Elektronische Signaturen

DISSERTATION

der Rechtswissenschaftlichen Fakultät
der Universität Zürich
zur Erlangung der Würde eines Doktors der Rechtswissenschaft

vorgelegt von
Simon Schlauri
von Oberbüren SG

genehmigt auf Antrag von
Prof. Dr. Rolf H. Weber

Schulthess Juristische Medien AG, Zürich

Dank

Besonderen Dank schulde ich meinem Doktorvater Prof. Dr. Rolf H. Weber für die wertvolle Unterstützung und die Freiheit, die er mir bei der Bearbeitung des Themas gewährte.

Sodann danke ich Herrn dipl. sc. nat. Reto Kohlas für die wertvollen Anregungen, die er mir im Rahmen zahlreicher Gespräche vermittelte, sowie Herrn Dr. iur. Oliver Frei, Herrn Rechtsanwalt Dr. iur. Franz J. Kessler und Herrn cand. iur. Christian Tannò für die sorgfältige und kritische Durchsicht des Manuskripts.

Zu Dank verpflichtet bin ich im Weiteren der Janggen-Pöhn-Stiftung, St. Gallen, deren Unterstützung es mir erlaubte, mich während eines halben Jahres ganz auf die vorliegende Arbeit zu konzentrieren.

Meinen Eltern, die mich stets liebevoll unterstützten, widme ich dieses Buch in grosser Dankbarkeit.

Zürich, im April 2002 Simon Schlauri

Inhaltsübersicht

Inhaltsverzeichnis III
Abkürzungsverzeichnis XVIII
Literaturverzeichnis XXIII
Materialien- und Rechtsquellenverzeichnis XXXVII

1. Teil: Grundlagen 1
§1 Einleitung 3
§2 Sicherheitsfragen im Internet 7
§3 Kryptographie 11
§4 Beweiseignung der digitalen Signatur 54
§5 Ökonomische Aspekte 60

2. Teil: Regelungsbereiche und internationaler Überblick 71
§6 Regelungsbereiche und -modelle 73
§7 Einige wichtige ausländische Regelungen im Überblick 87

3. Teil: Regelung im schweizerischen Recht 127
§8 Einleitung 129
§9 Sicherungsinfrastruktur 139
§10 Beweisrecht und Haftungsfragen 150
§11 Prozessuale Anerkennung 203
§12 Materiellrechtliche Anerkennung 210
§13 Zusammenfassung der Ergebnisse 244
Stichwortverzeichnis 253

Inhaltsverzeichnis

Abkürzungsverzeichnis XVIII

Literaturverzeichnis XXIII

Materialien- und Rechtsquellenverzeichnis XXXVII

1. Teil: Grundlagen 1

§1 Einleitung 3
I. Allgemeines 3
II. Thematik und Abgrenzung 4
III. Überblick über die Darstellung 5

§2 Sicherheitsfragen im Internet 7
I. Fragestellung 7
II. Abriss über die Funktionsweise des Internet 7
III. Vertraulichkeit 8
IV. Authentizität 8
V. Datenintegrität 8
VI. Nichtabstreitbarkeit 9
VII. Weitere Sicherheitsprobleme 10

§3 Kryptographie 11
I. Gang der Darstellung 11
II. Begriffe 11
A. Kryptographie 11
B. Digitale und elektronische Signatur 11
C. Digitalisierte Unterschrift 12
III. Digitale Signatur 12
A. Schlüsselpaar 12
B. Erzeugen der Signatur 13
1. Grundlagen 13
2. Signatur und Verschlüsselung 14
3. Hashwert 15
4. Kryptographische Sicherheit 15
5. Präsentationsproblem 17
a) Allgemeines 17
b) Vertrauenswürdige Hardware als Lösung 17
C. Aufbewahrung und Schutz des Signierschlüssels 19
1. Grundlagen 19
2. Soft- und Hardwareschutz 19
3. PIN oder Passwort 20

4. Biometrie 21
5. Anforderungen an Anwender und Software 22
D. Schlüsselzertifizierung 22
1. Grundlagen 22
2. Web of Trust 23
3. Zertifizierung 23
4. Veröffentlichung von Zertifikaten 25
5. Ablauf von Zertifikaten 26
6. Sperrung von Zertifikaten 26
7. Wurzelzertifikat und Zertifizierungshierarchie 27
8. Kreuzzertifizierung 28
9. ITU-T Empfehlung X.509 29
a) Allgemeines 29
b) Inhalt eines Zertifikats 29
c) Profile und Interoperabilitätsspezifikationen 31
10. Attributzertifikate und Zertifikatsmodifikation 31
E. Prüfen der Signatur 31
1. Grundlagen 31
2. Vergleich der Hashwerte 32
3. Überprüfung der Zertifikate insbesondere 32
4. Angriff durch Täuschung des Empfängers 33
F. Standards und Anwendungsbeispiele 33
1. Offene und geschlossene Benutzergruppen 33
2. Unterzeichnen von Dokumenten 34
a) E-Mail 34
b) Electronic Data Interchange 36
c) Form Signing 36
d) Code Signing 37
3. Digitale Signatur als digitaler Ausweis 37
a) Allgemeines 37
b) Einsatz als lokales Authentifizierungsmittel 38
c) Virtual Private Networks 38
d) Server-Authentifizierung 38
e) Client-Authentifizierung 39
f) E-Banking insbesondere 39
4. Digitale Signatur im M-Commerce 40
5. Identrus 41
6. Swisscert 42
a) Allgemeines 42
b) Dezentrale Registrierung 42
aa) Überblick über die Funktionsweise 42
bb) Identifikation des Signierschlüsselhalters 43
cc) Datenintegrität und Nichtabstreitbarkeit 43

c) Flexible Zertifikate . . . 44
IV. Verschlüsselung . . . 44
A. Vorbemerkung . . . 44
B. Symmetrische Verschlüsselung . . . 44
C. Asymmetrische Verschlüsselung . . . 45
D. Hybride Verfahren . . . 45
V. Zeitstempel . . . 46
A. Grundlagen . . . 46
B. Überblick über die Funktionsweise . . . 46
1. Erste Lösung: Vertrauen . . . 46
a) Vertrauenswürdige dritte Partei . . . 46
b) Hashwerte als Vereinfachung . . . 47
2. Zweite Lösung: Zeugnis der Öffentlichkeit . . . 47
a) Problemstellung . . . 47
b) Publikation eines Wurzel-Hashwertes . . . 47
3. Signierte Zeitstempel-Tokens als Hybridlösung . . . 49
4. Praktische Anwendung . . . 49
C. Zeitstempel als wichtiger Teil der Sicherungsinfrastruktur . . . 49
1. Rückdatierungsproblem . . . 49
2. Verlängerung der kryptographischen Sicherheit . . . 50
D. Unmittelbare Bedeutung für den Rechtsverkehr . . . 51
E. Gesetzliche Regelung von Zeitstempeldiensten . . . 52

§4 Beweiseignung der digitalen Signatur . . . 54
I. Fragestellung . . . 54
II. Beziehungen beim Erzeugen der digitalen Signatur . . . 54
A. Signierschlüssel – Prüfschlüssel . . . 54
B. Prüfschlüssel – Name . . . 55
C. Name – Schlüsselhalter . . . 55
D. Schlüsselhalter – Unterzeichner . . . 56
E. Unterzeichner – Dokument . . . 56
F. Signiertes Dokument – Signatur . . . 57
G. Abschliessender Überblick . . . 57
III. Ablauf und Sperrung des Zertifikats . . . 58
IV. Signaturprüfung . . . 58
V. Folgerungen . . . 58
A. Hohe Komplexität des Beweises . . . 58
B. Niedrige Beweiskraft . . . 59
C. Neue Fragestellung . . . 59

§5 Ökonomische Aspekte . . . 60
I. Fragestellung . . . 60
II. Gründe für die langsame Verbreitung der digitalen Signatur . . . 60
A. Pinguin-Effekt . . . 60

B. Infrastruktur-Inseln 61
C. Kosten-Nutzen-Analyse für den Anwender. 62
D. Fehlende Rentabilität von Zertifizierungsdiensten 63
E. Rechtliche Grundlagen 64
1. Rechtssicherheit 64
2. Überregulierung 64
F. Angst vor Überwachung 65
G. Fehlende Sensibilisierung für Sicherheitsprobleme 65
H. Zusammenfassung 66
III. Vorteile einer offenen Sicherungsinfrastruktur 66
A. Fragestellung 66
B. Vorteile für kleine und mittlere Unternehmen. 66
C. Vorteile für den Behördenverkehr 67
IV. Lösungsmöglichkeiten 68
A. Private Initiativen. 68
B. Staatliche Beteiligung an Zertifizierungsdiensten 68

2. Teil: Regelungsbereiche und internationaler Überblick 71

§6 Regelungsbereiche und -modelle 73
I. Fragestellung. 73
II. Anerkennung der elektronischen Signatur 73
A. Begriff 73
B. Materiellrechtliche Anerkennung 73
1. Regelungsbedarf. 73
2. Regelungsmodelle 74
3. Gewillkürte Form insbesondere 75
C. Prozessuale Anerkennung 75
1. Regelungsbedarf. 75
2. Regelungsmodelle 75
III. Beweisregeln. 76
A. Regelungsbedarf 76
B. Regelungsmodelle 76
IV. Sicherungsinfrastruktur. 77
A. Regelungsbedarf 77
B. Regelungsmodelle 77
1. Sicherungsinfrastruktur und Anerkennung der Signaturen 77
a) Ex-ante- und ex-post-Ansatz. 77
aa) Allgemeines 77
bb) Anerkennung der Zertifizierungsdiensteanbieter. 78
cc) Anerkennung von Verfahren und Komponenten 79
dd) Zuständigkeit zur Prüfung 79
ee) Bindung der Gerichte an die ex-ante-Prüfung 79

ff) Kombination von ex-post- und ex-ante-Ansatz 80
b) Funktionaler und technikrechtlicher Ansatz 80
aa) Begriffe 80
bb) Abstraktionsgrad 81
c) Wirtschaftliche Sichtweise 82
aa) Marktwirtschaftlicher und technikrechtlicher Ansatz . 82
bb) Technologieneutralität insbesondere 82
d) Zusammenfassung 83
2. Beweisregeln 84
3. Internationale Aspekte 84
V. Risikoverteilung und Haftungsordnung 85
VI. Öffentliches Recht und Strafrecht 86

§7 Einige wichtige ausländische Regelungen im Überblick 87
I. Gang der Darstellung 87
II. UNCITRAL 87
A. Einführung 87
B. Model Law on Electronic Commerce 88
C. Model Law on Electronic Signatures 89
1. Entstehung 89
2. Überblick über die Regelung 90
a) Allgemeines 90
b) Anwendungsbereich 90
c) Definitionen 90
d) Technologieneutralität 90
e) Auslegung 91
f) Parteiautonomie 91
g) Anerkennung und Echtheitsvermutung 91
h) Pflichten der Beteiligten 92
i) Internationale materiellrechtliche Anerkennung 93
III. EU-Richtlinienrecht 94
A. Überblick und Gang der Darstellung 94
B. Fernabsatzrichtlinie 95
1. Überblick 95
2. Ausnahmen vom Anwendungsbereich 96
C. Richtlinienentwurf zum Fernabsatz von Finanzdienstleistungen 96
D. E-Commerce-Richtlinie 97
1. Allgemeines 97
2. Dienste der Informationsgesellschaft 97
3. Elektronischer Vertragsabschluss 98
a) Enabling principle 98
b) Ausnahmen 98
E. Signaturrichtlinie 99

1. Allgemeines 99
2. Anwendungsbereich 99
3. Zertifizierungsdiensteanbieter 100
a) Keine Bewilligungspflicht. 100
b) Freiwillige Akkreditierung 101
4. Anerkennung der elektronischen Signatur 102
a) Überblick. 102
b) (Einfache) elektronische Signatur 103
aa) Definition 103
bb) Rechtswirkung 103
c) Fortgeschrittene elektronische Signatur 104
aa) Definition 104
bb) Rechtswirkung 105
d) Qualifizierte elektronische Signatur 105
aa) Definition 105
bb) Rechtswirkung 106
e) Qualifizierte Signatur mit Anbieterakkreditierung 107
5. Haftung der Zertifizierungsdiensteanbieter 107
6. Gemeinschaftsweite Anerkennung. 108
7. Internationale Anerkennung. 108
8. Datenschutz 108
IV. Deutschland. 109
A. Signaturgesetz 1997. 109
1. Allgemeines 109
2. Regelungsbereich und -modell. 109
3. Vorgezogener Anscheinsbeweis. 110
4. Praxis 111
B. Signaturgesetz 2001. 111
1. Regelungsbereich 111
2. Neue Definitionen 112
3. Sicherungsinfrastruktur 112
a) Zertifizierungsdiensteanbieter. 112
aa) Begriff 112
bb) Überwachungssystem und Meldepflicht 113
cc) Freiwillige Akkreditierung. 113
dd) Internationale Aspekte 114
ee) Anerkennung von Prüf- und Bestätigungsstellen. . . . 115
b) Qualifizierte Zertifikate. 115
aa) Allgemeines 115
bb) Dokumentation der Ausstellung. 115
cc) Sperrung. 115
dd) Attribute 116
c) Unterrichtungspflichten gegenüber dem Antragsteller . . . 116

d) Zeitstempel 116
4. Beweisrecht 117
5. Haftungsregelung 117
C. Formanpassungsgesetz 118
1. Regelungsbereich 118
2. Materiellrechtliche Aspekte 118
a) Regelungsmodell 118
b) Elektronische Form 119
c) Textform 120
d) Einheit der Vertragsurkunde 121
e) Teilnahme an der elektronischen Kommunikation 121
f) Gewillkürte Schriftform 121
g) Gewillkürte elektronische Form 121
3. Prozessuale Aspekte 122
a) Besonderheiten des deutschen Urkundenbeweises 122
b) Beweiserleichterung 123
aa) Begründung und Regelungsmodell 123
bb) Tatbestandsmerkmale des § 292a ZPO 124
cc) Bedeutung der Anbieterakkreditierung 124
c) Prozessuale Anerkennung? 124
d) Aktenverkehr mit Gerichten 125

3. Teil: Regelung im schweizerischen Recht 127

§8 Einleitung 129
I. Gang der Darstellung des dritten Teils 129
II. Gesetzgebung zur elektronischen Signatur 130
A. Anfänge 130
B. Zertifizierungsdiensteverordnung 131
C. ZertES 132
1. Entwicklung 132
2. Ziele und Mittel 133
III. Gesetzgebung in benachbarten Rechtsgebieten 134
A. Bundesgesetz über den elektronischen Geschäftsverkehr 134
1. Überblick 134
2. Fernabsatzverträge insbesondere 135
a) Allgemeines 135
b) Geltungsbereich der Art. 40b ff. VE-OR 135
c) Begriff des Fernabsatzvertrages 136
d) Widerrufsrecht für Fernabsatzverträge 136
B. Totalrevision der Bundesrechtspflege 137
1. Überblick 137
2. Elektronischer Rechtsverkehr insbesondere 137

§9 Sicherungsinfrastruktur 139
I. Regelungsmodell. 139
II. Überblick über die Regelung 140
A. Arten elektronischer Signaturen 140
B. Signatur- und Signaturprüfschlüssel 140
C. Zertifizierungsdiensteanbieter 141
1. Begriffe. 141
2. Akkreditierung, Anerkennung und Zertifizierung 141
3. Anerkennung ausländischer Anbieter. 143
4. Aufsicht 143
5. Pflichten der Anbieter qualifizierter Zertifikate 144
6. Beteiligung des Bundes 144
D. Qualifizierte Zertifikate 145
1. Definition und Inhalt 145
2. Keine Attributzertifikate. 146
E. Erzeugen und Prüfen von Signaturen 146
1. Signaturerstellungseinheit 146
2. Signaturprüfeinheit 147
3. Ausführungsbestimmungen 147
F. Haftung 147
1. Zertifizierungsdiensteanbieter 147
a) Allgemeines. 147
b) Kreis der Haftpflichtigen. 148
c) Milde Kausalhaftung mit Beweislastumkehr 148
d) Haftungsbeschränkungen 148
2. Anerkennungsstellen 149
3. Verjährung 149
G. Sanktionen 149

§10 Beweisrecht und Haftungsfragen 150
I. Fragestellung und Vorgehen 150
II. Beweisrechtliche Grundlagen 151
A. Ziel und Gegenstand des Beweises 151
B. Beweislast 151
C. Beweismass 152
1. Allgemeines 152
2. Gesetzliche Reduktion des Beweismasses 153
3. Zulässigkeit einer vertraglichen Beweismassreduktion 153
D. Mittelbarer und unmittelbarer Beweis 153
1. Begriffe. 153
2. Erfahrungssätze und Induktionsschlüsse 154
3. Vermutungen 155
a) Tatsächliche Vermutung 155

aa) Definition 155
bb) Beweiswürdigung und Beweisführungslast 155
cc) Beweismass. 155
dd) Widerlegung der tatsächlichen Vermutung 156
b) Gesetzliche Vermutung 156
aa) Begriff. 156
bb) Ohne Vermutungsbasis. 156
cc) Glaubhaft zu machende Vermutungsbasis 157
dd) Voll zu beweisende Vermutungsbasis 157
ee) Widerlegung 157
4. Anscheinsbeweis. 157
a) Ausgangslage. 157
b) Kasuistik 158
aa) Schiffskollisions-Fall 158
bb) Auffahrunfall-Fall. 159
cc) Arzthaftpflicht-Fall. 159
dd) Unfallversicherung 159
ee) Einschreibebrief-Fall 159
ff) EFTPOS-Fall 160
c) Dogmatische Einordnung des Anscheinsbeweises 161
aa) Fragestellung. 161
bb) Beweislasttheorie 161
cc) «Rechtsbeweis» 162
dd) Beweiswürdigung oder Beweismass 162
ee) Materiellrechtliche Theorie 164
ff) Zusammenfassung 164
d) Voraussetzungen des Anscheinsbeweises 164
aa) Fragestellung. 164
bb) Mangel an Beweismitteln bei beiden Parteien 165
cc) Vereitelung des Vertrags- bzw. Gesetzeszwecks 165
dd) Zumutbare Massnahmen des Beweisführers 166
ee) Beweismass: Überwiegende Wahrscheinlichkeit. . . . 166
ff) Zusammenfassung 167
E. Urkundenbeweis. 168
1. Begriff der Urkunde 168
a) Urkundenbeweis im System der Beweismittel 168
b) Weiter und enger Urkundenbegriff 168
c) Öffentliche und private Urkunden 169
d) Zivil- und strafrechtlicher Urkundenbegriff 169
e) Elektronisch gespeicherte Dokumente insbesondere. 169
2. Beweiskraft unterschriebener Papierurkunden 170
a) Beweis der Abgabe einer Unterschrift. 170
aa) Unterschriftenfälschung 170

bb) Urkundenverfälschungen 171
cc) Schriftverstellung 172
dd) Urkundenbeweis als Anscheinsbeweis 172
b) Beweis der Rekognition 173
3. Beweiskraft nicht unterzeichneter Urkunden 174
a) Nicht unterzeichnete Papierdokumente 174
b) Kopien und Scans 174
c) Telefax 174
d) Elektronisch gespeicherte Dokumente 175
e) Aufzeichnungen von Geschäftsbüchern 175
f) Zusammenfassung 175
4. Privilegierung der Urkunde als Beweismittel 176
a) Allgemeines 176
b) Provisorische Rechtsöffnung insbesondere 176
III. Beweisrecht und Haftungsfragen elektronisch signierter Dokumente . . 177
A. Echtheit 177
1. Allgemeines 177
a) Problemstellung 177
b) Fallgruppen 178
c) Darzulegende Indizienkette 178
2. Anscheinsbeweis für elektronische Signaturen 178
a) Voraussetzungen des Anscheinsbeweises 178
b) Symptomatischer Mangel an Beweismitteln 179
c) Vereitelung des Gesetzes- bzw. Vertragszwecks 179
d) Massnahmen zur Beweissicherung 180
e) Zusammenfassung 180
3. Bedeutung der ex-ante-Prüfung für das Gericht 180
a) Regelungsmodelle 180
b) Regelungvorschlag des Entwurfs 181
c) Interpretationsvorschlag 181
aa) Zweck der ex-ante-Prüfung 181
bb) Tatsächliche Vermutung der Echtheit? 181
cc) Beweismassreduktion 182
4. Signaturen ohne ex-ante-Prüfung und Rahmenvertrag 182
a) Anwendungsfälle 182
b) Beweisführung 182
c) Haftung des Signierschlüsselhalters 183
aa) Fragestellung 183
bb) Vertragliche Haftung zugunsten Dritter 183
cc) Haftung aus Stellvertretungsrecht 184
dd) Vertrauenshaftung 184
ee) Haftungserklärung des Schlüsselhalters 185
ff) Haftung aus Art. 59a E-OR? 186

d) Zusammenfassung 186
5. Signaturen ohne ex-ante-Prüfung mit Rahmenvertrag 187
a) Anwendungsfälle 187
b) Exkurs: Legitimationsmittel im Bankgeschäft. 187
aa) Vorbemerkung 187
bb) Girovertrag 187
cc) Rechtliche Natur des Überweisungsauftrages 188
dd) Dispositive Legitimationsordnung 188
ee) Parteiautonome Legitimationsordnung. 190
ff) Aufklärungs- und Sorgfaltspflichten 191
c) Beweisführung mittels elektronischer Signatur 191
aa) Parteiautonome Legitimationsordnung. 191
bb) Elektronische Signatur zur Legitimation 192
cc) Signatur für einzelne Transaktionsbefehle 192
dd) Reduzierte Sicherheitsanforderungen. 192
d) Haftungsfragen. 193
aa) Haftung des Anbieters für Aufklärung 193
bb) Haftung des Anbieters bei der Systemauswahl 193
cc) Haftung des Signierschlüsselhalters 194
6. Signaturen mit ex-ante-Prüfung ohne Rahmenvertrag 195
a) Anwendungsfälle 195
b) Beweisführung 195
aa) Basis des Anscheinsbeweises 195
bb) Zumutbare Massnahmen des Beweisführers 197
cc) Zusammenfassung: Darzulegende Indizien 198
dd) Widerlegung des Anscheinsbeweises. 198
c) Haftung des Signierschlüsselhalters 198
aa) Art. 59a E-OR. 198
bb) Überprüfung der Gültigkeit des Zertifikats 200
cc) Überprüfung des Inhalts des Zertifikats 200
7. Signaturen mit ex-ante-Prüfung und Rahmenvertrag 201
a) Anwendungsfälle 201
b) Beweisführung 201
c) Haftungsfragen. 201
aa) Haftung des Systembetreibers 201
bb) Haftung des Schlüsselhalters 201
B. Rekognition 202

§11 Prozessuale Anerkennung. 203
I. Fragestellung 203
II. Beweis mittels digitaler Signatur de lege lata 203
A. Fragestellung 203
B. Elektronische Einreichung 204

C. Einreichung in ausgedruckter Form 204
D. Einsatz als provisorischer Rechtsöffnungstitel 205
III. Beweis mittels digitaler Signatur de lege ferenda 205
A. Allgemeines 205
B. Formatproblem 206
C. Fehlende Auslastung der Prüfinfrastruktur 206
D. Konformitätsbestätigung als Lösungsvorschlag 206
1. Konzept 206
2. Konformitätsbestätigung als beglaubigte Kopie 207
3. Konformitätsbestätigung als Aufgabe der Kantone 208
E. Zusammenfassung 208
IV. Elektronische Signatur als hochtechnisches Beweismittel 209

§12 Materiellrechtliche Anerkennung 210
I. Fragestellung und Vorgehen 210
II. Materiellrechtliche Formvorschriften 210
A. Grundlagen 210
1. Grundsatz der Formfreiheit 210
2. Gesetzliche Formvorschriften 211
a) Gültigkeitsform 211
b) Beweisform 211
c) Formungültigkeit 211
3. Gewillkürte Formvorschriften 213
a) Allgemeines 213
b) Arten 213
c) Rechtsfolgen 213
B. Das schweizerische System der Formvorschriften 214
1. Überblick 214
2. Einfache Schriftlichkeit 214
a) Verurkundung 214
b) Unterschrift 214
aa) Formelles Element 214
bb) Materielles Element 215
3. Textform 216
a) Allgemeines 216
b) Textform im VE-BGEG insbesondere 217
4. Qualifizierte Schriftlichkeit 217
5. Beglaubigung von Unterschrift oder Handzeichen 217
6. Öffentliche Beurkundung 218
7. Qualifizierte Formen der öffentlichen Beurkundung 218
8. Sonderformen 219
C. Formzwecke und ihre Erfüllung durch elektronische Signaturen . . 219
1. Funktionale Äquivalenz 219

2. Rekognition 220
a) Vorbemerkung: Willenserklärungen 220
b) Begriff der Rekognition 220
c) Rekognition durch Handunterschrift 220
d) Rekognition durch elektronische Signatur 221
aa) (Einfache) elektronische Signatur 221
bb) Qualifizierte elektronische Signatur 222
e) Zusammenfassung 222
3. Beweis (Identität, Integrität) 222
a) Allgemeines 222
b) Einfache elektronische Signatur 223
c) Qualifizierte elektronische Signatur 223
d) Zusammenfassung 224
4. Übereilungsschutz 225
a) Allgemeines 225
b) Zeitliche Verzögerung 225
c) Verkehrsübung 226
d) Zusammenfassung 226
5. Dokumentenabschluss 227
6. Verhandlungsabschluss 227
7. Kontrolle 228
8. Perpetuierung 229
9. Inhaltsklarheit 230
10. Information 230
11. Zusammenfassung 230
III. Materiellrechtliche Anerkennung de lege lata 231
A. Fragestellung 231
B. Analoge Anwendung des Begriffs der Handunterschrift 231
C. Elektronische Signatur als Faksimile-Unterschrift 232
D. Elektronische Signatur als beglaubigtes Handzeichen 233
E. Fazit 233
IV. Materiellrechtliche Anerkennung de lege ferenda 233
A. Fragestellung 233
B. Art. 14 Abs. 2bis E-OR 234
1. Allgemeines 234
2. Tatbestand 234
a) Anwendungsbereich 234
b) Signaturprüfung 234
c) Qualifizierte elektronische Signatur 235
aa) Qualifiziertes Zertifikat 235
bb) Gültigkeit zum Signierzeitpunkt 235
cc) Fortgeschrittene elektronische Signatur 236
dd) Sichere Signiereinheit 236

d) Anbieteranerkennung 236
e) Name einer natürlichen Person 237
f) Beweis insbesondere 237
aa) Überprüfung durch das Gericht selbst 237
bb) Überprüfung mittels Gutachten 239
3. Rechtsfolge 239
C. Alternativen zu Ausnahmebestimmungen 240
1. Widerrufsrecht 240
2. Textform 240
3. Öffentliche Beurkundung 240
D. Wertung des bundesrätlichen Vorschlags 241
1. Übereilungsschutz jenseits von Fernabsatzverträgen 241
2. Unsichere Inkraftsetzung des Bundesgesetzes über den elektronischen Geschäftsverkehr 242
3. Ergebnis: Forderung nach Ausnahmebestimmungen 242
V. Einheit der Urkunde 242
VI. Aspekte der gewillkürten Form 243

§13 Zusammenfassung der Ergebnisse 244
I. Sicherungsinfrastruktur 244
II. Beweiswert elektronischer Signaturen 244
A. Problematik 244
B. Anscheinsbeweis 245
C. Anwendung auf elektronische Signaturen 246
1. Offene Benutzergruppen 246
2. Geschlossene Benutzergruppen 246
3. Widerlegung des Anscheinsbeweises 246
D. Bedeutung der ex-ante-Prüfung insbesondere 247
E. Nachzuweisende Indizien 247
1. Signaturen ohne Rahmenvertrag 247
a) Signaturen ohne Anbieteranerkennung 247
aa) Einfache elektronische Signaturen 247
bb) Qualifizierte elektronische Signaturen 247
b) Signaturen mit Anbieteranerkennung 248
2. Signaturen mit Rahmenvertrag 248
III. Haftungsfragen 249
A. Offene Benutzergruppen 249
1. Situation de lege lata 249
2. Situation de lege ferenda: Art. 59a E-OR 249
B. Geschlossene Benutzergruppen 249
C. Haftung der Zertifizierungsdiensteanbieter 250
IV. Prozessuale Anerkennung 250
V. Materiellrechtliche Anerkennung 251

A. Allgemeines 251
B. Kritik am bundesrätlichen Regelungsvorschlag. 251
C. Voraussetzungen des Art. 14 Abs 2bis E-OR 251

Stichwortverzeichnis 253

Abkürzungsverzeichnis

A.	Auflage
a.a.O.	am angeführten Ort
a.E.	am Ende
a.M.	anderer Meinung
AB	Amtliches Bulletin (NR: Nationalrat, SR: Ständerat)
ABl.	Amtsblatt der Europäischen Gemeinschaften, http://europa.eu.int/eur-lex/de/search/search_lif.html
Abs.	Absatz
AcP	Archiv für die civilistische Praxis (Tübingen)
AGB	Allgemeine Geschäftsbedingungen
AJP	Aktuelle Juristische Praxis (Lachen)
Anh	Anhang
Art.	Artikel
BAKOM	Bundesamt für Kommunikation
BBl	Bundesblatt, http://www.admin.ch/ch/d/ff/
Bd.	Band
BGB	Bürgerliches Gesetzbuch für das Deutsche Reich vom 18. August 1896
BGBl.	(deutsches) Bundesgesetzblatt, http://www.bundesanzeiger.de/bgbl1.htm
BGE	Entscheidungen des schweizerischen Bundesgerichts, http://www.bger.ch
BGEG	Bundesgesetz über den elektronischen Geschäftsverkehr (Teilrevisionen des Obligationenrechts und des Bundesgesetzes gegen den unlauteren Wettbewerb)
BGES	Bundesgesetz über die elektronische Signatur (neu ZertES)
BGHZ	(deutscher) Bundesgerichtshof in Zivilsachen
BJ	Bundesamt für Justiz
BJM	Basler Juristische Mitteilungen (Basel)
BK	Berner Kommentar
BlSchK	Blätter für Schuldbetreibung und Konkurs (Wädenswil)
Bst.	Buchstabe
BT-Drs.	Bundestagsdrucksache, http://dip.bundestag.de/parfors/parfors.htm
c't	c't Magazin für Computertechnik (Hannover), abrufbar gegen Entgelt unter http://www.heise.de/kiosk
CA	Certification Authority (=ZDA)
CPS	Certification Practice Statement
CR	Computer und Recht (München)
CRi	Computer und Recht international (München)
CRL	Certificate Revocation List
DES	Data Encryption Standard
Digma	Zeitschrift für Datenrecht und Informationssicherheit (Zürich)
Diss.	Dissertation
DNotZ	Deutsche Notar-Zeitschrift (Köln)
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992, SR 235.1
DuD	Datenschutz und Datensicherheit (Wiesbaden)

E	Entwurf
EBPP	Electronic Bill Presentment and Payment
EDI	Electronic Document Interchange
EDIFACT	Electronic Document Interchange for Administration, Commerce & Transport
EDV	Elektronische Datenverarbeitung
EFD	Eidgenössisches Finanzdepartement
EFTPOS	Electronic Funds Transfer at the Point of Sale, elektronische Zahlungsabwicklung am Verkaufspunkt
EG	Europäische Gemeinschaften
EJPD	Eidgenössisches Justiz- und Polizeidepartement
et al.	et alii (und andere)
EU	Europäische Union
f./ff.	und folgende
Fakten	Fakten: Die Zeitschrift für Datenschutz des Kantons Zürich (Zürich)
FMG	Fernmeldegesetz vom 30. April 1997, SR 784.10
FN	Fussnote
FormanpassungsG	(deutsches) Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, BGBl. I S. 1542 ff.
FTP	File Transfer Protocol
GestG	Bundesgesetz über den Gerichtsstand in Zivilsachen vom 24. März 2000, SR 272
GlG	Bundesgesetz über die Gleichstellung von Mann und Frau vom 24. März 1995, SR 151.1
Hrsg.	Herausgeber
HTML	Hypertext Markup Language
IETF	Internet Engineering Task Force
IMC	Internet Mail Consortium
i. S.	in Sachen
i. S. v.	im Sinne von
IP	Internet Protocol
IPRG	Bundesgesetz über das Internationale Privatrecht vom 18. Dezember 1987, SR 291
ITU	Internationale Fernmeldeunion
IuKDG	(deutsches) Gesetz zur Regelung der Rahmenbedingungen für Information- und Kommunikationsdienste, BGBl. I S. 1870 ff.
iX	iX Magazin für professionelle Informationstechnik (Hannover), abrufbar gegen Entgelt unter http://www.heise.de/kiosk
Jusletter	Jusletter (Bern), http://www.jusletter.ch
K&R	Kommunikation und Recht (Heidelberg)
KassGer	Kassationsgericht
KIG	Koordinationsgruppe Informationsgesellschaft
KKG	Bundesgesetz über den Konsumkredit vom 8. Oktober 1993, SR 221.214.1
KMU	Kleine und mittlere Unternehmen

KOM	Dokument der Europäischen Kommission, http://europa.eu.int/eur-lex/de/search/search_lip.html
LDAP	Lightweight Directory Access Protocol
LG	Landgericht
LGVE	Luzerner Gerichts- und Verwaltungsentscheide
LugÜ	Übereinkommen über die gerichtliche Zuständigkeit und die Vollstreckung gerichtlicher Entscheidungen in Zivil- und Handelssachen vom 16. September 1988, SR 0.275.11
m.H.	mit Hinweisen
MDR	Monatsschrift für deutsches Recht (Köln)
MIME	Multipurpose Internet Mail Extensions
MLEC	UNCITRAL Model Law on Electronic Commerce
MLES	UNCITRAL Model Law on Electronic Signatures
MMR	Multimedia und Recht (München)
MWSTG	Bundesgesetz über die Mehrwertsteuer vom 2. September 1999, SR 641.20
N	Note
NJW	Neue Juristische Wochenschrift (München/Frankfurt am Main)
NJW-CoR	Neue Juristische Wochenschrift-Computerreport (München)
Nr.	Nummer
NZZ	Neue Zürcher Zeitung (Zürich), abrufbar gegen Entgelt unter http://www.nzz.ch/gbiarchiv
OCSP	Online Certificate Status Protocol
OGer	Obergericht
OLG	Oberlandesgericht
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911, SR 220
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PIN	Persönliche Identifikationsnummer
PKCS	RSA Public Key Cryptography Standards
PKI	Public-Key-Infrastruktur, Sicherungsinfrastruktur
RA	Registration Authority (Registrierstelle)
recht	recht, Zeitschrift für Juristische Ausbildung und Praxis (Bern)
RegTP	(deutsche) Regulierungsstelle für Telekommunikation und Post
RSA	Verschlüsselungs- und Signieralgorithmus nach RIVEST, SHAMIR und ADLEMAN
Rz	Randziffer
S.	Seite
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAG	Schweizerische Aktiengesellschaft (Zürich)
sc.	scilicet; zu verstehen als
SchKG	Bundesgesetz über Schuldbetreibung und Konkurs vom 11. April 1889, SR 281.1
SchlT	Schlusstitel des ZGB
SET	Secure Electronic Transaction
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht (Zürich)

SigG 97	(deutsches) Signaturgesetz 1997 (in Art. 3 IuKDG)
SigG 01	(deutsches) Gesetz über Rahmenbedingungen für elektronische Signaturen 2001, BGBl. I S. 876 ff.
SigV 97	(deutsche) Signaturverordnung 1997, BGBl. 1997 I S. 2498 ff.
SigV 01	(deutsche) Signaturverordnung 2001, BGBl. I S. 3074 ff.
SigI	Signatur-Interoperabilitätsspezifikation
SIM	Subscriber Identification Module
SJZ	Schweizerische Juristen Zeitung (Zürich)
SOG	Solothurnische Gerichtspraxis
SR	Systematische Sammlung des Bundesrechts, http://www.admin.ch/ch/d/sr/sr.html
SSL	Secure Socket Layer
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0
TAN	Transaktionsnummer
TCP/IP	Transaction Control Program/Internet Protocol
Telepolis	Telepolis, Magazin der Netzkultur (Hannover)
THG	Bundesgesetz über die technischen Handelshemmnisse vom 6. Oktober 1995, SR 946.51
ULR/RDU	Uniform Law Review/Revue de Droit Uniforme (Rom)
UMTS	Universal Mobile Telecommunications System
UNCITRAL	United Nations Commission on International Trade Law
USB	Universal Serial Bus
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
UWG	Bundesgesetz gegen den unlauteren Wettbewerb vom 19. Dezember 1986, SR 241
VersR	Versicherungsrecht (Karlsruhe)
VE	Vorentwurf (Vernehmlassungsvorlage)
VPB	Verwaltungspraxis des Bundes, http://www.vpb .admin.ch
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WM	Wertpapier-Mitteilungen, Zeitschrift für Wirtschafts- und Bankrecht (Frankfurt a. M.)
WWW	World Wide Web
ZBGR	Schweizerische Zeitschrift für Beurkundungs- und Grundbuchrecht (Zürich)
ZBJV	Zeitschrift des bernischen Juristenvereins (Bern)
ZDA	Zertifizierungsdiensteanbieter
ZertDV	Verordnung über die Dienste der elektronischen Zertifizierung vom 12. April 2000, SR 784.103
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ehemals BGES)
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, SR 210
Ziff.	Ziffer
ZK	Zürcher Kommentar
ZKA	Zentraler Kredit-Ausschuss der Spitzenverbände des deutschen Kreditgewerbes
ZPO	Zivilprozessordnung

ZR	Blätter für Zürcherische Rechtsprechung (Zürich)
ZSR	Zeitschrift für Schweizerisches Recht (Basel)

Literaturverzeichnis

ALBRECHT Andreas (Signatur), Ist die elektronische Signatur untauglich?, Plädoyer 4/2001, 29

ALBRECHT Astrid (Biometrie), Biometrie zum Nutzen für Verbraucher?, Kriterien der Verbraucherfreundlichkeit biometrischer Verfahren, DuD 6/2000, 332 ff.

ALLENSTEIN Petra, Signaturgesetz und Signaturverordnung, Eine erste Einführung, in: HOEREN Thomas/SCHÜNGEL Martin (Hrsg.), Rechtsfragen der digitalen Signatur, Eine Einführung in Recht und Praxis der Zertifizierungsstellen, Berlin 1999, 15 ff.

ALTMANN Ralph, Herausforderer, Sechs Homebanking-Programme gegen Quicken im Test, c't 17/2001, 96 ff.

AMERICAN BAR ASSOCIATION (ABA), Digital Signature Guidelines, Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, August 1, 1996, http://www.abanet.org/scitech/ec/isc/digital_signature.html

AMONN Kurt/GASSER Dominik, Grundriss des Schuldbetreibungs- und Konkursrechts, 6. A. Bern 1997

BAKER & MCKENZIE, European Union Directive Country-by-Country Comparison Table, http://www.bmck.com/ecommerce/directive compindex.htm

BAUMANN Max/DÜRR David/LIEBER Viktor/MARTI Arnold/SCHNYDER Bernhard (ZK-BAUMANN/DÜRR/LIEBER/MARTY/SCHNYDER), Zürcher Kommentar zum Zivilgesetzbuch, 1. Teilband, Einleitung, Art. 1-7 ZGB, 3. A. Zürich 1998

BAUMBACH Adolf/LAUTERBACH Wolfgang/ALBERS Jan/HARTMANN Peter, Zivilprozessordnung, mit Gerichtsverfassungsgesetz und anderen Nebengesetzen, 59. A. München 2001

BECKER Hermann (BK-BECKER), Berner Kommentar zum Obligationenrecht, I. Abteilung, Allgemeine Bestimmungen, Art. 1-183 OR, Bern 1941

BEHRENS Michael/ROTH Richard, Sind wir zu vermessen, die PIN zu vergessen?, Erfahrungen aus einem Feldversuch, DuD 6/2000, 327 ff.

BETSCH Andreas/DEWITZ Karsten, Absperrung, Prüfung von Zertifikaten in Public-Key-Infrastrukturen, iX 6/2001, 162 ff.

BETSCHON Stephan (Nacht), Die Nacht der langen Schlüssel, Auf der Suche nach einer neuen Swisskey, NZZ Nr. 119, 25. Mai 2001, 88

BETSCHON Stephan (Identitäten), Digitale Identitäten für die Katz, Swisskey wird geschlossen, NZZ Nr. 108, 11. Mai 2001, 81

BIESER Wendelin, Das Gesetz zur digitalen Signatur: Der Umstieg vom «Papierdokument» zum «elektronischen Dokument», Fakten, Zeitschrift für Datenschutz des Kantons Zürich, 3/1997, 30 ff.

BIESER Wendelin/KERSTEN Heinrich, Elektronisch unterschreiben, Die digitale Signatur in der Praxis, 2. A. Heidelberg 1999

BIGLER-EGGENBERGER Margrit/KAUFMANN Claudia (Hrsg.; GlG-[Autor]), Kommentar zum Gleichstellungsgesetz, Basel 1997

BIRCHER Marcel, Zum sog. «Bundesgesetz über den elektronischen Geschäftsverkehr»: Die Revisionsbestrebungen des Bundesrates für OR und UWG, Diskussionsveranstaltung vom 22. Mai 2001, sic! 5/2001, 467 ff.

BITZER Frank/BRISCH Klaus M., Digitale Signatur, Grundlagen, Funktion und Einsatz, Berlin/Heidelberg 1999

BIZER Johann, Das Schriftformprinzip im Rahmen rechtsverbindlicher Telekooperation, DuD 4/1992, 169 ff.

BIZER Johann/HAMMER Volker, Elektronisch signierte Dokumente als Beweismittel, DuD 11/1993, 619 ff.

BIZER Johann/HERDA Siegfried, Kriterien zur Gewährleistung eines ausreichenden Beweiswertes digital signierter Dokumente im elektronischen Rechtsverkehr, in: HORSTER Patrick (Hrsg.), Digitale Signaturen – Grundlagen, Realisierungen, Rechtliche Aspekte, Anwendungen, Braunschweig/Wiesbaden 1996, 19 ff.

BIZER Johann/MIEDBRODT Anja, Die digitale Signatur im elektronischen Rechtsverkehr, Deutsches Signaturgesetz und Entwurf der Europäischen Richtlinie, in: KRÖGER Detlef/GIMMY, Marc A. (Hrsg.), Handbuch zum Internetrecht, Electronic Commerce – Informations-, Kommunikations- und Mediendienste, Berlin u.a. 2000, 135 ff.

BJ FACHSTELLE FÜR RECHTSINFORMATIK UND INFORMATIKRECHT (BJ, Projektskizze GovLink), Projektskizze, GovLink Framework, Ein Fundament für Electronic Government, GovLink Pilotanwendungen, Elektronischer Rechtsverkehr auf der Basis von GovLink, Version 1.0a, 26. Mai 2000, http://www.bj.admin.ch/themen/ri-ir/govlink/govlink10.pdf[1]

BLUM Felix (Entwurf), Entwurf eines neuen Signaturgesetzes, DuD 2/2001, 71 ff.

BLUM Felix (UNCITRAL), Das UNCITRAL-Modellgesetz zu elektronischen Signaturen, K&R 2/2000, 63 ff.

BRISCH, Klaus M. (Textform), Computer und Recht aktuell, Textform und elektronische Form, CR 8/1999, 537f.

BRISCH Klaus M. (Rahmenbedingungen), Gemeinsame Rahmenbedingungen für elektronische Signaturen, Richtlinienvorschlag der Europäischen Kommission, CR 8/1998, 492 ff.

BRITZ Jörg W., Urkundenbeweisrecht und Elektroniktechnologie, Eine Studie zur Tauglichkeit gesetzlicher Beweisregeln für elektronische Dokumente und ihre Reproduktionen im Zivilprozess, Schriftenreihe Recht der Computerpraxi, Bd. 4, München 1997

BRÜCKNER Christian, Schweizerisches Beurkundungsrecht, Zürich 1993

BRUNNER Alexander, Die Anwendung neuer Informations und Kommunikationstechniken im Zivilprozess und anderen Verfahren, Bibliothek zur Zeitschrift für Schweizerisches Recht/Beiheft 33, Basel/Genf/München 2000

BUCHER Eugen (Belastung), Wie lange noch Belastung des Kunden mit den Fälschungsrisiken im Bankverkehr?, Ein weiteres Mal Bemerkungen zu den AGB der Banken, recht 2/1997, 41 ff.

BUCHER Eugen (Wer haftet), Wer haftet wem?, Zum Problem der Tragung des Risikos betrügerisch veranlasster Bankvergütungen, recht 1984, 97 ff.

BUCHER Eugen (OR AT), Schweizerisches Obligationenrecht, Allgemeiner Teil ohne Deliktsrecht, Zürich 1979

[1] Internetadressen letztmals überprüft am 17. Januar 2002.

BÜHLER Alfred, Die Beweiswürdigung, in: LEUENBERGER Christoph (Hrsg.), Der Beweis im Zivilprozess, Schriften der Stiftung für die Weiterbildung schweizerischer Richterinnen und Richter SWR, Bd. 1, Bern 2000, 71 ff.

BÜHLER Alfred/EDELMANN Andreas/KILLER Albert, Kommentar zur aargauischen Zivilprozessordnung, Zivilrechtspflegegesetz (Zivilprozessordnung, ZPO) vom 18. Dezember 1984, 2. A. Aarau/Frankfurt a.M./Salzburg 1998

BUIS Eric (Überweisungsaufträge), Falsche Überweisungsaufträge – wer haftet?, Der Kontoinhaber trägt immer ein Risiko, NZZ Nr. 202, 1./2. September 2001, 25 = Jusletter 17. September 2001

BUIS Eric (Banküberweisung), Die Banküberweisung und der Bereicherungsausgleich bei fehlgeschlagenen Banküberweisungen, Schweizer Schriften zum Bankrecht, Bd. 63, Zürich 2000 = Diss. Zürich 2001

BÜLLESBACH Alfred/RIESS Joachim/MIEDBRODT Anja, Digitale Signaturen zwischen Anwendung und Regulierung am Beispiel der Situation in Europa, Japan und in den Vereinigten Staaten von Amerika, in: GEIS Ivo (Hrsg.), Die digitale Signatur – eine Sicherheitstechnik für die Informationsgesellschaft, Ein Leitfaden für Anwender und Entscheider, Eschborn 2000, 1 ff.

BÜLLINGEN Franz/HILLEBRAND Annette, Biometrie als Teil der Sicherungsinfrastruktur?, DuD 6/2000, 339 ff.

BÜTTIKER Daniel, Swisscert, http://www.swisscert.com/technology/SwissCERTwithBusinessCase.pdf

BV-[Autor]: AUBERT Jean-François/EICHENBERGER Kurt/MÜLLER Jörg Paul/RHINOW René A./SCHINDLER Dietrich (Hrsg.), Kommentar zur Bundesverfassung der Schweizerischen Eidgenossenschaft vom 29. Mai 1874, Loseblatt, 4 Bde., Basel/Zürich/Bern 1986, 6. Lieferung 1996

DEVILLE Rainer/KALTHEGENER Regina, Wege zum Handelsverkehr mit elektronischer Unterschrift, NJW-CoR 3/1997, 168 ff.

DIERING Manja/SCHMEH Klaus, Zertifizierter Paragrafendschungel, Signaturgesetze in Europa, c't 13/2001, 182 f.

DONZALLAZ Yves, Commentaire de la loi fédérale sur les fors en matière civile, Bern 2001

EBBING Frank, Schriftform und E-Mail, CR 5/1996, 271 ff.

ELLISON Carl/SCHNEIER Bruce, Ten Risks of PKI, What You're not Being Told about Public Key Infrastructure, Computer Security Journal 1/2000, 1 ff., http://www.counterpane.com/pki-risks.pdf

EMCH Urs/RENZ Hugo/BÖSCH Franz, Das Schweizerische Bankgeschäft, Das praktische Lehrbuch und Nachschlagewerk, 5. A. Thun 1998

EMMERT Ulrich, Haftung der Zertifizierungsstellen, CR 4/1999, 244 ff.

ENGELS Gudrun, Der Anscheinsbeweis der Kausalität, Unter besonderer Berücksichtigung der neueren Rechtsprechung, Europäische Hochschulschriften, Reihe II Rechtswissenschaft, Bd. 1563, Frankfurt a.M. 1994

ERBER-FALLER Sigrun, Die «elektronische Unterschrift» im Rechtsverkehr, in: GLADE Albert/REIMER Helmut/STRUIF Bruno (Hrsg.), Digitale Signatur und sicherheitssensitive Anwendungen, Braunschweig/Wiesbaden 1995, 115 ff.

FARRELL Joseph/SALONER Garth, Competition, Compatibility and Standards: The Economics of Horses, Penguins and Lemmings, in: GABEL H. Landis (Hrsg.), Product Standardization and Competitive Strategy, Amsterdam u.a. 1987, 1 ff.

FOX Dirk (Cross-Zertifikat), Cross-Zertifikat, DuD 2/2001, 105

FOX Dirk (DES), Data Encryption Standard (DES), DuD 12/2000, 736

FOX Dirk (Problem), Zu einem prinzipiellen Problem digitaler Signaturen, DuD 7/1998, 386 ff.

FOX Dirk/MÜLLER Maik, Neue Zertifikate für asymmetrische Sicherheitsprotokolle, in: HORSTER Patrick (Hrsg.), Trust Center, Grundlagen, Rechtliche Aspekte, Standardisierung, Realisierung, Braunschweig/Wiesbaden 1995, 165 ff.

FRANK Richard/STRÄULI Hans/MESSMER Georg, Kommentar zur zürcherischen Zivilprozessordnung, Gesetz über den Zivilprozess vom 13. Juni 1976, 3. A. Zürich 1997

FREI Oliver, Der Abschluss von Konsumentenverträgen im Internet, Diss. Zürich 2001

FRITZSCHE Jörg/MALZER Hans M., Ausgewählte zivilrechtliche Probleme elektronisch signierter Willenserklärungen, DNotZ 1995, 3 ff.

GASSER Dominik, Rechtsöffnung im Cyberspace?, AJP 1/2001, 91 ff.

GAUCH Peter/SCHLUEP Walter R./SCHMID Jörg/REY Heinz (GAUCH/SCHLUEP/SCHMID: Bd. 1; GAUCH/SCHLUEP/REY: Bd. 2), Schweizerisches Obligationenrecht, Allgemeiner Teil, 2 Bde., 7. A. Zürich 1998

GEIS Ivo, Die elektronische Signatur: Eine internationale Architektur der Identifizierung im E-Commerce, MMR 11/2000, 667 ff.

GIESSMANN Ernst-Günter/SCHMITZ Roland, Zum Gültigkeitsmodell für elektronische Signaturen nach SigG und X.509, DuD 7/2000, 401 ff.

GIGER Hans (BK-GIGER), Berner Kommentar zum Obligationenrecht, Band VI, 2. Abteilung, 1. Teilband, 3. Abschnitt, Der Grundstückkauf, Art. 216-221 OR, Bern 1997

GIOVANOLI Silvio/SCHAETZLE Marc (BK-GIOVANOLI/SCHAETZLE), Berner Kommentar zum Obligationenrecht, 2. Abteilung 7. Teilband, Die Bürgschaft, Spiel und Wette, Art. 516-529 OR, Der Leibrentenvertrag und die Verpfründung, Art. 516-529 OR, 2. A. Bern 1978

GISLER Michael, Vertragsrechtliche Aspekte Elektronischer Märkte – nach schweizerischem Obligationenrecht, Diss. St.Gallen 1999

GlG-[Autor], s. BIGLER-EGGENBERGER/KAUFMANN

GMÜR Max/HAFTER Ernst (BK-GMÜR/HAFTER), Berner Kommentar zum Zivilgesetzbuch, Einleitung, Personenrecht, Art. 1-89 ZGB, 2. A. Bern 1919

GOLLMANN Dieter, Computer Security, Chinchester u.a. 1999

GRABER Christian, Wie weiter nach dem Swisskey-Aus?, Kritische Momentaufnahme aus erster Hand nach der Einstellung des Zertifizierungsdienstes durch die Swisskey, Digma 2/2001, 84 f.

GREGER Reinhard (Anscheinsbeweis), Praxis und Dogmatik des Anscheinsbeweises, VersR 45/1980, 1091 ff.

GREGER Reinhard (Beweis), Beweis und Wahrscheinlichkeit, Das Beweiskriterium im Allgemeinen und bei den sogenannten Beweiserleichterungen, Berlin 1978

GRIMM Rüdiger/FOX Dirk, Entwurf einer EU-Richtlinie zu Rahmenbedingungen «elektronischer Signaturen», DuD 7/1998, 407 ff.

GUGGENBÜHL Markus, Die gesetzlichen Vermutungen des Privatrechts und ihre Wirkungen im Zivilprozess, Zürcher Studien zum Privatrecht, Bd. 92, Zürich 1990 = Diss. Zürich 1990

GUGGENHEIM Daniel (Contrats), Les contrats de la pratique bancaire suisse, 4. A. Genf 2000

GUGGENHEIM Daniel (Verträge), Die Verträge der schweizerischen Bankpraxis, 3. A. Zürich 1986

GULDENER Max, Schweizerisches Zivilprozessrecht, 3. A. Zürich 1979

GUT Matthias/WILDHABER Bruno, Der Beweiswert von EDI-Meldungen, http://www.law-it.ch/artikel/online/gut-wi.htm

HABSCHEID Walter, Schweizerisches Zivilprozess- und Gerichtsorganisationsrecht, Ein Lehrbuch seiner Grundlagen, 2. A. Basel 1990

HAMMER Volker, Signaturprüfungen nach SigI, DuD 2/2000, 96 ff.

HAMMER Volker/BIZER Johann, Beweiswert elektronisch signierter Dokumente, DuD 12/1993, 689 ff.

HÄRTING Niko, Der dauerhafte Datenträger, K&R 6/2001, 310 ff.

HELDRICH Karl, Die Form des Vertrages, Vorschläge zur Neugestaltung des Rechts auf Grund eines Referates, AcP 147 (1941), 89 ff.

HEUN Sven-Erik, Elektronisch erstellte oder übermittelte Dokumente und Schriftform, CR 1/1995, 2 ff.

HILLEBRAND Annette/BÜLLINGEN Franz, Erfolgsfaktoren digitaler Signaturen, Eine Analyse aus sozio-ökonomischer Sicht, DuD 2/2000, 80 ff.

HÖHN Ernst, Praktische Methodik der Gesetzesauslegung, Zürich 1993

HONSELL Heinrich, Schweizerisches Haftpflichtrecht, 3.A. Zürich 2000

HONSELL Heinrich/PIETRUSZAK Thomas, Der Vernehmlassungsentwurf zu einem Bundesgesetz über den elektronischen Geschäftsverkehr, AJP 7/2001, 771 ff.

HONSELL Heinrich/VOGT Nedim Peter/GEISER Thomas (Hrsg.; ZGB-[Autor]), Kommentar zum Schweizerischen Privatrecht, Schweizerisches Zivilgesetzbuch I, Art. 1-359 ZGB, Basel 1996

HONSELL Heinrich/VOGT Nedim Peter/WIEGAND Wolfgang (Hrsg.; OR-[Autor]), Kommentar zum schweizerischen Privatrecht, Obligationenrecht I, Art. 1-529 OR, 2. A. Basel 1996

HUNGER Patrick, Die Begründung der Geschäftsverbindung im Internet-Banking, Schweizer Schriften zum Bankrecht, Bd. 60, Zürich 2000 = Diss. Zürich 2000

HÜRLIMANN Hans, Der Urkundenbeweis im Zivilprozess, mit besonderer Berücksichtigung der ZPO für den Kanton Zug, Diss. Freiburg 1944

IMC (INTERNET MAIL CONSORTIUM), S/MIME and OpenPGP, http://www.imc.org/smime-pgpmime.html

JACCARD Michel (Projet), Le Projet de Loi fédérale sur les services de certification dans le domaine de la signature électronique, in: FELLMANN Walter/POLEDNA Thomas, Aktuelle Anwaltspraxis 2001/La pratique de l'avocat 2001, Bern 2002, 61 ff.

JACCARD Michel (Forme), Forme, preuve et signature électronique, in: JANNERET Vincent (Hrsg.), Aspects juridiques du commerce électronique, Zürich 2001, 113 ff.

JAEGER Jana Dominique, Die Umsetzung des UNCITRAL-Modellgesetzes über die internationale Handelsschiedsgerichtsbarkeit im Zuge der nationalen Reformen, Schriftenreihe

der August Maria Berges Stiftung für Arbitrales Recht, Bd. 9, Frankfurt a. M. 2001 = Diss. Köln 2000

JANISCH Sonja, Online Banking, Rechtsfragen des elektronischen Überweisungsverkehrs, Diskussionsreihe Bank & Börse, Bd. 21, Wien 2001 = Diss. Salzburg 1999

JANSON Philippe, Mehr Sicherheit und Komfort mit «Smartcards», Szenario möglicher Einsatzgebiete für intelligente Karten, NZZ Nr. 220, 23. September 1997, B9

JÖHRI Yvonne, Digitale Signatur, Tagung der Interdepartementalen Arbeitsgruppe «Digitale Signatur» vom 24. November 1998 in Biel, sic! 1/1999, 73 ff.

JÖRG Florian S./ARTER Oliver, Digitale Signaturen: Die Public-Key-Infrastruktur nach der neuen Zertifizierungsdiensteverordnung, ZBJV 2000, 449 ff.

KENNEDY Charles H./PASTOR M. Veronica, An Introduction to International Telecommunications Law, Boston/London 1996

KILGUS Sabine, Haftung für Unterschriftenfälschung im Bankverkehr und die Zulässigkeit ihrer Wegbedingung durch AGB, Schweizer Schriften zum Handels- und Wirtschaftsrecht, Bd. 103, Zürich 1988 = Diss. Zürich 1988

KILIAN Wolfgang, Möglichkeiten und zivilrechtliche Probleme eines rechtswirksamen elektronischen Datenaustauschs, DuD 11/1993, 606 ff.

KILIAN Wolfgang/HEUSSEN Benno (Hrsg.; KILIAN/HEUSSEN-[Autor]), Computerrechts-Handbuch, Computertechnologie in der Rechts- und Wirtschaftspraxis, 17. Ergänzungslieferung, 15. April 2001

KLETT Kathrin, Richterliche Prüfungspflicht und Beweiserleichterung, AJP 11/2001, 1293 ff.

KNEUBÜHLER Andreas, Die Einführung der digitalen Unterschrift verzögert sich, Für die Internet-Signatur fehlen gesetzliche Grundlagen – Banken lassen Pilotversuche mit Eigenentwicklungen laufen, SonntagsZeitung 11. November 2001, 85, http://www.sonntagszeitung.ch/stat/smd/index.htm

KOCH Hans-Joachim/RÜSSMANN Helmut, Juristische Begründungslehre, Eine einführung in Grundprobleme der Rechtswissenschaft, München 1982

KOFMEL EHRENZELLER Sabine, Art. 8 ZGB – Aktuelles zu einer vertrauten Beweisregel in nationalen und internationalen Fällen, ZBJV 2001, 813 ff.

KOHLAS Reto/MAURER Ueli, Reasoning About Pulic-Key Certification: On Bindings Between Entities and Public Keys, IEEE Journal on Selected Areas in Communications, No. 4/2000, 551 ff.

KÖNIG M. Michael (Praxis), Gespannt auf die Praxis, Juristische Überlegungen zum Fernabsatzgesetz, c't 15/2000, 160

KÖNIG M. Michael (Anschein), Wenn der Anschein trügt, Streit um den sorgfältigen Umgang mit EC-Karten, c't 25/1999, 248 ff.

KRAMER Ernst A., Juristische Methodenlehre, Bern 1998

KRAMER Ernst A./SCHMIDLIN Bruno (BK-KRAMER/SCHMIDLIN), Berner Kommentar zum Obligationenrecht, Band VI, 1. Abteilung, 1. Teilband, Allgemeine Einleitung in das schweizerische Obligationenrecht und Kommentar zu Art. 1-18 OR, Bern 1986

KREMPL Stefan (Finger), Zeigt her eure Finger, Erhebliche Schwächen bei biometrischen Verfahren, c't 4/2001, 62 f.

KREMPL Stefan (Signaturen), Wer braucht digitale Signaturen?, Von der Public-Key-Infrastruktur zur Sicherungszwangsgesellschaft, c't 2/2001, 60 ff.

KÜHN Ulrich, Technische Grundlagen digitaler Signaturverfahren, in: HOEREN Thomas/SCHÜNGEL Martin (Hrsg.), Rechtsfragen der digitalen Signatur, Eine Einführung in Recht und Praxis der Zertifizierungsstellen, Berlin 1999, 65 ff.

BK-KUMMER, s. LIVER/MEIER-HAYOZ et al.

KUNER Christopher, Das Signaturgesetz aus internationaler Sicht, CR 10/1997, 643 ff.

KUNER Christopher/MIEDBRODT Anja, Written Signature Requirements and Electronic Authentication: A Comparative Perspective, http://www.kuner.com/data/articles/signature_perspective.html

LEGLER Thomas (E-Commerce), Electronic Commerce mit digitalen Signaturen in der Schweiz, Kurzkommentar zur Zertifizierungsdiensteverordnung, Bern 2001

LEGLER Thomas (Notariat), Digitale Signaturen in der Schweiz: Vom realen zum virtuellen Notariat?, ZBGR 3/2001, 129ff.

LEIER Barbara, Haftung der Zertifizierungsstellen nach dem SigG, Betrachtung der geltenden und Überlegungen zur zukünftigen Rechtslage, MMR 1/2000, 13 ff.

LEPSCHIES Gunter, E-Commerce und Hackerschutz, Leitfaden für die Sicherheit elektronischer Zahlungssysteme, Braunschweig/Wiesbaden 1999

LEUENBERGER Christoph, Glaubhaftmachen, in: LEUENBERGER Christoph (Hrsg.), Der Beweis im Zivilprozess, Schriften der Stiftung für die Weiterbildung schweizerischer Richterinnen und Richter SWR, Bd. 1, Bern 2000, 107 ff.

LINDHOLM Pia/MAENNEL Frithjof A., Directive on Electonic Commerce (2000/31/EC), CRi 3/2000, 65 ff.

LIVER Peter/MEIER-HAYOZ Artur/MERZ Hans/JÄGGI Peter/HUBER Hans/FRIEDRICH Hans-Peter/KUMMER Max (BK-[Autor]), Berner Kommentar zum Zivilgesetzbuch, Einleitung, Art. 1-10 ZGB, Bern 1962

LUCKHARDT Norbert (PGP I), Pretty Good Privacy, Teil 1: Einstieg in das Web of Trust, c't 12/1999, 212 f.

LUCKHARDT Norbert (PGP II), Pretty Good Privacy, Teil 2: Schlüsselfragen und -antworten, c't 13/1999, 208 f.

LUCKHARDT Norbert (PGP III), Pretty Good Privacy, Teil 3: Dateibearbeitung und geteilte Schlüssel, c't 16/1999, 172 ff.

LÜDEMANN Volker/ADAMS Nils, Die elektronische Signatur in der Rechtspraxis, K&R 1/2002, 8 ff.

MALZER Hans Michael, Zivilrechtliche Form und prozessuale Qualität der digitalen Signatur nach dem Signaturgesetz, DNotZ 1998, 96 ff.

MAYER-SCHÖNENBERGER Viktor/PILZ Michael/REISER Christian/SCHMÖLZER Gabriele, Signaturgesetz, Praxiskommentar, Wien 1999

MEENTS Jan Geert, Verbraucherschutz bei Rechtsgeschäften im Internet, Anwendung und Wirkung klassischer Instrumentarien des Verbraucherschutzrechts und der europäischen Fernabsatzrichtlinie, Rechtsfragen der Wirtschaft, Bd. 20, Köln 1998 = Diss. Münster 1998

MEIER Isaak, Das Beweismass – ein aktuelles Problem des schweizerischen Zivilprozessrechts, BJM 2/1989, 57 ff.

BK-MEIER-HAYOZ, s. LIVER/MEIER-HAYOZ et al.

MENZEL Thomas, Elektronisch Signaturen, Schriftenreihe Rechtsinformatik, Bd. 2, Wien 2000

MERTES Paul, Die signaturgesetzkonforme Signatur in der Praxis – Ein Leitfaden für Einsteiger, in: GEIS Ivo (Hrsg.), Die digitale Signatur – eine Sicherheitstechnik für die Informationsgesellschaft, Eschborn 2000, 29 ff.

MERZ Hans, Vertrag und Vertragsschluss, 2. A. Freiburg 1992

BK-MERZ, s. LIVER/MEIER-HAYOZ et al.

MICHEL Lothar, Gerichtliche Schriftvergleichung, Eine Einführung in Grundlagen, Methoden und Praxis, Berlin/New York 1982

MIEDBRODT Anja, Signaturregulierung im Rechtsvergleich, Ein Vergleich der Regulierungskonzepte in Deutschland, Europa und in den Vereinigten Staaten von Amerika, Der elektronische Rechtsverkehr, Bd. 1, Baden-Baden 2000 = Diss. Frankfurt a. M. 2000

MK-[Autor], s. REBMANN/SÄCKER/RIXECKER

MÖCKE Frank, Shopping ohne Risiko, Gesetz räumt Rückgaberecht beim E-Commerce und Versandhandel ein, c't 9/2000, 34

MORITZ Hans-Werner, Quo vadis elektronischer Geschäftsverkehr, CR 1/2000, 61 ff.

MÜLLER Christoph Markus, Anscheinsbeweis im Strafprozess, Am Beispiel der Feststellung von Kausalität und von Dispositionsprädikaten, Schriften zum Prozessrecht, Bd. 144, Berlin 1998

MÜLLER Armin/WILDHABER Bruno/GLAUS Markus, Identrus: PKI der Finanzinstitute, http://www.itrust.ch/deutsch/articles/Identrus_V11.pdf

MÜLLER Thomas/WIRTH Markus (Hrsg.; MÜLLER/WIRTH-[Autor]), Gerichtsstandsgesetz, Kommentar zum Bundesgesetz über den Gerichtsstand in Zivilsachen, Zürich 2001

NIESING Matthias/SCHMEH Klaus, Schlüssel des Vertrauens, Digitale Ausweise im Internet, c't 4/2001, 224 ff.

OBERHOLZER Mirko Thomas (EBPP), Electronic Bill Presentment and Payment (EBPP), Neueste Rechtliche Entwicklungen bei Zahlungsverkehrssystemen, in: ARTER Oliver/JÖRG Florian S. (Hrsg.), Internet-Recht und Electronic Commerce Law, 1. Tagungsband, St. Gallen/Lachen 2001

OBERHOLZER Mirko Thomas (Digitale Signatur), Digitale Signatur und Verschlüsselung im elektronischen Handel, Grundlagen, rechtliche Aspekte, internationale Harmonisierungsbestrebungen und Beurteilung, in: BAUDENBACHER Carl (Hrsg.), Aktuelle Probleme des Europäischen und internationalen Wirtschaftsrechts, Bd. 2, Neuwied 1999, 399 ff.

OCHEL David/WEISSMANN Oliver, Schriftgut, PKI soll sichere Kommunikation gewährleisten, iX 9/2001, 44 ff.

OERTEL Klaus, Elektronische Form und notarielle Aufgaben im elektronischen Rechtsverkehr, MMR 7/2001, 419 ff.

OFTINGER Karl/STARK Emil W., Schweizerisches Haftpflichtrecht, Erster Band: Allgemeiner Teil, 5. A. Zürich 1995

OPPLIGER Rolf, Von der PKI zum Trust Management, Möglichkeiten und Grenzen einer Schweizer PKI aus technischer Sicht, Digma 2/2001, 70 ff.

OR-[Autor], s. HONSELL/VOGT/WIEGAND

PALANDT (PALANDT-[Autor]), Bürgerliches Gesetzbuch, Bd. 7, 60. A. München 2001

PAUL Werner, Die neuen PIN-Nummern der ec-Karten, NJW-CoR-Gespräch mit Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik (BSI), NJW-CoR 4/1998, 223 ff.

PESTALOZZI Simone R./VEIT Marc D., Elektronische Signaturen: schweizerische Regulierungsansätze im europäischen Umfeld, AJP 5/2000, 599 ff.

PIETRUSZAK Thomas, E-Commerce im Spiegel der Gesetzgebung, Eine Standortbestimmung – international und für die Schweiz, NZZ Nr. 222, 25. September 2001, B 46

PORDESCH Ulrich, Der fehlende Nachweis der Präsentation signierter Daten, DuD 2/2000, 89 ff.

PORDESCH Ulrich/NISSEN Kai, Fälschungsrisiken elektronisch signierter Dokumente, CR 9/1995, 562 ff.

PRIPLATA Christine/STAHLKE Colin, Kryptisch elliptisch, Public-Key-Verfahren mit ECC, iX 9/2001, 109 ff.

PROBST Thomas, Biometrie und SmartCards, Wie kann Datenschutz technisch sichergestellt werden?, DuD 6/2000, 322 ff.

PRÜTTING Hans, Gegenwartsprobleme der Beweislast, Eine Untersuchung moderner Beweislasttheorien und ihrer Anwendung insbesondere im Arbeitsrecht, München 1983

RAGGENBASS Marc, Die elektronische Signatur in der Schweiz auf der Zielgeraden, Anerkennung der elektronischen Unterschrift bereits im ersten Quartal 2002, NZZ Nr. 222, 25. September 2001, B 47

RAMSAUER Matthias, Die Regelung der Public Key Infrastruktur in der Schweiz, in: WEBER Rolf H./HILTY Reto M./AUF DER MAUR Rolf M. (Hrsg.), Geschäftsplattform Internet, Rechtliche und praktische Aspekte, Zürich 2000, 59 ff.

RASSMANN Steffen, Elektronische Unterschrift im Zahlungsverkehr, CR 1/1998, 36 ff.

REBMANN Kurt/SÄCKER Franz Jürgen/RIXECKER Roland (Hrsg.; MK-[Autor]), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, Allgemeiner Teil, §§ 1-240, AGB-Gesetz, 4. A. München 2001

REDEKER Helmut, EU-Signaturrichtlinie und Umsetzungsbedarf im deutschen Recht, CR 7/2000, 455 ff.

