 Anwendungsbeispiele für eine elektronische Signatur

Beispielhaft seien aufgeführt:

- Massensignaturen für elektronisch übermittelte Rechnungen
- Signaturen für gescannte Papierdokumente
- Zeitstempel für elektronische Archivierung von Dokumenten
- Individualsignaturen für Willenserklärungen und Bestätigungen

#### 5.1 Massensignaturen zur elektronischen Übermittlung von Rechnungen

Wenn Abrechnungen **elektronisch übermittelt** und diese zur Geltendmachung der Vorsteuer genutzt werden sollen, dann müssen in Deutschland elektronisch übermittelte Abrechnungen gemäß UStG § 14 Abs. 4 mit einer qualifizierten elektronischen Signatur versehen sein. Ohne qualifizierte elektronische Signatur können in Deutschland elektronisch übermittelte Abrechnungen vom Rechnungsempfänger nicht zur Geltendmachung der Vorsteuer genutzt werden.

Der Empfänger einer elektronisch übermittelten Rechnung muß sich auf Anfrage des Senders mit der elektronischen Übermittlung einverstanden erklärt haben und die elektronische Signatur sowie das Zertifikat des Signaturerstellers prüfen und diesen Vorgang protokollieren. Inzwischen bieten Zertifizierungsdiensteanbieter (ZDAs) neben der Rechnungssignierung im Auftrag zusätzlich die Prüfung der erstellten Signaturen als Servicedienstleistung an. Der Rechnungsempfänger erhält dann neben der Rechnung und der Signatur zusätzlich das elektronische Prüfprotokoll, das er gemäß GDPdU ebenfalls aufzubewahren hat.

Die Signierung von elektronischen Abrechnungen erfolgt meist über Verfahren, die im Batchverfahren automatisiert für jede einzelne Rechnung eine qualifizierte elektronische Signatur erstellt. Rechnungssignierungen können durch beauftragte Personen – in der Regel Mitarbeiter eines ZDAs - erfolgen.

Massensignaturen werden für Abrechnungen dadurch erstellt, indem der beauftragte Inhaber einer Signaturkarte für qualifizierte Signaturen den jeweiligen Signierungsautomatismus (z.B. für einen bestimmten Rechnungsstapel) durch Benutzung seiner Signaturkarte auslöst.

### 5.1.1 Hinweis für gescannte Rechnungen

Als Papierdokumente gesendete Abrechnungen können bei entsprechender Protokollierung vom Rechnungsempfänger eingescannt werden, ohne dass zur Aufbewahrung der nun elektronisch vorliegenden Abrechnung eine qualifizierte Signatur notwendig ist. Eine qualifizierte Signatur ist nur für eine elektronisch übermittelte Rechnung notwendig.

### 5.2 Signaturen für gescannte Papierdokumente

Auch bei bestimmten Scanvorgängen müssen teilweise die gescannten Belege mit qualifizierten Signaturen versehen werden, z.B. um die ordnungsgemäße Umwandlung des Papierdokuments in ein digitales Format zu dokumentieren. Dies betrifft derzeit vor allem abrechnungsrelevante Daten der Sozialversicherungsträger gemäß SRVwV bzw. SGB.

In der Regel muß eine qualifizierte elektronische Signatur einzeln erstellt werden und im Grunde muß auch jedes erstellte Image einzeln überprüft werden. Es gibt jedoch vereinzelt Ausnahmegenehmigungen für automatisierte Verfahren.

Eine auf dem Papier abgegebene Willenserklärung in Form einer Unterschrift kann allerdings dabei nicht übernommen werden, da das 2-dimensionale Abbild der gescannten Unterschrift als nicht beweiskräftig einzustufen ist.

### 5.3 Zeitstempel für elektronische Archivierung von Dokumenten

Zeitstempel können für das Einfrieren eines Dokumentenstatus sowie für die Archivierung von Dokumenten in elektronischen Archiven genutzt werden. Zweck der Stempelung ist der spätere Nachweis, dass der Dokumenteninhalte seit dem Zeitpunkt seiner Stempelung nicht verändert wurde. Ein Zeitstempel kann eine elektronische Signatur als Willenserklärung nicht ersetzen.

### 5.4 Zeitstempel als Ergänzung zu qualifizierten Signaturen

Zeitstempel dienen auch als Ergänzung zu qualifizierten Signaturen, da mit qualifizierten Signaturen die Signaturerstellungszeit nicht festgehalten wird. Mit einem Zeitstempel kann der Nachweis geführt werden, dass eine zertifikatsbasierte Signatur vor demjenigen Zeitpunkt erstellt wurde, an dem das Zertifikat ungültig wurde und somit die Verwendung des Private Keys zur Signaturerstellung noch erlaubt war (siehe auch [Gültigkeit von Zertifikaten](#)).

### 5.5 Individualsignaturen für Willenserklärungen, Verträge und Bestätigungen

Soweit persönliche Willenserklärungen oder andere Erklärungen im eigenen Namen oder für Dritte wie Unternehmen oder Behörden abgegeben werden, muß für jede einzelne Willenserklärung oder Bestätigung eine individuelle elektronische Signatur erstellt werden. Dabei ist für die Auswahl des Signaturverfahrens entscheidend, ob aufgrund gesetzlicher Vorgaben eine qualifizierte elektronische Signatur erforderlich ist oder nicht. Qualifizierte Signaturen können für alle Anforderungen eingesetzt werden, in den meisten Fällen ist jedoch eine einfache oder fortgeschrittene elektronische Signatur ausreichend.

#### 5.5.1 Signieren ohne vorherige Registrierung des Unterzeichners

Unternehmen können – soweit keine qualifizierte elektronische Signatur erforderlich ist – 100% aller Personen in ihre elektronischen Prozesse integrieren, ohne dass sich diese Personen für eine Signaturerstellung erst vorher registrieren lassen müssen.

Am Kundenschalter werden Kunden nach wie vor durch den Verkäufer identifiziert und deren persönliche Daten in den Kaufvertrag und meistens auch in die Kundendatenbank aufgenommen. Soweit also der Kunde mit einem Identifizierungsmerkmal wie seiner eigenhändigen Unterschrift die Bestellung auf einem Unterschriftentablett unterzeichnet und damit die Erstellung einer elektronischen Signatur auslöst und für weitere Erklärungen keine gesetzliche Schriftform erforderlich ist, kann aufgrund der bereits erfolgten Aufnahme der Kundendaten auf eine zusätzliche Identifizierung über ein Zertifikat verzichtet werden, da erst bei Bedarf die beweisrelevante Identifizierung durch einen Schriftsachverständigen mit der im elektronischen Dokument aufgenommenen Unterschrift erfolgt. Damit entstehen den Kunden bzw. den Unterzeichnern bei der Signaturerstellung weder Kosten noch Aufwände und das Unternehmen kann mit seinen Prozessen 100% der relevanten Personen bedienen.

#### 5.5.2 Signieren mit vorheriger Registrierung des Unterzeichners

Anders verhält sich dies jedoch, wenn eine qualifizierte elektronische Signatur erforderlich oder eine Verifizierung des Unterzeichners bereits während der Unterzeichnung erforderlich ist. So ist es zum Beispiel für anonyme Internet Geschäfte wünschenswert, dass die Identität eines anonym online signierenden Unterzeichners ermittelt werden kann.

Der Unterzeichner muß daher verifiziert werden, ob er überhaupt berechtigt ist, eine elektronische Signatur zu erstellen.

Bei der Erstellung einer qualifizierten Signatur erfolgt die Verifizierung durch die Überprüfung einer eingegeben PIN, bei Signaturverfahren mit eigenhändiger Unterschrift wird die Unterschrift überprüft.

Damit eine Verifizierung überhaupt erfolgen kann, muß sich der Unterzeichner für die Erstellung qualifizierter Signaturen bei einem ZDA registrieren lassen, der mit einem

elektronischen Zertifikat die Zuweisung des Public Keys und des korrespondierenden Private Keys bestätigt. Zusätzlich wird dem Unterzeichner noch eine 6-stellige PIN zugewiesen, mit der der Unterzeichner den Private Key zur Signaturerstellung erst freischalten kann.

Um eine Verifizierung anhand einer eigenhändigen Unterschrift durchführen zu können, muß der Unterzeichner bei einem Authentifizierungsdienst mehrere Vergleichsunterschriften (auch Templates genannt) hinterlegen. Das Anlegen solcher Templates wird als Enrolment bezeichnet.

Es sei der Hinweis erlaubt, dass Versandhäuser bei Onlinegeschäften die Kreditwürdigkeit eines Kunden weniger von der Verwendung zertifikatsbasierter Signaturverfahren, sondern meist von der Beurteilung anhand der Wohn- und Lieferadresse abhängig machen.

## 6 Gesetzliche Rahmenbedingungen

Es sei nochmals darauf hingewiesen, dass alle rechtlichen Betrachtungen lediglich die Sichtweise des Autors darstellen und daher nicht als verbindliche Aussage gewertet werden können.

Rechtsberatungen können nur von Rechtsanwälten durchgeführt werden. Es wird Ihnen daher zur Überprüfung jedweder Rechtsinterpretationen die Hinzuziehung eines Anwalts Ihres Vertrauens empfohlen.

### 6.1 Rechtliche Anforderungen an elektronische Signaturen

Im Signaturgesetz (SigG) und in der Verordnung zum Signaturgesetz (SigV) werden die elektronischen Signaturen selbst und insbesondere die Anforderungen an elektronische Signaturen und Zertifizierungsdiensteanbieter (ZDA) definiert.

Die Rahmenbedingungen jedoch, wann welche elektronische Signatur verwendet werden kann oder muß, werden nicht im Signaturgesetz definiert, sondern beruhen im wesentlichen auf dem Bürgerlichen Gesetzbuch (BGB), der Zivilprozessordnung (ZPO) und anderen Gesetzen sowie Rechts- und Verwaltungsverordnungen.

Um zu ermitteln, ob und wenn ja, welches Signaturverfahren eingesetzt werden kann oder muß, sollten die wichtigsten Fragen an den Anwendungsprozeß vorab geklärt werden:

- Per Gesetz oder per Verordnung explizit geforderte qualifizierte Signatur?
- Per Gesetz geforderte Schriftform?
- Per Gesetz geforderte Schriftform aber elektronische Form ausgeschlossen?
- Keine gesetzliche Schriftformerfordernis?
- Vorab-Identifizierung gewünscht oder sogar erforderlich?

#### 6.1.1 Gesetzliche Schriftform erfordert qualifizierte Signatur

In verschiedenen Gesetzen und Rechtsverordnungen wird für manche Willenserklärung Schriftform gemäß BGB § 126 gefordert und damit ist gemäß BGB §126a [Elektronische Form] eine qualifizierte elektronische Signatur erforderlich. Zusätzlich wird in verschiedenen Gesetzen ohne Verweis auf die gesetzliche Schriftform bereits explizit eine qualifizierte elektronische Signatur (manchmal mit Anbieterakkreditierung oder langfristiger Überprüfbarkeit) zur Unterzeichnung von elektronischen Dokumenten vorgeschrieben.

Soweit per Gesetz Schriftform für Vereinbarungen, Anträge, etc. gefordert ist, müssen für elektronische Dokumente bestimmte Signaturverfahren verwendet werden.

- Qualifizierte elektronische Signatur oder
- Qualifizierte elektronische Signatur mit Anbieterakkreditierung

### 6.1.1.1 Technische Anforderungen an die qualifizierte elektronische Signatur

Nach heutiger Gesetzgebung sind qualifizierte elektronische Signaturen ausschließlich zertifikatsbasierte Signaturverfahren. Zertifikatsbasierte Signaturverfahren erfordern, dass der Signaturersteller bei einem Trust Center (ZDA – Zertifizierungsdiensteanbieter) registriert ist und das Trust Center dem Signaturersteller ein asymmetrisches Schlüsselpaar (Private und Public Key) zugeordnet hat. Zusätzlich wird für einen bestimmten Zeitrahmen (meistens 2 – 3 Jahre) ein Zertifikat ausgestellt, das die Zusammengehörigkeit des öffentlichen Signaturprüfchlüssels (Public Key) und der Identität des Zertifikatsinhabers bestätigt. Da zum Public Key nur ein einziger Private Key paßt, ist somit auch der Private Key dem Zertifikatsinhaber zugeordnet.

Die praktische Erstellung solcher Signaturen ist derzeit fast ausschließlich über Chipkarten realisiert, jedoch sind auch andere Geräte wie USB Sticks möglich. Auf solchen Chipkarten wird der für eine zertifikatsbasierte elektronische Signatur notwendige Signaturschlüssel (Private Key) hinterlegt, der während eines Signiervorgangs durch Eingabe einer – ebenfalls auf der Chipkarte hinterlegten – 6-stelligen PIN (Verifizierung des Signaturerstellers) zur Erstellung einer Signatur freigeschaltet wird.

Zur Erstellung einer qualifizierten elektronischen Signatur muß eine „sichere Signaturerstellungseinheit“ (SSEE) verwendet werden. Diese SSEE ist der Chip der Signaturkarte, auf dem der übergebene Hashwert (Prüfsumme der Daten) mit dem Signaturschlüssel (Private Key) verschlüsselt und somit eine elektronische Signatur erstellt wird. Derzeit erfüllen lediglich bestimmte Chipkarten diese hohen Sicherheitsanforderungen.

Zwar wird angenommen, dass der Signaturersteller auch der rechtmäßige Karteninhaber ist, doch beweisen kann man dies nicht. Aus diesem Grund wurde für qualifizierte Signaturen der Anschein der Echtheit (ZPO § 371a) eingeführt.

*Die Beweisführung bei Gericht für qualifizierten Signaturen, dass der Zertifikatsinhaber **nicht signiert** hat, obliegt damit dem Zertifikatsinhaber.*

### 6.1.1.2 Erstellungsdatum qualifizierter Signaturen nur mit Zeitstempel möglich

Dieses provokante Kapitel soll auf eine wesentliches Leck in der Verwendung qualifizierter elektronischer Signaturen hinweisen.

Wenn in einer qualifizierten Signatur kein gesichertes Datum und keine gesicherte Uhrzeit mitgeführt wird, dann ist nach Ablauf der Zertifikatsgültigkeit nicht beweisbar, ob die Signatur zum Zeitpunkt ihrer Erstellung auf einem gültigen, also nicht bereits abgelaufenem Zertifikat beruht. Im Klartext heißt dies, dass mit qualifizierten Signaturkarten, für dessen Private Key die Zertifikatsgültigkeit bereits abgelaufen oder gesperrt ist, rückdatierbare Erklärungen signiert werden können. Mit einer abgelaufenen Signaturkarte können somit nachträglich scheinbar gültige Signaturen erstellt werden.

Einzig und alleine in Kombination mit einem sicheren Zeitstempel kann also gewährleistet werden, dass eine Signatur im Zeitraum der Zertifikatsgültigkeit erstellt wurde. Zeitstempel können jedoch nur online erstellt werden.

### 6.1.2 Formfreie Vereinbarungen ohne qualifizierte elektronische Signatur

In Deutschland besteht in der Regel Formfreiheit zur Gestaltung von geschäftlichen und privaten Vereinbarungen. Dies gilt für alle Rechtsgeschäfte, soweit für bestimmte Rechtsgeschäfte diese Formfreiheit nicht per Gesetz oder Rechtsverordnung ausdrücklich eingeschränkt wird, sei es durch Schriftformerfordernis oder expliziter Anforderung in Gesetzen oder durch Erfordernis notarieller Beglaubigung. Formfreie Vereinbarungen werden daher einzig und alleine zum Zweck der Beweisbarkeit der Vereinbarung unterzeichnet, nicht jedoch aufgrund einer gesetzlichen Erfordernis.

Formfreie Vereinbarungen machen ca. 95% aller schriftlichen Vereinbarungen aus. Bisher konnten sich im Bereich Individualsignaturen die zertifikatsbasierten Signaturverfahren nicht durchsetzen. Bei Massensignaturen kommt man in der Regel mit vereinzelt Signaturkarten aus, für formfreie Vereinbarungen müßten jedoch Signaturkarten massenhaft verbreitet sein.

Es gab in der Vergangenheit mehrere Ansätze, die Verbreitung von Signaturkarten zu fördern, z.B. durch Banken. Die Erfolge halten sich in sehr bescheidenen Grenzen, da Signaturen bzw. Zertifikate einzeln kostenpflichtig beantragt werden müssen. Eine automatische Mitlieferung einer Signaturfunktion auf einer Bankkarte ist nämlich aufgrund der damit verbundenen Identifizierung und Einwilligung des Antragsstellers hinsichtlich seiner Haftung ausgeschlossen.

So hatte man auch auf die Nutzung der Gesundheitskarte gehofft, diese Hoffnung ist bisher nicht erfüllt worden. Derzeit wird über die Einführung der Job-Karte diskutiert, mit der auch Signatur-Funktionen mitgeliefert werden können. Eine Umsetzung wird jedoch nicht vor 2008 erwartet und ob die Bürger dann massenhaft Signaturen beantragen werden, ist noch völlig offen.

Selbstverständlich können für formfreie Vereinbarungen qualifizierte Signaturen eingesetzt werden, zusätzlich stehen folgende Signaturverfahren zur Verfügung:

- Elektronische Signatur (auch „einfache“ elektronische Signatur genannt)
- Fortgeschrittene elektronische Signatur

#### 6.1.2.1 Vereinbarte Schriftform

Ohne gesetzliche Notwendigkeit wird für Geschäftsvereinbarungen und Willenserklärungen zur besseren Beweisfähigkeit der getroffenen Vereinbarungen in einem eventuellen Rechtsstreit freiwillig Schriftform vereinbart.

*Für eine elektronische Vereinbarung, die freiwillig erstellt wird und auch elektronisch signiert werden soll, muß gemäß BGB §127 [Vereinbarte Form] keine qualifizierte elektronische Signatur verwendet werden.*

Allerdings sollte das vereinbarte Signaturverfahren in der elektronisch signierten Vereinbarung genannt werden, da „im Zweifel“ die Empfänger des signierten Dokuments von der Verwendung einer qualifizierten elektronischen Signatur ausgehen können und gegebenenfalls die Nachsignierung mittels einer qualifizierten elektronischen Signatur verlangen können.

Auch sollte zur Ausräumung von Mißverständnissen der in vielen Verträgen vorhandene Passus „Änderungen bedürfen der Schriftform“ entsprechend angepaßt werden.

### 6.1.2.2 Nutzung nicht-qualifizierter Signaturen als Beweismittel

Einfache und fortgeschrittene elektronische Signaturen sind entgegen weit verbreiteter Meinung selbstverständlich als Beweismittel vor Gericht zugelassen, was auch ausdrücklich in Artikel 5 Abs.2 der für alle EU-Staaten verbindlichen EG-Signaturrichtlinie festgeschrieben wurde. Man spricht daher auch von 5.2 er - Signaturen. In Deutschland wird dies durch den §371 ZPO geregelt.

Bei der Auswahl von einfachen und fortgeschrittenen Signaturen sollte man beachten, dass deren Technologie als „beweiskräftig“ eine Chance vor Gericht hat. Im innerbetrieblichen Bereich kann zwar bereits eine E-Mail als Nachweis gelten, für Rechtsgeschäfte, auch wenn diese formfrei vereinbart werden, ist jedoch Beweiskraft und damit die Würdigung des Beweismittels durch das Gericht unabdingbar.

*Dabei ist es unerheblich, ob das Signaturverfahren nun der Definition im Signaturgesetz entsprechend als „einfache“ oder als fortgeschrittene Signatur gilt. Beide Signaturen gelten als Objekte des Augenscheins.*

Einen Anscheinsbeweis wie für die qualifizierte elektronische Signatur gibt es für „einfache“ und fortgeschrittene Signaturen nicht.

### 6.1.2.3 Fortgeschrittene Signaturen als Beweismittel

Auch für die fortgeschrittene elektronische Signatur gibt es zertifikatsbasierte Verfahren, die über die zugeteilten Zertifikate eine Identifizierung ermöglichen. Sie unterscheiden sich weder technisch noch in der Anwendung von qualifizierten Signaturen, jedoch unterliegen sie weder bei der Zertifikatserstellung noch bei der Verwendung von Signaturkomponenten den hohen Sicherheitsanforderungen an eine qualifizierte elektronische Signatur.

Mit einem zertifikatsbasierten Signaturverfahren für eine fortgeschrittene elektronische Signatur kann wie auch bei qualifizierten Signaturen nicht bewiesen werden, dass der Zertifikatsinhaber auch wirklich selbst signiert hat.

*Streitet der Zertifikatsinhaber die Erstellung einer fortgeschrittenen Signatur ab, dann liegt die Beweisführung bei der Gegenseite.*

Signaturkarten für fortgeschrittene Signaturen unterliegen privatrechtlichen Haftungsvereinbarungen, ähnlich wie bei Kreditkarten. Bemerkenswert ist, dass es bereits mehrere Gerichtsentscheide gibt, die Kreditkarteninhaber aus der privatrechtlichen Haftung entließen, da die PIN ausspähbar sei.

### **6.1.3 Einfache und fortgeschrittene elektronische Signatur ohne Zertifikat**

Neben zertifikatsbasierten Verfahren gibt es zusätzliche, ebenfalls gesetzeskonforme und rechtssichere Technologien, die auch ohne Zertifikate auskommen, indem die erst während der Signierung erstellte eigenhändige Unterschrift als Identifizierungsmerkmal im Dokument mitgeführt wird.

In diesem Zusammenhang hat das Bundesministerium für Wirtschaft mit seiner Stellungnahme vom 19.03.2003 bestätigt,

*dass fortgeschrittene Signaturen trotz des im (seit Januar 2005 korrigierten) Signaturgesetz verwendeten Begriffs „Signatur Schlüssel-Inhaber“ (korrekt gemäß EGSRL: Unterzeichner) keinen persönlich zugewiesenen Signatur Schlüssel benutzen müssen und damit auch kein Zertifikat ausgestellt werden muß.*

Maßgeblich für fortgeschrittene Signaturen ist aufgrund dieser nicht gewollten begrifflichen Abweichung auch aus Sicht des Bundesministeriums für Wirtschaft die auch für Deutschland verbindliche EG-Signaturrichtlinie (EGSRL).

Leider ist manchen Personen noch immer unklar, was in Artikel 2 Abs. 3 der EGSRL unter dem „Besitz einer Signaturerstellungseinheit“ zu verstehen ist. Besitz ist nämlich nicht Eigentum, sondern kann auch die vorübergehende Überlassung einer Signaturerstellungseinheit bedeuten.

Ob der „Besitz einer Signaturerstellungseinheit“ ein Sicherheitsaspekt oder eine ungerechtfertigte Technikregulierung ist, möchten wir hier nicht vertiefen. Aufzeigen möchten wir hingegen, dass die Verwendung einer auf Unterschriften basierenden Technologie ebenfalls eine sehr große Beweissicherheit bieten kann.

#### **6.1.3.1 Fortgeschrittene Signaturen benötigen asymmetrische Verschlüsselung**

Obwohl mit der seit Januar 2005 gültigen Anpassung des §2 Abs. 9 SigG dem Unterzeichner (im SigG Signatur Schlüsselinhaber genannt) der korrespondierende Signaturprüf Schlüssel nicht mehr zugeordnet sein muß, ist klarzustellen, dass gemäß §2 Abs. 4 SigG der Ersteller fortgeschrittener Signaturen weiterhin einmalige Signatur Schlüssel zur Signaturerstellung (Verschlüsselung Hashwert) und Signaturprüf Schlüssel (Entschlüsselung Hashwert) verwenden muß.

Praktisch bedeutet dies, dass asymmetrische Verschlüsselungsverfahren mit einem Private Key zur Verschlüsselung des Hashwertes und einem Public Key zur Entschlüsselung des Hashwertes eingesetzt werden müssen. Jedoch können der Signaturschlüssel und die Signaturerstellungseinheit dem Unterzeichner zur Nutzung - ohne Kenntnis des Schlüssels selbst - überlassen werden oder bei Bedarf erst während der Signatur erzeugt werden. Eine solche Signaturerstellungseinheit wird dem Unterzeichner entweder lokal oder online zur Verfügung gestellt.

### 6.1.3.2 Beweiskraft von nicht-qualifizierten Signaturen

Ein elektronisches Dokument mit einer „einfachen“ oder fortgeschrittenen Signatur gilt als Objekt des Augenscheins (§371 ZPO). Die unterschiedlichen gesetzlichen Einstufungen der Signaturverfahren besagen aber nicht, dass eine „einfache“ oder fortgeschrittene elektronische Signatur aufgrund ihrer rechtlichen Einstufung gemäß Signaturgesetz technisch unsicherer ist als eine qualifizierte elektronische Signatur. Soweit die Signaturerstellung mittels asymmetrischer Verfahren erfolgt, beruht eine fortgeschrittene elektronische Signatur auf dem selben Verfahren wie eine qualifizierte elektronische Signatur.

Gescannte Unterschriften, Faxe und Kopien, also reine 2-dimensionale Images, **können nicht als beweiskräftige Signaturverfahren eingestuft werden.**

Entscheidend für „beweiskräftige“ Signaturverfahren sind sicherlich die auch unter Artikel 2 Abs. 2 der EG-Signaturrichtlinie definierten Anforderungen (exakter Wortlaut im Anhang):

- Der Unterzeichner muß nachträglich identifizierbar sein
- Fälschungen am Dokument müssen bei Signaturprüfungen erkennbar sein
- Die Signatur muß eindeutig dem Unterzeichner zugeordnet werden können
- Bezüglich Sicherheit sollte der Unterzeichner Verfahren einsetzen, bei denen er zumindest eine Komponente zur Signaturerstellung unter seiner alleinigen Kontrolle halten kann.