REISER Cristof, Die Rechtsgrundlagen für das POS-System des deutschen Kreditgewerbes («electronic cash»), WM 1989, Sonderbeilage Nr. 3

RIESS Joachim, Signaturgesetz – Der Markt ist unsicher, DuD 9/2000, 530 ff.

RIHACZEK Karl (Schriftform), Schriftform – Elektronische Form, in: GLADE Albert/REIMER Helmut/STRUIF Bruno (Hrsg.), Digitale Signatur und sicherheitssensitive Anwendungen, Braunschweig/Wiesbaden 1995, 133 ff.

RIHACZEK Karl (Beweis), Der elektronische Beweis – die Lücke bei der Umsetzung von Technik zum Rechtsgebrauch, DuD 3/1994, 127 ff.

RIHM Thomas, E-Mail als Beweismittel im Zivilgerichtsverfahren, SJZ 21/2000, 497 ff.

RITTNER Fritz, Wettbewerbs- und Kartellrecht, Eine systematische Darstellung des deutschen und europäischen Rechts für Studium und Praxis, 6. A. Heidelberg 1999

ROMMÉ Oliver, Der Anscheinsbeweis im Gefüge von Beweiswürdigung, Beweismass und Beweislast, Prozessrechtliche Abhandlungen Heft 71, Köln/Berlin/Bonn/München 1989 = Diss. Saarbrücken 1988

ROSE Alan D., The Challenges for Uniform Law in the Twenty-First Century, ULR/RDU 1996, 9 ff.

ROSENBERG Leo/SCHWAB Karl Heinz/GOTTWALD Peter, Zivilprozessrecht, 15. A. München 1993

ROSENTHAL David (Missverständnisse), Digitale Signaturen: Von Missverständnissen und gesetzlichen Tücken, Jusletter, 29. Januar 2001

ROSENTHAL David (Bund), Digitale Signaturen: Der Bund will vorwärts machen, Anwaltsrevue 2/1999, 19 f.

ROSSNAGEL Alexander (Fortentwicklung), Signaturgesetz und Richtlinie für elektronische Signaturen, Zur Fortentwicklung der Signaturregelungen, http://www.uni-kassel.de/fb10/oeff_recht/publikationen/disDin99.ghk

ROSSNAGEL Alexander (Recht), Das neue Recht elektronischer Signaturen, Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO, NJW 25/2001, 1817 ff.

ROSSNAGEL Alexander (Signaturgesetz), Editorial, Das neue Signaturgesetz – Grundlage des elektronischen Rechtsverkehrs, MMR 4/2001, 201 f.

ROSSNAGEL Alexander (Signaturregelungen), Auf dem Weg zu neuen Signaturregelungen, Die Novellierungsentwürfe für SigG, BGB und ZPO, MMR 8/2000, 451 ff.

ROSSNAGEL Alexander (Standard), Der europäische Standard, Die elektronische Signatur der europäischen Richtlinie, in: GEIS Ivo (Hrsg.), Die digitale Signatur – eie Sicherheitstechnik für die Informationsgesellschaft, Ein Leitfaden für Anwender und Entscheider, Eschborn 2000, 195 ff.

ROSSNAGEL Alexander (Sicherheitsvermutung), Die Sicherheitsvermutung des Signaturgesetzes, NJW 45/1998, 3312 ff.

ROSSNAGEL Alexander (Rechtsverkehr), Digitale Signaturen im Rechtsverkehr, NJW-CoR 2/94, 96 ff.

RSA LABORATORIES, FAQ, RSA Laboratories' Frequently Asked Questions about Today's Cryptography, Version 4.1, http://www.rsasecurity.com/rsalabs/faq

RUF Peter, Notariatsrecht, Skriptum, Langenthal 1995

RÜSSMANN Helmut (Beweisrecht), Das Beweisrecht elektronischer Dokumente, http://rw20hr.jura.uni-sb.de/rw20/people/ruessmann/elbeweis/elbeweis.htm

RÜSSMANN Helmut (Herausforderung), Herausforderung Informationsgesellschaft: Die Anwendung moderner Technologien im Zivilprozess und anderen Verfahren, Schweiz, http://ruessmann.jura.uni-sb.de/grotius/Reports/schweiz.htm

RÜSSMANN Helmut (Haftungsfragen), Haftungsfragen und Risikoverteilung bei ec-Kartenmissbrauch, DuD 7/1998, 395 ff.

SANGIORGIO Didier, Neuerungen im elektronischen Verkehr mit dem Bundesgericht und den Bundesbehörden, in: FELLMANN Walter/POLEDNA Thomas, Aktuelle Anwaltspraxis 2001/La pratique de l'avocat 2001, Bern 2002, 47 ff.

SCHAUER Bernd, Electronic Commerce in der EU, Schriftenreihe des Ludwig Boltzmann Institutes für Europarecht, Bd. 3, Wien 1999

SchKG-[Autor], s. STAEHELIN/BAUER/STAEHELIN

SCHLAURI Simon (Basistechnologie), Die digitale Signatur: Basistechnologie des elektronischen Geschäftsverkehrs, in: ARTER Oliver/JÖRG Florian S. (Hrsg.), Internet-Recht und Electronic Commerce Law, 1. Tagungsband, St. Gallen/Lachen 2001, 55 ff.

SCHLAURI Simon (Bundesgesetz), Bundesgesetz über die elektronische Signatur: Die Vernehmlassungsvorlage des Bundesrates unter der Lupe, sic! 4/2001, 362 ff.

SCHLAURI Simon (Bundesgesetz WWW), Bundesgesetz über die elektronische Signatur: Die Vernehmlassungsvorlage des Bundesrates unter der Lupe, http://www.sf-fs.ch/berichte/2001/02052001VE_BGES.html (ausführlichere Fassung von SCHLAURI, Bundesgesetz)

SCHLAURI Simon (Kommunikation), Sichere elektronische Kommunikation, Digitale Signaturen ohne Schweizer Zertifizierstelle?, NZZ Nr. 119, 25. Mai 2001, 88

SCHLAURI Simon (E-Kuriere), «E-Kuriere»: Endlich sichere E-Mail für Anwälte?, Jusletter 4. Dezember 2000

SCHLAURI Simon/KOHLAS Reto, Vorentwurf zu einem Bundesgesetz über elektronische Signaturen, sic! 3/2001, 253 ff.

SCHMID Jörg (Beurkundung), Öffentliche Beurkundung von Schuldverträgen, Ausgewählte bundesrechtliche Probleme, 2. A. Freiburg 1989 = Diss. Freiburg 1988

SCHMID Leo (Unterschriftenwesen), Unterschriftenwesen im schweizerischen Privatrecht, Diss. Zug 1930

SCHMIDT Andreas U., Signiertes XML und das Präsentationsproblem, DuD 3/2000, 153 ff.

SCHÖBI Felix (Bundesgesetz), Bundesgesetz über die elektronische Signatur und Bundesgesetz über den elektronischen Geschäftsverkehr, Eröffnung des Vernehmlassungsverfahrens, Jusletter 22. Januar 2001

SCHÖBI Felix (Vertragsschluss), Vertragsschluss auf elektronischem Weg: Schweizer Recht heute und morgen, in: WEBER Rolf H./HILTY Reto M./AUF DER MAUR Rolf M. (Hrsg.), Geschäftsplattform Internet, Rechtliche und praktische Aspekte, Zürich 2000, 95 ff.

SCHÖNENBERGER Wilhelm/JÄGGI Peter (ZK-SCHÖNENBERGER/JÄGGI), Zürcher Kommentar zum Obligationenrecht, Teilband V 1a, Art. 1-17 OR, 3. A. Zürich 1973

SCHULZKI-HADDOUTI Christiane (Karten), Karten neu gemischt, Neue Chancen für die Chipkarte, c't 25/2000, 274 ff.

SCHULZKI-HADDOUTI Christiane (Unterschriftsüberreif), Unterschriftsüberreif, Digitale Signaturen brauchen Anwendungen, c't 21/1999, 54 ff.

SCHULZKI-HADDOUTI Christiane (Übereinkunft), Digitale Übereinkunft, EU-Richtlinie zur digitalen Signatur verabschiedet, c't 8/1999, 46

SCHULZKI-HADDOUTI Christiane (Marktmacht), Markt- oder Staatsmacht, Streit um digitale Signaturen, c't 1/1999, 58, http://www.heise.de/ct/99/01/058

SCHWENZER Ingeborg, Schweizerisches Obligationenrecht, Allgemeiner Teil, 2. A. Bern 2000

SEIDEL Ulrich (Dokumentenschutz I), Dokumentenschutz im elektronischen Rechtsverkehr (I), Bestandsaufnahme und Regelungsperspektiven, CR 7/1993, 409 ff.

SEIDEL Ulrich (Dokumentenschutz II), Dokumentenschutz im elektronischen Rechtsverkehr (II), Bestandsaufnahme und Regelungsperspektiven, CR 8/1993, 484 ff.

SIDLER Oliver, Beweislast liegt beim Schlüsselinhaber, Bemerkungen zum Entwurf des Bundesgesetzes über die elektronische Signatur (BGES), Digma 2/2001, 64 ff.

SIETMANN Richard (Zukunftstechnik), Zukunftstechnik mit Schwächen, OmniCard 2002, c't 3/2002, 30

SIETMANN Richard (Flankenschutz), Flankenschutz, Die HBCI-Sicherheitsarchitektur, c't 13/2001, 140 ff.

SIETMANN Richard (Kreuz), Das Kreuz mit den Karten, SmartCards mit Akzeptanzproblemen, c't 3/2001, 36f.

SPINDLER Gerald (Bankrecht I/II), Bankrecht und E-Commerce, 1. Teil, Jusletter 26. November 2001, 2. Teil, Jusletter 3. Dezember 2001

SPINDLER Gerald (Bemerkungen), Bemerkungen zum geplanten Bundesgesetz über den elektronischen Geschäftsverkehr, sic! 3/2001, 259 ff.

SPÜHLER Karl, Behauptungslast und Beweiswürdigung bei hochtechnischen Zusammenhängen, in: LEUENBERGER Christoph (Hrsg.), Der Beweis im Zivilprozess, Schriften der Stiftung für die Weiterbildung schweizerischer Richterinnen und Richter SWR, Bd. 1, Bern 2000, 93 ff.

STAEHELIN Adrian/BAUER Thomas/STAEHELIN Daniel (Hrsg.; SchKG-[Autor]), Kommentar zum Bundesgesetz über Schuldbetreibung und Konkurs, Unter Einbezug der Nebenerlasse, SchKG I, Art. 1-87, Basel/Genf/München 1998

STEINMANN Markus, Kundenidentifikation durch Code und ihre rechtliche Bedeutung im Bankwesen, Schweizer Schriften zum Bankrecht, Bd. 19, Zürich 1994

STRATENWERTH Günter, Schweizerisches Strafrecht, Besonderer Teil II: Straftaten gegen Gemeininteressen, 5. A. Bern 2000

STUDER Urs W./RÜEGG Viktor/EIHOLZER Heiner, Der Luzerner Zivilprozess, Luzern 1994

SURETY, INC., Digital Notary System, Technical Overview, http://www.surety.com/dns/technical.pdf

THOMANN Felix H., Sicherheit und Haftungsbeschränkungen im Internet-Banking, recht 4/1998, 160 ff.

VAN DEN HOF Simone, Digital Signature Law Survey, http://rechten.kub.nl/simone/ds-law-su.htm

VEHSLAGE Thorsten, Das neue Fernabsatzgesetz im Überblick, Verbraucherschutz im Electronic Commerce, DuD 9/2000, 546 ff.

VISCHER Frank/ALBRECHT Andreas C., Problematische Seiten der digitalen Signatur, Missbrauch und mögliche Folgen müssen gut bedacht sein, NZZ Nr. 116, 21. März 2001, 18

VOGEL Oscar/SPÜHLER Karl, Grundriss des Zivilprozessrechts, und des internationalen Zivilprozessrechts der Schweiz, 7. A. Bern 2001

VON DER CRONE Hans-Caspar, Rechtliche Aspekte der direkten Zahlung mit elektronischer Überweisung (EFTPOS), Schweizer Schriften zum Handels- und Wirtschaftsrecht, Bd. 109, Zürich 1988 = Diss. Zürich 1988

VON HARNIER Albrecht, Organisationsmöglichkeiten für Zertifizierungsstellen nach dem Signaturgesetz, Der elektronische Rechtsverkehr, Bd. 2, Baden-Baden 2000 = Diss. Kassel 2000

WALDER-RICHLI Hans Ulrich, Zivilprozessrecht, Nach den Gesetzen des Bundes und des Kantons Zürich unter Berücksichtigung anderer Zivilprozessordnungen, 4. A. Zürich 1996

WASSERMEYER Heinz, Der prima facie Beweis, Eine Studie über die rechtliche Bedeutung der Erfahrungssätze, Aschendorffs Juristische Handbücherei, Bd. 41, Münster (Westfahlen) 1954

WEBER Rolf H. (E-Commerce), E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, Zürich 2001

WEBER Rolf H. (BK-WEBER), Berner Kommentar zum Obligationenrecht, Band VI, 1. Abteilung, 5. Teilband, Die Folgen der Nichterfüllung, Art. 97-109 OR, Bern 2000

WEBER Rolf H. (Schweiz), Schweiz: Public Key Infrastruktur, CRi 3/2000, 86 ff.

WEBER Rolf H. (Elektronisches Geld), Elektronisches Geld, Erscheinungsformen und rechtlicher Problemaufriss, Schweizer Schriften zum Bankrecht, Bd. 58, Zürich 1999

WEBER Rolf H. (Kryptographie), Kryptographie – Schlagwort im Spannungsfeld von Geheimnisschutz und Sicherheitserwartungen, Fakten, Zeitschrift für Datenschutz des Kantons Zürich, 3/1997, 36 ff.

WEBER Rolf H. (Zahlungsaufträge), Haftung für Schäden bei Ausführung gefälschter Zahlungsaufträge, SJZ 6/1985, 85 ff.

WEBER Rolf H. (AGB), Allgemeine Geschäftsbdingungen der Banken – zum Problem einer Grenzziehung, SAG 1984, 150 ff.

WEBER Rolf H./JÖHRI Yvonne, Vertragsabschluss im Internet, in: WEBER Rolf H./HILTY Reto M./AUF DER MAUR Rolf M. (Hrsg.), Geschäftsplattform Internet, Rechtliche und praktische Aspekte, Zürich 2000, 39 ff.

WELSCH Günther, Das Signaturänderungsgesetz, Der Entwurf vom April 2000, DuD 7/2000, 408 ff.

WERNER Stefan, Elektronischer Zahlungsverkehr, Auswirkungen der Rechtsprechung zum ec-Kartensystem, MMR 1998, 338 ff.

WIEGAND Wolfgang, Geschäftsverbindung im E-Banking, in: WIEGAND Wolfgang (Hrsg.), E-Banking, Rechtliche Grundlagen, Bern 2002, 93 ff.

WILDHABER Bruno (Market Analysis), PKI/DC Market Analysis, Update January 2002, http://www.wildhaber.com, «Stuff», dann «The current state of PKI – A market analysis (January 2002)»

WILDHABER Bruno (Signaturgesetze), Signaturgesetze, Anwendung und Nutzen, Version 1.0, 7. September 2001, http://www.itrust.ch/deutsch/articles/Anwendung_Signaturgesetze_V10.pdf

WILDHABER Bruno (Ende), Das Ende von Swisskey – wie weiter?, Version 1.1, 30. Mai 2001, http://www.itrust.ch/deutsch/articles/Swisskey_10d.pdf

WOLFRUM Rüdiger (Hrsg.), Handbuch Vereinte Nationen, München 1991

WULFF Oliver, Das UNCITRAL Modellgesetz über den grenzüberschreitenden Überweisungsverkehr, Bielefeld 1998 = Diss. Regensburg 1996/97

ZÄCH Roger (BK-ZÄCH), Berner Kommentar zum Obligationenrecht, Band VI, 1. Abteilung, 2. Teilband, 2. Unterteilband, Stellvertretung, Art. 32-40 OR

ZEUNER Volker, Erfahrungen mit der Umsetzung des deutschen Signaturgesetzes, in: GEIS Ivo (Hrsg.), Die digitale Signatur – eine Sicherheitstechnik für die Informationsgesellschaft, Ein Leitfaden für Anwender und Entscheider, Eschborn 2000, 51 ff.

ZGB-[Autor], s. HONSELL/VOGT/GEISER

ZKA (ZENTRALER KREDIT-AUSSCHUSS; ZKA, Informationen), Informationen zu Hackerangriffen auf HBCI, http://www.hbci-zka.de/siz_hbci.nsf/ZKAPages/Aktuelles120500?OpenDocument

ZOBL Dieter (BK-ZOBL), Berner Kommentar zum Zivilgesetzbuch, 2. Abteilung, 5. Teilband, 2. Unterteilband, Art. 888-906 ZGB, 2. A. Bern 1996

ZÖLLER Richard (Hrsg.), Zivilprozessordnung, 22. A. Köln 2001 (ZÖLLER-[Autor])

Materialien- und Rechtsquellenverzeichnis

Schweiz

Allgemeines

Bericht der Groupe de Réflexion für eine Informationsgesellschaft in der Schweiz zuhanden des Schweizerischen Bundesrates, http://www.isps.ch/ger/stored_documents/PDF/52.pdf (Bericht Groupe de Réflexion)

Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz, BBl 1998, 2387 ff., http://www.isps.ch/ger/stored_documents/HTML/42.html

Berichte 1-3 der Koordinationsgruppe Informationsgesellschaft (KIG) an den Bundesrat, http://www.isps.ch/ger/about_us/reference (KIG, Bericht 1-3)

Digitale Signatur und Privatrecht (Vertragsrecht), Gutachten des Bundesamtes für Justiz vom 24. November 1998, VPB 1999 II 441, http://www.vpb.admin.ch/deutsch/doc/63/63.46.html (BJ, Gutachten)

Zertifizierungsdiensteverordnung

Verordnung über Dienste der elektronischen Zertifizierung, SR 784.103 (Zertifizierungsdiensteverordnung, ZertDV)

BAKOM, Verordnung vom 12. April 2000 über Dienste der elektronischen Zertifizierung (ZertDV), Kommentar (Kommentar ZertDV)

Technische und administrative Vorschriften über Dienste der elektronischen Zertifizierung, SR 784.103.1, http://www.bakom.ch/imperia/md/content/deutsch/telecomdienste/internet/digitalesignatur/digsig_prescriptions_oscert_v4_150801_de.pdf (Ausführungsbestimmungen zur ZertDV)

Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur

Bundesgesetz über die elektronische Signatur[1], Vernehmlassungsvorlage, Januar 2001, http://www.bj.admin.ch/themen/e-commerce/vn-ve-a-d.pdf (VE-BGES)

Bundesgesetz über die elektronische Signatur, Begleitbericht zur Vernehmlassungsvorlage, Januar 2001, http://www.bj.admin.ch/themen/e-commerce/vn-ber-a-d.pdf (Begleitbericht VE-BGES)

Vorentwurf zu einem Bundesgesetz über die elektronische Signatur, Zusammenstellung der Vernehmlassungen, http://www.bj.admin.ch/themen/e-commerce/vn-ber-bges.pdf (Zusammenstellung der Vernehmlassungen zum VE-BGES)

Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur, Entwurf, Juli 2001, http://www.bj.admin.ch/themen/e-commerce/bg-zertes-d.pdf (E-ZertES)

---

1 Ursprünglicher Titel des ZertES.

Botschaft zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES), 3. Juli 2001, BBl 2001, 5679 ff., http://www.bj.admin.ch/themen/e-commerce/bot-zertes-d.pdf (Botschaft ZertES)

Bundesgesetz über den elektronischen Geschäftsverkehr

Bundesgesetz über den elektronischen Geschäftsverkehr (Teilrevisionen des Obligationenrechts und des Bundesgesetzes gegen den unlauteren Wettbewerb), Vernehmlassungsvorlage, Januar 2001, http://www.bj.admin.ch/themen/e-commerce/vn-ve-b-d.pdf (VE-BGEG)

Bundesgesetz über den elektronischen Geschäftsverkehr (Teilrevisionen des Obligationenrechts und des Bundesgesetzes gegen den unlauteren Wettbewerb), Begleitbericht zur Vernehmlassungsvorlage, Januar 2001, http://www.bj.admin.ch/themen/e-commerce/vn-ber-b-d.pdf (Begleitbericht VE-BGEG)

Totalrevision Bundesrechtspflege

Bundesgesetz über das Bundesgericht (Bundesgerichtsgesetz), Entwurf, http://www.bj.admin.ch/themen/bgg/bot-bgg-d.pdf (E-BGG)

Botschaft zur Totalrevision der Bundesrechtspflege, 28. Februar 2001, BBl 2001, 4202 ff., http://www.bj.admin.ch/themen/bgg/bot-ber-d.pdf (Botschaft Totalrevision Bundesrechtspflege)

Vereinte Nationen

United Nations Commission on International Trade Law, Working Group on Electronic Commerce, Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures, 30 January 2001, A/CN.9/WG.IV/WP.88, http://www.uncitral.org/english/sessions/wg_ec/wp-88e.pdf (MLES und MLES Guide to Enactment)

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996, With additional article 5 *bis* as adopted in 1998, New York 1999, auch abrufbar unter http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm (MLEC und MLEC Guide to Enactment)

ITU (International Telecommunications Union), ITU-T Recommendation X.509 | ISO/IEC 9594-8: "Information Technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate Frameworks", Bezug gegen Entgelt unter http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-X.509-200003-I (ITU-T, Recommendation X.509)

Europäische Union

Signaturrichtlinie

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen, KOM (1998) 297 endg. (Vorschlag für eine Signaturrichtlinie)

Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen, KOM (1999) 195 endg. (Geänderter Vorschlag für eine Signaturrichtlinie)

Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. 2000 L 13/12 ff. (Signaturrichtlinie)

E-Commerce-Richtlinie

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, KOM (1998) 586 endg. (Vorschlag für eine E-Commerce-Richtlinie)

Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, ABl. 2000 L 178/1 ff. (E-Commerce-Richtlinie)

Fernabsatzrichtlinie

Richtlinie 97/7/EG des Europäischen Parlaments und des Rates vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz, ABl. 1997 L 144/19 ff. (Fernabsatzrichtlinie)

Richtlinie über den Fernabsatz von Finanzdienstleistungen

Geänderter Vorschlag des Europäischen Parlaments und des Rates vom 23. Juli 1999 für eine Richtlinie über den Fernabsatz von Finanzdienstleistungen an Verbraucher und zur Änderung der Richtlinie 97/7/EG und 98/27/EG, KOM (1999) 385 endg.

Gemeinsamer Standpunkt des Rates vom 19. Dezember 2001 im Hinblick auf den Erlass der Richtlinie des Europäischen Parlaments und des Rates über den Fernabsatz von Finanzdienstleistungen an Verbraucher und zur Änderung der Richtlinie 90/619/EWG des Rates und der Richtlinien 97/7/EG und 98/27/EG, http://register.consilium.eu.int/pdf/de/01/st12/12425-r1d1.pdf

Empfehlung der Kommission zu elektronischen Zahlungsinstrumenten

97/489/EG: Empfehlung der Kommission vom 30. Juli 1997 zu den Geschäften, die mit elektronischen Zahlungsinstrumenten getätigt werden (besonders zu den Beziehungen zwischen Emittenten und Inhabern solcher Instrumente), ABl. 1997 L 208/52 ff. (Empfehlung der Kommission zu elektronischen Zahlungsinstrumenten)

Datenschutzrichtlinie

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, ABl. 1995 L 281/31 (Datenschutzrichtlinie)

Deutschland

Signaturgesetz 1997 und Nebenerlasse

Bundesregierung, Begründung zum IuKDG, BT-Drs. 13/7385 (Begründung IuKDG)

Informations- und Kommunikationsdienstegesetz (IuKDG), BGBl. 1997 I S. 1870, 1872 (SigG 97)

Bundesregierung, Bericht über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des Informations- und Kommunikationsdienste-Gesetzes (IuKDG), BT-Drs. 14/1191 (Bundesregierung, IuKDG-Bericht)

Verordnung zur digitalen Signatur (Signaturverordnung - SigV), BGBl. 1997 I S. 2498 (SigV 97)

Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV, Signatur-Interoperabilitätsspezifikation, http://zeppo.rediris.es/ftp/mirror/dfncert/pca/SigG, Dateien sigi-a1.pdf, sigi-a1a.pdf, sigi-a2.pdf, sigi-a3.pdf, sigi-a4.pdf, sigi-a5.pdf, sigi-a6.pdf, sigia2-a.pdf und sigia4-a.pdf (SigI)

Signaturgesetz 2001 und Nebenerlasse

Bundesregierung, Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, BT-Drs. 14/4662 (Begründung SigG 01)

Beschlussempfehlung und Bericht des Ausschusses für Wirtschaft und Technologie (9. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – BT-Drs. 14/4662 – Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, BT-Drs. 14/5324 (Beschlussempfehlung SigG 01)

Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, BGBl. I S. 876 (SigG 01)

Verordnung zur digitalen Signatur (Signaturverordnung - SigV), BGBl. 2001 I S. 3074 (SigV 01)

Formanpassungsgesetz

Bundesregierung, Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr, BT-Drs. 14/4987 (Begründung FormanpassungsG)

Deutscher Bundestag, Rechtsausschuss, Beschlussempfehlung und Bericht zum Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, BT-Drs. 14/5561 (Beschlussempfehlung FormanpassungsG)

Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, BGBl. 2001 I S. 1542 (FormanpassungsG)

1. Teil: Grundlagen

§ 1 Einleitung

I. Allgemeines

Die *digitale* oder *elektronische Signatur* ist ein digitales Siegel, das die Identität des Ausstellers und die Unverändertheit digitaler Dokumente nachweist und es dem Aussteller verunmöglicht, seine Urheberschaft an diesen Dokumenten zu bestreiten.[1] Sie erfüllt damit bei der elektronischen Kommunikation ähnliche Funktionen wie die Handunterschrift auf Papier. 1

Bereits 1994 wurde im schweizerischen Nationalrat die rechtliche Gleichstellung von digitaler Signatur und Handunterschrift gefordert. Damit sollte ermöglicht werden, schriftformbedürftige Rechtsgeschäfte auch auf elektronischem Wege abzuschliessen. Im Frühling 2000 erliess der Bundesrat die *Zertifizierungsdiensteverordnung*, welche versuchsweise die zum Einsatz elektronischer Signaturen nötige *Sicherungsinfrastruktur* regeln sollte. Auf Anfang 2003 soll mit dem *Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)* ein Erlass in Kraft treten, der diese Verordnung ersetzt und nebst der Infrastruktur weitere Bereiche abdeckt, darunter die ursprünglich geforderte Gleichstellung der digitalen Signatur mit der Handunterschrift sowie Haftungsfragen.[2] 2

Wohl im Zusammenhang mit den überhöhten Erwartungen an die New Economy gegen Ende der Neunzigerjahre herrschte zunächst grosse Begeisterung über das neuartige Instrument. Die Komplexität der digitalen Signatur, die damit verbundenen Risiken und die nötigen Investitionen in eine öffentliche Sicherungsinfrastruktur wurden indessen vielfach unterschätzt. Zudem wurde anfänglich meist übersehen, dass es mit der Bereitstellung der Technologie allein nicht getan ist, sondern dass diese auf Anwendungen hin auszurichten ist, welche geeignet sind, die investierten Summen wieder zu amortisieren. Damit wird etwa die zunächst herrschende Vorstellung, dass digitale Signaturen in näherer Zukunft im Verkehr zwischen Konsumenten zum Einsatz gelangen werden, eher unwahrscheinlich, denn das mit digitalen Signaturen verbundene Sparpotential ist für Private aufgrund der nur kleinen Zahl digitalisierbarer Transaktionen wohl zu klein. Vielmehr sind dort Anwendungen zu erwarten, wo die Kommunikationsteilnehmer regelmässig sicherheitsbedürftige Transaktionen abwickeln und durch eine Digitalisierung Zeit und Geld gespart werden können; dies dürfte in erster Linie im unternehmensinternen Verkehr und im Verkehr zwischen Geschäftspartnern der Fall sein. Ebenfalls erfolgversprechend sind die Kommunikation zwischen Behörden sowie die Kommunikation zwischen Behörden und beruflich häufig mit solchen in Kontakt tretenden Personen wie beispielsweise Rechtsanwälten. Konsumenten werden digitale Signaturen, wenn überhaupt, wohl mehrheitlich in 3

---

1 Mehr zur Unterscheidung der Begriffe der elektronischen und digitalen Signatur hinten N 34 ff.
2 Eingehend hinten N 471 ff.

so genannten *geschlossenen Benutzergruppen* einsetzen, d.h. zur Kommunikation zwischen einem einzelnen Anbieter einer Dienstleistung auf der einen und einer Vielzahl von Nutzern auf der anderen Seite, wobei der Einsatz der Signatur vertraglich geregelt wird. Vornehmlich in diesen Fällen ist es möglich, die entstehenden Kosten demjenigen Teilnehmer aufzuerlegen, bei dem auch die Einsparungen anfallen; so könnte etwa ein Anbieter, der durch den Einsatz digitaler Signaturen Geld spart, die Gerätschaften seiner Kunden subventionieren, um diese zum Einsatz digitaler Signaturen zu bewegen.[3]

4 Vorweg zu beachten ist schliesslich, dass das Bundesgesetz über die Zertifizierungsdienste im Bereich der elektronischen Signatur dort nicht oder nur mittelbar anwendbar sein soll, wo die Bedingungen des Einsatzes digitaler Signaturen im geschilderten Sinn vertraglich oder allenfalls spezialgesetzlich geregelt werden. Die Bedeutung des ZertES in geschlossenen Benutzergruppen und im Verkehr zwischen Geschäftspartnern oder mit dem Staat dürfte damit eher gering sein. Nur in den seltenen Fällen, in denen schriftformbedürftige Rechtsgeschäfte elektronisch abgeschlossen werden sollen, ist der Einsatz gesetzeskonformer digitaler Signaturen zwingend nötig.

II. Thematik und Abgrenzung

5 Selbstverständlich hat eine Abhandlung über digitale Signaturen die gesetzlichen Grundlagen zu beschreiben – dem Entwurf zum ZertES kommt in diesem Buch denn auch eine wichtige Rolle zu. Aus den genannten Gründen ist indessen auch auf Anwendungsbereiche einzugehen, auf die das ZertES nicht unmittelbar anwendbar sein wird.

6 Nebst der bereits genannten Gleichstellung von digitaler Signatur und Handunterschrift sind die beweisrechtlichen Aspekte der digitalen Signatur (Beweiskraft und Beweiswürdigung digital signierter Dokumente sowie die Frage nach deren Zulassung zum Urkundenbeweis), einige Haftungsfragen sowie als Grundlage dieser Bereiche die Regelung der Sicherungsinfrastruktur zu besprechen. Die komplexe Regelung der Sicherungsinfrastruktur ist für den Anwender digitaler Signaturen indessen meist nur von untergeordneter Bedeutung, weshalb auf sie nur summarisch eingegangen wird. Die Haftung der Zertifizierungsdiensteanbieter schliesslich wird im Rahmen der ungefähr gleichzeitig mit der vorliegenden Abhandlung ebenfalls in Zürich erscheinenden Dissertation von Bianka S. DÖRR separat bearbeitet und daher an dieser Stelle nur summarisch behandelt.

7 Um den schweizerischen Vorschlag für ein ZertES in seinem rechtlichen Kontext darzustellen, soll auf dessen Vorbilder – das Modellgesetz der UNCITRAL zu elektronischen Signaturen, die EU-Signaturrichtlinie sowie die deutsche Umsetzung die-

---

3 Eingehender zu den ökonomischen Aspekten hinten N 221 ff.

ser Richtlinie – eingegangen werden. Hinzu kommen kurze Abrisse über den Vorschlag des Bundesrates für ein Bundesgesetz über den elektronischen Geschäftsverkehr (BGEG) sowie die Revision der Bundesrechtspflege soweit sie für das Thema relevant sind.

Nicht behandelt werden die über den unmittelbaren Zusammenhang mit der elektronischen Signatur hinaus gehenden öffentlichrechtlichen Aspekte (elektronischer Verkehr mit Behörden und Gerichten im Allgemeinen, elektronische Steuererklärung, Mehrwertsteuerrecht, Registerführung, elektronische Abstimmungen u. dgl.),[4] auf digitalen Signaturen basierende elektronische Zahlungssysteme wie SET und ECash,[5] die Aspekte des Strafrechts, die Frage der elektronischen Kontoeröffnung[6] sowie die sich stellenden Fragen des Wettbewerbs- und Wertpapierrechts.[7] 8

III. Überblick über die Darstellung

In der Literatur finden sich nur wenige für Juristen verständliche, aber dennoch für den Nachvollzug der gesetzlichen Regelungen ausreichend detaillierte Darstellungen der technischen Aspekte digitaler Signaturen. Ein grosser Teil des Materials ist zudem weit verstreut in einer Vielzahl von Aufsätzen zu Einzelproblemen. Der *erste Teil* der Abhandlung befasst sich daher zunächst eingehend mit den technischen Grundlagen (§§ 2-4). An seinem Ende finden sich zudem einige Überlegungen ökonomischer Natur (§ 5). 9

Der *zweite Teil* soll den rechtlichen Kontext der schweizerischen Signaturregulierung aufzeigen. Zunächst werden Regelungsbedarf und Regelungsmodelle der einzelnen 10

---

4 *Zu E-Government im Allgemeinen* etwa Maria BENNING/ Frank STEIMKE, Rathaus von zu Haus, Erste Symptome von Internetfähigkeit bei Behörden, c't 7/2001, 218 ff.; Rolf BRÜNDLER, E-Government: Einzug des Internet ins schweizerische und europäische Staatswesen, SJZ 18/2001, 396 ff.; Benno DEGRANDI, Die automatisierte Verwaltungsverfügung, Computer und Recht Bd. 3, Zürich 1977; Michael GISLER/Dieter SPAHNI (Hrsg.), eGovernment, Eine Standortbestimmung, Bern/Stuttgart/Wien 2001; J.E.J. PRINS (Hrsg.), Designing E-Government, On the Crossroads of Technological Innovation and Institutional Change, London/The Hague/Boston 2001; für Beispiele etwa auch SCHULZKI-HADDOUTI, Karten, 275 f.; vgl. auch die Seiten des Bundes zum E-Government unter http://www.e-gov.admin.ch sowie KIG, Bericht 3, 37 ff., 62 f. *Zum Steuerrecht* etwa Roger M. CADOSCH, Die digitale Signatur im Mehrwertsteuerrecht und die Auswirkungen auf den Electronic Commerce, Jusletter 5. Februar 2001; Rainer DENNER/Gilles RONCHI, Steuern und E-Commerce – Rechtliche Normierung und Optimierungspotenzial, in: Oliver ARTER/Florian S. JÖRG (Hrsg.), Internet-Recht und Electronic Commerce Law, 1. Tagungsband, St. Gallen/Lachen 2001, 289 ff., 318 ff.; OBERHOLZER, EBPP, 148 ff.; Bruno WILDHABER, Zertifikate erhalten Beweiskraft, Steuerverwaltung anerkennt elektronische Dokumente, NZZ Nr. 29, 5. Februar 2002, B5.

5 Dazu insbesondere WEBER, Elektronisches Geld, und etwa Joachim HENKEL, Bezahlen auf Draht, E-Payment: Wie der Rubel ins Rollen kommt, c't 6/2001, 270 ff.

6 Dazu etwa HUNGER, 1 ff.; Michael KUNZ, Aufsichtsrechtliche Probleme des E-Banking, in: Wolfgang WIEGAND (Hrsg.), E-Banking, Rechtliche Grundlagen, Bern 2002, 23 ff., 47 ff.; für *Deutschland* etwa SPINDLER, Bankrecht I, Rz 121 ff.

7 Zu Aspekten des Wettbewerbsrechts etwa Michel JACCARD, Droit de la concurrence et signature numérique, Quelques réflexions à la lumière de la concentration Swisskey SA, sic! 1/1999, 17 ff.

Teilbereiche gesetzlicher Signaturregulierungen dargestellt (§ 6), dann folgt der bereits erwähnte internationale Überblick (§ 7).

11 Der *dritte Teil* schliesslich befasst sich mit der schweizerischen Rechtslage, wie sie mit dem vorliegenden Entwurf zum ZertES geschaffen werden soll. Nach einem Überblick über den bisherigen Gang der Gesetzgebung im Bereich der digitalen Signatur und in einigen verwandten Rechtsgebieten (§ 8) wird zunächst die Regelung der Sicherungsinfrastruktur dargestellt (§ 9). Danach wird auf die Beweiskraft und -würdigung digitaler Signaturen eingegangen, wobei aus Gründen der kohärenteren Darstellung zugleich einige Haftungsfragen behandelt werden (§ 10). Weiter folgt die Frage der Zulassung zum Urkundenbeweis (§ 11) und als letzter Teil wird die vorgeschlagene Regelung der Gleichstellung von digitaler Signatur und Handunterschrift kritisch beleuchtet (§ 12).

12 Zum Schluss folgen eine Zusammenfassung der Ergebnisse (§ 13) und ein Stichwortverzeichnis.

§ 2 Sicherheitsfragen im Internet

I. Fragestellung

In diesem Paragraphen soll dargelegt werden, welche Sicherheitsfragen sich bei elektronischer Kommunikation im Allgemeinen und bei der Kommunikation über das Internet im Besonderen stellen, und es werden einige technische Begriffe erläutert. 13

II. Abriss über die Funktionsweise des Internet

Das Internet besteht aus Hunderttausenden von miteinander verbundenen Computernetzen, die von unabhängigen privaten oder öffentlichen Betreibern getragen werden. 14

Die gemeinsame technische Basis für alle Netzwerke und Rechner des Internet bildet das so genannte *TCP/IP-Protokoll*[8]. Es zeichnet sich durch *gerouteten, paketorientierten Datenverkehr* aus, d.h. für eine Verbindung wird nicht wie im traditionellen Telefonverkehr zwischen Anfangs- und Endpunkt eine durchgehende Leitung zusammengeschaltet, sondern die zu übermittelnden Daten werden in Pakete aufgeteilt und durch Knotenrechner *(Router)* abschnittsweise über die Teilstrecken der Verbindung weitergereicht. 15

Auf dem TCP/IP-Protokoll basieren die verschiedenen *Dienste*, die im Internet zur Verfügung stehen, wie E-Mail, Dateitransfer (FTP) oder das World Wide Web (WWW). Die Daten der Dienste werden zur Übermittlung in TCP/IP-Pakete «verpackt». 16

An einem solchen Dienst sind in der Regel zumindest zwei Softwareprodukte beteiligt: Auf der einen Seite die *Server*-Software, die den Dienst bereitstellt, und auf der anderen Seite die *Client*-Software, welche die Dienste der Server-Software in Anspruch nimmt und die Daten auf dem Rechner des Anwenders anzeigt.[9] 17

---

8 Transaction Control Program/Internet Protocol; das Protokoll wird durch die *Internet Engineering Task Force (IETF)* weiterentwickelt, einer offenen internationalen Gemeinschaft von Netzwerkdesignern und -betreibern, Herstellern entsprechender Produkte u.dgl., die sich mit der Fortentwicklung der Internet-Architektur beschäftigt; vgl. http://www.ietf.org/overview.html; KENNEDY/PASTOR, 43. Für eine kurze Einführung in TCP/IP siehe etwa GOLLMANN, 224 ff.

9 Bekannte Client-Softwareprodukte für E-Mail sind etwa Qualcomm Eudora, Microsoft Outlook oder Netscape Messenger. Im Bereich WWW sind Netscape Navigator, Microsoft Internet Explorer und Opera zu nennen.

III. Vertraulichkeit

18 TCP/IP-Pakete werden normalerweise unverschlüsselt übermittelt. Somit sind sowohl übermittelte E-Mail-Mitteilungen als auch WWW-Seiten grundsätzlich von jedem Router aus, bei dem die Pakete vorbeikommen, lesbar. Da es auch nicht möglich ist, den Weg der Pakete bei der Übermittlung im Voraus zu bestimmen, ist die *Vertraulichkeit* von über das Internet übermittelten Daten ohne zusätzliche Hilfsmittel nicht gewährleistet.[10]

IV. Authentizität

19 *Authentizität* liegt dann vor, wenn ein Dokument auf die als Aussteller angegebene Person zurückgeführt werden kann.[11]

20 Die Absenderadressen von E-Mail-Nachrichten können in aller Regel durch den Anwender in der E-Mail-Software frei eingestellt werden und sind damit beliebig fälschbar. Hinzu kommt, dass auch das Benutzerkonto, von dem aus eine E-Mail-Nachricht verschickt wurde, nicht immer eruierbar ist.[12] Die Authentizität von E-Mail-Nachrichten lässt sich daher oftmals nicht nachweisen.[13]

21 Auch im World Wide Web ist die Authentizität von Daten nicht sicher eruierbar: So ist es durch Manipulation eines Routers möglich, Abfragen auf einen falschen WWW-Server umzuleiten.[14]

V. Datenintegrität

22 Der Begriff der *Datenintegrität* ist ziemlich schwer zu definieren. Gemeinhin wird gesagt, Daten seien dann integer, wenn sie nicht durch Unberechtigte verändert wurden.[15]

---

10 GOLLMANN, 226 f.; LUCKHARDT, PGP I, 212.

11 Ähnlich etwa SEIDEL, Dokumentenschutz I, 412.

12 Voraussetzung der Eruierung ist, dass der Versand-Mailserver sowie der Zugangsanbieter (Access Provider) sichere Protokolle führen; vgl. etwa SPINDLER, Bankrecht II, Rz 137 m.H. Durch so genannte «anonyme Remailer», d.h. Internet-Mailserver, die gezielt zum anonymen Versand von E-Mail eingerichtet werden und jedermann offen stehen, kann indessen auch dies wirksam verunmöglicht werden; vgl. etwa Holger BLEICH, Selbstverdunkelung, Anonymes Mailen in der Praxis, c't 16/2000, 156 ff. Die Untersuchung des Ursprungs einer Nachricht wird zudem teilweise dadurch erschwert, dass beteiligte Unternehmen ihren Sitz im Ausland haben.

13 So etwa auch SPINDLER, Bankenrecht I, Rz 112.

14 Man spricht von *Spoofing*; GOLLMANN, 226 f.; Marco THORBRÜGGE, Lückenfüller, Verschlüsselte Kommunikation mit Windows, c't 16/1999, 176 ff., 179.

15 Eingehend GOLLMANN, 6; vgl. auch AMERICAN BAR ASSOCIATION, 51 f.

Sämtliche auf einem Computer gespeicherten Daten können schon durch einen wenig versierten Anwender problemlos verändert werden. Dies gilt auch für früher empfangene oder versandte (d.h. im Ausgangsordner gespeicherte) E-Mail-Nachrichten[16] oder für eigentlich nicht zur Nachbearbeitung vorgesehene Dokumentenformate, wie etwa das *Portable Document Format (PDF)*[17]. Leicht veränderbar sind grundsätzlich ebenso die Randdaten, also etwa das Erstellungs- oder Veränderungsdatum einer Datei oder Nachricht. 23

Auf nur einmal beschreibbare Medien wie CD-R[18] geschriebene Daten können zwar als solche nicht mehr geändert werden, hier besteht jedoch auf die naheliegende Möglichkeit, einen Datenträger mit leicht verändertem Inhalt einfach neu zu erstellen. Im Weiteren können Dateien auf einem derartigen Datenträger oftmals unsichtbar gemacht und durch neue ersetzt werden, ohne dass dies beim Aufruf der Inhaltsanzeige für den Datenträger erkennbar wäre.[19] 24

Bei der Datenübermittlung über das Internet kann ein Angreifer aufgrund des geschilderten Routing-Konzepts die über einen für ihn zugänglichen Router geleiteten Datenpakete nicht nur lesen, sondern auch verändern. 25

Weder bei der Speicherung von Daten auf normalen oder einmal beschreibbaren Datenträgern noch bei der Übermittlung von Daten über das Internet ist die Datenintegrität damit gewährleistet.[20] 26

Schliesslich ist noch darauf hinzuweisen, dass die Unterscheidung zwischen Authentizität und Integrität streng genommen nicht sinnvoll ist. Denn wenn ein Text als nicht authentisch gilt, hat die Prüfung der Integrität keinen Sinn, und wenn ein Text nicht integer ist, ist er gleichzeitig auch nicht mehr authentisch.[21] Im Folgenden wird daher nach Möglichkeit allgemeiner von *Echtheit* gesprochen. 27

VI. Nichtabstreitbarkeit

Nichtabstreitbarkeit (Non-Repudiation) liegt dann vor, wenn der Aussteller eines Dokumentes sich dessen Inhalt aufgrund des Nachweises von dessen Authentizität und Integrität anrechnen lassen muss.[22] Weil im elektronischen Datenverkehr weder 28

---

16 Die Nachrichten werden beispielsweise bei Netscape Messenger in einer einzigen grossen Datei im Klartext (d.h. für Menschen lesbar) aufbewahrt. Es ist ein Leichtes, diese Datei zu öffnen und zu verändern.

17 Ein weit verbreitetes Dokumentenformat des US-amerikanischen Herstellers Adobe; vgl. http://www.adobe.com/products/acrobat/adobepdf.html.

18 Zu unterscheiden sind CD-ROM (nicht beschreibbar), CD-R (einmal beschreibbar) und CD-RW (mehrmals beschreibbar).

19 Man spricht von *Sessions;* eingehend etwa Andy McFadden, CD-Recordable FAQ, Section 2, http://www.cdrfaq.org/faq02.html#S2-5.

20 So etwa auch Spindler, Bankenrecht I, Rz 112.

21 Ähnlich MLES Guide to Enactment, § 123; vgl. etwa auch Stratenwerth, § 36 N 13.

Authentizität noch Datenintegrität gewahrt sind, ist auch die Nichtabstreitbarkeit vielfach nicht gegeben.

29 Damit eignen sich elektronisch gespeicherte Dokumente in der Regel schlecht als Beweismittel.

VII. Weitere Sicherheitsprobleme

30 Hinzu treten – je nach Modell – auch der *Zugangsnachweis*,[23] die Nachvollziehbarkeit des Datenverkehrs durch Unberechtigte Dritte *(Datenspuren)*,[24] sowie die *sichere und dauernde Verfügbarkeit der Systeme*.[25] Diese Aspekte sind im Folgenden jedoch nicht von Belang.

---

22 AMERICAN BAR ASSOCIATION, 52 f.; ELLISON/SCHNEIER, 2; GOLLMANN, 227.

23 Dazu etwa SCHLAURI, E-Kuriere, Rz 1 ff.; SPINDLER, Bankrecht II, Rz. 137 ff.; vgl. auch SANGIORGIO, 58 f.

24 Vgl. etwa Marit KÖHNTOPP/Kristian KÖHNTOPP, Datenspuren im Internet, CR 4/2000, 248 ff., http://www.koehntopp.de/kris/artikel/datenspuren/CR_Datenspuren_im_Internet.pdf.

25 GOLLMANN, 4; entsprechende Angriffe werden als *Denial of Service Attacks* bezeichnet.

§3 Kryptographie

I. Gang der Darstellung

In der Folge wird zunächst die Funktionsweise der digitalen Signatur eingehend beschrieben. Der Aufbau der Abschnitte A bis E geht dabei vom Allgemeinen zum Speziellen. Am Ende der Darstellung der digitalen Signatur befindet sich ein Überblick über aktuelle Einsatzgebiete sowie Standardisierungsbemühungen. 31

Nach der Beschreibung der Signatur folgen Erläuterungen zur Verschlüsselung sowie zu so genannten Zeitstempeln. 32

II. Begriffe

A. Kryptographie

Die geschilderten Schwierigkeiten hinsichtlich Vertraulichkeit, Authentizität, Datenintegrität sowie Nichtabstreitbarkeit können durch *Kryptographie* angegangen werden. Kryptographie ist eine Disziplin der Informatik, die sich mit der Entwicklung und Bewertung von Verfahren der Verschlüsselung geheimer Daten befasst.[26] 33

B. Digitale und elektronische Signatur

Zur Kryptographie wird in neuerer Zeit nicht mehr nur die Verschlüsselung von Nachrichten gezählt, sondern auch Verfahren zur Absicherung von Datenintegrität und Authentizität. Weil diese beiden Sicherheitselemente in der Papierwelt durch Unterschriften gewährleistet werden, werden die Verfahren zur Absicherung dieser Bereiche auch als *digitale oder elektronische Signaturen* bezeichnet. 34

Teilweise werden diese beiden Begriffe synonym verwendet. Der Begriff der digitalen Signatur hat sich mittlerweile aber weitgehend für Verfahren eingebürgert, die auf so genannter *Public-Key-Kryptographie*[27] basieren und Authentizität sowie Datenintegrität gewährleisten.[28] Er ist also technisch definiert. 35

In Rechtstexten hingegen wird mehrheitlich der Begriff der elektronischen Signatur verwendet. Er wird teilweise sehr viel weiter gefasst als der Begriff der digitalen Signatur (so ist etwa weder der Einsatz von Public-Key-Kryptographie noch die Siche- 36

---

26 DUDEN, Das grosse Wörterbuch der deutschen Sprache, Bd. 4, 2. A. Mannheim u.a. 1993, 2012; eingehend etwa WEBER, Kryptographie, 36ff.

27 Dazu sogleich N 40.

28 MENZEL, 51; vgl. auch AMERICAN BAR ASSOCIATION, 40 ff.

rung der Datenintegrität Voraussetzung der «einfachen elektronischen Signatur» im Sinne von Art. 2 Bst. a E-ZertES).[29] Genau besehen ist dieser Unterschied indessen kaum von Bedeutung, denn zumindest dort, wo in so genannten offenen Benutzergruppen kommuniziert werden soll (also dort, wo auch die Erstkontakte auf elektronischem Weg stattfinden und damit kein Austausch geheimer Schlüssel und auch keine vertragliche Regelung der Kommunikation möglich ist), gibt es zur Public-Key-Kryptographie keine Alternativen,[30] und allein diese offenen Benutzergruppen werden jeweils durch gesetzliche Signaturregulierungen abgedeckt.[31] In der vorliegenden Arbeit werden die beiden Begriffe daher in der Regel synonym verwendet; differenziert wird nur dort, wo eine der beiden Bedeutungen klar im Vordergrund steht.

C. Digitalisierte Unterschrift

37 Von einer *digitalisierten Unterschrift* soll dann gesprochen werden, wenn eine nichtdigitale Vorlage in einen Computer eingelesen wurde (etwa durch Einscannen einer bestehenden Handunterschrift oder Unterzeichnen auf einem elektronischen Unterschriftenerfassungsgerät).

38 Dabei handelt es sich um eine normale elektronische Bilddatei, die mit digitalen Signaturen im geschilderten Sinne nichts gemeinsam hat. Digitalisierte Unterschriften sind genau gleich wie andere ungesicherte elektronisch gespeicherte Dokumente sehr leicht kopier- und manipulierbar und bieten diesen gegenüber in der Regel keinen Gewinn an Sicherheit.[32]

III. Digitale Signatur

A. Schlüsselpaar

39 Um digitale Signaturen einsetzen zu können, muss jeder Kommunikationspartner über ein Paar so genannter *kryptographischer Schlüssel* verfügen. Dies sind miteinander mathematisch korrelierende, mehrhundertstellige Zahlen, die – vereinfacht gesagt – aufgrund ihrer Grösse nicht erraten werden können.[33]

40 Mit dem einen dieser Schlüssel werden digitale Signaturen gesetzt *(Signierschlüssel)* und mit dem anderen überprüft *(Prüfschlüssel)*. Der Signierschlüssel ist geheim zu halten, weil jedermann, der auf ihn Zugriff hat, damit Signaturen setzen kann. Er wird daher auch *geheimer Schlüssel* oder *private key* genannt.[34] Der Prüfschlüssel hinge-

---

29 Hinten N 377 ff., 514 f.
30 Eingehend hinten N 303 ff.
31 Vgl. etwa hinten N 512.
32 Vorne N 19 ff.
33 Eingehend zur Sicherheit hinten N 51 ff.

gen muss allen potentiellen Adressaten zur Prüfung von Signaturen zur Verfügung stehen, weshalb er zu veröffentlichen ist. Er wird deswegen auch *öffentlicher Schlüssel* oder *public key* genannt.[35] Verfahren, die auf solchen Schlüsselpaaren basieren, werden gemeinhin als *Public-Key-Kryptographie* oder *asymmetrische Kryptographie* bezeichnet.[36]

41 Obwohl die Schlüssel mathematisch korrelieren, darf es nicht möglich sein, den Signierschlüssel aus dem Prüfschlüssel oder einer Signatur zu errechnen.[37]

42 Bei der Erzeugung des Signierschlüssels ist dafür zu sorgen, dass niemand ausser dem späteren Halter zu diesem Zugang erhält. Dies wird im einfachsten Fall dadurch erreicht, dass der Halter das Schlüsselpaar auf seinem eigenen Computersystem erzeugt, wo der Signierschlüssel sofort durch ein Passwort geschützt wird. Falls ausnahmsweise doch ein Dritter die Schlüssel erzeugt, muss dieser vertrauenswürdig sein und den Signierschlüssel vernichten, sobald er an den Halter übertragen wurde.

B. Erzeugen der Signatur

1. Grundlagen

43 Eine digitale Signatur ist ein für Menschen nicht lesbares Datenpaket von einigen hundert bis tausend Zeichen Länge, das durch eine mathematische Verknüpfung von Signierschlüssel und zu signierendem Text erzeugt wird. In die digitale Signatur fliessen damit sowohl die Eigenschaften des Textes als auch diejenigen des Signierschlüssels ein, womit sich sowohl Signaturen unterschiedlicher Texte als auch solche, die mit unterschiedlichen Signierschlüsseln erstellt wurden, voneinander unterscheiden lassen.

44 Das Erzeugen der digitalen Signatur geschieht durch Software. E-Mail-Clients weisen meist schon heute Funktionen zum Unterzeichnen von Nachrichten auf.[38] Wird eine E-Mail-Nachricht digital signiert, so wird die digitale Signatur automatisch als

---

34 AMERICAN BAR ASSOCIATION, 56; Die wohl aus dem Englischen übernommene Bezeichnung *privater Schlüssel* ist m.E. aus sprachlichen Gründen abzulehnen.

35 AMERICAN BAR ASSOCIATION, 56 f.

36 Vgl. auch MERTES, 32; AMERICAN BAR ASSOCIATION, 31.

37 GOLLMANN, 212. Beim so genannten RSA-Verfahren (dazu hinten N 169) besteht der Signierschlüssel aus zwei Primzahlen und der Prüfschlüssel aus deren Produkt – die Errechnung des Signierschlüssels setzt demnach eine Primfaktorzerlegung voraus, die bei ausreichenden Schlüssellängen auch mit schnellen Computern nicht binnen einer für einen Angreifer nützlichen Frist zu bewerkstelligen ist; Ueli MAURER, Sicherheit in Datennetzen, Studie im Auftrag des Datenschutzbeauftragten des Kantons Zürich, Fakten, Die Zeitschrift für Datenschutz des Kantons Zürich, Sondernummer 1/1996, 1 ff., 22. Zur kryptographischen Sicherheit insbesondere hinten N 51 ff.

38 So etwa Netscape Messenger oder Microsoft Outlook; vgl. auch hinten N 130.

«Attachment» an diese angehängt.[39] Im einfachsten Fall muss der Anwender hierzu seinen Wunsch zum Signieren nur durch Anklicken eines Optionsfeldes kundtun.

45 Soll nicht eine E-Mail-Nachricht unterzeichnet werden, sondern eine normale Datei auf einem Datenträger, so wird die digitale Signatur als normale Datei neben dem signierten Dokument gespeichert. Hierzu kommt andere Software zum Einsatz.[40]

46 Die Gesamtheit der zum Erzeugen digitaler Signaturen notwendigen Soft- und Hardware wird hier *Signiereinheit* genannt.

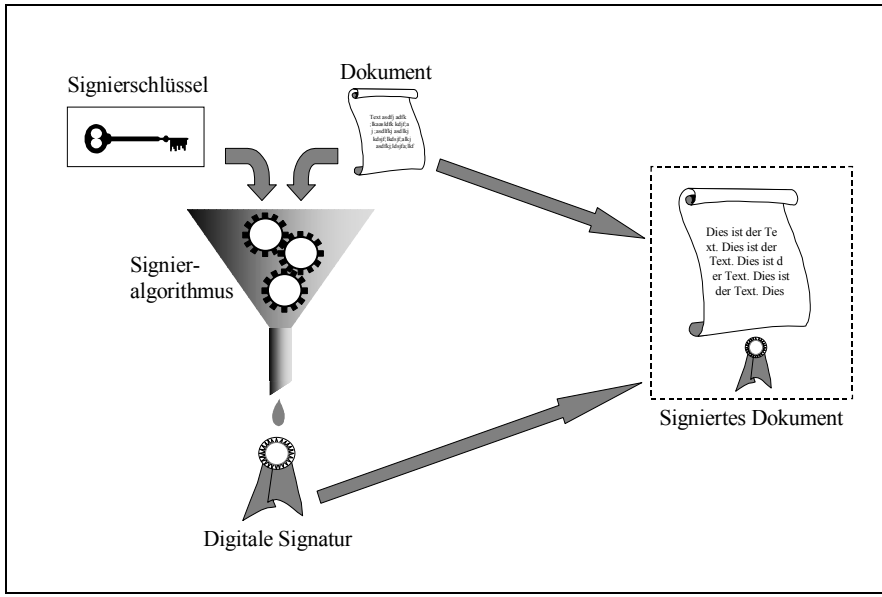

Abbildung 1: Erzeugen einer digitalen Signatur.

2. Signatur und Verschlüsselung

Die unterzeichnete Nachricht bleibt beim Signieren meist lesbar, weil die Signatur ja nur beigefügt wird.[41] Zur Sicherung der Vertraulichkeit ist aber zusätzlich eine Verschlüsselung des «Gesamtpaketes» von Nachricht und Signatur möglich.[42]

---

39 Zum hierfür eingesetzten S/MIME-Standard hinten N 129 f.

40 Für ein derartiges von E-Mail unabhängiges Beispiel MERTES, 33 ff.

41 Verfahren, die gleichzeitig auch die Nachricht unsichtbar machen, werden *opake* (d.h. verschleiernde) *Verfahren* genannt (BIZER/HERDA, 20 sprechen von *Signaturen mit Wiedergewinnung der Nachricht*). Eine eigentliche Verschlüsselung findet nicht statt, da der Prüfschlüssel ja für jedermann zugänglich ist. Derartige Verfahren können dann Anwendung finden, wenn der Text nicht ohne eine Signaturprüfung angezeigt werden soll; BIZER/HERDA, 28.

42 Zur Verschlüsselung hinten N 166 ff.

3. Hashwert

Der Signieralgorithmus erwartet als zu signierenden Input eine Zeichenkette bestimmter Länge. Bevor eine digitale Signatur daher gesetzt werden kann, muss aus der zu signierenden Nachricht, die ja beliebig lang sein kann, als erstes eine verkürzte Form erzeugt werden. Diese muss zudem für jeden Text wieder anders aussehen, denn es darf nicht passieren, dass verschiedene Texte dieselbe Signatur ergeben. Diese verkürzte Form der Nachricht wird *Hashwert*[43] genannt.[44] 48

Ein Hashwert ist demnach eine Zahl mit einer genau bestimmten Anzahl Stellen, beispielsweise 128 Bit, die für *jede Nachricht einen unterschiedlichen Wert aufweist*.[45] Man spricht aus diesem Grund auch von einem *digitalen Fingerabdruck* eines Dokuments; der Hashwert kann das Dokument *vertreten*. 49

Eine weitere Anforderung an eine solche Hashfunktion ist, dass sie nicht umkehrbar sein darf. Aus einem Hashwert darf die Originalnachricht nicht wiederhergestellt werden können. 50

```
FD:3C:8B:87:76:28:39:A5:CD:AA:BB:2A:18:2E:50:2D
```

Abbildung 2: Hashwert, im hexadezimalen Zahlensystem[46] dargestellt.

4. Kryptographische Sicherheit

Public-Key-Kryptographie basiert auf Problemen der Mathematik, für die es keine einfache und damit schnelle Lösungsmöglichkeit gibt.[47] Solche Probleme sind etwa die Primfaktorzerlegung (eingesetzt im am weitesten verbreiteten *RSA-Signaturverfahren*[48]), das Problem des diskreten Logarithmus[49], oder das «Travelling-Salesman-Problem»[50]. Durch Wahl geeigneter Schlüssellängen (d.h. durch Vergrösserung des 51

---

43 Hash = engl. *Prüfsumme.*

44 AMERICAN BAR ASSOCIATION, 42f.; Verfahren, mit denen solche kryptographischen Hashwerte erzeugt werden können, sind etwa *MD2*, *MD5* oder *SHA*; RSA LABORATORIES, 2.1.6. Die MD*x*-Verfahren gelten mittlerweile jedoch nicht mehr als sicher; OCHEL/WEISSMANN, 44.

45 Der Fachmann spricht von *Kollisionsfreiheit*. «Echte» Kollisionsfreiheit in dem Sinne, dass keine zwei Texte denselben Hashwert aufweisen, gibt es nicht, weil mit der unbegrenzten Anzahl Buchstaben, die der gehashte Text enthalten kann, natürlich mehr Kombinationen möglich sind als mit der begrenzten Anzahl Ziffern des Hashwertes; SigI, A4, 6. Kryptographische Kollisionsfreiheit liegt dann vor, wenn es *rechnerisch in für einen Angreifer nützlicher Frist unmöglich* ist, zwei Zeichenfolgen zu finden, die den gleichen Hashwert aufweisen; RSA LABORATORIES, 2.1.6.; SURETY, INC., 5-9.

46 Das hexadezimale Zahlensystem weist die Ziffernwerte 0-15 auf (statt 0-9 wie das herkömmliche dezimale Zahlensystem), wobei die Werte 10-15 durch die Buchstaben A-F ersetzt werden. Es wird zur besser lesbaren Darstellung binärer Werte eingesetzt (zwei Ziffern für 8 Bit bzw. ein Byte) und findet zur Darstellung der (binären) Hashwerte daher oft Verwendung.

47 RSA LABORATORIES, 2.3.

48 Zum Begriff N 169ff.; RSA LABORATORIES, 3.1.

so genannten *Schlüsselraumes*, also der Anzahl aller möglichen Schlüssel) kann verhindert werden, dass ein Angreifer den Signierschlüssel innert für ihn nützlicher Frist durch Ausprobieren aller möglichen Schlüsselvarianten herausfinden kann (so genannte *brute force attack*). Ein Verfahren kann dann als sicher bezeichnet werden, wenn der Aufwand für eine Berechnung grösser wird als der zu erwartende Ertrag eines erfolgreichen Angriffs.[51] Diese Sicherheit wird jedoch durch die kontinuierlich steigende Leistungsfähigkeit von Computern laufend vermindert, sodass die Verfahren und/oder die Schlüssellängen periodisch anzupassen sind.[52] Die Verfahren unterscheiden sich teilweise erheblich bezüglich der für ausreichende Sicherheit notwendigen Schlüssellängen.[53]

52 Zwar wurde bisher bei keinem dieser mathematischen Probleme *bewiesen*, dass keine einfache Lösungsmöglichkeit besteht, die eine Ermittlung von Signierschlüsseln in kurzer Zeit ermöglichen könnte. In Anbetracht dessen, dass die verbreitetsten Verfahren mittlerweile aber seit über 20 Jahren bekannt sind und jeglichen Angriffen standgehalten haben, werden diese Verfahren gemeinhin als sicher erachtet.[54] Allenfalls wird die Entwicklung so genannter *Quantencomputer* der kryptographischen Sicherheit gegenwärtiger Public-Key-Verfahren dereinst ein Ende bereiten.[55]

53 Alternativ zum Angriff auf die Public-Key-Verschlüsselung könnte ein Angreifer auch nach Kollisionen der verwendeten Hashfunktion[56] suchen, um eine Nachricht zu erzeugen, die trotz unterschiedlichem Inhalt den gleichen Hashwert wie die Originalnachricht und damit die gleiche Signatur aufweist. Dies kann allerdings durch die Verwendung kryptographisch sicherer Hashfunktionen verhindert werden.[57]

54 Die kryptographischen Algorithmen sind damit der stärkste Teil eines Systems zur Erstellung digitaler Signaturen. Ein potentieller Angreifer wird seine Zeit daher nicht mit Kryptoanalyse verschwenden, sondern sich viel eher auf andere Schwachstellen des Systems konzentrieren, also etwa versuchen, die Signierschlüssel durch Hacking zu beschaffen.[58]

---

49 Eingesetzt etwa im *ElGamal*-Verfahren; RSA LABORATORIES, 2.3.7; eingehend PRIPLATA/STAHLKE oder Volker MÜLLER/Sachar PAULUS, Elliptische Kurven und Public Key-Kryptographie, DuD 7/1998, 496.

50 Vgl. RSA LABORATORIES, 2.3.1. Aufgrund der fehlenden Eignung des so genannten X.509-Standards (N 100 ff.) für andere Verfahren als RSA wird heute aber nur die Primfaktorzerlegung genutzt; FOX/MÜLLER, 167 f.

51 BITZER/BRISCH, 106; Dirk FOX, Schlüsseltechnologie Kryptographie, DuD 9/1998, 492.

52 BIESER/KERSTEN, 29.

53 So ist etwa ElGamal gegenüber RSA diesbezüglich deutlich im Vorteil, was sich bei knappen Computerressourcen (etwa in Mobilgeräten) positiv auswirken könnte; PRIPLATA/STAHLKE, 109; vgl. aber soeben FN 50.

54 Eingehend etwa GOLLMANN, 220 f.

55 Richard SIETMANN, Kleine Sprünge, grosse Wirkung, Vom Quantensprung zum Quantenrechner, c't 25/2000, 118 ff., insbesondere Abschnitt «Quantencomputer: vom Bit zum Qubit»; vgl. auch Oliver MORSCH, 15=3x5, Primfaktrozerlegung mit einem Quantencomputer, NZZ Nr. 6, 9. Januar 2002, 63.

56 Soeben N 48 ff., vgl. auch N 57 und dort FN 45.

57 Arjen K. LENSTRA/Eric R. VERHEUL, Selecting Cryptographic Key Sizes, DuD 3/2000, 166.

5. Präsentationsproblem

a) *Allgemeines*

Eine grosse Schwierigkeit beim Design von Signiereinheiten liegt darin, dass die Signiersoftware zwar das vom Anwender gewollte Dokument auf dem Bildschirm anzeigen, im Hintergrund aber ein anderes Dokument signieren könnte. Um die Nichtabstreitbarkeit zu gewährleisten, muss sichergestellt sein, dass angezeigter und signierter Text übereinstimmen ("What you see is what you sign"). 55

Nebst dem Unterschieben falscher Dokumente etwa durch «bösartige Software» (Viren, Trojanische Pferde u. dgl.) können etwa Textteile durch besondere Farbgebung unsichtbar gemacht (weisser Text auf weissem Grund), Zeichen auf unterschiedlichen Computersystemen unterschiedlich dargestellt (abweichende Zeichensätze),[59] unsignierte Daten, die das signierte Dokument unbemerkt referenziert und anzeigt, verändert[60] oder fein aufgelöste Grafikdetails aufgrund schlechter Auflösung der Anzeige verschluckt werden.[61] Ohne die signierte Datei zu verändern führt all dies dazu, dass ein Dokument auf dem Prüfsystem anders angezeigt wird als auf dem Signiersystem. Man spricht hier gemeinhin vom *Präsentationsproblem*.[62] 56

b) *Vertrauenswürdige Hardware als Lösung*

Das Präsentationsproblem ist bei fremden Signierumgebungen besonders gravierend.[63] BIZER/HERDA schlagen daher vor, Signiervorgänge ausschliesslich in eigener gesicherter Systemumgebung durchzuführen, also etwa auf einem *Personal Digital Assistant (PDA)*.[64] Dies bewirkt zwar eine Steigerung der Sicherheit, Virenangriffe werden jedoch nicht ausgeschlossen.[65] 57

---

58 GOLLMANN, 203; ERBER-FALLER, 122 f.; FOX, Problem, 387; OCHEL/WEISSMANN, 44; OPPLIGER, 75; zum Schutz des Signierschlüssels hinten N 64 ff.

59 FOX, Problem, 387; PORDESCH, 90; SEIDEL, Dokumentenschutz II, 486.

60 Eine HTML- oder XML-Seite kann beispielsweise unmerklich Grafiken u. dgl. aus anderen Quellen beziehen und als Bestandteil anzeigen, oder ein Word-Dokument kann auf eine externe Dokumentenvorlage zugreifen, welche nach dem Setzen der Signatur verändert wird; diese und weitere Beispiele finden sich bei PORDESCH, 90.

61 So haben etwa Anzeigen von Personal Digital Assistants (PDAs) regelmässig eine sehr viel schlechtere Auflösung als normale Computerbildschirme; PORDESCH, 89.

62 Eingehend PORDESCH, 89; vgl. auch BIZER/HERDA, 25; SCHMIDT, 153.

63 BIZER/HERDA, 25; PORDESCH, 92.

64 BIZER/HERDA, 25.

65 Mit steigender Leistungsfähigkeit und Verbreitung können auch PDAs und Mobiltelefone Opfer von Viren werden; so auch ein ehemaliger Sprecher des deutschen Chaos Computer Club, zit. bei Stefan KREMPL, Hacker am Rande des Netzzusammenbruchs, Kongress des Chaos Computer Club in Berlin, NZZ Nr. 2, 4. Januar 2002, 64; für erste erfolgreiche Angriffe vgl. Patrick BRAUCH (pab.), Erster Virus für den Palm, c't 21/2000, 57; Volker ZETA (vza.), Trojanisches Pferd für Palm, c't 19/2000, 168; anders etwa Dirk BALFANZ/Edward W. FELTEN, Hand-Held Computers Can Be Better Smart Cards, in: Proceedings of USENIX Security '99, Washington, DC 1999, auch abrufbar unter http://www.cs.princeton.edu/sip/pub/pilotkey.php3, die indessen die Möglichkeit einer Virenverseuchung des PDA gar nicht erwähnen.

58 Um sicherzustellen, dass der Signaturhalter das richtige Dokument unterzeichnet, muss dieses durch vertrauenswürdige Hardware[66] angezeigt und «gehasht» werden. Derartige Hardwaresigniereinheiten[67], die eine eigene Anzeige aufweisen, werden *Klasse-3-Geräte* genannt.[68]

59 Der deutsche Hersteller Towitoko präsentierte mit dem «Chipdrive Monitor Kit» eine Lösung, welche in das Monitorkabel eingeschleift werden kann und damit die Daten auch auf dem normalen Monitor sicher anzeigt.[69] Andere Lösungen integrieren eine LCD-Anzeige mit wenigen Zeilen in den Kartenleser; sie kosten derzeit ungefähr zwischen 100 und 200 Franken.[70] Leider eignen sich beide Lösungen nur für kleine Datenmengen; ungelöst bleibt im Weiteren das Problem, dass eine derartige Anzeige nur eine beschränkte Anzahl von Dokumentenformaten unterstützen kann.

60 Einige der geschilderten Schwierigkeiten können umgangen werden, indem das Format der signierten Daten vereinfacht wird. PORDESCH schlägt etwa eine Beschränkung auf ein «Primitivformat» von 20 Zeichen pro Zeile und 20 Zeilen vor, das nur reinen Text ohne Formatierungen und Farben enthalten soll.[71] Eine weitere Möglichkeit wäre, das Format der signierten Datei sowie bestimmte Systemparameter (etwa die verwendeten Schriftarten u. dgl.) im signierten Dokument festzuhalten, sodass zur Überprüfung nachweislich wieder ein gleiches System eingesetzt werden kann; dies kann jedoch unmöglich für die mannigfaltigen Konfigurationsmöglichkeiten eines herkömmlichen PC geschehen.[72]

61 Bis zur Marktreife von wirklich sicheren Signiereinheiten für grössere Datenmengen und bis zur Etablierung von Standards zur Darstellung der signierten Dokumente dürfte noch einige Zeit verstreichen. Für grössere Datenmengen müssen daher vorderhand noch Softwarelösungen eingesetzt werden. Das Präsentationsproblem ist damit das schwerwiegendste Problem, das derzeit der technischen Absicherung der Nichtabstreitbarkeit durch digitale Signaturen noch entgegensteht.[73]

---

66 Eingehend hinten N 65, insbesondere FN 82.
67 Zum Begriff sogleich N 65.
68 Eingehend hinten N 65, 69, insbesondere FN 88.
69 TOWITOKO, CHIPDRIVE monitor kit macht digitale Signatur sicherer, http://www.towitoko.de/deutsch/187.htm.
70 Vgl. Axel KOSSEL (ad.), Geldkarte im Internet, c't 24/2000, 44; dazu KOBIL SYSTEMS, KAAN ProfessionalKlasse 3, http://www.kobil.de/seiten/d/ct/kaan_pro.htm; Axel KOSSEL (ad.), GeldKarte als Internetzahlungsmittel, c't 8/2001, 46; dazu auch cpays, Erstes System für GeldKarte-Zahlungen im Internet zugelassen, http://www.cpays.de/ger/public/single_news.php4?news_id=74.
71 PORDESCH, 94.
72 Eingehend zum Ganzen PORDESCH, 92 ff.
73 SCHMIDT, 158.

C. Aufbewahrung und Schutz des Signierschlüssels

1. Grundlagen

62 Die Handunterschrift ist durch körperliche und psychische Merkmale des Schreibenden geprägt; sie kann nicht von diesem getrennt werden und stellt quasi einen «unverlierbaren Schlüssel»[74] dar. Anders die digitale Signatur: Weil der Signierschlüssel bei Weitem zu lang ist, um in Erinnerung zu bleiben, muss er auf einem Datenträger gespeichert werden.[75] Dieser Datenträger ist nicht in natürlicher Weise an dessen rechtmässigen Halter gebunden. Wenn ihn ein Angreifer unberechtigterweise entwendet, so ist er in der Lage, digitale Signaturen zu setzen, die mit der Originalunterschrift identisch sind.

63 Die Sicherstellung der alleinigen Kontrolle des berechtigten Halters über den Signierschlüssel ist folglich ein sehr wichtiges Postulat im Rahmen einer rechtlichen Regelung der digitalen Signatur. Die eingesetzten Produkte müssen dafür Gewähr bieten, dass der Signierschlüssel weder direkt durch Menschen noch indirekt durch bösartige Software (Viren u. dgl.) ausgespäht werden kann.

2. Soft- und Hardwareschutz

64 Oftmals wird der Signierschlüssel auf einem herkömmlichen Datenträger wie einer Diskette oder Festplatte gespeichert.[76] Weil diesfalls sämtliche kryptographischen Operationen in Software auf dem Rechner ablaufen, soll dies in der Folge als *Softwaresigniereinheit* bezeichnet werden.

65 Die Speicherung des Signierschlüssels auf der Festplatte birgt das Risiko, dass dieser durch bösartige Software (Viren u. dgl.) ausgespäht oder sonstwie entwendet wird, ohne dass der Halter dies bemerkt.[77] Zur Lösung dieses Problems kann der

---

74 So schon Beat KLEINER, Automation und Mikrofilm im Bankgeschäft aus der Sicht des Juristen, SJZ 10/1973, 146 ff., 147.

75 MENZEL, 57.

76 Gemeinhin kommt zur Speicherung von Signierschlüsseln auf Datenträgern das *PKCS-#12*-Datenformat zur Anwendung (*Public Key Cryptography Standards, PKCS)*. Unter dieser Bezeichnung hat RSA Security verschiedene Standards für unterschiedliche Zwecke im Bereich Kryptographie geschaffen. PKCS #12 *(Personal Information Exchange Syntax)* definiert das Dateiformat für die Speicherung persönlicher kryptographischer Informationen wie Zertifikate, Signierschlüssel, Certificate Revocation Lists oder allgemein geheimer Information und wird durch marktübliche WWW-Browser unterstützt. PKCS #11 *(Cryptographic Token Interface Standard)* definiert eine Schnittstelle für die Kommunikation mit kryptographischen Tokens (dazu sogleich N 65). Mehr zu PKCS etwa bei Mohan ATREYA, Introduction to the PKCS Standards, http://www.rsasecurity.com/solutions/developers/whitepapers/IntroToPKCSstandards.pdf; LEPSCHIES, 165 f.

77 Die teilweise gehörte Empfehlung, den Schlüssel auf einer Diskette zu speichern, die sich nur dann im Laufwerk befinden darf, wenn der Schlüssel effektiv in Gebrauch ist (etwa bei ZKA, Informationen), erhöht die Sicherheit nur marginal, weil eine angreifende Software beliebig Zeit hat, auf das Einschieben der Diskette zu warten; so etwa auch Adrian SPALKA, zit. bei Katrin KOLBE, Digitale Signatur: Weiterhin sicher?, Zertifizierungsstellen: Abfangen der PIN alleine bringt nichts, http://www.heute.t-online.de/ZDFheute/artikel/0,1251,COMP-4099-4093,00.html.

Signierschlüssel in einem separaten angriffsresistenten Chip gespeichert werden. Denkbar ist, den Chip fest in einem Computer zu verbauen oder ihn ähnlich einer SIM-Karte in ein Mobiltelefon zu stecken.[78] Um den Chip nicht an ein bestimmtes Computersystem zu binden, wird er vielfach auch in ein so genanntes *Token* verbaut – etwa in eine *Chipkarte*[79] oder in einen kleinen Stecker für den USB-Bus[80] *(USB-Token*[81]*)*. Derartige Lösungen werden in der Folge als *Hardwaresigniereinheiten* bezeichnet.[82]

66 Die auf dem Markt verfügbaren Tokens weisen sehr unterschiedliche Sicherheitsniveaus auf.[83] Teilweise dienen sie bloss als Speicher für den Schlüssel, der wie ein normaler Datenträger gelesen werden kann und daher kaum mehr Sicherheit bietet als die Speicherung auf einem normalen Datenträger. Idealerweise können derartige Chips die Erzeugung der Schlüssel sowie die kryptographischen Operationen jedoch selbst durchführen. Diesfalls kann verhindert werden, dass der Signierschlüssel jemals in die unsichere Systemumgebung gelangt.[84]

3. PIN oder Passwort

67 Verstärkter Schutz gegen den Diebstahl des Tokens oder das Ausspähen einer Schlüsseldatei wird in der Regel durch eine PIN[85] oder ein Passwort erreicht. Um über den Schlüssel verfügen zu können, ist diesfalls nebst dem Zugriff auf die Schlüsseldatei bzw. (bei Hardwaresigniereinheiten) *Besitz* am Token auch *Wissen* nötig.

68 Ein Passwortschutz ist indessen oft nur beschränkt wirksam. Besteht das Passwort etwa aus wenigen Zeichen oder verwendet der Anwender ein umgangssprachliches Wort, so kann es mittels einer *brute force attack*, d.h. einer Angriffsmethode, bei der

---

78 Computer höherer Preisklassen enthalten manchmal derartige Krypto-Chips; vgl. etwa IBM, Security: IBM Secure Client, http://www.pc.ibm.com/ww/security/securitychip.html. Zum Einsatz digitaler Signaturen in Mobiltelefonen auch hinten N 150 ff. Zur Marktentwicklung etwa WILDHABER, Market Analysis.

79 Ähnlich einer EC-Karte; man spricht auch von *Smartcards*; vgl. etwa JANSON, B9.

80 Der *Universal Serial Bus* ist eine weit verbreitete Hardwareschnittstelle zum Anschluss von Peripheriegeräten an Personal Computer.

81 Dazu etwa Norbert LUCKHARDT, USB-Token statt SmartCard, c't 6/2000, 44.

82 Die Differenzierung zwischen Hard- und Softwaresigniereinheiten ist insofern ungenau, als auch eine Chipkarte oder eine andere Hardwaresigniereinheit ist nichts anderes ist als ein miniaturisierter Computer mit Festspeicher (ROM), Hauptspeicher (RAM), Prozessor und Ein-/Ausgabekanälen wie jeder gewöhnliche Personal Computer.Auch auf dieser laufen die Operationen letztlich in Software ab (zu Smartcards etwa Kai-Uwe MRKOR, Kartenspiele, Grundlagen der Chipkartenprogrammierung, c't 8/2000, 208 ff.; ein kurzer Überblick findet sich etwa bei JANSON). Der Unterschied besteht jedoch darin, dass die auf einer sicheren Hardwaresigniereinheit laufende Software nicht verändert werden kann, bzw. dass eine Veränderung (ein *Firmware-Update*) nur nach einem strengen Autorisierungsprotokoll durchgeführt werden darf, was Virenangriffe ausschliesst.

83 ELLISON/SCHNEIER, 2; MAYER-SCHÖNENBERGER/PILZ/REISER/SCHMÖLZER, 65; Gisela MEISTER/Monika HORAK, Risikoanalyse für Chipkartensysteme, in: Albert GLADE/Helmut REIMER/Bruno STRUIF (Hrsg.), Digitale Signatur und sicherheitssensitive Anwendungen, Braunschweig/Wiesbaden 1995, 232 ff.

84 BIESER/KERSTEN, 50; MAYER-SCHÖNENBERGER/PILZ/REISER/SCHMÖLZER, 65, 126.

85 *Persönliche Identifikationsnummer;* STEINMANN, 3.

alle möglichen Passwortvarianten durchprobiert werden, oder mittels einer Wörterbuchattacke, bei der sämtliche Wörter eines elektronischen Wörterbuchs durchprobiert werden, ermittelt werden.[86] Im Gegensatz zu Softwaresigniereinheiten können Hardwaresigniereinheiten aber immerhin erlauben, eine bestimmte maximale Anzahl misslungener Versuche festzulegen, nach denen die Signierfunktion gesperrt wird.

69 Wird das Passwort über die normale Tastatur des Computers eingegeben, so besteht im Weiteren das Risiko, dass die Eingabe durch bösartige Software (Viren, etc.) mitprotokolliert wird. Auch der Einsatz eines Tokens nützt diesfalls nur wenig, weil diesem durch die bösartige Software später eine PIN-Eingabe vorgetäuscht werden kann, wodurch ohne Interaktion des Opfers eine Signatur erzeugt werden kann.[87] Zur Erfüllung hoher Sicherheitsbedürfnisse sind derartige Lösungen daher ungeeignet. Um das Mitprotokollieren von Tastatureingaben zu verhindern, muss der Kartenleser oder das Token vielmehr unabhängig von der PC-Tastatur aktiviert werden können. Kartenleser etwa lassen sich dazu mit einer eigenen Tastatur ausstatten.[88]

4. Biometrie

70 Durch die geschilderten, auf Besitz und Wissen basierenden Systeme kann nicht verhindert werden, dass der Inhaber des Tokens dieses zusammen mit dem Passwort weitergibt,[89] oder dass dieses von einer Drittperson bei der Eingabe ausgespäht wird. Die Nichtabstreitbarkeit ist damit im Prinzip nicht gewährleistet.[90]

71 Erst eine Prüfung anhand nicht übertragbarer, *biometrischer Merkmale des Signierschlüsselhalters* wie etwa Fingerabdruck, Unterschrift, Eigenarten der Stimme oder der Iris stellt sicher, dass wirklich nur der berechtigte Inhaber das Token einsetzt.[91] Auch in diesem Fall muss natürlich die biometrische Prüfung durch das Token selbst oder zumindest durch ein vertrauenswürdiges Lesegerät durchgeführt wer-

---

86 Zur Wahl sicherer Passwörter etwa GOLLMANN, 20 ff.

87 Für die Beschreibung eines erfolgreichen derartigen Angriffs auf das Homebanking Computer Interface HBCI (hinten N 147) CHAOS COMPUTER CLUB, Fun with Internet Banking, http://pamphlet.ffm.ccc.de/b0t0m/ebanking.html; SIETMANN, Flankenschutz, 141. Eine Stellungnahme des ZKA findet sich bei ZKA, Informationen.

88 Man spricht von *Klasse-2-Kartenlesern*. Der deutsche *Zentrale Kredit-Ausschuss ZKA,* in dem die Spitzenverbände der deutschen Kreditwirtschaft vertreten sind, hat vier Klassen von Kartenlesern definiert. *Klasse-1-Kartenleser* weisen nur einen Einschubschacht für die Karte auf, allenfalls mit einer Leuchte, die Aktivität der Karte signalisiert. *Klasse-2-Kartenleser* weisen eine separate Tastatur auf (dazu hinten N 69). *Klasse-3-Kartenleser* integrieren eine gewisse Intelligenz, Firewall-Eigenschaften sowie ein separates Display; ALTMANN, 102; SCHULZKI-HADDOUTI, Karten, 274; SIETMANN, Flankenschutz, 141. *Klasse-4-Kartenleser* schliesslich weisen zusätzlich einen individuellen Signierschlüssel auf, welcher die durch sie erstellten digitalen Signaturen nebst dem Inhaber des eingeschobenen Tokens auch dem individuellen Terminal zuordnen lassen; Katrin KOLBE, Generationen von Chipkartenlesern, Das notwendige Zubehör für die digitale Signatur, http://www.heute.t-online.de/ZDFheute/artikel/0,1251,COMP-4099-4021,00.html.

89 Vgl. etwa PORDESCH/NISSEN, 564.

90 Ähnlich BEHRENS/ROTH, 327.

91 BÜLLINGEN/HILLEBRAND, 339; für eine Liste verfügbarer biometrischer Verfahren BEHRENS/ROTH, 328.

den, um zu verhindern, dass bösartige Software dem Token eine erfolgreiche Prüfung vorgaukelt.[92]

72 Tokens mit biometrischem Schutz des Signierschlüssels befinden sich derzeit in Entwicklung.[93] Ein Problem bildet die Grösse der biometrischen Referenzdaten, die auf dem Token abzuspeichern sind; dieses wird mit der steigenden Leistungsfähigkeit der Chips jedoch einfacher lösbar.[94] Weitere Bedenken bestehen hinsichtlich des Datenschutzes, der Anwenderakzeptanz sowie generell bezüglich der Sicherheit der Verfahren.[95]

5. Anforderungen an Anwender und Software

73 Signierhard- und -software stellt regelmässig um so höhere Anforderungen an den Anwender, je einfacher der eingesetzte Mechanismus ist. So muss etwa der Anwender einer Softwaresigniereinheit mit Antiviren- und Firewall-Software dafür sorgen, dass sein System virenfrei bleibt und gegen Hackerangriffe abgeschirmt wird. Weil Computerlaien mit dieser Aufgabe regelmässig überfordert sind, muss deren Rechner als unsichere Zone gelten.[96] Europäische Signaturgesetze verlangen daher vielfach den Einsatz von Hardwaresigniereinheiten mit vom Rechner unabhängiger Aktivierung.[97]

D. Schlüsselzertifizierung

1. Grundlagen

74 Der Einsatz digitaler Signaturen setzt voraus, dass die im Umlauf befindlichen Prüfschlüssel aus Sicht der auf die Signaturen vertrauenden Dritten *sicher ihren Haltern zugeordnet werden können*. Werden die Schlüssel via Internet übermittelt, so kann

---

92 Vorne N 69.

93 ROSSNAGEL, Signaturregelungen, 454; Dirk SCHEUERMANN/Scarlet SCHWIDERSKI-GROSCHE/Bruno STRUIF, Usability of Biometrics, in Relation to Electronic Signatures, GMD Report 118, http://www.gmd.de/publications/report/0118/Text.pdf, 47; WILDHABER, Market Analysis, Abschnitt «Future Developments». Zur Standardisierung vgl. etwa PROBST, 325; für einen interessanten Schweizer Prototyp, der auch als Signiereinheit dienen könnte etwa Stephan BETSCHON, Alles auf einer Karte, Biometrische Identifikation mit drahtloser Übertragung, NZZ Nr. 219, 21. September 2001, 81.

94 PROBST, 325.

95 So etwa Astrid ALBRECHT, zit. bei KREMPL, Finger, 62 f.; vgl. auch BÜLLINGEN/HILLEBRAND, 341 f.; Gunter LASSMANN, Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, Kriterienkatalog, TeleTrust Deutschland e.V., Arbeitsgruppe 6: Biometrische Identifikationsverfahren, 1998, http://www.teletrust.de/down/kritkat-1.zip; SCHULZKI-HADDOUTI, Karten, 276 f.; Richard SIETMANN, Geheimniskrämerei, Halten biometrische Erkennungssysteme, was sie versprechen?, c't 7/2000, 106 ff.; DERSELBE, Zukunftstechnik. Zum deutschen Projekt *BioTrusT* zur Erforschung der Akzeptanz und Nutzung von biometrischen Systemen BEHRENS/ROTH, 329 ff.; Christian THIEL, BioTrusT: Erfahrungen und Anforderungen aus Betreibersicht, DuD 6/2000, 351 ff.

96 Ähnlich auch OCHEL/WEISSMANN, 46.

97 Vgl. hinten N 386 und 537 ff.

der Empfänger einer Nachricht aber zunächst nicht sicher sein, wem der verwendete Prüfschlüssel wirklich gehört.[98]

75 Zur sicheren Zuordnung von Prüfschlüsseln zu Personen gibt es drei Verfahren: Erstens können die Schlüssel dem Empfänger signierter Nachrichten natürlich vorab physisch übergeben werden – man spricht von *Direct Trust –,* zweitens kann mit einem *Web of Trust* und drittens mit *Schlüsselzertifizierung (Hierarchical Trust)* gearbeitet werden.[99]

2. Web of Trust

76 Das Web of Trust ist ein Netz von Vertrauensbeziehungen, in dem Private, die ihrerseits über einen bereits beglaubigten Prüfschlüssel verfügen (so genannte *Introducer*) die Prüfschlüssel von Bekannten beglaubigen, d.h. durch ihre eigene digitale Signatur bezeugen, dass ein Schlüssel zu einer bestimmten Person gehört. Die Introducer ermöglichen damit anderen Bekannten, diesen Prüfschlüsseln zu vertrauen, obwohl sie deren Halter nicht kennen.[100]

77 Dies funktioniert in einem überschaubar grossen Anwenderkreis gut. Die Sicherheit wird jedoch beeinträchtigt, wenn der Kreis der Schlüsselhalter grösser wird und eine eventuelle Überprüfung der Zuordnung eines Schlüssels nicht mehr in Betracht kommt.[101]

78 Das am weitesten verbreitete Verschlüsselungs- und Signierprogramm auf Public-Key-Basis, *Pretty Good Privacy (PGP),* basiert auf einem Web of Trust.[102]

3. Zertifizierung

79 Bei der dritten und im Folgenden ausschliesslich betrachteten Variante wird das Problem der Zuordnung gelöst, indem die Zuordnung von Prüfschlüssel und rechtmässigem Halter[103] des zugehörigen Signierschlüssels durch eine für die Kommunikationspartner vertrauenswürdige dritte Partei *beglaubigt* wird. Man spricht von *Zertifizierung*.[104] Die dritte Partei wird gemeinhin *Zertifizierungsdiensteanbieter (ZDA),*

---

98 MERTES, 33; vorne N 18 ff.

99 Eingehend NIESING/SCHMEH, 225 ff.

100 Eingehend NIESING/SCHMEH, a.a.O.; vgl. auch ALLENSTEIN, 21; KÜHN, 82 ff.; MENZEL, 64.

101 ALLENSTEIN, 21; MENZEL, 64; NIESING/SCHMEH, 227.

102 PGP ist für Privatanwender kostenlos erhältlich; http://www.pgpi.org. Zu PGP im Allgemeinen LUCKHARDT, PGP I-III; Thomas ROESSLER, PGP – «Kryptographie fürs Volk», DuD 7/1998, 377 ff.; Ingmar CAMPHAUSEN, Schlüsselzertifizierung mit PGP, DuD 7/1998, 382; vgl. auch C'T, PGP Key Certification Authority, http://www.heise.de/ct/pgpCA.

103 Hier wird der Begriff des Schlüsselhalters und nicht etwa der des -inhabers gebraucht, um das Wesen der Bindung zwischen Schlüssel und Halter zum Ausdruck zu bringen: Die Bindung ist – ähnlich dem Eigentum – bloss gedacht und nicht physischer Natur. Sie wird durch einen Schlüsselverlust oder -diebstahl nicht aufgelöst; vgl. etwa auch AMERICAN BAR ASSOCIATION, 44 f., wo der Begriff «to hold a key» verwendet wird (der Schlüsselhalter wird indessen als *Subscriber*, etwa «Abonnent», bezeichnet, was m.E. im Deutschen unpassend wäre.)

104 Näher Heinrich KERSTEN, Zertifizierung und Signaturgesetz, CR 12/1998, 780 ff., 781.

Certification Service Provider (CSP)[105] *oder Certification Authority (CA)*[106] genannt.[107]

80 Die Beglaubigung erfolgt in einem ebenfalls elektronisch übermittelten Dokument, das *Zertifikat* genannt wird. Auch dieses wird durch eine digitale Signatur, diejenige des Zertifizierungsdiensteanbieters, gegen Fälschungen gesichert.[108] Wohl aus der englischen Bezeichnung *digital ID* abgeleitet, wird das Zertifikat teilweise auch als *digitale Identität* bezeichnet. Meines Erachtens müsste hier jedoch genau genommen von einem *digitalen Identitätsausweis* oder von einer *digitalen ID* gesprochen werden.

81 Das Zertifikat enthält einige Daten zur Identifikation des Schlüsselhalters, den Prüfschlüssel, eine Seriennummer, den Namen des Zertifizierungsdiensteanbieters sowie meist einen Hinweis auf das so genannte *Certification Practice Statement (CPS)*.[109] In Letzterem dokumentiert der Zertifizierungsdiensteanbieter sein Vorgehen bei der Erstellung der Zertifikate (insbesondere wie die Identität des Schlüsselhalters überprüft wird). Eine sichere Identitätsprüfung kann etwa durch physisches Erscheinen bei einer *Registrierstelle* und Vorlegen eines amtlichen Dokumentes erfolgen.[110] Teilweise wird aber auch bloss überprüft, ob die angegebene E-Mail-Adresse tatsächlich dem Antragsteller gehört (durch Zusenden eines Passwortes auf diese Adresse, welches der Antragsteller dann wieder einzugeben hat).

82 Die Anschaffung eines Zertifikats mit Hardware kostet derzeit rund 150 Franken, sofern der Signierschlüssel auf einem Token gespeichert ist; für jedes Folgejahr sind erneut rund 50 Franken zu bezahlen.[111]

---

105 Vgl. etwa MLES Guide to Enactment, §§ 53 ff.

106 AMERICAN BAR ASSOCIATION, 35 ff.; GOLLMANN, 219.

107 In der Schweiz hat im Jahre 1998 mit der Swisskey AG ein erster Zertifizierungsdiensteanbieter mit öffentlichem Angebot seine Arbeit aufgenommen. Der Betrieb von Swisskey wurde jedoch auf Ende 2001 wieder eingestellt. Zu den Gründen hinten N 235 ff.

108 Eingehend NIESING/SCHMEH, 225.

109 AMERICAN BAR ASSOCIATION, 38 f.

110 Für ein Beispiel vgl. etwa DEUTSCHE POST SIGNTRUST, Online-Antrag, http://www.signtrust.de/index.php?menu=online_antrag, insbesondere Abschnitt «Vorgehensweise im Detail» m.H.

111 REGULIERUNGSSTELLE FÜR TELEKOMMUNIKATION UND POST, FAQ, http://www.regtp.de/tech_reg_ tele/start/in_06-02-03-00-00_m/index.html, Frage 7.

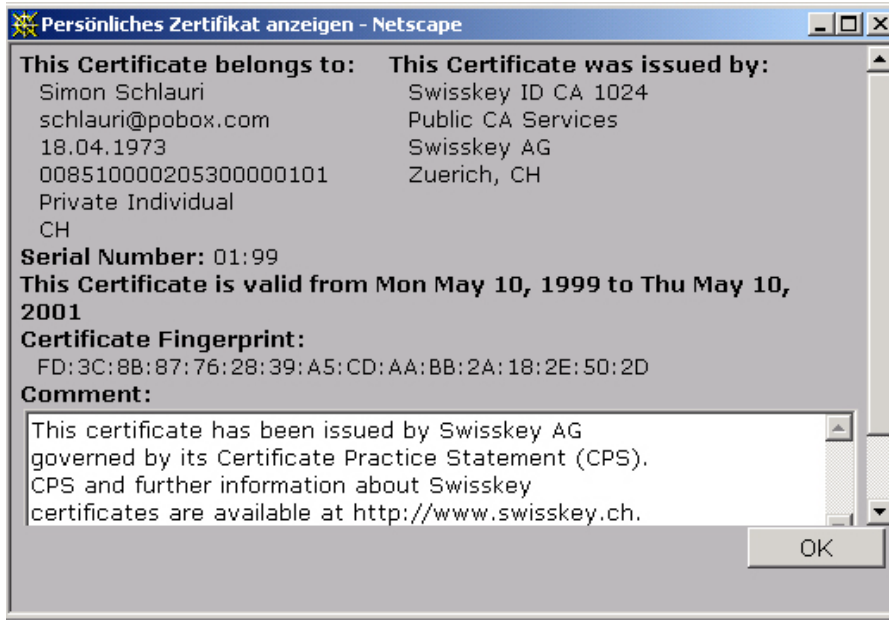

Abbildung 3: Ein Zertifikat von Swisskey AG, angezeigt in Netscape Communicator.

Die Gesamtheit aller im Zusammenhang mit der Zertifizierung eingerichteten Stellen wird *Public-Key-Infrastruktur (PKI)*[112] oder *Sicherungsinfrastruktur*[113] genannt. 83

4. Veröffentlichung von Zertifikaten

Auf Wunsch des Signierschlüsselhalters kann sein Zertifikat in einer öffentlich über das Internet zugänglichen Liste *(Certificate Repository)*[114] veröffentlicht werden. Dies ist in erster Linie dann sinnvoll, wenn mit dem Zertifikat auch verschlüsselt werden soll, da das Zertifikat bei Signaturen regelmässig zusammen mit der signierten Nachricht versandt wird.[115] Schon heute beherrscht Standardsoftware wie etwa Netscape Communicator den automatischen Bezug von Zertifikaten aus einem Certificate Repository. Dazu kommt in der Regel das LDAP-Protokoll zur Anwendung.[116] 84

---

112 Etwa MENZEL, 62; OPPLIGER, 70.
113 So etwa MIEDBRODT, 29; ROSSNAGEL, Recht, 1819.
114 AMERICAN BAR ASSOCIATION, 28 f.
115 Hinten N 95.
116 *Lightweight Directory Access Protocol*; vgl. etwa die Ausführungsbestimmungen zur ZertDV, 2.12.5, Anforderung 2.

5. Ablauf von Zertifikaten

85 Zertifikate werden regelmässig mit einem *Verfalldatum* versehen, was erlauben soll, der technischen Entwicklung etwa durch Anheben der Schlüssellängen zu folgen.[117] Das Verfalldatum wird bei der Anzeige des Zertifikats durch die Signaturprüfeinheit regelmässig mit angezeigt.[118]

6. Sperrung von Zertifikaten

86 Im Falle der *Kompromittierung des Signierschlüssels*, d.h., wenn dieser in die Hände Dritter gelangt ist, oder etwa wenn ein Mitarbeiter ein Unternehmen verlässt und eine entsprechende Vertretungsberechtigung verliert, ist das entsprechende Zertifikat bereits vor seinem Ablauf *zu sperren*. Teilweise wird auch von *Widerruf* oder *Revokation* gesprochen.[119]

87 Kann ein Zertifikat gesperrt werden, so muss ein auf dieses vertrauender Dritter umgekehrt die Möglichkeit haben, ein Zertifikat zu einem bestimmten Zeitpunkt auf seine Gültigkeit hin zu überprüfen (dieses zu *validieren*).[120]

88 Üblicherweise veröffentlichen die Zertifizierungsdiensteanbieter hierzu auf dem Internet in regelmässigen Zeitabständen eine *Zertifikatsrücknahmeliste (Certification Revocation List, CRL)*, d.h. eine Liste der gesperrten Zertifikate mit Informationen über Sperrzeitpunkt und -grund. Diese wird ihrerseits digital signiert, um die Vertrauenswürdigkeit zu gewährleisten und herkömmlicherweise als Ganzes heruntergeladen, um auch Offline-Zertifikatsprüfungen zu ermöglichen.[121] Erfahrungsgemäss müssen jedoch jährlich rund 10 Prozent der ausgegebenen Zertifikate eines Anbieters vorzeitig gesperrt werden, was bei grösseren Anwenderzahlen sofort zu riesigen Datenmengen führt. Das CRL-System ist damit nicht beliebig skalierbar.[122]

89 Eine Alternative zum Download der gesamten CRL besteht jedoch mittlerweile in der Abfrage *einzelner* Zertifikate mittels des so genannten *OCSP-Protokolls*[123] oder des bereits erwähnten LDAP-Protokolls.[124] Deren Nachteil liegt allerdings darin,

---

117 AMERICAN BAR ASSOCIATION, 54 f.; Vgl. schon N 51; zu Schwierigkeiten im Zusammenhang mit Wurzelzertifikaten etwa GIESSMANN/SCHMITZ, 401 ff.; OCHEL/WEISSMANN, 48 f.

118 Vgl. etwa Abbildung 3 auf Seite 25.

119 Vgl. etwa AMERICAN BAR ASSOCIATION, 59 f.

120 ITU-T, Recommendation X.509, 16 ff.

121 Das Format von Sperrlisten ist gemäss dem X.509-Standard festgelegt (N 100 ff.); zum Ganzen etwa BETSCH/DEWITZ oder OCHEL/WEISSMANN. Das CRL-System wird durch Standardsoftware meist unterstützt, so etwa durch Netscape 6.1; vgl. die Hilfefunktion von Netscape 6.1, Abschnitt «Zertifikate, Bestätigung» (erreichbar über den Hilfe-Index der Software).

122 Dazu etwa auch ELLISON/SCHNEIER, 6.

123 *Online Certificate Status Protocol;* vgl. BERTSCH/DERWITZ, Abschnitt «Online-Prüfung mit OCSP». Das OCSP wird mittlerweile auch durch Standardsoftware wie Netscape 6.1 und eine Reihe von Zertifizierungsdiensteanbieteren unterstützt; vgl. etwa die Darstellung in der Hilfefunktion von Netscape 6.1, Abschnitt «Zertifikate, Bestätigung».

124 Ausführungsbestimmungen zur ZertDV, 2.12.6, Anforderung 7; vgl. auch vorne N 84.

dass zur Abfrage eine Online-Verbindung mit dem Server des Zertifizierungsdiensteanbieters aufgebaut werden muss.[125]

7. Wurzelzertifikat und Zertifizierungshierarchie

90 Der Prüfschlüssel des *Zertifizierungsdiensteanbieters*, der zur Überprüfung von dessen *Zertifikaten* eingesetzt wird, ist ebenfalls mit einem Zertifikat versehen. Weil dieses Zertifikat die Wurzel für sämtliche Zertifizierungen darstellt, die vom Anbieter ausgehen, spricht man von einem *Wurzel- oder Root-Zertifikat*.[126]

91 Zur Unterzeichnung des Wurzelzertifikats kann einerseits dieses selbst verwendet werden (selbstzertifiziertes oder *self-signed* Wurzelzertifikat; [127] diesfalls ist der Zertifizierungsdiensteanbieter selbst die oberste Stufe der Zertifikathierarchie), andererseits kann die Zertifizierung der Wurzelzertifikate auch durch eine spezielle Certification Authority, die *Root Certification Authority* (in der Folge *Root CA*), stattfinden. Damit wird der Zertifikathierarchie eine weitere Ebene hinzugefügt.

92 In beiden Fällen besteht aber mindestens ein letztes selbstzertifiziertes Wurzelzertifikat. Falls eine Root CA eingesetzt wird, existiert nur *ein* Wurzelzertifikat, falls nicht, setzt jede Certification Authority ihr eigenes ein. Die zweite Lösung ist für den Empfänger digitaler Signaturen mit mehr Aufwand verbunden, weil er mehrere Wurzelzertifikate verwalten muss; dies kann durch so genannte Kreuzzertifizierung (dazu sogleich N 97) etwas gelindert werden.[128]

93 Weil das Wurzelzertifikat nicht seinerseits durch ein übergeordnetes Zertifikat gesichert ist, muss seine Authentizität anderweitig gewährleistet werden. Oder wie GOLLMANN sagt: "At the end, cryptographic protection has to be anchored in a non-cryptographic base."[129] Die Authentizität des Wurzelzertifikats kann etwa durch Publikation von dessen Hashwert in gedruckter Form erreicht werden, etwa in einem Periodikum oder einer Tageszeitung oder bei einer staatlichen oder staatlich anerkannten Root CA in einem Amtsblatt.

94 Immer öfter enthält E-Mail- und Browsersoftware schon von Haus aus eine ganze Reihe von Wurzelzertifikaten, womit sie ohne weiteren Konfigurationsaufwand (d.h. Importieren von Wurzelzertifikaten) in der Lage ist, digital signierte Nachrichten oder Webseiten zu überprüfen. Dies entlastet den Anwender jedoch grundsätzlich nicht davon, den Hashwert des jeweils eingesetzten Wurzelzertifikats zu überprüfen, denn es sind Angriffe denkbar, bei denen einer Signaturprüfeinheit neue Wurzelzertifikate hinzugefügt werden, um dem Anwender eine gültige Signatur vorzuspiegeln.

---

125 Zu weiteren Lösungen etwa BERTSCH/DEWITZ, Abschnitte «Verringerung des Datenaufkommens» und «Online-Prüfung mit OCSP».

126 Die AMERICAN BAR ASSOCIATION, 37, spricht von einem *Certification Authority Certificate*.

127 Vgl. etwa ITU, Recommendation X.509, 21.

128 ROSSNAGEL, Recht, 1820.

129 GOLLMANN, 220; GIESSMANN/SCHMITZ, 401, sprechen von einem *Vertrauensanker*.

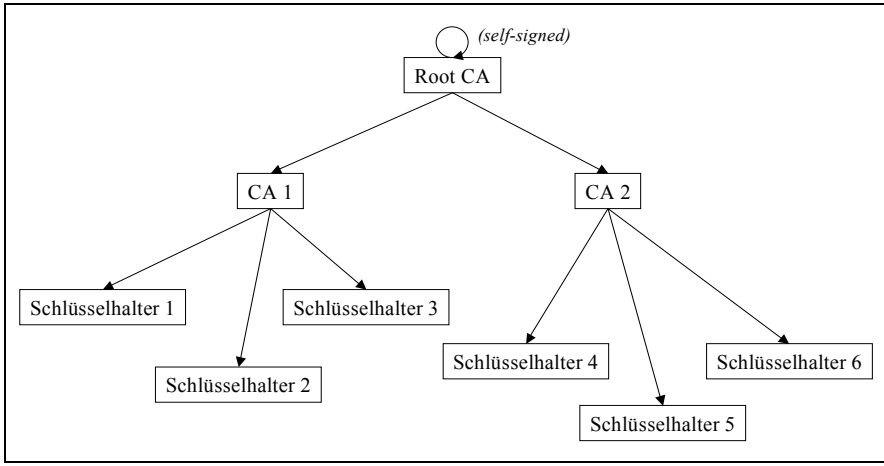

Abbildung 4: Wurzelzertifizierung mit Root CA.

95 Die gesamte Zertifikatkette der Zertifikathierarchie mit Ausnahme des Wurzelzertifikats wird bei einer nach dem üblicherweise eingesetzten S/MIME-Standard[130] codierten digitalen Signatur als Attachment an die signierte Mitteilung angehängt. So kann der Empfänger jede Signatur überprüfen, sofern diese nur durch einen Zertifizierungsdiensteanbieter innerhalb des Vertrauens-Baumes zertifiziert wurde, dessen Wurzelzertifikat er besitzt, und es ist nicht nötig, dass der Empfänger das Zertifikat des Absenders auf separatem Weg beschafft.[131]

96 Wenn eine Zertifizierung der Wurzelzertifikate einer staatlichen oder staatlich anerkannten Root CA vorbehalten bleibt und nur unter bestimmten Voraussetzungen erteilt wird, beispielsweise der Beachtung minimaler Sicherheitsstandards für die Ausstellung der Nutzerzertifikate, kann ein «Baum» von vertrauenswürdigen Zertifizierungsdiensteanbietern aufgebaut werden, deren Zertifikate von allen Beteiligten anerkannt werden.[132]

8. Kreuzzertifizierung

97 Nebst der Schaffung einer Root CA besteht auch die Möglichkeit, dass sich unabhängige Zertifizierungsdiensteanbieter gegenseitig Zertifikate ausstellen. Damit wird aus der Sicht des Anwenders eine weitere Ebene von Zertifikaten hinzugefügt. Man spricht von *Kreuzzertifizierung* oder *Cross-Certification*.[133] Mit Kreuzzertifizierung

130 Dazu hinten N 130, insbesondere FN 171.
131 Vgl. etwa KÜHN, 81 f.
132 Dem entspricht die Regelung des deutschen Signaturgesetzes bei der freiwilligen Akkreditierung von Zertifizierungsdiensteanbietern; ROSSNAGEL, Fortentwicklung, 2.3; hinten N 404, insbesondere FN 605.

kann erreicht werden, dass Zertifikate der einen Zertifikathierarchie von den Anwendern der anderen Hierarchie anerkannt werden können, ohne dass diese das Wurzelzertifikat des Zertifizierungsdiensteanbieters des einen Netzwerkes besitzen müssen.

98 Es können verschiedene Beschränkungen der Wirkung von Kreuzzertifikaten vorgesehen werden. So verhindert etwa eine Beschränkung der Länge der entstehenden Zertifikatsketten, dass ein Zertifizierungsdiensteanbieter, der ein Kreuzzertifikat für einen anderen ausstellt, diesen auch in das Netzwerk eines Zertifizierungsdiensteanbieters integrieren kann, durch welchen er selbst schon kreuzzertifiziert wurde.[134]

99 Die Problematik der Kreuzzertifizierung liegt in erster Linie bei den möglichen Unterschieden zwischen den Zertifikationspraktiken[135] der Zertifizierungsdiensteanbieter. Nur zwischen Anbieter, die mehr oder weniger deckungsgleiche Zertifizierungspraktiken aufweisen, ist eine Kreuzzertifizierung sinnvoll.[136]

9. ITU-T Empfehlung X.509

a) Allgemeines

100 Die Standardisierungs-Sektion der *Internationalen Telekommunikations-Union (ITU-T)*[137] verabschiedet regelmässig Empfehlungen zur technischen Ausgestaltung von Kommunikationsmitteln.

101 Bei der *ITU-T Empfehlung X.509* handelt es sich um einen internationalen Standard, der einen Rahmen für Public-Key-Zertifikate sowie die entsprechenden Verzeichnisdienste definiert. Geregelt werden etwa Inhalt und Datenstrukturen von Zertifikaten, Attributzertifikaten[138] oder Certificate Revocation Lists.[139]

b) Inhalt eines Zertifikats

102 Nach der ITU-T Empfehlung X.509 handelt es sich bei einem Zertifikat um einen Daten-Record[140] mit folgenden Feldern:[141]

---

133 Zum Ganzen ITU, Recommendation X.509, 19f.; FOX, Cross-Zertifikat, 105; Volker HAMMER, Cross-Zertifikate verbinden, DuD 2/2001, 65ff.; RAMSAUER, 65f.

134 FOX, Cross-Zertifikat.

135 Vgl. N 81.

136 FOX, Cross-Zertifikat, 105; zum ganzen auch OCHEL/WEISSMANN, 48.

137 Dazu etwa KENNEDY/PASTOR, 30 ff.

138 Dazu hinten N 115.

139 ITU-T, Recommendation X.509, Summary.

140 D.h. um eine Datenstruktur mit mehreren Feldern von teils unterschiedlicher Länge und unterschiedlichem Datentyp; die Felder können ihrerseits wieder als Records aufgegliederte Daten enthalten (vgl. etwa das Feld *signature*, N 105).

141 Zum Ganzen ITU, Recommendation X.509, 12 ff.; FOX/MÜLLER, 165 ff.; MENZEL, 71 ff.; OCHEL/WEISSMANN, 45f.; vgl. auch die Ausführungsbestimmungen zur ZertDV, 2.9.1, Anforderung 2, sowie 2.9.2.

103 • *version:* Ganzzahlige Nummer von 0 bis 2 für die Versionen 1, 2 oder 3 des Standards. Der übrige Aufbau des Daten-Records[142] hängt von dieser Versionsnummer ab[143];

104 • *serialNumber:* Ganzzahlige, nur einmal vorkommende Seriennummer des Zertifikats;

105 • *signature:* ein Daten-Record mit Informationen über die verwendeten Algorithmen für Hash und Signatur;

106 • *issuer:* identifiziert den Zertifizierungsdiensteanbieter (natürlichsprachlicher Name);

107 • *validity:* Geltungszeit (Anfang[144] und Ende);

108 • *subject:* identifiziert den Signierschlüsselhalter (natürlichsprachlicher Name);

109 • *subjectPublicKeyInfo:* Daten-Record mit Information über den verwendeten Signieralgorithmus sowie dem eigentlichen Prüfschlüssel (Public Key);

110 • *issuerUniqueIdentifier:* optionaler Parameter zur weiteren Identifikation des Zertifizierungsdiensteanbieters im Falle von identischen natürlichsprachlichen Namen;

111 • *subjectUniqueIdentifier:* optionaler Parameter zur weiteren Identifikation des Signierschlüsselhalters im Falle von identischen natürlichsprachlichen Namen;

112 • *extensions:* Ein oder mehrere weitere Daten-Records, deren Ausgestaltung in der Empfehlung noch nicht festgelegt ist. Die einzelnen Records enthalten ein «critical»-Feld. Wenn die Prüfsoftware auf ein Zertifikat stösst, welches ihr unbekannte Extensions enthält, kann sie diese ignorieren, wenn das Feld nicht gesetzt ist. Ist das Feld gesetzt und die Software erkennt die Extension nicht, so ist das Zertifikat zurückzuweisen und die Überprüfung der Signatur ist gescheitert.[145] In den Extensions kann etwa ein Hinweis auf das Certification Practice Statement[146] des Ausstellers stehen oder die Angabe eines maximalen Transaktionswertes oder des Geltungsbereichs[147] eines Zertifikats.[148]

113 Die ganze Datenstruktur ist durch den Zertifizierungsdiensteanbieter digital signiert.[149]

---

142 Etwa die Zulässigkeit so genannter Extensions; dazu sogleich N 112.
143 OCHEL/WEISSMANN, 45.
144 Die Definition einer Anfangszeit ist eigentlich nicht sinnvoll, weil ein Signierschlüssel, wenn er zu irgend einem Zeitpunkt kompromittiert war, nicht wieder sicher werden kann.
145 ITU, Recommendation X.509, 13.
146 Vorne N 81.
147 Dazu etwa hinten N 534 ff.
148 ITU, Recommendation X.509, 19.
149 ITU, Recommendation X.509, 12.

c) Profile und Interoperabilitätsspezifikationen

X.509 bietet seit Version 3 viele Erweiterungsmöglichkeiten,[150] weshalb Einschränkungen des Standards nötig sind, sollen die verwendeten Programme interoperabel bleiben; man spricht hierbei von *Profilen* oder *Interoperabilitätsspezifikationen*.[151] 114

10. Attributzertifikate und Zertifikatsmodifikation

Ein *Attributzertifikat* ist ein Zertifikat, das nicht einen Prüfschlüssel enthält, sondern auf ein anderes (Haupt-)Zertifikat verweist, indem es etwa dessen Seriennummer und Aussteller aufführt. Das Attributzertifikat enthält zusätzliche Attribute des entsprechenden Signierschlüsselhalters (wie Vertretungsrechte u. dgl.).[152] Der Sinn von Attributzertifikaten liegt darin, dass sie unabhängig vom Hauptzertifikat für ungültig erklärt werden oder eine kürzere Geltungsdauer aufweisen können (auch nur wenige Stunden). So kann man etwa dann, wenn ein Signierschlüsselhalter für eine bestimmte Zeit ein Vertretungsrecht erhalten soll, diesem ein nur für diese Zeit gültiges Attributzertifikat ausstellen.[153] 115

Alternativ kann auch das Hauptzertifikat durch den Zertifizierungsdiensteanbieter *modifiziert* werden.[154] Eine mögliche Problematik besteht hier darin, dass ein Zertifikat nach dem Unterzeichnen verändert werden kann. Deshalb muss m. E. das verwendete Zertifikat von der Signatur umfasst sein. 116

E. Prüfen der Signatur

1. Grundlagen

Die Prüfsoftware prüft, ob Nachrichteninhalt, Prüfschlüssel und Signatur zusammenpassen. Wurde der Text seit dem Setzen der Signatur verändert, oder passen Signier- und Prüfschlüssel nicht, so schlägt diese Überprüfung fehl. Die Software zeigt dem Anwender das Prüfresultat durch ein Symbol an.[155] Marktübliche E-Mail-Software, die digitale Signaturen unterstützt, führt diese Prüfung normalerweise beim Empfang signierter Nachrichten automatisch durch. 117

---

150 Im Rahmen der Extensions; soeben N 112.

151 NIESING/SCHMEH, 229; Klaus KEUS, Auf dem schwierigen Weg zu einer europaweiten Verständigung für elektronische Unterschriften, http://www.bsi.de/literat/tagung/cebit01/elekunt.pdf.

152 Details bei ITU, Recommendation X.509, 58 ff. oder SigI A1 (Zertifikate), 85 ff. Vgl. auch HAMMER, 101 und BIZER/MIEDBRODT, 148.

153 Vgl. etwa Begründung zum deutschen SigG 01, 23.

154 Vgl. etwa Ausführungsbestimmungen zur ZertDV, 2.10.3.5.

155 MERTES, 36 ff.; vgl. auch die Abbildung 5 auf Seite 32.

Betreff: Test
Datum: Sat, 03 Mar 2001 13:18:31 +0100
Von: Simon Schlauri <schlauri@pobox.com>
An: René Muster <rene.muster@test.ch>

<Dies ist der Inhalt der Mitteilung.>

Unterzeichnet

Abbildung 5: Eine digital signierte Nachricht, angezeigt von Netscape Messenger.

118 Die Gesamtheit der zum Überprüfen einer Signatur eingesetzten Soft- und Hardware wird *Signaturprüfeinheit* oder *Prüfeinheit* genannt. Es handelt sich hier üblicherweise um einen herkömmlichen Computer; der Einsatz eines kryptographischen Tokens ist unnötig, weil der Prüfschlüssel ja öffentlich ist.

2. Vergleich der Hashwerte

119 Genau besehen erstellt die Software des Empfängers zum Prüfen der Signatur einerseits den Hashwert der übermittelten Nachricht und ermittelt andererseits mittels des Prüfschlüssels den zuvor durch den Absender mit dessen privaten Schlüssel verschleierten Hashwert. Stimmen die beiden Hashwerte überein, so ist die Signatur *gültig*.[156]

3. Überprüfung der Zertifikate insbesondere

120 Im Weiteren ist die Gültigkeit der involvierten Zertifikate zu überprüfen, das Wurzelzertifikat sogar anhand eines nicht-digitalen Referenzwertes (z.B. seines publizierten Hashwertes).[157] Eine grosse Schwierigkeit liegt hierbei im fehlenden Know-how der Anwender oder in deren Bequemlichkeit. Die Signaturprüfeinheit sollte m.E. die Zertifikatsdaten oder zumindest Teile davon daher nicht nur auf Initiative des Anwenders hin und erst nach einigen Mausklicks, sondern bereits im Hauptfenster anzeigen.[158]

121 Die Abfrage der Gültigkeit von Zertifikaten über die Certificate Revocation List kann online und softwaregesteuert[159] sowie meist auch «von Hand» durch einen Besuch auf der Website des Zertifizierungsdiensteanbieters erfolgen. Um den Anwender zu entlasten, sollte die Signaturprüfeinheit die CRL bei jeder Signaturprüfung automatisch und ohne Benutzerinteraktion konsultieren; dies ist bei gängiger Software jedoch noch selten der Fall.[160]

---

156 Vgl. auch vorne N 48 ff.; eingehend HAMMER, 96 ff.
157 Vorne N 90 ff., 93.
158 Vgl. auch ELLISON/SCHNEIER, 4, 6 f.
159 Vorne N 85 ff.
160 Zur Frage, wie die Gültigkeit einer Signatur *nach dem Ablauf oder der Sperrung eines Zertifikats* geprüft werden kann hinten N 172 ff.

Sehr komplexe Probleme ergeben sich ferner bei einer Kompromittierung des Signierschlüssels des Zertifizierungsdiensteanbieters und einer Sperrung des Wurzelzertifikats; daher wird heute auf eine sehr hohe Sicherheit der entsprechenden Signierhardware Wert gelegt.[161] 122

4. Angriff durch Täuschung des Empfängers

Der Empfänger kann darüber getäuscht werden, welche Bereiche eines Dokumentes signiert sind. Problematisch ist dieser Aspekt besonders bei strukturierten, mit mehreren Signaturen versehenen Dokumenten.[162] Bei der Auswahl der Software ist daher darauf zu achten, dass jeweils das gesamte Dokument unterzeichnet wird bzw. bei einer nur teilweisen Unterzeichnung der Empfänger auf diesen Umstand hingewiesen wird. 123

Schliesslich ist es auch möglich, das Prüfsystem zu manipulieren.[163] Weil bei der Prüfung keine geheimen Daten (wie Signierschlüssel) zur Anwendung gelangen, läuft die Prüfung regelmässig auf einem herkömmlichen Computersystem, das gegen Angriffe nur schlecht abgeschirmt werden kann.[164] 124

F. Standards und Anwendungsbeispiele

Digitale Signaturen werden schon heute in einer Reihe von Anwendungen genutzt und durch eine Reihe von Standards geregelt. Im Folgenden soll ein kurzer Einblick in diese Bereiche gegeben werden. 125

1. Offene und geschlossene Benutzergruppen

Bei der Anwendung digitaler Signaturen ist zwischen *offenen* und *geschlossenen Benutzergruppen* zu unterscheiden. Nach BÜLLESBACH/RIESS/MIEDBRODT liegt eine geschlossene Benutzergruppe dann vor, wenn «es eine zentrale Stelle gibt, die Gesamtverantwortung für das von der Benutzergruppe verwendete System übernimmt und zwischen den Parteien (vorab begründete) rechtliche Beziehungen bestehen, durch die ihre Rechte und Pflichten geregelt sind.»[165] Ein Beispiel hierfür wäre etwa E-Banking. Offene Benutzergruppen hingegen basieren nicht auf bestehenden Rechtsbeziehungen, sondern entwickeln sich, indem eine Vielzahl von Nutzern ein bestimmtes Produkt oder eine unter einander kompatible Produktgruppe einsetzt.[166] 126

---

161 Zu dieser Problematik etwa GIESSMANN/SCHMITZ, 401 ff.

162 PORDESCH/NISSEN, 564.

163 Das Wurzelzertifikat kann besonders einfach angegriffen werden: Weil es bei den meisten Signiereinheiten möglich ist, mehrere Wurzelzertifikate gleichzeitig zu benutzen, könnte dem Empfänger einfach ein zusätzliches Wurzelzertifikat untergeschoben werden.

164 Vgl. schon N 118.

165 BÜLLESBACH/RIESS/MIEDBRODT, FN 5.

166 So bildet das World Wide Web eine riesige offene Benutzergruppe des HTML-Standards.

In offenen Benutzergruppen werden digitale Signaturen derzeit indessen nur selten eingesetzt.[167]

127 Ein Vorteil der vertraglichen Lösung liegt darin, dass durch sie bei tieferen Sicherheitsbedürfnissen auch Signaturen mit einem entsprechend tieferen Sicherheitsniveau eingesetzt werden können als dem vom Gesetzgeber vorgesehenen. Der Markt zerfällt hier daher in mehrere Segmente mit unterschiedlichen Anforderungen.[168]

128 Teilweise wird weiter zwischen geschlossenen und *semi-geschlossenen* Benutzergruppen unterschieden; eine semi-geschlossenes Benutzergruppe liegt vor, wenn alle Gruppenmitglieder untereinander kommunizieren können, während ein geschlossenes System nur die Kommunikation zwischen den Gruppenmitgliedern einerseits und der zentralen Stelle andererseits ermöglicht.[169]

2. Unterzeichnen von Dokumenten

a) E-Mail

129 Es gibt verschiedene Arten von Standards, Empfehlungen und «statements of common practice», die den E-Mail-Verkehr über das Internet regeln. Einige für den E-Mail-Verkehr eingesetzte Protokolle wurden bisher durch die Internet Engineering Task Force als Standards verabschiedet.[170] Andere haben sich mittlerweile auch ohne eine offizielle Standardisierung sehr weit verbreitet.

130 Der Einsatz von digitalen Signaturen und Public-Key-Verschlüsselung in E-Mail folgt üblicherweise den Standards *S/MIME*[171] oder *OpenPGP*[172]. Das wohl am weitesten verbreitete S/MIME wurde ursprünglich von RSA Security, Inc. entwickelt und 1999 durch die IETF standardisiert. Es basiert auf X.509-Zertifikaten und Signaturen[173], die gemäss MIME-Standard[174] als normale Attachments versandt werden, sodass Mail-Clients, die den Standard nicht unterstützen, die Nachricht dennoch anzeigen können.[175] OpenPGP basiert zwar auch auf MIME, verwendet aber Pretty-

---

167 BÜLLESBACH/RIESS/MIEDBRODT, 5; zu den Gründen hinten § 5.
168 HILLEBRAND/BÜLLINGEN, 83.
169 WILDHABER, Ende, 2.
170 Zu den Standards der IETF etwa Dirk FOX, Internet Standard, DuD 7/2000, 417.
171 *Secure Multipurpose Internet Mail Extensions*; es handelt sich um eine Erweiterung des *MIME*-Standards (dieser regelt das Format von an E-Mail-Nachrichten angehängten Dateien *[Attachments]*); zu MIME etwa http://www.oac.uci.edu/indiv/ehood/MIME/toc.html, insbesondere die Einführung zu Teil 1; zu S/MIME vgl. RSA SECURITY, S/MIME Frequently Asked Questions, http://www.rsasecurity.com/standards/smime/faq.html.
172 IMC, Abschnitt «About the Protocols»; vgl. auch Marco THORBRÜGGE, Sicherheit schlüsselfertig, PC Professionell 2/2001, http://www.zdnet.de/internet/artikel/sw/200102/safemail01_00-wc.html, Abschnitt «PGP und S-Mime: zwei Arten von Vertrauen».
173 Vorne N 100 ff.
174 Soeben FN 171.
175 IMC, Abschnitt «About the Protocols».

Good-Privacy-Zertifikate.[176] OpenPGP wurde durch die IETF ebenfalls standardisiert.[177] S/MIME und OpenPGP sind untereinander nicht kompatibel.[178]


```
--------------ms82279C06EE8EC1A0EEDE8694
Content-Type: text/plain; charset=iso-8859-2
Content-Transfer-Encoding: 8bit

<Inhalt der Mitteilung>

--------------ms82279C06EE8EC1A0EEDE8694
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: Kryptographische Unterschrift mit S/MIME

MIIIVwYJKoZIhvcNAQcCoIIISDCCCEQCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCC
Bk8wggPOMIIDN6ADAgECAgIBmTANBgkqhkiG9w0BAQQFADBwMQswCQYDVQQGEwJDSDEUMBIG
A1UEChMLU3dpc3NrZXkgQUcxGzAZBgNVBAsTElB1YmxpYyBDQSBTZXJ2aWNlczEQMA4GA1UE
BxMHWnVlcmljaDEcMBoGA1UEAxMTU3dpc3NrZXkgSUQgQ0EgMTAyNDAeFw05OTA1MTAwOTQ0
MjZaFw0wMTA1MTAwOTQ0MDBaMIGbMRswGQYDVQQKExJQcml2YXRlIEluZGl2aWR1YWwxHjAc
(…)
Sr0/gxdZ0cumn5cIpmqijo+umTBSBgkqhkiG9w0BCQ8xRTBDMAoGCCqGSIb3DQMHMA4GCCqG
SIb3DQMCAgIAgDAHBgUrDgMCBzANBggqhkiG9w0DAgIBQDANBggqhkiG9w0DAgIBKDANBgkq
hkiG9w0BAQEFAASBgCzV4FO3J6CufFBrWT7sLp8HdcAFlNk+flF/USq4qy9rKQV1rhsZzj18
ZrpG6hK7ms6mu7n9jrMKCPfAIahS1ppVwLbRjJb4y/vt4GIXqrNPrquWMsxUs/r2L7FLH+gx
mTAGrmKqkJkQREaPpSyWlolfl/3gH4B0raQvz9MXHDir
--------------ms82279C06EE8EC1A0EEDE8694--
```


Abbildung 6: Eine gemäss S/MIME-Standard signierte E-Mail-Nachricht.[179]

Obwohl es grundsätzlich möglich ist, Mail-Clients zu schreiben, die mehrere Standards zugleich verstehen, unterstützen derzeit einige bedeutende Produzenten solcher Software ausschliesslich S/MIME (etwa AOL/Netscape und Microsoft) und andere ausschliesslich PGP/MIME (etwa Qualcomm), sodass der Markt in zwei Segmente gespalten ist, die untereinander digitale Signaturen und Verschlüsselung nicht einsetzen können.[180] Diese Situation ist der Verbreitung digitaler Signaturen und der Verschlüsselung im Internet-Mailverkehr nicht eben förderlich. 131

176 Zu PGP vorne N 78 ff.

177 NIESING/SCHMEH, 229.

178 Eine (allerdings ziemlich technische) Übersicht über verfügbare Standards geben etwa Jörg SCHNEIDER/Martin BARTOSCH, Kryptographie-Standards und ihre APIs, Übersicht aus dem Blickwinkel des Anwendungsentwicklers, DuD 7/2000, 392 ff.

179 Die Nachricht besteht aus zwei Blöcken von MIME-Verwaltungsdaten: aus dem (lesbaren) Inhalt der Mitteilung (oberer Teil) sowie den nur computerlesbaren Daten von Signatur und Zertifikat als Attachment (unterer Teil; gekürzt). Vgl. auch Abbildung 5 auf Seite 32, die zeigt, wie eine derartige Nachricht dem Benutzer durch die Anwendungssoftware angezeigt wird.

180 NIESING/SCHMEH, 230 f.; Marktübersichten über Mail-Software mit Hinweisen auf deren S/MIME bzw. OpenPGP-Fähigkeiten findet sich etwa bei Jo BAGER/Patrick BRAUCH/Johannes ENDRES, E-Postboten am Start, E-Mail-Programme für Windows, Mac OS und Linux, c't 10/2001, 164 ff. oder bei Olaf PURSCHE, Alternativen: Für jeden Geldbeutel, PC Professionell 2/2001, http://www.zdnet.de/internet/artikel/sw/200102/safemail05_00-wc.html.

132 Hinzu kommt, dass die Standards teilweise noch zu offen definiert bzw. fehlerhaft umgesetzt sind, sodass sich Produkte unterschiedlicher Hersteller nicht verstehen, obwohl sie die gleichen Standards unterstützen.[181]

b) Electronic Data Interchange

133 *UN/EDIFACT (United Nations Rules for Electronic Data Interchange for Administration, Commerce and Transport)* ist eine Zusammenstellung von international anerkannten Standards und Richtlinien für den elektronischen Austausch von Daten, insbesondere im Zusammenhang mit dem Handel mit Gütern und Dienstleistungen zwischen unabhängigen automatisierten Informationssystemen.[182] UN/EDIFACT wurde 1987 durch die UN Economic Commission for Europe (UNECE) verabschiedet und wird laufend nachgeführt.[183] Der Standard ist derzeit die einzige weltweite und branchenübergreifende Norm für EDI und in stetiger Verbreitung begriffen. Zur Absicherung von UN/EDIFACT-Nachrichten können ebenfalls digitale Signaturen eingesetzt werden.

c) Form Signing

134 Sollen Daten über den WWW-Dienst eingegeben werden *(WWW-Formulare)*, so können die für E-Mail und EDI bestehenden Mechanismen nicht eingesetzt werden. Netscape Communications hat jedoch bereits 1997 eine Technologie eingeführt, die den Einsatz digitaler Signaturen auch hier zulässt; man spricht von *Form Signing*.[184]

135 Dem Anwender wird hierzu nach der Eingabe der Daten in ein Formular durch ein so genanntes JavaScript-Programm[185] der zu signierende Text präsentiert (etwa der Text einer Bestellung) mit der Aufforderung, das Zertifikat auszuwählen und das Passwort zur Freigabe des Signierschlüssels einzugeben. Die signierten Daten werden hernach an den WWW-Server übermittelt, wo sie anhand des Zertifikats ausgewertet werden können.[186]

---

181 Gerald SPIEGEL, Gesicherter Umschlagplatz, S/MIME-fähige E-Mail-Programme und -Plugins, c't 26/1999, 160 ff.; vorne N 114.

182 UNECE, UN/EDIFACT Draft Directory, Part 1 Introduction, http://www.unece.org/trade/untdid/texts/d100_d.htm, Ziff. 26; zum Ganzen etwa KILIAN/HEUSSEN-KILIAN, 23; vgl. auch GUT/WILDHABER; KILIAN, 606 ff.; zum Einsatz von EDI im Bereich E-Government BJ, Projektskizze GovLink, 1 ff.

183 KILIAN/HEUSSEN-KILIAN, 23 N 3.

184 NETSCAPE COMMUNICATIONS, Financial Institutions and Merchants (…), http://home.netscape.com/newsref/pr/newsrelease552.html; Netscape Communications, Netscape Form Signing, Sign Web Transactions as Easily as Paper Documents, http://developer.netscape.com/tech/security/formsign/formsign.html.

185 JavaScript ist eine Programmiersprache für kleine Programme, die durch die WWW-Clientsoftware während des Surfens heruntergeladen und ausgeführt werden können. Der Programmcode wird in normale HTML-Seiten eingebettet; vgl. etwa NETSCAPE COMMUNICATIONS, JavaScript Guide, http://home.netscape.com/eng/mozilla/3.0/handbook/javascript oder MOZILLA.ORG, JavaScript, http://www.mozilla.org/js.

186 Für ein Anwendungsbeispiel OBERHOLZER, EBPP, 127 ff., 129.

Der Vorteil dieses Vorgehens gegenüber signierter E-Mail liegt in der Form der eingegebenen Daten: Der Anwender gibt diese in eine vordefinierte Maske ein, worauf sie im EDV-System des Anbieters gleich elektronisch weiterverarbeitet werden können. Beim Versand von Information über E-Mail hingegen ist regelmässig ein menschlicher Eingriff nötig, weil die eingegebenen Daten nicht maschinenlesbar strukturiert sind. 136

d) Code Signing

Code Signing oder *Object Signing* ist eine Technik, die es erlaubt, Computerprogramme bzw. Teile davon (Objekte) mit digitalen Signaturen zu versehen, wodurch deren Verseuchung durch Viren sowie das Unterschieben trojanischer Pferde verhindert werden soll, was eine gefahrlose Verbreitung über das Internet ermöglicht.[187] Code Signing kann – nebst der Unterzeichnung normaler Software – etwa für WWW-Inhalte in den Sprachen Java[188], JavaScript[189] oder MacroMedia Flash[190] eingesetzt werden oder bei Treiberprogrammen für Betriebssysteme, die oftmals über das Internet aufdatiert werden. Code Signing wird regelmässig aus rein technischen Gründen und nicht zum Austausch juristisch relevanter Willenserklärungen eingesetzt; es hat damit höchstens mittelbare Auswirkungen auf den Rechtsverkehr. 137

3. Digitale Signatur als digitaler Ausweis

a) Allgemeines

Das Signieren von Nachrichten, Formularinhalten und Programmcode ist indessen nicht die einzige mögliche Anwendung digitaler Signaturen. Nicht minder wichtig ist deren Einsatz zu reinen Authentifikationszwecken, d.h. als *digitaler Ausweis*[191]: Der Schlüsselhalter – es kann sich dabei sowohl um einen Kunden (Client-Seite) als auch um einen Anbieter (Server-Seite) handeln – kann sich mit seiner digitalen Signatur über das Internet bei einer Gegenstelle sicher authentifizieren. 138

Obwohl der Schlüsselhalter keine zu signierenden Daten zu Gesicht bekommt, handelt es sich technisch gesehen auch hier um das Unterzeichnen eines Datenpaketes: Unterzeichnet werden ein kleines Datenpaket *(Token)* oder bestimmte Befehle, die an die Gegenstation gesandt werden.[192] Durch einen Sequenzzähler oder das Versehen des Tokens mit Zeitinformationen werden Doppeleinreichungen *(Replay Attacks)* vermieden. 139

---

187 Dazu etwa VERISIGN, Code Signing Digital IDs, http://www.verisign.com/products/signing/index.html.

188 Eine Programmiersprache für plattformunabhängige Programme, die auch im Internet oft Verwendung findet; vgl. etwa SUN MICROSYSTEMS, Java Technology, http://www.sun.com/java.

189 Vgl. soeben N 135.

190 Eine weit verbreitete proprietäre Sprache zur Beschreibung von Internet-Seiten; dazu http://www.macromedia.com.

191 Zum Begriff schon vorne N 80.

192 SIETMANN, Flankenschutz, 140.

140 Wird eine Signatur zu reinen Authentifikationszwecken eingesetzt, so kann allerdings die Nichtabstreitbarkeit nicht gewährt werden: Meldet sich etwa ein Anwender mit einer digitalen Signatur bei einem ein E-Banking-System an, so hat die Bank hernach nur das signierte Token als Beweismittel in der Hand und kann mithin nur die Anmeldung beweisen.[193] Die einzelnen Transaktionsaufträge hingegen werden nur durch das System der Bank aufgezeichnet, nicht aber durch den Kunden signiert, was Manipulationen ermöglicht, sofern das System der Bank nicht speziell abgesichert ist.

b) Einsatz als lokales Authentifizierungsmittel

141 Zunächst kann dieser Mechanismus selbstverständlich anstelle der gewohnten Kombination von Benutzerkennung und Passwort zur lokalen Anmeldung an einem Computer oder in einem lokalen Computernetzwerk eingesetzt werden. Jeder Anwender erhält hierzu ein Token, das er zur Anmeldung in den Leser steckt und mit einem Passwort aktiviert.[194]

c) Virtual Private Networks

142 Seit einiger Zeit existieren Techniken, um lokale Computernetze über das Internet zu einem für die Anwender transparenten Gesamtnetz zusammenzuhängen, d.h. die Anwender können auf alle Ressourcen in diesem Netz so zugreifen, wie wenn diese sich in ihrem lokalen Netz befänden. Man spricht von *Virtual Private Networks (VPNs)*.[195] Vertraulichkeit der Kommunikation und Authentizität der beteiligten Rechner werden dabei regelmässig durch Public-Key-Kryptographie gewährleistet. Wie beim Code Signing handelt es sich auch hier um eine rein technische Anwendung mit höchstens mittelbarer Bedeutung für den Rechtsverkehr.

d) Server-Authentifizierung

143 Netscape Communications entwickelte bereits im Jahre 1994 die so genannte *Secure-Socket-Layer-Schnittstelle (SSL)*, die basierend auf Public-Key-Kryptographie Ver-

---

193 SIETMANN, Flankenschutz, 141.

194 Ein kurzer Überblick über die sich bei derartigen Anwendung stellenden Schwierigkeiten findet sich etwa bei Paul D. REIGROTZKY, Smartcard und PKI erfolgreich eingesetzt, Betriebsorganisatorische Implementation einer PKI am Beispiel einer Bank, Digma 2/2001, 78 ff. Microsoft Windows XP Server enthält beispielsweise von Haus aus Mittel zur Verwaltung von Zertifikaten, die unter anderem für die lokale Authentifizierung eingesetzt werden können; Patrick GRABER/Greg SUTTER, PKI in Windows Whistler, Version 1.0, 17. September 2001, http://www.itrust.ch/deutsch/articles/PKI_Windows_Whistler_V10.pdf; vgl. auch die Windows-Hilfe. Man spricht von *Single Sign-on (SSO)*, wenn diese Anmeldung nur einmal beim Systemstart zu geschehen hat und danach für alle eingesetzten Softwareprodukte gültig ist, was den umständlichen und supportintensiven Einsatz mehrerer Passwörter vermeidet. Viele Single-Sign-on-Lösungen basieren auf digitalen Signaturen, es existieren aber auch auf der herkömmlichen Kombination von Benutzerkennung und Passwort basierende Programme; vgl. etwa Reto GRÜNENFELDER, Single Sign-on: Anmeldung genügt, Digma 2/2001, 35 ff.; kritisch zur Sicherheit von SSO-Systemen ELLISON/SCHNEIER, 7.