In der EGSRRL unter Artikel 2, Abs. 2c ist der Passus zu finden:

*Sie (die elektronische Signatur) wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann.*

Von Verfechtern der zertifikatsbasierten Signaturverfahren wird mit diesem Absatz falsch argumentiert, dass der Unterzeichner die Komponente der tatsächlichen Signaturerstellung (z.B. die Chipkarte) selbst unter Kontrolle haben müsse.

Dies darf jedoch nicht als örtliche Kontrolle mißverstanden werden, da auch die Kontrolle über eine Signaturkarte nur über dessen PIN erfolgt, deren Eingabe aber über eine an einem beliebigen Ort platzierbaren Tastatur erfolgen kann. Folglich kann der Unterzeichner mit PIN oder durch Unterschrift die Erstellung einer elektronischen

Signatur unter seiner alleinigen Kontrolle auslösen, unabhängig davon, wo sich die tatsächliche Signaturerstellungseinheit befindet.

### 6.1.3.3 Zuordnung der elektronischen Signatur zum Unterzeichner

Die Zuordnung der elektronischen Signatur zum Unterzeichner kann mit zwei Verfahren sichergestellt werden:

1. Bei zertifikatsbasierten Signaturkarten wird der Private Key des registrierten Zertifikatsinhabers zur Signaturerstellung genutzt. Der zum Private Key korrespondierende Public Key bzw. das Zertifikat über die Zuordnung des Public Keys zu einer Person ermöglicht die Identifizierung des Unterzeichners über das Trust Center bzw. dessen öffentlichen Verzeichnisdienstes. Über die Annahme, dass der Zertifikatsinhaber selbst unterzeichnet hat, gilt der Ersteller von qualifizierten Signaturen über das Zertifikat als identifiziert.

Wenn sich der Hashwert mit dem Public Key des Zertifikatsinhabers entschlüsseln läßt, muß der Hashwert mit dem korrespondierenden Private Key des Zertifikatsinhabers verschlüsselt worden sein, damit gilt die Signierung der Daten als nachgewiesen.

2. Bei zertifikatsfreien Verfahren wird die im elektronischen Dokument verschlüsselt abgelegte Unterschrift in den Hashwert einbezogen, der wiederum verschlüsselt in der elektronischen Signatur mitgeführt wird. Der Unterzeichner wird bei Bedarf anhand seiner Unterschrift durch einen Schriftsachverständigen als Ersteller der Unterschrift identifiziert. Da die Unterschrift ebenfalls in den Hashwert der elektronischen Signatur einbezogen wird, kann damit die Zusammengehörigkeit der signierten Daten und der Unterschrift nachgewiesen werden.

## 6.2 Elektronische Urkunden

### 6.2.1 Elektronische Dokumente mit qualifizierter Signatur

Für elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, ist dieser Aspekt durch den § 371a ZPO geregelt. Solche Dokumente werden wie unterschriebene Papierdokumente als Privaturkunden behandelt.

### 6.2.2 Eigenhändig unterschriebene elektronische Dokumente

Auf den ersten Blick scheinen gemäß §371a ZPO nur solche elektronische Dokumente die Anforderung an Privaturkunden zu erfüllen, die mit einer qualifizierten Signatur versehen sind.

Dagegen steht allerdings in dem §440 ZPO (Beweis der Echtheit von Privaturkunden) unter Nr. 2:

*Steht die Echtheit der Namensunterschrift fest oder ist das unter einer Urkunde befindliche Handzeichen notariell beglaubigt, so hat die über der Unterschrift oder dem Handzeichen stehende Schrift die Vermutung der Echtheit für sich.*

Die Verwendung der eigenhändigen Unterschrift als Identifizierungsmerkmal für fortgeschrittene Signaturen wird derzeit noch von zertifikatsorientierten Interessensgruppen mit diversen Argumenten in Abrede gestellt, obwohl die eigenhändige Unterschrift seit Jahrhunderten bei Papier als einwandfreies Identifizierungsmerkmal sowie als Beweis einer Erklärung zugelassen ist.

Eigenhändige Unterschriften bzw. deren digitalisierte Profile, die selbst von Mitarbeitern des BKA und Schriftsachverständigen als hervorragendes Identifizierungsmerkmal gewürdigt werden, werden durch den § 126a des BGB und den § 371a der ZPO gezielt als Identifizierungsmerkmal für elektronische Dokumente bei Schriftformerfordernis ausgeschlossen.

Wie schon erwähnt, stehen jedoch die §§ 439, 440 und 441 der ZPO im Widerspruch zu § 126a des BGB (Gesetzlich erforderliche Schriftform) und § 371a der ZPO (Elektronische Privaturkunde). Leider können wir an dieser Stelle noch keine Aussage treffen, ob in Zukunft eigenhändig unterschriebene elektronische Dokumente aufgrund der Unterschrift als Privaturkunden einzuordnen sind.

In dieser Angelegenheit gibt es derzeit eine Initiative beim Bundesministerium für Wirtschaft, um eine Klärung herbeizuführen.

Wir kommen nicht umhin, die angegebenen Gründe zu beleuchten. So sagte im Jahr 2005 das Bundesamt für Sicherheit in der Informationstechnik (BSI), dass mathematisch eine PIN immer sicher sei, sie sei entweder richtig oder falsch, eine Unterschrift dagegen aufgrund dessen, dass sie jedesmal anders sei, dagegen nur eine Wahrscheinlichkeit.

Diese Aussage ist natürlich nur dann zutreffend, wenn man

- a) das Wort „mathematisch“ nicht überhört und die Möglichkeiten der Weitergabe von Karte und PIN außer Betracht läßt („Dies ist nicht Gegenstand unserer Untersuchungen“, Zitat BSI) und
- b) mit einer elektronischen Signatur nicht nur eine Migration von papierabhängigen Prozessen auf elektronische Prozesse ermöglichen, sondern wie leider so oft in Deutschland gleichzeitig noch zusätzliche Funktionen verbinden möchte.

Unter sicherheitspolitischen Betrachtungen und dem Umstand, dass das Bundesministerium des Inneren bei der Entwicklung des Signaturgesetzes eine wesentliche Rolle spielte, wird deutlich, warum Ende der 90er Jahre eine Registrierung der Benutzer wünschenswert gewesen ist. Ergänzend kommt hinzu, dass die Banken befürchten, die mit PIN und Karte bei dem Benutzer liegende Haftung bei Verfahren mit

Unterschriften, zumindest dann, wenn diese als Authentifizierung dienen, selbst übernehmen zu müssen.

Wichtig zu wissen ist allerdings, dass eine Authentifizierung bereits während der Unterzeichnung von Papierurkunden bisher noch nie eine Anforderung war. Warum sollte dies dann bei einer Unterschrift, deren Profile während der Signaturerstellung aufgenommen werden, gefordert werden? Der Grund liegt alleine darin, dass die Vorstellung, einen Unterzeichner genauso wie Papierurkunden anhand seiner Unterschrift erst bei Bedarf zu identifizieren, bisher nicht ernsthaft in Betracht gezogen wurde.

### 6.3 Anpassung von Vertragsbestimmungen

In den meisten vertraglichen Vereinbarungen existiert der Passus, dass Änderungen der Vereinbarung in Schriftform zu erfolgen haben. Gemeint ist damit jedoch nicht die gesetzlich vorgeschriebene Schriftform gemäß BGB §126, sondern die freiwillige Schriftform gemäß BGB §127. Zur Ausräumung von Zweifeln bei Vereinbarungen, die nicht der gesetzlichen Schriftform unterliegen, sollten für elektronische Dokumente die entsprechenden Anpassungen vorgenommen werden. Dies könnte sinngemäß wie folgt aussehen (ohne Gewähr):

#### **Elektronisches Dokument**

Diese Vereinbarung kann als elektronisches Dokument in Textform mit einer elektronischen Signatur gemäß SigG § 2 Abs. 1 oder Abs. 2 versehen werden, die eine Identifizierung des Unterzeichners sowie die Erkennung nachträglicher Veränderungen der Daten ermöglicht und ausschließlich dem Unterzeichner zugeordnet ist.

#### **Nebenabsprachen, Änderungen:**

Nebenabsprachen sind nicht getroffen worden. Änderungen der Vereinbarung bedürfen der Schriftform oder Textform. Wird Textform verwendet, so ist diese von dem jeweiligen Vertragspartner mit einer elektronischen Signatur gemäß SigG § 2 Abs. 1 oder Abs. 2 zu versehen, die eine Identifizierung des Unterzeichners sowie die Erkennung nachträglicher Veränderungen der Daten ermöglicht und ausschließlich dem Unterzeichner zugeordnet ist.

Die Aufführung der qualifizierten elektronischen Signatur ist nicht notwendig, da diese die gesetzliche Schriftform und damit auch die freiwillige Schriftform erfüllt.

### 6.4 Betrachtungen angeblicher Erfordernisse einer qualifizierten Signatur

#### 6.4.1 Bundesdatenschutzgesetz § 4a

Über diesen Paragraphen stolpern die meisten Rechtsanwälte derjenigen Unternehmen, die direkt am Schalter Kunden Bestellungen aufnehmen. Optimierungsprozesse mit elektronischen Dokument werden alleine deswegen aufgegeben, weil angeblich der Kunde seine Datenschutzerklärung mit einer qualifizierten Signatur versehen müsse.

Dabei läßt der § 4a Abs. 1 des BDSG (siehe auch Kapitel Gesetze) sehr wohl die Möglichkeit einer Abweichung zu, nämlich dann, wenn wegen besonderer Umstände eine andere Form angemessen ist. Davon ausgehend, dass sich Versicherungen die Datenschutzerklärungen auf elektronischen Dokumenten mit eigenhändigen Unterschriften ohne qualifizierte Signatur unterzeichnen lassen, legt die Vermutung nahe, dass von deren Anwälten die Umstände bei der Antragsunterzeichnung und Erklärung zum Datenschutz mittels elektronischer Dokumente als besondere Umstände gewertet wird.

Zumal die Warnfunktion der Unterschrift als wichtigster Grund für die Schriftform und die Beweisfähigkeit durch fortgeschrittene Signaturen gegeben ist, könnte der Vorteil für beide Parteien als besonderer Umstand gewertet werden.

### 6.4.2 Ermächtigung zum Lastschrifteinzug

Lastschriftabkommen der Verbände der Kreditwirtschaft, Abschnitt I, Nummer 1:

*Im Rahmen des Lastschriftverfahrens wird zu Gunsten des Zahlungsempfängers über sein Kreditinstitut (1. Inkassostelle) von dem Konto des Zahlungspflichtigen bei demselben oder einem anderen Kreditinstitut (Zahlstelle) der sich aus der Lastschrift ergebende Betrag eingezogen, und zwar auf Grund*

- a) *einer dem Zahlungsempfänger von dem Zahlungspflichtigen erteilten **schriftlichen** Ermächtigung (Einzugsermächtigung) oder*
- b) *eines der Zahlstelle von dem Zahlungspflichtigen zu Gunsten des Zahlungsempfängers erteilten **schriftlichen** Auftrags (Abbuchungsauftrag).*

Das Lastschriftabkommen ist ein Abkommen zwischen den Verbänden der Kreditwirtschaft und somit keine gesetzliche Formvorschrift. Aus diesem Grund ist eine qualifizierte Signatur gesetzlich nicht erforderlich.

Es obliegt somit dem jeweiligen Zahlungsempfänger, ob er bei einer Ermächtigung mittels eines elektronischen Dokuments auf einer qualifizierten Signatur besteht oder eben nicht. Rechtlich gesehen reicht sogar eine E-Mail in Textform aus, doch sollte bei Einzugsermächtigungen und Abbuchungsaufträgen ein beweisfähiges Signaturverfahren genutzt werden.

### 6.4.3 Gesundheitsfragen und Kundenbelehrung

Zwar müssen Gesundheitsfragen und Belehrungen schriftlich dem Kunden ausgehändigt werden, die Antwort bzw. die Bestätigung des Kunden über den Erhalt der Unterlagen bedürfen jedoch nicht der Schriftform und damit keiner qualifizierten Signatur.

Dennoch ist aus Haftungsgründen auch in diesem Fall die Verwendung beweisfähiger Signaturen zu empfehlen.

## 7 Abweichungen des SigG zur EG-Signaturrichtlinie

Basierend auf dem alten Signaturgesetz von 1997 sind bei der Neufassung des SigG von 2001 mehrere Begriffe übernommen worden, die teilweise zu erheblichen Verunsicherungen geführt haben.

### 7.1 Signaturschlüssel-Inhaber anstatt Unterzeichner

In der EG-Signaturrichtlinie von 1999 wird immer vom Unterzeichner / Signatory gesprochen (Artikel 2), während im SigG der Begriff Signaturschlüssel-Inhaber verwendet wird. Dabei wird auch noch heute – wie in vielen Gesprächen mit Kunden immer wieder festgestellt – Inhaber mit Eigentümer verwechselt.

### 7.2 I. Gesetz zur Änderung des Signaturgesetzes


Mit dem am 11. Januar 2005 in Kraft getretenen I. Gesetz zur Änderung des Signaturgesetzes (SigÄndG) wurden verschiedene Anpassungen vorgenommen, die sowohl die Zertifizierungsdiensteanbieter (ZDA) betreffen, als auch die zertifikatsfreien Signaturen.

Insbesondere die Anpassung des §2 Abs. 9 SigG war ein enorm wichtiger Schritt für formfreie Vereinbarungen. War es in der vorherigen Fassung des SigG noch erforderlich, dass auch für fortgeschrittene Signaturen einem Unterzeichner der Signaturprüfchlüssel (=Public Key) mit eine Zertifikat qualifiziert zugeordnet sein mußte (laut BMWA nicht gewollt), so ist gemäß Neufassung des §2 Abs. 9 SigG ein Zertifikat jetzt nur noch für qualifizierte Signaturen zwingend notwendig.

In der Konsequenz bedeutet dies, dass zwar gemäß §2 Abs. 4 SigG zur Erstellung fortgeschrittener Signaturen einmalige kryptographische Schlüssel (Private Keys) verwendet werden müssen, der Unterzeichner jedoch nicht Eigentümer solcher kryptographischer Schlüssel sein muß. Somit kann er auch ihm nicht zugeordnete oder bei Bedarf erzeugte kryptographische Schlüssel verwenden.


Mit einer eigenhändigen Unterschrift als Identifikationsmerkmal kann außerdem die gemäß §2 Abs.2 SigG geforderte Identifizierung des Unterzeichners sichergestellt werden. Somit können gemäß deutschem SigG fortgeschrittene Signaturen auch ohne vorherige Beantragung eines Privaten Schlüssels und Zertifikats – also ohne vorherige Registrierung – erstellt werden.

## 7.3 BMWA Stellungnahme zu fortgeschrittenen Signaturen

 **Bundesministerium  
für Wirtschaft  
und Arbeit**


Bundesministerium für Wirtschaft und Arbeit • 53167 Bonn

**Rolf Schmoldt**



TEL-ZENTRALE +49 (0)1888 615-0 od. (0)228 615-0  
FAX +49 (0)1888 615-44 30 od. (0)228 615-44 30  
INTERNET [www.bmwa.bund.de](http://www.bmwa.bund.de)

BEARBEITET VON **Dr. Ernst Röder-Messell**

TEL.   
FAX  
EMAIL  
AZ  
DATUM Bonn, 19. März 2003

nachrichtlich:

Regulierungsbehörde für Telekommunikation  
und Post  
Referat IS 15  
Canisiusstraße 21  
55122 Mainz

BETREFF SigG/fortgeschrittene Signaturen  
HIER Definitionen des SigG  
BEZUG Ihr Schreiben vom 26.02.2003

Sehr geehrter Herr Schmoldt,

herzlichen Dank für Ihr Schreiben vom 26.02.2003. Sie erkundigen sich nach der Auslegung des Begriffs „fortgeschrittene Signatur“ in § 2 Nr. 2 SigG.

Das Signaturgesetz setzt die Vorgaben der EG-Signatur-Richtlinie um. Dabei wurde auf die Begriffe, die das erste Signaturgesetz von 1997 geprägt hat, zurückgegriffen. Schwerpunkt des ersten Gesetzes waren die Regelungen für die heute so genannte qualifizierte Signatur.

Die Signaturrichtlinie definiert fortgeschrittene Signaturen in Art. 2 Nr. 2 als 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.

HAUSANSCHRIFT Vilmembler Straße 76, 53123 Bonn  
VERKEHRSANBINDUNG Bus 632, 634, 635, 638, 639, 643, 843

Seite 2 von 2 Dementsprechend definiert das Signaturgesetz in § 2 Nr. 2 fortgeschrittene Signaturen als elektronische Signaturen, 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,

Durch die Übernahme der vom ersten Signaturgesetz geprägten Definitionen scheint der Gesetzestext eine Abweichung von der Regelung der Richtlinie nahe zu legen. Die Definition des Signaturschlüssel-Inhaber in § 2 Nr. 9 Signaturgesetz als natürliche Personen, die Signaturschlüssel besitzen und denen die zugehörigen Signaturprüfchlüssel durch qualifizierte Zertifikate zugeordnet sind, legt die Schlussfolgerung nahe, dass auch für fortgeschrittene Signatur ein vorher ausgestelltes qualifiziertes Zertifikat notwendig ist. Dagegen definiert die Signaturrechtlinie in Art. 2 Nr. 3 den Unterzeichner als eine Person, die eine Signaturerstellungseinheit besitzt und die entweder im eigenen Namen oder im Namen der von ihr vertretenen Stelle oder juristischen oder natürlichen Person handelt.

Der systematische Zusammenhang zeigt jedoch, dass die Abweichung von der Signaturrechtlinie nicht gewollt ist. Die Definitionen in § 2 Nr. 7 bis Nr. 15 SigG des Signaturgesetzes beziehen sich auf qualifizierte elektronische Signaturen. Insbesondere definiert § 2 Nr. 9 SigG den Signaturschlüssel-Inhaber einer qualifizierten Signatur nach § 2 Nr. 3 SigG. Daher ist § 2 Nr. 9 SigG nicht auf fortgeschrittene Signaturen anwendbar. Für fortgeschrittene Signaturen ist in Ausfüllung der Lücke die Definition des Unterzeichners aus Art. 2 Nr. 3 Signaturrechtlinie maßgeblich.

In teleologischer und gemeinschaftsrechtskonformer Auslegung der Definition der fortgeschrittenen Signatur ergibt sich damit, dass eine fortgeschrittene Signatur nach § 2 Nr. 2 SigG wie auch in der EG-Signatur-Richtlinie vorgesehen keine vorherige Erteilung eines qualifizierten Zertifikat voraussetzt.

Es war nicht Absicht der deutschen Umsetzung der gemeinschaftsrechtlichen Vorgaben, für die fortgeschrittenen Signaturen über die Anforderungen der Richtlinie hinauszugehen. Im Zuge der Überarbeitung des Signaturgesetzes soll dies klar gestellt werden.

Mit freundlichen Grüßen  
im Auftrag

  
Dr. Röder-Messell

## 8 Vorhaltung signierter Dokumente als Beweismittel

Aufgrund vieler Gespräche erscheint uns der Hinweis wichtig, dass vor allem die Begriffe Gültigkeit und Beweisfähigkeit in den Diskussionen oft verwechselt werden. Gültigkeit bezieht sich bei Signaturen vor allem auf die Verwendbarkeit von Zertifikaten und Verschlüsselungsalgorithmen, während sich die Beweisfähigkeit vor allem auf die erstellte Signatur bezieht.

### 8.1 Gültigkeit und Beweisfähigkeit von elektronischen Signaturen

Ordnungsgemäß erstellte elektronische Signaturen sind ab Zeitpunkt ihrer Erstellung immer gültig und unterliegen keinen zeitlichen Beschränkungen!

Ungültig werden „nur“ die zur Signaturerstellung verwendeten Verschlüsselungsalgorithmen sowie bei zertifikatsbasierten Signaturverfahren die ausgegebenen Zertifikate.

#### 8.1.1 Gültigkeit von Zertifikaten

Zertifikate sind durchschnittlich 2 – 3 Jahre gültig, maximal 5 Jahre. Gültigkeit bedeutet, dass der dem Unterzeichner zugeordnete Private Key nur während dieser Zeit für eine Signaturerstellung verwendet werden darf und dann im Trust Center, nicht jedoch auf der Karte selbst, als gesperrt markiert wird. Nach der Sperre müssen die Zertifikate für qualifizierte Signaturen und deren Public Keys noch weitere 5 Jahre vom ZDA (Zertifizierungsdienst-Anbieter) zur Identifizierung vorgehalten werden, Zertifikate für qualifizierte Signaturen mit Anbieterakkreditierung sogar 30 Jahre.

Hintergrund für die beschränkte Gültigkeit des Zertifikats und damit die Verwendbarkeit des Signaturschlüssels ist die mögliche Änderung der Länge des Signaturschlüssels oder gar die eventuelle Änderung des Verschlüsselverfahrens. Die derzeit anerkannten und gültigen Verschlüsselungsverfahren und Signaturschlüssellängen werden jährlich von der Bundesnetzagentur (früher RegTP) im Internet veröffentlicht.

#### 8.1.2 Gültigkeit von Verschlüsselungsalgorithmen

Man geht davon aus, dass in Zukunft die derzeit eingesetzten Algorithmen der Verschlüsselungsverfahren geknackt werden und damit der zur Signaturerstellung verwendete private Schlüssel aus dem öffentlichen Schlüssel (dem Public Key) errechnet werden kann.

Dann könnte ein elektronisches Dokument verändert werden, der auf Basis der veränderten Daten neu erstellte Hashwert mit dem errechneten Private Key neu verschlüsselt werden und somit Dokumenteninhalte und elektronische Signatur gefälscht werden. Als Zeitraum für die derzeitige Verwendbarkeit heutiger Verschlüsselungsalgorithmen werden im allgemeinen 6 Jahre genannt. Der tatsächliche Zeitraum dürfte deutlich höher sein. Aus Sicherheitsgründen wird aber für die geprüften Verschlüsselungsverfahren eine maximale Gültigkeit von 5 Jahren angenommen, weshalb

man die Gültigkeit von Zertifikaten und damit die Verwendung der ausgegebenen Private Keys auf diesen Zeitraum beschränkt.

### 8.1.3 Erhaltung der Beweisfähigkeit von Signaturen

Trifft man für den Zeitraum nach Ablauf der Verwendbarkeit von Verschlüsselungsalgorithmen keine Vorkehrungen, dann besteht die Gefahr, dass die Beweiskraft heute signierter jedoch nicht sicher verwahrter Dokumente zumindest in Frage gestellt werden kann. Diesem wird vorgebeugt, indem die signierten Daten sowie die erstellten Signaturen selbst mit einem aktuellen Zeitstempel versehen werden. Dieser Vorgang wird auch als Nachsignierung, manchmal auch als Übersignierung bezeichnet.

Die aktuelle Gültigkeit von Verschlüsselungsalgorithmen und die akzeptierten Schlüssellängen sind auf der Web-Site der Bundesnetzagentur (früher RegTP) veröffentlicht.

### 8.2 Ablage oder Archivierung von signierten Dokumenten?

Die Frage, ob ein signiertes Dokument in einer Ablage gehalten oder in ein elektronisches Archiv gestellt werden soll, ergibt sich aus der Frage, wann ein signiertes Dokument als Beweismittel benötigt wird. Wenn dies innerhalb von 1 - 2 Jahren nach Signierung notwendig wird, ist - unabhängig von sonstigen zu empfehlenden Sicherungsmaßnahmen - eine Vorhaltung auf einer Festplatte theoretisch ausreichend, da bei einer Signaturprüfung die Verschlüsselungsverfahren noch gültig sind.

#### 8.2.1 Nachsignierung / Übersignierung

Anders verhält es sich jedoch bei Dokumenten, die erst nach Ablauf der Gültigkeit der Verschlüsselungsverfahren als Beweismittel herangezogen werden.

Eine Möglichkeit zur Erhaltung der Beweiskraft eines elektronisch signierten Dokuments ist die sogenannte Nachsignierung vor Ablauf der Gültigkeit von Verschlüsselungsalgorithmen. Irrtümlich wird darunter manchmal verstanden, dass der ursprüngliche Unterzeichner nochmals signieren müsse. Dies ist nicht erforderlich.

Eine Nachsignierung kann durch einen – bei Bedarf qualifizierten – Zeitstempel realisiert werden. So wird bei signierten Dokumenten mit eingebetteter Signatur über die gesamte Datei ein neuer Hashwert erstellt und die neue elektronische Signatur oder der neue Zeitstempel mit den neuen Verschlüsselungsalgorithmen erstellt. Bei elektronischen Dokumenten, deren Signaturen nicht im Dokument eingebettet sind, sondern extern gehalten werden, müssen auch die externen Signaturen in den Hashwert der Nachsignatur einbezogen werden.

Die Datumsangabe bei einem Zeitstempel ist notwendig, um den Status des elektronischen Dokuments selbst sowie der dazugehörigen Signaturen zum Erstellungszeitpunkt festzuhalten. Soll ein nachsigniertes signiertes Dokument (hier liegt

kein Schreibfehler vor), geprüft werden, dann wird zuerst der Hash des Zeitstempels mit einem neu erstellten Hash verglichen und erst dann die Hashwerte der ursprünglichen Signaturen überprüft.

Nachsignierungen sind also wie Umschläge zu verstehen, die bei der Prüfung von "außen nach innen" zu prüfen sind.

### 8.2.2 Nachsignierung oder revisionssicheres Archiv?

Nachsignierungen sind natürlich aus grundsätzlichen Signaturbetrachtungen sinnvoll, berücksichtigen jedoch nicht die Möglichkeiten, die uns bereits aus dem Umfeld elektronischer Archivierung zur Verfügung stehen.