195 Dazu etwa Daniel BACHFELD, Sicheres Netz im Netz, Der Aufbau von Virtual Private Networks, c't 17/2001, 164 ff.

schlüsselung und sichere Identifikation von WWW-Servern gegenüber Clients ermöglicht.[196] SSL setzte sich im WWW als Sicherheitsstandard durch (derzeit in der dritten Version). Es gehört heute zum Repertoire jedes WWW-Servers, der sichere Dienste anbietet und wird durch alle marktüblichen Browserprogramme unterstützt.[197]

e) Client-Authentifizierung

144 Soll nicht der Server gegenüber dem Client, sondern der Client gegenüber dem Server identifiziert werden, so spricht man von *Client-Authentifizierung*. Hierbei werden Zertifikat und Signierschlüssel auf dem Client eingerichtet. Beim Aufruf der Webseite erscheint ein Dialogfeld, welches den Anwender zur Auswahl des einzusetzenden Zertifikats und zur Eingabe des Passworts zur Freigabe des Signierschlüssels auffordert.

145 Client-Authentifizierung mittels digitaler Signaturen wird heute prinzipiell schon durch die marktüblichen Browser unterstützt (als Teil des genannten SSL-Standards). Aufgrund technischer Schwierigkeiten vor allem bei der Installation und Integration sicherer Kartenleser in die Browser wird bisher jedoch oftmals separate Software eingesetzt.[198]

f) E-Banking insbesondere

146 Zur Server-Authentifizierung finden digitale Signaturen im E-Banking schon seit jeher Verwendung, Client-Authentifizierung allerdings wird noch selten eingesetzt. Die UBS AG führte im Jahr 2000 mit der UBS Internet Card einen ersten Pilotversuch mit auf digitalen Signaturen basierender Client-Authentifizierung durch.[199] Dabei wurde ein Klasse-1-Kartenleser eingesetzt. Etwas später folgte die Post mit ihrem Finanzdienstleistungsportal YellowNet, wobei allerdings nur unsichere[200] Softwaresiniereinheiten zum Einsatz kamen.[201]

147 In Deutschland wurde im Namen der Spitzenverbände der Kreditwirtschaft im Jahre 1997 das so genannte *Homebanking Computer Interface (HBCI)* entwickelt, ein Standard zur Client-Authentifizierung und Unterzeichnung von Transaktionen beim E-Banking.[202] HBCI wird durch marktübliche Finanzbuchhaltungs-Software wie

---

196 BÜLLESBACH/RIESS/MIEDBRODT, 2; GOLLMANN, 232 ff.; MENZEL, 44 f.; vgl. auch NETSCAPE COMMUNICATIONS, Product Security, SSL 3.0 Specification, http://www.netscape.com/eng/ssl3.

197 Eine SSL-Verbindung wird regelmässig durch ein Schloss-Symbol am unteren Rand des Browser-Fenster angezeigt; wird dieses angeklickt, so erscheint das *Serverzertifikat*.

198 Dies war etwa bei der UBS Internet Card der Fall; dazu sogleich N 146.

199 Dazu etwa IBM ZURICH RESEARCH LABORATORY, News, The smart way to access UBS telebanking, http://www.zurich.ibm.com/news/00/telebanking.html.

200 Vorne N 64 ff.

201 Zum Einsatz digitaler Signaturen im E-Banking in der Schweiz vgl. etwa KNEUBÜHLER, 85.

202 Näheres auf der Website des Zentralen Kredit-Ausschusses, http://www.hbci-zka.de; vgl. auch ZENTRALER KREDIT-AUSSCHUSS, HBCI, Spezifikation, Download: Übersicht der HBCI-Spezifikationen, http://www.hbci-zka.de/spezifikation/2.html; SIETMANN, Flankenschutz, 140 ff.; SPINDLER, Bankenrecht I, Rz 83 ff.

Quicken unterstützt und ermöglicht, dass der Kunde seine Transaktionen nicht mehr über ein WWW-Interface eingeben muss, sondern nur mehr in seine Software. HBCI soll die bisher übliche PIN/TAN[203]-Anmeldung im Laufe der Zeit ersetzen. Derzeit basiert HBCI je nach Ausgestaltung auf symmetrischer oder asymmetrischer Kryptographie. Signierschlüssel können auf einem kryptographischen Token oder einer Diskette gespeichert werden.[204]

148 Als neuere Entwicklung ist das so genannte *Electronic Bill Presentment and Payment (EBPP)* zu nennen. Aus der Sicht des Kunden bietet EBPP einen zentralen Anlaufpunkt, bei dem an ihn gerichtete Rechnungen zusammenlaufen, von wo aus er Rechnungen stellen oder die Bezahlung durchführen und den Eingang von Zahlungen überwachen kann. Das System richtet sich primär an Geschäftskunden. Auch bei EBPP sollen digitale Signaturen Verwendung finden, so basiert eine von OBERHOLZER demonstrierte EBPP-Lösung auf Form Signing.[205] WILDHABER erwartet aufgrund der nun in Kraft tretenden Signaturgesetze in den Jahren 2002 und 2003 ein namhaftes Wachstum dieses Angebotes.[206]

149 Schliesslich ist auf Zahlungssysteme für den Internet-Zahlungsverkehr hinzuweisen. So basieren etwa *Secure Electronic Transaction (SET)* – ein System für den sicheren Einsatz von Kreditkarten über das Internet – und *ECash* – ein auf so genannten kryptographischen Einweg-Token basierendes System zur Bezahlung von Klein- und Kleinstbeträgen – auf digitalen Signaturen.[207] Eine breitere Markteinführung solcher Systeme erscheint indessen vorderhand ziemlich unwahrscheinlich.

4. Digitale Signatur im M-Commerce

150 Mit der Entwicklung des *WAP*-Standards[208] und insbesondere der Versteigerung der Lizenzen für die *UMTS*-Frequenzbänder[209] verlagerte sich das Interesse in letzter Zeit mehr und mehr in Richtung der Nutzung des Internet über mobile Endgeräte. Während sich der WAP-Standard mangels Abwärtskompatibilität zum HTML-Standard[210], mangels ausreichender Übertragungskapazitäten und deswegen auch mangels wirklich sinnvoller Anwendungen bisher kaum über Nischenbereiche hinaus

---

203 Unter einer *TAN (Transaktionsnummer)* versteht man eine mit jeder neuen Authentifikation wechselnde Nummer. TANs werden in der Regel auf *Streichlisten* festgehalten.

204 Die unsichere Speicherung auf Diskette hat denn auch bereits zu erfolgreichen Angriffen geführt; SIETMANN, Flankenschutz, 141; vgl. auch vorne N 64 ff. und dort FN 87; zu den juristischen Implikationen dieser ungenügenden Sicherheit hinten N 734. Eine Marktübersicht über Homebanking-Software mit Hinweisen auf deren HBCI-Fähigkeiten findet sich etwa bei ALTMANN, 96 ff.

205 OBERHOLZER, EBPP, 127 ff., 129, 133; zur Marktentwicklung etwa Ivo CATHOMEN, Phönixe aus der Paynet-Asche, Alles Easy-Billy oder was?, NZZ Nr. 237, 12. Oktober 2001, 75; Peter RÁSONYI (pra.), Paynet lebt, NZZ Nr. 284, 6. Dezember 2001, 27; für Form Signing vorne N 134 ff.

206 WILDHABER, Market Analysis, Abschnitt «Details».

207 Eingehend dazu WEBER, Elektronisches Geld, 1 ff.

208 *Wireless Application Protocol;* ein 1998 lanciertes Protokoll zum Abruf von gegenüber HTML vereinfachten WWW-Seiten durch Mobiltelefone; eingehend http://www.wapforum.org.

209 *Universal Mobile Telecommunications System;* ein Standard für schnelle Datenübertragung über Mobilfunkstrecken; http://www.umts-forum.org.

etablieren konnte, werden die schnelleren Übertragungsraten von UMTS und die gleichzeitig erfolgende technische Entwicklung im Bereich der mobilen Endgeräte dazu führen, dass die meisten WWW-Inhalte auch mobil abrufbar werden. Damit öffnet sich ein weites Feld für Anwendungen, bei denen der Kunde in allen Situationen des täglichen Lebens spontan über das Internet Verträge abschliessen kann. Gemeinhin wird hier von *Mobile Commerce (M-Commerce)* gesprochen.[211]

151 Bemerkenswert ist dabei, dass sich das Mobiltelefon – weil meist nur durch eine Person genutzt – zu einem idealen Träger für Identifikationsmittel wie Signierschlüssel entwickeln könnte: Seit einiger Zeit wird daher daran gearbeitet, digitale Signaturen in Chips einzupflanzen, die in einen zusätzlichen Steckplatz[212] des Mobiltelefons passen *(Wireless Identification Module; WIM)* und eine sichere Identifikation des Anwenders im M-Commerce erlauben sollen.[213] Diese Technologie hat hier insbesondere den Vorteil der bequemeren Handhabung – die Eingabe der herkömmlichen Identifikationselemente (Benutzerkennung, PIN, Passwort) über eine Telefontastatur ist mühsam –, weshalb sie als Hoffnungsträger für die Verbreitung digitaler Signaturen in Verbrauchermärkten gilt.[214]

152 Zu beachten ist, dass die im Bereich herkömmlicher PC bestehenden Sicherheitsfragen (bösartige Software, die sich Zugriff auf einen Signierschlüssel oder ein Passwort verschaffen kann u. dgl.)[215] auch bei Mobiltelefonen stellen werden, sobald diese dem Anwender die Möglichkeit bieten, zusätzliche Software zu laden. Dies wird mit der Verschmelzung von Mobiltelefon und PDA aktuell.[216]

5. Identrus

153 Im Weiteren ist die 1998 gestartete *Identrus*-Initiative zu erwähnen. Identrus ist ein weltweites Joint Venture von Finanzinstituten,[217] die auf privater Basis eine Public-

---

210 *Hypertext Markup Langage;* die wichtigste Seitenbeschreibungssprache zur Gestaltung von WWW-Dokumenten.

211 Für das EU-Projekt *GNIUS (GSM Network for Improved access to Universal Services)*, das eine sichere, homogene Plattform für den Zugang zu Informations- und E-Commerce-Angeboten über unterscheidliche Zugangspunkte schaffen will vgl. Michael SCHMIDT, 'Genie' für den M-Commerce, EU-Projekt GNIUS für sicheren und zuverlässigen Mobile Commerce, c't 1/2002, 194 ff. Wie der Name sagt, setzt GNIUS allerdings noch nicht auf UMTS auf.

212 Mobiltelefone besitzen schon heute einen Steckplatz für das *SIM-Modul (Subscriber Identification Module)*.

213 Zur Bedeutung kabelloser Dienste für den E-Commerce etwa Stefan ENGEL-FLECHSIG, Radicchio – a Global Initiative for Security in Wireless E-Commerce, DuD 9/2000, 527; http://www.radicchio.org; vgl. auch die Website des MoSign-Projekts, http://www.mosign.de und dazu SPINDLER, Bankrecht I, Rz 95; KREMPL, Signaturen, 60; zur Sicherheit im M-Commerce etwa Michael SCHMIDT, Geld in der Luft, Wie sicher ist E-Commerce über Mobilfunk?, c't 9/2001, 222 ff.

214 SCHULZKI-HADDOUTI, Karten, 278 f.; ZEUNER, 67 f.

215 Vorne N 64 ff.

216 Vgl. N 57, insbesondere FN 65.

217 Beteiligt sind beispielsweise Citigroup, J.P. Morgan Chase & Co., die Deutsche Bank. Die Technologie wird etwa durch IBM und Compaq beigesteuert; IDENTRUS, Partners List, http://www.identrus.com/fi/partner-list.xml.

Key-Infrastruktur aufbauen. Ziel ist, im Geschäftsverkehr vertrauenswürdige elektronische Kommunikation zu ermöglichen.[218]

154 Die Filialen der beteiligten Finanzinstitute dienen als Registrierungsstellen, die Daten werden hernach an ein zentrales Rechenzentrum weitergeleitet, das die Zertifikate ausstellt. Im Weiteren besteht ein hierarchischer «Baum» von Verträgen mit Identrus auf einer ersten, Finanzinstituten auf einer zweiten und Unternehmen, welche die Signaturen schliesslich zum Verkehr untereinander einsetzen, auf einer dritten Stufe (diese Unternehmen dürften in der Regel auch Firmenkunden der Finanzinstitute sein). In den Verträgen wird die Haftung geregelt und es wird beispielsweise festgelegt, dass die Unternehmen Signaturen von anderen Unternehmen des Netzes anerkennen.[219] Die Finanzinstitute können für ihre Kunden Garantien bis zu einen gewissen Höhe abgeben (etwa für die Liquidität), wodurch die Vertrauenswürdigkeit der Zertifikate gesteigert wird, was gerade im internationalen Verkehr sehr sinnvoll sein kann.[220] Identrus-Zertifikate («Global IDs») sind innerhalb des gesamten Netzwerkes anerkannt. Der Einsatz von Identrus-Zertifikaten ausserhalb des Netzwerkes wird allerdings ausgeschlossen und jede Haftung hierfür abgelehnt.[221] Es handelt sich demnach im Prinzip um eine geschlossene Benutzergruppe.[222]

6. Swisscert

a) Allgemeines

155 Im Jahre 2001 stellte das Zürcher Unternehmen Swisscert AG ein System vor, das einerseits die teuren Registrierungsstellen überflüssig machen und andererseits die Flexibilität von Attributzertifikaten auf normale Zertifikate übertragen soll. Das System wird als Alternative zum herkömmlichen Modell einer Public-Key-Infrastruktur dargestellt. Es war Anfang Januar 2002 noch nicht operativ.[223]

b) Dezentrale Registrierung

aa) Überblick über die Funktionsweise

156 Die Swisscert-Lösung basiert auf kryptographischen Tokens, die mit einem Fingerabdrucksensor versehen sind und als «elektronische Registrierungsstelle» dienen. Der Schlüsselhalter kauft sich das Token bei einem beliebigen Händler und initiali-

---

218 Zum Ganzen die Website von IDENTRUS, http://www.identrus.com; vgl. auch MÜLLER/WILDHABER/GLAUS (insbesondere 2, 3); zur Marktentwicklung WILDHABER, Market Analysis, Abschnitt «Global PKI Systems»; vgl. auch SPINDLER, Bankrecht I, Rz 102.

219 MÜLLER/WILDHABER/GLAUS, 2.

220 MÜLLER/WILDHABER/GLAUS, 4 f.

221 IDENTRUS, Identity Certificate Policy, http://www.identrus.com/knowledge/pubs/Identrus_Certificate_Policy.pdf, 8.

222 WILDHABER, Ende, 2, spricht von einem *semi-geschlossenen System*, weil die Teilnehmer untereinander Nachrichten signieren können.

223 Die Informationen auf den folgenden Seiten stammen zum Teil aus einem Interview mit Daniel BÜTTIKER, Verwaltungsrat von Swisscert AG, geführt am 3. Oktober 2001 in Zürich.

siert dieses zu Hause an seinem Rechner. Bei der Initialisierung wird der Fingerabdruck des Schlüsselhalters aufgenommen und das Schlüsselpaar erzeugt. Der Prüfschlüssel wird hernach zusammen mit dem Fingerabdruck und (optional) mit den Personalien des Schlüsselhalters verschlüsselt an den Zertifizierungsdiensteanbieter gesandt, welche den Fingerabdruck archiviert sowie das Zertifikat erzeugt, an den Schlüsselhalter zurücksendet und allenfalls in einem Certificate Repository publiziert.[224]

bb) Identifikation des Signierschlüsselhalters

157 Anders als beim zuvor beschriebenen Modell mit Identifikationsprüfung durch eine Registrierungsstelle (RA) wird bei Swisscert keine (teure) Vorab-Identifikation durch einen RA-Mitarbeiter durchgeführt. Der Inhaber des Tokens könnte daher auch Zertifikate mit falschen Daten erzeugen; ausgenommen bleibt einzig der Fingerabdruck, der nicht fälschbar ist.

158 Wird das Zertifikat in *geschlossenen Benutzergruppen* eingesetzt, so hat der Systembetreiber (etwa eine Bank als Betreiberin eines E-Banking-Systems) die Möglichkeit, die Identifikation selbst vorzunehmen, etwa indem sich der Benutzer zunächst mit den herkömmlichen Authentifikationsmitteln (PIN/TAN) anmeldet und hernach sein Zertifikat registriert, oder indem der Systembetreiber dem Benutzer mittels eingeschriebener Post eine Kennung zusendet, die dieser hernach wieder einzugeben hat.

159 Ein Einsatz in *offenen Benutzergruppen* ist hingegen insofern problematisch, als allein die Fingerabdruckdaten noch keinen Schluss auf die Identität des Unterzeichners liefern, sondern erst bei einem auf anderem Wege ausfindig gemachten Unterzeichner durch die Fingerabdruckdaten der Beweis der Urheberschaft geführt werden kann. Lässt sich also ein Angreifer ein Zertifikat auf einen falschen Namen ausstellen und bezieht damit Leistungen, so muss der Systembetreiber zunächst dessen tatsächliche Identität ausfindig machen, was in Anbetracht der vielfältigen Vertuschungsmöglichkeiten im Internet nicht in allen Fällen möglich ist.[225]

160 Das Swisscert-System gewährleistet daher die Authentifikation des Unterzeichners nicht ohne eine zusätzliche sichere Identifikation.

cc) Datenintegrität und Nichtabstreitbarkeit

161 Weil auch das Swisscert-System auf Public-Key-Signaturen beruht, ist die Datenintegrität gleich gut gesichert wie bei einer herkömmlichen Public-Key-Infrastruktur. Steht die Identität des Schlüsselhalters fest,[226] so ist auch die Nichtabstreitbarkeit im Rahmen der Sicherheit des Gesamtsystems gewährleistet.

---

224 Zum Ganzen BÜTTIKER, 1 ff.
225 Vorne N 19 ff.
226 Soeben N 157 ff.

c) Flexible Zertifikate

162 Als weiterer Fortschritt wird die Flexibilität von Swisscert-Zertifikaten genannt. Will ein Systembetreiber einem Swisscert-Zertifikat ein Attribut zuweisen, so wendet er sich an die zentrale CA. Diese erzeugt das gewünschte Zertifikat neu, ohne das Schlüsselpaar des Anbieters zu modifizieren.[227] Eigentliche Attributzertifikate sind damit nicht nötig.[228]

163 Laut Swisscert soll dies den Systembetreibern ermöglichen, auf das Abbilden der Zertifikatsnummer auf die Kunden- oder Kontoidentifikation zu verzichten, weil eine Kundennummer direkt in verschlüsselter Form in ein Zertifikat eingebracht werden kann.[229]

164 Weil mehrere derartige Attribute in ein Zertifikat integriert werden können, kann dieses von unterschiedlichen Anbietern und für unterschiedliche Anwendungen genutzt werden.

IV. Verschlüsselung

A. Vorbemerkung

165 Digitale Signaturen sind geeignet, Authentizität und Integrität von Daten abzusichern. Soll bei der Übermittlung auch die Vertraulichkeit gewahrt werden, so ist zusätzlich Verschlüsselung nötig. Digitale Signaturen können einfach mit Verschlüsselungstechniken kombiniert werden.

B. Symmetrische Verschlüsselung

166 Das herkömmliche Verständnis von Verschlüsselung basiert darauf, dass zur Verschlüsselung und Entschlüsselung jeweils der *gleiche geheime Schlüssel* eingesetzt wird. Man spricht hier auch von *symmetrischen Verfahren*.[230]

167 Die am weitesten verbreitete symmetrische Verschlüsselungsmethode ist heutzutage *DES (Data Encryption Standard)*.[231] Seine Sicherheit schwindet jedoch zusehends aufgrund der rasch fortschreitenden Entwicklung in der Computertechnik, weshalb seit Oktober 1999 zunächst der Einsatz einer dreifachen Variante *(Triple-DES)* empfohlen und hernach *Rijndael*[232] als neuer Standard definiert wurde.[233]

---

227 BÜTTIKER, 26 ff., 31 ff.
228 Vorne N 115.
229 BÜTTIKER, 31 ff.
230 GOLLMANN, 211 f.; vgl. etwa auch JÖRG/ARTER, 458 ff.
231 Dazu etwa FOX, DES, 736; GOLLMANN, 212 f.
232 Sprich: *reindohl*.

Symmetrische Verschlüsselung setzt voraus, dass der geheime Schlüssel *vor* Aufnahme der Kommunikation auf sicherem Wege, also etwa via Telefon oder persönlich, ausgetauscht werden kann. Genau diese Voraussetzung ist aber bei der Kommunikation über das Internet nicht gegeben: Schon beim ersten Kontakt soll möglichst eine vertrauliche Verbindung zwischen den beiden Kommunikationspartnern aufgebaut werden können. Daher müssen alternative Verfahren eingesetzt werden.[234] 168

C. Asymmetrische Verschlüsselung

Das derzeit am weitesten verbreitete Verfahren, welches für den Datenaustausch über offene Netzwerke wie das Internet eingesetzt werden kann, wurde bereits 1978 von den US-Amerikanern Ron RIVEST, Adi SHAMIR und Leonard ADLEMAN entwickelt.[235] Das nach seinen Erfindern benannte *RSA-Verfahren* basiert – gleich wie digitale Signaturen – auf einem Schlüssel*paar* pro Kommunikationspartner, wovon ein Schlüssel zur Ver- und der andere zur Entschlüsselung eingesetzt wird. Der Entschlüsselungsschlüssel bleibt geheim, der Verschlüsselungsschlüssel wird veröffentlicht. Weil die Verschlüsselungsschlüssel öffentlich sind, ist kein geheimer Schlüsselaustausch mehr nötig. 169

Die Verwendung eines Paares unterschiedlicher Schlüssel führte zum Begriff des *asymmetrischen Verfahrens*; asymmetrische Verschlüsselung bildet nebst der digitalen Signatur den zweiten Anwendungsbereich der Public-Key-Kryptographie.[236] 170

D. Hybride Verfahren

Ein Nachteil der asymmetrischen Verfahren im Vergleich zu symmetrischen Verfahren liegt im grossen Rechenaufwand bei der Verschlüsselung grosser Datenmengen. Daher werden in der Praxis *hybride Verfahren* verwendet, bei welchen die tatsächliche Verschlüsselung anhand eines für jede Übermittlung mittels eines Zufallsgenerators neu erzeugten *Session Key* symmetrisch erfolgt, welcher danach asymmetrisch verschlüsselt und zusammen mit dem Dokument verschickt wird. Bei der Entschlüsselung wird zuerst der Session Key entschlüsselt, um danach damit den Text zu entschlüsseln.[237] 171

---

233 Zum Ganzen FOX, DES, 736; Stefan LUCKS/Rüdiger WEIS, Der DES-Nachfolger Rijndael, DuD 12/2000, 711 ff.; vgl. auch Patrick BRAUCH (pab.), Belgisches Krypto-Verfahren setzt sich durch, c't 22/2000, 84.

234 GOLLMANN, 212; NIESING/SCHMEH, 224.

235 Ron RIVEST/Adi SHAMIR/Leonard ADLEMAN, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (1978), 120 ff.

236 Weitere Public-Key-Verfahren neben RSA sind etwa ElGamal, Merkle-Hellmann, Knapsack oder LUC; RSA LABORATORIES, 3.6.8; vgl. auch GOLLMANN, 216 f.; JÖRG/ARTER, 460 ff.

237 Man spricht auch von einer *digital envelope;* vgl. zum Ganzen BITZER/BRISCH, 97 f.; RSA LABORATORIES, 3.1.7.

V. Zeitstempel

A. Grundlagen

172 Ein *Zeitstempel (timestamp)* ist eine Bescheinigung für die Existenz bestimmter digitaler Daten zu einem bestimmten Zeitpunkt.[238] Zeitstempel werden durch *Zeitstempeldiensteanbieter*[239] erzeugt.[240]

173 Nach einem Überblick über verschiedene mögliche Verfahren soll die Bedeutung von Zeitstempeldiensten im Rahmen der elektronischen Kommunikation im Allgemeinen und der Sicherungsinfrastruktur im Besonderen geschildert werden.

B. Überblick über die Funktionsweise

1. Erste Lösung: Vertrauen

a) Vertrauenswürdige dritte Partei

174 Eine Lösung, um die Existenz von Daten zu einem bestimmten Zeitpunkt nachzuweisen, liegt darin, diese einem vertrauenswürdigen Dritten vorzulegen und diesen nötigenfalls als Zeugen einzusetzen. Die Daten können dazu selbstverständlich elektronisch übermittelt werden.

175 Einerseits können die Daten danach beim Zeitstempeldiensteanbieter hinterlegt bleiben – man spricht hier auch von *Notariatsdiensten*[241]; andererseits ist es aber auch möglich, dass der Zeitstempeldiensteanbieter den Daten die Information über die aktuelle Zeit hinzufügt, dieses Datenpaket digital signiert und zurückschickt. Das Resultat ist der Zeitstempel[242], der aus den gestempelten Daten, der Zeitangabe und der digitalen Signatur des Anbieters besteht. Die digitale Signatur des Zeitstempeldienstes beweist, dass die Daten dem Anbieter vorgelegen haben. Die Sicherheit beruht aber auch hier auf der Vertrauenswürdigkeit des Zeitstempeldiensteanbieters.[243]

176 Die für Zeitstempeldiensteanbieter zu fordernde Vertrauenswürdigkeit gleicht in vielerlei Hinsicht derjenigen von Zertifizierungsdiensteanbietern, weshalb es nahe liegt, Zertifizierungsdiensteanbieter auch als Zeitstempeldiensteanbieter anzuerkennen.[244]

---

238 AMERICAN BAR ASSOCIATION, 63 f.; MERTES, 40.

239 Auch *Time Stamping Authorities (TSA)*.

240 Die Ausführungsbestimmungen zur ZertDV, 51, sprechen von *Datierungsdiensten*. Zum Ganzen etwa HAMMER, 101; RSA LABORATORIES, Frage 7.11 m.H.; SigI, A4.

241 SigI, A4, 12.

242 Genauer: das Zeitstempel-Token. Der Begriff Token steht einerseits für ein Datenpaket (im Falle des Zeitstempel-Tokens) und andererseits für ein mobiles Gerät zur Speicherung von Signierschlüsseln (vorne N 65). Diese Bedeutungen sind auseinanderzuhalten.

243 Vgl. etwa die Ausführungsbestimmungen der ZertDV, 51.

244 Zum Begriff der Anerkennung hinten N 280 ff.

b) *Hashwerte als Vereinfachung*

Weil die Übermittlung vollständiger Dateien unpraktisch und auch aus Gründen der Vertraulichkeit ungünstig ist, werden digitale Daten regelmässig gehasht[245], bevor sie an den Zeitstempeldiensteanbieter übermittelt werden.[246] Weil der Hashwert für jedes Dokument unterschiedlich ausfällt, kann er hierbei das Dokument vertreten, und weil vom Hashwert nicht mehr auf das Ursprungsdokument geschlossen werden kann, bleibt die Vertraulichkeit gewahrt.[247] 177

2. Zweite Lösung: Zeugnis der Öffentlichkeit

a) *Problemstellung*

Die notwendige Vertrauenswürdigkeit des Zeitstempeldiensteanbieters ist ein Schwachpunkt der beschriebenen Lösungen mit Aufbewahrung der Dokumente oder Ausstellung digital signierter Bestätigungen. Weil die Aussagen des Zeitstempeldiensteanbieters die Basis des Nachweises darstellen, könnte ein solcher Anbieter seine Systeme zurückdatieren und Zeitstempel erzeugen, welche den Eindruck erweckten, vor dem tatsächlichen Zeitpunkt erzeugt worden zu sein. Aus diesem Grund verlören sämtliche jemals erzeugten Zeitstempel eines Zeitstempeldiensteanbieters mit dem Ende seiner Vertrauenswürdigkeit ihre Beweiskraft (etwa dann, wenn ihm die rechtliche Anerkennung entzogen wird).[248] 178

b) *Publikation eines Wurzel-Hashwertes*

Anders als das Problem der Zuordnung von Prüfschlüsseln zu Personen (Zertifizierung), das keine rein kryptographisch sichere Lösung erlaubt, weil bei der Identitätsprüfung durch die Registrierstelle immer ein Mensch involviert ist, kann das Problem der Vertrauenswürdigkeit von Zeitstempeln mit kryptographischer Sicherheit gelöst werden. Dies geschieht, indem die dem Zeitstempeldiensteanbieter vorliegenden Hashwerte regelmässig *in gedruckter Form publiziert* werden, also etwa in einer Tageszeitung, die vielfach archiviert wird. 179

Auch hier wird zunächst regelmässig eine Hashfunktion eingesetzt, um die Menge der zu publizierenden Daten zu reduzieren. Man spricht diesfalls von *Hash-Bäumen*, weil die Vielzahl der Hashwerte der Ursprungsdokumente (evtl. über *Intermediate Hashes*) zusammengefasst und erneut gehasht werden, bis nur noch ein Wurzel-Hash zur täglichen Publikation übrig bleibt.[249] Dieser publizierte Wurzel-Hash beweist 180

---

245 Zum Begriff des Hashwertes schon vorne N 48 ff.

246 Vgl. RSA LABORATORIES, 7.11; SigI, A4, 15 f.

247 SigI, A4, 15 f.

248 Für den Fall der Kompromittierung des Zeitstempelsignierschlüssels gilt grundsätzlich das Gleiche. Ein (vertrauenswürdiger) Zertifizierungsdiensteanbieter kann eine Kompromittierung seines Schlüssels jedoch aufdecken, indem er sämtliche ausgestellten Zeitstempel in einer einmal beschreibbaren Protokollierungskomponente festhält. Daher muss ein Zeitstempeldiensteanbieter auf Antrag eigene Zeitstempel überprüfen können. Zum Ganzen SigI, A4, 12.

249 Vgl. SURETY, INC., 10 ff., 18, sowie Abbildung 7.

weiterhin die Existenz jeder einzelnen Verzweigung des gesamten Baumes zurück bis zu allen Ursprungsdokumenten für den Zeitpunkt seiner Publikation, denn ein Verändern einzelner Einträge veränderte auch ihn und fiele beim Vergleich mit der gedruckten Fassung sofort auf.[250]

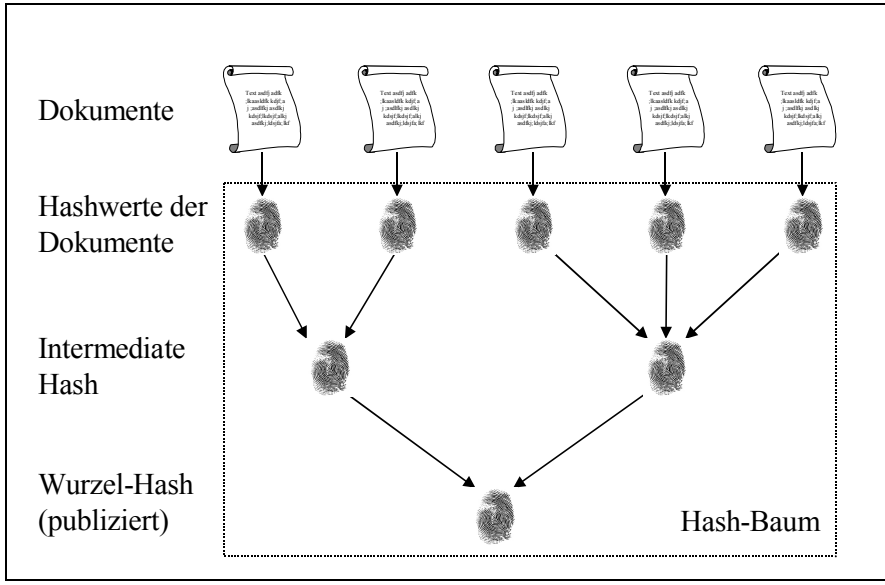

Abbildung 7: Hash-Baum.

181 Bei diesem Modell besteht ein Zeitstempel-Token im einfachsten Fall aus der Zeitangabe, dem Hashwert des gestempelten Dokumentes sowie allen Intermediate Hashes der anderen Äste, die nötig sind, um aus dem Dokument den Wurzel-Hash erneut zu berechnen. Das Token wird überprüft, indem der aus ihm berechnete Wurzel-Hash mit dem publizierten Wurzel-Hash verglichen wird. Eine digitale Signatur zur Absicherung des Tokens ist nicht nötig, weil die Integrität des Baumes bereits durch die Publikation des Wurzel-Hashwertes gesichert ist.

182 Die hierbei geschaffene Evidenz basiert nicht mehr auf der Aussage des Zeitstempeldiensteanbieters, sondern auf der durch jedermann überprüfbaren Wurzel in der physikalischen Welt und dem auf der Hashfunktion basierenden kryptographischen Nachweis. Die vom Zeitstempeldiensteanbieter verlangte Vertrauenswürdigkeit ist damit bedeutend kleiner: Es könnte zwar weiterhin sein, dass bei der Erzeugung der Hashwerte Fehler unterlaufen, was zur Folge hätte, dass die dabei erzeugten Zeit-

250 Details bei SURETY, INC.

stempel wertlos wären. Es ist jedoch unmöglich, ein rückdatiertes oder verändertes Dokument in das System einzuschmuggeln.

3. Signierte Zeitstempel-Tokens als Hybridlösung

183 Die Überprüfung eines derartigen Tokens setzte allerdings voraus, dass man die entsprechende Publikation und spezielle Prüfsoftware zur Hand hat, was nicht praktikabel ist. Um eine sofortige Überprüfung mit einer bereits bestehenden gewissen Vertrauenswürdigkeit zu gestatten, wäre es daher weiterhin möglich, das Zeitstempel-Token – wie eingangs geschildert – mit der digitalen Signatur des Zeitstempeldiensteanbieters zu versehen. Wird die Echtheit bestritten, so kann das Token anhand der gedruckten Daten überprüft werden.

4. Praktische Anwendung

184 Telesec, das als Zertifizierungsdiensteanbieterin akkreditierte Tochterunternehmen der Deutschen Telekom AG, bietet zur Erstellung von Zeitstempeln eine eigene Software an. Um einen Zeitstempel zu erzeugen, muss dem Programm die Position der zu stempelnden Datei mitgeteilt werden. Das Programm erstellt hernach einen Hashwert und übermittelt diesen an den Zeitstempelserver der Telesec. Zur Überprüfung wird ebenfalls wieder die entsprechende Software eingesetzt.[251]

185 Der US-amerikanische Anbieter Surety, Inc.[252] bietet seit 1992 im Internet einen Zeitstempel- und Notariatsdienst im Sinne der Lösung mit Zeugnis der Öffentlichkeit an. Nachteil des Systems von Surety ist, dass ohne Internet-Verbindung zu Surety keine Überprüfung stattfinden kann. Damit sind die Zeitstempel nur so lange überprüfbar, als Surety tätig bleibt. Auch Surety setzt eine besondere Client-Software ein, um die Dateien zu hashen und an den Zeitstempelserver zu übertragen.

186 Bis heute wurden Zeitstempelmechanismen noch nicht in Standard-E-Mail-Software integriert.

C. Zeitstempel als wichtiger Teil der Sicherungsinfrastruktur

1. Rückdatierungsproblem

187 Die Sperrung eines Zertifikats – etwa nach einem Verlust des Signierschlüssels – muss ex nunc wirken, weil sich der Signierschlüsselhalter ansonsten seiner Verpflichtungen einfach durch eine Zertifikatssperrung entledigen könnte. Nach der Sperrung gesetzte Signaturen dürfen zudem nicht mehr verbindlich sein, weil der Schlüsselhalter ansonsten trotz einer Sperrung riskiert, für Fälschungen zu haften.[253]

---

251 Eingehend MERTES, 40 ff.
252 Vgl. http://www.surety.com.

188 Voraussetzung für den Schluss von einer digitalen Signatur auf die Verbindlichkeit eines signierten Textes ist damit nebst dem positiven Resultat der Signaturprüfeinheit[254] *die Gültigkeit des Zertifikats im Moment der Unterzeichnung*[255]. Um die Vertrauenswürdigkeit der digitalen Signatur zu wahren, muss die Überprüfung des zu Grunde liegenden Zertifikats aber *auch nach dessen Sperrung bzw. nach Ablauf von dessen Gültigkeitsdauer* möglich sein.[256]

189 Das Ablaufdatum des Zertifikats ergibt sich aus dem Zertifikat selbst.[257] Ob und gegebenenfalls wann ein Zertifikat gesperrt wurde, kann anhand der CRL festgestellt werden.[258] Der Signierzeitpunkt hingegen, oder genauer gesagt *die Existenz der Signatur vor diesen beiden Zeitpunkten,* kann nicht anhand der im signierten Text enthaltenen Zeitangaben (etwa dem Absendezeitpunkt einer E-Mail-Nachricht) festgestellt werden, denn ein Angreifer könnte diese – etwa durch Rückdatierung seines Computersystems – manipulieren.[259] Der Zeitpunkt kann vielmehr nur durch Beweismittel belegt werden, die nicht durch einen Angreifer beeinflusst werden können, also etwa durch eine Zeugenaussage oder eben durch einen Zeitstempel.

190 Zeitstempel sind damit integraler Bestandteil jeder Sicherungsinfrastruktur, die Nichtabstreitbarkeit gewährleisten will.[260]

2. Verlängerung der kryptographischen Sicherheit

191 Digitale Signaturen verlieren mit der Zeit aufgrund der stetig wachsenden Rechnerleistung ihre kryptographische Sicherheit und damit ihre Beweiskraft.[261] Soll eine digital signierte Willenserklärung auf längere Zeit hinaus beweisbar bleiben, so muss ihre Echtheit indessen auch über diesen Zeitpunkt hinaus nachgewiesen werden können. Hierfür ist nachzuweisen, dass eine Signatur *zu einem Zeitpunkt gesetzt wurde, zu dem das entsprechende Verfahren noch sicher war.*

192 Dieser Nachweis kann durch einen vor dem Ende der Sicherheit einer Signatur gesetzten Zeitstempel geführt werden, dessen kryptographische Sicherheit länger anhält als die der Signatur.[262] Auch Zeitstempel verlieren mit der Zeit ihre kryptographische Sicherheit. Durch wiederholtes Setzen von Zeitstempeln mit jeweils wieder

---

253 Ähnlich die Ausführungsbestimmungen zur ZertDV, 2.10.3.6.
254 Vgl. N 117 ff.
255 Zur Gültigkeit von Zertifikaten N 85 ff.; vgl. auch JACCARD, Projet, 90.
256 ELLISON/SCHNEIER, 6; SigI, A4, 8 f.; vgl. auch hinten N 748 ff.
257 Vorne N 85.
258 Beide Daten sollten durch eine moderne Signaturprüfeinheit angezeigt werden; vorne N 86 ff.
259 Dazu schon PORDESCH/NISSEN, 566.
260 Vgl. etwa SigI, A4, 8 f.; ALBRECHT, Signatur, 29; RSA LABORATORIES, 7.11; CLUSIS, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 162; Alexander ROSSNAGEL, Digitale Signaturen im Rechtsverkehr, NJW-CoR 2/94, 96 ff., 100; JÖRG/ARTER, 476 ff.; ELLISON/SCHNEIER, 6; SCHLAURI/KOHLAS, 258.
261 Vgl. schon vorne N 51 ff.
262 Etwa aufgrund längerer Schlüssel; vorne N 51.

zeitgemässer Sicherheit kann die kryptographische Sicherheit digitaler Signaturen aber im Prinzip beliebig verlängert werden.[263]

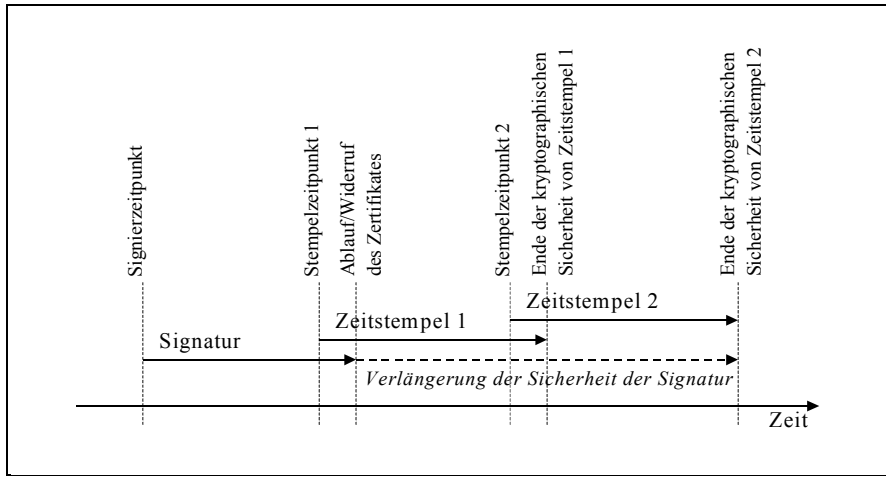

Abbildung 8: Verlängerung der kryptographischen Sicherheit digitaler Signaturen durch Zeitstempel.

D. Unmittelbare Bedeutung für den Rechtsverkehr

193 Die Bedeutung von Zeitstempeln erschöpft sich jedoch nicht in diesen technischen Zusammenhängen und damit in bloss mittelbaren Auswirkungen auf den Rechtsverkehr. Vielmehr kann die Existenz einer bestimmten Information oder das Wissen einer Person über diese (bzw. der Zeitpunkt der Kenntnisnahme) auch unmittelbare juristische Relevanz haben, etwa dann, wenn eine Person ihre Kenntnis einer bestimmten Information zu einem bestimmten Zeitpunkt nachweisen will.[264]

194 Die unmittelbare Bedeutung der Zeitstempel für den Rechtsverkehr darf indessen nicht überschätzt werden, weil Zeitstempel nicht den exakten Nachweis des Entstehens oder Bekanntwerdens von Daten erbringen können (d. h. etwa den Zeitpunkt des Setzens einer Signatur), sondern nur den Nachweis, dass diese zu einem bestimmten Zeitpunkt *existierten* (die Daten entstanden also *irgendwann* vor dem Setzen des Zeitstempels oder wurden der Partei, welche den Zeitstempel setzte, *irgendwann* vor dem Setzen des Zeitstempels bekannt).[265] Mittels Zeitstempeln kann daher beispiels-

---

263 BIESER/KERSTEN, 65 f.; ERBER-FALLER, 123; RSA LABORATORIES, 7.11.

264 BIESER, 31; BIESER/KERSTEN, 65 f.; BITZER/BRISCH, 6; DEVILLE/KALTHEGENER, 171; JÖRG/ARTER, 476; KÜHN, 86 ff.; LEPSCHIES, 52 ff.; SigI, A4, 8.

265 MERTES, 40.

weise der Empfänger einer Nachricht nicht nachweisen, dass diese bei ihm erst *nach* einem bestimmten Zeitpunkt einging.

195 Im Weiteren kann auch der Absender durch Zeitstempel auch nicht nachweisen, dass eine Nachricht den Empfänger vor einem bestimmten Zeitpunkt erreichte, es sei denn, der Zeitstempel wird – wie bei der eingeschriebenen Post – durch einen Mittler gesetzt, der damit nebst der Existenz bestimmter Daten auch deren Zugang bezeugt.[266]

E. Gesetzliche Regelung von Zeitstempeldiensten

196 Bei der Integration von Zeitstempelmechanismen in die Rechtsordnung sollte in erster Linie auf einfache Überprüfbarkeit geachtet werden, womit die zweite geschilderte Lösung (Zeugnis der Öffentlichkeit) wohl ausser Betracht fällt. Angesichts dessen, dass mit den Zertifizierungsdiensteanbietern bereits anerkannte vertrauenswürdige Parteien bestehen, spricht m.E. nichts dagegen, nur Systeme zuzulassen, die auf der Vertrauenswürdigkeit der Aussage einer anerkannten Organisation beruhen. Um diese Vertrauenswürdigkeit weiter zu stärken, könnte im Hintergrund allenfalls zusätzlich ein Hashbaum-System vorgeschrieben werden, das die Überprüfbarkeit der Zeitstempel gewährt. Dies entspräche der beschriebenen Hybridlösung.

197 Die Bedeutung von Zeitstempeln wird in Literatur[267] und Gesetzgebung[268] oftmals auf die Fixierung der geschilderten unmittelbar rechtlich relevanten Zeitpunkte reduziert, während ihre Bedeutung als integraler Bestandteil der Sicherungsinfrastruktur verkannt wird. Ein Verzicht auf Zeitstempel führte jedoch den übrigen zur Absicherung der Sicherungsinfrastruktur getriebenen Aufwand völlig ad absurdum, denn nach dem Ablauf oder der (gar durch den Unterzeichner selbst auszulösenden) Sperrung eines Zertifikats ist der Nachweis der vorgängigen Existenz einer damit erzeugten Signatur unabdingbare Voraussetzung für das Fortdauern ihrer Beweiskraft. Nachdem der VE-BGES dies noch völlig ignorierte,[269] führte der Bundesrat im E-ZertES nun eine entsprechende Bestimmung ein, was grundsätzlich zu begrüssen ist.[270]

198 Der neu eingeführte Art. 12 E-ZertES sieht nun vor, dass Zertifizierungsdiensteanbieter auf Verlangen des *Signierschlüsselhalters* einen Zeitstempel setzen müssen. Eine Verlängerung der kryptographischen Sicherheit digitaler Signaturen und

---

266 Zu einer Nachbildung der eingeschriebenen Post auf elektronischem Weg etwa SCHLAURI, E-Kuriere, Rz 1 ff.

267 So bei BIESER, 31; BIESER/KERSTEN, 65 f.; BITZER/BRISCH, 6; DEVILLE/KALTHEGENER, 171; KÜHN, 86 ff.; LEPSCHIES, 52 ff.

268 Etwa im VE-BGES.

269 Was beispielsweise zur Folge gehabt hätte, dass – zumindest entsprechend dem Wortlaut des Vorentwurfs – auch nach der Kompromittierung und Sperrung eines Zertifikats digitale Signaturen mit Echtheitsvermutung hätten erzeugt werden können; dazu schon SCHLAURI/KOHLAS, 258.

270 So auch ALBRECHT, Signatur, 29; JACCARD, Projet, 77.

ihre Konservierung über die Gültigkeit des Zertifikats hinaus liegt indessen regelmässig nur im Interesse des auf die Signatur vertrauenden Dritten. Ein Mechanismus zur Verlängerung der Sicherheit digitaler Signaturen sollte daher so ausgestaltet sein, dass dieser Dritte ihn ohne Mithilfe des ursprünglichen Unterzeichners auslösen kann. Die Lösung von Art. 12 E-ZertES ist damit zu eng, weil sie das Recht auf Zeitstempel nur Signierschlüsselinhabern zugesteht; vielmehr sollte jedermann, der die Sicherheit einer digitalen Signatur bewahren möchte, die Möglichkeit haben, einen Zeitstempel zu verlangen, und zwar unabhängig davon, ob er selbst über einen Signierschlüssel verfügt.[271]

[271] Vgl. zur Problematik etwa §16 des deutschen E-SigV 2001 sowie dessen Begründung, die Stellungnahme des deutschen Bundestages zum FormanpassungsG sowie die entsprechende Gegenäusserung der Bundesregierung (Begründung FormanpassungsG, 35, 42). §17 der deutschen SigV sieht vor, dass elektronische Signaturen vor dem Ende ihrer kryptographischen Sicherheit neu signiert werden müssen, wobei ein Zeitstempel zu integrieren ist.

§4 Beweiseignung der digitalen Signatur

I. Fragestellung

199 Nachdem die Funktionsweise der digitalen Signatur und einiger verwandter Technologien beschrieben wurde, stellt sich nun die Frage, welchen Nutzen dieses Instrument im Rechtsverkehr tatsächlich bringen kann. Es ist zu fragen, welche Schlüsse aus dem Vorhandensein einer digitalen Signatur gezogen werden können, von welchen Prämissen dabei ausgegangen werden kann (allenfalls auch nach einer gesetzlichen Festlegung von Mindeststandards), und ob typischerweise Lücken zurückbleiben.

200 Zunächst ist hierfür die einer digitalen Signatur zu Grunde liegende Kette von Beziehungen zu untersuchen, denn, wie ELLISON/SCHNEIER sagen: "Security is a chain; it's only as strong as the weakest link. The security of any CA-based system is based on many links and they're not all cryptographic. People are involved."[272] Danach folgen Überlegungen zu Ablauf und Sperrung der Zertifikate sowie zur Signaturprüfung.

II. Beziehungen beim Erzeugen der digitalen Signatur

A. Signierschlüssel – Prüfschlüssel

201 Zunächst ist sicher zu stellen, dass der Einsatz eines bestimmten Prüfschlüssels den Schluss auf einen bestimmten Signierschlüssel zulässt. Für einen Prüfschlüssel darf es daher nur einen bestimmten Signierschlüssel geben und umgekehrt. Im Weiteren darf der Signierschlüssel nicht aus dem Prüfschlüssel (oder der Signatur) ableitbar sein, und der verwendete Hash-Algorithmus muss kryptographisch sicher sein.[273]

202 Die Sicherheit einer Reihe von kryptographischen Verfahren ist wissenschaftlich anerkannt. Die Kryptographie stellt bei der Beurteilung einer Signatur nicht das Hauptproblem dar.[274]

---

272 ELLISON/SCHNEIER, 1.

273 Vorne N 51 ff.; BIZER/HERDA, 22; ROSSNAGEL, Sicherheitsvermutung, 3314, spricht von *kryptologischer Sicherheit*.

274 Vorne N 54.

B. Prüfschlüssel – Name

203 Die Zuordnung von Schlüsselpaar und Schlüsselhalter *(Personalisierung des Schlüsselpaares)*[275] geschieht über die Zertifizierung der Zusammengehörigkeit von Schlüssel und Namen des Halters, dem bei Verwechslungsgefahr ein unterscheidendes Element hinzugefügt wird.[276]

204 Von der kryptographischen Sicherheit des Zertifikats kann ausgegangen werden, weil diese ihrerseits durch eine digitale Signatur gewährleistet wird.[277]

205 Das Vertrauen in die Zertifizierung setzt Vertrauen in den entsprechenden Zertifizierungsdiensteanbieter voraus; denn ist beispielsweise dessen Signierschlüssel nicht vor Zugriffen Dritter geschützt, oder sind dessen Mitarbeiter bestechlich, so können Zertifikate gefälscht werden.[278] Dieses Vertrauen kann durch sinnvolle Organisation des Zertifizierungsdiensteanbieters, etwa durch Protokollierung der sicherheitsrelevanten Aktivitäten oder das Vier-Augen-Prinzip für bestimmte Tätigkeiten, erhöht werden.[279] Fehler sind jedoch nicht auszuschliessen.

C. Name – Schlüsselhalter

206 Die Beziehung zwischen Name und Schlüsselhalter wird durch die Überprüfung der Personalien des Schlüsselhalters zum Zeitpunkt der Schlüsselzuweisung mittels eines Ausweises, Handelsregisterauszuges o.ä. festgestellt.[280] Auch hier ist die Vertrauenswürdigkeit des Anbieters Grundlage der Vertrauenswürdigkeit der Zuordnung. Kommt eine separate Registrierstelle zum Einsatz, so muss auch diese vertrauenswürdig sein.[281]

207 Die Überprüfung der Personalien ist einer der fehleranfälligsten Schritte – in erster Linie deshalb, weil menschliches Handeln notwendig ist und weil eine geschickte Ausweisfälschung bei der üblichen visuellen Prüfung kaum zu entdecken ist. Zumindest die Überprüfbarkeit des Vorganges für den Fall der Bestreitung könnte aber durch Archivierung einer Ausweiskopie und eine in Gegenwart des Personals zu leistende Handunterschrift des Schlüsselhalters mit hoher Sicherheit gewährleistet werden.[282]

---

275 MERTES, 32.
276 BIZER/HERDA, 22; ELLISON/SCHNEIER, 3.
277 Soeben N 201 f.
278 ELLISON/SCHNEIER, 1 f.; ERBER-FALLER, 123.
279 ROSSNAGEL, Sicherheitsvermutung, 3314, spricht daher von *Organisationssicherheit*.
280 BIZER/HERDA, 23; ELLISON/SCHNEIER, 3 f., 6.
281 ELLISON/SCHNEIER, 4.
282 Der E-ZertES sieht solches leider nicht vor; zur Sicherheit von Handunterschriften hinten N 639 ff.

D. Schlüsselhalter – Unterzeichner

208 Das Erzeugen von Signaturen muss dem Schlüsselhalter vorbehalten bleiben, d.h. Schlüsselhalter und Unterzeichner müssen identisch sein.[283]

209 Ein Schlüsseldiebstahl kann wie beschrieben durch Abspeicherung des Signierschlüssels auf einem kryptographischen Token erschwert werden (Besitzelement), das durch ein Passwort (Wissenselement) vor dem Zugriff Dritter geschützt wird und aus dem der Signierschlüssel nicht ausgelesen werden kann.[284] Das Ausspähen des Passwortes durch Hacking oder Viren kann durch eine sichere Signiereinheit (etwa einen Kartenleser mit integrierter Tastatur) verhindert werden.[285]

210 Eine Passwortlösung bleibt allerdings nur ungenügend absicherbar gegenüber dem physischen Ausspähen des Passwortes bei der Eingabe durch eine anwesende Person oder einer in der Nähe des Eingabeterminals installierten Kamera und einen darauf folgenden Diebstahl des Tokens.[286] Im Weiteren kann der Schlüsselhalter den Schlüssel jederzeit selbst weitergeben. Der Einsatz des Schlüssels durch den Schlüsselhalter ist bei der Passwortlösung daher nicht positiv nachweisbar.[287]

211 Als Lösungsmöglichkeit bietet sich in Zukunft die biometrische Bindung des Schlüssels an den Halter an.[288]

E. Unterzeichner – Dokument

212 Das zu signierende Dokument muss dem Unterzeichner zum Zeitpunkt des Erzeugens der Signatur in seinen wesentlichen Teilen sichtbar gemacht werden.[289] Hierzu müsste eine Signiereinheit zum Einsatz kommen, die das Dokument unabhängig vom (wie erwähnt unsicheren) Rechner des Halters anzeigt.[290] Derzeit sind allerdings keine preiswerten, universell verwendbaren Signiereinheiten auf dem Markt, die auch grössere Datenmengen unabhängig vom Rechner sicher anzeigen könnten. Die Dokumentenanzeige muss daher mittels des Rechners erfolgen, womit eine Sicherheitslücke bestehen bleibt.[291]

---

283 BIZER/HERDA, 23; ELLISON/SCHNEIER, 2; ERBER-FALLER, 123; ROSSNAGEL, Sicherheitsvermutung, 3314, spricht von *physischer Sicherheit* bzw. *Zugriffssicherheit*.

284 BIZER/HERDA, 23; vorne N 64 ff.

285 Vorne N 69.

286 Erfolgreiche derartige Angriffe auf das EC-System werden etwa bei PAUL, 223 ff. beschrieben.

287 So etwa auch ERBER-FALLER, 123.

288 Vorne N 70 ff.

289 Vorne N 55 ff.; BIZER/HERDA, 23; ROSSNAGEL, Sicherheitsvermutung, 3314, spricht von *Anwendungssicherheit*.

290 Etwa ein Klasse-3-Kartenleser; vorne N 69, insbesondere FN 88.

291 So etwa auch FOX, Problem, 386 ff.; OCHEL/WEISSMANN, 46; ROSSNAGEL, Signaturregelungen, 459; vorne N 55 ff.

F. Signiertes Dokument – Signatur

Veränderungen des signierten Dokumentes müssen bei der Prüfung sichtbar werden.[292] Kann von der kryptographischen Sicherheit des angewandten Verfahrens (Hashfunktion, Signieralgorithmus) ausgegangen werden, so gilt dies auch für die Beziehung zwischen Dokument und Signatur. An dieser Stelle bestehen damit keine Schwierigkeiten.[293] 213

G. Abschliessender Überblick

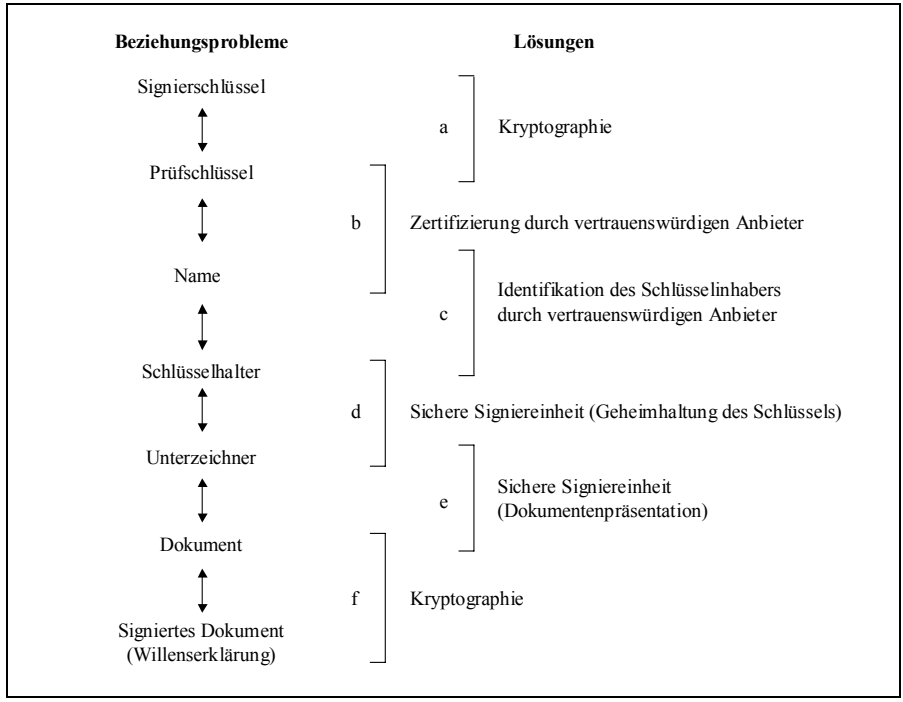

Abbildung 9: Beziehungsprobleme beim Erzeugen digitaler Signaturen.[294]

---

292 BIZER/HERDA, 23 f.
293 Vgl. schon vorne N 201 ff.
294 Nach BIZER/HERDA, 21; vgl. auch OBERHOLZER, Digitale Signatur, 444 f.

III. Ablauf und Sperrung des Zertifikats

214 Der Gefahr, dass eine Signatur nach dem Ablauf oder Sperrung des Zertifikats ihre Beweiskraft einbüsst, kann durch Zeitstempel wirksam begegnet werden.[295]

IV. Signaturprüfung

215 Ein Angreifer könnte versuchen, die Signaturprüfeinheit des Adressaten einer signierten Nachricht zu manipulieren, anstatt den Signierschlüssel des Signaturhalters zu entwenden (er könnte dem Opfer etwa ein falsches Wurzelzertifikat unterschieben).[296] Weil eine derartige Prüfung regelmässig auf einem handelsüblichen Computersystem ohne zusätzliche Hardware stattfindet, ist das entsprechende Risiko verhältnismässig hoch.[297] Es wächst zudem, wenn die Prüfung auf einem fremden System durchgeführt wird.[298] Weitere Schwierigkeiten liegen im fehlenden Know-how und in der Bequemlichkeit des Anwenders; unterlässt dieser, das Zertifikat einer empfangenen Nachricht zu untersuchen, so kann er einer Fälschung aufliegen.[299]

216 Anders als eine «Fälschung» der digitalen Signatur mittels eines entwendeten Signierschlüssels, welche sich durch nichts von einer «echten» Unterschrift unterscheidet, fällt eine derartige Manipulation indessen spätestens bei der Überprüfung der Signatur auf einem nachweislich unmanipulierten System auf. Das Risiko eines Angreifers, entdeckt zu werden, ist also hoch, und die Sicherheit des durch den Empfänger verwendeten Prüfverfahrens damit *zumindest aus der Sicht des angeblichen Unterzeichners* eher weniger bedeutend als diejenige des Signierverfahrens.

V. Folgerungen

A. Hohe Komplexität des Beweises

217 Um den Nachweis der Echtheit einer digitalen Signatur zu führen, sind alle genannten Elemente als Indizienkette nachzuweisen.[300] Dieser Beweis ist höchst komplex. Auch wenn man prinzipiell von der Beweisbarkeit der einzelnen Indizien ausgeht, so wird das Risiko, einzelne Glieder dieser Kette nicht nachweisen zu können, doch so gross, dass das ursprüngliche Ziel, durch die digitale Signatur ein der Handunter-

---

295 Vorne N 172 ff.
296 Vorne N 124, insbesondere FN 163.
297 ELLISON/SCHNEIER, 2 f.
298 HAMMER/BIZER, 691 f.
299 Vorne N 123 f.
300 ROSSNAGEL, Sicherheitsvermutung, 3314; vgl. etwa auch schon HAMMER/BIZER, 690 ff.

schrift ebenbürtiges, einfach handhabbares Beweisinstrument zu schaffen, verfehlt wird.[301] Hinzu kommt, dass ein derart komplexer Beweis nicht ohne aufwändige Sachverständigengutachten zu erbringen ist. Deren Kosten wären im Vergleich zu den in den vorgesehenen Einsatzbereichen zu erwartenden Streitwerten oftmals völlig unverhältnismässig.[302]

B. Niedrige Beweiskraft

218 Wie gezeigt wurde, ist die Komplexität des Beweises zudem nicht das einzige Problem. Wichtige Indizien wie etwa die Tatsache, dass tatsächlich der Schlüsselhalter und nicht ein Dritter den Signierschlüssel eingesetzt hat oder dass dem Schlüsselhalter das signierte Dokument auch tatsächlich korrekt präsentiert wurde, sind bis heute gar nicht positiv nachweisbar.

C. Neue Fragestellung

219 Tatsache bleibt aber, dass digitale Signaturen bisher das einzige Mittel sind, um die desolate Sicherheitslage in offenen Computernetzen signifikant zu verbessern. Will man auf dieses Instrument nicht verzichten, so fragt sich, ob es Wege und Mittel gibt, mit den beschriebenen Mängeln zu leben.

220 Zunächst ist an Haftungsnormen zu denken, mit denen die neu anfallenden Risiken sinnvoll auf die beteiligten Parteien verteilt werden können.[303] Hinzu kommt eine Vorabprüfung der sicherheitsrelevanten Komponenten, Abläufe und Organisation, die Vertrauenswürdigkeit schaffen und es damit erlauben könnte, die Komplexität des Beweises auf ein absolutes Minimum zu senken.[304] Dort wo auch eine derartige Prüfung nach dem Stand der Technik keine überzeugende Sicherheit schaffen kann, stellt sich die Frage, ob nicht – in Anlehnung an die Praxis zum *Anscheinsbeweis* – durch eine massvolle Reduktion des Beweismasses eine pragmatische Lösung gefunden werden könnte.[305]

---

301 Ähnlich ROSSNAGEL, Signaturregelungen, 459.
302 Vgl. etwa BIZER, 173 f.
303 So etwa auch WIEGAND, 130; dazu hinten N 542 ff. (Haftung der Zertifizierungsdiensteanbieter), sowie die entsprechenden Abschnitte in § 10 ab N 667 (Schlüsselhalter und Dritter).
304 BIZER/HERDA, 26; ROSSNAGEL, Sicherheitsvermutung, 3314; DERSELBE, Signaturregelungen, 459.
305 Eingehend hierzu § 10 ab N 667 ff.

§ 5 Ökonomische Aspekte

I. *Fragestellung*

221 Die Technik der digitalen Signatur ist seit 1978 bekannt. Zertifizierungsdienste wurden in Deutschland bereits 1997 gesetzlich geregelt. Der erste öffentliche Zertifizierungsdiensteanbieter in der Schweiz, Swisskey AG, war von August 1998 bis Dezember 2001 tätig. Und dennoch haben digitale Signaturen bis heute – sieht man einmal von SSL ab, das jedoch in erster Linie für technische Anwendungen und nicht für den Austausch und die Absicherung rechtlich relevanter Willenserklärung eingesetzt wird – nur sehr langsame Verbreitung erfahren.[306] So rechnete die deutsche Telesec im ersten Jahr mit 30'000 verkauften Zertifikaten und verkaufte bloss deren 300,[307] und Swisskey fertigte während ihres rund dreijährigen Betriebes trotz Investitionen von 25 Millionen Franken nur 6'000 Zertifikate für Private und 3500 für Firmenkunden aus.[308]

222 Es ist demnach zu fragen, wo die Gründe für diese langsame Verbreitung der Technik liegen könnten, wo die tatsächlichen Bedürfnisse liegen und ob es allenfalls sinnvoll und möglich wäre, staatliche Förderungsmassnahmen zu ergreifen.

II. *Gründe für die langsame Verbreitung der digitalen Signatur*

A. Pinguin-Effekt

223 Neue Technologien, die auf Kompatibilität angewiesen sind, kämpfen in *offenen Benutzergruppen* mit der Schwierigkeit, dass sie erst dann Nutzen abwerfen, wenn sie einmal durch eine hinreichend grosse Anzahl von Marktteilnehmern eingesetzt werden.[309] Kommt eine neue Technologie auf den Markt, sind die Marktteilnehmer unsicher, ob andere Marktteilnehmer ihnen bei einem Umstieg folgen werden und haben Angst, durch einen zu frühen Umstieg Geld zu verlieren. Die Folge davon ist, dass sich auch im Vergleich zum status quo bessere Technologien während langer Zeit nur sehr langsam verbreiten oder überhaupt nie durchsetzen. FARRELL/SALONER sprechen von *excess inertia*[310] oder vom so genannten *Pinguin-Effekt*.[311]

---

306 Vgl. auch WILDHABER, Market Analysis, Abschnitt «PKI Enabled Services and Applications».
307 HILLEBRAND/BÜLLINGEN, 80.
308 BETSCHON, Identitäten, 81; zum Ganzen auch SCHULZKI-HADDOUTI, Karten, 274 ff.
309 Man spricht von *Netzwerkexternalitäten;* FARRELL/SALONER, 5.
310 Etwa «überschiessende Trägheit» – im Gegensatz zu *excess momentum,* das vorliegt, wenn eine an sich schlechte neue Technologie aufgrund bestimmter Umstände (bestehende gute Reputation des Herstellers u. dgl.) durch die Anwender vorschnell übernommen wird; FARRELL/SALONER, 10.

Digitale Signaturen unterliegen diesem Phänomen: So lange potentielle Empfänger signierter Nachrichten nicht über Prüfinfrastruktur verfügen oder deren Software beim Empfang signierter Nachrichten gar Fehlfunktionen zeigt,[312] wird ein potentieller Absender die Technologie nicht einsetzen, und so lange keine signierten Nachrichten zu erwarten sind, werden die Empfänger keine funktionierende Prüfinfrastruktur anschaffen.[313] 224

In *geschlossenen Benutzergruppen* ist der Pinguin-Effekt hingegen wenig bedeutsam, weil höhere Nutzerzahlen dem einzelnen Anwender keinen Zusatznutzen verschaffen. Allenfalls damit vergleichbar ist der Effekt der bisher fehlenden Erfahrung: Die Anbieter sicherer Dienste (wie Banken) warten mit der Einführung digitaler Signaturen ab, bis Erfahrungswerte vorliegen. 225

B. Infrastruktur-Inseln

Für den Einsatz digitaler Signaturen zwischen zwei Kommunikationspartnern müssen beide die gleichen Standards verwenden *(Interoperabilität)*. Wie erwähnt kann ein Anwender einer S/MIME-kompatiblen Mail-Software nicht mit einem Anwender einer dem OpenPGP-Standard entsprechenden Software kommunizieren.[314] Zudem erlaubt der X.509-Standard eine Reihe von Implementationsvarianten, die untereinander nicht kompatibel zu sein brauchen, was die Verbreitung digitaler Signaturen behindert.[315] Durch Interoperabilitätsspezifikationen kann dem zwar abgeholfen werden, solche befinden derzeit jedoch teilweise erst in Ausarbeitung und flossen meist noch nicht in aktuelle Produkte ein.[316] 226

Hinzu kommt, dass der Zertifizierungsdiensteanbieter von allen Kommunikationsteilnehmern anerkannt sein muss. Gerade im internationalen Bereich besteht möglicherweise das Problem, dass die zur Auswahl stehenden Zertifizierungsdiensteanbieter in einem der beteiligten Länder keine Registrierungsstellen betreiben. 227

Schliesslich haben die Betreiber von Systemen, die Authentifizierung mittels digitalen Signaturen voraussetzen (etwa Banken), oftmals aus strategischen Gründen kein Interesse daran, die eingesetzten Signaturen auch ausserhalb der vorgesehenen Be- 228

---

311 Angelehnt an eine Schar hungriger Pinguine, die sich auf einer Eisscholle befindet, um von dort zu fischen, aber Angst vor Raubfischen hat, weshalb die Tiere zögern, ins Wasser zu springen: Alle warten ab, bis ein erster springt. Erst wenn dieser nicht gefressen wird, springen weitere und immer mehr, bis sich schliesslich der ganze Rest auf einmal hineinstürzt; FARRELL/SALONER, 10 ff., 13 f.; HILLEBRAND/BÜLLINGEN, 81 sprechen von einem *rekursiven Marktprozess;* vgl. auch BETSCHON, Identitäten, 81.

312 Microsoft Outlook etwa stürzt nach der Erfahrung des Verfassers beim Empfang signierter Nachrichten teilweise ab.

313 Ähnlich WILDHABER, Signaturgesetze, 5.

314 Vorne N 130.

315 Ähnlich GRABER, 84.

316 Vorne N 114.

nutzergruppe zuzulassen oder Signaturen aus fremden Benutzergruppen anzuerkennen.[317]

229 Dies führt dazu, dass der Einsatz digitaler Signaturen derzeit auf *Infrastruktur-Inseln* verstreut ist, zwischen denen keine Kommunikation stattfinden kann.[318]

C. Kosten-Nutzen-Analyse für den Anwender

230 Der Umstieg auf digitale Signaturen wird nur dann stattfinden, wenn sich Anwendungen finden, die dem Nutzer einen finanziellen Vorteil bringen, der die anfallenden Kosten deckt.[319]

231 Die derzeit verfügbaren Systeme sind teilweise für die Endanwender in Installation und Betrieb noch zu komplex. So ist auch die Installation eines einfachen Kartenlesers auf Windows 2000 aufgrund fehlender oder fehlerhafter Implementation der Betriebssystemschnittstellen nur schwer durchzuführen.[320]

232 Die Einrichtung einer sicheren Signiereinheit ist im Weiteren derzeit noch teuer. Zu den Hardwarekosten kommen die Kosten für die Zertifizierung sowie allenfalls für den technischen Support.[321] Gerade angesichts des geschilderten Pinguin-Effekts ist derzeit der Anreiz in offenen Benutzergruppen klein, Signierinfrastruktur anzuschaffen.[322]

233 Im Geschäftsverkehr kann die einfachere Abwicklung sicherer Transaktionen Einfluss auf die Attraktivität eines Unternehmens als Geschäftspartner haben. Hinzu kommt allenfalls die positive Reputation des Einsatzes moderner Technologien. An dieser Stelle kann deshalb ein Anwendungsbereich für digitale Signaturen gesehen werden.[323] Konsumenten hingegen profitieren von solchen Vorteilen kaum,[324] weshalb es bei funktionierendem Wettbewerb unwahrscheinlich ist, dass ein Unternehmen seine Abnehmer (insbesondere Konsumenten) ohne zusätzliche Anreize zum Einsatz digitaler Signaturen bewegen kann.[325] Die Vorstellung, dass sich digitale Signaturen im Konsumentenbereich schnell verbreiten werden, ist damit zu relativieren.[326]

---

317 Dazu sogleich N 235 ff.

318 Zum Ganzen Christoph THIEL, Internationale Public-Key-Infrastrukturen aus Nutzersicht, DuD 9/2000, 523 ff., 523.

319 HILLEBRAND/BÜLLINGEN, 83; WILDHABER, Signaturgesetze, 4.

320 So die leidvollen Erfahrungen des Verfassers; ähnlich auch Stefan KLEIN, zit. bei SIETMANN, Kreuz, 36.

321 OPPLIGER, 75.

322 Ähnlich Peter MANDOS und Stefan KLEIN, beide zit. SIETMANN, Kreuz, 36.

323 KREMPL, Signaturen, 60; vgl. auch ROSENTHAL, Missverständnisse, Rz 6.

324 Ähnlich ROSENTHAL, Missverständnisse, Rz 6; vgl. aber immerhin die Bemerkungen zur gesteigerten Bequemlichkeit digitaler Signaturen in Mobiltelefonen vorne N 151.

325 OPPLIGER, 74 f.

Die Erklärung indessen, dass das Publikum auf den Einsatz digitaler Signaturen verzichtet, weil damit zu hohe Fälschungsrisiken verbunden sind, die auf den Schlüsselhalter zurückfallen könnten,[327] dürfte m.E. eher nicht zutreffen – sind doch etwa EFTPOS-Kartensysteme (EC-Karte, Postcard) und insbesondere E-Banking-Systeme[328] mit vergleichbaren Risiken behaftet und erfreuen sich trotzdem grosser Beliebtheit. 234

D. Fehlende Rentabilität von Zertifizierungsdiensten

Eine weitere Schwierigkeit liegt darin, dass die Schlüsselzertifizierung nach verbreiteter Ansicht ein Verlustgeschäft ist.[329] Ausdruck dieser Schwierigkeiten ist etwa die Aufgabe der Swisskey AG nach nur rund drei Jahren Betrieb.[330] 235

Die Fixkosten für Aufbau und Betrieb von Zertifizierungsinfrastruktur und Registrierungsstellen betragen rund 25-30 Millionen Franken – Beträge, die auch bei einer sehr weiten Verbreitung der Technik allein durch den Verkauf von Zertifikaten, die in der Regel unter 100 Franken kosten, kaum hereinzuholen sind.[331] 236

Zertifizierungsdienste müssen damit *durch die Anwendungen der Signaturen quersubventioniert* werden, also etwa durch Einsparungen gegenüber den herkömmlichen Legitimationsmitteln.[332] Diese Einsparungen sind aber gerade bei kleinen Transaktionswerten oftmals zu niedrig, weil der Anteil an Betrugsfällen normalerweise schon gering ist.[333] 237

Im Weiteren ist ein Anbieter, der den Einsatz einer Public-Key-Infrastruktur finanziert, kaum bereit, die Infrastruktur der Konkurrenz mitzufinanzieren.[334] Er wird daher bestrebt sein, seine Zertifikate für die Konkurrenz nutzlos zu machen. Hinzu kommt, dass die Tokens bedruckbar und damit willkommene Werbeträger und Mittel zur Kundenbindung sind[335] und schliesslich, dass der Einsatz von Zertifikaten jen- 238

326 ALBRECHT, Signatur, 29; Ross ANDERSON, Cambridge University, zit. bei KREMPL, Signaturen, 60; Christian LANGENBACH, zit. bei KREMPL, Signaturen, 63; LÜDEMANN/ADAMS, 12; vgl. auch FREI, N 326.

327 So etwa WIEGAND, 130f.

328 Dazu hinten N 714ff.

329 Vgl. etwa BETSCHON, Nacht, 88; DERSELBE, Identitäten, 81; WILDHABER, Ende, 2f.; SCHLAURI, Bundesgesetz, 342.

330 Vgl. etwa BETSCHON, Identitäten, 81; GRABER, 84f.; WILDHABER, Ende, 1ff.

331 WILDHABER, Ende, 1 ff.; a.M. ELLISON/SCHNEIER, 1 (gemeint sind dort aber wohl unsichere Zertifikate mit ausschliesslicher Prüfung der E-Mail-Adresse, für deren Erzeugung die Grenzkosten in der Tat minimal sind). Kleinere und mittlere Unternehmen, die eine interne PKI oder eine PKI für eine geschlossene Benutzergruppe betreiben wollen, aber nicht über die Ressourcen für den Aufbau verfügen, können immerhin den Einsatz eines Application Service Providers (ASP) in Betracht ziehen, d.h. das Outsourcing des Betriebs von Hard- und Software, an eine Drittfirma; WILDHABER, Ende, 2; vgl. auch DERSELBE, Market Analysis, Abschnitt «Recommendations».

332 WILDHABER, Ende, 2f.; DERSELBE, Signaturgesetze, 4; ähnlich Sabine KOCKSKÄMPER, zit. bei SIETMANN, Kreuz, 36.

333 ALBRECHT, Signatur, 29.

334 LÜDEMANN/ADAMS, 12; WILDHABER, Ende, 3.

seits geschlossener Benutzergruppen mit weiteren Investitionen verbunden ist.[336] Damit entstehen in erster Linie *geschlossene Benutzergruppen*,[337] und die Aussicht, bald eine Vielzahl unterschiedlicher Anwendungen mit einem einzigen Zertifikat nutzen zu können, ist damit eher gering.

239 In geschlossenen Benutzergruppen stellt sich zudem die Frage, ob eine PKI überhaupt das richtige Mittel zur Absicherung der Kommunikation ist – kann doch oftmals bereits die herkömmliche Kombination von Benutzerkennung und Passwort, allenfalls in Kombination mit einer TAN, zu tieferen Preisen ausreichende Sicherheit liefern. Insbesondere dann, wenn nur Authentifikation, nicht aber Nichtabstreitbarkeit durch Sicherung der Datenintegrität etwa durch Form Signing gefragt ist, bietet die PKI in der Regel oft nur wenige Vorteile gegenüber den herkömmlichen Authentifizierungsmethoden.

E. Rechtliche Grundlagen

1. Rechtssicherheit

240 Die Rechtsgrundlagen, welche die für einen Einsatz in offenen Benutzergruppen nötige Rechtssicherheit schaffen sollen, sind teilweise noch lückenhaft. Die Rechtssicherheit ist sowohl seitens der Zertifizierungsdiensteanbieter von Bedeutung – diese sind kaum bereit, Investitionen zu tätigen, die möglicherweise durch einen kurz darauf folgenden Federstrich des Gesetzgebers wertlos werden – als auch auf Seiten der Anwender, für die der Einsatz einer Signatur sinnlos ist, wenn keine Sicherheit über deren rechtliche Würdigung besteht.[338]

2. Überregulierung

241 Vielfach ist auch zu hören, dass hohe gesetzliche Sicherheitsanforderungen der Verbreitung digitaler Signaturen abträglich seien.[339]

---

335 Arno FIEDLER, zit. bei SCHULZKI-HADDOUTI, Unterschriftsüberreif, 55.

336 Damit digitale Signaturen in offenen Benutzergruppen Rechtswirkung erlangen, sind u.U. teurere, gesetzlich anerkannte Zertifikate nötig (dazu hinten N 689 ff.) – dies kann in geschlossenen Benutzergruppen unterbleiben, weil die gewünschten Rechtswirkungen dort auf vertraglichem Wege herbeigeführt werden können (privatautonome Legitimationsordnung; hinten N 714 ff., N 723 ff.). Zudem setzt sich der Zertifizierungsdiensteanbieter höheren Haftungsrisiken aus. Im Weiteren sind möglicherweise Investitionen in Treibersoftware (und entsprechenden Kundensupport) nötig, um die Kartenleser auch mit marktüblichen E-Mail- oder Browserprogrammen einzusetzen.

337 Dazu schon SCHLAURI, Bundesgesetz WWW, Abschnitt «Einführung»; SCHLAURI, Kommunikation, 88.

338 Ähnlich Alain BEUCHAT, PKI ist und bleibt eine Frage der Zeit, Digma 2/2001, 82 f., 82; GRABER, 84; KREMPL, Signaturen, 61; ROSSNAGEL, Recht, 1818, weist zudem auf die fehlende internationale Regelung hin. Vgl. auch KIG, Bericht 3, 43 ff., 47, 63, wo vor allem auch auf das bisher fehlende Engagement der Kantone hingewiesen wird.

339 KREMPL, Signaturen, 61; SCHULZKI-HADDOUTI, Marktmacht, 58; Christoph THIEL, Marktentwicklung im Umfeld digitaler Signaturen, DuD 2/2000, 77 ff., 79; WILDHABER, Signaturgesetze, 5; DERSELBE, Ende, 2.

Selbstverständlich kann es nicht angehen, durch technisch und wirtschaftlich nicht erfüllbare Regelungen die Verbreitung digitaler Signaturen zu unterbinden. Meines Erachtens ist eine strikte Regulierung jedoch – wenn überhaupt – sicher nicht der einzige Grund für die bloss schleppende Verbreitung dieser Technik, denn sonst hätten sich die unregulierten Verfahren bereits deutlich weiter verbreitet als die regulierten. Insbesondere hinsichtlich des Einsatzes in offenen Benutzergruppen ist m.E. sogar das Gegenteil der Fall: Ohne eine verhältnismässig rigide Regulierung ist ein solcher Einsatz gar nicht denkbar, weil der Empfänger einer Signatur ansonsten keine Gewissheit über deren Eignung zum Ersatz der Schriftform in Formvorschriften erhält. Ähnliches gilt hinsichtlich der Beweiseignung der Verfahren.[340] 242

F. Angst vor Überwachung

Die Möglichkeit, Internet-Nutzer durch Zertifikate eindeutig zu identifizieren, hat in der Politik offenbar bereits erste Gelüste nach Überwachung geweckt, was auf der anderen Seite bei Bürgerrechtlern Befürchtungen weckt, das Internet könnte durch einen flächendeckenden «Ausweiszwang» zum «am stärksten regulierten Ort, den man sich nur vorstellen kann»[341] werden. 243

Meines Erachtens sind derartige Befürchtungen jedoch überzogen: Einerseits riskiert schon heute jeder Benutzer des Internet, Opfer von Schnüffelattacken zu werden,[342] und andererseits wäre eine derartige «Ausweispflicht» im offenen Internet wohl kaum durchsetzbar. Durch die Zulassung von auf Pseudonyme lautenden Zertifikaten können hier schliesslich Bedenken ausgeschaltet werden.[343] 244

G. Fehlende Sensibilisierung für Sicherheitsprobleme

Schliesslich fehlt bei weiten Teilen der Benutzer des Internet schlicht das Bewusstsein für die im Internet drohenden Gefahren und erst recht für die Möglichkeit, diese mit digitalen Signaturen einzudämmen.[344] GOLLMANN spricht gar von einem *Dilemma der Computersicherheit,* wonach Computerlaien zwar spezifische Sicherheitsbedürfnisse haben, jedoch keine entsprechende Fachkompetenz.[345] 245

---

340 Ähnlich etwa auch BÜLLINGEN/HILLEBRAND, 83; kritisch etwa RIESS, 533. Vgl. auch hinten N 281f., 683ff.

341 So Lawrence LESSIG, zit. bei KREMPL, Signaturen, 62.

342 Zu Cookies etwa GOLLMANN, 191f.

343 Ähnlich LANGENBACH (FN 326).

344 GRABER, 84; KREMPL, Signaturen, 60; LANGENBACH (FN 326).

345 GOLLMANN, 10.

H. Zusammenfassung

246 Für die bisher nur langsame Verbreitung digitaler Signaturen besteht eine Reihe von Gründen. Zu nennen sind zunächst *technische* Gründe wie die bisher teilweise nicht ausreichend genaue Standardisierung und damit die fehlende Interoperabilität sowie die für den Endanwender zu hohe Komplexität der Systeme, dann *ökonomische* Gründe wie die Tatsache, dass eine Signatur für den Anwender erst dann Nutzen abwirft, wenn auch viele andere Anwender existieren, die hohen Einstiegskosten oder dass lange nicht gesehen wurde, dass Public-Key-Infrastrukturen nur über deren Anwendungen finanziert werden können. Hinzu kommen die bisher teilweise bestehende *Rechtsunsicherheit* sowie der *schlechte Informationsstand* der potentiellen Anwender.

III. Vorteile einer offenen Sicherungsinfrastruktur

A. Fragestellung

247 Die Marktentwicklung geht derzeit in Richtung geschlossener Benutzergruppen, die sich um einzelne Angebote herum bilden und bei denen die Rechtsfolgen des Einsatzes digitaler Signaturen einem Rahmenvertrag entspringen.[346] Die Gesetzgebung sowohl in der Schweiz als auch in der EU zielt hingegen in Richtung offener Benutzergruppen – es soll möglich sein, auch ohne Rahmenvertrag mittels digitaler Signaturen zu kommunizieren. Aufgrund der Marktentwicklung fragt es sich nun, ob überhaupt ein Bedürfnis für eine offene Sicherungsinfrastruktur mit einer staatlichen Anerkennung der Anbieter und Signaturen besteht.[347]

B. Vorteile für kleine und mittlere Unternehmen

248 Der Aufbau einer PKI ist Know-how- und kostenintensiv. Er lohnt sich daher erst, wenn sich ein Angebot an einen grösseren Personenkreis zu richten vermag, womit *kleine und mittlere Unternehmen* diese Technik von vornherein nicht selbständig nutzen können. Sollen digitale Signaturen auch für KMU einsetzbar sein, müssen diese kostengünstigen Zugriff auf eine bestehende PKI und deren Zertifikate haben, sodass sie nur noch die Server-Infrastruktur zur Verfügung stellen,[348] nicht jedoch die Zertifizierung und Registrierung selbst durchführen müssen. Dies könnte m. E. durch eine offene PKI gewährleistet werden.

---

346 Vorne N 126, 237.
347 So auch WILDHABER, Signaturgesetze, 5.
348 Hierzu kann allenfalls auch auf einen Application Service Provider ausgewichen werden; vorne N 236, insbesondere FN 331.

C. Vorteile für den Behördenverkehr

249 Bund und Kantone arbeiten derzeit am Aufbau von E-Government-Strukturen für den Verkehr zwischen den Behörden sowie zwischen Behörden und Bürgern – so sollen dereinst etwa elektronische Steuererklärungen, elektronische Abstimmungen oder elektronische Eingaben an Gerichte möglich sein.[349]

250 Das Bedürfnis nach Datenschutz gerade im öffentlichen Bereich verlangt nach sicheren Kommunikationswegen. Es wäre aber vielfach nicht sinnvoll, die einzelnen Verwaltungseinheiten mit der Einrichtung entsprechender Infrastruktur zu beauftragen (etwa mit der Ausgabe von Passwörtern und Streichlisten). Vielmehr bietet sich der Aufbau einer zentralen und für beliebige Anwendungen offenen PKI geradezu an.[350]

251 Auch hier ist jedoch darauf hinzuweisen, dass der Einsatz digitaler Signaturen nur zwischen Behörden sowie zwischen Behörden und häufig mit den Behörden kommunizierende Personen sinnvoll ist.[351] Die Vorstellung hingegen, jeder Bürger werde seine Steuererklärung demnächst digital signieren, ist unrealistisch, weil sich die Anschaffung entsprechender Hardware bloss für diesen einzigen Zweck nicht lohnt.[352] Entstehen für den Staat durch den Einsatz digitaler Signaturen grosse finanzielle Einsparungen, so stellt sich aber immerhin die Frage, ob nicht die Anschaffung der Signierhardware von staatlicher Seite zu unterstützen wäre.[353]

252 Nicht zu vergessen ist schliesslich, dass der Einsatz digitaler Signaturen meist nur im Zusammenspiel mit einer Ausrichtung der gesamten Arbeitsabläufe auf den elektronischen Verkehr zu Einsparungen führen kann. Dies führt zu nicht zu unterschätzenden Einstiegskosten.[354]

---

349 Dazu etwa hinten N 320 f., 505 ff.

350 So die Botschaft Totalrevision Bundesrechtspflege, 4263; Botschaft ZertES, 5686; WILDHABER, Ende, 3; Rolf OPPLIGER, Konsequenzen des Swisskey-Ausstiegs, Digma 2/2001, 101, spricht indessen von einer Trennung von verwaltungsintern und -extern eingesetzter Infrastruktur.

351 Etwa Anwälten, die auf elektronischem Wege Akteneinsicht wahrnehmen wollen oder Firmen, die eine Vielzahl von Belegen einreichen müssen; Botschaft Totalrevision Bundesrechtspflege, 4263; BJ, Projektskizze GovLink, 2. Vgl. auch die Hinweise auf den Mehrwertsteuerbereich in FN 4.

352 Ähnlich Arno FIEDLER, zit. bei SCHULZKI-HADDOUTI, Unterschriftsüberreif, 54.

353 Es handelt sich im Prinzip um die geschilderte Finanzierung der Public-Key-Infrastruktur über Anwendungen; vorne N 237. Vgl. auch HILLEBRAND/BÜLLINGEN, 83.

354 So etwa Matthias RAMSAUER, zit. bei SCHLAURI, Bundesgesetz, 364.

IV. Lösungsmöglichkeiten

A. Private Initiativen

253 Die genannte Identrus-Initiative[355] könnte das Problem des Fehlens einer offenen PKI zumindest im Geschäftsverkehr lösen, die Kommunikation mit und zwischen Konsumenten hingegen (etwa Nutzung von Zertifikaten zur Client-Authentifizierung im E-Banking) wird zumindest vorderhand nicht abgedeckt.[356] Hinzu kommt, dass Staaten, welche sich für ihre öffentlichen Dienste einer PKI bedienen wollen, möglicherweise nicht allein auf ausländische Anbieter vertrauen wollen.[357]

254 Swisscert wird zwar voraussichtlich eine kostengünstiges Angebot aufbauen, das sich auch an KMU richtet. Weil dieses jedoch keine eindeutige Vorab-Identifikation der Teilnehmer vorsieht, werden zumindest sichere elektronische *Erstkontakte* nicht möglich sein.[358]

255 Ferner ist *IG-Top* zu nennen, eine Initiative, zu der sich eine Reihe von Unternehmen und Behörden zusammengefunden haben, um die Arbeit von Swisskey weiterzuführen.[359] Das weitere Vorgehen von IG-Top ist derzeit indessen noch nicht festgelegt.[360]

B. Staatliche Beteiligung an Zertifizierungsdiensten

256 Die Tatsache, dass unabhängige Zertifizierungsdiensteanbieter bisher nicht rentabel geführt werden können, wirft die Frage nach einer staatlichen Beteiligung am Betrieb von Zertifizierungsdiensten oder gar dem Betrieb von Zertifizierungsdiensten durch den Staat auf. Wie gezeigt wurde, hat der Staat im Bereich des elektronischen Behördenverkehrs ein eigenes Interesse an Zertifizierungsdiensten, zudem wird von einigen Seiten geltend gemacht, der Staat müsse sich nebst der Ausgabe von papierenen Personalausweisen auch der Ausgabe digitaler Ausweise annehmen.[361] Der

---

355 Vorne N 153 ff.

356 SPINDLER, Bankrecht I, 102.

357 So etwa Bundesrätin Ruth METZLER-ARNOLD in einer Rede vom 17. Mai 2001, http://www.ejpd.admin.ch/Doks/Reden/010516a-d.htm; dazu auch BETSCHON, Nacht, 88.

358 Vorne N 155 ff.

359 Etwa Arthur Andersen, die Informatikdienste der ETH Zürich, Hewlett Packard Schweiz, Payserv Geschäftsbereich Swisskey, Swisscom, SWX und die Zürcher Kantonalbank.

360 Vgl. die Website von IG-Top, http://www.igtop.ch.

361 Abwägend Bundesrätin Ruth METZLER-ARNOLD (FN 357); BETSCHON, Identitäten, 81; vgl. auch die dringliche Interpellation von Nationalrat Günter PAUL sowie die entsprechende Nationalratsdebatte, AB NR 2001, 869 ff.; dazu auch Monika ROSENBERG, Digitale Signaturen und unfallträchtige Fahrer, Nationalrat debattiert Revision des Strassenverkehrsgesetzes, NZZ Nr. 142, 22. Juni 2001, 17; WIEGAND, 130 f.; WILDHABER, Ende, 3. In Deutschland bestehen beispielsweise Pläne, amtliche Ausweisdokumente längerfristig mit biometrischen Merkmalen zu versehen; SIETMANN, Zukunftstechnik.

E-ZertES enthält deshalb mit Art. 20 Abs. 3 eine entsprechende gesetzliche Grundlage.[362]

257 Sollten sich in der Tat keine privaten Anbieter finden, so ist m.E. bei einem staatlichen Eingreifen zumindest die Zusammenarbeit mit der Wirtschaft zu suchen[363] – aufgrund der Kleinheit des schweizerischen Marktes[364] allenfalls auch grenzüberschreitend: In Deutschland etwa wurden mittlerweile eine Reihe von Anbietern akkreditiert, die den Anforderungen der schweizerischen Gesetzgebung weitgehend entsprechen, womit sich vielleicht eine Möglichkeit zum Aufbau eines schweizerischen Netzes von Registrierungsstellen in Zusammenarbeit mit einem deutschen Anbieter ergäbe. Solche "Public Private Partnerships" werden etwa auch von der Koordinationsgruppe Informationsgesellschaft des Bundes[365] propagiert.[366]

258 Weil der Staat – anders als private Anbieter[367] – kein Interesse daran hat, die Verwendung von Zertifikaten zu limitieren, könnte eine derartige PKI auch als Kondensationspunkt für den Einsatz einer offenen PKI in der Wirtschaft dienen. Pilotprojekte zum Einsatz digitaler Signaturen in Behörden können für die Wirtschaft zudem wertvolle Erfahrungen schaffen und die Nachahmung fördern.[368]

---

362 Vgl. auch hinten N 531.

363

364 Diese sieht etwa Bruno WILDHABER (zit. bei SCHLAURI, Kommunikation) als Hindernis für die Etablierung von Zertifizierungsdiensteanbietern in der Schweiz.

365 Dazu hinten N 475.

366 KIG, Bericht 3, 26f., 54f.

367 Vorne N 238.

368 HILLEBRAND/BÜLLINGEN, 84.

2. Teil: Regelungsbereiche und internationaler Überblick

§6 Regelungsbereiche und -modelle

I. Fragestellung

Mit Blick auf andere, bereits fortgeschrittene Rechtsordnungen können fünf Bereiche ausgemacht werden, in denen der Gesetzgeber aktiv werden muss: Die Frage nach der Erfüllung von Formvorschriften, die Frage nach der Zulassung der elektronischen Signatur zum Beweis und insbesondere zum Urkundenbeweis, die hierzu nötige Regelung der Sicherungsinfrastruktur, die Haftungsordnung und schliesslich die Integration der elektronischen Signatur in das öffentliche Recht (elektronischer Behördenverkehr, etc.). 259

Im Folgenden soll auf den konkreten Regelungsbedarf und den möglichen Gehalt derartiger Regelungen eingegangen werden. 260

II. Anerkennung der elektronischen Signatur

A. Begriff

Unter *Anerkennung* der elektronischen Signatur versteht man deren Gleichsetzung mit der Handunterschrift im Bereiche von Formvorschriften.[369] Gesetzliche Formvorschriften finden sich einerseits im materiellen Recht und andererseits im Prozessrecht. Prozessuale Formerfordernisse können ihrerseits unterteilt werden in Anforderungen an den Urkundenbeweis und Anforderungen an elektronisch übermittelte Rechtsschriften. Letztere werden in dieser Untersuchung nicht behandelt.[370] 261

B. Materiellrechtliche Anerkennung

1. Regelungsbedarf

Die Gleichstellung von elektronischer Signatur und Handunterschrift im Bereich der materiellrechtlichen Formvorschriften wird meist als eines der dringendsten Postulate an den Gesetzgeber betrachtet.[371] Rechtsgeschäfte, die für ihre Gültigkeit laut Gesetz der Schriftform bedürfen, wie etwa die Forderungsabtretung nach Art. 165 OR, das Schenkungsversprechen nach Art. 243 Abs. 1 OR oder die Pfandbestellung über Forderungen nach Art. 900 Abs. 1 ZGB, sollen auch digital signiert abgeschlossen 262

---

369 Botschaft ZertES, 5680; geänderter Vorschlag für eine EU-Signaturrichtlinie, 5.

370 Ein Überblick über die Rechtsgebiete, in denen eine Anerkennung der elektronischen Signatur zu regeln ist findet sich bei KIG, Bericht 3, 43 ff.

371 So schon eine Motion von 1994 der damaligen Nationalrätin SPOERRY; dazu hinten N 471.

werden können. Interessant ist ferner die Frage, wie Vereinbarungen über die Form von Verträgen (gewillkürte Form) hinsichtlich des Einsatzes elektronischer Signaturen zu beurteilen sind.

263 Die Gleichstellung von Handunterschrift und elektronischer Signatur im materiellrechtlichen Bereich soll hier als *materiellrechtliche Anerkennung* bezeichnet werden.

2. Regelungsmodelle

264 Es fragt sich zunächst, ob die elektronische Signatur allenfalls durch eine geltungszeitlich-teleologische Auslegung oder analoge Anwendung *bestehender* Normen möglich wäre *(richterrechtliches Modell)*.[372] Dies könnte dann der Fall sein, wenn die elektronische Signatur die vom Gesetzgeber in einer bestimmten Formvorschrift genutzten Funktionen der Handunterschrift ebenfalls besitzt (zu nennen sind etwa die Beweisfunktion, die Übereilungsschutz- oder Warnfunktion sowie die Rekognitionsfunktion[373]).

265 Das richterrechtliche Modell hat jedoch den gravierenden Nachteil, dass die Parteien zum Zeitpunkt des Vertragsabschlusses noch keine Sicherheit über die zukünftige Anerkennung ihres Verfahrens haben, weshalb meist eine gesetzliche Regelung bevorzugt wird.

266 Für eine solche sind drei Regelungsmodelle denkbar: Erstens kann Gleichsetzung von Handunterschrift und elektronischer Signatur auf dem Wege der Anerkennung im Rahmen jeder einzelnen gesetzlichen Formvorschrift erfolgen – etwa jeweils durch einen zusätzlichen Absatz *(Anerkennung auf Stufe der einzelnen Normen)*. In Anbetracht der schieren Masse gesetzlicher von Formvorschriften[374] scheidet dieses Vorgehen jedoch als unpraktikabel aus. Als zweite Variante bietet sich eine *ausnahmslose Gleichsetzung* von Handunterschrift und elektronischer Signatur durch eine *Anerkennungsnorm* an (etwa im Rahmen des Allgemeinen Teils des Obligationenrechts),[375] und drittens kommt eine differenzierte, durch *Ausnahmebestimmungen abgeschwächte Gleichsetzung* in Betracht, welche auf diejenigen Fälle Rücksicht nimmt, in denen die elektronische Signatur von der Handunterschrift erfüllten Funktionen nur ungenügend erfüllen kann.[376]

---

372 Für eine materiellrechtliche Anerkennung auf dem Wege des Richterrechts etwa EBBING, 273. Unter *Richterrecht* (d.h. durch das Gericht neu geschaffenes Recht) wird nach traditioneller Auffassung nur die Lückenfüllung verstanden, während die Auslegung als Nachvollzug eines bereits Bestehenden gesehen wird (dazu etwa BK-MEIER-HAYOZ, N 137 ff. zu Art. 1 ZGB; ZK-BAUMANN/DÜRR/LIEBER/MARTY/SCHNYDER, Vorbemerkungen zu Art. 1 und 4 ZGB, N 29 ff.). Nach der hier vertretenen Auffassung sind jedoch die Übergänge zumindest fliessend, denn auch bei der Auslegung trägt das Gericht eigene Gedanken in das Gesetz hinein (dazu etwa HÖHN, 108 ff.). Der Begriff des richterrechtlichen Modells scheint daher passend.

373 Eingehend hinten N 833 ff.

374 Allein im OR finden sich rund 100 Formvorschriften; BJ, Gutachten, 446. Die deutsche Rechtsordnung enthält gesamthaft rund 3800 Formvorschriften; BIESER/KERSTEN, 37.

375 Dieses Modell wird in der Schweiz favorisiert; hinten N 921 f.

376 Die E-Commerce-Richtlinie der EU lässt solche Ausnahmen zu; hinten N 442.

3. Gewillkürte Form insbesondere

267 Nach einer materiellrechtlichen Anerkennung der elektronischen Signatur im Bereich gesetzlicher Formvorschriften stellt sich die Frage, ob die elektronische Signatur auch dann zur Erfüllung gewillkürter Formvorschriften ausreichen soll, wenn die Parteien dies nicht explizit vereinbart haben. Um in diesem Bereich für Rechtssicherheit zu sorgen, sind daher möglicherweise Auslegungsregeln vorzusehen, ähnlich derjenigen von Art. 16 Abs. 2 OR.[377]

C. Prozessuale Anerkennung

1. Regelungsbedarf

268 Die Verbreitung der manuellen Unterschrift im Rechtsverkehr basiert allerdings weniger auf deren Einsatz im Bereich gesetzlicher Formvorschriften, als vielmehr auf der verglichen mit anderen Beweismitteln hohen Beweiskraft von Urkunden.[378] Einerseits werden Urkunden gemeinhin als sehr überzeugende Beweismittel betrachtet, und andererseits sind sie gegenüber anderen Beweismitteln in bestimmten Fällen sogar gesetzlich privilegiert (so sind etwa nur unterzeichnete Urkunden als Titel für eine provisorische Rechtsöffnung im Sinne von Art. 82 Abs. 1 SchKG zulässig).[379]

269 Elektronisch signierte Dokumente sind indessen nach herrschender Lehre de lege lata nur zum Augenscheinsbeweis zugelassen.[380] Es stellt sich somit die Frage, ob und auf welchem Weg der Urkundenbeweis auch für diese geöffnet werden könnte. Dies soll als *prozessuale Anerkennung* bezeichnet werden.

270 Ein besonderes Hindernis liegt dabei in der vorderhand fehlenden Ausstattung der Gerichte mit technischen Mitteln und Know-how zur Durchführung der Gültigkeitsprüfung.

2. Regelungsmodelle

271 Bei der Zulassung zum Urkundenbeweis ist gleich wie bei der materiellrechtlichen Anerkennung auf die vom Gesetzgeber genutzten Eigenschaften der Handunterschrift abzustellen (dabei geht es in erster Linie um Beweiskraft und praktische Beweiseignung). Auch die prozessuale Anerkennung kann mittels eines *gesetzlichen* oder – im Lichte einer zuvor erfolgten materiellrechtlichen Anerkennung – *richterrechtlichen Modells* erreicht werden.[381]

---

377 Das deutsche Formanpassungsgesetz führt einige derartige Auslegungsregeln ein; hinten N 452 f.
378 So etwa auch BIZER/MIEDBRODT, 137; HAMMER/BIZER, 689; PESTALOZZI/VEIT, 602.
379 Eingehender dazu hinten N 663 ff.
380 Hinten N 777 f.
381 So etwa die Botschaft ZertES, 5688; für eine richterrechtliche prozessuale Anerkennung nach deutschem Recht etwa noch KILIAN, 609.

272 Eine Möglichkeit zur Lösung des Problems der technischen Ausrüstung der Gerichte bestünde m.E. in der Einrichtung einer zentralen Stelle, welche die korrekte Gültigkeitsprüfung elektronischer Signaturen und die Übereinstimmung der eingesetzten Zertifikate mit dem Gesetz in Form einer Papierurkunde bestätigt.[382]

III. Beweisregeln

A. Regelungsbedarf

273 Die Praxis geht bei unverdächtigen handschriftlich signierten Urkunden im Sinne einer tatsächlichen Vermutung von deren Echtheit aus.[383] Angesichts der sich bei elektronischen Signaturen stellenden Beweisschwierigkeiten[384] ist dies dort indessen nicht möglich. Folge davon ist, dass – zumindest ohne zusätzliche Indizien für die Echtheit – trotz einer gültigen Signatur das einfache Bestreiten der Echtheit durch den Beweisgegner im Prinzip ausreicht, um den Beweis zu vereiteln.

274 Es ist daher zu fragen, ob elektronischen Signaturen auf irgendeine Weise ähnliche Beweiskraft verliehen werden könnte wie Handunterschriften.

B. Regelungsmodelle

275 Zur Lösung dieses Problems sind drei unterschiedliche Regelungsmodelle denkbar: Erstens kann die Entscheidung, ob elektronische Signaturen einen Beweis erbringen können, weiterhin den Gerichten überlassen bleiben, wobei sie die Möglichkeit haben, im Sinne eines *Anscheins- oder prima-facie-Beweises* das Beweismass zu senken.[385]

276 Zweitens kann eine derartige Beweismasssenkung durch den Gesetzgeber vorweggenommen werden, was höhere Rechtssicherheit schafft. Dies soll als *gesetzlicher Anscheinsbeweis* bezeichnet werden.[386]

277 Drittens besteht noch die Möglichkeit, eine *widerlegbare gesetzliche Vermutung* der Echtheit elektronischer Signaturen zu statuieren, was eine Beweislastumkehr zulasten des angeblichen Unterzeichners bewirkt und diesen daher vor erhebliche Beweisprobleme stellen kann. Eine solche war im Vorentwurf zum schweizerischen Signaturgesetz vorgesehen, wurde aber im Entwurf wieder gestrichen.[387]

---

382 Eingehend hinten N 788 ff.
383 Eingehend hinten N 639 ff.
384 Vorne N 217 ff.
385 Eingehend hinten N 588 ff. sowie 673 ff.
386 Vgl. etwa die Regelung in *Deutschland*; hinten N 456 ff.
387 Der Entwurf favorisiert nun die freie richterliche Beweiswürdigung; hinten N 684.

IV. Sicherungsinfrastruktur

A. Regelungsbedarf

278 Um Rechtsfolgen an den Einsatz elektronischer Signaturen anknüpfen zu können, müssen zuverlässige Signaturverfahren und Signier- und Prüfanwendungen zur Anwendung kommen (*technische Sicherheit* bzw. *Anwendungssicherheit*), das eingesetzte Personal muss vertrauenswürdig sein *(personelle Sicherheit),* es muss für die Prüfung und Überwachung der Sicherheit gesorgt sein *(organisatorische Sicherheit),* und die Anbieter müssen schliesslich ausreichende finanzielle Mittel für Haftungsfälle aufbringen können *(finanzielle Sicherheit)*.[388]

279 Wenn elektronische Signaturen in geschlossenen Benutzergruppen eingesetzt werden sollen, so können die gewünschten Rechtsfolgen zu einem grossen Teil auch auf vertraglichem Wege herbeigeführt werden. Aufgrund der Komplexität der Materie und den entsprechenden Schwierigkeiten bei der Auswahl geeigneter Verfahren stellt sich hier indessen die Frage nach einem *staatlich anerkannten Gütesiegel* für bestimmte Signaturverfahren und Zertifizierungsdiensteanbieter.[389]

B. Regelungsmodelle

1. Sicherungsinfrastruktur und Anerkennung der Signaturen

a) Ex-ante- und ex-post-Ansatz

aa) Allgemeines

280 Die Regelung der rechtlichen Anerkennung von Signaturverfahren kann einem *ex-post-*[390] oder einem *ex-ante-Ansatz*[391] folgen. Beim ex-post-Ansatz entscheidet das Gericht[392] erst dann über die Anerkennung einer Signatur, wenn diese in einem konkreten Gerichtsverfahren umstritten ist, also *erst nach dem Einsatz des Verfahrens*. Bei der ex-ante-Regelung hingegen wird ein Signaturverfahren und insbesondere der Zertifizierungsdiensteanbieter durch eine eigens hierfür geschaffene Stelle (*Anerkennungsstelle* oder *Certification Body*) *bereits vor der Anwendung* anerkannt (diese *Anerkennung der Zertifizierungsdienstanbieter* ist von der Anerkennung der Signaturen zu unterscheiden), und das Gericht ist in der Folge in bestimmter Weise an diesen Entscheid gebunden.[393]

---

388 Eingehend MIEDBRODT, 54 ff.; BIZER/MIEDBRODT, 143 f.; BÜLLESBACH/RIESS/MIEDBRODT, 8 ff.
389 Vorne N 242.
390 «Im nachhinein».
391 «Von vornherein».
392 Oder eine andere zuständige Stelle; in der Folge soll der Einfachheit halber nur von Gericht die Rede sein.
393 Hinten N 290 ff., 683 ff.

281 Das Vertrauen der Anwender in Anbieter und Verfahren basiert beim ex-ante-Ansatz in erster Linie auf der Prüfung durch die Anerkennungsstelle und erst in zweiter Linie auf der Haftung der Zertifizierungsdiensteanbieter für Verletzungen ihrer gesetzlichen Pflichten, während es beim ex-post-Ansatz allein auf der Haftung der Zertifizierungsdiensteanbieter beruht.[394]

282 Für die ex-ante-Regelung sprechen die – gerade im Bereich der Formvorschriften bedeutende – höhere Rechtssicherheit und die im Vergleich zu den Gerichten höhere Fachkompetenz spezialisierter Anerkennungsstellen,[395] während die ex-post-Regelung vor allem die Anerkennung von auf ausländischen Zertifikaten basierenden Signaturen vereinfacht.[396]

bb) Anerkennung der Zertifizierungsdiensteanbieter

283 Für die ex-ante-Prüfung von Zertifizierungsdiensteanbietern sind verschiedene Modelle denkbar:

284 • Eine erste Möglichkeit bestünde in der Schaffung eines *staatlichen Monopols* und einer verwaltungsinternen Regelung der Ausgabe von Zertifikaten.[397] Diese Möglichkeit wurde jedoch bisher nirgends verwirklicht.[398]

285 • Als zweite Möglichkeit könnte das Gemeinwesen die Ausstellung von Zertifikaten mit Rechtswirkungen einer generellen Bewilligungspflicht unterstellen und damit konzessionierten Unternehmen vorbehalten, welche bestimmte technische und organisatorische Voraussetzungen erfüllen *(Konzessionssystem)*. In reiner Form verwirklicht, unterstünden sämtliche Zertifizierungsdiensteanbieter dieser Bewilligungspflicht, was dann, wenn die vorgesehenen Rechtswirkungen gar nicht erwünscht wären[399] oder auch vertraglich herbeigeführt werden könnten[400] eine Überregulierung bedeutete.

286 • Ein dritter ex-ante-Ansatz besteht darin, die gesetzlichen Rechtsfolgen von Zertifikaten (bzw. den darauf beruhenden Signaturen) von einer *freiwilligen Anerkennung* der Zertifizierungsdiensteanbieter abhängig zu machen. Wer Zertifikate ohne die gesetzlich vorgesehenen Rechtswirkungen ausstellen will, darf dies

---

394 Ähnlich Ivo GEIS, Die elektronische Signatur als Bestandteil rechtssicheren Geschäftsverkehrs, in: Ivo GEIS (Hrsg.), Die digitale Signatur – eine Sicherheitstechnik für die Informationsgesellschaft, Ein Leitfaden für Anwender und Entscheider, 155 ff.; vgl. aber hinten N 760 bezüglich Art. 59a E-OR, der die Haftung des Schlüsselhalters unverständlicherweise auf Zertifikate mit ex-ante-Prüfung beschränkt und damit die Etablierung nicht anerkannter Anbieter im Bereich offener Benutzergruppen zu verhindern droht.

395 ROSSNAGEL, Fortentwicklung, Abschnitt 2.4; vgl. auch BIZER/HERDA, 25 f.; ROSENTHAL, Bund, 20; kritisch zum Bedürfnis nach einer ex-ante-Prüfung etwa SCHULZKI-HADDOUTI, Karten, 275.

396 Dazu hinten N 311 ff.

397 Genau besehen handelt es sich gar nicht um eine «Anerkennung», da der Staat selbst tätig wird und der Begriff der Anerkennung das Tätigwerden eines Dritten voraussetzt.

398 FRITZSCHE/MALZER, 23, plädierten etwa noch für dieses Modell; vgl. auch MLES Guide to Enactment, § 58. Zur staatlichen Unterstützung der Anbieter aus ökonomischen Gründen vorne N 256 ff.

399 Bei technischen Anwendungen digitaler Signaturen; vorne N 137, 142.

400 Im Rahmen geschlossener Benutzergruppen.

weiterhin tun. Soll ein Zertifikat jedoch das Setzen von Signaturen mit den gesetzlich vorgesehenen Rechtswirkungen ermöglichen, so muss sich der Anbieter durch eine Anerkennungsstelle prüfen lassen. Weil die Anerkennung bei diesem Modell grundsätzlich freiwillig bleibt, spricht man auch vom *Prinzip der freiwilligen Anerkennung der Zertifizierungsdiensteanbieter*.[401] Dieses liegt der schweizerischen Signaturgesetzgebung bzw. den entsprechenden Entwürfen seit jeher zu Grunde.[402]

cc) Anerkennung von Verfahren und Komponenten

287 Nebst der Zuverlässigkeit der Zertifizierungsdiensteanbieter sind auch die eingesetzten kryptographischen Verfahren sowie die Signatur- und Prüfeinheiten für die Sicherheit der Verfahren von Bedeutung. Auch sie können ex ante oder ex post geprüft werden.

288 Eine ex-ante-Prüfung kann einerseits unabhängig von einer Anerkennung von Zertifizierungsdiensteanbietern erfolgen (d.h. die Hersteller der Produkte stellen entsprechende Anträge bzw. der Staat prüft vorhandene Techniken von Amtes wegen).[403] Andererseits ist es möglich, die Anerkennung von Zertifizierungsdiensteanbietern von deren Kompetenz zur Auswahl sicherer Komponenten abhängig zu machen und allenfalls eine Pflicht der Anbieter zu statuieren, ihren Kunden nur sichere Geräte zu empfehlen oder auszuhändigen.[404]

dd) Zuständigkeit zur Prüfung

289 Hinsichtlich der für die ex-ante-Prüfung der Anbieter und Techniken zuständigen Stellen kann weiter differenziert werden. Während das schweizerische System eine Prüfung und Anerkennung durch private Stellen vorsieht, sind etwa nach deutschem Recht staatliche Stellen zuständig, welche sich aber auf die Mithilfe Privater stützen.[405]

ee) Bindung der Gerichte an die ex-ante-Prüfung

290 Schliesslich ist zu entscheiden, welche Wirkung eine derartige ex-ante-Prüfung der Anbieter für die Gerichte überhaupt haben soll. Dies kann in erster Linie durch die Gestaltung der Anerkennungsnorm beeinflusst werden.

291 Der Schluss von der ex-ante-Prüfung auf die Anerkennung einer Signatur[406] kann in einer *ersten Variante* den Gerichten überlassen werden *(richterrechtliches Modell)*. Dies setzt allerdings voraus, dass die Anerkennungsnorm nicht unmittelbar auf die

---

401 Vgl. etwa RAMSAUER, 66; JÖRG/ARTER, 465 f.; LEGLER, E-Commerce, 9.

402 Sowohl die ZertDV als auch alle Entwürfe zum ZertES gehen davon aus; hinten N 512.

403 Diesem Ansatz folgt etwa die EU-Signaturrichtlinie hinsichtlich sicherer Signiereinheiten; hinten N 387.

404 Dem letzteren Ansatz folgt Art. 9 Abs. 2 E-ZertES; vgl. auch hinten N 528.

405 Hinten N 521 ff. sowie N 422.

406 Zu unterscheiden vom Schluss auf die Echtheit einer Signatur; dazu hinten N 309.

ex-ante-Prüfung abstellt (d.h. dass die Prüfung selbst nicht als Tatbestandsmerkmal aufgeführt ist), sondern nur auf bestimmte Eigenschaften von Verfahren und Anbietern.[407] Immerhin kann ein Gericht bei erfolgter Prüfung durch die Anerkennungsstelle allenfalls von einer tatsächlichen Vermutung oder einem Anscheinsbeweis für diese Eigenschaften ausgehen.

292 Eine *zweite Variante* besteht in einer an die ex-ante-Prüfung anknüpfenden *widerlegbaren gesetzlichen Vermutung* und eine *dritte* in einer entsprechenden unwiderlegbaren Vermutung *(Fiktion)* der Anerkennungsvoraussetzungen.[408] Für Letztere kann die ex-ante-Prüfung auch unmittelbar als Tatbestandsmerkmal in die Anerkennungsnorm aufgenommen werden.[409]

ff) Kombination von ex-post- und ex-ante-Ansatz

293 Die *EU-Signaturrichtlinie* geht zunächst von einem ex-post-Ansatz aus, was es unter anderem erlaubt, die gemeinschaftsweite Verkehrsfähigkeit von Zertifikaten und Signaturen sicherzustellen: Signaturen, welche die generell-abstrakten Anforderungen der Anerkennungsnorm (Art. 5 Abs. 1 der Richtlinie) erfüllen, sind gemeinschaftsweit materiellrechtlich anerkannt.[410] Mitgliedstaaten, die *zusätzlich* ein ex-ante-System vorsehen wollen, können dies nach Art. 3 Abs. 2 der Richtlinie tun. Anders als beim Prinzip der freiwilligen Anerkennung dürfen die genannten Rechtswirkungen der Signatur jedoch nicht von dieser Anerkennung[411] abhängig gemacht werden.[412]

b) Funktionaler und technikrechtlicher Ansatz

aa) Begriffe

294 Zu fragen ist hernach, wie die Anerkennungsvoraussetzungen formuliert werden sollen, an die sich die Gerichte (beim ex-post-Ansatz) bzw. die Anerkennungsstelle (beim ex-ante-Ansatz) zu halten haben. Dabei ist zwischen einem *funktionalen Ansatz* und einem *technikrechtlichen Ansatz* zu unterscheiden.

295 Der – teilweise als moderner bezeichnete[413] – funktionale Ansatz geht von den Funktionen von Handschriftlichkeit und Papierdokument aus, die der Gesetzgeber in den Formvorschriften nutzt, also etwa dem Beweis von Authentizität oder Integrität eines

---

407 So könnte für eine Anerkennung etwa verlangt sein, eine Signatur müsse «für den gewählten Zweck ausreichend sicher» sein (ähnlich etwa Art. 6(1) des UNCITRAL Model Law on Electronic Signatures; hinten N 340 ff.), wobei eine ex-ante-Prüfung, deren Voraussetzungen anderswo festgeschrieben sind, als Anhaltspunkt für diese Sicherheit dienen kann. Auch das deutsche Formanpassungsgesetz basiert auf diesem Modell; hinten N 444 ff.

408 Die Frage wurde auf ähnliche Weise bei der Ausarbeitung des UNCITRAL Model Law on Electronic Signatures angesprochen; hinten N 340.

409 Vgl. etwa Art. 14 Abs. 2bis E-OR; hinten N 894 ff.

410 Als Beweismittel irgendeiner Art, nicht aber zwingend zum Urkundenbeweis; hinten N 379 f.

411 In der EU *Akkreditierung* genannt; hinten N 373 f.

412 Eingehend hinten N 373 f.

413 Beispielsweise bei BLUM, UNCITRAL, 65.

Textes oder der Warnfunktion.[414] Eine funktionale Regelung, die auf die Authentifizierungsfunktion abstellt, könnte demgemäss etwa folgendermassen lauten:

> *Elektronische Signatur: Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.*[415]

Eine technikrechtliche Definition basiert hingegen auf bestimmten, für ein Verfahren typischen Eigenschaften. Sie könnte etwa folgendermassen lauten: 296

> *Elektronische Signatur: Ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle versehen ist.*[416]

Dieser Ansatz geht deutlich von den Eigenschaften der Public-Key-Verfahren aus. 297

bb) Abstraktionsgrad

Sowohl funktionaler als auch technikrechtlicher Ansatz können in unterschiedlichen Abstraktionsgraden ausgestaltet werden. 298

Naturgemäss ist indessen nur die technikrechtliche Variante einem höchsten Konkretisierungsgrad zugänglich. So schreiben etwa die Ausführungsbestimmungen zur schweizerischen Zertifizierungsdiensteverordnung Inhalt und Datenformat einzelner Datenfelder eines Zertifikats vor, um dessen Verkehrsfähigkeit zu sichern;[417] eine funktionale Umschreibung dieser Voraussetzung wäre undenkbar. Die EU-Signaturrichtlinie definiert in Anhang I ebenfalls technikrechtlich den vorgeschriebenen Zertifikatsinhalt, beschränkt sich dabei jedoch auf eine abstraktere Formulierung. 299

Der funktional formulierte Art. 6 des UNCITRAL Model Law on Electronic Signatures (MLES) setzt für eine Anerkennung zunächst voraus, dass eine Signatur an den Unterzeichner gebunden ist (Authentifizierung), dass sie allein durch diesen kontrolliert werden kann, dass Änderungen an der Signatur nachträglich erkennbar sind sowie dass Veränderungen am Text nach der Unterzeichnung erkennbar sind (Sicherung der Datenintegrität). Art. 6 Abs. 3 MLES konkretisiert diesen Ansatz weiter, in dem er Kriterien zur Bestimmung der Sicherheit aufführt.[418] 300

Im Rahmen des ex-ante-Ansatzes ist eine technikrechtliche Formulierung zu bevorzugen, weil nur sie ausreichende Rechtssicherheit für die Zertifizierungsdiensteanbieter bietet. Der ex-post-Ansatz lässt sich indessen sowohl funktional als auch technikrechtlich verwirklichen.[419] 301

---

414 Eingehend zu diesen Funktionen hinten N 833 ff.
415 Vgl. Art. 2 Nr. 1 der EU-Signaturrichtlinie; dazu hinten N 377 ff.
416 Vgl. § 2 Abs. 1 des deutschen Signaturgesetzes von 1997; dazu hinten N 400 ff.
417 Ausführungsbestimmungen zur ZertDV, 2.9.1.
418 Eingehend hinten N 340 ff.

c) *Wirtschaftliche Sichtweise*

aa) Marktwirtschaftlicher und technikrechtlicher Ansatz

302 MIEDBRODT unterscheidet in einer wirtschaftlichen Sichtweise zwischen einem *«marktwirtschaftlichen»* und einem *«technikrechtlichen»* Ansatz,[420] wobei Ersterem die Auffassung zu Grunde liegt, «dass die Spezifizierung der Anforderungen an Anbieter elektronischer Signaturverfahren zunächst den Kräften des Marktes überlassen bleiben sollte und es derzeit lediglich Aufgabe des Gesetzgebers ist, die gesetzlichen Rahmenbedingungen zu schaffen, damit sich diese Marktkräfte entfalten können», wohingegen das zentrale Anliegen des Letzteren darin liegt, «die Voraussetzungen der Infrastruktur für elektronische Signaturen zu regeln, um eine beweissichere Kommunikation zwischen zwei einander unbekannten Parteien zu ermöglichen.»[421]

bb) Technologieneutralität insbesondere

303 Die Auffassung, man solle die Entwicklung von Signaturverfahren dem Markt überlassen, geht gemeinhin mit der Forderung nach *technologieneutraler Ausgestaltung des Rechts* einher, d.h. nach einer Regelung, welche keine bestimmte Technologie gegenüber anderen bevorzugt. Oftmals wird auch argumentiert, es sei nicht absehbar, welche neuen Signaturmechanismen in Zukunft noch erfunden werden würden, weshalb insbesondere eine Beschränkung auf Public-Key-Verfahren zu vermeiden sei.[422]

304 Diese Forderung basiert auf der Annahme, dass eine ganze Reihe unterschiedlicher Methoden zur Sicherung von Datenintegrität und -authentizität denkbar seien. Zumindest in *offenen Benutzergruppen* ist dies jedoch gerade hinsichtlich des Public-Key-Prinzips nicht der Fall: Jedes Verfahren zur Sicherung von Integrität und Authentizität digitaler Kommunikation ohne Möglichkeit zu sicheren Erstkontakten muss *in irgendeiner Form* auf einem durch einen vertrauenswürdigen Dritten sicher einer Person zugeordneten öffentlichen Prüfschlüssel und einem zu diesem korrelierenden geheimen Signierschlüssel basieren, denn ohne einen öffentlichen Prüfschlüssel kann eine Signatur nicht sicher überprüft werden, und ohne einen geheimen Signierschlüssel können gar keine individuellen, fälschungssicheren Signaturen gesetzt werden. Das Public-Key-Prinzip ist damit eine *notwendige, universelle Komponente* sämtlicher in offenen Benutzergruppen denkbaren Signaturverfahren.[423]

---

419 Das UNCITRAL-Modellgesetz basiert wie gezeigt auf einem funktionalen und die EU-Signaturrichtlinie auf einem technikrechtlichen ex-post-Ansatz.

420 MIEDBRODT, 37; vgl. auch BÜLLESBACH/RIESS/MIEDBRODT, 6.

421 Die EU-Signaturrichtlinie kombiniert marktwirtschaftlichen und technikrechtlichen Ansatz. Während die «einfache» und die «fortgeschrittene elektronische Signatur» dem marktwirtschaftlichen Ansatz folgen (funktional, ex post), entspricht die «qualifizierte elektronische Signatur» (eingehend zu diesen Begriffen hinten N 375 ff.) dem technikrechtlichen Ansatz (ex post, ergänzt durch eine für die Mitgliedstaaten freiwillige ex-ante-Lösung); eingehend MIEDBRODT, 37, 86 ff.

422 So etwa MLES Guide to Enactment, § 106.

423 Ähnlich GRIMM/FOX, 407 f.; SCHLAURI/KOHLAS, 254.

Davon machen auch die fälschlicherweise immer wieder als Alternative zu Public-Key-Verfahren genannten[424] biometrischen Verfahren keine Ausnahme, denn biometrische Merkmale sind erstens nicht geheim (Fingerabdrücke etwa finden sich im Umfeld einer Person massenhaft) und eignen sich damit nicht als Signierschlüssel, und können zweitens ohne Kombination mit Public-Key-Kryptographie nicht zur Sicherung der Datenintegrität dienen.[425] 305

Der Ansatz der Technologieneutralität ist selbstverständlich insofern zu befürworten, als sämtliche Teile einer Regelung, die *nicht* durch das Public-Key-Prinzip vorausgesetzt werden, entsprechend auszugestalten sind. Dies gilt zunächst einmal für alle Fälle, in denen auch Signaturen geregelt werden sollen, die in *geschlossenen Benutzergruppen* zur Anwendung kommen: Weil hier regelmässig ein physischer Kontakt vorausgeht, können auch andere als Public-Key-Verfahren zur Anwendung kommen.[426] Im Weiteren gibt es wie beschrieben eine auch ganze Reihe unterschiedlicher Public-Key-Signaturverfahren.[427] Um den Wettbewerb zwischen diesen Verfahren nicht zu behindern, muss eine Regelung entsprechend technologieneutral ausgestaltet sein. 306

d) Zusammenfassung

Es gibt eine Anzahl unterschiedlicher Modelle zur Regelung der Sicherungsinfrastruktur. Bei ihrer Beurteilung ist zunächst zu fragen, ob die Voraussetzungen für die rechtliche Anerkennung elektronischer Signaturen zum Zeitpunkt der Beurteilung (d.h. im Verhältnis zum Signiervorgang *ex post*) durch die Gerichte oder bereits vor dem Einsatz eines Verfahrens *(ex ante)* durch eine spezialisierte Stelle geprüft werden sollen. 307

Werden die Voraussetzungen ex ante durch eine (in der Regel staatlich anerkannte) Stelle geprüft, so verlangt das Legalitätsprinzip deren detaillierte technische Umschreibung *(technikrechtlicher Ansatz)*. Bei einer ex-post-Anerkennung können die Voraussetzungen indessen einerseits technikrechtlich, andererseits aber auch in Anlehnung an die Funktionen der Handunterschrift formuliert werden *(funktionaler Ansatz)*. 308

---

424 Etwa bei Stefan KREMPL, Wie geht's weiter mit den digitalen Signaturen?, Telepolis 2. Mai 1999, http://www.heise.de/tp/deutsch/inhalt/te/2803/1.html, Abschnitt «Biometrie statt Kryptographie für die digitale Signatur».

425 Das Anhängen der durch einen Fingerabdruckscanner digitalisierten Fingerabdruckdaten ist nicht sicherer als das Anhängen einer digitalisierten Handunterschrift; vorne N 37f. Biometrie kann aber sehr wohl zu Authentifizierungszwecken eingesetzt werden, sofern hierzu sichere Hardware Verwendung findet. Kombiniert man derartige Hardware mit einem Signierschlüssel, so sind sehr sichere digitale Signaturen möglich; vorne N 70ff.

426 Das Homebanking Computer Interface HBCI etwa kann auch mit symmetrischen Signaturverfahren arbeiten (sog. *Message Authentication Code; MAC*); dazu ZENTRALER KREDIT-AUSSCHUSS, HBCI Schnittstellenspezifikation, Teil A, http://www.hbci-zka.de/download/HBCI220D/HBCI22a.pdf, Abschnitt VI.2; zu HBCI vorne N 147.

427 Sowohl für das Setzen der Signatur selbst als auch für das Erzeugen des Hashwertes können unterschiedliche Algorithmen eingesetzt werden; vorne N 48, 51, insbesondere FN 44.

2. Beweisregeln

309 Soll die Beweiskraft elektronischer Signaturen durch gesetzliche Beweisregeln erhöht werden, so kann dies wie erwähnt entweder durch eine Fiktion oder widerlegbare Vermutung der Echtheit oder mittels eines gesetzlich geregelten Anscheinsbeweises geschehen.[428] An die Stelle des regelmässig sehr schwierigen Nachweises der Echtheit einer konkreten elektronischen Signatur tritt der vereinfachte Nachweis einer Vermutungs- bzw. Anscheinsbasis. Auch diesfalls sind sowohl ein ex-ante- als auch ein ex-post-Ansatz denkbar.

310 So beruht etwa der gesetzliche Anscheinsbeweis des deutschen § 292a ZPO[429] auf der Qualifikation der zu prüfenden Signatur als eine «qualifizierte elektronische Signatur» im Sinne von § 2 Nr. 3 des Signaturgesetzes handelt. Diese wiederum ist definiert als auf einem zum Signierzeitpunkt gültigen Zertifikat mit bestimmten Eigenschaften beruhend und mit einer sicheren Signiereinheit erstellt. Der Nachweis dieser Merkmale kann entweder ex post erbracht werden[430] oder aber, indem dargelegt wird, dass es sich um eine Signatur handelt, welche auf einem Zertifikat eines ex ante geprüften Anbieters beruht.

3. Internationale Aspekte

311 Der ex-post-Ansatz erlaubt eine einfache Anerkennung von auf ausländischen Zertifikaten basierenden Signaturen anhand abstrakter, nicht herkunftsabhängiger Kriterien. Wird indessen ein ex-ante-Ansatz gewählt, ist die Frage zu beantworten, was mit Signaturen zu geschehen hat, die auf Zertifikaten ausländischer Anbieter beruhen. Insoweit stehen erneut verschiedene Regelungsmodelle zur Auswahl:

312 • Zunächst ist es möglich, ausländische Anbieter einfach zum *normalen Anerkennungsprozedere* zuzulassen.[431] Dabei ist für ausländische Anbieter jedoch eine zusätzliche Prüfung bzw. Kontrolle durch einen anderen als deren Heimatstaat nötig, mit entsprechend höheren Kosten und umgekehrt reduziertem Wettbewerbsdruck für die inländischen Anbieter.[432]

313 • Daher ist es unter Umständen sinnvoll, im Ausland bereits anerkannte Anbieter einem *erleichterten Anerkennungsprozedere* zu unterwerfen. Die Anbieter haben dabei etwa darzulegen, dass die ausländischen Normen gleichwertig zu den inländischen sind, können sich aber die Detailprüfung ersparen.[433]

314 • Ein weiterer Weg ist die *pauschale staatsvertragliche Anerkennung* sämtlicher in einem bestimmten Staat anerkannten Anbieter. Sie hat den Vorteil, dass für in-

---

428 Vorne N 275 f.
429 Eingehend hinten N 456 ff.
430 Was zwar noch immer mit gewissen Unsicherheiten behaftet ist, aber gleichwohl einfacher als der praktisch kaum zu erbringende Nachweis der Echtheit der Signatur.
431 Vgl. Art. 4 Abs. 2 VE-BGES.
432 PESTALOZZI/VEIT, 604, sprechen von «neuen technischen Handelshemmnissen».
433 Der E-ZertES sieht in Art. 3 Abs. 2 eine solche Lösung vor; hinten N 525.

ländische Anbieter in diesem Staat Gegenrecht verlangt werden und dass eine zweite Anerkennung für die Anbieter ganz unterbleiben kann.[434]

- Ferner können die in bestimmten Staaten anerkannten Anbieter auch *ex lege* anerkannt werden. Dabei entfällt aber die genannte Möglichkeit, für inländische Anbieter Gegenrecht zu verlangen.[435] 315
- Schliesslich lassen sich im Sinne des geschilderten *ex-post-Ansatzes* zusätzlich zu den Regeln zur Anerkennung abstrakte Kriterien definieren, nach denen ein Zertifikat trotz fehlender Anerkennung des Anbieters die im Gesetz statuierten Rechtsfolgen nach sich ziehen soll (dies entspricht dem geschilderten kombinierten Ansatz der EU-Signaturrichtlinie[436]). Eine Anerkennung des Anbieters entfällt diesfalls, die Lösung birgt jedoch die genannten Nachteile des ex-post-Ansatzes.[437] 316

V. Risikoverteilung und Haftungsordnung

Ob überhaupt Regelungsbedarf für eine gesonderte Haftungsordnung besteht, war ursprünglich umstritten. Das erste deutsche Signaturgesetz von 1997 sah beispielsweise gar keine Haftungsnormen vor, weil davon ausgegangen wurde, die bestehenden Regeln würden ausreichen.[438] 317

Die Problematik einer fehlenden Regelung liegt indessen zum einen in Begründung der (ausservertraglichen) Haftung der Zertifizierungsdiensteanbieter gegenüber Dritten, die sich auf deren Zertifikate verlassen, und zum andern ist allein aus der Tatsache, dass jemand ein Zertifikat besitzt, noch nicht unbedingt seine Pflicht herzuleiten, den Signierschlüssel geheim zu halten. 318

Auf die Haftung der Zertifizierungsdiensteanbieter wird im Rahmen dieser Abhandlung nur summarisch eingegangen. Es sei auf die Dissertation von DÖRR verwiesen.[439] 319

---

434 Botschaft ZertES, 5714; Felix SCHÖBI, zit. bei SCHLAURI, Bundesgesetz, 363; der E-ZertES sieht zusätzlich zur individuellen Anerkennung eine solche pauschale staatsvertragliche Anerkennung vor; Art. 19 E-ZertES.

435 So etwa auch Felix SCHÖBI, zit. bei SCHLAURI, Kommunikation. Der Ansatz der ex-lege-Anerkennung der Anbieter wurde in der Vernehmlassung zum VE-BGES für die in der EU anerkannten Anbieter gefordert; SWICO, in: Zusammenstellung der Vernehmlassungen zum E-ZertES, 139.

436 Vorne N 293.

437 N 282.

438 Hinten N 403.

439 Vorne N 6.

VI. Öffentliches Recht und Strafrecht

320 Im Bereiche des öffentlichen Rechts (vornehmlich Verwaltungsrecht) kann durch elektronische Signaturen die Grundlage für elektronische Kommunikation zwischen Bürgern und Staat sowie zwischen Behörden geschaffen werden. Die Zulässigkeit des elektronischen Behördenverkehrs und die Anerkennung der elektronischen Signatur sind hier aufgrund des Legalitätsprinzips gesetzlich zu regeln.[440]

321 Wo die Haftungsnormen nicht ausreichen, um die Beteiligten zu disziplinieren, sind im Weiteren allenfalls Strafnormen vorzusehen. So stellte etwa Art. 22 VE-BGES die Ausfertigung von angeblich gesetzeskonformen Zertifikaten durch nicht anerkannte Zertifizierungsdiensteanbieter unter Strafe. Das deutsche Signaturgesetz von 2001 weist gar einen ausführlichen Bussenkatalog auf.[441]

322 Der E-ZerES verzichtet nun indessen auf Strafnormen und ersetzt diese in Art. 16 durch eine Ausweitung der Haftung auch auf nicht anerkannte Zertifizierungsdiensteanbieter. Anwendbar bleiben aber auf jeden Fall die lauterkeitsrechtlichen Strafnormen sowie die Normen des Bundesgesetzes über die technischen Handelshemmnisse.[442]

323 Eine Revision des *Urkundenstrafrechts* erübrigt sich, weil Aufzeichnungen auf Bild- und Datenträgern bereits de lege lata unter den strafrechtlichen Urkundenbegriff nach Art. 110 Ziff. 5 StGB fallen, sofern sie Urkundenfunktion erfüllen.[443]

---

440 Eingehender KIG, Bericht 3, 46 f.
441 § 21 SigG 01.
442 Hinten N 542 ff., 551.
443 Zum Urkundenstrafrecht etwa Niklaus SCHMID, Computer- sowie Check- und Kreditkarten-Kriminalität, Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994, 41 ff.

§ 7 Einige wichtige ausländische Regelungen im Überblick

I. Gang der Darstellung

Bevor auf die schweizerischen Entwürfe eingegangen wird, soll die Materie anhand bereits verabschiedeter ausländischer Regelungen dargelegt werden. Ziel ist dabei weniger eine detailreiche Darstellung der einzelnen Regelungen als eine solche, die sich auf die groben Striche beschränkt und dem Leser ermöglichen soll, die schweizerischen Vorschläge im internationalen Kontext zu sehen. 324

Zum Einstieg soll anhand des UNCITRAL-Modellgesetzes über elektronische Signaturen ein Überblick über die den Regelungen zu Grunde liegenden Prinzipien geschaffen werden. Hernach wird die für die Schweizer Regelung sehr bedeutsame EU-Signaturrichtlinie dargestellt und am Schluss mit dem deutschen Signaturgesetz eine ihrer Umsetzungsvarianten. Eine Darstellung der US-amerikanischen Gesetzgebung würde indessen den Rahmen dieser Abhandlung sprengen.[444] 325

II. UNCITRAL

A. Einführung

Die *United Nations Commission on International Trade Law (UNCITRAL)* wurde 1966 durch die UNO-Generalversammlung gegründet. Die Kommission erhielt das Mandat, die Harmonisierung und Vereinheitlichung des internationalen Handelsrechts voranzutreiben; sie ist zur zentralen Behörde der UNO im Bereich des internationalen Handelsrechts geworden und hat sich bisher etwa mit internationalem Güterverkehr und damit zusammenhängenden Transaktionen,[445] internationaler Schiedsgerichtsbarkeit, öffentlichem Beschaffungswesen, internationalen Zahlungs- 326

---

444 Dazu etwa AMERICAN BAR ASSOCIATION, 1 ff.; BAKER & MCKENZIE, Electronic and Digital Signature Resources, http://www.bmck.com/ecommerce/topic-esignatures.htm m.H.; BÜLLESBACH/RIESS/MIEDBRODT, 16 ff.; François DESSEMONTET, The European Approach to E-Commerce and Licensing, Brooklyn Journal of International Law, 1/2000, 59 ff.; KUNER/MIEDBRODT; MIEDBRODT, 119 ff.; Anja MIEDBRODT, Das Signaturgesetz in den USA, Electronic Signatures in Global and National Commerce Act, DuD 9/2000, 541 ff.; DIESELBE, Regelungsansätze und -strukturen US-amerikanischer Signaturgesetzgebung, DuD 7/1998, 389 ff.; Stephan SCHUMACHER, Digitale Signaturen in Deutschland, Europa und den U.S.A., Ein Problem, zwei Kontinente, Drei Lösungen?, CR 12/1998, 759 ff.; VAN DEN HOF; Bill ZOELLICK, Electronic Signatures, Commentary on the Electronic Signatures in Global and National Commerce Act, http://www.fastwater.com/Library/B2BEconomy/DigitalSigs/DigSig-Commentary.php3.