Eine Alternative zur Nachsignierung besteht durch die Übernahme des elektronischen Dokuments samt seiner elektronischen Signaturen in eine elektronisches Archiv. So können signierte Dokumente sowie auch separat gehaltene elektronische Signaturen mit einem Zeitstempel versehen werden und anschließend elektronisch archiviert werden.

Alternativ zur Nachsignierung übernimmt ab Zeitpunkt der Archivierung das elektronische Archiv die Verantwortung für die Nichtveränderbarkeit des Dokuments bzw. der elektronischen Signaturen. Für elektronische Archive, die solche Anforderungen erfüllen, hat sich - obwohl nicht immer korrekt - im Sprachgebrauch der Begriff „revisionssicheres Archiv“ etabliert.

### 8.2.3 Erhalt von Formerfordernissen durch revisionssichere Archive?

Mittels eines vom zuständigen Finanzamt abgenommenen revisionssicheren Archivs läßt sich wie bereits erwähnt die Nichtveränderung eines Dokuments sowie einer separat gehaltenen elektronischen Signatur seit Archivierung nachweisen.

Ob jedoch ein revisionssicheres Archiv ohne Nachsignierung der Dokumente auch Formerfordernisse wie z.B. gesetzliche Schriftform gewährleisten kann, ist aus unserer Sicht nicht geklärt. Zumindest haben wir dazu keine erkennbaren rechtliche Vorgaben gefunden.

Hinsichtlich der Anforderungen, die ein revisionssicheres Archiv erfüllen muß, verweisen wir an dieser Stelle auf die Publikationen entsprechender Beratungsunternehmen (siehe [Links und Kontakte](#)) sowie den VOI Verband Organisations- und Informationssysteme e.V. [www.voi.de](http://www.voi.de).

## 9 Biometrie und Unterschrift

In den letzten Jahren sind biometrische Verfahren enorm verbessert worden, so dass einem Einsatz dieser Verfahren nichts im Wege steht. Unterscheiden müssen wir allerdings passive biometrische Merkmalen wie Fingerprint oder Iriserkennung von aktiven biometrischen Merkmalen wie Spracherkennung oder eigenhändige Unterschrift.

Dabei kommt allerdings der Unterschrift eine besondere Bedeutung als Willenserklärung mit gleichzeitiger Lebenderkennung zu. Die eigenhändige Unterschrift enthält dazu eine Warn- und Schutzfunktion, da eine Unterschrift niemals ungewollt erstellt werden kann.

### 9.1 Biometrische Authentifizierungsverfahren für qualifizierte Signaturen

Biometrische Verfahren wie Finger-, Gesicht- und Iriserkennung sind Verfahren, die anhand von körpereigenen Merkmalen die Identifizierung einer Person ermöglichen und damit die PIN ersetzen können. Beim Einsatz mit qualifizierten elektronischen Signaturen soll dadurch sichergestellt werden, dass ein zugeordneter geheimer Schlüssel (Private Key) auf der Signaturkarte auch wirklich nur von der berechtigten Person freigeschaltet wird.

Demzufolge gilt laut Signaturverordnung als Anforderung an Produkte, die eine qualifizierte elektronische Signaturen leisten, dass "sichere Signaturerstellungseinheiten" (die Signaturkarte) gewährleisten müssen, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch **Besitz und Wissen** (Besitz = Karte oder Stick, etc.) oder durch **Besitz und ein oder mehrere biometrische Merkmale** angewendet werden kann". Da jedoch das sogenannte Matching (die Prüfalgorithmen) auf der sicheren Signaturerstellungseinheit, also dem Chip der Signaturkarte, ablaufen müssen (MOC = Match on Card), sind aufgrund des begrenzten Speicherraumes des Chips die biometrischen Algorithmen im Gegensatz zu einer relativ einfachen PIN Prüfung bisher nicht auf den Signaturkarten unterbringbar.

### 9.2 Eigenhändige Unterschrift für Signaturen ohne Zertifikate

Einfache und fortgeschrittene elektronische Signaturen können auch ohne Zertifikat erstellt werden. Deshalb werden von einigen Signaturanbietern eigenhändige Unterschriften zur späteren Identifizierung des Unterzeichners durch forensische Spezialisten wie Schriftsachverständige im elektronischen Dokument gespeichert und über den Hashwert der elektronischen Signatur mit den signierten Daten verknüpft.

Soweit eine Identifizierung bereits während der Signaturerstellung gewünscht ist, können sich Personen bei einem entsprechenden Authentifizierungsdienst registrieren (Enrolment) und ihre Templates (Vergleichsunterschriften) hinterlegen, anhand derer dann während jeder Signierung die Authentifizierung des Unterzeichners durchgeführt wird. Zwar ist die beschriebene Authentifizierung ein vorbeugender Schutz, die haftungsrelevante Identifizierung ergibt sich aber erst anhand der im Dokument mitgeführten eigenhändigen Unterschrift.

### 10 Welche Dokumente sind zur Signierung geeignet?

#### 10.1 Erstellung des Hashwertes

Das derzeit größte Problem ist neben die Kompatibilität der Strukturen von elektronischen Signaturen vor allem das applikationsbedingte Verfahren zur Erstellung des Hashwertes. Soweit eine Datei als Datenstrom zur Erstellung eines Hashwertes genutzt wird, der sogenannten **File-Signierung**, ist eine Hashwarterstellung recht unproblematisch.

Schwieriger wird es jedoch bei der Erstellung von Hashwerten für Dokumente, die aktiv von den verschiedensten Applikationen unter den verschiedensten Betriebssystemen im Arbeitsspeicher geladen sind. Soweit also der Aufbau des Hashwertes nicht über das gesamte Dokument (Datei-Hash) sondern über den Inhalt oder Teil-Inhalt des Dokuments erfolgt, auch **Content-Signierung** genannt, gestaltet sich die Hashwarterstellung bei jeder Applikation gänzlich unterschiedlich. So sind z.B. bei MS-Word-Dokumenten die Kopf- und Fußzeilen der verschiedenen Abschnitte einzubeziehen, Formularfelder zu berücksichtigen, etc., bei PDF Dokumenten die unterschiedlichen signierten Versionen des Dokuments.

##### 10.1.1 Signierung von Verweisen

Ein weitaus ernsteres Problem für Anwender und Signaturüberprüfende stellen Verweise auf externe dynamische Daten dar, wie z.B. Fonts, Druckdatum, Verzeichnishinweise, eingebettete Tabellen oder Bilder, Makro-bedingte Anzeigen, etc.. Für den Betrachter ist nicht transparent, ob die angezeigten Daten nun im Dokument eingebettet sind oder ob nur der Link auf die extern gehaltenen Daten in den Hashwert einbezogen wurde. Mit dem neuen PDF/A Format sind erste Schritte gemacht worden, um die Verwendung dynamische Daten in beweisrelevanten Dokumenten einzuschränken bzw. auszuschließen.

#### 10.2 Betrachtungen verschiedener Dokument-Formate

##### 10.2.1 MS-Office / Dokumente mit dynamischen Verknüpfungen

Stellvertretend für Dokumente, die unter Textverarbeitungssystemen, Tabellenkalkulationen und sonstigen Programmen, die Verknüpfungen und dynamische Daten erlauben, haben wir MS-Office betrachtet.

Für die MS-Office Produkte ist die Behandlung von Verweisen ein sehr schwieriges Thema. So müßte ein entsprechender Signaturhandler letzt endlich dafür Sorge tragen, dass weder zum Dokument gehörende noch sonstige Makros aktiviert sind. Auch um das komplette Dokument mit all seinen Bereichen, Abschnitten, Kopf- und Fußzeilen, Drucker-abhängigen Seitenanzeigen, ersetzte Schriften (falls sich die gewählte Schrift nicht auf dem Anzeige-Rechner befindet) zu überprüfen, ob es auch korrekt angezeigt wird, müßten enorme Zusatzinformationen mit jeder Signatur mitgeführt werden.

Zu der für diese Prüfungen notwendigen Rechenzeit kommen noch Prüfungen, ob bei geringer Farbauflösung nicht erkennbare Schriftzeichen bei einer höheren Farbauflösung doch sichtbar würden und ob bei jedem einzelnen Zeichen Vordergrundfarbe gleich Hintergrundfarbe ist. Neben den teilweise nicht mehr zumutbaren Rechenzeiten auch mit sehr schnellen Rechnern kommt dazu, dass nicht nur applikationsbedingte Einstellungen berücksichtigt werden müssen, sondern auch systemabhängige Einstellungen (Zeichendarstellung Byte oder Doppelbyte) in den Hashwert einbezogen werden müssten.

Natürlich werden MS-Office Produkte stets weiterentwickelt, was oft dazu führt, dass sich der Aufbau der mit diesen Produkten erstellten Dokumente verändert. So werden bei MS-Word ältere Dokumente von neuen Applikationsversionen beim Laden des Dokuments konvertiert. Soweit also Funktionen der Applikation (z.B. Word, Excel) zur Datenermittlung innerhalb des Dokuments verwendet werden, kann dies mit konvertierten älteren Dokumenten bei der Hasherstellung zur Signaturprüfung einen anderen Hashwert ergeben.

Dies bedeutet, dass – vorausgesetzt, man würde alle relevanten Daten in den Hash mit einbeziehen – sehr wahrscheinlich eine Signaturprüfung nur unter der derjenigen Version der Applikation durchgeführt werden kann, unter welcher auch die Signatur und damit der in der Signatur mitgeführte Hash erstellt wurde. Dies betreffe unter Umständen auch die Betriebssystem-Version.

MS-Office Produkte sollten daher nur dann zur Content-Signierung verwendet werden, wenn das signierte Dokument innerhalb von wenigen Jahren nach Signierung als Beweismittel verwendet werden wird.

### 10.2.2 TIFF

TIFF Formate, also reine Bilddateien, bieten hinsichtlich der Lesbarkeit des Formats große Chancen, auch noch in 30 – 50 Jahren interpretiert und angezeigt werden zu können.

Es sei jedoch darauf verwiesen, dass TIFF selbst keinen Standard darstellt, sondern nur die Komprimierung von TIFF – Dateien standardisiert ist. Die einzelnen TIFF – Formate können also untereinander erheblich abweichen. Es sollte also genau geprüft werden, welches TIFF – Format eingesetzt werden soll. Dies gilt besonders dann, wenn die elektronische(n) Signatur(en) in die TIFF – Datei eingebettet werden soll.

Für Mehrfachsignaturen durch unterschiedliche Personen in echten Workflowsystemen besteht die Möglichkeit, TIFF-Dokument und die Signaturen getrennt zu verwalten.

Es ist also auch beim TIFF – Format Vorsicht geboten, dass die fälschlich oft angenommene Gewährleistung der Formatlesbarkeit nicht durch ein proprietäres TIFF – Format oder eine proprietäre Verwaltung der zusätzlichen Signaturen erkaufte wird.

TIFF Formate (aber auch vermehrt JPEG) werden derzeit vorrangig als Nachweisdokumente wie z.B. beim Scannen buchungsrelevanter Daten erstellt und als Datei signiert (File-Signatur).

### 10.2.3 XML

Obwohl sich XML als eine Standard Datenbeschreibung etabliert, ist auch hier die eventuelle Proprietät bei der Verwaltung signierter XML-Daten zu berücksichtigen. Auch bei XML werden die Anzeigeformate, die darin gezeigten und signierten Daten sowie die Signaturen getrennt verwaltet. Zur Validierung einer Signatur müssen neben den Daten selbst auch die Anzeigetemplates für den gesamten Lifecycle des Dokuments vorgehalten werden.

Eine Signierung eines XML Datensatzes macht erst dann Sinn, wenn in dem XML-Datensatz selbst auch die relevanten Anzeige – Informationen der XML-Daten im entsprechenden Kontext enthalten sind oder zu dem XML-Datensatz kein spezieller Kontext vonnöten ist.

### 10.2.4 Adobe - PDF

Adobe PDF Dokumente sind als einziges Format für eine Content-Signierung geeignet, da die Signierung auf den "Hintergrund" und Formularfelder beschränkt werden kann. Bei eventuell eingebettete Links wird der Signaturvorgang abgebrochen. Kommentare werden in der Regel nicht in den Hash einbezogen.

Aus den meisten Applikationen können PDF Dokumente erstellt werden und diese dann als Willenserklärungen, Bestätigungen, Dokumentationen etc. signiert und archiviert werden. Allerdings sei hier der Hinweis erlaubt, dass es nur sehr wenige Signatur-Anwendungen für PDF gibt, die eine gesicherte Anzeige (Secure Viewer) durch entsprechendes Abfangen nicht eingebetteter Informationen (Fonts, Streams, etc.) ermöglichen.

Die durch Adobe unterstützten PDF Spezifikationen erlauben ab Version 1.5 die Nutzung von Signaturfeldern. Mit der Einführung solcher Signaturfelder können sämtliche für eine elektronische Signatur relevante Daten gespeichert und im PDF Dokument mitgeführt werden. Es sei darauf verwiesen, dass nur solche PDF Signaturverfahren verwendet werden sollten, die sich exakt an die PDF Spezifikationen für elektronische Signaturen halten. In der Regel ist dies das Byte-Range Verfahren.

Adobe PDF ist das bisher einzige Format, das eine Content - Signatur mit Mehrfachsignaturen sowie Bereichsignaturen für echten Workflow - Einsatz erlaubt. Einige Anbieter verwenden auch freie Open Source Libraries für PDF, die sich jedoch nur bedingt an die PDF Spezifikationen halten und hinsichtlich der Kompatibilität von Signaturen als proprietär einzuschätzen sind.

### 10.2.5 PDF/A

Derzeit wird im Bereich der Langzeitarchivierung insbesondere das neue PDF/A Format diskutiert. Dies soll die bereits oben geschilderten bei Signaturen auszuklammernden Bereiche wie externe Links berücksichtigen. Im Gegensatz zu unserer Aussage in der Version 4.0 dieses Leitfadens mußten wir uns von Adobe belehren lassen, dass PDF/A sehr wohl auch Signaturfelder berücksichtigt, zumindest ab der noch in 2006 zu erwartenden Acrobat Version 8.

### 10.2.6 PDF – Open Source

An dieser Stelle ist äußerste Vorsicht geboten. Viele Personen unterliegen leider der falschen Annahme, der Begriff PDF selbst stehe bereits für einen Standard. Die wenigsten Anbieter erfüllen die Anforderungen der PDF-Spezifikationen für elektronische Signaturen. So werden z.B. anstelle der Signaturfelder die Kommentarfelder zur Ablage der Signaturen genutzt, was natürlich bei einer zweiten Signatur oder bei einer Signatur mit einem anderen Verfahren automatisch zu Inkompatibilitäten und damit in der Regel auch zur Ungültigkeit von bereits erstellten Signaturen kommt.

### 10.2.7 E-Mails

E-Mails sind im S/MIME Format signierbar. Dazu gibt es eine gewisse Konformität, soweit bestimmte Umgebungsparameter von den Clients eingehalten werden.

Allerdings sei hier darauf verwiesen, dass E-Mails derzeit nicht durch mehrere Personen signierbar sind. Sicherlich werden signierte Dokumente weiterhin als Anhang versendet, da E-Mails kaum im Sinne von Formularen oder Verträgen eingesetzt werden. Die Signierung von E-Mails betrifft eher die unverfälschte Übersendung von Informationen und bei qualifizierten Signaturen die Möglichkeit der Überprüfung, ob die E-Mail tatsächlich vom angegebenen Absender stammt.

## II Technische Aspekte

Mit den nachfolgenden, zum Teil sehr vereinfachenden Ausführungen sollen technische Komponenten und Aspekte von elektronischen Signaturen lediglich in ihrem wesentlichen Kern verständlich gemacht werden. Sicherheitsanforderungen an die Systemumgebung – im SigG auch Anwendungskomponenten genannt - während einer Signatur-Erstellung werden mit diesen Ausführungen nicht berücksichtigt. Auch Aspekte zur Verschlüsselung von Dokumenten und sicherer Datenübertragung werden hier nicht behandelt. Eine exzellente Beschreibung von Verschlüsselungs- und Hash-Algorithmen sowie weiterer tiefergehender technischer Aspekte zur elektronischen Signatur finden Sie in der 2006 erschienenen Publikation **Grundlagen der elektronischen Signatur** des BSI, erschienen bei der SecuMedia Verlags-GmbH, ISBN 3-922746-74-8, [info@secumedia.de](mailto:info@secumedia.de).

### II.1 Die grundsätzliche Struktur einer elektronischen Signatur

Aus den zu signierenden Daten wird ein Hashwert (Prüfsumme) gebildet, der in der sogenannten Signatur, einer Datenstruktur, mitgeführt wird. Bildet man zu einem späteren Zeitpunkt mit dem selben Hashverfahren den Hashwert erneut aus den signierten Daten, dann muß sich aus den signierten Daten exakt der selbe Hashwert ergeben, ansonsten sind die Daten nach ihrer Signierung verändert worden.

Es ist daher sicherzustellen, dass der bei der Signierung erstellte Hashwert nicht mehr verändert werden kann. Aus diesem Grund wird der Hashwert während der Signaturerstellung verschlüsselt und für eine Signaturprüfung entschlüsselt, um ihn gegen einen erneut erstellten Hashwert auf Gleichheit zu vergleichen.

Einfache elektronische Signaturen können dazu einen symmetrischen Schlüssel verwenden. Das bedeutet, dass zur Verschlüsselung und zur Entschlüsselung des Hashwertes der selbe Schlüssel verwendet wird. Dieses Verfahren hat jedoch einen großen Nachteil. Wer nämlich den symmetrischen Schlüssel kennt, kann - zumindest theoretisch – die Daten ändern und den daraus resultierenden neuen Hashwert erneut verschlüsseln und damit eine gefälschte Signatur erstellen.

Um diesen Nachteil symmetrischer Verschlüsselung auszuschließen, werden für fortgeschrittene und qualifizierte Signaturen zur Signaturerstellung per SigG §2 Nr.4 einmalige Signaturschlüssel gesetzlich vorgeschrieben und deshalb asymmetrische Verschlüsselungsverfahren eingesetzt.

Der Vorteil der asymmetrischen Verschlüsselung besteht darin, dass

- I. der Hashwert mit dem Public Key des asymmetrischen Schlüsselpaares von jedermann entschlüsselt und damit gegen einen neu erstellten Hashwert verglichen werden kann (Signaturprüfung) und

2. ein nach einer Datenänderung neu erstellter Hashwert nicht durch Unbefugte verschlüsselt werden kann, da der Private Key weder bekannt ist, noch aus dem Public Key errechnet werden kann.

### 11.2 Beispiel einer symmetrischen Verschlüsselung

Eines der einfachsten symmetrischen Verschlüsselungsverfahren ist die bitweise Verschlüsselung. Im nachfolgenden Beispiel wird das XOR – Verfahren gezeigt. Dabei wird jedes einzelne Bit eines Wertes mit dem an gleicher Stelle sitzenden Bit eines anderen Wertes verglichen. Als Ergebnis des XOR Verfahrens (exklusives Oder, entweder oder) wird binär 1 gesetzt, wenn nur **einer** der beiden Bit-Vergleichswerte gleich 1 ist.

#### Binäre XOR Verschlüsselung:

Dezimal 65	HEX 41	Binär 0100 0001	Zeichen "A" (das Datum)
Dezimal 51	HEX 33	Binär 0011 0011	Zeichen "3" (der Schlüssel)
Dezimal 114	HEX 72	Binär 0111 0010	Zeichen "r" (verschlüsseltes Byte)

#### Binäre XOR Entschlüsselung:

Dezimal 114	HEX 72	Binär 0111 0010	Zeichen "r" (Verschlüsseltes Datum)
Dezimal 51	HEX 33	Binär 0011 0011	Zeichen "3" (der Schlüssel)
Dezimal 65	HEX 41	Binär 0100 0001	Zeichen "A" (das Original - Datum)

Natürlich sind in der Praxis die Schlüssel nicht wie in unserem Beispiel lediglich 8 Bit groß, sondern eben 40 Bit, 128 Bit oder noch größer. Auch wird natürlich nicht das doch recht einfache XOR Verfahren verwendet, sondern wesentlich komplexere Verschlüsselungsverfahren.

Asymmetrische Verschlüsselungsalgorithmen arbeiten teilweise bereits mit Schlüssellängen von 4096 Bit.

### 11.3 Symmetrische Verschlüsselung

Symmetrische Verschlüsselungsverfahren bzw. deren Schlüssel können wie oben dargestellt zum Verschießen und zum Öffnen genutzt werden, wie für eine Wohnungstür. Dabei ist jedoch nicht der Schlüssel selbst entscheidend, ob es sich um eine symmetrische Verschlüsselung handelt, sondern die dazu verwendeten Verschlüsselungsalgorithmen.

### **Vorteil symmetrischer Verschlüsselungsverfahren**

Mit symmetrischen Verschlüsselungsalgorithmen können große Daten (z.B. Text, Bilder) aufgrund ihrer geringeren Schlüssellänge schneller als mit asymmetrischen Algorithmen verschlüsselt werden.

### **Nachteil symmetrischer Verschlüsselungsverfahren**

Der Nachteil ist, dass jeder, der den Schlüssel kennt, die Information entschlüsseln, dann ändern und schließlich wieder mit dem selben Schlüssel verschlüsseln kann – und keiner merkt es.

### 11.4 Asymmetrisches Verschlüsselungsverfahren

Asymmetrische Verschlüsselungsalgorithmen benötigen immer zwei Schlüssel. Verschlüsselt man eine Information mit einem der beiden Schlüssel, kann man die verschlüsselte Information nur mit dem anderen Schlüssel wieder entschlüsseln.

Einen der beiden Schlüssel hält man geheim, dies ist der Private Key. Den anderen Schlüssel stellt man der Öffentlichkeit zur Verfügung, dieses ist der Public Key.

Asymmetrische Schlüssel sind sehr komplex (2048 oder 4096 Bit), was die Errechnung des Private Keys aus dem öffentlich bekannten Public Key verhindern soll.

#### Vorteil einer asymmetrischen Verschlüsselung

Werden Daten mit einem Private Key verschlüsselt, dann kann zwar jeder die Information mit dem Public Key entschlüsseln (was beim Hashwert einer elektronischen Signatur ja gewollt ist), aber nicht erneut verschlüsseln, da der Private Key unbekannt ist.

Werden hingegen Daten mit einem Public Key verschlüsselt, dann kann nur der Besitzer des korrespondierenden Private Keys diese Daten wieder entschlüsseln, was i.d.R. für die Verschlüsselung von geheimen Informationen eingesetzt wird.

#### Nachteil einer asymmetrischen Verschlüsselung

Asymmetrische Verschlüsselungsverfahren sind wegen der Komplexität der Schlüssel (2048 oder 4096 Bit) sehr langsam und daher nur zur Verschlüsselung kleiner Datenmengen wie z.B. den Hashwert einer Signatur geeignet. Das inzwischen als kritisch betrachtete Verfahren MD5 liefert z.B. einen 128 Bit großen Wert, das SHA Verfahren einen 160 bis 512 (SHA 512) Bit großen Wert.

Bei großen Datenmengen wie Dokumenten verwendet man daher asymmetrische Algorithmen in Kombination mit symmetrischen Verschlüsselungsverfahren, indem man zuerst einen symmetrischen Key erzeugt und dann z.B. einen Text mit diesem symmetrischen Key (hier auch Session Key genannt) verschlüsselt und dann den "kleinen" symmetrischen Key mit einem asymmetrischen Key verschlüsselt. Dabei muß der verschlüsselte Session Key natürlich mitgeführt werden, da die Entschlüsselung auch nur 2-stufig erfolgen kann.

#### Verwendung asymmetrischer Schlüsselpaare für Signaturen

Verschlüsselt man einen Hashwert mit einem Private Key, kann jeder mit dem dazugehörigen Public Key den Hashwert entschlüsseln und gegen einen neuen Hashwert vergleichen, aber wie bereits beschrieben nicht erneut mit dem unbekanntem Private Key verschlüsseln. Dieses Verfahren wird bei der Erstellung einer elektronischen Signatur bzw. bei der Verschlüsselung des Hashwertes verwendet.

Soweit einer Person ein asymmetrisches Schlüsselpaar in Form eines elektronischen Zertifikats, welches u.a. auch den Public Key beinhaltet, zugeordnet ist, kann man als zusätzliche Funktionalität deren Identität und weitere Informationen über den Zertifikatsinhaber über einen öffentlichen Verzeichnisdienst (ein im Internet verfügbarer Server des ZDA) ermitteln. Daher kommt die Bezeichnung Public Key Infrastructure (PKI).

### 11.5 Der Hash(-wert)

Eigentlich müßte man von dem Hashwert sprechen, aber in der Informationstechnologie wird oft nur der Begriff „Hash“ verwendet.

Der Hash ist schlicht das Ergebnis eines hochkomplexen Prüfsummenverfahrens. Mit standardisierten Hash-Verfahren (z.B. MD5, SHA-1, etc.) kann der Hashwert von Daten erstellt werden. Dabei können auch Daten nacheinander in den Hashwert einbezogen werden, z.B. einzelne Felder eines PDF-Dokuments. Aus dem Hashwert können jedoch die Daten nicht wieder ermittelt werden. Hash-Verfahren funktionieren also nur in eine Richtung.

Die wiederholte Verwendung des selben Hash-Verfahrens für die selben Daten (z.B. ein elektronisches Dokument oder Teile eines Dokuments) muß den selben Hashwert ergeben. Kommt ein anderer Wert heraus, dann sind die Daten zwischenzeitlich geändert worden. Dieser Vergleich ist die Signaturprüfung.

#### 11.5.1 Datei- / File-Signierung

Unter File-Signierung wird die Einbeziehung der gesamten Datei in den Hashwert der Signatur verstanden. Dabei wird in der Regel die Signatur getrennt von der eigentlichen Datei gehalten bzw. verwaltet, manche Applikationen ermöglichen ein "Anhängen" der elektronischen Signatur an die signierte Datei.