445 Aus diesen Bemühungen entstand das Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf («Wiener Kaufrecht»), SR 0.221.211.1.

systemen sowie elektronischem Geschäftsverkehr beschäftigt.[446] Die UNCITRAL-Generalversammlung wird derzeit von vier Arbeitsgruppen zur Durchführung von Vorbereitungsarbeiten unterstützt; eine davon ist die *UNCITRAL Working Group on Electronic Commerce*.[447]

327 Die erarbeiteten Dokumente können als *Konventionen*, *Modellgesetze*, *Legal Guides* oder *Statements of Principle* ausgestaltet werden.[448] Konventionen haben bindenden Charakter.[449] Modellgesetze sollen den UNO-Mitgliedstaaten als Beispiele für die eigene Gesetzgebung dienen und haben lediglich Empfehlungscharakter.[450] Legal guides und Statements of Principle enthalten keine Regelungsvorschläge, beschreiben jedoch die in einem bestimmten Gebiet auftretenden Rechtsfragen bzw. entsprechenden Prinzipien und sind damit Entscheidungshilfen sowohl für nationale Gesetzgeber als auch für privat tätige Juristen, die vertragliche Regelungen entwerfen wollen.[451]

B. Model Law on Electronic Commerce

328 Am 16. Dezember 1996 verabschiedete die UNCITRAL-Generalversammlung ein Modellgesetz zum elektronischen Geschäftsverkehr (*UNCITRAL Model Law on Electronic Commerce*).[452] Es bezweckt, den nationalen Gesetzgebern eine Zusammenstellung von international akzeptierbaren Regeln zur Verfügung zu stellen, um damit rechtliche Hindernisse für den elektronischen Geschäftsverkehr zu beseitigen und Rechtssicherheit zu schaffen.[453]

329 Das Model Law basiert auf dem Ansatz der *funktionalen Äquivalenz (functional equivalence approach)*. Dabei wird der Anwendungsbereich von rechtlichen Begriffen wie «Schrift», «Unterschrift» oder «Original» ausgedehnt, was vermeiden soll, die auf traditioneller Schriftform basierenden Normen modifizieren zu müssen und dadurch die dahinter stehenden Konzepte zu verändern. Der Ansatz der funktionalen Äquivalenz beruht auf einer Analyse der Zwecke und Funktionen der traditionellen papierbasierten Regeln und der Frage danach, wie diese Zwecke und Funktionen auch auf dem Wege der elektronischen Kommunikation erfüllt werden könnten.[454]

330 Das Modellgesetz behandelt folgende Aspekte:

- Rechtliche Anerkennung von Datennachrichten *(data messages);*

---

446 Zum Ganzen WOLFRUM, 120 N 1 ff.
447 BLUM, UNCITRAL, 64; Helmut VOLGER (Hrsg.), Lexikon der Vereinten Nationen, München/Wien 2000, 535; WOLFRUM, 120 N 9.
448 So etwa Gerold HERRMANN, The UNCITRAL Arbitration Law: a Good Model of a Model Law, ULR/RDU 1998, 483 ff., 483; ROSE, 14.
449 JAEGER, 36 f.
450 Vgl. etwa MLES Guide to Enactment, § 26; JAEGER, 36 f.; WULFF, 23.
451 WULFF, 20 f.; ROSE, 14.
452 UNCITRAL, 2.
453 MLEC Guide to Enactment, § 2.
454 MLEC Guide to Enactment, § 15 ff.

- Schriftlichkeit;
- Unterschrift;
- Original eines Dokumentes;
- Aufbewahrung von Dokumenten;
- Elektronischer Austausch von Willenserklärungen;
- Zuschreibung von Datennachrichten, die durch Vertreter oder Computer erzeugt wurden;
- Empfangsbestätigung;
- Versand- und Empfangszeitpunkt;
- Güterverkehr und Transportdokumente.

331 Interessant ist an dieser Stelle in erster Linie Artikel 7 des Modellgesetzes, der besagt, dass ein elektronisches Signaturverfahren dann als funktional äquivalent zur Handunterschrift gilt, wenn es erstens den Unterzeichner identifiziert und dessen Willen ausdrückt, sich die in der Datennachricht enthaltene Information anrechnen zu lassen und zweitens einen dem Zweck der Datennachricht angemessenen Grad an Zuverlässigkeit aufweist. Der Artikel basiert damit auf den zwei grundlegendsten Funktionen der Unterschrift, der Beweis- und der Rekognitionsfunktion.[455]

C. Model Law on Electronic Signatures

1. Entstehung

332 Die Regelung von Art. 7 des Model Law on Electronic Commerce lässt eine Reihe von Fragen im Bereich der elektronischen Signatur unbeantwortet, weshalb die UNCITRAL im Jahre 1996 die Working Group on Electronic Commerce beauftragte, die Wünschbarkeit und Machbarkeit detaillierterer einheitlicher Regeln für diesen Bereich abzuklären.[456] Diese Abklärungen führten zu einem positiven Resultat, worauf die Arbeit im Januar 1998 aufgenommen wurde.[457] Im September 2000 wurden diese Regeln als Modellgesetz *(UNCITRAL Model Law on Electronic Signatures, MLES)* verabschiedet.[458] Ende 2001 waren noch Arbeiten am *Guide to Enactment* (einer Art Kommentar) im Gange.

---

455 MLEC Guide to Enactment, §§ 53 ff., 56; mehr zu den Funktionen der Unterschrift hinten N 833 ff.
456 MLES Guide to Enactment, § 12.
457 MLES Guide to Enactment, § 13-15.
458 MLES Guide to Enactment, § 25.

2. Überblick über die Regelung

a) Allgemeines

333 Das MLES statuiert eine Reihe abstrakter Grundregeln und Prinzipien zum Umgang mit elektronischen Signaturen.

b) Anwendungsbereich

334 Der Anwendungsbereich des Modellgesetzes beschränkt sich gemäss Art. 1 auf den kommerziellen Kontext. Normen mit Konsumentenschutzzweck sind explizit ausgenommen.

c) Definitionen

335 Art. 2 MLES definiert die elektronischen Signatur sehr weit als «Daten in elektronischer Form, die einer Datennachricht beigefügt oder logisch mit dieser verknüpft sind, die zur Identifikation des Unterzeichners bezüglich dieser Datennachricht verwendet werden können und die Anerkennung des in der Datennachricht enthaltenen Textes durch den Unterzeichner ausdrücken.»[459] Die Definition folgt dem geschilderten funktionalen Ansatz.[460] Anders als noch in einigen Entwürfen vorgesehen, verzichtet das MLES auf unterschiedliche Signaturtypen.[461]

d) Technologieneutralität

336 Eine der bedeutendsten Forderungen des MLES ist das in Art. 3 festgehaltene Prinzip der *Technologieneutralität*[462], gemäss dem in den Gesetzen die Möglichkeit offen gehalten werden soll, zu einem späteren Zeitpunkt heute noch unbekannte Verfahren anzuerkennen (Wettbewerbsneutralität).[463] Gedacht wurde dabei etwa an Verfahren mit Biometrie, Passwörtern, digitalisierten Handunterschriften o.ä.[464] Insbesondere sollen die Staaten auch Techniken anerkennen, die nicht mit Public-Key-Kryptographie arbeiten. Dem entspricht auch die soeben zitierte weite Definition der elektronischen Signatur, die nicht nur Public-Key-Verfahren umfassen soll. Weil das MLES auch für in geschlossenen Benutzergruppen eingesetzte Systeme Bedeutung hat,[465] ist der Ansatz der Technologieneutralität an dieser Stelle sinnvoll.[466]

---

459 "Data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message."

460 Vorne N 329.

461 Der ursprünglich vorgesehene zweistufige Ansatz mit sicheren und weniger sicheren Signaturen hat jedoch in der EU-Signaturrichtlinie seinen Niederschlag gefunden; BLUM, UNCITRAL, 65; hinten N 375 ff.

462 Teilweise wird auch von *Principle of Non-Discrimination* gesprochen; MLES Guide to Enactment, § 106.

463 MLES Guide to Enactment, § 106.

464 MLES Guide to Enactment, §§ 33 f., 82; BLUM, UNCITRAL, 64.

465 Hinten N 339.

466 Vgl. auch vorne N 303 ff.

Obwohl das MLES von Technologieneutralität ausgeht, nimmt es in einigen Bestimmungen auf die allein für Public-Key-Verfahren relevanten Zertifizierungsdienste Bezug, freilich unter dem Vorbehalt, dass sich eine elektronische Signatur tatsächlich auf solche stützt.[467] 337

e) Auslegung

Bei der Auslegung der auf dem MLES basierenden Gesetze ist gemäss Art. 4 MLES der internationale Ursprung der Regeln zu beachten, und bei der Lückenfüllung ist auf die dem MLES zugrunde liegenden Prinzipien Rücksicht zu nehmen. 338

f) Parteiautonomie

Die Anwender elektronischer Signaturen sind nach Art. 5 MLES frei, die Anforderungen an die zwischen ihnen eingesetzten elektronischen Signaturen durch vertragliche Übereinkunft zu heben oder zu senken. Nicht explizit geregelt ist das Verhältnis dieser Freiheit zu Interessen Dritter oder des Staates, welche durch parteiautonom modifizierte Regelungen tangiert werden könnten; laut Guide to Enactment werden zwingende Vorschriften durch Art. 5 nicht berührt.[468] 339

g) Anerkennung und Echtheitsvermutung

Art. 6 MLES bestimmt, dass elektronische Signaturen, die eine für den Zweck der signierten Nachricht angemessene Sicherheit aufweisen, die gesetzlichen (Absatz 1) oder gewillkürten (Absatz 2) Formvorschriften erfüllen sollen; das MLES folgt damit einem funktionalen ex-ante-Ansatz, was angesichts der internationalen Ausrichtung nicht verwundert. Art. 6 entspricht diesbezüglich Art. 7 des Model Law on Electronic Commerce.[469] Wie erwähnt beschlägt das MLES ausschliesslich den kaufmännischen Verkehr;[470] der Warnzweck[471] der Unterschrift, der vor allem im Konsumentenbereich relevant ist, kann daher vernachlässigt werden, und die Frage, ob eine Signatur ein Schriftformerfordernis erfüllen kann, hängt in erster Linie von der Sicherheit der eingesetzten Verfahren ab (Beweisfunktion).[472] 340

Absatz 3 definiert zusätzlich zu den Absätzen 1 und 2 einen (nicht abschliessenden) Katalog von Kriterien zur Beurteilung der Sicherheit mit dem Ziel, für die Anwender Rechtssicherheit zu schaffen.[473] Der Guide to Enactment geht davon aus, Absatz 3 beantworte die Frage der Anerkennung im Sinne von Absatz 1 *ex ante*, im Gegensatz zur *ex-post*-Anerkennung von Art. 7 MLEC.[474] Ein ex-post-Ansatz kann jedoch aufgrund seiner generell-abstrakten Natur auch durch eine noch so weitgehende Konkre- 341

467 Vgl. Art. 9 MLES; dazu hinten N 346.
468 MLES Guide to Enactment, § 110.
469 Vorne N 332.
470 Vorne N 334.
471 Dazu hinten N 857 ff.
472 Dazu hinten N 847 ff.
473 MLES Guide to Enactment, § 117.
474 MLES Guide to Enactment, § 117; zu den Begriffen schon vorne N 280 ff.

tisierung nicht in einen ex-ante-Ansatz umgewandelt werden. Diesem entspricht erst das Konzept von Art. 7 MLES, gemäss dem die Staaten die Möglichkeit haben, eine ex-ante-Prüfung sicherer Verfahren vorzusehen.[475]

342 Ob das Kriterium der Sicherheit nach Art. 6 (1) MLES bei Vorliegen der im Katalog von Abs. 3 beschriebenen Merkmale bloss widerleglich vermutet wird *(presumption)* oder ob die Akzeptanz einer elektronischen unmittelbar von den aufgestellten Kriterien abhängt (*substantive rule;* unwiderlegbare Vermutung), wird den nationalen Gesetzgebern überlassen.[476]

343 Von einer solchen Vermutung der Sicherheit (welche als Rechtsfolge die Anerkennung einer Signatur nach sich zieht) sind die Vermutung der Echtheit einer Signatur und (davon abhängig) die Vermutung, dass ein Unterzeichner durch das Setzen der Signatur den signierten Text anerkannte *(presumption of signing; Vermutung der Rekognition)*, zu unterscheiden. Die Frage nach der Notwendigkeit einer presumtion of signing war heftig umstritten.[477] Anders als noch in einigen Entwürfen vorgesehen,[478] erwähnt sie die Endfassung des MLES nicht mehr. Die Frage, ob eine solche Vermutung bestehen soll, wird damit weiterhin durch das nationale Recht entschieden.[479]

h) Pflichten der Beteiligten

344 Signierschlüsselhalter, Zertifizierungsdiensteanbieter und auf die Signatur vertrauende Dritte haben bestimmte Pflichten zu befolgen. Grundsätzlich haben sie mit angemessener Sorgfalt zu handeln und/oder angemessene Mittel zur Verfügung zu stellen, um Missbräuche zu verhindern oder aufzudecken. Zudem werden eine Reihe konkreter Pflichten statuiert.

345 *Der Signierschlüsselhalter* muss nach Art. 8 MLES

- den nichtautorisierten Gebrauch seines Signierschlüssels mit angemessener Sorgfalt zu verhindern suchen;
- sofern sein Signierschlüssel kompromittiert wurde oder ein erhebliches entsprechendes Risiko besteht, dass dies geschehen ist, ohne ungebührliche Verzögerung jede Person benachrichtigen, von der er vernünftigerweise ausgehen muss, dass sie sich auf seine elektronische Signatur verlassen würde;
- und wenn ein Zertifikat zum Einsatz kommt, angemessene Sorgfalt walten lassen, um die Richtigkeit und Vollständigkeit der darin enthaltenen Daten zu gewährleisten.

---

475 MLES Guide to Enactment, § 127 ff.
476 MLES Guide to Enactment, § 118; vgl. BLUM, UNCITRAL, 66.
477 BLUM, UNCITRAL, 66.
478 Vgl. etwa Artikel 6 (1) des Entwurfs vom 29. Juni 1999, A/CN.9/WG.IV/WP.82, http://www.uncitral.org/english/workinggroups/wg_ec/wp-82.pdf.
479 Dazu schon BLUM, UNCITRAL, 66; MLES Guide to Enactment, § 119; vgl. zur Rekognition hinten N 836 ff.

Sofern ein Zertifizierungsdiensteanbieter involviert ist, muss dieser nach Art. 9 MLES 346

- entsprechend der in seinem Certification Practice Statement[480] gemachten Aussagen handeln;
- angemessene Sorgfalt walten lassen, um die Richtigkeit und Vollständigkeit der im Zertifikat enthaltenen Daten zu gewährleisten;
- den auf Signaturen vertrauenden Dritten auf angemessene Weise zugängliche Mittel zur Verfügung stellen, um sich über die relevanten Daten zu informieren;[481]
- auf angemessene Weise zugängliche Mittel zur Verfügung stellen für eine Information der auf die Signatur vertrauenden Dritten im Kompromittierungsfalle und für die Zertifikatssperrung, falls derartige Dienste vorgesehen sind und
- vertrauenswürdige Systeme[482] einsetzen.[483]

Der *auf eine Signatur vertrauende Dritte* muss nach Art. 11 MLES 347

- die angemessenen Schritte unternehmen, um die Zuverlässigkeit einer Signatur zu überprüfen und
- die angemessenen Schritte unternehmen, um die Gültigkeit, Suspendierung oder Sperrung eines einer Signatur allfällig zu Grunde liegenden Zertifikats überprüfen und dessen allfällige Nutzungs- oder Transaktionswertbeschränkungen beachten.

i) Internationale materiellrechtliche Anerkennung

Ausländische Zertifikate und elektronische Signaturen dürfen gemäss Art. 12 MLES 348 nicht aufgrund ihrer geografischen Herkunft oder dem Ort der Niederlassung des Zertifizierungsdiensteanbieters diskriminiert werden.[484] Sofern eine ausländische elektronische Signatur oder ein Zertifikat eine im Wesentlichen zu inländischen Signaturen äquivalente Sicherheit bietet, so sollen sie die gleichen Rechtsfolgen nach sich ziehen. Zur Beurteilung der Sicherheit sind internationale Standards beizuziehen. Aus diesem Grund wird Art. 6 MLES seine Bedeutung auch dann nicht verlieren, wenn eine ex-ante-Prüfung nach Art. 7 vorgesehen ist (kombinierte Lösung von ex-ante- und ex-post-Regelungsansatz).[485]

---

480 Vorne N 81.

481 Dazu gehören die Identität von Zertifizierungsdiensteanbieter und Signierschlüsselhalter, Gültigkeit des Signierschlüssels und Kontrolle des Halters, Identifikationsmethode bei der Zertifizierung, Nutzungs- oder Transaktionswertbeschränkungen des Zertifikats, Haftungsbeschränkungen des Zertifizierungsdiensteanbieters sowie die Frage, ob eine Revokation möglich ist; Art. 9(1)(d) MLES.

482 Art. 10 MLES definiert einen (nicht abschliessenden) Kriterienkatalog, um diese Vertrauenswürdigkeit zu bestimmen.

483 Dazu etwa auch EMMERT, 249.

484 Vgl. auch N 336.

485 Vorne N 293.

349 Vereinbaren die Parteien, im internationalen Verkehr bestimmte Signaturen oder Zertifikate zu verwenden, so soll diese Vereinbarung für die grenzüberschreitende Anerkennung ausreichend sein.

III. EU-Richtlinienrecht

A. Überblick und Gang der Darstellung

350 Der elektronische Geschäftsverkehr ist für die Entwicklung des europäischen Binnenmarktes von grosser Bedeutung. Unterschiedliche Regelungen können in diesem Bereich zu Handelshemmnissen führen, was es zu vermeiden gilt. Die Europäische Union hat daher eine Reihe von *Richtlinien*[486] verabschiedet, welche eine *Harmonisierung* der Rechtsordnungen in diesem Bereich bewirken sollen.

351 In einem näheren Zusammenhang mit elektronischen Signaturen stehen die *Fernabsatzrichtlinie*[487], welche jedoch nicht nur den elektronischen Geschäftsverkehr, sondern den Fernabsatz im Allgemeinen betrifft (d.h. etwa auch telefonische oder schriftliche Bestellungen)[488], die *E-Commerce-Richtlinie*[489], die unter anderem elektronische Vertragsabschlüsse regelt, und schliesslich natürlich die *Signaturrichtlinie*[490], die einen Rechtsrahmen für elektronische Signaturen aufzieht. Hinzu kommt ein *Entwurf für eine Richtlinie über den Fernabsatz von Finanzdienstleistungen*[491], der die Anliegen der Fernabsatzrichtlinie auch im Bereich der Finanzdienstleistungen verfolgen will.

352 Bevor auf die Signaturrichtlinie eingegangen wird, wird im Folgenden mit einem Abriss über die Fernabsatz- und E-Commerce-Richtlinie der allgemeinere EU-Rechtsrahmen für den E-Commerce geschildert.

---

486 Richtlinien der Europäischen Union sind, im Gegensatz zu *Verordnungen*, nur hinsichtlich ihres Ziels, nicht jedoch hinsichtlich der anzuwendenden Mittel für die Mitgliedstaaten relevant. Sie müssen von den Mitgliedstaaten jeweils binnen einer bestimmten Frist in das nationale Recht übernommen (umgesetzt) werden. Dazu statt vieler Matthias HERDEGEN, Europarecht, 3. A. München 2001, N 177 ff.

487 Richtlinie 97/7/EG des Europäischen Parlaments und des Rates vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz; ABl. 1997 L 144/19ff.

488 MORITZ, 66.

489 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs; ABl. 2000 L 178/1 ff.

490 Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen; ABl. 2000 L 13/12 ff.

491 Vorschlag des Europäischen Parlaments und des Rates vom 23. Juli 1999 für eine Richtlinie über den Fernabsatz von Finanzdienstleistungen an Verbraucher und zur Änderung der Richtlinie 97/7/EG und 98/27/EG, KOM (1999) 385 endg.

B. Fernabsatzrichtlinie

1. Überblick

Die am 20. Mai 1997 verabschiedeten Fernabsatzrichtlinie[492] bezweckt die Vereinheitlichung des Verbraucherschutzes[493] bei Fernabsatzgeschäften[494] und will damit die Verwirklichung des Binnenmarktes fördern und das Ansehen der Fernabsatzbranche erhöhen.[495] Die Richtlinie war bis Juni 2000 umzusetzen.[496] Sie sieht ein auf drei Säulen basierendes Schutzkonzept vor:[497] 353

- Im Fernabsatz besteht die Gefahr, dass der Verbraucher ungenügend über Identität des Lieferanten, wesentliche Eigenschaften der Ware u.dgl. informiert wird.[498] Zudem ist er sich möglicherweise nicht über die ihm zustehenden Rechte im Klaren.[499] Der Verbraucher soll daher gemäss Art. 4 Fernabsatzrichtlinie vorvertraglich über eine Reihe von Punkten unterrichtet werden.[500] 354
- Mit Hilfe elektronischer Technologien übermittelte Information ist häufig nicht beständig. Die durch den Art. 4 Fernabsatzrichtlinie geforderte Information soll dem Verbraucher daher gemäss Art. 5 der Richtlinie schriftlich oder auf einem für ihn verfügbaren Datenträger bestätigt werden.[501] 355
- Der Verbraucher hat regelmässig keine Möglichkeit, das bestellte Erzeugnis vor Vertragsabschluss zu sehen oder die Eigenschaften einer Dienstleistung ausreichend zur Kenntnis zu nehmen (keine *«goods-in-hand»*-Entscheidung).[502] Er er- 356

---

492 Soeben FN 487.

493 *Verbraucher* im Sinne von Art. 2 Abs. 2 Fernabsatzrichtlinie ist eine natürliche Person, die beim Abschluss von Verträgen im Sinne der Richtlinie zu Zwecken handelt, die nicht ihrer gewerblichen oder beruflichen Tätigkeit zugerechnet werden können.

494 Unter einem Vertragsabschluss im Fernabsatz versteht die Richtlinie jeden zwischen einem Lieferer und einem Verbraucher geschlossenen, eine Ware oder eine Dienstleistung betreffenden Vertrag, der im Rahmen eines für den Fernabsatz organisierten Vertriebs- bzw. Dienstleistungssystems des Lieferers geschlossen wird, wobei dieser für den Vertrag bis zu dessen Abschluss einschliesslich des Vertragsabschlusses selbst ausschliesslich eine oder mehrere Fernkommunikationstechniken verwendet; Art. 2 Nr. 1 und vorausgehende Bemerkung 9 Fernabsatzrichtlinie; VEHSLAGE, 546. Von Bedeutung ist insbesondere, dass nur Verträge mit Lieferern, die ein auf den Fernabsatz ausgerichtetes Vertriebs- bzw. Dienstleistungssystem betreiben, betroffen sind. Der Betreiber eines Geschäftes, der nur gelegentlich auf dem Wege des Fernabsatzes Produkte versendet, wird damit nicht erfasst; dazu und zu den aus der unscharfen Formulierung entstehenden Abgrenzungsschwierigkeiten etwa MEENTS, 184 ff.

495 Fernabsatzrichtlinie, vorausgehende Erwägung 1; MEENTS, 173 f.

496 Art. 18 i.V.m. Art. 15 Abs. 1 der Richtlinie; für ein Umsetzungsbeispiel vgl. das deutsche Fernabsatzgesetz, BGBl. I, S. 897 ff.; dazu insbesondere VEHSLAGE, 546 ff.; vgl. auch KÖNIG, Praxis, 160; MÖCKE, 34; Frank MÖCKE, Angstschweiss beim Discounter, Rücksenderecht für Versandartikel ist nun Gesetz, c't 14/2000, 48.

497 Eingehend MEENTS, 173 ff.; vgl. etwa auch MÖCKE, 34; KÖNIG, Praxis, 160; VEHSLAGE, 546 ff.

498 Fernabsatzrichtlinie, vorausgehende Erwägung 11; MORITZ, 62.

499 Fernabsatzrichtlinie, vorausgehende Erwägung 19.

500 Zur Umsetzung in *Deutschland* VEHSLAGE, 547.

501 Fernabsatzrichtlinie, vorausgehende Erwägung 13; zur Umsetzung in *Deutschland* VEHSLAGE, 547; zum dauerhaften Datenträger und der Frage, ob E-Mail hierfür ausreicht HÄRTING, 310 ff.

502 Fernabsatzrichtlinie, vorausgehende Erwägung 14; HONSELL/PIETRUSZAK, 785.

hält daher nach Art. 6 der Richtlinie ein nachträgliches Widerrufsrecht von mindestens sieben Tagen,[503] das er ohne Angabe von Gründen, allerdings gegen Erstattung der Kosten für den Rücktransport, geltend machen kann.[504] Ein derartiges Widerrufsrecht kann ebenfalls als Kompensation der durch den Einsatz elektronischer Signaturen möglicherweise verloren gegangenen Warnfunktion der gesetzlich vorgesehenen Schriftform dienen[505] und so den Einsatz elektronischer Signaturen auch im Konsumentenbereich ermöglichen.[506]

357 Ferner enthält die Richtlinie unter anderem Vorschriften zur Erfüllung von Verträgen, zum Einsatz von Zahlungskarte, lauterkeitsrechtliche Regeln sowie Regeln über die zivilprozessualen Durchsetzungsmöglichkeiten.[507]

2. Ausnahmen vom Anwendungsbereich

358 Vom Anwendungsbereich der Richtlinie vollständig ausgeschlossen sind nach Art. 3 unter anderem Finanzdienstleistungen (inklusive E-Banking),[508] Verträge über den Bau von Immobilien, Verträge, die unter Verwendung von Warenautomaten u. dgl. zu Stande kommen und Versteigerungen.[509] Weitere Bereiche, die ausgenommen werden, sind etwa die Lieferung von Produkten des täglichen Bedarfs, die vom Händler im Rahmen häufiger oder regelmässiger Fahrten geliefert werden und gewisse Verträge, die eine Erfüllung zu einem bestimmten Zeitpunkt vorsehen.[510]

C. Richtlinienentwurf zum Fernabsatz von Finanzdienstleistungen

359 Am 19. Dezember 2001 verabschiedete der Rat einen gemeinsamen Standpunkt für eine Richtlinie über den Fernabsatz von Finanzdienstleistungen. Diese Richtlinie soll unter anderem die Anliegen der Fernabsatzrichtlinie auch im Bereich der Finanzdienstleistungen verfolgen.[511] Sie soll dazu etwa Informationspflichten und ein im Vergleich zur Fernabsatzrichtlinie auf 14-30 Tage verlängertes Widerrufsrecht einführen (um Spekulationsgeschäfte zu Lasten des Anbieters auszuschliessen allerdings nicht im Bereich von Instrumenten mit schwankendem Wert).[512]

---

503 Die Frist beginnt, wenn die Informationspflichten gemäss Art. 5 der Richtlinie erfüllt sind, bei Waren mit dem Tag des Eingangs beim Verbraucher und bei Dienstleistungen mit dem Vertragsabschluss; Art. 6 der Richtlinie.

504 MORITZ, 67; zur Umsetzung in *Deutschland* VEHSLAGE, 547 f.; kritisch HONSELL/PIETRUSZAK, 776 ff.

505 So etwa Botschaft ZertES, 5687.

506 Mehr dazu hinten N 923 f., 926 ff.

507 MORITZ, 67.

508 Im Anhang der Richtlinie gesondert aufgelistet; Finanzdienstleistungen wurden vom Geltungsbereich der Richtlinie ausgenommen, weil eine separate Regelung für zweckmässiger gehalten wurde; MEENTS, 209 ff.; zu dieser separaten Regelung N 359.

509 Eingehend MEENTS, 208 ff.; MORITZ, 66.

510 MORITZ, 66.

D. E-Commerce-Richtlinie

1. Allgemeines

Am 8. Juni 2000 verabschiedeten das Europäische Parlament und der Rat eine *Richtlinie über den elektronischen Geschäftsverkehr*[513] *(E-Commerce-Richtlinie)*. Ziel ist die Förderung des elektronischen Geschäftsverkehrs im Binnenmarkt und der Wettbewerbsfähigkeit der europäischen Wirtschaft. Mittel dazu ist die Harmonisierung von Vorschriften zum elektronischen Geschäftsverkehr.[514] Die Richtlinie musste bis zum 17. Januar 2002 in nationales Recht umgesetzt werden.[515] 360

2. Dienste der Informationsgesellschaft

Die Richtlinie betrifft den freien Verkehr so genannter *Dienste der Informationsgesellschaft*. Darunter sind Dienstleistungen zu verstehen, «die in der Regel gegen Entgelt im Fernabsatz mittels Geräten für die elektronische Verarbeitung (einschliesslich digitaler Kompression) und Speicherung von Daten auf individuellen Abruf eines Empfängers erbracht werden»[516], also etwa der Online-Verkauf von Waren, Informationsübermittlung über Kommunikationsnetze, Zugangsvermittlung zu Kommunikationsnetzen, kommerzielle Kommunikation (Werbung), Online-Informationsdienste, Instrumente zur Datensuche u. dgl.[517] Die Richtlinie fasst Regeln zur Niederlassung der Diensteanbieter, kommerziellen Kommunikation, elektronischem Vertragsabschluss und Verantwortlichkeit der Vermittler in Kommunikationsnetzen zusammen. 361

---

511 Gemeinsamer Standpunkt des Rates vom 19. Dezember 2001 im Hinblick auf den Erlass der Richtlinie des Europäischen Parlaments und des Rates über den Fernabsatz von Finanzdienstleistungen an Verbraucher und zur Änderung der Richtlinie 90/619/EWG des Rates und der Richtlinien 97/7/EG und 98/27/EG; http://register.consilium.eu.int/pdf/de/01/st12/12425-r1d1.pdf. Vgl. auch René HÖLTSCHI (Ht.), Die EU regelt «Fernabsatz» von Finanzprodukten, Harmonisierter Konsumentenschutz, NZZ Nr. 225, 28. September 2001, 25; sowie den geänderten Vorschlag des Europäischen Parlamentes und des Rates vom 23. Juli 1999 für eine Richtlinie über den Fernabsatz von Finanzdienstleistungen an Verbraucher und zur Änderung der Richtlinie 97/7/EG und 98/27/EG, KOM (1999) 385 endg.

512 Zum Ganzen etwa Domino BURKI, E-Banking: Fernabsatz von Finanzdienstleistungen in der EU, SJZ 18/2001, 391 ff., 393 ff.; MEENTS, 213 f.

513 Vorne N 351, insbesondere FN 489.

514 EU-Kommission, Vorschlag für eine E-Commerce-Richtlinie, 6 ff.; vgl. auch SCHAUER, 173.

515 Art. 22 Abs. 1 E-Commerce-Richtlinie; zur Umsetzung etwa BAKER & MCKENZIE.

516 E-Commerce-Richtlinie, vorausgehende Erwägung 17, mit Hinweis auf die bereits früher erfolgte Definition in der Richtlinie 98/34/EG des Europäischen Parlamentes und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften über die Dienste der Informationsgesellschaft, ABl. 1998 L 204/37.

517 E-Commerce-Richtlinie, vorausgehende Erwägung 18.

3. Elektronischer Vertragsabschluss

a) *Enabling principle*

362 An dieser Stelle ist besonders das *enabling principle* von Art. 9 der E-Commerce-Richtlinie über elektronische Vertragsschlüsse von Bedeutung.[518] Die Mitgliedstaaten werden verpflichtet, Rechtsvorschriften zu ändern, die die Verwendung elektronisch geschlossener Verträge behindern könnten. Dies gilt insbesondere für Formvorschriften, für beweisrechtliche Vorschriften, die die Durchsetzbarkeit elektronisch geschlossener Verträge beschlagen, aber etwa auch für Vorschriften zur Archivierung von Verträgen oder andere Vorschriften, die den elektronischen Vertragsabschluss gegenüber dem herkömmlichen benachteiligen (etwa eine Notwendigkeit, Kopien elektronischer Vertragsschlüsse zur Gültigkeit einer Behörde vorzulegen, sofern dies beim papierenen Vertrag nicht ebenfalls vorgeschrieben ist[519]).[520] Die Mitgliedstaaten sollen systematisch ihre Rechtsvorschriften auf Anpassungsbedarf hin überprüfen.[521] Die Richtlinie ergänzt damit die im Folgenden beschriebene EU-Signaturrichtlinie, welche die Gleichsetzung von Handunterschrift und elektronischer Signatur bringt.[522]

b) *Ausnahmen*

363 Nach Art. 9 Abs. 2 der Richtlinie können folgende Verträge durch die Mitgliedstaaten vom elektronischen Geschäftsverkehr ausgeschlossen werden:

- Verträge, die Rechte an Immobilien mit Ausnahme von Mietrechten begründen oder übertragen (Bst. a);
- Verträge, bei denen die Mitwirkung von Gerichten, Behörden oder öffentliche Befugnisse ausübenden Berufen gesetzlich vorgeschrieben ist (Bst. b);
- Bürgschaftsverträge und Verträge über Sicherheiten, die von Personen ausserhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit eingegangen werden (Bst. c);
- Verträge im Bereich des Familien- oder Erbrechts (Bst. d).

364 Mögliche Gründe für diese Ausnahmen gibt es unterschiedliche.[523] Immobiliengeschäfte sowie Bürgschaften und andere Sicherheiten werden wohl aus Gründen des (auch beim Einsatz elektronischer Signaturen) verminderten Übereilungsschutzes[524]

---

518 LINDHOLM/MAENNEL, 65; zum Ganzen auch SCHAUER, 201 ff.; Markus LUBITZ, Electronic Contracts: A view across the Channel – The English Perspective, K&R 2/2001, 96 ff., 101 ff.

519 Beispiel bei LINDHOLM/MAENNEL, 68 und SCHAUER, 203.

520 E-Commerce-Richtlinie, vorausgehende Erwägung 34; LINDHOLM/MAENNEL, 68.

521 E-Commerce-Richtlinie, vorausgehende Erwägung 34.

522 Vorschlag für eine E-Commerce-Richtlinie, 27.

523 Die Kommission spricht davon, dass Flexibilität bewirkt und Umständen Rechnung getragen werden soll, in denen die Beschränkung der Verwendung elektronischer Verträge legitim sein kann. Zum Ganzen Vorschlag für eine E-Commerce-Richtlinie, 29.

524 OERTEL, 421; hinten N 857 ff.

ausgenommen (Immobiliengeschäfte allenfalls zusätzlich aufgrund der erhöhten Anforderungen an die Beweisqualität von Registereinträgen zu Grunde liegenden Dokumenten). Ähnliche Motive dürften hinter der Ausnahme für familien- und erbrechtliche Verträge stehen.

365 Die Regelung lässt zudem die Möglichkeit der Mitgliedstaaten unberührt, Formvorschriften aufzustellen, die elektronisch erfüllt werden können. Die Funktionen, die bisher durch Schriftlichkeitserfordernisse erfüllt wurden,[525] können damit also etwa auch durch den Einsatz elektronischer Signaturen erfüllt werden.[526]

E. Signaturrichtlinie

1. Allgemeines

366 Nebst den durch die E-Commerce-Richtlinie harmonisierten Punkten besteht vor allem im Bereich der elektronischen Signatur grosser Harmonisierungsbedarf, denn der EU-Binnenmarkt droht durch unterschiedliche technische Anforderungen der Mitgliedstaaten an elektronische Signaturen behindert zu werden.[527] Ziel ist eine diskriminierungsfreie Geltung der elektronischen Signatur innerhalb aller Mitgliedstaaten.[528] Am 13. Dezember 1999 verabschiedeten Europäisches Parlament und Rat daher eine *Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (Signaturrichtlinie)*[529]. Die Richtlinie war bis zum 19. Juli 2001 umzusetzen.[530]

2. Anwendungsbereich

367 Die Richtlinie beschränkt sich nicht ausdrücklich auf den elektronischen Geschäftsverkehr; es werden auch Willensäusserungen erfasst, welche nicht dem Vertragsabschluss dienen.[531] In geschlossenen Benutzergruppen aufgrund vertraglicher Vereinbarung eingesetzte Systeme werden von der Richtlinie nicht berührt.[532]

368 Nach Art. 1 Abs. 2 der Richtlinie sind Aspekte im Zusammenhang mit dem Abschluss und der Gültigkeit von Verträgen oder anderen rechtlichen Verpflichtungen,

---

525 Beweis-, Übereilungsschutzfunktion, u. dgl.; Details hinten N 833 ff.

526 E-Commerce-Richtlinie, vorausgehende Erwägung 35; LINDHOLM/MAENNEL, 68; SCHAUER, 202 f.

527 Signaturrichtlinie, vorausgehende Erwägungen 4 und 5; Vorschlag für eine Signaturrichtlinie, 4 ff.; BRISCH, Rahmenbedingungen, 493; BIZER/MIEDBRODT, 151.

528 Vorschlag für eine Signaturrichtlinie, 6; BLUM, UNCITRAL, 70.

529 ABl. 2000 L 13/12.

530 Art. 13 Abs. 1 der Richtlinie; einen Überblick über die unterschiedlichen Umsetzungen der Mitgliedstaaten gibt etwa Jos DUMORTIER/Regina RINDERLE, Umsetzung der Signaturrichtlinie in den europäischen Mitgliedstaaten, CRi 1/2001, 5 ff.; vgl. auch BAKER & MCKENZIE sowie VAN DEN HOF.

531 So etwa BRISCH, Rahmenbedingungen, 493, unter Bezugnahme auf die deutsche Bundesregierung.

532 Signaturrichtlinie, vorausgehende Erwägung 16; vgl. auch Vorschlag für eine Signaturrichtlinie, 3, 6 ff.

für die nach einzelstaatlichem Recht oder Gemeinschaftsrecht Formvorschriften zu erfüllen sind, nicht erfasst. Damit sind laut BRISCH Rechtsgeschäfte gemeint, die der Mitwirkung von Behörden bedürfen (Ehevertrag), oder gewisse höchstpersönliche Rechtsgeschäfte familien- oder erbrechtlicher Art (Testament u. dgl.).[533] Die entsprechenden Willenserklärungen können durch die Mitgliedstaaten aber bereits gestützt auf Art. 9 Abs. 2 der E-Commerce-Richtlinie vom elektronischen Verkehr ausgenommen werden,[534] womit sich m. E. bei diesen die Frage der Zulassung elektronischer Signaturen im Grunde erübrigt. REDEKER[535] sieht in Art. 1 und 5 der Richtlinie einen Widerspruch, der dahingehend aufzulösen sei, dass Art. 5 der Richtlinie die Änderung nur dort verlangt, wo Formvorschriften allein Beweisfunktion haben, nicht aber etwa dem Übereilungsschutz dienen.[536] Weil die im Rahmen einer bestimmten Formvorschrift eingesetzten Funktionen der Unterschrift aber oftmals nicht klar zu trennen sind, läge m. E. in einer solchen Interpretation die Gefahr eines erneuten Auseinanderdriftens der mitgliedstaatlichen Regelungen. Hinzu kommt, dass aufgrund der Ausnahmen von Art. 9 Abs. 2 der E-Commerce-Richtlinie sowie des Widerrufsrechts der Fernabsatzrichtlinie bereits eine grosse Zahl von Formvorschriften mit überwiegender Warnfunktion entschärft wurden. REDEKERS Auffassung ist daher m. E. ebenfalls abzulehnen.

369 Die Bedeutung von Art. 1 Abs. 2 erschliesst sich m. E. vielmehr aus der vorausgehenden Erwägung 17: Danach zielt die Richtlinie nicht auf eine Harmonisierung der nationalen Vertragsrechte und der entsprechenden Formvorschriften ab, d. h. nicht auf die Frage, welche Vertragstypen einer besonderen Form bedürfen. Harmonisiert wird vielmehr ausschliesslich die Zulassung von elektronischen Unterschriften für den Fall, dass derartige Formvorschriften eine Handunterschrift verlangen (einfache Schriftlichkeit).

3. Zertifizierungsdiensteanbieter

a) Keine Bewilligungspflicht

370 Art. 3 Abs. 1 der Richtlinie verbietet den Mitgliedstaaten, die Bereitstellung von Zertifizierungsdiensten von einer Bewilligung abhängig zu machen.[537] Die Richtlinie folgt damit zunächst einem *ex-post-Ansatz*[538]: Erfüllt eine Signatur bestimmte Voraussetzungen,[539] so ist sie der Handunterschrift gleichgestellt, ohne dass der Zertifizierungsdiensteanbieter oder das eingesetzte Verfahren einer expliziten Anerkennung bedürfte. Ob die Voraussetzungen erfüllt sind, wird erst im Nachhinein im Rahmen eines allfälligen Prozesses geklärt. Sind sie es trotz gegenteiliger Deklarati-

533 BRISCH, Rahmenbedingungen, 493; vgl. etwa auch PESTALOZZI/VEIT, 603.
534 Vorne N 363.
535 REDEKER, 458.
536 Zu den Funktionen der Unterschrift hinten N 833 ff.
537 Vgl. auch ROSSNAGEL, Recht, 1820.
538 Zu den Begriffen vorne N 280 ff.
539 Hinten N 385 ff.

on des Anbieters nicht, so haftet dieser für die Verletzung der gesetzlichen Vorschriften.[540] Eine eigentliche Anerkennung der Anbieter erübrigt sich deshalb.

371 Art. 3 Abs. 3 der Richtlinie verlangt von den Mitgliedstaaten die Einführung eines Überwachungssystems für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate[541] ausstellen. Dies setzt voraus, dass die Zertifizierungsdiensteanbieter ihre Tätigkeit beim Staat *anmelden*.[542] Bei der Ausgestaltung des Überwachungssystems sind die Mitgliedstaaten grundsätzlich frei.[543]

372 Anhang II der Richtlinie definiert eine grössere Zahl von Anforderungen an die Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen. Darunter fallen die Zuverlässigkeit ihrer Systeme und ausreichende fachliche Qualifikation des Personals, die Bereitstellung von Verzeichnisdiensten, die sichere Überprüfung der Identität der Signierschlüsselhalter, das Vorliegen einer ausreichenden finanziellen Deckung für Haftungsfälle sowie die Aufzeichnung und Aufbewahrung der Informationen über qualifizierte Zertifikate für Gerichtsverfahren. Die Anbieter müssen die Antragsteller zudem vor dem Vertragsabschluss mit einem dauerhaften Kommunikationsmittel (allenfalls auch elektronisch) über die Bedingungen der Verwendung des Zertifikats informieren, also etwa über Nutzungsbeschränkungen oder das Vorgehen im Streitfalle. *Nicht* vorgesehen ist hingegen eine Informationspflicht über die rechtlichen Auswirkungen der elektronischen Signatur.

b) Freiwillige Akkreditierung

373 Die durch den ex-post-Ansatz entstehende Rechtsunsicherheit[544] kann gemäss Art. 3 Abs. 2 der Richtlinie von den Mitgliedstaaten durch Einführung eines *freiwilligen Akkreditierungsverfahrens*[545] beseitigt werden. In diesem bescheinigen die Mitgliedstaaten den Zertifizierungsdiensteanbietern auf Antrag ex ante, die Voraussetzungen der Richtlinie zu erfüllen.[546] Die freiwillige Akkreditierung erlaubt zudem auch die ex-ante-Überprüfung sämtlicher beteiligten technischen Komponenten, während die Richtlinie nur eine solche für sichere Signaturerstellungseinheiten vorschreibt, sowie – sofern ein Mitgliedstaat dies will – eine Anhebung des Sicherheitsniveaus über das der qualifizierten elektronischen Signatur der Richtlinie hinaus.[547]

---

540 Dazu etwa ROSSNAGEL, Standard, 206 ff.

541 Ein qualifiziertes Zertifikat ist ein Zertifikat, das in Anhang I der Richtlinie aufgeführte Kriterien erfüllt und von einem Zertifizierungsdiensteanbieter ausgestellt wurde, der den Anforderungen von Anhang II der Richtlinie genügt; vgl. N 386.

542 Vgl. etwa GEIS, 668 f., 670 f.; REDEKER, 456.

543 GEIS, 669.

544 Vorne N 282.

545 Nach schweizerischer Teminologie *Anerkennungsverfahren*; unter Akkreditierung wird in der Schweiz die Zulassung der die Anerkennung durchführenden Prüfstellen durch den Staat verstanden; N 521 ff.

546 Christoph BRENN, Das österreichische Signaturgesetz – Unterschriftenersatz in elektronischen Netzwerken, Österreichische Juristen-Zeitung, 1999, 587 ff., 589; REDEKER, 457 f.; für die Umsetzung in *Deutschland* GEIS, 670 f.

547 ROSSNAGEL, Signaturgesetz, 202.

374 Die Richtlinie verfolgt damit einen kombinierten Ansatz, der einerseits das ex-post- und andererseits ex-ante-Modell umsetzt.[548]

4. Anerkennung der elektronischen Signatur

a) Überblick

375 Die Richtlinie folgt bei der Definition der Signatur einer komplizierten *Schachteltechnik*.[549] Sie definiert eine (einfache) *elektronische Signatur* und eine *fortgeschrittene elektronische Signatur*.[550] Hinzu kommt die fortgeschrittene elektronische Signatur, die auf einem *qualifizierten Zertifikat* beruht und mittels einer *sicheren Signaturerstellungseinheit* erstellt wurde (hier *qualifizierte elektronische Signatur* genannt), sowie eine Signatur, die zusätzlich auf einem durch einen *akkreditierten Zertifizierungsdiensteanbieter* ausgestellten Zertifikat beruht (hier *qualifizierte elektronische Signatur mit Anbieterakkreditierung*). Alle Arten elektronischer Signaturen sind vor Gericht zum Beweise zuzulassen, qualifizierte elektronische Signaturen sind zudem materiellrechtlich anzuerkennen.[551]

376 Die Hintergründe dieser Regelung liegen im Streit zwischen den Vertretern des ex-ante- und denjenigen des ex-post-Ansatzes und im Bedürfnis nach technologieneutraler Ausgestaltung.[552]

---

548 BÜLLESBACH/RIESS/MIEDBRODT, 13; vgl. auch vorne N 293.

549 BLUM, UNCITRAL, 66.

550 Diese Einteilung beruht auf Entwürfen des UNCITRAL Model Law on Electronic Signatures welche auch eine Einteilung vorsahen; BLUM, UNCITRAL, 65. Die Endfassung des MLES verzichtet hingegen auf eine Unterteilung.

551 ROSSNAGEL, Standard, 216 ff.

552 ROSSNAGEL, Standard, 195 ff., 200 f.; SCHULZKI-HADDOUTI, Übereinkunft, 46; DIESELBE, Marktmacht, 58.

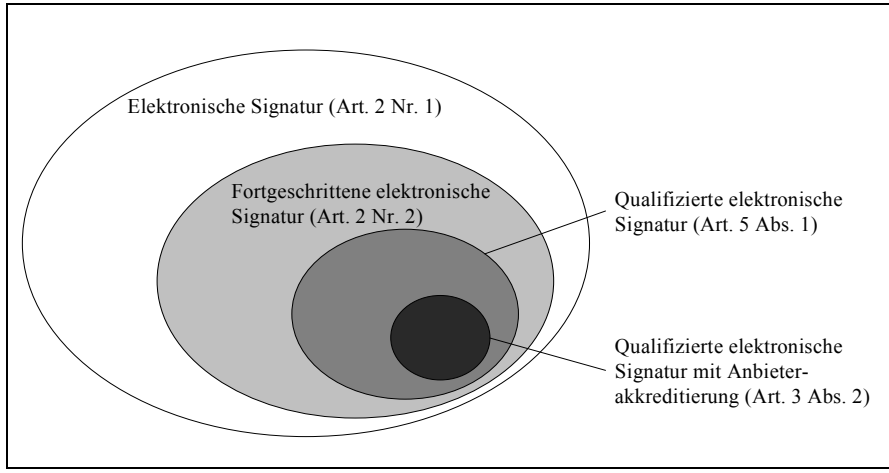

Abbildung 10: Elektronische Signaturen gemäss EU-Signaturrichtlinie.

b) (Einfache) elektronische Signatur

aa) Definition

377 Art. 2 Nr. 1 der Richtlinie definiert die *elektronische Signatur* in Anlehnung an das UNCITRAL Model Law on Electronic Signatures als «Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.» Diese Definition folgt dem geschilderten funktionalen Ansatz[553] und widerspiegelt die technologieneutrale Ausrichtung der Richtlinie.[554]

378 Ein minimales Sicherheitsniveau des eingesetzten Verfahrens ist nicht Voraussetzung für das Vorliegen einer elektronischen Signatur. Die tatsächliche Sicherheit soll vielmehr erst im Einzelfall vor Gericht geprüft werden. Deshalb werden vom Begriff der elektronischen Signatur im Prinzip auch völlig unsichere Verfahren wie eingescannte Handunterschriften erfasst.[555]

bb) Rechtswirkung

379 Art. 5 Abs. 2 der Richtlinie legt fest, dass einer einfachen elektronischen Signatur nicht allein deshalb die rechtliche Wirksamkeit abgesprochen werden darf und dass sie nicht allein deshalb vor Gericht nicht als Beweismittel zugelassen werden darf,

553 Vorne N 294 ff.; vgl. etwa PESTALOZZI/VEIT, 600 f.

554 Geänderter Vorschlag für eine Signaturrichtlinie, 4; BRISCH, Rahmenbedingungen, 494; GRIMM/FOX, 407; kritisch ROSSNAGEL, Standard, 202 f.; vgl. auch die Kritik an der Forderung nach Technologieneutralität vorne N 303 ff.

555 BLUM, Entwurf, 71; GEIS, 669; ROSSNAGEL, Recht, 1819; vorne N 37 f.

weil sie *i)* in elektronischer Form vorliegt, *ii)* nicht auf einem qualifizierten Zertifikat[556] beruht, *iii)* nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder *iv)* nicht mittels einer sicheren Signaturerstellungseinheit erstellt wurde. In diesem *Diskriminierungsverbot* liegt die einzige Rechtswirkung, die die Richtlinie für einfache elektronische Signaturen vorsieht.[557]

380 Die Forderung nach der Zulassung der elektronischen Signatur zum Beweis richtet sich in erster Linie an Mitgliedstaaten, welche eine *Beweisform* kennen, d.h. eine beweisrechtliche Vorschrift, welche zum Beweis von Ansprüchen ab einer bestimmten Höhe eine handschriftlich unterzeichnete Urkunde voraussetzt.[558] Das deutsche und das schweizerische Recht kennen eine solche Beweisform nicht, sondern gehen von der freien richterlichen Beweiswürdigung aus, in deren Rahmen elektronische Signaturen zum Beweis bereits zugelassen sind.[559]

c) Fortgeschrittene elektronische Signatur

aa) Definition

381 Nach Art. 2 Nr. 2 der Richtlinie ist eine *fortgeschrittene elektronische Signatur* eine elektronische Signatur, die folgende Voraussetzungen erfüllt: Sie ist *i)* ausschliesslich dem Unterzeichner zugeordnet (was etwa bedeutet, dass ein Zertifizierungsdiensteanbieter einen bestimmten Schlüssel nicht mehreren Haltern zugleich zuordnen darf),[560] ermöglicht *ii)* die Identifizierung des Halters, wird *iii)* mit Mitteln erstellt, die der Halter unter seiner alleinigen Kontrolle halten kann und ist *iv)* so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.[561] Wie bei der einfachen elektronischen Signatur handelt es sich auch hier um eine funktionale Umschreibung.

382 Damit eine Signatur als fortgeschrittene elektronische Signatur gelten kann, muss sie folglich – anders als die einfache elektronische Signatur – ein bestimmtes Sicherheitsniveau aufweisen. Während eine eingescannte Unterschrift daher nicht mehr als fortgeschrittene Signatur gelten kann, ist dies für eine mit dem Programm Pretty Good Privacy[562] gesetzte Signatur der Fall, obwohl dort keine Zertifizierung, sondern ein Web of Trust verwendet wird.[563]

---

556 Details hinten N 385 ff.

557 Vgl. etwa ROSSNAGEL, Standard, 202 f.

558 Etwa Frankreich; zur Umsetzung der Richtlinie in Frankreich etwa Amrei AUGUSTIN, Frankreich: Neue Regeln für elektronische Signaturen, CRi 2/2001, 60 ff., 61; hinten N 804.

559 BLUM, UNCITRAL, 66 oder BIZER/MIEDBRODT, 160; ROSSNAGEL, Standard, 219; vgl. auch hinten N 777 f., 804.

560 Vgl. Begründung zum deutschen SigG 01, 18. Eine fortgeschrittene elektronische Signatur kann zudem beispielsweise auch in einem technischen System zur Authentisierung verschiedener miteinander kommunizierender Komponenten oder Prozesse untereinander eingesetzt werden, wobei kein Bezug zu einem Unterzeichner bestehen muss; für Beispiele etwa vorne N 137 und 142.

561 Vgl. etwa die Begründung zum deutschen SigG 01, 18; für Österreich MENZEL, 83.

562 Vorne N 76 ff.

383 Die Signaturrichtlinie äussert sich zwar nicht explizit zur Frage, ob Zertifikate auch auf juristische Personen ausgestellt werden können, die Definition der fortgeschrittenen elektronischen Signatur mit ihrem Hinweis auf eine Identifikation und die Nennung von Attributen mit Vertretungsrechten im Anhang I der Richtlinie (welche gerade bei juristischen Personen von Bedeutung sind) sprechen jedoch eher für eine ausschliessliche Zulassung natürlicher Personen.[564]

bb) Rechtswirkung

384 Hinsichtlich der Rechtsfolgen besteht kein Unterschied zwischen einfachen und fortgeschrittenen elektronischen Signaturen.[565] Beide Verfahren werden hinsichtlich der in der Richtlinie aufgestellten Voraussetzungen sowie der Beweiskraft durch die Gerichte ex post gewürdigt.[566] Selbstverständlich hat die fortgeschrittene elektronische Signatur aufgrund ihres festgeschriebenen Sicherheitsniveaus faktische Vorteile als Beweismittel.

d) Qualifizierte elektronische Signatur

aa) Definition

385 Soll eine elektronische Signatur *materiellrechtlich anerkannt* sein,[567] so muss es sich nach Art. 5 Abs. 1 Bst. a der Richtlinie um eine fortgeschrittene Signatur handeln, die auf einem *qualifizierten Zertifikat* beruht und mittels einer *sicheren Signaturerstellungseinheit* erstellt wurde.[568] Die Richtlinie definiert diesen Signaturtypus nicht eigens. In Anlehnung an das deutsche Signaturgesetz 01 soll in dieser Untersuchung von *qualifizierter elektronischer Signatur* die Rede sein.[569] GEIS spricht von *fortgeschrittenen elektronischen Signaturen besonderer Qualität*.[570]

386 Ein *qualifiziertes Zertifikat* ist gemäss Art. 2 Nr. 10 der Richtlinie ein Zertifikat, das die Anforderungen des Anhangs I[571] der Richtlinie erfüllt und von einem Zertifizierungsdiensteanbieter bereitgestellt wird, der die Anforderungen des Anhangs II[572] der Richtlinie erfüllt. Das Vorliegen dieser Voraussetzungen wird auch diesfalls erst ex post durch die Gerichte überprüft.

---

563 Begründung zum deutschen SigG 01, 18.

564 So auch BRISCH, Rahmenbedingungen, 495; anders MENZEL, 97, der von einer Freistellung ausgeht.

565 ROSSNAGEL, Recht, 1819.

566 ROSSNAGEL, Standard, 216; anders SCHULZKI-HADDOUTI, Übereinkunft, 46.

567 D.h. «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»; Art. 5 Abs. 1 Bst. a Signaturrichtlinie.

568 Zum Ganzen etwa auch PESTALOZZI/VEIT, 602f.

569 Art. §2 Nr. 3 SigG 01; ähnlich Art. 2 Bst. c E-ZertES.

570 GEIS, 668.

571 Es handelt sich durchwegs um Vorschriften über den Inhalt des Zertifikats.

572 Technische Vorschriften (auf relativ abstraktem Niveau), Vorschriften über Haftungssubstrat u.dgl.

387 Die Anforderungen an *sichere Signaturerstellungseinheiten* werden in Anhang III festgehalten. Anders als bei den Anforderungen der übrigen Anhänge wird nach Anhang III die Übereinstimmung mit den Vorgaben ex ante durch eine staatliche Stelle festgestellt. Diese Anerkennung muss von allen Mitgliedstaaten anerkannt werden.[573]

388 Anders als noch bei der fortgeschrittenen elektronischen Signatur folgt die Definition der qualifizierten elektronischen Signatur dem *technikrechtlichen Ansatz*. Mit der qualifizierten elektronischen Signatur weicht die Signaturrichtlinie zudem insofern vom Grundsatz der Technologieneutralität ab, als nur noch Public-Key-Verfahren zulässig sind, denn nur diese benötigen Zertifikate.[574]

bb) Rechtswirkung

389 Zur bereits für einfache und fortgeschrittene Signaturen geltenden Zulassung zum Beweis kommt bei qualifizierten elektronischen Signaturen die materiellrechtliche Anerkennung nach Art. 5 Abs. 1 der Richtlinie.

390 Ausgenommen von der Anerkennung der qualifizierten elektronischen Signatur ist nach Art. 3 Abs. 7 der öffentliche Bereich. Hier können die Mitgliedstaaten zusätzliche Anforderungen aufstellen.[575] Die Anforderungen müssen jedoch objektiv, transparent, verhältnismässig und nichtdiskriminierend sein und dürfen sich nur auf die spezifischen Merkmale der betreffenden Anwendung beziehen.

391 Art. 5 Abs. 1 Bst. b der Richtlinie, der die Zulassung einer qualifizierten elektronischen Signatur zum Beweis vorschreibt, ist m.E. obsolet, weil sich diese bereits aus Art. 5 Abs. 2 ergibt; bilden doch qualifizierte elektronische Signaturen eine Untermenge der (einfachen) elektronischen Signaturen.[576] Eine gesetzliche Anhebung der Beweiskraft wird für die qualifizierte elektronische Signatur ebenso wenig verlangt wie die Zulassung zum Urkundenbeweis.[577]

---

573 Art. 3 Abs. 4 Signaturrichtlinie; vgl. auch BÜLLESBACH/RIESS/MIEDBRODT, 14; ROSSNAGEL, Signaturregelungen, 456.

574 Unklar BRISCH, Rahmenbedingungen, 496. DIERING/SCHMEH, 183, gehen davon aus, dass bereits die fortgeschrittene elektronische Signatur eine Public-Key-Signatur sei. Dies ist de facto korrekt, weil nur Public-Key-Verfahren die geforderten Eigenschaften aufweisen (auf in geschlossenen Benutzergruppen eingesetzte Systeme, die auch durch andere Techniken realisierbar sind, ist die Richtlinie nicht anwendbar; N 303, 367), ergibt sich m.E. aber nicht explizit aus der Definition.

575 Vgl. GEIS, 668 f.; Günter WELSCH/Kathrin BREMER, Die europäische Signaturrichtlinie in der Praxis, DuD 2/2000, 85 ff., 86.

576 Vorne N 375 ff.

577 Letzteres war in Art. 5 Abs. 2 des Vorschlages für eine Signaturrichtlinie von 1998 noch vorgesehen: «Die Mitgliedstaaten stellen sicher, dass [qualifizierte] elektronische Signaturen (…) in Gerichtsverfahren in gleicher Weise wie handschriftliche Unterschriften als Beweismittel zugelassen sind»; MENZEL, 170; BLUM, UNCITRAL, 66 FN 40. Vgl. auch BRISCH, Rahmenbedingungen, 496; GRIMM/FOX, 408; REDEKER, 458.

e) Qualifizierte Signatur mit Anbieterakkreditierung

392 Die Tatsache, dass eine elektronische Signatur auf dem Zertifikat eines akkreditierten Anbieters beruht, hat auf ihre rechtliche Beurteilung nur insofern Einfluss, als die Voraussetzungen für ihre *Einordnung als qualifizierte elektronische Signatur* und damit ihre Zulässigkeit als Beweismittel und ihre materiellrechtliche Anerkennung bereits ex ante geprüft sind, was zusätzliche Rechtssicherheit schafft.[578] Die Akkreditierung kann wie erwähnt auch dazu benutzt werden, über die Signaturrichtlinie hinausgehende Anforderungen an die Anbieter zu stellen, um damit die Vertrauenswürdigkeit der Anbieter zu fördern.[579]

5. Haftung der Zertifizierungsdiensteanbieter

393 In Art. 6 regelt die Signaturrichtlinie die Haftung derjenigen Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausgeben. Die Haftung des Signierschlüsselhalters und diejenige des auf die Signatur vertrauenden Dritten sind nicht geregelt.[580]

394 Der Zertifizierungsdiensteanbieter haftet für

- die Korrektheit und Vollständigkeit der Angaben im Zertifikat zum Zeitpunkt der Ausstellung (Abs. 1 Bst. a);
- die Kontrolle des Unterzeichners über den dem zertifizierten Prüfschlüssel entsprechenden Signierschlüssel[581] (Abs. 1 Bst. b);
- die Möglichkeit der komplementären Nutzung von Signier- und Prüfschlüssel, sofern er beide erzeugt hat (Abs. 1 Bst. c);
- die rechtzeitige Publikation der Zertifikatssperrung (Abs. 2).[582]

395 Die Haftungsregelung soll dem ex-post-Ansatz zu einem angemessenen Sicherheitsniveau verhelfen.[583] Die Haftung ist ausgeschlossen, wenn der Anbieter nachweist, dass er nicht fahrlässig gehandelt hat; es handelt sich also um eine *Verschuldenshaftung mit Beweislastumkehr*.[584] Die Zertifizierungsdiensteanbieter müssen zudem die Möglichkeit haben, im Zertifikat Beschränkungen des Verwendungsbereichs sowie einen maximalen Transaktionswert anzugeben[585] und damit ihre Haftung zu beschränken.[586] Schliesslich wird vorausgesetzt, dass der Dritte *vernünftigerweise* auf

---

578 Vorne N 292 f.; ROSSNAGEL, Signaturgesetz, 202.

579 So insbesondere Signaturrichtlinie, vorausgehende Bemerkung 11; geänderter Vorschlag für eine Signaturrichtlinie, 4; BRISCH, Rahmenbedingungen, 495; vorne N 373.

580 BRISCH, Rahmenbedingungen, 497; vgl. immerhin N 395.

581 Die Richtlinie spricht von Signaturerstellungsdaten; Art. 2 Nr. 4.

582 Vgl. auch ROSSNAGEL, Standard, 214 f.

583 GRIMM/FOX, 407, 408; ROSSNAGEL, Standard, 214; vorne N 281.

584 Art. 6 Abs. 1 und 2 der Richtlinie, jeweils a. E.; PESTALOZZI/VEIT, 605 sprechen von einer *Gefährdungshaftung*, beziehen sich dabei aber offenbar noch auf den Richtlinienvorschlag, der noch eine Gefährdungshaftung statuierte (dazu etwa EMMERT, 248 f.).

585 Art. 6 Abs. 3 und 4 der Richtlinie.

586 BRISCH, Rahmenbedingungen, 498.

das Zertifikat vertraute, d.h. es kann etwa von ihm verlangt werden, das Zertifikat auf seine Gültigkeit hin zu prüfen.[587]

6. Gemeinschaftsweite Anerkennung

396 Der ex-post-Ansatz von Art. 5 Abs. 1 der Richtlinie führt dazu, dass qualifizierte elektronische Signaturen unabhängig vom Sitzland des Zertifizierungsdiensteanbieters anerkannt werden.

397 Einzig die Akkreditierung der Zertifizierungsdiensteanbieter, die jedoch – abgesehen vom öffentlichen Bereich[588] – weder für die materiellrechtliche Anerkennung noch zur Zulassung von Signaturen zum Beweis vorausgesetzt werden darf, kann durch die Mitgliedstaaten unterschiedlich geregelt werden.

7. Internationale Anerkennung

398 Zertifikate von in Drittländern niedergelassenen Zertifizierungsdiensteanbietern können in der EU nach Art. 7 Abs. 1 der Richtlinie auf folgenden drei Wegen anerkannt werden:[589]

- Akkreditierung in einem Mitgliedstaat und Erfüllung der Voraussetzungen der Richtlinie;
- Einstehen eines in einem Mitgliedstaat niedergelassenen Anbieters für den im Drittland niedergelassenen Anbieter;[590]
- Anerkennung im Rahmen von bi- oder multilateralen Abkommen.[591]

8. Datenschutz

399 Art. 8 der Richtlinie erklärt die Datenschutzrichtlinie[592] für anwendbar. Zudem dürfen die Daten nur unmittelbar von der betroffenen Person oder mit deren Zustimmung erfasst werden und ohne deren Zustimmung nicht zu anderweitigen Zwecken als zur Erstellung des Zertifikats verwendet werden. Zertifizierungsdiensteanbieter müssen ferner die Möglichkeit haben, Zertifikate auf ein Pseudonym auszustellen.[593]

---

587 Kritisch zum Begriff «vernünftigerweise» BRISCH, Rahmenbedingungen, 498; vgl. auch Art. 11 MLES; vorne N 347.

588 Vorne N 390.

589 ROSSNAGEL, Standard, 219; allgemeines zur internationalen Anerkennung der Anbieter vorne N 311 ff.

590 Etwa mittels Kreuzzertifizierung; dazu vorne N 97 ff.

591 Zur Frage, ob ZertDV-konforme Zertifikate den Anforderungen der Signaturrichtlinie genügen etwa PESTALOZZI/VEIT, Elektronische Signaturen, 605.

592 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; ABl. 1995 L 281/31.

593 Zum Datenschutz etwa ROSSNAGEL, Standard, 215 f.

IV. Deutschland

A. Signaturgesetz 1997

1. Allgemeines

Am 1. August 1997 trat in Deutschland nach Italien das zweite europäische Gesetz über elektronische Signaturen in Kraft *(SigG 97)*.[594] Es war als Artikel 3 eines *Gesetzes zur Regelung der Rahmenbedingungen für Information- und Kommunikationsdienste* (Multimediagesetz; IuKDG)[595] ausgestaltet und hatte in erster Linie Experimentcharakter.[596] 400

Gestützt auf § 16 SigG 97 wurde eine *Signaturverordnung (SigV 97)* erlassen,[597] und gestützt auf § 12 Abs. 2 dieser Signaturverordnung verfasste das BSI (Bundesamt für Sicherheit in der Informationstechnik) einen rund 300 Seiten zählenden *Massnahmenkatalog* zur Gewährleistung der Sicherheit von Zertifizierungsstellen.[598] Dieser sollte beispielhaft Lösungen zur Erfüllung der Vorgaben von Gesetz und Verordnung aufzeigen. 401

Ferner schlossen sich Zertifizierungsdiensteanbieter zusammen, um – mit Unterstützung durch das BSI – *Interoperabilitätsspezifikationen*[599] zu schaffen, die den Einsatz und die Kompatibilität von Produkten unterschiedlicher Hersteller ermöglichen sollten.[600] 402

2. Regelungsbereich und -modell

Das SigG 97 regelte einzig die Sicherungsinfrastruktur, diese jedoch auf sehr detaillierte Art und Weise im Sinne des geschilderten technikrechtlichen Ansatzes.[601] Die materiellrechtliche und prozessuale Anerkennung der elektronischen Signatur sowie 403

---

594 Das italienische Gesetz vom 15. März 1997 regelte allerdings ausschliesslich die Zulassung elektronischer Signaturen zum Beweis; dazu etwa Giovanni BUONOMO, Italian Laws and Regulations Concerning the Creation, Storage, and Transmission of Documents by Means of Computer-Based Systems and Digital Signature, http://www1.oecd.org/dsti/sti/it/secur/act/emef21.pdf, 3; BÜLLESBACH/RIESS/MIEDBRODT, 12; zum deutschen Gesetz etwa ALLENSTEIN, 15 ff.

595 BGBl. I S. 1870 ff.; dazu insbesondere die Begründung der Bundesregierung, BT-Drs. 13/7385, sowie etwa Stefan ENGEL-FLECHSIG/Fritjof A. MAENNEL/Alexander TETTENBORN, Das neue Informations- und Kommunikationsdienste-Gesetz, NJW 45/1997, 2981 ff., 2988 ff.; GISLER, 195 ff.; MALZER, 96 f.

596 ROSSNAGEL, Signaturgesetz, Abschnitt III.

597 Dazu etwa Christopher KUNER, Signaturverordnung, CR 1/1998, 62.

598 BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, Massnahmenkatalog für digitale Signaturen, Auf Grundlage von SigG und SigV, Entwurf, 1997 (nicht mehr elektronisch verfügbar); vgl. auch DIERING/SCHMEH, 183.

599 Abgekürzt *SigI*.

600 Bundesregierung, IuKDG-Bericht, 39; HAMMER, 96 ff., 98; zu neueren Entwicklungen etwa Richard SIETMANN, Eine Hürde weniger, ISIS-MTT soll die digitale Signatur massentauglich machen, c't 20/2001, 59.

Haftungsfragen wurden nicht geregelt – die Anerkennung sowie öffentlich-rechtliche Bereiche im Hinblick auf eine später folgende Regelung im Rahmen einer Revision der entsprechenden Normen, für die das Signaturgesetz als Referenzregelung dienen sollte,[602] und die Haftung auf Grund der Annahme, die bestehenden Regeln genügten.[603]

404 Nach § 4 Abs. 1 SigG 97 bedurfte der Betrieb einer (im SigG 97 noch so genannten) *Zertifizierungsstelle* einer Genehmigung der zuständigen Behörde[604], welche auf Antrag zu erteilen war, sofern die von Gesetz und Verordnung aufgestellten Voraussetzungen gegeben waren.[605] Die Formulierung dieser Bestimmung gab zu einigen Diskussionen Anlass: Sie wurde teilweise als generelle Genehmigungspflicht für den Betrieb von Zertifizierungsdiensten missverstanden,[606] richtigerweise war eine Genehmigung jedoch nur für Zertifizierungsdienste im Sinne des Gesetzes, nicht aber für andere Anwendungen vorausgesetzt. Dies daher, weil andere Verfahren für digitale Signaturen gemäss § 1 Abs. 2 SigG 97 explizit zum Gebrauch zugelassen waren, soweit nicht digitale Signaturen nach dem Gesetz vorgeschrieben waren.[607]

3. Vorgezogener Anscheinsbeweis

405 Nach § 1 Abs. 1 SigG 97 war der Zweck des Gesetzes, «Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können.» Es sollte eine «hohe faktische Gesamtsicherheit»[608] geschaffen werden, die als Basis für einen *vorgezogenen Anscheinsbeweis* für die Echtheit dienen sollte.[609] Ohne eine gesetzliche Vermutung oder eine andere gesetzliche Beweisregel aufzustellen, sollte dem auf eine Signatur vertrauenden Dritten durch die rein

---

601 BÜLLESBACH/RIESS/MIEDBRODT, 8 f.; MIEDBRODT, 52; BLUM, UNCITRAL, 65, spricht gar von einem dirigistischen Modell; kritisch auch ALLENSTEIN, 58 und KUNER, 644 ff.; zum technikrechtlichen Ansatz vorne N 294 ff.

602 Bundesregierung, IuKDG-Bericht, 39. Zur Revision der Formvorschriften im Privatrecht vgl. hinten N 439 ff.

603 BLUM, UNCITRAL, 68; kritisch zur fehlenden Regelung der materiellrechtlichen und prozessualen Anerkennung etwa Ivo GEIS, Die digitale Signatur, NJW 45/1997, 3000 ff., 3002 f.; GEIS, 671; MALZER, 112. Zur Haftung der Zertifizierungsdiensteanbieter etwa LEIER, EMMERT sowie DÖRR (N 6).

604 Es handelt sich um die bereits bestehende *Regulierungsstelle für Telekommunikation und Post (RegTP)*, welche nach § 66 Telekommunikationsgesetz i. V. m. § 3 SigG 97 mit dieser neuen Aufgabe betraut worden war; vgl. http://www.regtp.de.

605 Bei Erteilung dieser Genehmigung wurde durch die Genehmigungsbehörde ein besonderes Zertifikat für den Anbieter ausgestellt; § 4 Abs. 5 SigG 97; ROSSNAGEL, Fortentwicklung, 2.3.; VON HARNIER, 49. Das SigG 97 folgte damit dem Root-System; dazu vorne N 96.

606 Dazu etwa MIEDBRODT, 63 m. H.; vgl. etwa auch PESTALOZZI/VEIT, 603.

607 ALLENSTEIN, 33 f.; KUNER, 634; MIEDBRODT, 63; REDEKER, 456; ROSSNAGEL, Fortentwicklung, 2.3.; DERSELBE, Recht, 1817.

608 Begründung IuKDG, 28.

609 Eingehend ROSSNAGEL, Sicherheitsvermutung, 3315 ff. und mit ihm BLUM, UNCITRAL, 67; vgl. auch BIESER/KERSTEN, 32; MALZER, 100 ff.; MIEDBRODT, 43 ff.; ROSSNAGEL, Fortentwicklung, 2.4; VON HARNIER, 55 f.; zum Begriff des Anscheinsbeweises hinten N 588 ff.

faktische Sicherheit der Verfahren die Beweisführung erleichtert werden.[610] In diesem vorgezogenen Anscheinsbeweis lag die einzige Rechtsfolge des SigG 97.[611]

4. Praxis

406 Gerichtsentscheide zum Gesetz waren bis zum Inkrafttreten der im Folgenden beschriebenen Novelle am 22. Mai 2001 keine ergangen. Bis dahin hatten ein halbes Dutzend Zertifizierungsdiensteanbieter im Sinne des Gesetzes eine Bewilligung eingeholt.[612] Die Anzahl ausgestellter Zertifikate lag weit unter den anfänglichen Erwartungen, was aber mit den in anderen Ländern gemachten Erfahrungen übereinstimmte.[613]

B. Signaturgesetz 2001

407 Das Signaturgesetz 1997 wurde im Jahre 2001 zur Anpassung der Rechtslage an die EU-Signaturrichtlinie und an die Erkenntnisse einer ersten Evaluierung[614] durch ein *Gesetz über Rahmenbedingungen für elektronische Signaturen*[615] *(SigG 01)* vollständig ersetzt.[616] Am 22. November 2001 trat die ebenfalls novellierte Signaturverordnung *(SigV 01)* in Kraft.[617]

1. Regelungsbereich

408 Während sich das SigG 97 auf die Regelung der Sicherungsinfrastruktur beschränkte, umfasst das SigG 01 neu auch Bestimmungen zur Haftung der Zertifizierungsdiensteanbieter sowie einen Bussenkatalog.[618] Die materiellrechtliche Anerkennung wird durch ein separates *Formanpassungsgesetz* vorgenommen.[619] Die prozessuale Anerkennung unterbleibt.[620]

---

610 Vgl. auch hinten N 588 ff.; 673 ff.

611 ROSSNAGEL, Fortentwicklung, 2.3.

612 DIERING/SCHMEH, 183; REGULIERUNGSSTELLE FÜR TELEKOMMUNIKATION UND POST, Genehmigte Zertifizierungsstellen / Akkreditierte Zertifizierungsdiensteanbieter, http://www.regtp.de/tech_reg_tele/in_06-02-02-00-00_m/06/index.html.

613 Vorne N 221 ff.; eingehend zu den Erfahrungen mit dem Gesetz Bundesregierung, IuKDG-Bericht, 1 ff.; ZEUNER, 51 ff.

614 Bundesregierung, IuKDG-Bericht; dazu etwa Alexander TETTENBORN, Die Evaluierung des Signaturgesetzes und Umsetzung der EG-Signaturrichtlinie, in: Ivo GEIS (Hrsg.), Die digitale Signatur – eie Sicherheitstechnik für die Informationsgesellschaft, Ein Leitfaden für Anwender und Entscheider, Eschborn 2000, 231 ff.; vgl. auch ROSSNAGEL, Recht, 1818, insbesondere FN 7 m.H.

615 BGBl. I S. 876 ff.; vgl. auch Begründung SigG 01, BT-Drs. 14/4662 sowie Beschlussempfehlung SigG 01, BT-Drs. 14/5324.

616 Vgl. Begründung SigG 01, 14, 16 f.; eingehend ROSSNAGEL, Recht, 1818, 1819 ff.; DERSELBE, Signaturregelungen, 451.

617 BGBl. I S. 3074 ff.

618 Vgl. Begründung SigG 01, 16.

619 Dazu hinten N 439 ff.

620 N 461.

409 In geschlossenen Benutzergruppen eingesetzte Systeme sind vom Anwendungsbereich des Gesetzes ausgenommen.[621]

2. Neue Definitionen

410 Die Definitionen des SigG 97 wurden an Art. 2 der Signaturrichtlinie angepasst.[622] Die Definition der einfachen elektronischen Signatur wird in § 2 Nr. 1 SigG 01 und die fortgeschrittene elektronische Signatur in § 2 Nr. 2 SigG 01 definiert; beide Definitionen entsprechen denjenigen der Richtlinie.

411 Art. 5 Abs. 1 der Richtlinie sieht für *fortgeschrittene elektronische Signaturen*, die auf einem *qualifizierten Zertifikat* basieren und mittels einer *sicheren Signaturerstellungseinheit* erzeugt wurden (d.h. die Anforderungen der Anhänge I-III der Richtlinie erfüllen), besondere Rechtsfolgen vor.[623] Das SigG 01 bezeichnet derartige Signaturen kurz als *qualifizierte elektronische Signaturen*.

412 Die qualifizierte elektronische Signatur mit Anbieterakkreditierung wird nicht explizit definiert.[624]

3. Sicherungsinfrastruktur

a) Zertifizierungsdiensteanbieter

aa) Begriff

413 Obwohl das SigG 01 alle Signatur-Definitionen der Signaturrichtlinie übernimmt, regelt es allein *qualifizierte elektronische Signaturen*.[625] Der Begriff des Zertifizierungsdiensteanbieters ist daher auf Anbieter qualifizierter Zertifikate beschränkt.

414 Ein Zertifizierungsdienstenabieter ist demnach gemäss § 2 Nr. 10 SigG 01 eine natürliche oder juristische Person, die *qualifizierte Zertifikate* oder *qualifizierte Zeitstempel* ausstellt.[626]

415 Nach § 4 Abs. 5 SigG 01kann der Zertifizierungsdiensteanbieter Aufgaben an Dritte (Registrierstellen u. dgl.) übertragen, wenn er diese in sein Sicherheitskonzept mit einbezieht.[627]

---

621 Begründung SigG 01, 17.
622 Zum Ganzen Begründung SigG 01, 18 ff.; BLUM, Entwurf, 71.
623 Vorne N 385 ff.
624 Zur Einteilung der Signaturverfahren nach deutschem Recht etwa ROSSNAGEL, Recht, 1819 f.; DERSELBE, Signaturregelungen, 452.
625 §§ 1 Abs. 2 und 2 Nr. 8 SigG 01; vgl. auch Begründung SigG 01, 16 f.
626 § 2 Nr. 8 SigG 01; vgl. etwa BLUM, Entwurf, 72; zu den Begriffen sogleich N 431 ff., 423.
627 ROSSNAGEL, Recht, 1820.

bb) Überwachungssystem und Meldepflicht

An die Stelle der Genehmigung für Anbieter von Zertifikaten mit Rechtswirkung tritt nach Art. 3 Abs. 3 der Richtlinie ein Überwachungssystem, welches im Falle von Deutschland eine Meldepflicht vor Aufnahme der Tätigkeit, Kontrollen durch die zuständige Behörde[628] sowie Bussgelder im Falle der Verletzung der gesetzlichen Pflichten[629] vorsieht.[630] Die Meldepflicht umfasst Nachweise für Zuverlässigkeit, Fachkunde und Deckungsvorsorge, das Aufzeigen eines Sicherheitskonzeptes und eine Erläuterung, wie der Anbieter dieses umgesetzt hat.[631] Eine detaillierte Prüfung vor der Aufnahme des Betriebs unterbleibt im Unterschied zum SigG 97 und zur im Folgenden beschriebenen freiwilligen Akkreditierung.[632] Die Kontrolle der Angaben und von deren weiteren Erfüllung erfolgt vielmehr nur Stichprobeweise im Rahmen einer periodischen nachträglichen Überwachung.[633] Die Behörde kann einem Anbieter den Betrieb auch untersagen, sofern er bestimmte Voraussetzungen nicht erfüllt.[634] 416

cc) Freiwillige Akkreditierung

Die §§15 und 16 SigG 01 sehen neu eine freiwillige Akkreditierung der Anbieter im Sinne von Art. 3 Abs. 2 der Richtlinie vor.[635] Diese dient zunächst als Gefäss für die unter altem Recht ausgestellten Bewilligungen (Investitionsschutz für Zertifizierungsdiensteanbieter).[636] Dann ermöglicht sie die Ausstellung von Zertifikaten mit im Vergleich zur qualifizierten elektronischen Signatur zum Teil weiter erhöhter Sicherheit[637] und erlaubt die Schaffung höherer Rechtssicherheit hinsichtlich materiellrechtlicher Anerkennung der Signaturen und Beweiskraft.[638] Schliesslich kann die ex-ante-Prüfung unabhängig von der Frage der Anerkennung auch als *Gü-* 417

---

628 Es handelt sich wie schon beim SigG 97 um die *RegTP* (vgl. schon N 404, insbesondere FN 604); §§3 und 19 Abs. 1 SigG 01 i.V.m. §66 Telekommunikationsgesetz; vgl. auch Begründung SigG 01, 31; BLUM, Entwurf, 77f.; WELSCH, 408.

629 Diese entsprechen ungefähr den Genehmigungsvoraussetzungen des SigG 97; ROSSNAGEL, Signaturregelungen, 453.

630 §§4 Abs. 3, 19, 20 und 21 SigG 01; ROSSNAGEL, Recht, 1820; DERSELBE, Signaturregelungen, 456; GEIS, 670; WELSCH, 408 ff.; kritisch zu den Bussgeldern RIESS, 534.

631 §4 Abs. 2 SigG 01; Begründung SigG 01, 20.

632 ROSSNAGEL, Signaturgesetz, 202.

633 ROSSNAGEL, Signaturgesetz, 201, kritisiert die für diese Aufgabe völlig unzureichende personelle Ausstattung der zuständigen Behörde.

634 §19 Abs. 3 SigG 01.

635 Eingehend dazu etwa ROSSNAGEL, Recht, 1821f.; DERSELBE, Signaturregelungen, 453 ff.; vgl. auch BLUM, Entwurf, 73 und WELSCH, 413 ff.; zur Richtlinie vorne N 373.

636 Die Voraussetzungen der Akkreditierung stimmen mit den Genehmigungsvoraussetzungen des SigG 97 weitestgehend überein; Begründung SigG 01, 27.

637 So sind etwa Certificate Revocation Lists akkreditierter Anbieter für 30 Jahre, solche für qualifizierte elektronische Signaturen jedoch nur für zwei Jahre aufzubewahren, und für Erstere wird die Aufbewahrung im Konkurs des Anbieters erst noch durch die Regulierungsbehörde sichergestellt. Zu den Sicherheitsstufen (noch unter dem SigG 97) etwa ROSSNAGEL, Fortentwicklung, 2.4; vgl. auch Begründung SigG 01, 28f.; ROSSNAGEL, Signaturgesetz, 202; eingehend zu den Unterschieden zwischen qualifizierten elektronischen Signaturen und solchen mit Anbieterakkreditierung ROSSNAGEL, Recht, 1822 f.

tezeichen für die Anbieter und Verfahren gesehen werden,[639] was anerkannte Anbieter unter Umständen auch für geschlossene Benutzergruppen interessant macht.

418 Die in Art. 3 Abs. 7 der Richtlinie vorgesehene Möglichkeit, für öffentliche Bereiche eine Ausnahme vom Grundsatz der Bewilligungsfreiheit vorzusehen, wird mit § 15 Abs. 2 SigG 01 genutzt: Für den öffentlichen Bereich können durch zusätzliche Rechtsvorschrift qualifizierte elektronische Signaturen mit Anbieterakkreditierung verlangt werden.[640]

dd) Internationale Aspekte

419 Die Anforderungen der Richtlinie bezüglich e*infacher und fortgeschrittener elektronischen Signaturen* waren in Deutschland aufgrund des Prinzips der freien richterlichen Beweiswürdigung bereits nach früherem Recht erfüllt.[641]

420 *Qualifizierte elektronische Signaturen* von Anbietern mit Sitz in einem anderen Mitgliedstaat werden durch § 23 Abs. 1 SigG 01 den inländischen gleichgestellt und somit materiellrechtlich anerkannt.[642] Weisen sie zusätzlich *Anbieterakkreditierung* auf, so sind sie inländischen qualifizierten elektronischen Signaturen mit Anbieterakkreditierung gleichgestellt, sofern sie nachweislich die gleiche Sicherheit aufweisen und dies durch die für die Akkreditierung zuständige Behörde *festgestellt* wurde.[643] Diese Gleichstellung kann nicht ex lege erfolgen, weil die Mitgliedstaaten das Sicherheitsniveau ihres Akkreditierungssystems autonom festlegen können und ausländische Anbieter das deutsche Niveau damit u.U. nicht erreichen. Ferner können sich EU-Anbieter auch normal in Deutschland akkreditieren lassen.[644]

421 Öffentlich als qualifiziert ausgestellte Zertifikate von in *Drittstaaten* ansässigen Anbietern sind in Deutschland dann als solche anerkannt, wenn *i)* der Anbieter in einem anderen EU-Mitgliedstaat akkreditiert ist, *ii)* ein EU-Anbieter für das Zertifikat einsteht oder *iii)* das Zertifikat im Rahmen einer bi- oder multilateralen Vereinbarung anerkannt ist.[645] Die Regelung entspricht Art. 7 Abs. 1 der Signaturrichtlinie.[646] Soll ein Anbieter zusätzlich als in Deutschland akkreditiert gelten, so ist wie für die An-

---

638 Vorne N 280 ff., 373; zur Sicherheitsvermutung hinten N 456 ff.; vgl. auch GEIS, 670 f. und ROSSNAGEL, Fortentwicklung, 3 a.E.

639 § 15 Abs. 1 SigG 01; ROSSNAGEL, Signaturregelungen, 545; kritisch zur Frage, ob ein Gütezeichen durch den Staat abzugeben sei RIESS, 533. Technisch gesehen ist in Deutschland ein System mit staatlicher Wurzelinstanz vorgesehen, welche den akkreditierten Anbietern (BLUM, Entwurf, 77, spricht fälschlicherweise von *allen* Anbietern) ein spezielles Zertifikat zur Signierung der durch sie ausgestellten Zertfikate ausstellt; dazu ROSSNAGEL, Signaturregelungen, 452 und vorne N 90 ff.

640 Begründung SigG 01, 28; GEIS, 670; ROSSNAGEL, Recht, 1823; DERSELBE, Signaturregelungen, 545; zur Richtlinie vorne N 390.

641 Begründung SigG 01, 16; vorne N 379 f.

642 Begründung SigG 01, 16, 33; ROSSNAGEL, Recht, 1824.

643 Begründung SigG 01, 33; § 17 Abs. 2 E-SigV; kritisch zur Notwendigkeit einer solchen Feststellung RIESS, 534; vgl. etwa auch SPINDLER, Bankrecht I, Rz 102.

644 Dazu Begründung SigG 01, 34 sowie etwa BLUM, Entwurf, 73.

645 § 23 Abs. 1 SigG 01; ROSSNAGEL, Recht, 1824; DERSELBE, Signaturregelungen, 456.

646 Vorne N 398.

bieter anderer Mitgliedstaaten eine Beurteilung durch die für die Akkreditierung zuständige deutsche Behörde nötig.[647]

ee) Anerkennung von Prüf- und Bestätigungsstellen

422 Die Prüfung des Sicherheitskonzepts bei der Akkreditierung von Zertifizierungsdiensteanbietern nach § 15 Abs. 2 SigG 01 sowie die Prüfung von Produkten für elektronische Signaturen nach § 15 Abs. 7 und 17 SigG 01 wird durch *private Stellen* durchgeführt. Die Anerkennung dieser Stellen wird durch § 18 SigG 01 geregelt.[648] Bei der Aufsicht über die Einhaltung des Gesetzes kann sich die Regulierungsstelle für Telekommunikation und Post zudem gemäss § 19 Abs. 1 SigG 01 ebenfalls privater Stellen bedienen.

b) Qualifizierte Zertifikate

aa) Allgemeines

423 Die Definition des qualifizierten Zertifikats folgt der Signaturrichtlinie (§ 2 Nr. 6 SigG 01).[649] Der Zertifikatsinhalt richtet sich nach § 7 SigG 01 und § 14 SigV 01. Qualifizierte Zertifikate können nur für natürliche Personen ausgestellt werden.[650] Nach §5 Abs. 3 SigG 01 ist auf Verlangen des Antragstellers anstelle des Namens ein Pseudonym aufzunehmen.[651]

bb) Dokumentation der Ausstellung

424 Die Ausstellung der Zertifikate ist so zu dokumentieren, dass die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind.[652] Entsprechend Anhang II Bst. i der Richtlinie kann dies auch in elektronischer Form geschehen. Die Dokumentation muss für den Signierschlüsselhalter einsehbar sein.[653]

cc) Sperrung

425 Zertifikate sind zu sperren, wenn

- der Signierschlüsselhalter dies wünscht;
- das Zertifikat aufgrund falscher Angaben ausgestellt wurde;
- der Zertifizierungdiensteanbieter den Betrieb einstellt und kein anderer Anbieter dessen Zertifikate übernimmt;
- oder wenn die zuständige Behörde nach § 19 Abs. 4 eine Sperrung verfügt.[654]

---

647 GEIS, 673.
648 Vgl. etwa ROSSNAGEL, Recht, 1825; WELSCH, 409.
649 Vorne N 371, insbesondere FN 541.
650 § 2 Nr. 7 SigG 01; vgl. etwa WELSCH, 411; die Richtlinie ist diesbezüglich unklar; vorne N 383.
651 Zur Aufhebung von Pseudonymen, welche zu Gunsten von Privaten neu durch ein Gericht zu prüfen ist, § 14 Abs. 2 SigG 01; Begründung SigG 01, 26; eingehend ROSSNAGEL, Recht, 1821, DERSELBE, Signaturregelungen, 453; vgl. auch WELSCH, 411 f.
652 § 10 Abs. 1 SigG 01; Begründung SigG 01, 24.
653 § 10 Abs. 2 SigG 01; Begründung SigG 01, a.a.O.

426 Neu ist die Bestimmung von § 8 Abs. 2, wonach eine Sperrung auch durch diejenige Stelle verlangt werden kann, welche zur Bestätigung der im Zertifikat enthaltenen Attribute zuständig war.[655]

dd) Attribute

427 Qualifizierte Zertifikate können nach § 7 Abs. 1 Nr. 9 SigG 01 auch Attribute des Signierschlüsselhalters enthalten, also etwa Angaben über Vertretungsverhältnisse, berufsbezogene Angaben zur Person (Bewilligungen zur Ausübung bestimmter Tätigkeiten u. dgl.) o. ä. Die Aufnahme von Attributen bedarf neu der Einwilligung allfällig belasteter Personen (bei Vertretungsverhältnissen) bzw. der Bestätigung der zuständigen Stellen.[656]

428 § 7 Abs. 2 sieht vor, dass derartige Attribute auch in einem gesonderten Attributzertifikat festgehalten werden können, welches bloss eine Referenz auf ein Hauptzertifikat enthält, nicht jedoch einen Prüfschlüssel.[657]

c) Unterrichtungspflichten gegenüber dem Antragsteller

429 Der Zertifizierungsdiensteanbieter hat den Antragsteller auf ein Zertifikat gemäss § 6 Abs. 1 SigG 01 über die *technischen Massnahmen* zur Geheimhaltung seines Signierschlüssels zu unterrichten. Zudem hat sich der Zertifizierungsdiensteanbieter davon zu überzeugen, dass der Signierschlüsselhalter über eine sichere Signaturerstellungseinheit verfügt.[658] Im Weiteren muss er den Signierschlüsselhalter auf die Notwendigkeit hinweisen, alte Signaturen bei Bedarf vor dem Verlust ihrer Vertrauenswürdigkeit zu zeitstempeln.[659]

430 Nach § 6 Abs. 2 und 3 SigG 01 besteht ausserdem eine Pflicht, den Antragsteller über die *rechtlichen Wirkungen* der Signaturen zu informieren.[660] Diese Belehrung bezweckt, die Warnfunktion der elektronischen Signatur zu verstärken.[661]

d) Zeitstempel

431 Während § 9 SigG 97 noch eine Pflicht der Zertifizierungsdiensteanbieter zur Ausstellung von Zeitstempeln vorsah, wurde diese im SigG 01 zu einer Wahldienstleistung abgeschwächt.[662] Begründet wird dies mit der Formulierung von Bst. c des An-

---

654 D. h. wenn Tatsachen die Annahme rechtfertigen, dass qualifizierte Zertifikate gefälscht oder nicht hinreichend fälschungssicher sind oder dass sichere Signaturerstellungseinheiten Sicherheitsmängel aufweisen; § 8 Abs. 1 SigG 01; zum Ganzen WELSCH, 412.

655 Begründung SigG 01, 23; ROSSNAGEL, Signaturregelungen, 453; vgl. auch vorne b).

656 ROSSNAGEL, Recht, 1820; DERSELBE, Signaturregelungen, 453; vgl. auch sogleich N 425 f.

657 Zu Attributzertifikaten vorne N 115 f.

658 § 5 Abs. 6 SigG 01. Dies geht über die Anforderungen der Richtlinie hinaus; RIESS, 533.

659 Die Bestimmung spricht allerdings unklar von einer *Neusignierung*, erst § 17 SigV 01 nennt den Zeitstempel; vgl. auch sogleich N 431 ff.

660 Auch dies wird durch die Signaturrichtlinie nicht vorausgesetzt; zum Ganzen etwa ROSSNAGEL, Recht, 1820 f.

661 Vgl. etwa Begründung SigG 01, 22; FRITZSCHE/MALZER, 22.

hanges II der Richtlinie, welcher Zeitstempel nur mittelbar erwähnt,[663] woraus zu schliessen sei, dass es sich nicht um eine Pflichtdienstleistung handeln könne.[664]

Die Anforderungen an Zeitstempel wurden zudem neu technologieneutral formuliert, sodass nun sinnvollerweise auch Verfahren ohne Signatur zugelassen sind.[665] 432

4. Beweisrecht

Der auf dem ex-ante-Ansatz beruhende vorgezogene Anscheinsbeweis des alten § 1 Abs. 1 SigG 97[666] kann für Signaturen ohne Anbieterakkreditierung nicht mehr aufrecht erhalten werden, weil diese ja erst ex post geprüft werden.[667] 433

Neu ist indessen der durch das Formanpassungsgesetz eingeführte § 292a ZPO sowie eine Vermutung für die Sicherheit der Verfahren nach § 15 Abs. 1 Satz 4 SigG 01.[668] 434

5. Haftungsregelung

Die von Art. 6 der Richtlinie verlangten Regelungen und die im Evaluationsbericht der Bundesregierung zum IuKDG[669] gemachten Vorschläge betreffend die Haftung von Zertifizierungsdiensteanbietern werden durch die §§ 11 und 12 SigG 01 umgesetzt, ja sogar erweitert. Die Vorschrift klärt auch die bisher unsichere Rechtslage bezüglich der ausservertraglichen Haftung von Zertifizierungsdiensteanbietern für Vermögensschäden.[670] 435

Während die Haftung nach Art. 6 der Richtlinie nur die Richtigkeit der zertifizierten Daten zum Zeitpunkt der Ausstellung des Zertifikats, für den tatsächlichen Besitz des Antragstellers am Signierschlüssel, für die tatsächliche Nutzungsmöglichkeit von Signier- und Prüfschlüssel sowie für eine nicht korrekt durchgeführte Sperrung des Zertifikats umfasst,[671] betrifft § 11 SigG 01 den gesamten Geschäftsprozess.[672] 436

Gemäss Abs. 2 der Bestimmung handelt es sich um eine Verschuldenshaftung mit Beweislastumkehr, die aber laut Abs. 3 durch im Zertifikat aufzuführende Nutzungs- oder Transaktionswertbeschränkungen begrenzt werden kann.[673] Der Entlastungsbe- 437

---

662 § 9 SigG 01; Begründung SigG 01, 17.

663 «[Zertifizierungsdiensteanbieter] müssen gewährleisten, dass Datum und Uhrzeit der Ausstellung oder der Sperrung eines Zertifikats genau bestimmt werden können.»

664 Begründung SigG 01, 23.

665 Begründung SigG 01, 17; zu den Verfahren vorne N 174 ff.

666 Vorne N 405.

667 ROSSNAGEL, Recht, 1819; DERSELBE, Signaturregelungen, 452.

668 Dazu hinten N 456 ff.

669 Das SigG 97 bildete Teil des IuKDG; vorne N 407.

670 Vorne N 403; Begründung SigG 01, 24; GEIS, 671; vgl. auch ROSSNAGEL, Fortentwicklung, 3 sowie LEIER.

671 Vorne N 393 ff.

672 Begründung SigG 01, 24 ff.; eingehend ROSSNAGEL, Recht, 1823; DERSELBE Signaturregelungen, 455; kritisch RIESS, 533.

673 Begründung SigG 01, 25; GEIS, 671; ROSSNAGEL, Signaturregelungen, 455.

weis für beauftragte Dritte ist gemäss Abs. 4 ausgeschlossen, weil die umfassenden Haftungsregeln (insbesondere auch zur Deckungsvorsorge) bei der Auslagerung von Aufgaben an Dritte regelmässig nicht greifen würden.[674]

438 § 12 SigG 01 verlangt eine Deckungsvorsorge von 250'000 Euro pro haftungsauslösendem Ereignis.[675]

C. Formanpassungsgesetz

1. Regelungsbereich

439 Wie erwähnt regelt das SigG 01 wie schon das SigG 97 die materiellrechtliche und prozessuale Anerkennung der elektronischen Signatur nicht;[676] dieser Bereich wird vielmehr durch ein *Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr*[677] *(FormanpassungsG)* geregelt, welches am 1. August 2001 in Kraft getreten ist.[678] Das Gesetz umfasst ausschliesslich Änderungen an bereits bestehenden Gesetzen wie dem BGB, der ZPO, dem Handelsgesetzbuch, verschiedenen Gerichtsordnungen, der Grundbuchordnung sowie dem Verbraucherkreditgesetz.[679]

440 Wichtigstes Ziel der Regelung ist, zentral eine übersichtliche Regelung der neuen Formvorschriften zu schaffen, um eine Verzettelung in einer Vielzahl von Regelungen zu vermeiden.[680] Ergänzend werden prozessuale Vorschriften über die Einreichung von Schriftsätzen und Erklärungen angepasst.

2. Materiellrechtliche Aspekte

a) Regelungsmodell

441 Das FormanpassungsG definiert zusätzlich zu den in § 125 ff. BGB bereits geregelten Arten von Formvorschriften (gesetzliche und gewillkürte Schriftlichkeit, notarielle Beurkundung und öffentliche Beglaubigung) neu eine *elektronische Form* als Ersatz für die Schriftform (§ 126a BGB) sowie eine *Textform* für Fälle, in denen die Handunterschrift entbehrlich ist (§ 126b BGB).[681]

442 Die elektronische Form kann nach dem neuen § 126 Abs. 3 BGB die schriftliche Form überall dort ersetzen, wo das Gesetz nicht ausdrücklich eine Ausnahme von der

---

674 Begründung SigG 01, a.a.O.; vgl. auch BLUM, Entwurf, 76.
675 ROSSNAGEL, Recht, 1818; DERSELBE, Signaturregelungen, 456; WELSCH, 410.
676 Vorne N 408.
677 BGBl. I S. 1542 ff.; vgl. auch die Begründung, BT-Drs. 14/4987, sowie Beschlussempfehlung und Bericht des Bundestags-Rechtsausschusses, BT-Drs. 14/5561.
678 Art. 35 FormanpassungsG; LÜDEMANN/ADAMS, 9.
679 Vgl. etwa LÜDEMANN/ADAMS, 9 ff.; eingehend ROSSNAGEL, Recht, 1818 f., 1825 ff.
680 Begründung FormanpassungsG, 10, 18.
681 Begründung FormanpassungsG, 10; LÜDEMANN/ADAMS, 9.

Gleichstellung macht. Das FormanpassungsG folgt damit dem geschilderten Ansatz der durch Ausnahmebestimmungen abgeschwächten pauschalen Anerkennung.[682]

Die Zulassung der Textform erfolgt durch Änderung der betroffenen Bestimmungen. 443

b) Elektronische Form

Der neue § 126a BGB lautet: «Soll die gesetzlich vorgeschriebene schriftliche Form 444
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.» Mit der Bestimmung setzt der deutsche Gesetzgeber Art. 9 der E-Commerce-Richtlinie (enabling principle) sowie Art. 5 der Signaturrichtlinie um (materiellrechtliche Anerkennung).[683]

Auch die qualifizierte elektronische Signatur erfüllt die Warnfunktion nur relativ 445
schwach.[684] Gerade in Bereichen, in denen diese eine herausragende Rolle spielt, wurden daher Ausnahmebestimmungen geschaffen. Es sind dies die Kündigung des Arbeitsverhältnisses,[685] die Bürgschaftserkärung,[686] das Leibrentenversprechen zur Gewährung familienrechtlichen Unterhalts,[687] das Versprechen[688] und die Schuldanerkenntnis.[689] Hinzu kommen Ausnahmen für das Grundbuch- und Schiffsregisterrecht, wo das Verfahrensrecht die Anbringung eines Eintragungsantrags in schriftlicher Form vorsieht. Insoweit müssen die Rechtsgrundlagen für elektronischen Dokumentenverkehr noch geschaffen werden.[690] Weitere Ausnahme bestehen im Bereich der Arbeitsverträge, in dem die Tarifvertragsparteien im Rahmen ihrer Tarifautonomie über Formvorschriften zu befinden haben,[691] beim Arbeitszeugnis, welches in elektronischer Form derzeit nur schlecht als Bewerbungsunterlage eingereicht werden könnte,[692] beim Verbraucherkreditvertrag, beim Vertrag über die Teilnutzung von Wohngebäuden sowie bei bestimmten Informationspflichten des Arbeitgebers, die aufgrund von übergeordnetem EU-Recht schriftlich sein müssen.[693]

---

682 Dazu vorne N 265.

683 Begründung FormanpassungsG, 14 und 15; LÜDEMANN/ADAMS, 8, 10; eingehend ROSSNAGEL, Recht, 1825; SPINDLER, Bankrecht II, Rz 149 ff.; vorne N 362 ff., N 389 f.

684 Begründung FormanpassungsG, 15 ff., 17; hinten N 857 ff.

685 Art. 1 Nr. 7 FormanpassungsG; § 623 BGB; Begründung FormanpassungsG, 22.

686 Art. 1 Nr. 9 FormanpassungsG; § 766 BGB; Begründung FormanpassungsG, 22.

687 Art. 1 Nr. 8a FormanpassungsG; § 761 BGB; Begründung FormanpassungsG, 36. Die Beschränkung auf *familienrechtlichen* Unterhalt ergibt sich daraus, dass das Leibrentenversprechen in Art. 9 Abs. 2 der E-Commerce-Richtlinie nicht als zulässige Ausnahme von der materiellrechtlichen Anerkennung der elektronischen Unterschrift vorgesehen ist (vorne N 363), in familienrechtlichen Angelegenheiten aber Ausnahmen gemacht werden können; Begründung FormanpassungsG, 43.

688 Dieses entspricht ungefähr dem Schenkungsversprechen nach Art. 243 OR; Art. 1 Nr. 10 FormanpassungsG; § 780 BGB; Begründung FormanpassungsG, 22.

689 Art. 1 Nr. 11 FormanpassungsG; § 781 BGB; Begründung FormanpassungsG, 22.

690 Begründung FormanpassungsG, 12 f.

691 Begründung FormanpassungsG, 14 f.

692 Art. 1 Nr. 8 FormanpassungsG; Begründung FormanpassungsG, 22.

446 Das Erfordernis des Beifügens des Namens des Unterzeichners wird laut Begründung zur Gewährleistung der Identitätsfunktion der Unterschrift benötigt.[694] Diese erfolgt jedoch m.E. durch Signatur und Zertifikat bereits in ausreichender Weise. Durch das Hinzufügen des Namens als ein unterschriftsähnliches Verhalten wird aber immerhin die relativ schwache Warn- und Dokumentenabschlussfunktion[695] der elektronischen Signatur gestärkt. Das Beifügen des Namens hat so zwar einerseits eine gewisse Berechtigung, schafft aber andererseits auch zusätzliche Komplexität, welche zu einer erhöhten Zahl versehentlich nichtiger Rechtsgeschäfte führen könnte. Dieser Nachteil überwiegt die gewonnenen Vorteile m.E. deutlich. Der schweizerische Gesetzgeber verzichtet denn auch richtigerweise auf dieses Erfordernis.[696]

c) Textform

447 Der neue § 126b BGB lautet: «Ist durch Gesetz Textform vorgeschrieben, so muss die Erklärung in einer Urkunde oder auf eine andere zur dauerhaften Wiedergabe in Schriftzeichen geeignete Weise abgegeben werden, die Person des Erklärenden genannt und der Abschluss der Erklärung durch Nachbildung der Namensunterschrift oder anders erkennbar gemacht werden.»[697]

448 Die Textform verzichtet auf die Unterschrift und verlangt nur noch die in lesbaren Schriftzeichen fixierte Erklärung (worunter auch eine durch den Empfänger entsprechend darstellbare elektronische Übermittlung fällt, nicht jedoch eine gesprochene Mitteilung).[698] Sie ersetzt die Schriftform dort, wo *i)* kein öffentliches Interesse an erheblichen Beweiswirkungen besteht, wo ein Text *ii)* keine erheblichen Rechtsfolgen nach sich zieht bzw. diese einfach rückgängig zu machen sind und wo es *iii)* keines Übereilungsschutzes bedarf.[699] Es geht dabei in erster Linie um Informations- und Dokumentationsanforderungen, welche mangels Dauerhaftigkeit der Aufzeichnung nicht mündlich erfüllt werden können, bei denen das Schriftformerfordernis aber unverhältnismässig ist, wie etwa bei Verbraucherkrediten die Bestätigung der Vertragsbedingungen gegenüber dem Verbraucher oder seine Unterrichtung bei Änderungen des Jahreszinses.[700] Ziel ist teilweise auch die Vereinfachung von Massenvorgängen, wie etwa bestimmter Mitteilungen im Versicherungswesen.[701]

---

693 Der Verbraucherkreditvertrag aufgrund der Verbraucherkreditrichtlinie (87/102/EWG; dazu SPINDLER, Bankenrecht II, Rz 150) der Vertrag über die Teilnutzung von Wohngebäuden aufgrund der Time-Sharing-Richtlinie (94/47/EWG) und die Informationspflichten des Arbeitgebers gemäss Richtlinie 91/533/EWG; vgl. Begründung FormanpassungsG, 27, 31.

694 Begründung FormanpassungsG, 16; hinten N 847 ff.

695 Zur Abschlussfunktion Begründung FormanpassungsG, 16 sowie hinten N 864 ff.

696 Hinten N 894 ff.

697 Vgl. LÜDEMANN/ADAMS, 9 f.; zur Textform auch hinten N 821 ff.

698 Begründung FormanpassungsG, 19 f.; zum etwa noch im deutschen Fernabsatzgesetz gebräuchlichen Begriff dauerhaften Datenträgers und der Frage, ob E-Mail hierfür ausreicht OLG München, K&R 313 ff. und dazu HÄRTING, 310 ff.

699 Begründung FormanpassungsG, 12, 18, 19.

700 Art. 16 Nr. 2 FormanpassungsG; § 5 Abs. 1 Verbraucherkreditgesetz; Begründung FormanpassungsG, 27; Andreas MÜGLICH, Neue Formvorschriften für den E-Commerce, Zur Umsetzung der EU-Signaturrichtlinie in deutsches Recht, MMR 1/2000, 7 ff., 12.

d) Einheit der Vertragsurkunde

Setzt das Gesetz eine Form für den Vertragsabschluss voraus, so konnte diese gemäss § 126 Abs. 2 BGB schon bisher nur durch Unterzeichnung der selben Vertragsurkunde durch beide Parteien oder zumindest durch Unterzeichnung gleich lautender Vertragsurkunden erfüllt werden. Der Vertragsabschluss durch Unterzeichnen von Offerte und Akzept war ausgeschlossen.[702] 449

Dies gilt nach § 126a Abs. 2 nun auch für die elektronische Form. Obwohl es technisch möglich ist, ein mit einer elektronischen Signatur versehenes Dokument mit einer zweiten Signatur zu versehen,[703] ist allerdings nur vom Unterzeichnen jeweils gleich lautender Dokumente die Rede.[704] 450

e) Teilnahme an der elektronischen Kommunikation

Das Gesetz nimmt das Einverständnis des Empfängers zur elektronischen Kommunikation nicht vorweg. Eine elektronische Nachricht gilt weiterhin nur dann als zugegangen, wenn der Empfänger zumindest durch konkludentes Handeln die Anwendung elektronischer Kommunikationsmittel gebilligt hat und daher mit dem Eingang elektronischer Nachrichten rechnen musste. Allein im Besitz eines Signierschlüssels liegt keine derartige Billigung.[705] 451

f) Gewillkürte Schriftform

Zur Erfüllung einer gewillkürten Schriftform gelten nach § 127 Abs. 1 BGB im Zweifel auch die Vorschriften der §§ 126 - 126b BGB, d.h. bei vereinbarter Schriftform ist auch die elektronische Form möglich.[706] 452

g) Gewillkürte elektronische Form

Ist die elektronische Form vereinbart, so gilt im Zweifel auch eine einfache elektronische Signatur nach § 2 Nr. 1 SigG 01 als ausreichend (d.h. etwa eine eingescannte Unterschrift). Dies entspricht der Rechtsprechung zu § 127 BGB, wonach nebst der explizit genannten telegrafischen Übermittlung auch ein Telefax oder die Aushändigung einer Kopie zur Erfüllung ausreicht.[707] Immerhin bleibt es den Parteien unbenommen, nachträglich eine qualifizierte elektronische Signierung nach § 126a BGB (oder sollte diese nicht möglich sein, eine manuelle Unterzeichnung) zu verlangen.[708] 453

---

701 ROSSNAGEL, Signaturregelungen, 457; BRISCH, Textform und elektronische Form, 537; vgl. Art. 31 FormanpassungsG und dazu Begründung FormanpassungsG, 31.

702 PALANDT-HEINRICHS, N 4 zu § 126 BGB.

703 Etwa nach dem S/MIME-Standard; vgl. auch BRISCH, Textform und elektronische Form, 537f.

704 Zum Ganzen Begründung FormanpassungsG, 17 ff.; vgl. insbesondere auch die Abweichungen bei der gewillkürten Schriftform nach § 127 BGB und dazu Begründung FormanpassungsG, 20 ff.; vgl. auch FRITZSCHE/MALZER, 24.

705 Begründung FormanpassungsG, 12, 15; ROSSNAGEL, Signaturregelungen, 457.

706 Vgl. soeben N 451.

707 PALANDT-HEINRICHS, N 1f. zu § 127 BGB.

708 § 127 Abs. 3 BGB; Begründung FormanpassungsG, 21.

3. Prozessuale Aspekte

a) Besonderheiten des deutschen Urkundenbeweises

454 Die Echtheit der Unterschrift ist durch die sich auf die Urkunde stützende Partei nachzuweisen, ohne dass ihr dafür gesetzliche Beweiserleichterungen zustünden.[709] Dies entspricht der schweizerischen Rechtslage.[710]

455 Im Weiteren weist das deutsche Urkundenbeweisrecht indessen zwei gesetzliche Beweisregeln auf, welche dem schweizerischen Recht fremd sind: Nach § 440 Abs. 2 ZPO hat eine (unterschriebene) Privaturkunde die *widerlegbare Vermutung der Echtheit* für sich, sofern die Echtheit der Unterschrift feststeht, d.h. der Urkundentext gilt als unverändert,[711] und nach § 416 ZPO begründen echte unterzeichnete Privaturkunden im Weiteren den *vollen Beweis für die Abgabe der in ihr enthaltenen Erklärungen durch die Aussteller.*[712] Dabei handelt es sich um eine unwiderlegbare Vermutung; ein Gegenbeweis kann nur insofern erbracht werden, als der Aussteller die willentliche Begebung (Inverkehrsetzung) der Urkunde bestreitet, also behauptet, sie sei ihm entzogen worden.[713] Beide Vermutungen betreffen ausschliesslich die formelle Beweiskraft der Urkunde, d.h. die Tatsache, dass die beurkundete Erklärung abgegeben wurde, nicht jedoch die materielle Beweiskraft, d.h. die Richtigkeit des verurkundeten Inhaltes.[714]

---

709 § 440 Abs. 1 ZPO; RÜSSMANN, Beweisrecht, Abschnitt «Die Bedeutung des § 416 ZPO für Wissenserklärungen».

710 Hinten N 648 ff.

711 BAUMBACH/LAUTERBACH/ALBERS/HARTMANN, N 1 zu § 440 ZPO.

712 ZÖLLER-GEIMER, N 1 zu § 440 ZPO; RÜSSMANN, Beweisrecht, Abschnitt «Beweiskraft für die Abgabe der Erklärung».

713 Die Begebung wird allerdings ebenfalls (widerlegbar) vermutet; BAUMBACH/LAUTERBACH/ALBERS/HARTMANN, N 1 zu § 440 ZPO; RÜSSMANN, Beweisrecht, Abschnitt «Beweiskraft für das Inverkehrbringen der Erklärung»; Begründung FormanpassungsG, 25.

714 ZÖLLER-GEIMER, N 5 f. vor § 415 ZPO.

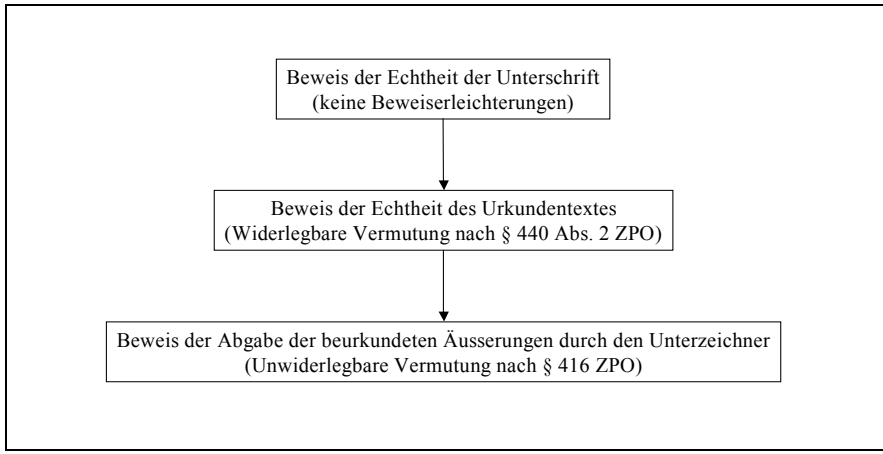

Abbildung 11: Der Urkundenbeweis nach deutschem Recht.

b) Beweiserleichterung

aa) Begründung und Regelungsmodell

456 In der Begründung zum FormanpassungsG wird angeführt, der Beweis der Echtheit der Unterschrift könne bei einer elektronischen Signatur bereits durch eine *einfache Behauptung des Signierschlüsselhalters*, die Erklärung stamme nicht von ihm, widerlegt werden.[715] Diese Aussage basiert offenbar auf der (m.E. korrekten) Annahme, dass die für einen den Echtheitsbeweis der elektronischen Signatur zu erbringende Indizienkette regelmässig zu komplex wäre, um in jedem Glied zur vollen Überzeugung des Gerichts bewiesen werden zu können.[716]

457 Um diese Situation zu korrigieren, statuiert § 292a ZPO einen *gesetzlichen Anscheinsbeweis*[717]*:* Der Beweis mittels einer qualifizierten elektronischen Signatur kann demnach nur durch Tatsachen erschüttert werden, die *ernstliche Zweifel* daran begründen, dass die Erklärung mit dem Willen des Signierschlüsselhalters abgegeben worden ist, und nicht mehr durch die blosse Behauptung einer Fälschung.[718] Hinzu

---

715 Begründung FormanpassungsG, 25.

716 So auch ROSSNAGEL, Signaturregelungen, 459; eingehend vorne N 199 ff. Die Beweiserleichterung wird im Weiteren damit begründet, dass nur sie die Akzeptanz elektronischer Signaturen im Rechtsgeschäftsverkehr zu gewährleisten möge und dass ein elektronisches Dokument, welches eine «weitaus höhere» Sicherheit als ein handschriftlich unterzeichnetes Dokument aufweise, diesem gegenüber nicht schlechter gestellt werden dürfe. Schliesslich wird auf die widersprüchliche Praxis zum Anscheinsbeweis beim Missbrauch von EC-Karten hingewiesen (dazu hinten N 723, insbesondere FN 1127), welche es bei der elektronischen Signatur zu verhindern gelte; Begründung FormanpassungsG, 44.

717 Vorne N 276.

kommt bei Signaturen mit Anbieterakkreditierung eine Sicherheitsvermutung nach § 15 Abs. 1 Satz 4 SigG 01.[719]

bb) Tatbestandsmerkmale des § 292a ZPO

458 § 292a ZPO findet unter zwei tatbestandsmässigen Voraussetzungen Anwendung. Die erste besteht in der erfolgreichen «Prüfung nach dem Signaturgesetz», d.h. einem positiven Prüfresultat einer gesetzeskonformen Signaturprüfeinheit. Die zweite besteht im Vorliegen einer qualifizierten elektronischen Signatur.[720]

cc) Bedeutung der Anbieterakkreditierung

459 Die wohl bedeutendste Wirkung der *Anbieterakkreditierung* besteht darin, den Nachweis des Vorliegens einer qualifizierten elektronischen Signatur vorweg zu nehmen: Die Gerichte können anhand des von der Regulierungsstelle für Telekommunikation und Post für akkreditierte Anbieter verwendeten Wurzelzertifikats unmittelbar auf die Akkreditierung des Zertifizierungsdiensteanbieters und damit, auf dem Wege der Sicherheitsvermutung von § 15 Abs. 1 Satz 4,[721] auf eine qualifizierte elektronische Signatur schliessen.[722]

460 Fehlt die Akkreditierung indessen, so ist zu diesem Nachweis regelmässig ein Sachverständigengutachten nötig, welches sämtliche Voraussetzungen für das Vorliegen einer qualifizierten elektronischen Signatur behandelt. Dessen Resultat und richterliche Würdigung sind mit erheblicher Unsicherheit behaftet, weshalb die nach § 292a ZPO vorgesehenen Beweiswirkungen praktisch wohl nur von Signaturen mit Anbieterakkreditierung erreicht werden dürften.[723]

c) Prozessuale Anerkennung?

461 Die Beweisführung mittels elektronisch signierter Dokumente erfolgt weiterhin nach den Vorschriften über den Augenscheinsbeweis und nicht nach denjenigen für den Urkundenbeweis, wie dies vereinzelt gefordert worden war.[724] Dies laut Begründung daher, weil erstens einem elektronischen Dokument die Verkörperung fehle, auf wel-

---

718 Vgl. schon vorne N 275 f.; möglich blieben etwa (substanzierte) Vorbringen, wonach dem Signierschlüsselhalter das Token gestohlen worden oder das der Signatur zugrunde liegende Zertifikat gefälscht sei. Kann ein Signaturverfahren als solches im Laufe der Zeit nicht mehr als sicher betrachtet werden, so könnte auch dies vorgebracht werden. Zum Ganzen OERTEL, 420; LÜDEMANN/ADAMS, 11, 12; kritisch etwa BIZER/MIEDBRODT, 145 f.; kritisch ROSSNAGEL, Recht, 1826; DERSELBE, Signaturregelungen, 459.

719 Begründung SigG 01, 28; ROSSNAGEL, Recht, 1822.

720 OERTEL, 420; ROSSNAGEL, Signaturregelungen, 459; SPINDLER, Bankrecht I, Rz 98; zur Frage ob der Anscheinsbeweis auch andere Signaturverfahren (insbesondere HBCI) zur Anwendung kommen kann a.a.O, Rz 84 ff.; vgl. auch die Stellungnahme des Bundesrates sowie die Gegenäusserung der Bundesregierung, Begründung FormanpassungsG 36 f., 44.

721 Vorne N 457; ROSSNAGEL, Recht, 1826.

722 § 15 Abs. 1 Satz 4 SigG 01; ROSSNAGEL, Signaturregelungen, 460; vgl. auch hinten N 683 ff.

723 OERTEL, 420; ROSSNAGEL, Recht, 1826; DERSELBE, Signaturregelungen, 459.

724 Begründung FormanpassungsG, 23, 25; vgl. auch FRITZSCHE/MALZER, 19; HAMMER/BIZER, 698; ROSSNAGEL, Signaturregelungen, 459 m.H.; SPINDLER, Bankrecht I, Rz 76.

che die für Privaturkunden bestimmten Vorschriften zugeschnitten seien, und zweitens die geschilderten gesetzlichen Vermutungen der hohen Beweiskraft elektronisch signierter Dokumente nicht gerecht würden.[725] Für die deutsche Rechtslage ist dem wohl zuzustimmen, während die Dinge in der Schweiz anders liegen.[726]

d) Aktenverkehr mit Gerichten

462 Die durch Art. 2 FormanpassungsG eingebrachten Änderungen lassen für Schriftsätze und Erklärungen der Parteien sowie für Erklärungen Dritter neu die Einreichung als elektronisches Dokument zu. Dabei tritt – sofern eine Unterschrift gefordert ist – nach dem neu eingefügten § 130a ZPO die qualifizierte elektronische Signatur an die Stelle der Handunterschrift.

463 Die Bestimmung des genauen Zeitpunkts der Einführung wurde an die Verordnungsgeber delegiert, weil die Gerichte zunächst mit Infrastruktur auszurüsten sind. Ebenfalls an die Verordnungsgeber delegiert wird die Entscheidung, in welchen Dokumentenformaten die Eingaben zu erfolgen haben.[727]

464 Die Zustellung elektronischer Dokumente von den Gerichten an die involvierten Personen wurde im Rahmen eines separaten *Gesetzes zur Reform des Verfahrens bei Zustellungen im gerichtlichen Verfahren (Zustellungsreformgesetz*[728]*)* geregelt.

---

725 Begründung FormanpassungsG, 25; eingehend etwa auch RÜSSMANN, Beweisrecht.

726 Dazu hinten N 777 f.

727 Zum Ganzen Begründung FormanpassungsG, 23 ff.; Georg BORGES, Prozessuale Formvorschriften und der elektronische Rechtsverkehr, K&R 4/2001, 196 ff., 207 ff.; ROSSNAGEL, Recht, 1825 f.

728 BGBl. I S. 1206 ff.

3. Teil: Regelung im schweizerischen Recht

§ 8 Einleitung

I. Gang der Darstellung des dritten Teils

465 Nachdem in einem ersten Teil technische und ökonomische Aspekte elektronischer Signaturen und in einem zweiten Teil Regelungsbedarf und -modelle sowie mögliche Umsetzungen in geltendes Recht beschrieben wurden, soll im nun folgenden dritten Teil die für die Schweiz vorgesehene Regelung dargestellt werden. Dabei wird auf den gegenwärtig vorliegenden Entwurf des Bundesrates für ein Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) Bezug genommen.

466 In der Folge ist zunächst auf die bisherigen gesetzgeberischen Aktivitäten des Bundes im Bereich der elektronischen Signatur einzugehen (§ 8 II). Hernach werden mit dem Vorentwurf für ein Bundesgesetz über den elektronischen Geschäftsverkehr und dem Entwurf für die Totalrevision der Bundesrechtspflege zwei weitere aktuelle Gesetzgebungsprojekte beschrieben, soweit sie elektronische Signaturen betreffen (§ 8 III).[729]

467 § 9 beschreibt die vorgesehene Regelung der Sicherungsinfrastruktur, welche die Grundlage für die übrigen Regelungsbereiche darstellt. Weil diese Regelung indessen für die Anwendung elektronischer Signaturen nur selten unmittelbare Bedeutung hat, sondern sich in erster Linie an die Zertifizierungsdiensteanbieter richtet, beschränkt sich diese Darstellung auf das vorgeschlagene Regelungsmodell sowie einen kurzen Überblick über dessen Umsetzung.

468 Wie in § 4 angesprochen ist die Beweiskraft der Verfahren aufgrund der komplexen Indizienkette sowie einiger in der Natur bestimmter Indizien liegender Schwierigkeiten genau besehen nicht ausreichend, um eine volle Überzeugung des Gerichts von der Echtheit einer elektronisch signierten Urkunde zu begründen. Anders als noch der Vorentwurf verzichtet der Entwurf des Bundesrates indessen auf eine explizite beweisrechtliche Regelung dieses Problems, was die Frage nach einer richterrechtlichen Lösung aufwirft. In § 10 wird nach einer Auseinandersetzung mit den Grundlagen des Beweisrechts auf diese Frage eingegangen.

469 Eine flächendeckende Ausstattung der Gerichte mit Signaturprüfeinheiten brächte einige technische sowie organisatorische Probleme mit sich und dürfte sich vorderhand mangels Verbreitung der Verfahren nicht lohnen. § 11 schildert zunächst einen Lösungsansatz für diese Schwierigkeiten und behandelt danach die prozessuale Anerkennung der elektronischen Signatur, und zwar sowohl hinsichtlich des normalen Urkundenbeweises als auch hinsichtlich der provisorischen Rechtsöffnung.

---

729 Vgl. zu elektronischen Belegen im Mehrwertsteuerwesen die Literatur in FN 4.

470 Obwohl die materiellrechtliche Anerkennung regelmässig als eines der ersten Postulate genannt wird, wenn die Integration elektronischer Signaturen in die Rechtsordnung zur Sprache kommt, dürfte sie m. E. vorderhand nur eine untergeordnete Bedeutung erlangen; denn zunächst werden Anwendungen in geschlossenen Benutzergruppen im Vordergrund stehen, und auch wenn sich elektronische Signaturen dereinst in offenen Benutzergruppen etablieren sollten, so werden diese wohl mehrheitlich im formfreien Bereich zur Anwendung gelangen.[730] Gerade bei der materiellrechtlichen Anerkennung weicht der Bundesrat indessen vom Vorbild des EU-Richtlinienrechts ab, indem er auf Ausnahmebestimmungen gänzlich verzichtet. § 12 geht zunächst auf die das schweizerische System gesetzlicher Formvorschriften sowie auf die damit verfolgten Zwecke ein und nimmt dann zum Vorschlag des Bundesrates Stellung. Abschliessend ist genau auf die vorgeschlagene Anerkennungsnorm Art. 14 Abs. 2bis E-OR einzugehen.

II. Gesetzgebung zur elektronischen Signatur

A. Anfänge

471 Der Startschuss zur Integration elektronischer Signaturen in die schweizerische Rechtsordnung kam von der damaligen Nationalrätin Vreni SPOERRY. Sie lud den Bundesrat mit einer *Motion* vom 16. März 1994 ein, eine «Gesetzesvorlage zur Änderung von Artikel 14 des schweizerischen Obligationenrechts vorzulegen, damit elektronische Unterschriften rechtsverbindlich erfolgen können.»[731] Der Bundesrat stimmte der Motionärin in seiner Antwort grundsätzlich zu, beurteilte die Sache aber nicht als dringlich, weil sich einerseits die technischen Voraussetzungen noch in einer Testphase befänden und andererseits zunächst die internationale Entwicklung abzuwarten sei. Der Schweiz würde hier zudem keine Pionierrolle zustehen.[732] Die Motion wurde schliesslich in ein Postulat umgewandelt und überwiesen.[733]

472 In Anbetracht der steigenden Bedeutung der neuen Informations- und Kommunikationstechnologie beschloss der Bundesrat am 28. Februar 1996 die Einsetzung einer verwaltungsunabhängigen *Groupe de Réflexion* zur Gewinnung von Entscheidgrundlagen und Ideen für die Erarbeitung und Umsetzung einer schweizerischen Strategie und zur Verabschiedung eines Aktionsplanes in diesem Bereich. Die Gruppe tagte am 28. Juni 1996 erstmals. Der im Juni 1997 erschienene Bericht[734] nennt u.a. die Gleichsetzung von elektronischer Signatur und Handunterschrift sowie Regeln für

---

730 Vorne N 247, 268.
731 AB NR 1994, 1883 f.
732 AB NR 1994, 1884.
733 AB NR 1994, 1884.
734 Bericht Groupe de Réflexion, http://www.isps.ch/ger/stored_documents/PDF/52.pdf.

die Etablierung einer Sicherungsinfrastruktur als notwendige rechtliche Rahmenbedingungen für den E-Commerce.[735]

473 Am 18. Februar 1998 veröffentlichte der Bundesrat u.a. gestützt auf diese Vorarbeiten ein *Strategiepapier «für eine Informationsgesellschaft in der Schweiz»*.[736] Darin beauftragte er unter anderem EJPD, EFD und UVEK, «die digitale Signatur einzuführen und zu diesem Zweck eine Public Key Infrastructure zu konzipieren sowie die dafür notwendigen Regeln zu erarbeiten.»[737] Hierfür wurde eine *interdepartementale Arbeitsgruppe «DigSig»* gebildet, in der auch interessierte Kreise aus dem Privatsektor Einsitz hatten.[738]

474 Am 24. November 1998 stellte diese Arbeitsgruppe ihre Resultate an einer Tagung vor[739] und präsentierte zwei Papiere zur Sicherungsinfrastruktur bzw. zu digitaler Signatur und Privatrecht.[740]

475 Zu erwähnen ist an dieser Stelle schliesslich die Koordinationsgruppe Informationsgesellschaft (KIG), deren Einsetzung ebenfalls im Rahmen der bundesrätlichen Strategie «für eine Informationsgesellschaft in der Schweiz» beschlossen wurde,[741] und die in ihren Berichten an den Bundesrat regelmässig auf Aspekte der Public-Key-Infrastruktur eingeht.[742]

B. Zertifizierungsdiensteverordnung

476 Am 4. Juli 1999 übergab die genannte Arbeitsgruppe DigSig den Entwurf einer *Verordnung über eine Public-Key-Infrastruktur PKI in der Schweiz (PKIV)* zusammen mit einem erläuternden Bericht an über 150 Personen und Organisation zur Konsultation.[743] Wie bereits aus dem Erlasstitel ersichtlich, beschränkte sich der Entwurf auf die Regelung der PKI. Die rechtliche Anerkennung der elektronischen Signatur und die Haftungsregelungen sollten dabei vorläufig aussen vor bleiben.[744]

---

735 Bericht Groupe de Réflexion, 36.

736 Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz; http://www.isps.ch/ger/stored_documents/HTML/42.html.

737 Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz, Ziff. 33; PESTALOZZI/VEIT, 601.

738 LEGLER, E-Commerce, 13f.

739 JÖHRI, 73ff.; LEGLER, E-Commerce, 14; David ROSENTHAL, Unterschreiben mit einem Mausklick, Rechtliche Probleme bei der Anwendung digitaler Signaturen, NZZ Nr. 217, 20. November 1998.

740 Das Letztere wurde in der VPB publiziert (BJ, Gutachten); zum Ganzen BJ, Gutachten, FN 1.

741 KIG, Bericht 1, 7.

742 So wird die Frage aufgeworfen, inwieweit der Bund allen Bürgern eine digitaler Identitätskarte zur Verfügung stellen soll (allenfalls Integration eines Chips in die herkömmliche Identitätskarte); KIG, Bericht 3, 40f. Im Weiteren wird etwa auf das bislang mangelnde Engagement der Kantone bezüglich der Integration elektronischer Signaturen in deren Rechtsordnungen kritisiert; KIG, Bericht 3, 30f., 63.

743 LEGLER, E-Commerce, 14.

744 Kommentar ZertDV, 1; Botschaft ZertES, 5680; JACCARD, Projet, 63.

477 Am 12. April 2000 verabschiedete der Bundesrat die Verordnung unter dem definitiven Namen *Verordnung über Dienste der elektronischen Zertifizierung (Zertifizierungsdiensteverordnung; ZertDV)* und setzte sie auf den 1. Mai 2000 in Kraft.[745] Aufgrund der unsicheren gesetzliche Grundlage[746] wurde sie bloss als befristete Versuchsregelung erlassen mit dem Ziel, die Verordnung bald durch ein formelles Gesetz zu ersetzen, welches sämtliche Aspekte im Zusammenhang mit der elektronischen Signatur regeln sollte.[747]

478 Die Ausführungsbestimmungen zur ZertDV traten am 1. September 2001 in Kraft.[748]

C. ZertES

1. Entwicklung

479 Am 17. Januar 2001 gab der Bundesrat den Vorentwurf für ein *Bundesgesetz über elektronische Signaturen (BGES)* für rund zweieinhalb Monate in die Vernehmlassung *(VE-BGES)*.[749] Das BGES sollte nebst der Regelung der Sicherungsinfrastruktur, die weitgehend der ZertDV entsprach,[750] noch weitere für eine Integration elektronischer Signaturen in die Rechtsordnung notwendige Regelungen umfassen, wie die materiellrechtliche Anerkennung, Haftungsfragen und Fragen des Registerrechts.[751]

480 Bereits am 6. Juli 2001 verabscheidete der Bundesrat Entwurf und Botschaft zu dem nun so genannten *Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)* zuhanden des Parlaments.[752] Vorgesehen war ursprünglich eine Behandlung in der Wintersession 2001 in beiden Parlamentskammern gleichzeitig. Mittlerweile haben sich gegenüber diesem Zeitplan jedoch Verzögerungen ergeben; voraussichtlich wird der Ständerat in der Sommersession 2002 als Erstrat über

---

745 SR 784.103; dazu JACCARD (Forme), 113 ff.; JÖRG/ARTER, 449 ff.; LEGLER, E-Commerce, 1 ff.; Thomas LEGLER, Startschuss für elektronische Zertifizierungsdienste, Bundesrätliche Verordnung schafft eine rechtliche Grundlage, NZZ Nr. 94, 20. April 2000, 87 = Jusletter 8. Mai 2000; PESTALOZZI/VEIT, 601, 603 ff.; RAMSAUER 59 ff.; WEBER, Schweiz, 86 ff.

746 Die Verordnung stützt sich auf das Bundesgesetz über die technischen Handelshemmnisse (THG) und das Fernmeldegesetz (FMG), ohne dass in diesen Erlassen eine explizite Delegation an den Gesetzgeber vorgenommen worden wäre; vgl. Kommentar ZertDV, 1; JÖRG/ARTER, 450; PESTALOZZI/VEIT, 601.

747 Art. 1 Abs. 1 und Art. 21 Abs. 2 ZertDV; Kommentar ZertDV, 1. Dieses Vorgehen entspricht offenbar der gängigen Praxis des BAKOM, sofern ein Erlass innert nützlicher Frist in ein umfassendes Gesetz einfliessen soll; LEGLER, E-Commerce, 15.

748 SR 784.103.1.

749 http://www.bj.admin.ch/themen/e-commerce/vn-ve-a-d.pdf; dazu Begleitbericht VE-BGES; SCHÖBI, Bundesgesetz, Rz. 1 ff.; SIDLER. Zu den Resultaten der Vernehmlassung vgl. die Zusammenfassung der Stellungnahmen zum VE-BGES, http://www.bj.admin.ch/themen/e-commerce/vn-ber-bges.pdf; Botschaft ZertES, 5690 f.

750 Begleitbericht VE-BGES, 10; Botschaft ZertES, 5686.

751 RAGGENBASS, B47; vgl. auch vorne N 259 ff.

752 BBl 2001, 5679 ff.; vgl. dazu etwa RAGGENBASS, B47; SCHLAURI, Basistechnologie, 55 ff.

die Vorlage befinden, womit das Gesetz – nach Ablauf der Referendumsfrist – frühestens auf Anfang 2003 in Kraft treten kann.

481 Die Ausführungsbestimmungen sollen nach Aussagen des BAKOM möglichst gleichzeitig mit dem ZertES in Kraft treten. Entwürfe sind derzeit nicht verfügbar, sodass in der Folge auf die Ausführungsbestimmungen der ZertDV, von welchen die Bestimmungen zum ZertES nicht mehr stark abweichen dürften, Bezug genommen wird.

482 Mit geschilderten Entwicklung gingen eine grössere Anzahl parlamentarische Vorstösse einher, auf die an dieser Stelle nicht weiter eingegangen werden soll.[753]

2. Ziele und Mittel

483 Art. 1 Abs. 2 E-ZertES nennt als Ziele des Gesetzes die Förderung eines breiten Angebotes an sicheren Diensten zur elektronischen Zertifizierung, die Begünstigung der Verwendung qualifizierter elektronischer Signaturen[754] sowie die internationale Anerkennung von Zertifizierungsdiensteanbietern und ihrer Leistungen.[755]

484 Die bisher fehlende materiellrechtliche Anerkennung elektronischer Signaturen soll durch einen neuen Art. 14 Abs. 2bis OR eingeführt werden.[756] Der E-ZertES regelt daher die Voraussetzungen für die zur Anerkennung der Signaturen nötige Anerkennung der Zertifizierungsdiensteanbieter.

485 Der materiellrechtlichen Anerkennung der Signaturen wird indessen bei deren Förderung meist eher untergeordnete Bedeutung zugesprochen.[757] Die Anbieteranerkennung kann m. E. indessen auch in weiteren Bereichen von Bedeutung sein: In offenen Benutzergruppen muss der Empfänger einer unterzeichneten Nachricht auch im formfreien Bereich Gewissheit über die Beweiseignung des verwendeten Verfahrens haben; die staatliche Anerkennung des Anbieters kann hierfür als *Gütesiegel* dienen, das Rechtssicherheit schafft,[758] und weil die Anbieteranerkennung die Beweisführung mit elektronischen Signaturen vereinfacht, könnte sie zudem auch im Bereiche geschlossener Benutzergruppen durchaus sinnvoll sein.[759]

486 Die *prozessuale Anerkennung* (d. h. die Zulassung elektronisch signierter Dokumente zum Urkundenbeweis) soll sich nach der Ansicht des Bundesrates aus der materiellrechtlichen von selber ergeben. Sie wird daher nicht explizit geregelt.[760] Auch eine

---

753 Näheres bei LEGLER, E-Commerce, FN 27.
754 Zum Begriff hinten N 515.
755 Vgl. Botschaft ZertES, 5684, 5692.
756 Botschaft ZertES, 5684 f.
757 Vgl. schon N 470.
758 Vgl. vorne N 242, 279.
759 Hinten N 764 ff. Die Botschaft ZertES, 5692, geht indessen davon aus, dass sich die Rechtsfolgen bei Signaturen mit und ohne Anbieteranerkennung kaum unterscheiden und misst der Anbieteranerkennung entsprechend geringe Bedeutung zu.
760 Botschaft ZertES, 5688; eingehend hinten N 772 ff.

beim Vorliegen bestimmter Eigenschaften einer Signatur greifende gesetzliche *Beweiserleichterung*, wie sie in Deutschland geschaffen wurde,[761] ist im Entwurf – anders als noch im Vorentwurf – nicht mehr vorgesehen; elektronische Signaturen bleiben bezüglich Beweiskraft anderen Beweismitteln gleichgestellt und unterstehen der freien richterlichen Beweiswürdigung.[762]

III. Gesetzgebung in benachbarten Rechtsgebieten

A. Bundesgesetz über den elektronischen Geschäftsverkehr

1. Überblick

487 Gleichzeitig mit dem VE-BGEG wurde eine Vernehmlassungsvorlage für ein *Bundesgesetz über den elektronischen Geschäftsverkehr (BGEG)* veröffentlicht *(VE-BGEG)*.[763] Die Vorlage vereinigt eine Anzahl verschiedener Neuerungen unter einem Dach, etwa zum elektronischen Vertragsabschluss, zu Konsumentenfernabsatzverträgen (teilweiser Nachvollzug der EU-Fernabsatzrichtlinie betreffend Widerrufsrecht und Informationspflichten[764]), zum Kaufrecht (Verlängerung der Gewährleistungsfrist und Nachbesserungsrecht) sowie zum Lauterkeitsrecht (neue ausservertragliche Informationspflichten im Fernabsatz und elektronischen Geschäftsverkehr).[765] Der Titel der Vorlage ist damit insofern unpassend, als sich der Themenkreis nicht nur auf elektronisch abgeschlossene Rechtsgeschäfte beschränkt.

488 Ursprünglich war geplant, BGES und BGEG als Gesamtpaket zu verabschieden. Bedenken der Wirtschaft, die Verabschiedung des BGES könnte sich verzögern, führten schliesslich jedoch zu einer Aufteilung der beiden Vorlagen.[766] Mit der Botschaft zum BGEG ist nicht vor der zweiten Hälfte 2002 zu rechnen, in Kraft treten dürfte der Erlass frühestens 2004.[767]

---

761 Vorne N 456 ff.
762 Vgl. jedoch hinten N 673 ff.
763 http://www.bj.admin.ch/themen/e-commerce/intro-d.htm.
764 Zur Fernabsatzrichtlinie vorne N 353 ff.
765 Zum Ganzen FREI, N 623 ff.; HONSELL/PIETRUSZAK, 771 ff.; SPINDLER, Bemerkungen, 259 ff.; BIRCHER, 467 ff.
766 Vgl. dazu auch hinten N 928
767 PIETRUSZAK, B46.