Diese Methode der Hashwert-Erstellung ist vor allem für solche Dokumente geeignet, die nach ihrer Signierung nur noch für Beweiszwecke abgelegt werden. Eine Mehrfachsignierung ist durch Erstellung mehrerer Signaturen ebenfalls möglich, die zusätzlichen Signaturdateien müssen entsprechend verwaltet werden.

Die Signatur-Erstellungs- und Signatur-Validierungsmodule sind selbständige Anwendungen, die unabhängig vom Dokumententyp den Hashwert erstellen. Die Hashwert-Erstellung erfolgt auf Betriebssystem- bzw. Dateiebene.

#### 11.5.2 Inhalt- / Content-Signierung

Bei einer Content - Signierung werden nur bestimmte Teile, Bereiche, Felder eines elektronischen Dokuments in den Hashwert einbezogen. Eine solche Hashwert-Erstellung kann nur auf Applikationsebene erfolgen, d.h. ein PDF-Dokument muß durch eine Applikation wie Acrobat, Adobe Reader oder andere die jeweiligen Formate lesbaren Applikationen geöffnet sein. Die Hashwert - Erstellung erfolgt durch ein für die

jeweilige Applikation entwickeltes PlugIn, das den Hashwert an die Signaturerstellungskomponente weitergibt.

Der zuerst scheinbare Nachteil der Content - Signierung auf Applikationsebene wandelt sich jedoch dann zum Vorteil, wenn es sich bei den elektronischen Dokumenten um Dokumente eines Sachbearbeitervorgangs handelt. Für jeden Prozeß - Schritt können Daten aus der Anwendungsapplikation dynamisch geladen und signiert werden und somit ein einziges Dokument für mehrere Workflow - Schritte als Beweismittel gehalten werden.

So können z.B. im Bereich Antragsstellung die Ergebnisse der Sachbearbeiterprüfung ergänzend zum Bearbeitungssystem (z.B. XML - basierte Anwendung) in das bereits vom Antragsteller signierte Dokument importiert werden und vom Sachbearbeiter unterzeichnet werden.

Content - Signierungen bedingen bei Massensignaturen durch das Öffnen und Schließen der Dokumente einen geringeren Durchsatz, ermöglichen jedoch enorme Einsparungen bei der Signaturverwaltung, da die Signaturen direkt im Dokument abgelegt werden.

### 11.6 Das Zertifikat

Ein elektronisches Zertifikat ist eine elektronische Bescheinigung, dass einer Person der Public Key eines neu erstellten asymmetrischen Schlüsselpaares zeitlich begrenzt zugeordnet wurde und die bürgerliche Identität der Person nach bestimmten Regeln vorab (z.B. bei der Antragsstellung für eine Signaturkarte) festgestellt wurde. Ein Zertifikat kann derzeit nur an Personen und nicht an Unternehmen oder Institutionen ausgegeben werden. Allerdings gibt es seit 2006 Bestrebungen des Signaturbündnisses, auch Unternehmenszertifikate rechtlich zu ermöglichen.

Qualifizierte Zertifikate dürfen nur von registrierten Zertifizierungsdiensteanbietern (ZDA, Trust Center) ausgestellt werden. Der internationale Begriff für ZDA ist CA (Certificate Authority). Es gibt Zertifikate in verschiedenen Abstufungen. Dies richtet sich nach dem Status des jeweiligen Zertifizierungsdiensteanbieters, welche Arten von Zertifikate dieser anbieten darf, z.B. für fortgeschrittene oder qualifizierte Signaturen.

### 11.7 Qualifizierte elektronische Signatur

Bei einer qualifizierten elektronischen Signatur muß der Unterzeichner Inhaber eines zum Zeitpunkt der Signaturerstellung (noch) gültigen, qualifiziert zugewiesenen Zertifikats sein und ihm somit vom ZDA der Public Key eines asymmetrischen Schlüsselpaar zugeordnet worden sein. Der zum Public Key korrespondierende Private Key sowie eine 6-stellige PIN werden auf einer Signaturkarte abgelegt und die Signaturkarte dem Antragsteller ausgehändigt.

Unabhängig von der rechtlichen Einordnung (einfache / fortgeschrittene / qualifizierte Signatur) ist eine auf Zertifikaten aufsetzende elektronische Signatur eine Datenstruktur, die folgende wesentlichen Informationen enthält:

- Hashwert (z.B. des Dokumenteninhalts)
- Angaben über das genutzte Hash-Verfahren
- Angaben über das genutzte Verschlüsselungs-Verfahren
- Public Key (des Zertifikats-Inhabers)

Eine solche Datenstruktur könnte ohne Sicherheitsvorkehrungen natürlich verändert werden. Deshalb wird der in der elektronischen Signatur hinterlegte Hashwert mit dem Private Key des Zertifikatsinhabers verschlüsselt. Es sei hier nochmals der Hinweis erlaubt, dass lediglich Bestandteile der elektronischen Signatur verschlüsselt werden (z.B. der Hashwert), nicht jedoch die signierten Daten selbst.

Dieses Signaturverfahren hat mehrere Vorteile. Durch den Public Key kann nun der Hashwert von einer entsprechenden Prüfsoftware entschlüsselt und für eine Signaturprüfung herangezogen werden, nach eventueller Veränderung der Daten jedoch nicht mit dem selben Private Key erneut verschlüsselt werden, da der Private Key unbekannt ist. Mit dem Public Key kann das Zertifikat und damit die Identität des Unterzeichners online ermittelt werden (somit der Unterzeichner identifiziert werden) und durch die nochmalige Erstellung des Hashwertes und dessen Vergleich gegen den in der Signatur gespeicherten und mit dem Public Key entschlüsselten Hashwert läßt sich die Integrität des Dokumenteninhalts überprüfen.

Ein Nachteil der qualifizierten elektronische Signatur ist die wegen des Zertifikats und der damit verbundenen Zuordnung eines asymmetrischen Schlüsselpaares vorher notwendige Registrierung des Unterzeichners. Qualifizierte Signaturen können nur von registrierten Personen erstellt werden.

Einen Unsicherheitsfaktor stellen jedoch solche Signaturen dar, die mit Signaturkarten erstellt werden, deren Zertifikate bereits abgelaufen, nicht erneuert und damit ungültig sind. Man kann mit ungültigen Signaturkarten Dokumente in den ursprünglichen Gültigkeitszeitraum des Zertifikats zurückdatiert signieren. Will man den Signaturzeitpunkt eindeutig festhalten, benötigt man in Ergänzung zur Signatur noch einen sogenannten Zeitstempel.

### 11.7.1 Sicherheitsanforderungen

Bezüglich Sicherheitsanforderungen müssen mehrer Aspekte unterschieden werden:

- Bei der Erstellung und Zuweisung von asymmetrischen Schlüsselpaaren zu Personen (wobei der jeweilige Public Key im Zertifikat enthalten ist) werden insbesondere bei qualifizierten Signaturen sehr hohe Sicherheitsanforderungen an die ZDAs (Zertifizierungsdiensteanbieter) gestellt, da mit der Zuordnung eines Zertifikats bzw. des Public Keys eine entsprechende Haftung für den Antragsteller einer Signaturkarte entsteht (s. ZPO § 371a).

- Die technische Beschaffenheit des Chips einer Signaturkarte für qualifizierte Signaturen, auch sichere Signaturerstellungseinheit (SSEE, international SSCD – Secure Signature Creation Device) genannt, unterliegt ebenfalls sehr hohen Sicherheitsanforderungen, da dort der einmalig existierende Private Key des asymmetrischen Schlüsselpaares sowie die 6-stellige PIN oder biometrische Merkmale, die zur Freischaltung des Private Keys dienen, nicht auslesbar hinterlegt sind. Außerdem ist auf dem Chip auch das jeweilige Authentifizierungsverfahren, das sogenannte Matching hinterlegt, in der Regel ein PIN-Prüfverfahren.
- Für die Freischaltungsprüfung des Private Keys zur Signaturerstellung durch den Unterzeichnenden – auch Authentifizierung genannt - wird fast ausschließlich das PIN-Verfahren verwendet. Es sind neben Wissensverfahren auch biometrische Verfahren erlaubt, jedoch praktisch nicht im Einsatz.
- Bei der Erstellung von qualifizierten Signaturen "sollen" sichere Anwendungs-komponenten verwendet werden. Dies betrifft u.a. die Kartenlesegeräte und die Softwarekomponenten, die für die Hasherstellung und die Anzeige der zu signierenden Daten zuständig sind. Ob jedoch solch sichere Komponenten tatsächlich verwendet wurden, ist über die erstellte Signatur nachträglich nicht mehr nachprüfbar. Der Signaturersteller müßte sich vor jeder von ihm erstellten Signatur davon überzeugen, ob er tatsächlich eine sichere Anwendungskomponente benutzt.

### 11.8 Erstellung zertifikatsbasierter Signaturen mit Signaturkarte

Nach der Beantragung einer Signaturkarte und erfolgreicher Feststellung der bürgerlichen Identität wird vom ZDA ein asymmetrisches Schlüsselpaar erstellt und der Private Key auf der Signaturkarte hinterlegt. Der Public Key wird in Form eines Zertifikats dem Antragsteller zugeordnet, ebenfalls auf der Signaturkarte hinterlegt und zusätzlich in einem Verzeichnisdienst veröffentlicht. Der Unterzeichner bzw. Signaturersteller (Benutzer der Signaturkarte und damit des Private Keys) ist damit über den Public Key ermittelbar.

Damit nur der Eigentümer einer Signaturkarte elektronische Signaturen erstellen kann, werden vom ZDA auf der Signaturkarte zusätzlich eine nicht auslesbare 6-stellige PIN oder biometrische Daten (praktisch nicht vorkommend) hinterlegt. Der Private Key wird erst dann zur Signaturerstellung verwendet, nachdem der Signaturersteller die korrekte PIN eingegeben hat (Authentifizierung).

Praktisch fordern Software-Anwendungen (Anwendungskomponenten) während eines Signiervorgangs den Signaturersteller auf, die Signaturkarte in das entsprechende Kartenlesegerät einzuführen und seine PIN einzugeben.

Nach Freischaltung des Private Keys wird nun in dem Chip der Signaturkarte (der Signaturerstellungseinheit) der von der Anwendungskomponente erstellte und an die Signaturerstellungseinheit (den Chip) übergebene Hash des Dokumenteninhalts mit dem Private Key verschlüsselt und eine elektronische Signatur mit den entsprechenden

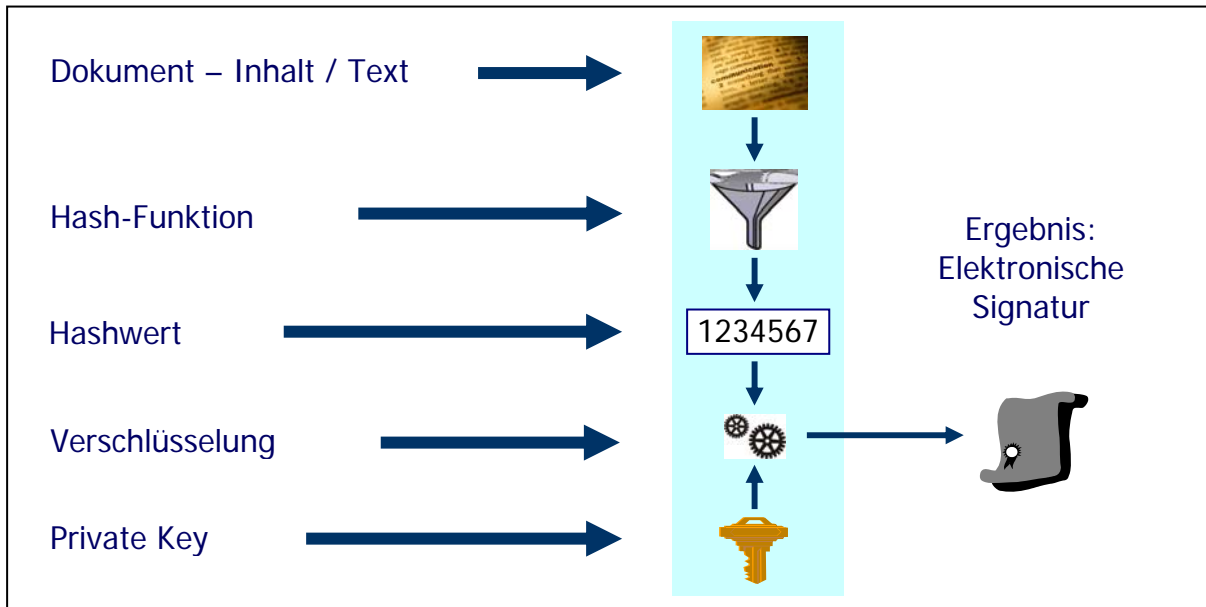
# StepOver

## Leitfaden zur e-Signatur

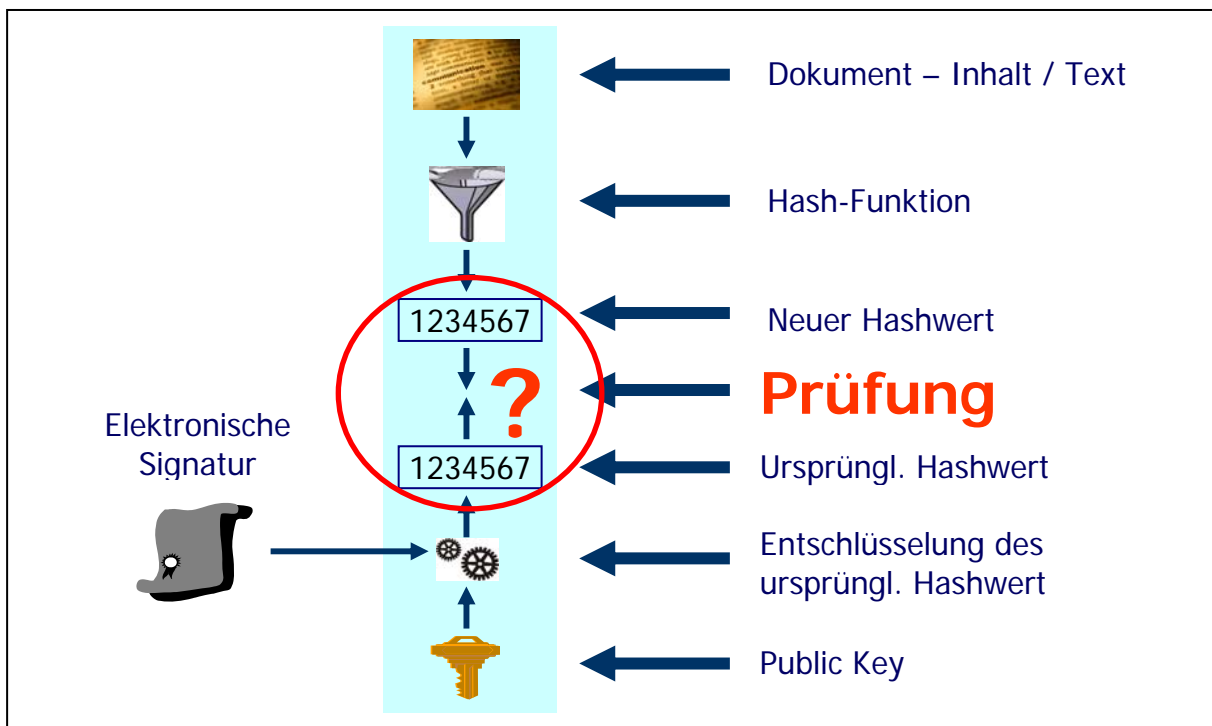
Step Over  
the next step in business

Inhalten erstellt. Anschließend gibt die Signaturkarte die elektronische Signatur an die Anwendungskomponente zurück, von der die Signatur dann als Signatur-Datei (File-Signatur) zur Verfügung gestellt wird oder in das Dokument eingebettet wird (Content-Signatur).

### 11.9 Graphische Darstellung der Signaturerstellung und deren Prüfung



Durch erneute Erstellung des Hashwertes kann zu jedem beliebigen Zeitpunkt durch Vergleich gegen den in der elektronischen Signatur gehaltenen Hashwert die Integrität des Dokuments / der Daten überprüft werden.



Falls der Signaturersteller ein Zertifikat besitzt, kann anhand des Public Keys das zugehörige Zertifikat beim ZDA und darüber der gültige Verwendungszeitraum der Signaturkarte (bzw. des Private Keys) sowie die bürgerliche Identität des Signaturerstellers ermittelt werden.

Zwar wird per Gesetz angenommen, dass der Signaturersteller auch der rechtmäßige Karteninhaber ist, doch beweisen kann man dies nicht. Aus diesem Grund wurde für qualifizierte Signaturen der Anschein der Echtheit (seit April 2005 ZPO § 371a, früher ZPO § 292a) eingeführt, womit die Haftung für die Verwendung der Signaturkarte dem Karten-Eigentümer (=Zertifikatsinhaber) auferlegt wird.

### 11.10 Fortgeschrittene elektronische Signatur

Eine zertifikatsbasierte fortgeschrittene Signatur kann technisch genauso wie eine qualifizierte elektronische Signatur erstellt werden, allerdings sind die Sicherheitsanforderungen an die technischen Signaturkomponenten sowie an die Zertifikatserstellung geringer als an qualifizierte Signaturen.

*Zur Erstellung einer fortgeschrittenen elektronischen Signatur muß ein Unterzeichner kein Zertifikat besitzen, d.h. eine Zuordnung eines asymmetrischen Schlüsselpaares zum Unterzeichner ist nicht erforderlich.*

Zwar müssen bei fortgeschrittenen Signaturen die selben Sicherungsverfahren mittels einmaliger kryptographischer Schlüssel (asymmetrische Verfahren) verwendet werden, doch können bei fortgeschrittenen Signaturen neben zertifikatsbasierten Identifizierungsverfahren auch andere Identifizierungsverfahren eingesetzt werden. Dazu verweisen wir auf das Schreiben des BMWA vom 19.03.2003 sowie das am 11. Januar in Kraft getretene 1. SigÄndG.

Allerdings muß (wie auch bei einer qualifizierten Signatur)

1. der Unterzeichner identifizierbar sein
2. der Unterzeichner die Signatur mit Mitteln erstellen können, die seiner alleinigen Kontrolle unterliegen,
3. die Signatur ausschließlich dem Unterzeichner zugeordnet werden können,
4. die Veränderung von Daten erkennbar sein,
5. die elektronische Signatur mit einem einmaligen Code oder Private Key verschlüsselt werden und
6. der Unterzeichner im Besitz einer Signaturerstellungseinheit sein

### 11.11 Nicht-qualifizierte Signaturen mit eigenhändiger Unterschrift

Soweit der Unterzeichner nicht im Besitz eines Zertifikats ist, kann bei gleicher Sicherheit der elektronischen Signatur die Identifizierung mit anderen Mitteln und erst bei Bedarf, also nach Signaturerstellung erfolgen. Als Alternative zur zertifikatsbasierten Identifizierung bietet sich die eigenhändige Unterschrift an.

### II.11.1 Signaturerstellung mit Signaturdienst

Da einem zertifikatslosen Unterzeichner kein asymmetrisches Schlüsselpaar zugeordnet ist, kann daraus folgernd der Unterzeichner zur Erstellung der elektronischen Signatur und asymmetrischen Verschlüsselung des Hash auf ein fremdes asymmetrisches Schlüsselpaar zurückgreifen, das ihm z.B. von einem Signaturdienst zur Verfügung gestellt wird. Allerdings wird dem Unterzeichner nicht der Schlüssel ausgehändigt, sondern der Signaturdienst erstellt die Signatur für den Unterzeichner.

#### Der Ablauf:

Der Unterzeichner unterschreibt entweder auf einem Grafik- oder Schreibtablett oder auf der Schreibfläche eines Tablet-PCs. Dabei wird die gesamte Schreibdynamik erfaßt. Dies sind im wesentlichen X,Y-Position und Schreibdruck sowie Schreibgeschwindigkeit und Beschleunigung. Für die erfaßte Unterschrift wird nun ein symmetrischer Schlüssel von der Signatursoftware generiert, mit dem die Unterschrift verschlüsselt wird. Danach wird die verschlüsselte Unterschrift im elektronischen Dokument abgelegt.

Anschließend wird der symmetrische Schlüssel durch einen in der Software mitgeführten Public Key verschlüsselt und der verschlüsselte symmetrische Key ebenfalls im Dokument abgelegt.

Danach wird ein Hashwert unter Einbezug des Dokumenteninhalts sowie der verschlüsselten Unterschrift und des verschlüsselten symmetrischen Keys gebildet und wie bei einer qualifizierten Signatur eine elektronische Signatur erstellt, die dann anstatt mit dem Private Key des Unterzeichners (dem ja keiner zugewiesen wurde) z.B. mit dem Private Key eines Signaturdienstes verschlüsselt wird.

Die derart erstellte elektronische Signatur kann genauso wie bei einer qualifizierten Signatur mit dem Public Key entschlüsselt werden und durch Neuerstellung des Hashwertes kann die Integrität des Dokuments überprüft werden. Gleichzeitig ermöglicht dies auch die Integritätsprüfung der verschlüsselten Unterschrift sowie des verschlüsselten symmetrischen Schlüssels.

Die beweisrelevante Identifizierung der Person wird wie bei Papierdokumenten erst bei Bedarf durchgeführt. Im Streitfall vor Gericht wird vom Signaturdienst mit dem Private Key des Signaturdienstes zuerst einmal der symmetrische Schlüssel entschlüsselt, mit dem wiederum die Unterschrift entschlüsselt wird.

Die dann in ihrer ursprünglichen Form vorliegende Unterschrift wird dazu genutzt, die gesamte Schreibdynamik der Unterschrift 3-dimensional darzustellen, anhand der ein Schriftsachverständiger durch Vergleich gegen erneut abzugebende Unterschriftenproben die Identifizierung des Unterzeichners durchführen kann.

Neben der Erfüllung aller sicherheitsrelevanter Aspekte eliminieren Verfahren mit eigenhändigen Unterschriften u.a. auch das Problem der PIN-Ausspähung und der Lebenderkennung bei der Signaturerstellung.

### 11.11.2 Signaturerstellung ohne Signaturdienst

Lokale Signaturerstellung ohne Signaturdienst und ohne Signaturkarten ist ebenfalls möglich. Die Verwendung von asymmetrischen Schlüsseln zur Signaturerstellung gestaltet sich jedoch sehr problematisch. So könnte ein Private Key nicht an ein einziger Stelle (Signaturkarte oder auf dem Server eines Signaturdienstes) gehalten werden, sondern müßte mit der Anwendungskomponente (der Software) jedes Mal mit ausgeliefert werden. Damit würde die gesetzliche Anforderung gemäß §2 Abs. 4 SigG an fortgeschrittene Signaturen nicht erfüllt.

Ein solches auf – in der Software hinterlegten – Schlüsseln und lokaler Rechnerzeit basierendes Signaturverfahren eignet sich kaum für die Signierung beweisrelevanter Dokumente. Solche Verfahren dienen eher für interne Prozesse oder für unkritische Bereiche.

Das Risiko eines solchen Verfahrens liegt darin, dass der Schlüssel eventuell millionenfach verteilt ist. Man stelle sich vor, der Schlüssel würde publik, alle damit verschlüsselten Daten und / oder Dokumente könnten entschlüsselt, geändert und mit dem selben Schlüssel wieder verschlüsselt werden.

An dieser Stelle sei der Hinweis in eigener Sache erlaubt, dass die StepOver GmbH ein Verfahren zur Offline - Erstellung fortgeschrittener Signaturen ohne Zertifikat entwickelt hat. Gleichzeitig bitten wir um Nachsicht, dass wir in diesem Fall aus Gründen des Wettbewerbs auf eine detaillierte Beschreibung verzichten.

## 12 Checkliste

Diese kleine Checkliste stellt lediglich eine sehr grobe Zusammenfassung der wichtigsten relevanten Aspekte dar und soll als Anregung verstanden werden.

### 12.1 Zusammenstellung relevanter Aspekte

#### Beabsichtigter Zweck

- Nice to have Effekt ?
- Beweisfähiges Dokument gewünscht ?

#### Analyse des zu optimierenden Prozesses

- Willenserklärung ?
- Empfangsbescheinigung ?
- Dokumentation / Haftungsnachweis ?
- Rechnungserstellung ?
- Scannen ?

#### Ermittlung technischer Anforderungen

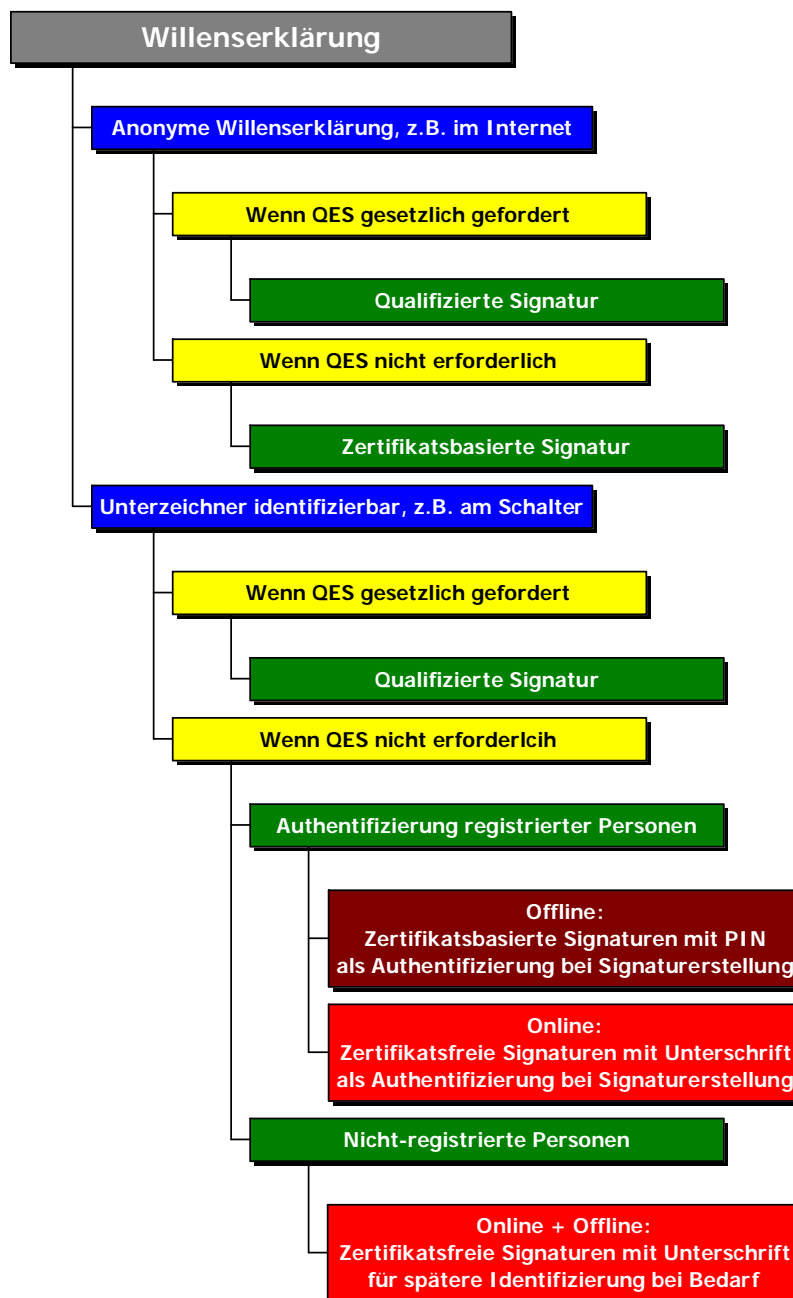
- Anonymes Signieren im Internet erforderlich ?
- Qualifizierte Signaturen mit Zeitangabe durch zusätzlichen Zeitstempel ?
- Offline / Online Signaturen bzw. Zeitstempel ?
- Besitzen die Unterzeichner eventuell erforderliche Signaturkarten ?
- Vorab-Identifizierung gewünscht oder sogar erforderlich ?
- Ist der Unterzeichner beim Signieren persönlich identifizierbar ?

#### Rechtliche Aspekte

- Per Gesetz oder per Verordnung explizit geforderte qualifizierte Signatur ?
- Per Gesetz geforderte Schriftform ?
- Per Gesetz geforderte Schriftform aber elektronische Form ausgeschlossen ?
- Keine gesetzliche Schriftformerfordernis ?

### 12.2 Beispiel für die Vorgehensweise bei der Analyse

Am Beispiel der Willenserklärung soll die Vorgehensweise bei der Analyse verdeutlicht werden. Natürlich können auch hier wieder nur Anregungen gegeben werden. So können z.B. Aspekte einer tieferen Ebene u.U. eine wesentlich größere Bedeutung haben, als dies im nachstehenden Beispiel dargestellt wird.



### 13 Politische Aspekte

#### 13.1 Warum hält man am PIN Verfahren fest

Von einer entsprechenden Interessensgruppe wird weiterhin - seit inzwischen zehn Jahren – die Ansicht verbreitet, dass die qualifizierte Signatur kurz vor dem Durchbruch stehe, obwohl diese in den allermeisten Fällen überhaupt nicht notwendig ist. Mit diesen suggestiven Aussagen wird zumindest in Deutschland der Blick von anderen bereits im Ausland erfolgreich eingesetzten und auch in Deutschland vollkommen legalen Signaturverfahren abgelenkt. Der TeleTrusT e.V. hat dies in seiner Stellungnahme von 2004 als vorauseilende Technikregulierung bezeichnet. Setzt sich die qualifizierte elektronische Signatur in einem Bereich nicht durch, wird diese einfach von entsprechenden Lobbyisten forciert in die verschiedensten Gesetze zugunsten des zertifikatsbasierten Verfahrens fest hineingeschrieben und verankert.

Die Interpretationsfreiheit, was eine elektronische Signatur sei und welche technischen Verfahren sicher seien, wird dem vom Innenministerium kontrollierten BSI – Bundesamt für Sicherheit in der Informationstechnik überlassen, das auch heute noch offiziell behauptet, dass die Verwendung einer PIN aus mathematischer Sicht das einzige sichere Authentifizierungsverfahren sei. Auf die Frage, welchen Stellenwert die Weitergabe einer PIN habe, erklärte das BSI allen Ernstes, dies spiele für die Sicherheitsbewertung des PIN Verfahrens keine Rolle. Eine seltsame Rolle spielt das sogenannte Signaturbündnis, in dem vor allem Banken und der Sparkassenverband den Ton angeben. Seit 2006 gibt es zwar das sogenannte Anwenderforum, an dem nun auch Anbieter von zertifikatsfreien Lösungen teilnehmen dürfen, praktisch geht es aber nur um zertifikatsbasierte Lösungen.

Den Schlüssel zum Verständnis bietet die gemäß § 371a der Zivilprozessordnung (ZPO) auf den Signaturkarteninhaber abgeschobene Haftung. Banken haben ein Interesse, weder die Haftung noch – trotz eigener Prozeßoptimierung - die Kosten für neue verbraucherfreundliche Verfahren zu übernehmen. Deshalb soll das PIN Verfahren, das eine Abschiebung der Haftung auf den einzelnen Signaturkarteninhaber ermöglicht, auch auf jeden Fall beibehalten werden. Ausnahmen bieten lediglich Sparkassen, Raiffeisenbanken und Versicherungen.

Hier treffen sich die Interessen der Großbanken und das übertriebene Sicherheitsbedürfnis der deutschen Sicherheitsbehörden. Beginnt die angloamerikanische Aktivität bei 60% Sicherheit und erreicht 80% durch praktische Erfahrung, so beginnt die deutsche Seele erst mit der Umsetzung, wenn theoretisch 80% erreichbar sind, nur – es fehlen dann 5 Jahre praktische Erfahrung. Innovationsfreiheit wird in Deutschland durch weltfremde Systemspezialisten der Behörden zugunsten einer starken Chipkarten-Lobby erfolgreich verhindert. Zusammenfassend läßt sich sagen, dass das Erfordernis eines Zertifikats für qualifizierte elektronische Signaturen eine übertriebene, überflüssige, einschränkende und wegen des PIN Verfahrens eine unsichere Anforderung zur Identitätsermittlung darstellt. Anstatt die Einführung elektronischer Signaturen zu

vereinfachen, wird dies durch die zusätzlichen Anforderungen des Bundesministeriums des Innern vielmehr behindert.

### 13.2 Kontroverse Positionen

Mit wenigen Fragen möchten wir kontroverse Aspekte bei Individualsignaturen aufzeigen:

#### **Nur die qualifizierte Signatur ersetzt eine unterschriebene Urkunde**

**Pro:** Nur die qualifizierte Signatur ersetzt die eigenhändige Unterschrift unter einer auf Papier abgegeben Willenserklärung.

**Kontra:** Dies ist unwichtig. Entscheidend ist im Zivilprozeß die Beweisbarkeit der Willenserklärung. Dies kann ggf. auch mit anderen Signaturverfahren nachgewiesen werden. Eine qualifizierte Signatur ist lediglich dann erforderlich, wenn dies explizit aufgrund eines Gesetzes oder die gesetzliche Schriftform aufgrund eines Gesetzes erforderlich ist

Für ca. 95% der wirtschaftlichen Vereinbarungen besteht Formfreiheit, eine qualifizierte Signatur wird für die wenigsten Geschäftsprozesse benötigt. Warum soll also der Unterzeichner eine Signaturkarte beantragen und bezahlen, wenn nicht er, sondern nur die Unternehmen zu seinem finanziellen Nachteil davon einen Vorteil haben?

#### **Nur die qualifizierte Signatur macht Sinn**

**Pro:** In manchen Fällen wird Schriftform benötigt. Dafür muß die qualifizierte elektronische Signatur verwendet werden. Warum soll man unterschiedliche Verfahren einsetzen, wenn man mit einer qualifizierten Signatur alle Anforderungen abdecken kann?

**Kontra:** Es gibt Bereiche, in denen eine zertifikatsbasierte Signatur sinnvoll ist. Dies betrifft vor allem das Internet mit anonymer Signierung. Allerdings haben nur recht wenige Personen eine Signaturkarte. Will man also in anderen Bereichen, z.B. am Schalterbetrieb oder im Außendienst auf elektronische Prozesse umstellen, müssen zur Erfassung sämtlicher Unterzeichner solche Verfahren eingesetzt werden, die auch eine Signierung ohne vorherige Registrierung ermöglichen.

#### **Sicherheit mit der qualifizierten Signatur**

**Pro:** Mit der qualifizierten Signatur ist der Unterzeichner identifizierbar. Das bringt Sicherheit für den Empfänger eines signierten Dokuments.

**Kontra:** Der Unterzeichner ist nur unter der Annahme identifizierbar, dass der Karteninhaber selbst signiert hat. Dies kann jedoch technisch nie bewiesen werden. Karte und PIN können weitergegeben werden. Dagegen bieten

# StepOver

## Leitfaden zur e-Signatur

Step Over  
the next step in business

Signaturverfahren mit eigenhändiger Unterschrift eine sehr hohe Identifikationsmöglichkeit des Unterzeichners.

## **I4 Links und Kontakte**

### **I4.1 GDPdU**

Zum Thema GDPdU verweisen wir auf den von Zöller & Partner GmbH verfaßten und beim VOI (<http://www.voi.de>) erschienenen und kostenfrei ladbaren GDPdU-Leitfaden.

### **I4.2 Unternehmen und Verbände**

#### **CCES - Competence Center Elektronische Signaturen**

Das CCES ist aus dem Arbeitskreis Elektronische Signaturen des VOI Verband Organisations- und Informationssysteme e.V. hervorgegangen. Das CCES ist derzeit das einzige Gremium, in dem sich DMS-Anbieter und Anbieter von Signaturverfahren im direkten Dialog befinden. Das CCES versteht sich als neutraler und kompetenter Informationsanbieter zu allen Bereichen der elektronischen Signaturen.

Kontakt: <http://www.voi.de>

#### **Deutsche Post Com GmbH, Geschäftsbereich Signtrust**

Die Deutsche Post Com GmbH als Nachfolger der Signtrust GmbH ist akkreditierter Zertifizierungsdiensteanbieter (ZDA). DP Com ist Herausgeber von ISIS/MTT-konformen Zertifikaten und vermarktet und vertreibt Lösungen rundum qualifizierter und anderer elektronischer Signaturen.

Kontakt: <http://www.signtrust.de>

#### **TeleTrusT Deutschland e.V.**

Der gemeinnützige Verein TeleTrusT setzt sich seit seiner Gründung 1989 für vertrauenswürdige Anwendungen des elektronischen Geschäftsverkehrs in Wirtschaft und Verwaltung ein. Er hat sich mit der interdisziplinären Zusammenarbeit der Fachleute seiner Mitgliedsunternehmen in Arbeitsgruppen und Projekten zum Kompetenzverbund für angewandte Kryptographie und Biometrie entwickelt. Wichtige Voraussetzungen für herstellerunabhängige Produkte und Services des elektronischen Geschäftsverkehrs bilden derzeit die TeleTrusT-Angebote "European Bridge-CA" und "ISIS-MTT".

Kontakt: <http://www.teletrust.de>

### **I4.3 SigLab – Signaturlabor**

#### **Signaturen zum Anfassen und Ausprobieren im Bonner SigLab**

Das SigLab ist ein in 2001 eröffnetes Schulungslabor, welches zur praktischen Erprobung von elektronischen Signaturen dient und zur Sensibilisierung der Anwender in diesem Themenfeld beitragen soll. Zahlreiche Firmen und Verbände aus der IT-Sicherheit unterstützten das SigLab mit Ihren Produkten, Informationen und Best-Practice-Beispielen. Ein ständiger Ausbau der Produktlandschaft und Berichte von Entwicklern

# StepOver Leitfaden zur e-Signatur

Step Over  
the next step in business

und Anwendern tragen zur Markttransparenz bei. Das SigLab ist herstellernerutral und vertreibt keines der angezeigten Produkte.

Zur Zeit finden sich über 30 Signaturprodukte aus unterschiedlichen Bereichen im SigLab. Darunter u.a. auch biometrische Anwendungen (Unterschriften, Fingerabdruck), Anwendungen auf Basis von Chipkarten sowie Software basierte Lösungen.

Im SigLab finden regelmäßig Workshops für Entscheider aus Wirtschaft und Verwaltung. Auf Anfrage sind auch Workshops vor Ort im Unternehmen möglich.

Kontakt: <http://www.siglab.de>

### 14.4 Die StepOver GmbH

Die StepOver GmbH mit Hauptsitz in Stuttgart und Niederlassungen in Frankfurt, Madrid und Minsk wurde 2001 gegründet und ist Europas führender Hersteller von Hardware und Software zur handgeschriebenen elektronischen Signatur. Versicherungen, Banken und Industrie können mit den Produkten der StepOver GmbH papierlos mit Dritten Geschäfte tätigen.

Ein wichtiger Ansatzpunkt zur Optimierung von Geschäftsprozessen ist die Beseitigung der auf Papier geleisteten Unterschrift und des damit verbundenen Medienbruchs.

Durch die Eliminierung des Medienbruchs wird ein durchgängiger elektronischer Ablauf möglich, der eine Beschleunigung aller Geschäftsprozesse sowie Kosteneinsparungen mit sich bringt.

#### **Alleinstellungsmerkmale der StepOver GmbH:**

- Sicherheitsrelevante Abstimmung von Hardware- und Software unter einem Dach.
- Hardware und Software „Made in Germany“ !
- Forschung an Zukunfts-Technologien in Zusammenarbeit mit der Otto-von-Guericke-Universität Magdeburg und dem Fraunhofer Institut.
- Die StepOver GmbH ist europäischer Marktführer für Hard- und Software zur handgeschriebenen elektronischen Signatur.
- Erfahrung mit bedeutenden Referenzkunden.
- Höchste Qualität und Funktionalität.

Kontakt: [www.StepOver.de](http://www.StepOver.de)

### 15 Autoren

#### **Rolf Schmoldt**

Schmoldt ist Komplementär und Geschäftsführer der Signature Perfect KG und beschäftigt sich seit 1999 mit den Themen elektronische Signatur und Authentifizierung mittels eigenhändiger Unterschriften.

Seit 2002 leitet Schmoldt das Competence Center Elektronische Signaturen des VOI e.V. und hat zur Korrektur des Signaturgesetzes 2005 beigetragen.

Schmoldt hat Anfang der 90er als UNIX Systemprogrammierer an der Entwicklung von elektronischen Archivierungssystemen für Großbanken mitgewirkt und sich anschließend beim Aufbau von internationalen Vertriebsstrukturen für Dokumenten Management, Workflow und Systeme zur Zeichenerkennung einen Namen gemacht.

### 16 Kurz-Glossar und verwendete Abkürzungen

AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BMI	Bundesministerium des Innern
BMWA	bis 2005: Bundesministerium für Wirtschaft und Arbeit
BMWI	ab 2006: Bundesministerium für Wirtschaft und Technologie
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authorization (Trust Center, siehe ZDA)
CCES	Competence Center Elektronische Signaturen (des VOI e.V.)
DMS	Dokument Management System(e)
EGSRL	EG-Signaturrechtlinie
GOBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
Hash(-wert)	Prüfsumme definierter Länge, von der nicht auf den Inhalt geschlossen werden kann
PKI	Public Key Infrastructure
Private Key	Geheimer Schlüssel eines asymmetrischen Schlüsselpaares
Public Key	Öffentlich bekannter Schlüssel eines asymmetrischen Schlüsselpaares
QES	Qualifizierte elektronische Signatur
Reg TP	Regulierungsbehörde für Telekommunikation und Post jetzt Bundesnetzagentur
SGB I	Sozialgesetzbuch - Erstes Buch (I) Allgemeiner Teil
SGB 4	Sozialgesetzbuch - Viertes Buch (IV) Gemeinsame Vorschriften für die Sozialversicherung
SigG	Signaturgesetz
SigV	Verordnung zum Signaturgesetz
SRVwV	Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung
USTG	Umsatzsteuergesetz
VOI	Verband Organisations- und Informationssysteme e.V.
VVG	Versicherungsvertragsgesetz
VwVfG	Verwaltungsverfahrensgesetz

# StepOver

## Leitfaden zur e-Signatur

Step Over  
the next step in business

ZDA           Zertifizierungsdienst-Anbieter, Trust Center  
ZPO           Zivilprozessordnung

### 17 Deutsche Gesetze, Verordnungen und Vorschriften

Dieses Kapitel soll einen Überblick über die derzeit wichtigsten deutschen Gesetze, Verordnungen und Vorschriften ermöglichen, die im Zusammenhang mit elektronischen Signaturen stehen. Wir haben uns erlaubt, nur die relevanten Auszüge aus den Gesetzestexten wiederzugeben.

Auch aufgrund der sich immer wieder ändernden Gesetzeslage können wir natürlich keine Haftung oder Gewährleistung auf Vollständigkeit oder korrekter Wiedergabe der Texte übernehmen.

Alle Texte wurden dem Service der Juris GmbH entnommen, der über die Web-Seiten des Bundesjustizministeriums öffentlich zugänglich ist. Stand der Gesetzestexte ist der 3. Dezember 2003, soweit die Gesetzestexte nicht mit einem Datum versehen sind.

Sie können den jeweils aktuellen Link zu den Gesetzen über folgende Web-Site erreichen.

[http://bundesrecht.juris.de/bundesrecht/GESAMT\\_index.html](http://bundesrecht.juris.de/bundesrecht/GESAMT_index.html)

### AO § 87a Elektronische Kommunikation

(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet. Ein elektronisches Dokument ist zugegangen, sobald die für den Empfang bestimmte Einrichtung es in für den Empfänger bearbeitbarer Weise aufgezeichnet hat. Übermittelt die Finanzbehörde Daten, die dem Steuergeheimnis unterliegen, sind diese Daten mit einem geeigneten Verfahren zu verschlüsseln.

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

(3) Eine durch Gesetz für Anträge, Erklärungen oder Mitteilungen an die Finanzbehörden angeordnete Schriftform kann, soweit nicht durch Gesetz etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Die Signierung mit einem Pseudonym ist nicht zulässig.

(4) Eine durch Gesetz für Verwaltungsakte oder sonstige Maßnahmen der Finanzbehörden angeordnete Schriftform kann, soweit nicht durch Gesetz etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Für von der

Finanzbehörde aufzunehmende Niederschriften gilt Satz 1 nur, wenn dies durch Gesetz ausdrücklich zugelassen ist.

(5) Ist ein elektronisches Dokument Gegenstand eines Beweises, wird der Beweis durch Vorlegung oder Übermittlung der Datei angetreten; befindet diese sich nicht im Besitz des Steuerpflichtigen oder der Finanzbehörde, gilt § 97 Abs. 1 und 3 entsprechend. Der Anschein der Echtheit eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz übermittelten Dokuments, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass das Dokument mit dem Willen des Signaturschlüssel-Inhabers übermittelt worden ist.

(6) Bis zum 31. Dezember 2005 kann abweichend von Absatz 3 Satz 2 die qualifizierte elektronische Signatur mit Einschränkungen nach Maßgabe einer Rechtsverordnung nach § 150 Abs. 6 eingesetzt werden. In der Rechtsverordnung kann auch bestimmt werden, dass bis zum 31. Dezember 2005 bei elektronisch übermittelten Verwaltungsakten abweichend von Absatz 4 Satz 2 die qualifizierte elektronische Signatur mit in der Rechtsverordnung zu regelnden Einschränkungen eingesetzt werden kann.

### **BDSG § 4a Einwilligung**

(Stand Oktober 2006)

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. **Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.** Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

### **BGB § 125 Nichtigkeit wegen Formmangels**

(Stand Mai 2005)

Ein Rechtsgeschäft, welches der durch Gesetz vorgeschriebenen Form ermangelt, ist nichtig. Der Mangel der durch Rechtsgeschäft bestimmten Form hat im Zweifel gleichfalls Nichtigkeit zur Folge.

### **BGB § 126 Schriftform**

(Stand Mai 2005)

(1) Ist durch Gesetz schriftliche Form vorgeschrieben, so muß die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden.

(2) Bei einem Vertrag muß die Unterzeichnung der Parteien auf derselben Urkunde erfolgen. Werden über den Vertrag mehrere gleichlautende Urkunden aufgenommen, so genügt es, wenn jede Partei die für die andere Partei bestimmte Urkunde unterzeichnet.

(3) Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt.

(4) Die schriftliche Form wird durch die notarielle Beurkundung ersetzt.

### **BGB § 126a Elektronische Form**

(Stand Mai 2005)

(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.

### **BGB § 126b Textform**

(Stand Mai 2005)

Ist durch Gesetz Textform vorgeschrieben, so muß die Erklärung in einer Urkunde oder auf andere zur dauerhaften Wiedergabe in Schriftzeichen geeignete Weise abgegeben, die Person des Erklärenden genannt und der Abschluss der Erklärung durch Nachbildung der Namensunterschrift oder anders erkennbar gemacht werden.

### **BGB § 127 Vereinbarte Form**

(Stand Mai 2005)

(1) Die Vorschriften des § 126, des § 126a oder des § 126b gelten im Zweifel auch für die durch Rechtsgeschäft bestimmte Form.

(2) Zur Wahrung der durch Rechtsgeschäft bestimmten schriftlichen Form genügt, soweit nicht ein anderer Wille anzunehmen ist, die telekommunikative Übermittlung und bei einem Vertrag der Briefwechsel. Wird eine solche Form gewählt, so kann nachträglich eine dem § 126 entsprechende Beurkundung verlangt werden.

(3) Zur Wahrung der durch Rechtsgeschäft bestimmten elektronischen Form genügt, soweit nicht ein anderer Wille anzunehmen ist, auch eine andere als die in § 126a bestimmte elektronische Signatur und bei einem Vertrag der Austausch von Angebots- und Annahmeerklärung, die jeweils mit einer elektronischen Signatur versehen sind. Wird eine solche Form gewählt, so kann nachträglich eine dem § 126a entsprechende elektronische Signierung oder, wenn diese einer der Parteien nicht möglich ist, eine dem § 126 entsprechende Beurkundung verlangt werden.

### BGB § 355 Widerrufsrecht bei Verbraucherverträgen

(1) Wird einem Verbraucher durch Gesetz ein Widerrufsrecht nach dieser Vorschrift eingeräumt, so ist er an seine auf den Abschluss des Vertrags gerichtete Willenserklärung nicht mehr gebunden, wenn er sie fristgerecht widerrufen hat. Der Widerruf muß keine Begründung enthalten und ist in Textform oder durch Rücksendung der Sache innerhalb von zwei Wochen gegenüber dem Unternehmer zu erklären; zur Fristwahrung genügt die rechtzeitige Absendung.

(2) Die Frist beginnt mit dem Zeitpunkt, zu dem dem Verbraucher eine deutlich gestaltete Belehrung über sein Widerrufsrecht, die ihm entsprechend den Erfordernissen des eingesetzten Kommunikationsmittels seine Rechte deutlich macht, in Textform mitgeteilt worden ist, die auch Namen und Anschrift desjenigen, gegenüber dem der Widerruf zu erklären ist, und einen Hinweis auf den Fristbeginn und die Regelung des Absatzes 1 Satz 2 enthält. Wird die Belehrung nach Vertragsschluss mitgeteilt, beträgt die Frist abweichend von Absatz 1 Satz 2 einen Monat. Ist der Vertrag schriftlich abzuschließen, so beginnt die Frist nicht zu laufen, bevor dem Verbraucher auch eine Vertragsurkunde, der schriftliche Antrag des Verbrauchers oder eine Abschrift der Vertragsurkunde oder des Antrags zur Verfügung gestellt werden. Ist der Fristbeginn streitig, so trifft die Beweislast den Unternehmer.

(3) Das Widerrufsrecht erlischt spätestens sechs Monate nach Vertragsschluss. Bei der Lieferung von Waren beginnt die Frist nicht vor dem Tag ihres Eingangs beim Empfänger. Abweichend von Satz 1 erlischt das Widerrufsrecht nicht, wenn der Verbraucher nicht ordnungsgemäß über sein Widerrufsrecht belehrt worden ist.

### BGB § 484 Schriftform bei Teilzeit-Wohnrechteverträgen

(1) Der Teilzeit-Wohnrechtevertrag bedarf der schriftlichen Form, soweit nicht in anderen Vorschriften eine strengere Form vorgeschrieben ist. Der Abschluss des Vertrags in elektronischer Form ist ausgeschlossen. Die in dem in § 482 bezeichneten, dem Verbraucher ausgehändigten Prospekt enthaltenen Angaben werden Inhalt des Vertrags, soweit die Parteien nicht ausdrücklich und unter Hinweis auf die Abweichung vom Prospekt eine abweichende Vereinbarung treffen. Solche Änderungen müssen dem Verbraucher vor Abschluss des Vertrags mitgeteilt werden. Unbeschadet der Geltung der Prospektangaben nach Satz 3 muß die Vertragsurkunde die in der in § 482 Abs. 2 bezeichneten Rechtsverordnung bestimmten Angaben enthalten.

(2) Der Unternehmer hat dem Verbraucher eine Vertragsurkunde oder Abschrift der Vertragsurkunde auszuhändigen. Er hat ihm ferner, wenn die Vertragssprache und die Sprache des Staates, in dem das Wohngebäude belegen ist, verschieden sind, eine beglaubigte Übersetzung des Vertrags in der oder einer zu den Amtssprachen der Europäischen Union oder des Übereinkommens über den Europäischen Wirtschaftsraum zählenden Sprache des Staates auszuhändigen, in dem das Wohngebäude belegen ist. Die Pflicht zur Aushändigung einer beglaubigten Übersetzung entfällt, wenn sich das Nutzungsrecht auf einen Bestand von Wohngebäuden bezieht, die in verschiedenen Staaten belegen sind.

### BGB § 492 Schriftform, Vertragsinhalt

(1) Verbraucherdarlehensverträge sind, soweit nicht eine strengere Form vorgeschrieben ist, schriftlich abzuschließen. Der Abschluss des Vertrags in elektronischer Form ist ausgeschlossen. Der Schriftform ist genügt, wenn Antrag und Annahme durch die Vertragsparteien jeweils getrennt schriftlich erklärt werden. Die Erklärung des Darlehensgebers bedarf keiner Unterzeichnung, wenn sie mit Hilfe einer automatischen Einrichtung erstellt wird. Die vom Darlehensnehmer zu unterzeichnende Vertragserklärung muß angeben:

1. den Nettodarlehensbetrag, gegebenenfalls die Höchstgrenze des Darlehens,
2. den Gesamtbetrag aller vom Darlehensnehmer zur Tilgung des Darlehens sowie zur Zahlung der Zinsen und sonstigen Kosten zu entrichtenden Teilzahlungen, wenn der Gesamtbetrag bei Abschluss des Verbraucherdarlehensvertrags für die gesamte Laufzeit der Höhe nach feststeht, bei Darlehen mit veränderlichen Bedingungen, die in Teilzahlungen getilgt werden, einen Gesamtbetrag auf der Grundlage der bei Abschluss des Vertrags maßgeblichen Darlehensbedingungen,
3. die Art und Weise der Rückzahlung des Darlehens oder, wenn eine Vereinbarung hierüber nicht vorgesehen ist, die Regelung der Vertragsbeendigung,
4. den Zinssatz und alle sonstigen Kosten des Darlehens, die, soweit ihre Höhe bekannt ist, im Einzelnen zu bezeichnen, im Übrigen dem Grunde nach anzugeben sind, einschließlich etwaiger vom Darlehensnehmer zu tragender Vermittlungskosten,
5. den effektiven Jahreszins oder, wenn eine Änderung des Zinssatzes oder anderer preisbestimmender Faktoren vorbehalten ist, den anfänglichen effektiven Jahreszins; zusammen mit dem anfänglichen effektiven Jahreszins ist auch anzugeben, unter welchen Voraussetzungen preisbestimmende Faktoren geändert werden können und auf welchen Zeitraum Belastungen, die sich aus einer nicht vollständigen Auszahlung oder aus einem Zuschlag zu dem Darlehen ergeben, bei der Berechnung des effektiven Jahreszinses verrechnet werden,
6. die Kosten einer Restschuld- oder sonstigen Versicherung, die im Zusammenhang mit dem Verbraucherdarlehensvertrag abgeschlossen wird,
7. zu bestellende Sicherheiten.

(1a) Abweichend von Absatz 1 Satz 5 Nr. 2 ist kein Gesamtbetrag anzugeben bei Darlehen, bei denen die Inanspruchnahme bis zu einer Höchstgrenze freigestellt ist, sowie bei Immobiliendarlehensverträgen. Immobiliendarlehensverträge sind Verbraucherdarlehensverträge, bei denen die Zurverfügungstellung des Darlehens von der Sicherung durch ein Grundpfandrecht abhängig gemacht wird und zu Bedingungen erfolgt, die für grundpfandrechtl. abgesicherte Darlehensverträge und deren Zwischenfinanzierung üblich sind; der Sicherung durch ein Grundpfandrecht steht es gleich, wenn von einer Sicherung gemäß § 7 Abs. 3 bis 5 des Gesetzes über Bausparkassen abgesehen wird.

(2) Effektiver Jahreszins ist die in einem Prozentsatz des Nettodarlehensbetrags anzugebende Gesamtbelastung pro Jahr. Die Berechnung des effektiven und des anfänglichen effektiven Jahreszinses richtet sich nach § 6 der Verordnung zur Regelung der Preisangaben.

(3) Der Darlehensgeber hat dem Darlehensnehmer eine Abschrift der Vertragserklärungen zur Verfügung zu stellen.

(4) Die Absätze 1 und 2 gelten auch für die Vollmacht, die ein Darlehensnehmer zum Abschluss eines Verbraucherdarlehensvertrags erteilt. Satz 1 gilt nicht für die Prozessvollmacht und eine Vollmacht, die notariell beurkundet ist.

### **SGB I § 36a 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 elektronischen Signatur nach dem Signaturgesetz zu versehen. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, ist nicht zulässig.

(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, übermittelt sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück.

(4) Die Träger der Sozialversicherung einschließlich der Bundesanstalt für Arbeit, ihre Verbände und Arbeitsgemeinschaften verwenden unter Beachtung der Grundsätze der Wirtschaftlichkeit und Sparsamkeit im jeweiligen Sozialleistungsbereich Zertifizierungsdienste nach dem Signaturgesetz, die eine gemeinsame und bundeseinheitliche Kommunikation und Übermittlung der Daten und die Überprüfbarkeit der qualifizierten elektronischen Signatur auf Dauer sicherstellen. Diese Träger sollen über ihren jeweiligen Bereich hinaus Zertifizierungsdienste im Sinne des Satzes 1 verwenden. Die Sätze 1 und 2 gelten entsprechend für die Leistungserbringer nach dem Fünften und dem Elften Buch und die von ihnen gebildeten Organisationen.

### **SGB 4 § 110d Beweiswirkung**

Ist eine Unterlage nach § 110a Abs. 2 auf anderen dauerhaften maschinell verwertbaren Datenträgern als Bildträgern aufbewahrt und

1. die Wiedergabe mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz dessen versehen, der die Wiedergabe auf dem dauerhaften Datenträger hergestellt hat, oder
2. bei urschriftlicher Aufzeichnung des Textes nur in gespeicherter Form diese mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz dessen versehen ist, der den Text elektronisch signiert hat,

# StepOver

## Leitfaden zur e-Signatur

Step Over  
the next step in business

und ist die qualifizierte elektronische Signatur dauerhaft überprüfbar, können der öffentlich-rechtlichen Verwaltungstätigkeit die Daten auf diesem dauerhaften Datenträger zugrunde gelegt werden, soweit nach den Umständen des Einzelfalles kein Anlass ist, ihre sachliche Richtigkeit zu beanstanden.

### **SigG § 1 Zweck und Anwendungsbereich**

(Stand Mai 2005)

- (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.

### **SigG § 2 Begriffsbestimmungen**

(Stand Mai 2005)

Im Sinne dieses Gesetzes sind

1. "elektronische Signaturen" Daten in elektronischer Form, die anderen elektronischen Daten beifügt 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. "Signaturprüf Schlüssel" elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden,
6. "Zertifikate" elektronische Bescheinigungen, mit denen Signaturprüf Schlüssel 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. "Signatur Schlüssel-Inhaber" natürliche Personen, die Signaturschlüssel besitzen; bei qualifizierten elektronischen Signaturen müssen ihnen die zugehörigen Signaturprüfchlüssel durch qualifizierte Zertifikate zugeordnet sein,
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.

### **SigV § 15 Anforderungen an Produkte für qualifizierte elektronische Signaturen**

(Stand Mai 2005)

(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 I 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.

### SRVwV § 36- Allgemeine Verwaltungsvorschrift über das Rechnungswesen

vom 15. Juli 1999 (BAnz. Nr. 145 a vom 06.08.1999)

#### Vierter Abschnitt: Buchführung

#### § 36 Aufbewahrung

(1) Schriftliche Unterlagen dürfen vor Ablauf der betreffenden Aufbewahrungsfrist vernichtet werden, wenn

1. sie auf einen maschinell verwertbaren Datenträger so übertragen sind, dass sie in bildlicher Form wiedergegeben werden können,
2. die bildliche Wiedergabe mit den zu vernichtenden Unterlagen übereinstimmt und sie die darin enthaltenen Daten erkennbar macht,
3. durch digitale Signatur dessen, der die bildliche Wiedergabe erzeugt hat, die Übereinstimmung der bildlichen Wiedergabe mit der Unterlage bestätigt und dadurch die unbemerkte Veränderung der Unterlage ausgeschlossen ist,
4. die Daten während der Dauer der Aufbewahrungsfrist verfügbar sind,
5. die bildliche Darstellung jederzeit innerhalb angemessener Frist wieder hergestellt werden kann und
6. für die Aufzeichnung, die Aufbewahrung der Datenträger und die bildliche Wiedergabe ein bestimmtes Verfahren vorgegeben ist und dieses Verfahren der Dienstanweisung nach § 40 entspricht.

(2) Für die Aufbewahrung von Unterlagen, die auf einem maschinell verwertbaren Datenträger erstellt wurden, gilt Absatz 1 entsprechend mit der Maßgabe, dass die bildliche Übereinstimmung nicht sichergestellt sein muß. Es muß jedoch sichergestellt sein, dass die schriftlichen Unterlagen jederzeit in ihrer ursprünglichen Fassung inhaltlich unverändert erzeugt werden können.

(3) Eine Vernichtung von Unterlagen nach Absatz 1 sowie der Verzicht auf die Ausfertigung einer schriftlichen Unterlage nach Absatz 2 sind unzulässig, wenn die Unterlagen für andere als Buchführungszwecke in Papierform aufzubewahren sind.

### UStG § 14 Ausstellung von Rechnungen

(Stand Mai 2005)

(1) Rechnung ist jedes Dokument, mit dem über eine Lieferung oder sonstige Leistung abgerechnet wird, gleichgültig, wie dieses Dokument im Geschäftsverkehr bezeichnet wird. Rechnungen sind auf Papier oder vorbehaltlich der Zustimmung des Empfängers auf elektronischem Weg zu übermitteln.

(2) Führt der Unternehmer eine Lieferung oder eine sonstige Leistung nach § 1 Abs. 1 Nr. 1 aus, gilt Folgendes:

1. führt der Unternehmer eine steuerpflichtige Werklieferung (§ 3 Abs. 4 Satz 1) oder sonstige Leistung im Zusammenhang mit einem Grundstück aus, ist er verpflichtet, innerhalb von sechs Monaten nach Ausführung der Leistung eine Rechnung auszustellen;
2. führt der Unternehmer eine andere als die in Nummer 1 genannte Leistung aus, ist er berechtigt, eine Rechnung auszustellen. Soweit er einen Umsatz an einen anderen Unternehmer für dessen Unternehmen oder an eine juristische Person ausführt, ist er verpflichtet, innerhalb von sechs Monaten nach Ausführung der Leistung eine Rechnung auszustellen.

Unbeschadet der Verpflichtungen nach Satz 1 Nr. 1 und 2 Satz 2 kann eine Rechnung von einem in Satz 1 Nr. 2 bezeichneten Leistungsempfänger für eine Lieferung oder sonstige Leistung des Unternehmers ausgestellt werden, sofern dies vorher vereinbart wurde (Gutschrift). Die Gutschrift verliert die Wirkung einer Rechnung, sobald der Empfänger der Gutschrift dem ihm übermittelten Dokument widerspricht. Eine Rechnung kann im Namen und für Rechnung des Unternehmers oder eines in Satz 1 Nr. 2 bezeichneten Leistungsempfängers von einem Dritten ausgestellt werden.

(3) Bei einer auf elektronischem Weg übermittelten Rechnung müssen die Echtheit der Herkunft und die Unversehrtheit des Inhalts gewährleistet sein durch

1. eine qualifizierte elektronische Signatur oder eine qualifizierte elektronische Signatur mit Anbieter-Akkreditierung nach dem Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), das durch Artikel 2 des Gesetzes vom 16. Mai 2001 (BGBl. I S. 876) geändert worden ist, in der jeweils geltenden Fassung, oder
2. elektronischen Datenaustausch (EDI) nach Artikel 2 der Empfehlung 94/820/EG der Kommission vom 19. Oktober 1994 über die rechtlichen Aspekte des elektronischen Datenaustausches (ABl. EG Nr. L 338 S. 98), wenn in der Vereinbarung über diesen Datenaustausch der Einsatz von Verfahren vorgesehen ist, die die Echtheit der Herkunft und die Unversehrtheit der Daten gewährleisten, und zusätzlich eine zusammenfassende Rechnung auf Papier oder unter den Voraussetzungen der Nummer 1 auf elektronischem Weg übermittelt wird.

(4) Eine Rechnung muß folgende Angaben enthalten:

1. den vollständigen Namen und die vollständige Anschrift des leistenden Unternehmers und des Leistungsempfängers,

2. die dem leistenden Unternehmer vom Finanzamt erteilte Steuernummer oder die ihm vom Bundesamt für Finanzen erteilte Umsatzsteuer-Identifikationsnummer,
3. das Ausstellungsdatum,
4. eine fortlaufende Nummer mit einer oder mehreren Zahlenreihen, die zur Identifizierung der Rechnung vom Rechnungsaussteller einmalig vergeben wird (Rechnungsnummer),
5. die Menge und die Art (handelsübliche Bezeichnung) der gelieferten Gegenstände oder den Umfang und die Art der sonstigen Leistung,
6. den Zeitpunkt der Lieferung oder sonstigen Leistung oder der Vereinnahmung des Entgelts oder eines Teils des Entgelts in den Fällen des Absatzes 5 Satz 1, sofern dieser Zeitpunkt feststeht und nicht mit dem Ausstellungsdatum der Rechnung identisch ist,
7. das nach Steuersätzen und einzelnen Steuerbefreiungen aufgeschlüsselte Entgelt für die Lieferung oder sonstige Leistung (§ 10) sowie jede im Voraus vereinbarte Minderung des Entgelts, sofern sie nicht bereits im Entgelt berücksichtigt ist,
8. den anzuwendenden Steuersatz sowie den auf das Entgelt entfallenden Steuerbetrag oder im Fall einer Steuerbefreiung einen Hinweis darauf, dass für die Lieferung oder sonstige Leistung eine Steuerbefreiung gilt und
9. in den Fällen des § 14b Abs. 1 Satz 5 einen Hinweis auf die Aufbewahrungspflicht des Leistungsempfängers.

In den Fällen des § 10 Abs. 5 sind die Nummern 7 und 8 mit der Maßgabe anzuwenden, dass die Bemessungsgrundlage für die Leistung (§ 10 Abs. 4) und der darauf entfallende Steuerbetrag anzugeben sind. Unternehmer, die § 24 Abs. 1 bis 3 anwenden, sind jedoch auch in diesen Fällen nur zur Angabe des Entgelts und des darauf entfallenden Steuerbetrags berechtigt.

(5) Vereinnahmt der Unternehmer das Entgelt oder einen Teil des Entgelts für eine noch nicht ausgeführte Lieferung oder sonstige Leistung, gelten die Absätze 1 bis 4 sinngemäß. Wird eine Endrechnung erteilt, sind in ihr die vor Ausführung der Lieferung oder sonstigen Leistung vereinnahmten Teilentgelte und die auf sie entfallenden Steuerbeträge abzusetzen, wenn über die Teilentgelte Rechnungen im Sinne der Absätze 1 bis 4 ausgestellt worden sind.

(6) Das Bundesministerium der Finanzen kann mit Zustimmung des Bundesrates zur Vereinfachung des Besteuerungsverfahrens durch Rechtsverordnung bestimmen, in welchen Fällen und unter welchen Voraussetzungen

1. Dokumente als Rechnungen anerkannt werden können,
2. die nach Absatz 4 erforderlichen Angaben in mehreren Dokumenten enthalten sein können,
3. Rechnungen bestimmte Angaben nach Absatz 4 nicht enthalten müssen,
4. eine Verpflichtung des Unternehmers zur Ausstellung von Rechnungen mit gesondertem Steuerausweis (Absatz 4) entfällt oder
5. Rechnungen berichtigt werden können.

### VVG § 3

(1) Der Versicherer ist verpflichtet, eine von ihm unterzeichnete Urkunde über den Versicherungsvertrag (Versicherungsschein) dem Versicherungsnehmer auszuhändigen. Eine Nachbildung der eigenhändigen Unterschrift genügt.

(2) Ist ein Versicherungsschein abhanden gekommen oder vernichtet, so kann der Versicherungsnehmer von dem Versicherer die Ausstellung einer Ersatzurkunde verlangen. Unterliegt der Versicherungsschein der Kraftloserklärung, so ist der Versicherer erst nach der Kraftloserklärung zur Ausstellung verpflichtet.

(3) Der Versicherungsnehmer kann jederzeit Abschriften der Erklärungen fordern, die er mit Bezug auf den Vertrag abgegeben hat. Der Versicherer hat ihn bei der Aushändigung des Versicherungsscheins auf dieses Recht aufmerksam zu machen. Bedarf der Versicherungsnehmer der Abschriften für die Vornahme von Handlungen gegenüber dem Versicherer, die an eine bestimmte Frist gebunden sind, und sind sie ihm nicht schon früher vom Versicherer ausgehändigt worden, so ist der Lauf der Frist von der Stellung des Verlangens bis zum Eingang der Abschriften gehemmt.

(4) Die Kosten der Ersatzurkunde sowie der Abschriften hat der Versicherungsnehmer zu tragen und auf Verlangen vorzuschießen.

(5) Wird der Vertrag nicht durch eine Niederlassung des Versicherers im Geltungsbereich dieses Gesetzes abgeschlossen, so ist im Versicherungsschein die Anschrift des Versicherers und der Niederlassung, über die der Vertrag abgeschlossen worden ist, anzugeben.

### VVG § 5a

(1) Hat der Versicherer dem Versicherungsnehmer bei Antragstellung die Versicherungsbedingungen nicht übergeben oder eine Verbraucherinformation nach § 10a des Versicherungsaufsichtsgesetzes unterlassen, so gilt der Vertrag auf der Grundlage des Versicherungsscheins, der Versicherungsbedingungen und der weiteren für den Vertragsinhalt maßgeblichen Verbraucherinformation als abgeschlossen, wenn der Versicherungsnehmer nicht innerhalb von vierzehn Tagen nach Überlassung der Unterlagen in Textform widerspricht. Satz 1 ist nicht auf Versicherungsverträge bei Pensionskassen anzuwenden, die auf arbeitsvertraglichen Regelungen beruhen. § 5 bleibt unberührt.

(2) Der Lauf der Frist beginnt erst, wenn dem Versicherungsnehmer der Versicherungsschein und die Unterlagen nach Absatz 1 vollständig vorliegen und der Versicherungsnehmer bei Aushändigung des Versicherungsscheins schriftlich, in drucktechnisch deutlicher Form über das Widerspruchsrecht, den Fristbeginn und die Dauer belehrt worden ist. Der Nachweis über den Zugang der Unterlagen obliegt dem Versicherer. Zur Wahrung der Frist genügt die rechtzeitige Absendung des Widerspruchs. Abweichend von Satz 1 erlischt das Recht zum Widerspruch jedoch ein Jahr nach Zahlung der ersten Prämie.

(3) Gewährt der Versicherer auf besonderen Antrag des Versicherungsnehmers sofortigen Versicherungsschutz, so kann der Verzicht auf Überlassung der Versicherungsbedingungen und der Verbraucherinformation bei Vertragsschluß vereinbart werden. Die Unterlagen sind dem Versicherungsnehmer auf Anforderung, spätestens mit dem Versicherungsschein zu überlassen. Wenn der Versicherungsvertrag sofortigen Versicherungsschutz gewährt, hat der Versicherungsnehmer insoweit kein Widerspruchsrecht nach Absatz 1.

### VVG § 8

(1) Eine Vereinbarung, nach welcher ein Versicherungsverhältnis als stillschweigend verlängert gilt, wenn es nicht vor dem Ablauf der Vertragszeit gekündigt wird, ist insoweit nichtig, als sich die jedesmalige Verlängerung auf mehr als ein Jahr erstrecken soll.

(2) Ist ein Versicherungsverhältnis auf unbestimmte Zeit eingegangen (dauernde Versicherung), so kann es von beiden Teilen nur für den Schluß der laufenden Versicherungsperiode gekündigt werden. Die Kündigungsfrist muß für beide Teile gleich sein und darf nicht weniger als einen Monat, nicht mehr als drei Monate betragen. Auf das Kündigungsrecht können die Parteien in gegenseitigem Einverständnis bis zur Dauer von zwei Jahren verzichten.

(3) Ein Versicherungsverhältnis, das für eine Dauer von mehr als fünf Jahren eingegangen worden ist, kann zum Ende des fünften oder jedes darauf folgenden Jahres unter Einhaltung einer Frist von drei Monaten gekündigt werden. Satz 1 gilt nicht für die Lebens- und Krankenversicherung.

(4) Wird mit Ausnahme der Lebensversicherung ein Versicherungsverhältnis mit einer längeren Laufzeit als einem Jahr abgeschlossen, so kann der Versicherungsnehmer innerhalb einer Frist von vierzehn Tagen ab Unterzeichnung des Versicherungsantrages seine auf den Vertragsabschluß gerichtete Willenserklärung schriftlich widerrufen. Zur Wahrung der Frist genügt die rechtzeitige Absendung des Widerrufs. Die Frist beginnt erst zu laufen, wenn der Versicherer den Versicherungsnehmer über sein Widerrufsrecht belehrt und der Versicherungsnehmer die Belehrung durch Unterschrift bestätigt hat. Unterbleibt die Belehrung, so erlischt das Widerrufsrecht einen Monat nach Zahlung der ersten Prämie. Das Widerrufsrecht besteht nicht, wenn und soweit der Versicherer auf Wunsch des Versicherungsnehmers sofortigen Versicherungsschutz gewährt oder wenn die Versicherung nach dem Inhalt des Antrags für die bereits ausgeübte gewerbliche oder selbständige berufliche Tätigkeit des Versicherungsnehmers bestimmt ist.

(5) Bei der Lebensversicherung kann der Versicherungsnehmer innerhalb einer Frist von vierzehn Tagen nach Abschluß des Vertrages vom Vertrag zurücktreten. Zur Wahrung der Frist genügt die rechtzeitige Absendung der Rücktrittserklärung. Die Frist beginnt erst zu laufen, wenn der Versicherer den Versicherungsnehmer über sein Rücktrittsrecht belehrt und der Versicherungsnehmer die Belehrung durch Unterschrift bestätigt hat. Unterbleibt die Belehrung, so erlischt das Rücktrittsrecht einen Monat nach Zahlung der ersten Prämie. Die Sätze 1 bis 4 finden keine Anwendung auf Versicherungsverhältnisse bei Pensionskassen, die auf arbeitsvertraglichen Regelungen beruhen.

(6) Die Absätze 4 und 5 finden keine Anwendung, soweit der Versicherungsnehmer ein Widerspruchsrecht nach § 5a hat.

### VVG § 16

(1) Der Versicherungsnehmer hat bei der Schließung des Vertrags alle ihm bekannten Umstände, die für die Übernahme der Gefahr erheblich sind, dem Versicherer anzuzeigen. Erheblich sind die

Gefahrumsstände, die geeignet sind, auf den Entschluß des Versicherers, den Vertrag überhaupt oder zu dem vereinbarten Inhalt abzuschließen, einen Einfluß auszuüben. Ein Umstand, nach welchem der Versicherer ausdrücklich und schriftlich gefragt hat, gilt im Zweifel als erheblich.

(2) Ist dieser Vorschrift zuwider die Anzeige eines erheblichen Umstandes unterblieben, so kann der Versicherer von dem Vertrag zurücktreten. Das gleiche gilt, wenn die Anzeige eines erheblichen Umstandes deshalb unterblieben ist, weil sich der Versicherungsnehmer der Kenntnis des Umstandes arglistig entzogen hat.

(3) Der Rücktritt ist ausgeschlossen, wenn der Versicherer den nicht angezeigten Umstand kannte oder wenn die Anzeige ohne Verschulden des Versicherungsnehmers unterblieben ist.

### VwVfG § 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 elektronischen Signatur nach dem Signaturgesetz zu versehen. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, ist nicht zulässig.

(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.

### VwVfG § 33 Beglaubigung von Dokumenten

(1) Jede Behörde ist befugt, Abschriften von Urkunden, die sie selbst ausgestellt hat, zu beglaubigen. Darüber hinaus sind die von der Bundesregierung durch Rechtsverordnung bestimmten Behörden im Sinne des § 1 Abs. 1 Nr. 1 und die nach Landesrecht zuständigen Behörden befugt, Abschriften zu beglaubigen, wenn die Urschrift von einer Behörde ausgestellt ist oder die Abschrift zur Vorlage bei einer Behörde benötigt wird, sofern nicht durch Rechtsvorschrift die Erteilung beglaubigter Abschriften aus amtlichen Registern und Archiven anderen Behörden ausschließlich vorbehalten ist; die Rechtsverordnung bedarf nicht der Zustimmung des Bundesrates.

(2) Abschriften dürfen nicht beglaubigt werden, wenn Umstände zu der Annahme berechtigen, dass der ursprüngliche Inhalt des Schriftstücks, dessen Abschrift beglaubigt werden soll, geändert worden ist, insbesondere wenn dieses Schriftstück Lücken, Durchstreichungen, Einschaltungen, Änderungen, unleserliche Wörter, Zahlen oder Zeichen, Spuren der Beseitigung von Wörtern, Zahlen und Zeichen enthält oder wenn der Zusammenhang eines aus mehreren Blättern bestehenden Schriftstücks aufgehoben ist.

(3) Eine Abschrift wird beglaubigt durch einen Beglaubigungsvermerk, der unter die Abschrift zu setzen ist. Der Vermerk muß enthalten

1. die genaue Bezeichnung des Schriftstücks, dessen Abschrift beglaubigt wird,
2. die Feststellung, dass die beglaubigte Abschrift mit dem vorgelegten Schriftstück übereinstimmt,
3. den Hinweis, dass die beglaubigte Abschrift nur zur Vorlage bei der angegebenen Behörde erteilt wird, wenn die Urschrift nicht von einer Behörde ausgestellt worden ist,
4. den Ort und den Tag der Beglaubigung, die Unterschrift des für die Beglaubigung zuständigen Bediensteten und das Dienstsiegel.

(4) Die Absätze 1 bis 3 gelten entsprechend für die Beglaubigung von

1. Ablichtungen, Lichtdrucken und ähnlichen in technischen Verfahren hergestellten Vervielfältigungen,
2. auf fototechnischem Wege von Schriftstücken hergestellten Negativen, die bei einer Behörde aufbewahrt werden,
3. Ausdrucken elektronischer Dokumente,
4. elektronischen Dokumenten,
  - a) die zur Abbildung eines Schriftstücks hergestellt wurden,
  - b) die ein anderes technisches Format als das mit einer qualifizierten elektronischen Signatur verbundene Ausgangsdokument erhalten haben.

(5) Der Beglaubigungsvermerk muß zusätzlich zu den Angaben nach Absatz 3 Satz 2 bei der Beglaubigung

1. des Ausdrucks eines elektronischen Dokuments, das mit einer qualifizierten elektronischen Signatur verbunden ist, die Feststellungen enthalten,
  - a) wen die Signaturprüfung als Inhaber der Signatur ausweist,
  - b) welchen Zeitpunkt die Signaturprüfung für die Anbringung der Signatur ausweist und
  - c) welche Zertifikate mit welchen Daten dieser Signatur zugrunde lagen;
2. eines elektronischen Dokuments den Namen des für die Beglaubigung zuständigen Bediensteten und die Bezeichnung der Behörde, die die Beglaubigung vornimmt, enthalten; die Unterschrift des für die Beglaubigung zuständigen Bediensteten und das Dienstsiegel nach Absatz 3 Satz 2 Nr. 4 werden durch eine dauerhaft überprüfbare qualifizierte elektronische Signatur ersetzt.

Wird ein elektronisches Dokument, das ein anderes technisches Format als das mit einer qualifizierten elektronischen Signatur verbundene Ausgangsdokument erhalten hat, nach Satz 1 Nr. 2 beglaubigt, muß der Beglaubigungsvermerk zusätzlich die Feststellungen nach Satz 1 Nr. 1 für das Ausgangsdokument enthalten.

(6) Die nach Absatz 4 hergestellten Dokumente stehen, sofern sie beglaubigt sind, beglaubigten Abschriften gleich.

### VwVfG § 37 Bestimmtheit und Form des Verwaltungsaktes

(1) Ein Verwaltungsakt muß inhaltlich hinreichend bestimmt sein.

(2) Ein Verwaltungsakt kann schriftlich, elektronisch, mündlich oder in anderer Weise erlassen werden. Ein mündlicher Verwaltungsakt ist schriftlich oder elektronisch zu bestätigen, wenn hieran ein berechtigtes Interesse besteht und der Betroffene dies unverzüglich verlangt. Ein elektronischer

Verwaltungsakt ist unter denselben Voraussetzungen schriftlich zu bestätigen; § 3a Abs. 2 findet insoweit keine Anwendung.

(3) Ein schriftlicher oder elektronischer Verwaltungsakt muß die erlassende Behörde erkennen lassen und die Unterschrift oder die Namenswiedergabe des Behördenleiters, seines Vertreters oder seines Beauftragten enthalten. Wird für einen Verwaltungsakt, für den durch Rechtsvorschrift die Schriftform angeordnet ist, die elektronische Form verwendet, muß auch das der Signatur zugrunde liegende qualifizierte Zertifikat oder ein zugehöriges qualifiziertes Attributzertifikat die erlassende Behörde erkennen lassen.

(4) Für einen Verwaltungsakt kann für die nach § 3a Abs. 2 erforderliche Signatur durch Rechtsvorschrift die dauerhafte Überprüfbarkeit vorgeschrieben werden.

(5) Bei einem schriftlichen Verwaltungsakt, der mit Hilfe automatischer Einrichtungen erlassen wird, können abweichend von Absatz 3 Unterschrift und Namenswiedergabe fehlen. Zur Inhaltsangabe können Schlüsselzeichen verwendet werden, wenn derjenige, für den der Verwaltungsakt bestimmt ist oder der von ihm betroffen wird, auf Grund der dazu gegebenen Erläuterungen den Inhalt des Verwaltungsaktes eindeutig erkennen kann.

### VwVfG § 69 Entscheidung

(1) Die Behörde entscheidet unter Würdigung des Gesamtergebnisses des Verfahrens.

(2) Verwaltungsakte, die das förmliche Verfahren abschließen, sind schriftlich zu erlassen, schriftlich zu begründen und den Beteiligten zuzustellen; in den Fällen des § 39 Abs. 2 Nr. 1 und 3 bedarf es einer Begründung nicht. Ein elektronischer Verwaltungsakt nach Satz 1 ist mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur zu versehen. Sind mehr als 50 Zustellungen vorzunehmen, so können sie durch öffentliche Bekanntmachung ersetzt werden. Die öffentliche Bekanntmachung wird dadurch bewirkt, dass der verfügende Teil des Verwaltungsaktes und die Rechtsbehelfsbelehrung im amtlichen Veröffentlichungsblatt der Behörde und außerdem in örtlichen Tageszeitungen bekannt gemacht werden, die in dem Bereich verbreitet sind, in dem sich die Entscheidung voraussichtlich auswirken wird. Der Verwaltungsakt gilt mit dem Tage als zugestellt, an dem seit dem Tage der Bekanntmachung in dem amtlichen Veröffentlichungsblatt zwei Wochen verstrichen sind; hierauf ist in der Bekanntmachung hinzuweisen. Nach der öffentlichen Bekanntmachung kann der Verwaltungsakt bis zum Ablauf der Rechtsbehelfsfrist von den Beteiligten schriftlich oder elektronisch angefordert werden; hierauf ist in der Bekanntmachung gleichfalls hinzuweisen.

(3) Wird das förmliche Verwaltungsverfahren auf andere Weise abgeschlossen, so sind die Beteiligten hiervon zu benachrichtigen. Sind mehr als 50 Benachrichtigungen vorzunehmen, so können sie durch öffentliche Bekanntmachung ersetzt werden; Absatz 2 Satz 3 gilt entsprechend.

### **ZPO § 292a Anscheinsbeweis bei qualifizierter elektronischer Signatur**

(Ab April 2005 ersetzt durch §371a ZPO)

### **ZPO § 144 Augenschein; Sachverständige**

(Stand Mai 2005)

(1) Das Gericht kann die Einnahme des Augenscheins sowie die Begutachtung durch Sachverständige anordnen. Es kann zu diesem Zweck einer Partei oder einem Dritten die Vorlegung eines in ihrem oder seinem Besitz befindlichen Gegenstandes aufgeben und hierfür eine Frist setzen. Es kann auch die Duldung der Maßnahme nach Satz 1 aufgeben, sofern nicht eine Wohnung betroffen ist.

(2) Dritte sind zur Vorlegung oder Duldung nicht verpflichtet, soweit ihnen diese nicht zumutbar ist oder sie zur Zeugnisverweigerung gemäß den §§ 383 bis 385 berechtigt sind. Die §§ 386 bis 390 gelten entsprechend.

(3) Das Verfahren richtet sich nach den Vorschriften, die eine auf Antrag angeordnete Einnahme des Augenscheins oder Begutachtung durch Sachverständige zum Gegenstand haben.

### **ZPO § 371 Beweis durch Augenschein**

(Stand Mai 2005)

(1) Der Beweis durch Augenschein wird durch Bezeichnung des Gegenstandes des Augenscheins und durch die Angabe der zu beweisenden Tatsachen angetreten. **Ist ein elektronisches Dokument Gegenstand des Beweises, wird der Beweis durch Vorlegung oder Übermittlung der Datei angetreten.**

(2) Befindet sich der Gegenstand nach der Behauptung des Beweisführers nicht in seinem Besitz, so wird der Beweis außerdem durch den Antrag angetreten, zur Herbeischaffung des Gegenstandes eine Frist zu setzen oder eine Anordnung nach § 144 zu erlassen. Die §§ 422 bis 432 gelten entsprechend.

(3) Vereitelt eine Partei die ihr zumutbare Einnahme des Augenscheins, so können die Behauptungen des Gegners über die Beschaffenheit des Gegenstandes als bewiesen angesehen werden.

### **ZPO § 371a Beweiskraft elektronischer Dokumente**

(Stand Mai 2005)

(1) Auf private elektronische Dokumente, die mit einer **qualifizierten elektronischen Signatur** versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich

auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.

(2) Auf elektronische Dokumente, die von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind (öffentliche elektronische Dokumente), finden die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Ist das Dokument mit einer qualifizierten elektronischen Signatur versehen, gilt § 437 entsprechend.

### ZPO § 286 Freie Beweiswürdigung

(Stand Mai 2005)

(1) Das Gericht hat unter Berücksichtigung des gesamten Inhalts der Verhandlungen und des Ergebnisses einer etwaigen Beweisaufnahme nach freier Überzeugung zu entscheiden, ob eine tatsächliche Behauptung für wahr oder für nicht wahr zu erachten sei. In dem Urteil sind die Gründe anzugeben, die für die richterliche Überzeugung leitend gewesen sind.

(2) An gesetzliche Beweisregeln ist das Gericht nur in den durch dieses Gesetz bezeichneten Fällen gebunden.

### ZPO § 453 Beweiswürdigung bei Parteivernehmung

(Stand Mai 2005)

(1) Das Gericht hat die Aussage der Partei nach § 286 frei zu würdigen.

(2) Verweigert die Partei die Aussage oder den Eid, so gilt § 446 entsprechend.

### ZPO § 416 Beweiskraft von Privaturkunden

(Stand Mai 2005)

Privaturkunden begründen, sofern sie von den Ausstellern unterschrieben oder mittels notariell beglaubigten Handzeichens unterzeichnet sind, vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen von den Ausstellern abgegeben sind.

### ZPO § 439 Erklärung über Echtheit von Privaturkunden

(Stand Mai 2005)

(1) Über die Echtheit einer Privaturkunde hat sich der Gegner des Beweisführers nach der Vorschrift des § 138 zu erklären.

(2) Befindet sich unter der Urkunde eine Namensunterschrift, so ist die Erklärung auf die Echtheit der Unterschrift zu richten.

(3) Wird die Erklärung nicht abgegeben, so ist die Urkunde als anerkannt anzusehen, wenn nicht die Absicht, die Echtheit bestreiten zu wollen, aus den übrigen Erklärungen der Partei hervorgeht.

### ZPO § 440 Beweis der Echtheit von Privaturkunden

(Stand Mai 2005)

- (1) Die Echtheit einer nicht anerkannten Privaturkunde ist zu beweisen.
- (2) Steht die Echtheit der Namensunterschrift fest oder ist das unter einer Urkunde befindliche Handzeichen notariell beglaubigt, so hat die über der Unterschrift oder dem Handzeichen stehende Schrift die Vermutung der Echtheit für sich.

### ZPO § 441 Schriftvergleichung

(Stand Mai 2005)

- (1) Der Beweis der Echtheit oder Unechtheit einer Urkunde kann auch durch Schriftvergleichung geführt werden.
- (2) In diesem Fall hat der Beweisführer zur Vergleichung geeignete Schriften vorzulegen oder ihre Mitteilung nach der Vorschrift des § 432 zu beantragen und erforderlichenfalls den Beweis ihrer Echtheit anzutreten.
- (3) Befinden sich zur Vergleichung geeignete Schriften in den Händen des Gegners, so ist dieser auf Antrag des Beweisführers zur Vorlegung verpflichtet. Die Vorschriften der §§ 421 bis 426 gelten entsprechend. Kommt der Gegner der Anordnung, die zur Vergleichung geeigneten Schriften vorzulegen, nicht nach oder gelangt das Gericht im Falle des § 426 zu der Überzeugung, dass der Gegner nach dem Verbleib der Schriften nicht sorgfältig geforscht habe, so kann die Urkunde als echt angesehen werden.
- (4) Macht der Beweisführer glaubhaft, dass in den Händen eines Dritten geeignete Vergleichungsschriften sich befinden, deren Vorlegung er im Wege der Klage zu erwirken imstande sei, so gelten die Vorschriften des § 431 entsprechend.

### ZPO § 442 Würdigung der Schriftvergleichung

(Stand Mai 2005)

Über das Ergebnis der Schriftvergleichung hat das Gericht nach freier Überzeugung, geeignetenfalls nach Anhörung von Sachverständigen, zu entscheiden.

### 18 Richtlinie 1999/93/EG EG-Signaturrechtlinie

Eine Haftung oder Gewährleistung auf Vollständigkeit oder korrekter Wiedergabe der Texte kann nicht übernommen werden.

Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

*Amtsblatt Nr. L 013 vom 19/01/2000 S. 0012 - 0020*

#### RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 13. Dezember 1999

über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

#### DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION -

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 47 Absatz 2, Artikel 55 und 95,

auf Vorschlag der Kommission(1),

nach Stellungnahme des Wirtschafts- und Sozialausschusses(2),

nach Stellungnahme des Ausschusses der Regionen(3),

gemäß dem Verfahren des Artikels 251 des Vertrags(4),

in Erwägung nachstehender Gründe:

- (1) Am 16. April 1997 hat die Kommission dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuß und dem Ausschuß der Regionen eine Mitteilung mit dem Titel "Europäische Initiative für den elektronischen Geschäftsverkehr" vorgelegt.
- (2) Am 8. Oktober 1997 hat die Kommission dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuß und dem Ausschuß der Regionen eine Mitteilung über "Sicherheit und Vertrauen in elektronische Kommunikation - Ein europäischer Rahmen für digitale Signaturen und Verschlüsselung" unterbreitet.
- (3) Am 1. Dezember 1997 hat der Rat die Kommission aufgefordert, so bald wie möglich einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über digitale Signaturen vorzulegen.
- (4) Elektronische Kommunikation und elektronischer Geschäftsverkehr erfordern "elektronische Signaturen" und entsprechende Authentifizierungsdienste für Daten. Divergierende Regeln über die rechtliche Anerkennung elektronischer Signaturen und die Akkreditierung von Zertifizierungsdiensteanbietern in den Mitgliedstaaten können ein ernsthaftes Hindernis für die elektronische Kommunikation und den elektronischen Geschäftsverkehr darstellen. Klare gemeinschaftliche Rahmenbedingungen für elektronische

Signaturen stärken demgegenüber das Vertrauen und die allgemeine Akzeptanz hinsichtlich der neuen Technologien. Die Rechtsvorschriften der Mitgliedstaaten sollten den freien Waren- und Dienstleistungsverkehr im Binnenmarkt nicht behindern.

- (5) Die Interoperabilität von Produkten für elektronische Signaturen sollte gefördert werden. Gemäß Artikel 14 des Vertrags umfaßt der Binnenmarkt einen Raum ohne Binnengrenzen, in dem der freie Warenverkehr gewährleistet ist. Es sind grundlegende Anforderungen zu erfüllen, die speziell für Produkte für elektronische Signaturen gelten, um so den freien Verkehr im Binnenmarkt zu gewährleisten und das Vertrauen in digitale Signaturen zu fördern, wobei die Verordnung (EG) Nr. 3381/94 des Rates vom 19. Dezember 1994 über eine Gemeinschaftsregelung der Ausfuhrkontrolle von Gütern mit doppeltem Verwendungszweck(5) und der Beschluß 94/942/GASP des Rates vom 19. Dezember 1994 über die vom Rat angenommene gemeinsame Aktion zur Ausfuhrkontrolle von Gütern mit doppeltem Verwendungszweck(6) unberührt bleiben.
- (6) Mit der vorliegenden Richtlinie wird die Erbringung von Dienstleistungen im Bereich der Vertraulichkeit von Informationen nicht harmonisiert, wenn für derartige Dienstleistungen einzelstaatliche Vorschriften hinsichtlich der öffentlichen Ordnung oder Sicherheit gelten.
- (7) Der Binnenmarkt gewährleistet die Freizügigkeit von Personen, wodurch Bürger und Gebietsansässige der Europäischen Union zunehmend mit Stellen in anderen Mitgliedstaaten als demjenigen ihres Wohnsitzes in Verbindung treten müssen. Die Möglichkeit der elektronischen Kommunikation könnte in dieser Hinsicht von großem Nutzen sein.
- (8) Die rasche technologische Entwicklung und der globale Charakter des Internet erfordern ein Konzept, das verschiedenen Technologien und Dienstleistungen im Bereich der elektronischen Authentifizierung offensteht.
- (9) Elektronische Signaturen werden bei einer Vielzahl von Gegebenheiten und Anwendungen genutzt, die zu einem großen Spektrum neuer Dienste und Produkte im Zusammenhang mit oder unter Verwendung von elektronischen Signaturen führen. Die Definition solcher Produkte und Dienste sollte sich nicht auf die Ausstellung und Verwaltung von Zertifikaten beschränken, sondern sollte auch alle sonstigen Dienste und Produkte einschließen, die elektronische Signaturen verwenden oder mit ihnen zusammenhängen, wie Registrierungsdienste, Zeitstempel, Verzeichnisdienste, Rechnerdienste oder Beratungsdienste in Verbindung mit elektronischen Signaturen.
- (10) Der Binnenmarkt ermöglicht es Zertifizierungsdiensteanbietern, grenzüberschreitend tätig zu werden, um ihre Wettbewerbsfähigkeit zu steigern und damit Verbrauchern und Unternehmen ohne Rücksicht auf Grenzen neue Möglichkeiten des sicheren Informationsaustausches und elektronischen Geschäftsverkehrs zu eröffnen. Um das gemeinschaftsweite Anbieten von Zertifizierungsdiensten über offene Netze zu fördern, sollten Anbieter von Zertifizierungsdiensten diese ungehindert ohne vorherige Genehmigung bereitstellen können. Vorherige Genehmigung bedeutet nicht nur eine Erlaubnis, wonach der betreffende Zertifizierungsdiensteanbieter einen Bescheid der einzelstaatlichen Stellen einholen muß, bevor er seine Zertifizierungsdienste erbringen kann, sondern auch alle sonstigen Maßnahmen mit der gleichen Wirkung.

- (11) Freiwillige Akkreditierungssysteme, die auf eine Steigerung des Niveaus der erbrachten Dienste abzielen, können Zertifizierungsdiensteanbietern den geeigneten Rahmen für die Weiterentwicklung ihrer Dienste bieten, um das auf dem sich entwickelnden Markt geforderte Maß an Vertrauen, Sicherheit und Qualität zu erreichen. Diese Systeme sollten die Entwicklung bester Praktiken durch Zertifizierungsdiensteanbieter fördern. Zertifizierungsdiensteanbietern sollte es freistehen, sich akkreditieren zu lassen und Akkreditierungssysteme zu nutzen.
- (12) Zertifizierungsdienste sollten entweder von einer öffentlichen Stelle oder einer juristischen oder natürlichen Person angeboten werden können, sofern diese im Einklang mit den einzelstaatlichen Rechtsvorschriften niedergelassen ist. Die Mitgliedstaaten sollten es Anbietern von Zertifizierungsdiensten nicht untersagen, auch ohne freiwillige Akkreditierung tätig zu sein. Es ist darauf zu achten, dass Akkreditierungssysteme den Wettbewerb im Bereich der Zertifizierungsdienste nicht einschränken.
- (13) Die Mitgliedstaaten können entscheiden, wie sie die Überwachung der Einhaltung der Bestimmungen dieser Richtlinie gewährleisten. Diese Richtlinie schließt nicht aus, dass privatwirtschaftliche Überwachungssysteme geschaffen werden. Diese Richtlinie verpflichtet die Zertifizierungsdiensteanbieter nicht, eine Überwachung im Rahmen eines geltenden Akkreditierungssystems zu beantragen.
- (14) Es ist wichtig, ein ausgewogenes Verhältnis zwischen den Bedürfnissen der Verbraucher und der Unternehmen herzustellen.
- (15) Anhang III enthält die Anforderungen für sichere Signaturerstellungseinheiten zur Gewährleistung der Funktionalität fortgeschrittener elektronischer Signaturen. Er deckt nicht die gesamte Systemumgebung ab, in der die Einheit betrieben wird. Das Funktionieren des Binnenmarktes verlangt von der Kommission und den Mitgliedstaaten, rasch zu handeln, damit die Stellen benannt werden können, die für die Bewertung der Übereinstimmung von sicheren Signaturerstellungseinheiten mit den Anforderungen des Anhangs III zuständig sind. Um den Markterfordernissen zu entsprechen, muß die Bewertung der Übereinstimmung rechtzeitig und effizient erfolgen.
- (16) Diese Richtlinie leistet einen Beitrag zur Verwendung und rechtlichen Anerkennung elektronischer Signaturen in der Gemeinschaft. Es bedarf keiner gesetzlichen Rahmenbedingungen für elektronische Signaturen, die ausschließlich in Systemen verwendet werden, die auf freiwilligen privatrechtlichen Vereinbarungen zwischen einer bestimmten Anzahl von Teilnehmern beruhen. Die Freiheit der Parteien, die Bedingungen zu vereinbaren, unter denen sie elektronisch signierte Daten akzeptieren, sollte respektiert werden, soweit dies im Rahmen des innerstaatlichen Rechts möglich ist. Elektronischen Signaturen, die in solchen Systemen verwendet werden, sollte die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht abgesprochen werden.
- (17) Diese Richtlinie zielt nicht darauf ab, nationales Vertragsrecht, insbesondere betreffend den Abschluß und die Erfüllung von Verträgen, oder andere, außervertragliche Formvorschriften bezüglich der Unterschriften zu harmonisieren. Deshalb sollten die Regelungen über die rechtliche Wirksamkeit elektronischer Signaturen unbeschadet einzelstaatlicher Formvorschriften gelten, die den Abschluß von Verträgen oder die Festlegung des Ortes eines Vertragsabschlusses betreffen.

- (18) Das Speichern und Kopieren von Signaturerstellungsdaten könnte die Rechtsgültigkeit elektronischer Signaturen gefährden.
- (19) Elektronische Signaturen werden im öffentlichen Bereich innerhalb der staatlichen und gemeinschaftlichen Verwaltungen und im Kommunikationsverkehr zwischen diesen Verwaltungen sowie zwischen diesen und den Bürgern und Wirtschaftsteilnehmern eingesetzt, z. B. in den Bereichen öffentliche Auftragsvergabe, Steuern, soziale Sicherheit, Gesundheit und Justiz.
- (20) Durch harmonisierte Kriterien im Zusammenhang mit der Rechtswirkung elektronischer Signaturen läßt sich gemeinschaftsweit ein kohärenter Rechtsrahmen aufrechterhalten. In den einzelstaatlichen Rechtsvorschriften sind verschiedene Anforderungen für die Rechtsgültigkeit handschriftlicher Unterschriften niedergelegt. Zertifikate können dazu dienen, die Identität einer elektronisch signierenden Person zu bestätigen. Auf qualifizierten Zertifikaten beruhende fortgeschrittene elektronische Signaturen zielen auf einen höheren Sicherheitsstandard. Fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und von einer sicheren Signaturerstellungseinheit erstellt werden, können nur dann gegenüber handschriftlichen Unterschriften als rechtlich gleichwertig angesehen werden, wenn die Anforderungen für handschriftliche Unterschriften erfüllt sind.
- (21) Um die allgemeine Akzeptanz elektronischer Authentifizierungsmethoden zu fördern, ist zu gewährleisten, dass elektronische Signaturen in allen Mitgliedstaaten in Gerichtsverfahren als Beweismittel verwendet werden können. Die rechtliche Anerkennung elektronischer Signaturen sollte auf objektiven Kriterien beruhen und nicht mit einer Genehmigung für den betreffenden Zertifizierungsdiensteanbieter verknüpft sein. Die Festlegung der Rechtsgebiete, in denen elektronische Dokumente und elektronische Signaturen verwendet werden können, unterliegt einzelstaatlichem Recht. Diese Richtlinie läßt die Befugnis der einzelstaatlichen Gerichte, über die Übereinstimmung mit den Anforderungen dieser Richtlinie zu befinden, unberührt; sie berührt auch nicht die einzelstaatlichen Vorschriften über die freie gerichtliche Würdigung von Beweismitteln.
- (22) Diensteanbieter, die ihre Zertifizierungsdienste öffentlich anbieten, unterliegen den einzelstaatlichen Haftungsregelungen.
- (23) Die Entwicklung des internationalen elektronischen Geschäftsverkehrs erfordert grenzüberschreitende Vereinbarungen unter Beteiligung von Drittländern. Um die weltweite Interoperabilität zu gewährleisten, könnten Vereinbarungen mit Drittländern über multilaterale Regeln betreffend die gegenseitige Anerkennung der Zertifizierungsdienste nützlich sein.
- (24) Zur Stärkung des Vertrauens der Nutzer in die elektronische Kommunikation und den elektronischen Geschäftsverkehr müssen die Zertifizierungsdiensteanbieter die Vorschriften über den Datenschutz und den Schutz der Privatsphäre achten.
- (25) Die Bestimmungen über die Nutzung von Pseudonymen in Zertifikaten hindern die Mitgliedstaaten nicht daran, eine Identifizierung der Personen nach Gemeinschaftsrecht oder einzelstaatlichem Recht zu verlangen.

- (26) Die zur Durchführung dieser Richtlinie erforderlichen Maßnahmen sind gemäß Artikel 2 des Beschlusses 1999/468/EG des Rates vom 28. Juni 1999 zur Festlegung der Modalitäten für die Ausübung der der Kommission übertragenen Durchführungsbefugnisse(7) zu erlassen.
- (27) Die Kommission nimmt zwei Jahre nach der Umsetzung dieser Richtlinie eine Überprüfung vor, um unter anderem sicherzustellen, dass der technologische Fortschritt oder Änderungen des rechtlichen Umfelds keine Hindernisse für die Realisierung der erklärten Ziele dieser Richtlinie mit sich gebracht haben. Sie sollte die Auswirkungen verwandter technischer Bereiche prüfen und dem Europäischen Parlament und dem Rat hierüber einen Bericht vorlegen.
- (28) Nach den in Artikel 5 des Vertrags niedergelegten Grundsätzen der Subsidiarität und der Verhältnismäßigkeit kann das Ziel der Schaffung harmonisierter rechtlicher Rahmenbedingungen für die Bereitstellung elektronischer Signaturen und entsprechender Dienste von den Mitgliedstaaten nicht ausreichend erreicht werden und läßt sich daher besser durch die Gemeinschaft verwirklichen. Diese Richtlinie geht nicht über das zur Erreichung dieses Ziels erforderliche Maß hinaus -

HABEN FOLGENDE RICHTLINIE ERLASSEN:

### Artikel I - Anwendungsbereich

Diese Richtlinie soll die Verwendung elektronischer Signaturen erleichtern und zu ihrer rechtlichen Anerkennung beitragen. Sie legt rechtliche Rahmenbedingungen für elektronische Signaturen und für bestimmte Zertifizierungsdienste fest, damit das reibungslose Funktionieren des Binnenmarktes gewährleistet ist.

Es werden weder Aspekte im Zusammenhang mit dem Abschluß und der Gültigkeit von Verträgen oder anderen rechtlichen Verpflichtungen, für die nach einzelstaatlichem Recht oder Gemeinschaftsrecht Formvorschriften zu erfüllen sind, erfaßt, noch werden im einzelstaatlichen Recht oder im Gemeinschaftsrecht vorgesehene Regeln und Beschränkungen für die Verwendung von Dokumenten berührt.

### Artikel 2 - Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

1. "elektronische Signatur" Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen;
2. "fortgeschrittene elektronische Signatur" eine elektronische Signatur, die folgende Anforderungen erfüllt:
  - a) Sie ist ausschließlich dem Unterzeichner zugeordnet;
  - b) sie ermöglicht die Identifizierung des Unterzeichners;
  - c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;
  - d) sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann;
3. "Unterzeichner" eine Person, die eine Signaturerstellungseinheit besitzt und die entweder im eigenen Namen oder im Namen der von ihr vertretenen Stelle oder juristischen oder natürlichen Person handelt;
4. "Signaturerstellungsdaten" einmalige Daten wie Codes oder private kryptographische Schlüssel, die vom Unterzeichner zur Erstellung einer elektronischen Signatur verwendet werden;
5. "Signaturerstellungseinheit" eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturerstellungsdaten verwendet wird;
6. "sichere Signaturerstellungseinheit" eine Signaturerstellungseinheit, die die Anforderungen des Anhangs III erfüllt;
7. "Signaturprüfdaten" Daten wie Codes oder öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden;

8. "Signaturprüfeinheit" eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturprüfdaten verwendet wird;
9. "Zertifikat" eine elektronische Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und die Identität dieser Person bestätigt wird;
10. "qualifiziertes Zertifikat" ein Zertifikat, das die Anforderungen des Anhangs I erfüllt und von einem Zertifizierungsdiensteanbieter bereitgestellt wird, der die Anforderungen des Anhangs II erfüllt;
11. "Zertifizierungsdiensteanbieter" eine Stelle oder eine juristische oder natürliche Person, die Zertifikate ausstellt oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellt;
12. "Produkt für elektronische Signaturen" Hard- oder Software bzw. deren spezifische Komponenten, die von einem Zertifizierungsdiensteanbieter für die Bereitstellung von Diensten für elektronische Signaturen verwendet werden sollen oder die für die Erstellung und Überprüfung elektronischer Signaturen verwendet werden sollen;
13. "freiwillige Akkreditierung" eine Erlaubnis, mit der die Rechte und Pflichten für die Erbringung von Zertifizierungsdiensten festgelegt werden und die auf Antrag des betreffenden Zertifizierungsdiensteanbieters von der öffentlichen oder privaten Stelle, die für die Festlegung dieser Rechte und Pflichten sowie für die Überwachung ihrer Einhaltung zuständig ist, erteilt wird, wenn der Zertifizierungsdiensteanbieter die sich aus der Erlaubnis ergebenden Rechte nicht ausüben darf, bevor er den Bescheid der Stelle erhalten hat.

### Artikel 3 - Marktzugang

1. Die Mitgliedstaaten machen die Bereitstellung von Zertifizierungsdiensten nicht von einer vorherigen Genehmigung abhängig.
2. Unbeschadet des Absatzes I können die Mitgliedstaaten freiwillige Akkreditierungssysteme einführen bzw. beibehalten, die auf die Steigerung des Niveaus der erbrachten Zertifizierungsdienste abzielen. Alle mit diesen Systemen verknüpften Anforderungen müssen objektiv, transparent, verhältnismäßig und nichtdiskriminierend sein. Die Mitgliedstaaten dürfen die Zahl der akkreditierten Zertifizierungsdiensteanbieter nicht aus Gründen einschränken, die in den Geltungsbereich dieser Richtlinie fallen.
3. Die Mitgliedstaaten tragen dafür Sorge, dass ein geeignetes System zur Überwachung der in ihrem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter, die öffentlich qualifizierte Zertifikate ausstellen, eingerichtet wird.
4. Die Übereinstimmung sicherer Signaturerstellungseinheiten mit den Anforderungen nach Anhang III wird von geeigneten öffentlichen oder privaten Stellen festgestellt, die von den Mitgliedstaaten benannt werden. Die Kommission legt nach dem Verfahren des Artikels 9 Kriterien fest, anhand deren die Mitgliedstaaten bestimmen, ob eine Stelle zur Benennung geeignet ist.

Die von den in Unterabsatz I genannten Stellen vorgenommene Feststellung der Übereinstimmung mit den Anforderungen des Anhangs III wird von allen Mitgliedstaaten anerkannt.

5. Die Kommission kann nach dem Verfahren des Artikels 9 Referenznummern für allgemein anerkannte Normen für Produkte für elektronische Signaturen festlegen und im Amtsblatt der Europäischen Gemeinschaften veröffentlichen. Die Mitgliedstaaten gehen davon aus, dass die Anforderungen nach Anhang II Buchstabe f) und Anhang III erfüllt sind, wenn ein Produkt für elektronische Signaturen diesen Normen entspricht.
6. Die Mitgliedstaaten und die Kommission arbeiten unter Berücksichtigung der Empfehlungen für die sichere Signaturprüfung in Anhang IV und im Interesse des Verbrauchers zusammen, um die Entwicklung und die Nutzung von Signaturprüfeinheiten zu fördern.
7. Die Mitgliedstaaten können den Einsatz elektronischer Signaturen im öffentlichen Bereich möglichen zusätzlichen Anforderungen unterwerfen. Diese Anforderungen müssen objektiv, transparent, verhältnismäßig und nichtdiskriminierend sein und dürfen sich nur auf die spezifischen Merkmale der betreffenden Anwendung beziehen. Diese Anforderungen dürfen für grenzüberschreitende Dienste für den Bürger kein Hindernis darstellen.

### Artikel 4 - Binnenmarktgrundsätze

1. Jeder Mitgliedstaat wendet die innerstaatlichen Bestimmungen, die er aufgrund dieser Richtlinie erlässt, auf die in seinem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter und deren Dienste an. Die Mitgliedstaaten dürfen die

# StepOver

## Leitfaden zur e-Signatur

Bereitstellung von Zertifizierungsdiensten, die aus anderen Mitgliedstaaten stammen, in den unter diese Richtlinie fallenden Bereichen nicht einschränken.

2. Die Mitgliedstaaten tragen dafür Sorge, dass Produkte für elektronische Signaturen, die den Anforderungen dieser Richtlinie entsprechen, frei im Binnenmarkt verkehren können.

### Artikel 5 - Rechtswirkung elektronischer Signaturen

1. Die Mitgliedstaaten tragen dafür Sorge, dass fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und die von einer sicheren Signaturerstellungseinheit erstellt werden,
  - a) die rechtlichen Anforderungen an eine Unterschrift in bezug auf in elektronischer Form vorliegende Daten in gleicher Weise erfüllen wie handschriftliche Unterschriften in bezug auf Daten, die auf Papier vorliegen, und
  - b) in Gerichtsverfahren als Beweismittel zugelassen sind.
2. Die Mitgliedstaaten tragen dafür Sorge, dass einer elektronischen Signatur die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen wird,
  - weil sie in elektronischer Form vorliegt oder
  - nicht auf einem qualifizierten Zertifikat beruht oder
  - nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder
  - nicht von einer sicheren Signaturerstellungseinheit erstellt wurde.

### Artikel 6 - Haftung

1. Die Mitgliedstaaten gewährleisten als Mindestregelung, dass ein Zertifizierungsdiensteanbieter, der ein Zertifikat als qualifiziertes Zertifikat öffentlich ausstellt oder für ein derartiges Zertifikat öffentlich einsteht, in bezug auf Schäden gegenüber einer Stelle oder einer juristischen oder natürlichen Person, die vernünftigerweise auf das Zertifikat vertraut, dafür haftet, dass
  - a) alle Informationen in dem qualifizierten Zertifikat zum Zeitpunkt seiner Ausstellung richtig sind und das Zertifikat alle für ein qualifiziertes Zertifikat vorgeschriebenen Angaben enthält,
  - b) der in dem qualifizierten Zertifikat angegebene Unterzeichner zum Zeitpunkt der Ausstellung des Zertifikats im Besitz der Signaturstellungsdaten war, die den im Zertifikat angegebenen bzw. identifizierten Signaturprüfdaten entsprechen,
  - c) in Fällen, in denen der Zertifizierungsdiensteanbieter sowohl die Signaturstellungsdaten als auch die Signaturprüfdaten erzeugt, beide Komponenten in komplementärer Weise genutzt werden können,  
es sei denn, der Zertifizierungsdiensteanbieter weist nach, dass er nicht fahrlässig gehandelt hat.
2. Die Mitgliedstaaten gewährleisten als Mindestregelung, dass ein Zertifizierungsdiensteanbieter, der ein Zertifikat als qualifiziertes Zertifikat öffentlich ausgestellt hat, in bezug auf Schäden gegenüber einer Stelle oder einer juristischen oder natürlichen Person, die vernünftigerweise

auf das Zertifikat vertraut, für den Fall haftet, dass der Widerruf des Zertifikats nicht registriert worden ist, es sei denn, der Zertifizierungsdiensteanbieter weist nach, dass er nicht fahrlässig gehandelt hat.

3. Die Mitgliedstaaten tragen dafür Sorge, dass Zertifizierungsdiensteanbieter in einem qualifizierten Zertifikat Beschränkungen für die Verwendung des Zertifikates angeben können; diese Beschränkungen müssen für Dritte erkennbar sein. Der Zertifizierungsdiensteanbieter haftet nicht für Schäden, die sich aus einer über diese Beschränkungen hinausgehenden Verwendung des qualifizierten Zertifikats ergeben.
4. Die Mitgliedstaaten tragen dafür Sorge, dass Zertifizierungsdiensteanbieter in dem qualifizierten Zertifikat eine Grenze für den Wert der Transaktionen angeben können, für die das Zertifikat verwendet werden kann; diese Grenze muß für Dritte erkennbar sein. Der Zertifizierungsdiensteanbieter haftet nicht für Schäden, die sich aus der Überschreitung dieser Höchstgrenze ergeben.
5. Die Absätze 1 bis 4 gelten unbeschadet der Richtlinie 93/13/EWG des Rates vom 5. April 1993 über mißbräuchliche Klauseln in Verbraucherverträgen(8).

### Artikel 7 - Internationale Aspekte

1. Die Mitgliedstaaten tragen dafür Sorge, dass Zertifikate, die von einem Zertifizierungsdiensteanbieter eines Drittlandes öffentlich als qualifizierte Zertifikate ausgestellt werden, den von einem in der Gemeinschaft niedergelassenen Zertifizierungsdiensteanbieter ausgestellten Zertifikaten rechtlich gleichgestellt werden, wenn
  - a) der Zertifizierungsdiensteanbieter die Anforderungen dieser Richtlinie erfüllt und im Rahmen eines freiwilligen Akkreditierungssystems eines Mitgliedstaats akkreditiert ist oder
  - b) ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen dieser Richtlinie erfüllt, für das Zertifikat einsteht oder
  - c) das Zertifikat oder der Zertifizierungsdiensteanbieter im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Gemeinschaft und Drittländern oder internationalen Organisationen anerkannt ist.
2. Um grenzüberschreitende Zertifizierungsdienste mit Drittländern und die rechtliche Anerkennung fortgeschrittener elektronischer Signaturen, die aus Drittländern stammen, zu erleichtern, unterbreitet die Kommission gegebenenfalls Vorschläge mit dem Ziel, die effiziente Umsetzung von Normen und internationalen Vereinbarungen über Zertifizierungsdienste zu erreichen. Insbesondere unterbreitet sie dem Rat bei Bedarf Vorschläge zur Erteilung von geeigneten Mandaten zur Aushandlung bilateraler und multilateraler Vereinbarungen mit Drittländern und internationalen Organisationen. Der Rat beschließt mit qualifizierter Mehrheit.
3. Wird die Kommission über Schwierigkeiten unterrichtet, auf die Unternehmen der Gemeinschaft beim Marktzugang in Drittländern stoßen, so kann sie erforderlichenfalls dem Rat Vorschläge für ein geeignetes Mandat zur Aushandlung vergleichbarer Rechte für Unternehmen der Gemeinschaft in diesen Drittländern vorlegen. Der Rat beschließt mit qualifizierter Mehrheit.

Die gemäß diesem Absatz ergriffenen Maßnahmen lassen die Verpflichtungen der Gemeinschaft und der Mitgliedstaaten im Rahmen der einschlägigen internationalen Übereinkünfte unberührt.

### Artikel 8 - Datenschutz

1. Die Mitgliedstaaten tragen dafür Sorge, dass Zertifizierungsdiensteanbieter und die für die Akkreditierung und Aufsicht zuständigen nationalen Stellen die Anforderungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr(9) erfüllen.
2. Die Mitgliedstaaten tragen dafür Sorge, dass Zertifizierungsdiensteanbieter, die öffentlich Zertifikate ausstellen, personenbezogene Daten nur unmittelbar von der betroffenen Person oder mit ausdrücklicher Zustimmung der betroffenen Person und nur insoweit einholen

können, als dies zur Ausstellung und Aufrechterhaltung des Zertifikats erforderlich ist. Die Daten dürfen ohne ausdrückliche Zustimmung der betroffenen Person nicht für anderweitige Zwecke erfaßt oder verarbeitet werden.

3. Unbeschadet der Rechtswirkungen, die Pseudonyme nach einzelstaatlichem Recht haben, hindern die Mitgliedstaaten Zertifizierungsdiensteanbieter nicht daran, im Zertifikat ein Pseudonym anstelle des Namens des Unterzeichners anzugeben.

### **Artikel 9 - Ausschuß**

1. Die Kommission wird von einem "Ausschuß für elektronische Signaturen" (im folgenden "Ausschuß" genannt) unterstützt.
2. Bei einer Bezugnahme auf diesen Absatz finden die Artikel 4 und 7 des Beschlusses 1999/468/EG Anwendung, wobei Artikel 8 desselben Beschlusses zu beachten ist.

Der Zeitraum nach Artikel 4 Absatz 3 des Beschlusses 1999/468/EG wird auf drei Monate festgesetzt.

3. Der Ausschuß gibt sich eine Geschäftsordnung.

### Artikel 10 - Aufgaben des Ausschusses

Der Ausschuß präzisiert die in den Anhängen festgelegten Anforderungen, die Kriterien nach Artikel 3 Absatz 4 und die allgemein anerkannten Normen für Produkte für elektronische Signaturen, die gemäß Artikel 3 Absatz 5 festgelegt und veröffentlicht werden, nach dem Verfahren des Artikels 9 Absatz 2.

### Artikel 11 - Notifizierung

1. Die Mitgliedstaaten übermitteln der Kommission und den übrigen Mitgliedstaaten folgende Informationen:
  - a) Angaben zu nationalen freiwilligen Akkreditierungssystemen einschließlich zusätzlicher Anforderungen gemäß Artikel 3 Absatz 7,
  - b) Namen und Anschriften der für Akkreditierung und Aufsicht zuständigen nationalen Stellen und der in Artikel 3 Absatz 4 genannten Stellen sowie
  - c) Namen und Anschriften aller akkreditierten nationalen Zertifizierungsdiensteanbieter.
2. Die Informationen gemäß Absatz 1 und diesbezügliche Änderungen sind von den Mitgliedstaaten so bald wie möglich zu übermitteln.

### Artikel 12 - Überprüfung

1. Die Kommission überprüft die Durchführung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat spätestens zum 19. Juli 2003 darüber Bericht.
2. Bei der Überprüfung ist unter anderem festzustellen, ob der Anwendungsbereich dieser Richtlinie angesichts der technologischen und rechtlichen Entwicklungen und der Marktentwicklung geändert werden sollte. Der Bericht umfaßt insbesondere eine Bewertung der Harmonisierungsaspekte auf der Grundlage der gesammelten Erfahrungen. Gegebenenfalls sind dem Bericht Vorschläge für Rechtsvorschriften beizufügen.

### Artikel 13 - Durchführung

1. Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie vor dem 19. Juli 2001 nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Wenn die Mitgliedstaaten diese Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.
2. Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten innerstaatlichen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

### **Artikel 14 - Inkrafttreten**

Diese Richtlinie tritt am Tag ihrer Veröffentlichung im Amtsblatt der Europäischen Gemeinschaften in Kraft.

### **Artikel 15 - Adressaten**

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am 13. Dezember 1999.

Im Namen des Europäischen Parlaments

Die Präsidentin

N. FONTAINE

Im Namen des Rates

Der Präsident

S. HASSI

- (1) ABl. C 325 vom 23.10.1998, S. 5.
- (2) ABl. C 40 vom 15.2.1999, S. 29.
- (3) ABl. C 93 vom 6.4.1999, S. 33.
- (4) Stellungnahme des Europäischen Parlaments vom 13. Januar 1999 (ABl. C 104 vom 14.4.1999, S. 49). Gemeinsamer Standpunkt des Rates vom 28. Juni 1999 (ABl. C 243 vom 27.8.1999, S. 33) und Beschluß des Europäischen Parlaments vom 27. Oktober 1999 (noch nicht im Amtsblatt veröffentlicht). Beschluß des Rates vom 30. November 1999.
- (5) ABl. L 367 vom 31.12.1994, S. 1. Verordnung geändert durch die Verordnung (EG) Nr. 837/95 (ABl. L 90 vom 21.4.1995, S. 1).
- (6) ABl. L 367 vom 31.12.1994, S. 8. Beschluß zuletzt geändert durch den Beschluß 1999/193/GASP (ABl. L 73 vom 19.3.1999, S. 1).
- (7) ABl. L 184 vom 17.7.1999, S. 23.
- (8) ABl. L 95 vom 21.4.1993, S. 29.
- (9) ABl. L 281 vom 23.11.1995, S. 31.

## ANHANG I

Anforderungen an qualifizierte Zertifikate

Qualifizierte Zertifikate müssen folgende Angaben enthalten:

- a) Angabe, dass das Zertifikat als qualifiziertes Zertifikat ausgestellt wird;

- b) Angabe des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist;
- c) Name des Unterzeichners oder ein Pseudonym, das als solches zu identifizieren ist;
- d) Platz für ein spezifisches Attribut des Unterzeichners, das gegebenenfalls je nach Bestimmungszweck des Zertifikats aufgenommen wird;
- e) Signaturprüfdaten, die den vom Unterzeichner kontrollierten Signaturerstellungsdaten entsprechen;
- f) Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikats;
- g) Identitätscode des Zertifikats;
- h) die fortgeschrittene elektronische Signatur des ausstellenden Zertifizierungsdiensteanbieters;
- i) gegebenenfalls Beschränkungen des Geltungsbereichs des Zertifikats und
- j) gegebenenfalls Begrenzungen des Wertes der Transaktionen, für die das Zertifikat verwendet werden kann.

### ANHANG II

#### Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen

##### Zertifizierungsdiensteanbieter

- a) müssen die erforderliche Zuverlässigkeit für die Bereitstellung von Zertifizierungsdiensten nachweisen;
- b) müssen den Betrieb eines schnellen und sicheren Verzeichnisdienstes und eines sicheren und unverzüglichen Widerrufsdienstes gewährleisten;
- c) müssen gewährleisten, dass Datum und Uhrzeit der Ausstellung oder des Widerrufs eines Zertifikats genau bestimmt werden können;
- d) müssen mit geeigneten Mitteln nach einzelstaatlichem Recht die Identität und gegebenenfalls die spezifischen Attribute der Person überprüfen, für die ein qualifiziertes Zertifikat ausgestellt wird;
- e) müssen Personal mit den für die angebotenen Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen beschäftigen; dazu gehören insbesondere Managementkompetenzen, Kenntnisse der Technologie elektronischer Signaturen und Vertrautheit mit angemessenen Sicherheitsverfahren; sie müssen ferner geeignete Verwaltungs- und Managementverfahren einhalten, die anerkannten Normen entsprechen;
- f) müssen vertrauenswürdige Systeme und Produkte einsetzen, die vor Veränderungen geschützt sind und die die technische und kryptographische Sicherheit der von ihnen unterstützten Verfahren gewährleisten;
- g) müssen Maßnahmen gegen Fälschungen von Zertifikaten ergreifen und in den Fällen, in denen sie Signaturerstellungsdaten erzeugen, die Vertraulichkeit während der Erzeugung dieser Daten gewährleisten;
- h) müssen über ausreichende Finanzmittel verfügen, um den Anforderungen der Richtlinie entsprechend arbeiten zu können. Sie müssen insbesondere in der Lage sein, das Haftungsrisiko für Schäden zu tragen, zum Beispiel durch Abschluß einer entsprechenden Versicherung;
- i) müssen alle einschlägigen Informationen über ein qualifiziertes Zertifikat über einen angemessenen Zeitraum aufzeichnen, um insbesondere für Gerichtsverfahren die Zertifizierung nachweisen zu können. Die Aufzeichnungen können in elektronischer Form erfolgen;
- j) dürfen keine Signaturerstellungsdaten von Personen speichern oder kopieren, denen Schlüsselmanagementdienste angeboten werden;
- k) müssen, bevor sie in Vertragsbeziehungen mit einer Person eintreten, die von ihnen ein Zertifikat zur Unterstützung ihrer elektronischen Signatur wünscht, diese Person mit einem dauerhaften Kommunikationsmittel über die genauen Bedingungen für die Verwendung des Zertifikats informieren, wozu unter anderem Nutzungsbeschränkungen

für das Zertifikat, die Existenz eines freiwilligen Akkreditierungssystems und das Vorgehen in Beschwerde- und Schlichtungsverfahren gehören. Diese Angaben müssen schriftlich - gegebenenfalls elektronisch übermittelt - in klar verständlicher Sprache vorliegen. Wichtige Teilinformationen werden auf Antrag auch Dritten zur Verfügung gestellt, die auf das Zertifikat vertrauen;

- l) müssen vertrauenswürdige Systeme für die Speicherung von Zertifikaten in einer überprüfbaren Form verwenden, so dass
  - nur befugte Personen Daten eingeben und ändern können;
  - die Angaben auf ihre Echtheit hin überprüft werden können;
  - Zertifikate nur in den Fällen öffentlich abrufbar sind, für die die Zustimmung des Inhabers des Zertifikats eingeholt wurde;
  - technische Veränderungen, die die Einhaltung dieser Sicherheitsanforderungen beeinträchtigen, für den Betreiber klar ersichtlich sind.

### ANHANG III

#### Anforderungen an sichere Signaturerstellungseinheiten

1. Sichere Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass
  - a) die für die Erzeugung der Signatur verwendeten Signaturstellungsdaten praktisch nur einmal auftreten können und dass ihre Geheimhaltung hinreichend gewährleistet ist;
  - b) die für die Erzeugung der Signatur verwendeten Signaturstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die Signatur vor Fälschungen bei Verwendung der jeweils verfügbaren Technologie geschützt ist;
  - c) die für die Erzeugung der Signatur verwendeten Signaturstellungsdaten von dem rechtmäßigen Unterzeichner vor der Verwendung durch andere verlässlich geschützt werden können.
2. Sichere Signaturerstellungseinheiten verändern die zu unterzeichnenden Daten nicht und verhindern nicht, dass diese Daten dem Unterzeichner vor dem Signaturvorgang dargestellt werden.

### ANHANG IV

#### Empfehlungen für die sichere Signaturprüfung

Während des Signaturprüfungsvorgangs ist mit hinreichender Sicherheit zu gewährleisten, dass

- a) die zur Überprüfung der Signatur verwendeten Daten den Daten entsprechen, die dem Überprüfer angezeigt werden,
- b) die Signatur zuverlässig überprüft wird und das Ergebnis dieser Überprüfung korrekt angezeigt wird,
- c) der Überprüfer bei Bedarf den Inhalt der unterzeichneten Daten zuverlässig feststellen kann,
- d) die Echtheit und die Gültigkeit des zum Zeitpunkt der Überprüfung der Signatur verlangten Zertifikats zuverlässig überprüft werden,
- e) das Ergebnis der Überprüfung sowie die Identität des Unterzeichners korrekt angezeigt werden,
- f) die Verwendung eines Pseudonyms eindeutig angegeben wird, und
- g) sicherheitsrelevante Veränderungen erkannt werden können.