2. Fernabsatzverträge insbesondere

a) Allgemeines

An dieser Stelle ist in erster Linie die teilweise Umsetzung der EU-Fernabsatzrichtlinie hinsichtlich eines siebentägigen Widerrufsrechts für Fernabsatzverträge interessant,[768] denn dieses wird gelegentlich angeführt, um das Fehlen von Ausnahmen für den Bereich des Konsumentenschutzes von der Anerkennung elektronischer Signaturen zu rechtfertigen.[769] 489

Systematisch gesehen nimmt der Vorentwurf die Regelung für Fernabsatzverträge in wenig übersichtlicher Weise[770] zusammen mit einer partiellen Neuregelung der Haustürgeschäfte in den Art. 40a-h VE-OR vor. 490

b) Geltungsbereich der Art. 40b ff. VE-OR

Die Art. 40b ff. VE-OR sind gemäss Art. 40a VE-OR auf Fernabsatz- und Haustürverträge anwendbar, die 491

- bewegliche Sachen und Dienstleistungen betreffen;[771]
- für den persönlichen oder familiären Gebrauch des Kunden bestimmt sind;
- bei denen der Anbieter im Rahmen einer beruflichen oder gewerblichen Tätigkeit gehandelt hat.[772]

Ausgeschlossen sind Verträge, 492

- bei denen die Leistung des Kunden 100 Franken nicht übersteigt;[773] 493
- über Finanzdienstleistungen, namentlich Versicherungsverträge;[774] 494
- über verderbliche Güter sowie Güter, die aufgrund ihrer Beschaffenheit nicht zurückgegeben werden oder die nach genauen Angaben des Kunden angefertigt werden; 495
- über Dienstleistungen, die eindeutig auf die persönlichen Bedürfnisse des Kunden zugeschnitten sind;[775] 496
- über Wetten und Lotterien. 497

---

768 Vgl. Begleitbericht VE-BGEG, 7.
769 Vgl. etwa Botschaft ZertES, 5687; SCHÖBI, Vertragsschluss, 101; eingehend hinten N 923 f.
770 Kritisch auch HONSELL/PIETRUSZAK, 780; positiver FREI, N 684.
771 Vgl. FREI, N 626; HONSELL/PIETRUSZAK, 781.
772 Begleitbericht VE-BGEG, 11.
773 Begleitbericht VE-BGEG, 11; FREI, N 631; HONSELL/PIETRUSZAK, 781.
774 Dies entspricht der Regelung der Fernabsatzrichtlinie; das Widerrufsrecht soll in der EU jedoch durch eine entsprechende Richtlinie hinsichtlich Finanzdienstleistungen doch noch eingeführt werden; vorne N 359. Der Bundesrat gibt an, diese Richtlinie später separat nachvollziehen zu wollen; Begleitbericht VE-BGEG, 11, 32
775 Kritisch HONSELL/PIETRUSZAK, 781 sowie FREI, N 634.

c) *Begriff des Fernabsatzvertrages*

498 Art. 40c VE-OR definiert den Fernabsatzvertrag als Vertrag, der ohne gleichzeitige körperliche Anwesenheit der Vertragsparteien abgeschlossen wird und bei dem der Anbieter im Rahmen eines für den Fernabsatz organisierten Vertriebssystems ausschliesslich ein oder mehrere Fernkommunikationsmittel verwendet.[776] Beim Fernabsatzvertrag handelt es sich damit nicht um einen eigenen Vertragstyp, sondern um einen Vertrag irgend eines Typs, der im Fernabsatz geschlossen wurde. Darunter fallen nicht nur auf elektronischem Weg geschlossene Verträge, sondern auch solche, die über Printmedien, Telefon, Fernsehen oder Radio zustande kommen.[777]

499 Anbieter, die im Rahmen ihrer konventionellen Geschäftstätigkeit nur gelegentlich auch Bestellungen auf dem Wege des Fernabsatzes entgegen nehmen, sind nach Art. 40c VE-OR nicht betroffen.[778]

500 Nicht als Fernabsatzverträge gelten nach Art. 40c Abs. 2 VE-OR Versteigerungen, Verträge, die unter Verwendung von Warenautomaten oder automatisierten Geschäftsräumen abgeschlossen werden sowie Verträge mit Betreibern von Fernmeldeanlagen durch Benutzung öffentlicher Telefone.

d) *Widerrufsrecht für Fernabsatzverträge*

501 Nach Art. 40e VE-OR kann der Kunde seinen Antrag zum Vertragsabschluss oder seine Annahmeerklärung innerhalb von sieben Tagen in Papierform oder auf elektronischem Weg widerrufen. Die Frist beginnt zu laufen, sobald der Kunde den Vertrag beantragt oder angenommen hat und von den Angaben Kenntnis genommen hat, die zu machen der Anbieter nach Art. 40d VE-OR verpflichtet ist (diese betreffen unter anderem das Bestehen des Widerrufsrechts selbst).

502 Die Regelung des Widerrufsrechts dient in erster Linie dem Nachvollzug der Fernabsatzrichtlinie.[779] Während diese indessen durch das Widerrufsrecht dem Konsumenten eine goods-in-hand-Entscheidung ermöglichen und dadurch dessen Vertrauen in den Fernabsatz fördern will,[780] sieht die Botschaft den Grund für die Einführung eines Widerrufsrechts allein beim Übereilungsschutz.[781] In der Folge unterscheiden sich die Regelungen teilweise. Insbesondere setzt die Richtlinie den Beginn des Fristenlaufs auf das Eintreffen der Ware fest, während der VE-OR auf den Zeitpunkt von Offerte oder Akzept des Kunden abstützt.[782]

503 Vom Widerrufsrecht ausgenommen sind nach Art. 40f Bst. b VE-OR Audio- und Videoaufzeichnungen sowie Software, sofern sie vom Kunden bereits entsiegelt wur-

---

776 Vgl. Begleitbericht VE-BGEG, 12 f.; FREI, N 546 ff., 628; HONSELL/PIETRUSZAK, 782 f.
777 HONSELL/PIETRUSZAK, 776.
778 Begleitbericht VE-BGEG, 13; FREI, N 629; HONSELL/PIETRUSZAK, 782 f.
779 Begleitbericht VE-BGEG, 6 f., 11.
780 Vorne N 356.
781 Begleitbericht VE-BGEG, 6 f., 11; SPINDLER, Bemerkungen, 26.
782 FREI, N 669 ff.; kritisch HONSELL/PIETRUSZAK, 785.

den oder die heruntergeladen werden können,[783] und zwar deshalb, weil keine Kontrolle über eine allfällige weitere Nutzung durch den Kunden möglich ist.[784] Im Weiteren kann der Kunde nach Art. 40f Bst. a VE-OR bei Dienstleistungen ausdrücklich auf das Widerrufsrecht verzichten, sofern diese vor dem Ablauf der Widerrufsfrist erbracht wird.[785]

504 Die Rechtsfolge des Widerrufs besteht in der Pflicht zur Rückerstattung beider Leistungen, wobei der Kunde die Kosten für die Rücksendung der Ware tragen muss.[786]

B. Totalrevision der Bundesrechtspflege

1. Überblick

505 Am 28. Februar 2001 verabschiedete der Bundesrat Entwurf und Botschaft für eine Totalrevision der Bundesrechtspflege, welche u.a. die Schaffung eines Bundesgerichtsgesetzes, eines Bundesstrafgerichtsgesetzes und eines Bundesverwaltungsgerichtsgesetzes, sowie Änderungen an weiteren Gesetzen vorsieht.[787] Kernbereiche der Revision sind die Schaffung von Einheitsbeschwerden (Zivil-, Strafsachen, öffentlich-rechtliche Angelegenheiten), der Ausbau der richterlichen Vorinstanzen (Bundesstraf- und -verwaltungsgericht), Anhebung der Streitwertgrenzen mit gleichzeitiger Möglichkeit für das Bundesgericht, Rechtsfragen von grundsätzlicher Bedeutung trotz unterschrittener Streitwertgrenze an sich zu ziehen.[788]

2. Elektronischer Rechtsverkehr insbesondere

506 An dieser Stelle ist nur von Bedeutung, dass im Rahmen der Totalrevision der Bundesrechtspflege auch die gesetzlichen Grundlagen für den elektronischen Rechtsverkehr in eidgenössischen Verwaltungs- und Gerichtsverfahren geschaffen werden sollen.[789] Dabei geht es einerseits um die Übermittlung von Rechtsschriften an die Behörden und andererseits um die Eröffnung von Rechtsakten an die Parteien.[790] Letztere soll weiterhin nur zulässig sein, wenn die Partei zugestimmt hat.[791] Der zum elektronischen Verkehr mit den Behörden befugte Personenkreis soll nicht beschränkt werden, auch wenn davon auszugehen ist, dass in erster Linie Personen mit

---

783 FREI, N 641; HONSELL/PIETRUSZAK, a.a.O.
784 Begleitbericht VE-BGEG, 17.
785 FREI, N 640; kritisch HONSELL/PIETRUSZAK, a.a.O.
786 Art. 40g VE-OR; Begleitbericht VE-BGEG, 17; FREI, N 674 ff.
787 BBl 2001, 4202 ff.
788 Botschaft Totalrevision Bundesrechtspflege, 4207 f.
789 Botschaft ZertES, 5686; vgl. insbesondere auch SANGIORGIO, 47 ff.
790 Botschaft Totalrevision Bundesrechtspflege, 4261; zur elektronischen Eröffnung von Rechtsakten insbesondere SANGIORGIO, 55 ff.
791 Botschaft Totalrevision Bundesrechtspflege, 4269 f.; Art. 36 und Art. 56 Abs. 3 E-BGG; SANGIORGIO, 55.

regelmässigen Behördenkontakten, wie beispielsweise Anwälte, vom Angebot Gebrauch machen werden.[792]

507 Die Bundesbehörden sollen schrittweise auf den elektronischen Verkehr vorbereitet werden. Im Rahmen des Projektes *GovLink* des Bundes werden die hierzu nötigen technischen und organisatorischen Grundlagen[793] ausgearbeitet und zunächst in Pilotprojekten getestet.[794] Ziel ist, binnen zehn Jahren mit sämtlichen Behörden den elektronischen Verkehr zu ermöglichen.[795] Als eine der ersten Stellen soll das Bundesgericht den elektronischen Rechtsverkehr aufnehmen.[796]

508 Sind Schriftstücke zu unterzeichnen, so soll bei elektronischer Einreichung neu auch eine anerkannte elektronische Unterschrift[797] zulässig sein.[798] Die Botschaft[799] spricht noch von Signaturen, die der ZertDV entsprechen; diese regelt jedoch die Anerkennung elektronischer Signaturen gerade nicht, sondern spricht vorerst nur von den Anbietern. Sinnvollerweise sollte die Anerkennung der Signaturen im BGG daher auf die Anerkennungsnorm des E-ZertES (Art. 14 Abs. 2bis E-OR) verweisen.

509 Eine ausnahmslose Zulassung der elektronischen Signatur ist möglich, weil diese alle im Prozessrecht genutzten Funktionen der Handunterschrift erfüllen kann und weil insbesondere die in den übrigen Bereichen teilweise problematisch Warnfunktion kaum von Bedeutung ist.[800]

510 Als Beilagen zu elektronischen Rechtsschriften sollen gemäss einem modifizierten Art. 52 Abs. 1 BZP neu auch elektronische Kopien *(Scans)* zulässig sein, wobei diese gleich behandelt werden sollen wie bisher Fotokopien, d.h. bis zur Bestreitung der Echtheit ist kein Original vorzulegen.[801] *Nicht näher geregelt* wird die Einordnung elektronisch signierter Dokumente im System der Beweismittel (prozessuale Anerkennung als Urkunde).[802] Die Einordnung ist hier aber mangels unterschiedlicher Rechtsfolgen wohl auch nicht von grosser Bedeutung.

---

792 Botschaft Totalrevision Bundesrechtspflege, 4263; vorne N 251.
793 So beispielsweise ein einheitliches Dokumentenformat.
794 Zu GovLink etwa BJ, Projektskizze GovLink, 4 ff., 7 f. Vgl. auch Botschaft Totalrevision Bundesrechtspflege, 4266.
795 Botschaft Totalrevision Bundesrechtspflege, 4262; vgl. Art. 49 Abs. 4 E-BGG.
796 Botschaft Totalrevision Bundesrechtspflege, 4262; zum Ganzen auch SANGIORGIO, 52.
797 Dazu hinten N 894 ff.
798 Eingehend SANGIORGIO, 51; das Bundesgericht lehnt bisher die Einreichung von Fotokopien, Fax u.dgl. konsequent ab; SANGIORGIO, 49.
799 Botschaft Totalrevision Bundesrechtspflege, 4264.
800 Botschaft Totalrevision Bundesrechtspflege, 4263 ff.; zu den Funktionen der Handunterschrift hinten N 833 ff.; vgl. auch SANGIORGIO, 51.
801 Botschaft Totalrevision Bundesrechtspflege, 4265; eingehend SANGIORGIO, 52 f.; vgl. hinten N 655 f.
802 Eingehend dazu hinten N 772 ff.

§9 Sicherungsinfrastruktur

I. Regelungsmodell

511 Zunächst soll das Regelungsmodell dargestellt und danach ein kurzer Einblick in die Umsetzung gegeben werden.[803]

512 Der E-ZertES folgt dem Prinzip der freiwilligen Anerkennung der Zertifizierungsdiensteanbieter: Die Ausstellung digitaler Zertifikate ist grundsätzlich frei; soll jedoch eine elektronische Signatur materiellrechtlich anerkannt sein, so muss sie auf dem Zertifikat eines gemäss Art. 3 ff. E-ZertES anerkannten Zertifizierungsdiensteanbieters basieren.[804] Hinsichtlich der materiellen Anerkennung wird also *ausschliesslich* ein ex-ante-Ansatz verfolgt.[805] Das schweizerische Modell unterscheidet sich damit von demjenigen der EU, bei dem die materiellrechtliche Anerkennung auf einem ex-post-Ansatz in Kombination mit einem für die Mitgliedstaaten *fakultativ* vorzusehenden ex-ante-Ansatz basiert.[806] Begründet wird das Abweichen zum einen mit der beim ex-post-Ansatz fehlenden Rechtssicherheit hinsichtlich Anerkennung und zum anderen damit, dass Signaturen ohne Anbieteranerkennung im formfreien Bereich gar keine oder nur geringe Nachteile mit sich zögen.[807]

513 Gleich wie die Signaturrichtlinie folgt der E-ZertES bei der Beschreibung der Voraussetzungen für die Anerkennung von Anbietern und Signaturen einem technikrechtlichen und nicht einem funktionalen Ansatz. Damit eine elektronische Signatur materiellrechtlich anerkannt ist, müssen daher eine Vielzahl technischer Voraussetzungen erfüllt sein.[808]

---

803 Für detailliertere Darstellungen der PKI-Regelung vgl. die Botschaft ZertES, SCHLAURI, Basistechnologie, 76 ff. sowie die Literatur zur ZertDV (N 477, insbesondere FN 745).

804 Vgl. schon vorne N 286; zu Art. 59a E-OR, der die Haftung des Schlüsselhalters dann wieder auf Zertifikate *mit* Anbieteranerkennung beschränkt und damit das Prinzip der freiwilligen Anerkennung zu untergraben droht hinten N 760.

805 Zum ex-ante- und ex-post-Ansatz vorne N 280 ff.

806 Vorne N 370 ff., 416 ff.; zu beachten ist, dass die Signaturrichtlinie dort, wo der E-ZertES von Anerkennung spricht, den Begriff der Akkredierung verwendet, während der E-ZertES die staatliche Zulassung der Anerkennungsstellen als Akkreditierung bezeichnet; vgl. Art. 3 ZertES und Art. 3 Abs. 2 der Signaturrichtlinie.

807 Botschaft ZertES, 5692.

808 Vgl. Art. 14 Abs. 2bis E-OR i.V.m. Art. 2 Bst. c E-ZertES sowie Art. 5 Abs. 1 Signaturrichtlinie; zu den Begriffen vorne N 294 ff.

II. Überblick über die Regelung

A. Arten elektronischer Signaturen

514 Die Definitionen des E-ZertES sind eng an die EU-Signaturrichtlinie bzw. an das deutsche Signaturgesetz 2001 angelehnt.[809]

515 Die *(einfache) elektronische Signatur* sowie die *fortgeschrittene elektronische Signatur* werden in beinahe wortwörtlicher Übernahme der Signaturrichtlinie funktional definiert. Das Vorliegen einer elektronischen oder einer fortgeschrittenen elektronischen Signatur zieht indessen keine besonderen Rechtsfolgen nach sich; diese Definitionen dienen einzig als Basis für die Definition der *qualifizierten elektronischen Signatur*.[810]

516 Die qualifizierte elektronische Signatur wiederum wird technikrechtlich definiert als eine fortgeschrittene elektronische Signatur, die auf einer *sicheren Signaturerstellungseinheit* nach Art. 6 Abs. 1 und 2 E-ZertES und auf einem *qualifizierten und zum Zeitpunkt des Erzeugens gültigen Zertifikat* beruht. Die qualifizierte elektronische Signatur entspricht damit – abgesehen vom Erfordernis der Gültigkeit des Zertifikats zum Zeitpunkt des Erzeugens – dem nach Art. 5 Abs. 1 der Signaturrichtlinie materiellrechtlich anerkannten Signaturtyp.[811] Mit der Voraussetzung des qualifizierten Zertifikats für die qualifizierte elektronische Signatur verlässt der Entwurf den Boden der Technologieneutralität zumindest hinsichtlich des Einsatzes von Public-Key-Kryptographie, denn Zertifikate haben ohne Public-Key-Kryptographie keinen Sinn.[812] Kritik am Fehlen von Technologieneutralität[813] ist indessen nicht angebracht.[814] Wichtig ist schliesslich, dass auch zur Qualifikation einer Signatur als qualifizierte elektronische Signatur *keine Anbieteranerkennung* vonnöten ist, aber sehr wohl für deren materiellrechtliche Anerkennung nach Art. 14 Abs. 2bis E-OR.

B. Signatur- und Signaturprüfschlüssel

517 Art. 2 Bst. d und 4 E-ZertES übernehmen die Begriffe *Signatur-* und *Signaturprüfschlüssel* des deutschen Signaturgesetzes anstelle der komplizierten Begriffe der Signaturrichtlinie (*Signaturerstellungs- und Prüfdaten*).[815]

---

809 Art. 2 E-ZertES; Botschaft ZertES, 5692 f.; JACCARD, Projet, 66; zu den Definitionen der Signaturrichtlinie vorne N 375 ff., zu denjenigen des SigG 01 N 410 ff.

810 Die von Art. 5 Abs. 2 der Signaturrichtlinie geforderte Zulassung (einfacher) elektronischer Signaturen zum Beweis entspricht in der Schweiz seit jeher geltendem Recht; vorne N 380; hinten N 775 ff., 804. Weitere Regelungen können daher entfallen.

811 Dieser wird in der Richtlinie jedoch nicht gesondert definiert; vorne N 385 ff.

812 Vorne N 303 ff.; vgl. auch JACCARD, Projet, 65; ähnlich RAGGENBASS, B47; für das deutsche SigG 01 ROSSNAGEL, Recht, 1819.

813 Geäussert etwa bei JACCARD, Projet, 65 f.

814 Vorne N 303 ff.

Meines Erachtens wären jedoch die Begriffe *Signierschlüssel* und *Prüfschlüssel* vorzuziehen, weil sie klarer bzw. zumindest kürzer sind.[816] Weil die gesetzliche Terminologie noch nicht definitiv ist, soll hier weiterhin von Signier- und Prüfschlüssel gesprochen werden. 518

C. Zertifizierungsdiensteanbieter

1. Begriffe

Anbieterinnen von Zertifizierungsdiensten werden in Art. 2 Bst. g E-ZertES definiert als Stellen, die im Rahmen einer elektronischen Umgebung Daten bestätigen und zu diesem Zweck digitale Zertifikate ausstellen. Aus Gründen der Verständlichkeit der Formulierungen wäre m.E. der männliche, zusammengesetzte Begriff des *Zertifizierungsdiensteanbieters* vorzuziehen.[817] Auf die Übernahme der vorgeschlagenen Form wird daher im Folgenden verzichtet. 519

Die *Anerkennungsstelle* wird in Art. 2 Bst. h E-ZertES definiert als eine Stelle, die nach dem Akkreditierungsrecht für die Anerkennung der Anbieterinnen von Zertifizierungsdiensten akkreditiert ist.[818] Die Norm verweist damit auf die einschlägigen Bestimmungen des Bundesgesetzes über die technischen Handelshemmnisse[819] sowie der Verordnung über das schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitätsbewertungs-, Anmelde- und Zulassungsstellen.[820] 520

2. Akkreditierung, Anerkennung und Zertifizierung

Der E-ZertES folgt dem bereits in der ZertDV aufgenommenen Modell der Anerkennung durch private *Anerkennungsstellen*, die ihrerseits durch eine staatliche *Akkreditierungsstelle* akkreditiert sind.[821] Diese Regelung bewirkt eine weitgehende Entlastung der Administration des Bundes von der technisch anspruchsvollen Aufgabe der Prüfung.[822] 521

---

815 § 2 Nr. 4 und 5 SigG 01.

816 Vgl. schon Simon SCHLAURI/Reto KOHLAS, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 50.

817 Simon SCHLAURI/Reto KOHLAS, a.a.O.

818 Mit einer *Akkreditierung* wird formell die Kompetenz einer Stelle anerkannt, nach international massgebenden Anforderungen bestimmte Prüfungen oder Konformitätsbewertungen durchzuführen. Art. 2 AkkBV; Kommentar ZertDV, 2.

819 THG; SR 946.51.

820 AkkBV, SR 946.512; vgl. Botschaft ZertES, 5686, 5702 f.

821 Vgl. schon vorne N 280 ff.

822 RAMSAUER, 67; vgl. auch PESTALOZZI/VEIT, 603 f.

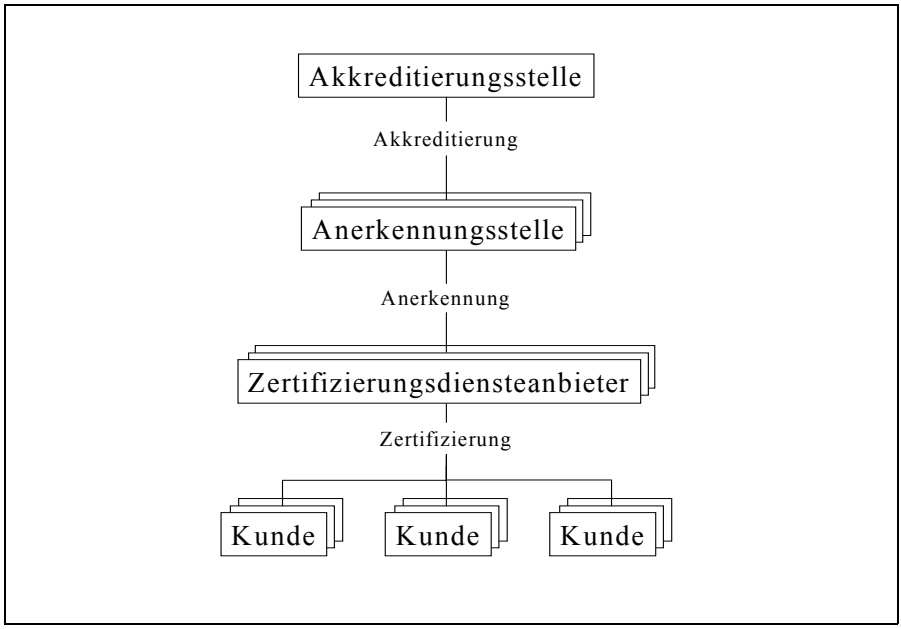

Abbildung 12: Akkreditierung, Anerkennung und Zertifizierung gemäss ZertDV und E-ZertES.[823]

522 Sofern das ZertES keine besonderen Vorschriften enthält, richtet sich das Verfahren nach dem Bundesgesetz über die technischen Handelshemmnisse.[824] Gemäss Art. 4 Abs. 1 E-ZertES bezeichnet der Bundesrat die Akkreditierungsstelle.[825] Wird keine Anerkennungsstelle akkreditiert, so kann der Bundesrat die Akkreditierungsstelle auch als Anerkennungsstelle bezeichnen.[826] Dies dürfte indessen nicht nötig sein, weil sich KPMG im Januar 2002 als Anerkennungsstelle nach der ZertDV akkreditieren liess.[827] Die Anerkennungsstellen melden der Akkreditierungsstelle die von ihnen anerkannten Anbieter. Die Akkreditierungsstelle publiziert eine entsprechende Liste.[828] Diese muss auch entzogene oder gelöschte Anerkennungen mit dem Zeitpunkt des Entzuges bzw. der Löschung enthalten, weil ansonsten die materiellrecht-

---

823 Nach RAMSAUER, 69.

824 Art. 15 Abs. 1 E-ZertES; Botschaft ZertES, 5686.

825 Dies unterscheidet sich von der Regelung in Art. 5 THG, wonach die Schweizerische Akkreditierungsstelle SAS zuständig ist.

826 Art. 4 Abs. 2 E-ZertES.

827 KPMG, Erste Zertifizierungsstelle für Public Key Infrastructure in Europa, KPMG durch die METAS-SAS in Bern akkreditiert, http://www.kpmg.ch/library/attachments/press/Media_Release_PKI_d_9865685.pdf.

828 Art. 5 E-ZertES; Botschaft ZertES, 5695.

liche Anerkennung einer vor dem Entzug der Anerkennung erstellten Signatur nicht mehr überprüft werden kann.[829]

523 Die Anerkennung ist ein privatrechtliches Rechtsgeschäft, während die Akkreditierung öffentlichrechtlicher Natur ist.[830]

524 Die Voraussetzungen der Anerkennung werden in Art. 3 E-ZertES geregelt. Der Bundesrat erlässt Ausführungsbestimmungen.[831] Für eine ausführliche Beschreibung sei auf die Botschaft ZertES, 5693 ff., auf den Kommentar des BAKOM zur ZertDV, 2 ff., sowie auf RAMSAUER, 69 ff. verwiesen.

3. Anerkennung ausländischer Anbieter

525 Anders als die Regelung von Art. 5 Abs. 1 der Signaturrichtlinie sieht der E-ZertES keine ex-post-Anerkennung von Signaturen vor. Nur eine solche würde es indessen ermöglichen, Signaturen, die auf Zertifikaten ausländischer Anbieter beruhen, ohne weiteres anzuerkennen. Im Ausland in einem gleichwertigen Verfahren anerkannte Anbieter sollen sich jedoch immerhin einem erleichterten Anerkennungsverfahren unterziehen können, um Doppelspurigkeiten zu vermeiden.[832]

526 Im Weiteren sieht Art. 19 E-ZertES in Anlehnung an das THG vor, dass der Bundesrat Abkommen über die Anerkennung ausländischer elektronischer Signaturen, Zertifizierungsdiensteanbieter, ganzer Akkreditierungs- bzw. Anerkennungssysteme, Prüfverfahren u. dgl. schliessen kann.[833] Der Grund dafür, weshalb diese Regelung einem ex-post-Ansatz vorgezogen wurde,[834] liegt darin, dass nur mittels einer staatsvertraglichen Anerkennung für schweizerische Anbieter Gegenrecht verlangt werden kann.[835]

4. Aufsicht

527 Nach erfolgter Anerkennung werden die Zertifizierungsdiensteanbieter gemäss Art. 15 Abs. 1 E-ZertES von den Anerkennungsstellen beaufsichtigt. Die Massnahmen bei Verletzung von Pflichten entsprechen gemäss dieser Bestimmung dem Akkreditierungsrecht; sie gehen bis hin zum Entzug der Anerkennung.[836]

---

829 Hinten N 910 f.

830 Botschaft ZertES, 5694; kritisch KANTON BASEL-STADT, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 59 f.; vgl. auch KPMG, a. a. O., 62 ff.; SWICO, a. a. O., 64; TREUHANDKAMMER, a. a. O., 64 f.

831 Botschaft ZertES, 5693.

832 Botschaft ZertES, 5693; vorne N 313, 316; sehr kritisch JACCARD, Projet, 68 f.

833 Botschaft ZertES, 5702.

834 Vorne N 316.

835 Vorne N 314.

836 Botschaft ZertES, 5700.

5. Pflichten der Anbieter qualifizierter Zertifikate

528 Die Art. 8-13 E-ZertES regeln die grundsätzlichen Pflichten der Zertifizierungsdiensteanbieter. Dazu gehören etwa die korrekte Identifikation des Antragstellers, Informationspflichten gegenüber dem Antragsteller, Dokumentationspflichten, die Ungültigerklärung von Zertifikaten, das Führen von Certificate Revocation List und Certificate Repository, das Setzen von Zeitstempeln[837] und das Vorgehen bei der Einstellung der Geschäftstätigkeit. Teilweise wird der Bundesrat zum Erlass von Ausführungsvorschriften ermächtigt.[838]

529 Art. 14 E-ZertES statuiert zudem die datenschutzrechtliche Besonderheit, dass Personendaten ausschliesslich zur Erfüllung ihrer Aufgaben bearbeitet und nicht gehandelt werden dürfen.[839]

530 Entgegen dem klaren Wortlaut dieser Bestimmungen unterstehen nicht nur anerkannte Zertifizierungsdiensteanbieter diesen Pflichten, sondern *alle Anbieter,* die *qualifizierte Zertifikate* ausstellen. Dies ergibt sich indessen erst aus Art. 16 Abs. 1 E-ZertES, der bestimmt, dass alle Anbieter qualifizierter Zertifikate haftbar seien für die Verletzung der Pflichten *anerkannter* Anbieter.[840] Die Systematik dieser Regelung ist missverständlich und bedarf in der Endfassung des Gesetzes dringend der Korrektur.[841]

6. Beteiligung des Bundes

531 Art. 20 Abs. 3 E-ZertES ermächtigt den Bundesrat, eine Verwaltungseinheit des Bundes zu beauftragen, qualifizierte Zertifikate auch für den Privatrechtsverkehr[842] auszustellen oder sich an einem privaten Zertifizierungsdiensteanbieter zu beteiligen, um den Gesetzeszweck, d.h. die Förderung eines breiten Angebotes an sicheren Diensten zur elektronischen Zertifizierung und der Verwendung qualifizierter elektronischer Signaturen,[843] zu erfüllen. Der Artikel wurde eingefügt, weil nach der Aufgabe von Swisskey unsicher ist, ob sich in nächster Zeit wieder eine private Trägerschaft für einen anerkannten Zertifizierungsdiensteanbieter finden wird.[844]

---

837 Die Formulierung von Art. 12 E-ZertES, wonach auf Begehren des *Signierschlüsselhalters* ein Zeitstempel auszustellen ist, zielt jedoch an der tatsächlichen Interessenlage vorbei; vorne N 198.

838 Eingehender zu den Pflichten Botschaft ZertES, 5696 ff.; JACCARD, Projet, 73 ff.

839 Botschaft ZertES, 5700; Art. 4 Abs. 3 DSG hingegen erlaubt das Bearbeiten von Personendaten zu *jedem* Zweck, vorausgesetzt, dies wird bei der Beschaffung angegeben, ist aus den Umständen ersichtlich oder gesetzlich vorgesehen. Kritisch JACCARD, Projet, 79.

840 Botschaft ZertES, 5700; JACCARD, Projet, 84; anders noch SCHLAURI, Basistechnologie, 98.

841 Kritisch auch JACCARD, Projet, 84 f.

842 Zertifizierungsdienste zum Zwecke des Behördenverkehrs gehören zur *administrativen Hilfstätigkeit*, die (nach allerdings strittiger Auffassung) keiner gesonderten gesetzlichen Grundlage bedarf; Ulrich HÄFELIN/Georg MÜLLER, Grundriss des allgemeinen Verwaltungsrechts, 3. A. Zürich 1998, N 343a m.H.

843 Art. 1 Abs. 2 E-ZertES; vorne N 483 ff.

844 Botschaft ZertES, 5686, 5703; zustimmend JACCARD, Projet, 69; vgl. schon vorne N 256 ff.

D. Qualifizierte Zertifikate

1. Definition und Inhalt

532 Damit eine elektronische Signatur nach Art. 14 Abs. 2bis E-OR materiellrechtlich anerkannt ist, muss sie auf einem *qualifizierten Zertifikat* beruhen.[845] Dieses wird in Art. 2 Bst. d E-ZertES definiert als ein digitales Zertifikat, das die Anforderungen von Art. 7 E-ZertES erfüllt.

533 Art. 7 E-ZertES wiederum entspricht weitestgehend der Regelung von Anhang I der EU-Signaturrichtlinie.[846] Ein qualifiziertes Zertifikat muss nach Abs. 1 mindestens folgende Angaben enthalten *(absolut notwendiger Zertifikatsinhalt):*[847]

- Seriennummer;
- Hinweis, dass es sich um ein qualifiziertes Zertifikat handelt;[848]
- Namen oder Pseudonym des Halters des zertifizierten Prüfschlüssels (auch einer juristischen Person[849]), der im Falle einer Verwechslungsmöglichkeit mit einem unterscheidenden Zusatz zu versehen ist;
- Signaturprüfschlüssel;
- Gültigkeitsdauer des Zertifikats;[850]
- Namen, Niederlassungsstaat und qualifizierte elektronische Signatur des Anbieters.

534 Sofern vorhanden ebenfalls in das Zertifikat aufzunehmen *(bedingt notwendiger Zertifikatsinhalt)* sind:

- spezifische Attribute des Signierschlüsselhalters wie Vertretungsrechte;[851]
- Geltungsbereich des Zertifikats;
- maximaler Transaktionswert.[852]

---

845 Vorne N 516; hinten N 899 ff.

846 Botschaft ZertES, 5695; vorne N 386.

847 Vgl. auch vorne N 100 ff. sowie JACCARD, Projet, 71 ff.

848 Erst mit der Bezeichnung als qualifiziertes Zertifikat gilt ein Zertifikat demnach auch als solches; dies ist unabhängig von den übrigen Voraussetzungen. Mit ihr unterwirft sich der Zertifizierungsdiensteanbieter den Pflichten nach dem ZertES; hinten N 530.

849 Botschaft ZertES, 5696. Auf Pseudonym oder auf eine juristische Person lautende Signaturen sind materiellrechtlich allerdings nicht anerkannt, denn Art. 14 Abs. 2bis E-OR setzt ein qualifiziertes Zertifikat voraus, das auf den *Namen* einer *natürlichen Person* lautet; vgl. hinten N 911 f.

850 Das Festlegen eines Anfangsdatums wäre, obwohl vorgesehen, nicht nötig; vorne N 107, insbesondere FN 144.

851 Der Vertretene hat für einen solchen Eintrag sein Einverständnis zu geben; Art. 8 Abs. 1 E-ZertES; Botschaft ZertES, 5696. Ein derartiges Attribut ist die einzige Möglichkeit, einem Zertifikat Vertretungswirkung für eine juristische Person zu geben, denn ein qualifiziertes Zertifikat, das nicht auf eine natürliche Person lautet, hat nach Art. 7 Abs. 3 E-ZertES explizit keine Vertretungswirkung; kritisch JACCARD, Projet, 72 f. Zu bedauern ist schliesslich, dass die Anwendbarkeit der Bestimmung auf die Vertretung *juristischer* Personen beschränkt wird; so auch JACCARD, a.a.O.

852 Art. 7 Abs. 2 E-ZertES.

535 Zur Wirkung dieser Klauseln vgl. hinten N 762 f. Die Details des Formates regelt der Bundesrat in den Ausführungsbestimmungen.[853]

2. Keine Attributzertifikate

536 Echte Attributzertifikate[854] sind im E-ZertES nicht vorgesehen. Die Botschaft verwendet den Begriff «Attributszertifikat» für den Fall, dass ein Zertifikat nach Art. 7 Abs. 2 Bst. a E-ZertES Informationen über bestimmte Eigenschaften des Signierschlüsselhalters wie Vertretungsrechte u. dgl. enthält.[855] Dabei handelt es sich jedoch um «extensions» des Hauptzertifikats[856] und nicht um echte Attributzertifikate.[857]

E. Erzeugen und Prüfen von Signaturen

1. Signaturerstellungseinheit

537 Art. 6 E-ZertES regelt die grundlegenden Eigenschaften *sicherer Signiereinheiten* (oder *Signaturerstellungseinheiten* wie das Gesetz etwas umständlich sagt) und Signaturprüfeinheiten.[858] Der Einsatz einer sicheren Signiereinheit ist gemäss Art. 14 Abs. 2bis E-OR Voraussetzung für die materiellrechtliche Anerkennung. Dies entspricht Art. 5 Abs. 1 der Signaturrichtlinie.[859]

538 Damit eine Signiereinheit als sicher gilt, muss sie nach Art. 6 Abs. 2 E-ZertES folgendes gewährleisten:

- Der Prüfschlüssel darf praktisch nur einmal auftreten können und seine Geheimhaltung muss hinreichend gewährleistet sein;
- der Prüfschlüssel darf mit hinreichender Sicherheit nicht abgeleitet werden können;
- der Signierschlüssel muss vom Halter vor der Verwendung durch andere verlässlich geschützt werden können;
- die Signatur muss bei Verwendung der jeweils verfügbaren Technologie vor Fälschungen geschützt sein.

---

853 Art. 7 Abs. 4 E-ZertES; schon die Ausführungsbestimmungen der ZertES nehmen dazu auf die X.509-Empfehlung der ITU-T Bezug; dazu vorne N 100 ff.

854 Vorne N 115 f.

855 Botschaft ZertES, 5696.

856 Zum Begriff vorne N 112.

857 Das deutsche Signaturgesetz hingegen sieht echte Attributzertifikate vor; § 7 Abs. 2 SigG 01; vorne N 428.

858 Zu Signier- und Prüfeinheiten vorne N 64 ff.

859 Vorne N 385; hinten N 908.

Die Formulierungen sind eng an Anhang III der EU-Signaturrichtlinie angelehnt[860] und können eigentlich ausschliesslich durch Klasse-3-Kartenleser erfüllt werden, weil nur diese ausreichenden Schutz gewährleisten (Präsentationsproblem).[861] Weil derartige Geräte indessen derzeit jedoch noch keine grösseren Datenmengen signieren können, dürften vorderhand auch Klasse-2-Geräte akzeptiert werden – der Hinweis auf die «jeweils verfügbare Technologie» ermöglicht dies. 539

2. Signaturprüfeinheit

Art. 6 Abs. 3 E-ZertES bestimmt eine Reihe von Voraussetzungen für Signaturprüfeinheiten, wie etwa, dass signierte Daten, Identität des Unterzeichners, Verwendung eines Pseudonyms und Prüfresultat hinsichtlich Gültigkeit des Zertifikats und Datenintegrität zuverlässig angezeigt werden. Die Formulierung entstammt weitgehend Anhang IV der Signaturrichtlinie, der indessen nur empfehlenden Charakter hat.[862] Die Bedeutung dieser Bestimmung dürfte darin liegen, dass die Zertifizierungsdiensteanbieter ihren Kunden entsprechende Empfehlungen abzugeben haben. Auf die Rechtswirkung einer Signatur hat die Prüfeinheit indessen selbstverständlich keinen Einfluss. 540

3. Ausführungsbestimmungen

Nach Art. 6 Abs. 1 E-ZertES regelt der Bundesrat die Erzeugung von Signier- und Prüfschlüsseln sowie Detailvorschriften für das Erzeugen und Prüfen von Signaturen; er hat dabei auf die technische Entwicklung Rücksicht zu nehmen. Angesichts der schnellen technischen Entwicklung ist eine Delegation an die Exekutive sicher sinnvoll.[863] 541

F. Haftung

1. Zertifizierungsdiensteanbieter

a) Allgemeines

Nach Art. 16 E-ZertES haften die Zertifizierungsdiensteanbieter dem Signierschlüsselhalter oder Dritten, die sich auf ein gültiges qualifiziertes Zertifikat verlassen haben für Schäden, die sich aus der Verletzung der durch das Gesetz und die Ausführungsvorschriften statuierten Pflichten ergeben. Eine Haftung besteht damit beispielsweise bei einer mangelhaften Identitätsprüfung bei der Ausstellung von Zertifikaten oder bei der verzögerten Publikation einer Zertifikatssperrung. Die Haf- 542

---

860 Botschaft ZertES, 5695; zur Richtlinie vorne N 387.

861 Kartenleser mit separater Tastatur zur PIN-Eingabe und Anzeige für den zu signierenden Text; eingehend vorne N 55 ff., 64 ff.

862 Botschaft ZertES, 5695.

863 So auch JACCARD, Projet, 70 f.

tungsregelungen des ZertES gehen denjenigen anderer Bundesgesetze als leges speciales vor.[864]

b) Kreis der Haftpflichtigen

543 Der Kreis der Haftpflichtigen wurde bewusst nicht auf anerkannte Anbieter beschränkt, um beispielsweise auch Fälle zu erfassen, in denen ein Anbieter fälschlicherweise eine Anerkennung vorgibt. Haftungsvoraussetzung ist nur die Ausgabe qualifizierter Zertifikate.[865]

c) Milde Kausalhaftung mit Beweislastumkehr

544 Anders als die Regelung der EU-Signaturrichtlinie, die eine Verschuldenshaftung verlangt,[866] statuiert der E-ZertES eine *milde Kausalhaftung*, d.h. eine Haftung bei Pflichtverletzungen, die unabhängig von einem Verschulden eintritt.[867]

545 Nach Art. 16 Abs. 2 E-ZertES trägt der Anbieter die Beweislast für die Erfüllung der Pflichten aus dem E-ZertES und den Ausführungsbestimmungen. Dies erklärt sich aus seiner im Vergleich zu potentiellen Geschädigten besseren Sachkenntnis und der näheren Beziehung zur Sache.[868]

546 Die Norm ist dahingehend zu interpretieren, dass von einem Anbieter nur die *in seinem Einflussbereich* liegenden Massnahmen gefordert werden dürfen.[869] Die Ausführungsbestimmungen geben näheren Aufschluss bei der Bestimmung dieser Massnahmen. Weil die Anbieter nicht für Vorfälle haften, die ausserhalb ihres Einflussbereiches liegen, und weil eine Pflichtverletzung im Sinne des Gesetzes in den allermeisten Fällen mit einem Verschulden einhergeht, nähern sich die Lösungen von Schweiz und EU zumindest sehr stark an.[870]

547 Die Botschaft begründet indessen nicht, weshalb überhaupt von der EU-Regelung abgewichen wird. Aus Gründen der Europa-Kompatibilität wäre eine explizit formulierte Verschuldenshaftung wohl vorzuziehen gewesen.[871]

---

864 Botschaft ZertES, 5686. Für Details zur Haftung der Zertifizierungsdiensteanbieter sei auf die Botschaft ZertES, 5700 ff. sowie auf die erwähnte Dissertation von DÖRR (vorne N 6) verwiesen. Zur Risikoverteilung zwischen Signierschlüsselhalter und auf die Signatur vertrauendem Dritten nach Art. 59a E-OR vgl. hinten N 755 ff.

865 Botschaft ZertES, 5692, 5700 f.; vgl. die Kritik an der irreführenden Systematik vorne N 530.

866 Vorne N 393 ff.

867 Botschaft ZertES, 5701; Bianka S. DÖRR, zit. bei SCHLAURI, Bundesgesetz, 363; RAGGENBASS, B47.

868 Botschaft ZertES, 5701.

869 Botschaft ZertES, 5701; RAGGENBASS, B47; kritisch zur Offenheit der Formulierung JACCARD, Projet, 83.

870 HONSELL, N 23 und SCHWENZER, N 49.08, postulieren gar eine Gleichsetzung von Kausalhaftung mit Entlastungsmöglichkeit und Verschuldenshaftung.

871 Für eine Gefährdungshaftung indessen etwa EMMERT, 248.

d) Haftungsbeschränkungen

548 Die Bestimmungen zur Haftung sind nach Art. 16 Abs. 3 E-ZertES zwingender Natur. Eine Exkulpation bei durch Hilfspersonen verursachten Schäden ist ebenfalls ausgeschlossen, weil damit allenfalls die für Zertifizierungsdiensteanbieter verschärften Haftungsbestimmungen umgangen werden könnten.[872]

2. Anerkennungsstellen

549 Art. 17 E-ZertES statuiert eine Haftung der Anerkennungsstellen bei Pflichtverletzungen analog zu derjenigen für Zertifizierungsdiensteanbieter nach Art. 16 E-ZertES.[873]

3. Verjährung

550 Art. 18 E-ZertES statuiert eine einjährige relative (ab Kenntnisnahme von Schaden und Person des Ersatzpflichtigen) und eine zehnjährige absolute Verjährungsfrist. Vorbehalten bleiben vertragliche Ansprüche. Die Fristen des E-ZertES entstammen dem Deliktsrecht; sollten dessen Fristen später angepasst werden, so soll dies auch beim ZertES geschehen.[874]

G. Sanktionen

551 Im Gegensatz zum Vorentwurf und zur Regelung in § 21 des deutschen SigG 01 verzichtet der Entwurf auf Straf- oder Verwaltungssanktionen. Die Botschaft verweist m. E. zurecht auf die einschlägigen Bestimmungen des Lauterkeitsrechts sowie des THG.[875]

---

872 Zur Beschränkung von Geltungsbereich und maximaler Transaktionssumme in Zertifikaten vgl. vorne N 534 und hinten N 762 f.; für *Deutschland* vgl. schon vorne N 437.

873 Botschaft ZertES, 5702.

874 Botschaft ZertES, 5702.

875 Botschaft ZertES, 5686; Art. 23-30 THG; Art. 23 ff. UWG.

§ 10 Beweisrecht und Haftungsfragen

I. Fragestellung und Vorgehen

552 Wie bereits dargelegt, sind eine Reihe unterschiedlicher Indizien nachzuweisen, damit von der Echtheit einer elektronischen Signatur ausgegangen werden kann.[876] Eine erste Schwierigkeit des Beweises mit elektronisch signierten Dokumenten besteht in der Fülle und Komplexität dieser Voraussetzungen, die im Einzelnen vor Gericht nachzuweisen regelmässig nur mittels eines umfangreichen Sachverständigengutachtens gelingen könnte. Eine zweite Schwierigkeit besteht darin, dass einzelne Elemente der Indizienkette naturgemäss gar nicht zur vollen Überzeugung des Gerichts nachgewiesen werden könnten, sodass der Beweis mittels digitaler Signatur genau besehen vielfach zu scheitern drohte.[877]

553 Digitale Signaturen stellen jedoch die einzige Möglichkeit dar, die Beweisbarkeit elektronischer Kommunikation in offenen Benutzergruppen den Anforderungen an einen überzeugenden Beweis vor Gericht zumindest anzunähern. In Anbetracht des Bedürfnisses nach verbesserter Sicherheit stellt sich daher die Frage, ob es juristische Möglichkeiten gibt, um die problematische Beweissicherheit zu verbessern und um die Komplexität des Beweises mittels digitaler Signaturen zu reduzieren. Das Ziel liegt in der Schaffung eines prozessökonomischen, bezüglich Praxistauglichkeit möglichst der Handunterschrift gleich gestellten Instrumentes.

554 Während Art. 17 Abs. 1 VE-BGES noch eine gesetzliche Echtheitsvermutung für digitale Signaturen statuierte – der *angebliche Unterzeichner* hätte demnach eine Fälschung beweisen müssen – verzichtet der E-ZertES auf eine gesetzliche Regelung für diese Fragen. In der Folge wird daher der Blick auf die Möglichkeit einer richterrechtlichen Lösung gelenkt. Zunächst ist ein vertiefter Blick auf die rechtlichen und logischen Hintergründe der Beweisführung zu werfen.

555 Aus Gründen der kohärenteren Darstellung werden in diesem Paragraphen auch einige Haftungsfragen zwischen Signierschlüsselinhaber und auf die Signatur vertrauendem Dritten angesprochen.

---

876 Vorne N 199 ff.
877 Vorne N 217 ff.

II. Beweisrechtliche Grundlagen

A. Ziel und Gegenstand des Beweises

556 *Ziel des Beweises* ist es, das Gericht von der Wahrheit oder Unwahrheit von Sachbehauptungen zu *überzeugen.*[878] *Gegenstand des Beweises* sind Tatsachen, Erfahrungssätze (d.h. der Erfahrung entspringende Aussagen über Zusammenhänge zwischen Tatsachen[879]) und vereinzelt auch Rechtssätze, die nicht durch die Parteien anerkannt oder bereits gerichtsnotorisch sind.[880]

B. Beweislast

557 Gelingt es nicht, das Gericht von einem Sachverhalt zu überzeugen *(non liquet*[881]*)*, so muss dieses dennoch zu einem Urteil kommen können: Das «non liquet» in der Tatfrage darf nicht zu einem «non liquet» in der Rechtsfrage führen.[882] Wie dies zu geschehen hat, wird durch *Beweislastregeln* bestimmt. Aus ihnen ergibt sich, welche Partei die Folgen der Beweislosigkeit zu tragen hat.[883]

558 Von dieser (*objektiven* oder auch *gesetzlichen*) *Beweislast* ist die *subjektive Beweislast* oder *Beweisführungslast* zu unterscheiden.[884] Sie kann im Laufe des Verfahrens ändern und liegt bei derjenigen Partei, deren Version des Sachverhaltes nach Auffassung des Gerichts in einem bestimmten Prozessstadium nicht erwiesen ist. Der Beweisgegner kann nun insofern Zweifel am vorläufigen Beweisergebnis wecken, als die Überzeugung des Gerichts wieder unter das geforderte Beweismass gedrückt wird.[885]

559 Bei der Verteilung der Beweislast lässt sich der Gesetzgeber grundsätzlich von Billigkeitsüberlegungen leiten, d.h. von materiellrechtlichen Erwägungen.[886] Die Beweislast muss so verteilt werden, «dass das Urteil, falls ein erheblicher Sachumstand beweislos bleibt, den Sachverhalt so unterstellt, dass es, sollte es damit die Wahrheit nicht treffen, derjenigen Partei den Nachteil bringt, für die solches Versagen des Rechtsganges weniger unbillig erscheint.»[887] Entscheidend für die Verteilung sind etwa die typische Nähe einer Partei zum Beweis oder der Grundsatz, dass im Zweifel eher für die Gültigkeit eines Rechtsgeschäfts zu entscheiden ist.[888]

---

878 ROSENBERG/SCHWAB/GOTTWALD, § 113 I; WALDER-RICHLI, § 28 N 1.
879 Eingehend hinten N 567 ff.
880 Statt vieler GULDENER, 318 f.
881 Eigentlich «es fliesst nicht», übertragen «es ist nicht klar.»
882 WASSERMEYER, 2.
883 BK-KUMMER, N 20 zu Art. 8 ZGB; PRÜTTING, 14 ff.
884 Dazu HABSCHEID, N 869 f.; BK-KUMMER, N 31 ff. zu Art. 8 ZGB.
885 KLETT, 1296.
886 BK-KUMMER, N 112 zu Art. 8 ZGB.
887 BK-KUMMER, N 114 zu Art. 8 ZGB.

560 In der Schweiz ist die Beweislast in Art. 8 ZGB sowie in einer Reihe spezieller Vorschriften geregelt.[889] Art. 8 ZGB steht als Generalklausel auf hohem Abstraktionsniveau, sodass eine weitere Konkretisierung notwendig ist.[890] Hierzu sind die anzuwendenden materiellrechtlichen Normen hinsichtlich ihrer systematischen Stellung und ihres Aufbaus zu untersuchen: Jede Partei trägt die Beweislast für diejenigen Tatsachen, welche die Voraussetzungen der Rechtsnorm bilden, die sie zu ihren Gunsten anführt.[891]

561 Verträge über die Beweislastverteilung *(Beweislastverträge)* werden gemeinhin als zulässig betrachtet, sofern sie dispositivrechtliche Bereiche betreffen und nicht gegen Art. 27 ZGB verstossen.[892]

C. Beweismass

1. Allgemeines

562 Unter Beweismass versteht man den Grad an Überzeugung bezüglich der tatbestandsmässigen Voraussetzungen einer Norm, der beim Gericht vorliegen muss, damit die Norm angewandt werden kann. Das Beweismass gibt also an, *wann* der Beweis gelungen ist.[893]

563 Das *Regelbeweismass* – d.h. das Beweismass, das gilt, wenn keine das Beweismass verändernden Spezialnormen anwendbar sind – liegt bei der *vollen Überzeugung* des Gerichts, die keinerlei vernünftige Zweifel mehr zulässt.[894] Die volle Überzeugung ist indessen zu unterscheiden von einem naturwissenschaftlichen Beweis. Würde ein solcher gefordert, so könnte der Beweis nur in den wenigsten Fällen erbracht werden – praktisch jeder Beweis ist daher im Vergleich zu einer exakten, naturwissenschaftlichen Tatsachenfeststellung ein blosser Wahrscheinlichkeitsbeweis.[895]

---

888 BK-KUMMER, N 124f. zu Art. 8 ZGB; etwa zum Nachweis des Verschuldens nach Art. 97 OR BK-WEBER, N 128 zu Art. 99 OR.

889 BK-KUMMER, N 126ff. zu Art. 8 ZGB; KLETT, 1296.

890 Einige Autoren sprechen gar von einer *Leerformel*, so etwa Georges HUGUENIN-DUMITTAN, Behauptungslast, Substantiierungspflicht und Beweislast, Zürcher Studien zum Verfahrensrecht Bd. 53, Zürich, 1980, 122. Nach herrschender Ansicht enthält Art. 8 ZGB jedoch durchaus die Grundsätze der Beweislastverteilung; dazu ZGB-SCHMID, N 38 zu Art. 8 ZGB m.H.

891 BK-GMÜR/HAFTER, N 10 zu Art. 8 ZGB; KLETT, 1296; BK-KUMMER, N 132 zu Art. 8 ZGB; Hans SCHMID, Art. 8: Überblick und Beweislast, in: Christoph LEUENBERGER (Hrsg.), Der Beweis im Zivilprozess, Schriften der Stiftung für die Weiterbildung schweizerischer Richterinnen und Richter SWR Bd. 1, Bern 2000, 11ff., 18f.

892 BGE 85 II 504; HABSCHEID, N 652; VOGEL/SPÜHLER, 10 N 57; a.M. BK-KUMMER, N 373 ff. zu Art. 8 ZGB; für *Deutschland* etwa Sven-Erik HEUN, Die Reduzierung des zivilprozessualen Risikos beim Einsatz digitaler Dokumente durch vertragliche Vereinbarungen, in: Ivo GEIS (Hrsg.), Das digitale Dokument, Eschborn 1995, 81ff.

893 HABSCHEID, N 858; PRÜTTING, 59.

894 BGE 118 II 238 E. 3c, 98 II 242 E. 5.; HABSCHEID, N 858; KLETT, 1294.

895 MEIER, 61.

2. Gesetzliche Reduktion des Beweismasses

564 Vielfach verlangt das Gesetz nur das *Glaubhaftmachen* bestimmter Tatsachen, d.h. das Gericht muss eine mögliche Sachverhaltsvariante in einem gewissen Grade für wahrscheinlicher halten als die anderen; gewisse Zweifel dürfen dabei bestehen bleiben.[896]

565 Mögliche Gründe für eine solche Regelung gibt es viele: So kann etwa bei vorläufigen Entscheiden, die den Sachentscheid nicht präjudizieren, das Interesse an einer beschleunigten Abwicklung höher zu gewichten sein als dasjenige an einer sachlich richtigen Lösung.[897] In einer zweiten Normengruppe bedient sich der Gesetzgeber des Glaubhaftmachens, um typischerweise bei einer Partei auftretende Beweisschwierigkeiten zu korrigieren.[898] Im Weiteren wird blosses Glaubhaftmachen in einer Reihe prozessrechtlicher Normen verlangt,[899] und schliesslich ist das Glaubhaftmachen eines Interesses teilweise Voraussetzung für eine Einsichtnahme in Register.[900]

3. Zulässigkeit einer vertraglichen Beweismassreduktion

566 Eine vertragliche Reduktion des Beweismasses muss m.E. in den Schranken von Art. 27 ZGB und im Rahmen des dispositiven Rechts zulässig sein. Denn wenn eine (bedingungslose) Modifikation der *Beweislast* durch einen Beweislastvertrag zulässig ist,[901] so muss dies m.E. auch für eine Modifikation der *Beweisführungslast* gelten, die unter der Bedingung steht, dass eine Partei einen bestimmten Sachverhalt bloss *glaubhaft* macht.

D. Mittelbarer und unmittelbarer Beweis

1. Begriffe

567 Beweismittel können entweder unmittelbar zu den fraglichen Tatsachen führen oder über Schlüsse, die gestützt auf Erfahrungen über bestimmte Lebensvorgänge gezogen werden; im ersteren Fall spricht man von *unmittelbarem*, im letzteren von *mittelbarem Beweis* oder *Indizienbeweis*.[902] Mittelbare Beweise sind die Regel, und zwar

---

896 Vgl. LEUENBERGER, 118f.; HABSCHEID, N 859.

897 Dies ist beispielsweise bei vorläufigen Massnahmen der Fall, bei denen die drohenden nicht leicht wiedergutzumachenden Nachteile regelmässig nur glaubhaft zu machen sind; MEIER, 71.

898 So kann nach Art. 42 Abs. 2 OR das Gericht die Höhe des nicht ziffernmässig nachweisbaren Schadens auch bloss einschätzen; MEIER, 68; oder in Art. 6 GlG wird zunächst ein Glaubhaftmachen der Geschlechterdiskriminierung verlangt, um hernach die Beweisführungslast für das Fehlen einer Diskriminierung der Gegenpartei aufzuerlegen; KLETT, 1296; GlG-STEIGER-SACKMANN, N 1 zu Art. 6 GlG; vgl. auch hinten N 579ff.

899 Beispiele etwa bei LEUENBERGER, 116f.; vgl. auch MEIER, 71.

900 Diesfalls wird das Geheimhaltungsinteresse offenbar tiefer eingestuft als das Interesse an einem einfachen und raschen Beweis; vgl. LEUENBERGER, 117f.

901 Vorne N 557ff.

schon deshalb, weil sich Gerichte normalerweise mit bereits vergangenen Sachverhalten beschäftigen.[903] So ist etwa ein Urkundenbeweis für den Abschluss eines Vertrages genau besehen bloss ein mittelbarer Beweis für die frühere gegenseitige Willensäusserung der Parteien.

2. Erfahrungssätze und Induktionsschlüsse

568 Der Schluss von einem Indiz auf den zu beweisenden Geschehensablauf erfolgt über einen oder mehrere *Erfahrungssätze*. Solche Erfahrungssätze können *deterministischer oder statistischer Natur* sein.[904]

569 Von einem deterministischen Erfahrungssatz spricht man, wenn dieser für alle zu erwartenden Fälle Geltung hat und damit eine eindeutige Stellungnahme erlaubt,[905] wie etwa die Aussage, dass Wasser bei null Grad Celsius gefriert (Naturgesetz). Selbstverständlich kann ein deterministischer Erfahrungssatz auch fehlerhaft sein; er wird diesfalls durch den Nachweis eines einzigen ihm zuwider laufenden Geschehens widerlegt.[906] Über lange Zeit unwiderlegt, können deterministische Erfahrungssätze jedoch zu ausgesprochen sicheren Schlüssen verhelfen.

570 Statistische Erfahrungssätze hingegen machen nicht eine eindeutige Aussage über *alle* zu erwartenden Fälle, sondern nur über die statistische Verteilung von in der Vergangenheit beobachteten Geschehensabläufen (Wahrscheinlichkeit).[907] So besteht etwa ein statistischer Erfahrungssatz dafür, dass ein Autofahrer, der mit seinem Wagen auf das Trottoir gerät, Verschulden trägt.[908] Zweifellos gibt es Fälle, in denen kein Verschulden besteht, etwa aufgrund einer plötzlichen Bewusstlosigkeit. Auf statistischen Erfahrungssätzen beruhende Schlüsse sind mit der im Erfahrungssatz ausgedrückten Unsicherheit behaftet.

571 Erfahrungssätze machen genau genommen ausschliesslich Aussagen über *bekannte* Tatsachen. Auf Erfahrungssätze gestützte Schlüsse *(Induktionsschlüsse)* sind indessen eigentlich nicht zulässig, denn ein unbekanntes Einzelereignis kann früher gemachten Erfahrungen immer zuwiderlaufen.[909] Dass bei der Beweisführung Induktionsschlüsse aber dennoch zur Anwendung gelangen, liegt daran, dass ein unmittelbarer Beweis für Geschehensabläufe vielfach nicht zu führen ist und ein Beharren darauf oft zu Beweislosigkeit führte.[910] Zu beachten ist indessen, dass ein Induktions-

---

902 Statt vieler HABSCHEID, N 638; MEIER, 65 differenziert nach der Anzahl vorliegender Indizien: Beruht die Überzeugung des Gerichts auf einem einzigen Indiz, so spricht er von einer tatsächlichen Vermutung, sind mehrere Indizien gemeinsame Grundlage der Überzeugung, so handelt es sich um einen eigentlichen Indizienbeweis.

903 Ähnlich ROMMÉ, 11.

904 Zum Ganzen etwa ROMMÉ, 7 ff. oder KOCH/RÜSSMANN, 277 ff.

905 KOCH/RÜSSMANN, 285; ROMMÉ, 13 ff.

906 KOCH/RÜSSMANN, 330 f.; ROMMÉ, 14.

907 KOCH/RÜSSMANN, 287; ROMMÉ, 13 ff.

908 Beispiel bei PRÜTTING, 103; RÜSSMANN, Haftungsfragen, 399 geht etwa von 70-90% Wahrscheinlichkeit aus.

909 Eingehend etwa KOCH/RÜSSMANN, 326 ff.

schluss immer nur zu einer *Hypothese* über einen Geschehensablauf führt und niemals zu dessen sicherem Beweis.[911] Gerade ein auf statistischen Erfahrungssätzen basierender Beweis muss daher bereits durch relativ schwache Indizien, welche die Hypothese als unwahrscheinlich erscheinen lassen, zu widerlegen sein. Mehr kann vom Beweisgegner nicht verlangt werden.[912]

3. Vermutungen

a) Tatsächliche Vermutung

aa) Definition

572 Tatsächliche Vermutungen sind Schlussfolgerungen von bewiesenen auf nicht bewiesene Tatsachen, die das Gericht aufgrund der beschriebenen Erfahrungssätze zieht.[913]

bb) Beweiswürdigung und Beweisführungslast

573 Ob von einer tatsächlichen Vermutung ausgegangen werden kann oder nicht, ist eine Frage der richterlichen Beweiswürdigung.[914] Wird das Vorliegen einer tatsächlichen Vermutung bejaht, so führt dies zu einer Umkehr der Beweisführungslast; am Beweisgegner liegt es dann, die Überzeugung des Gerichts wieder zu erschüttern, indem er weitere Beweismittel vorlegt.[915]

cc) Beweismass

574 Es fragt sich, ob allein in der Berücksichtigung einer tatsächlichen Vermutung bereits eine Reduktion des Beweismasses liegt, was ihre Anwendung ausschliessen würde, wenn das Regelbeweismass gefordert ist.

575 Falls die einem mittelbaren Beweis zugrunde liegenden Erfahrungssätze bestritten und nicht gerichtsnotorisch sind, müssen auch sie bewiesen werden, denn der mittelbare Beweis kann nur gelingen, wenn *beide* ihm zugrundeliegenden Prämissen – Indiz und Erfahrungssatz – überzeugend nachgewiesen sind.

576 Ein mittelbarer Beweis kann damit an verschiedenen Hürden scheitern: Es ist *erstens* möglich, dass ein Indiz selbst nicht mit Sicherheit nachgewiesen ist (etwa eine nur beschränkt Zeugenaussage). *Zweitens* könnte der Nachweis des Erfahrungssatzes nicht überzeugen, und *drittens* ist es (bei statistischen Erfahrungssätzen) möglich, dass die durch den Erfahrungssatz ausgedrückte Wahrscheinlichkeit selbst zu gering ist, als dass dieser die Überzeugung des Gerichts begründen könnte.

---

910 KOCH/RÜSSMANN, 327f.; vorne N 563.
911 KOCH/RÜSSMANN, 328.
912 ROMMÉ, 6 m.H.; ROSENBERG/SCHWAB/GOTTWALD, 664.
913 Ähnlich BK-KUMMER, N 317f., 362 zu Art. 8 ZGB; KLETT, 1296; VOGEL/SPÜHLER, 10 N 50.
914 MEIER, 65; BK-KUMMER N 368 zu Art. 8 ZGB.
915 PRÜTTING, 23 ff.; vgl. auch vorne N 558.

577 Vermögen Indiz und Erfahrungssatz das Gericht im Rahmen der freien richterlichen Beweiswürdigung indessen zu *überzeugen*, so ist gegen ihre Berücksichtigung nichts einzuwenden, denn in der Tatsache, dass das Gericht eine blosse Hypothese über den Sachverhalt zulässt,[916] liegt allein noch keine Reduktion des Beweismasses.[917]

dd) Widerlegung der tatsächlichen Vermutung

578 Eine tatsächliche Vermutung basiert auf Erfahrungssätzen und damit letztlich nur auf einer Hypothese über den Sachverhalt. Diese Hypothese wird durch Tatsachen, die einen anderen Geschehensablauf als wahrscheinlich erscheinen lassen, bereits erschüttert. Ihre Widerlegung erfordert daher nicht den Beweis des Gegenteils, sondern nur ein *Erschüttern* der Hypothese.[918] Anders ist dies indessen bei der sogleich beschriebenen gesetzlichen Vermutung.

b) Gesetzliche Vermutung

aa) Begriff

579 Eine *gesetzliche Vermutung* ist eine Norm, in welcher der Gesetzgeber ein bestimmtes Merkmal (eine Tatsache[919] oder eine Rechtsposition[920]) als bestehend festlegt.[921]

580 Es lassen sich widerlegbare und unwiderlegbare Vermutungen unterscheiden. Letztere werden oft auch als Fiktionen bezeichnet.[922] In der Folge sollen mit dem Begriff der gesetzlichen Vermutung jeweils nur widerlegbare Vermutungen bezeichnet werden.

bb) Ohne Vermutungsbasis

581 Wenn eine gesetzliche Vermutung *keine tatsächliche Vermutungsbasis* aufweist,[923] entspricht sie einer von der Regelbeweislast des Art. 8 ZGB abweichenden Beweislastregel.[924] Teilweise werden derartige Fälle daher gar nicht als Vermutungen bezeichnet.[925]

---

916 N 571.
917 Dazu etwa BK-KUMMER, N 365, 368 zu Art. 8 ZGB; MEIER, 66 f., 71; ROSENBERG/SCHWAB/GOTTWALD, 660 ff., 663.
918 N 571; anders RÜSSMANN, Haftungsfragen, 397.
919 Diesfalls handelt es sich um eine *Tatsachenvermutung;* VOGEL/SPÜHLER, 10 N 46.
920 Diesfalls ist von einer *Rechtsvermutung* die Rede; VOGEL/SPÜHLER, 10 N 47; KLETT, 1296.
921 Vgl. etwa PRÜTTING, 48 m.H.; VOGEL/SPÜHLER, 10 N 45.
922 VOGEL/SPÜHLER, 10 N 49; PRÜTTING, 49, differenziert indessen zwischen unwiderlegbaren Vermutungen und Fiktionen abhängig von der Vorstellung des Gesetzgebers bezüglich der Übereinstimmung von Vermutungsgegenstand und Lebenswirklichkeit.
923 Vgl. etwa die Vermutung des guten Glaubens nach Art. 3 Abs. 1 ZGB.
924 PRÜTTING, 48; GULDENER, 30.
925 GUGGENBÜHL, 14 f.

cc) Glaubhaft zu machende Vermutungsbasis

582 Wird eine tatsächliche Vermutungsbasis verlangt, können entweder über eine reine Beweislastumkehr hinausgehende Zwecke verfolgt werden, oder es kann die harte Wirkung der Beweislastumkehr gemildert werden. So ist beispielsweise nach Art. 6 GlG zuerst eine Geschlechterdiskriminierung glaubhaft zu machen, bevor eine gesetzliche Vermutung dieser Diskriminierung greift. Der Gesetzgeber nimmt dadurch auf der einen Seite der Beweislastumkehr etwas an Härte, und auf der anderen Seite werden von vornherein aussichtslose Fällen frühzeitig abgeblockt.[926]

583 Eine derartige Vermutung setzt das durch sie vom Begünstigten verlangte Beweismass auf ein blosses Glaubhaftmachen herab und ändert den Beweisgegenstand (nur noch die Vermutungsbasis, nicht jedoch der vermutete Sachverhalt ist zu beweisen).[927] Sie hat damit eine *Hebelwirkung*, die es dem Gesetzgeber erlaubt, eine typischerweise schlechte Beweislage zu korrigieren.

dd) Voll zu beweisende Vermutungsbasis

584 Vielfach gilt aber auch für die Vermutungsbasis das volle Beweismass (etwa bei der an den Besitz einer beweglichen Sache anknüpfenden Eigentumsvermutung nach Art. 930 Abs. 1 ZGB). Diesfalls wird nur der Beweisgegenstand geändert, nicht jedoch das Beweismass, worin aber regelmässig noch immer eine Vereinfachung der Beweisführung liegt.[928]

ee) Widerlegung

585 Während die tatsächliche Vermutung auf einer Sachverhaltshypothese basiert und damit durch deren blosses Erschüttern widerlegt werden kann,[929] ist eine gesetzliche Vermutung eine Anweisung an das Gericht, von einer bestimmten Sachverhaltsvariante auszugehen und erst beim *Beweis des Gegenteils* davon abzuweichen.[930]

586 Selbstverständlich ist es auch möglich, die Vermutungs*basis* zu widerlegen *(Gegenbeweis)*.[931]

4. Anscheinsbeweis

a) Ausgangslage

587 Der Eigentümer einer Sache kann deren Diebstahl bei seiner Geltendmachung gegenüber der Diebstahlversicherung typischerweise nicht zur vollen Überzeugung des Gerichts darlegen, denn es wäre ihm beispielsweise immer möglich, die Sache zu

---

926 KLETT, 1297; LEUENBERGER, 115.
927 GUGGENBÜHL, 72 ff.
928 KLETT, 1296; MEIER, 69.
929 Vorne N 571.
930 KLETT, 1296 f.
931 KLETT, 1297.

verstecken oder zu veräussern und danach den Verlust geltend zu machen, ohne dass dies erkennbar wäre. Würde an ihn indessen der Anspruch gestellt, einen geltend gemachten Diebstahl streng zu beweisen, so wäre in den meisten Fällen ein «non liquet» die Folge, und die Versicherung hätte nicht zu bezahlen, womit der Zweck von Diebstahlversicherungsverträgen regelmässig vereitelt würde. Die Gerichtspraxis trägt dieser Situation Rechnung, indem sie auch dann von einem Diebstahl ausgeht, wenn die dürftige Beweislage die volle Überzeugung des Gerichts eigentlich gar nicht zu begründen vermag.[932]

588 Ähnliche Beweisschwierigkeiten und ihre Korrektur durch die Praxis dürften bei der Beurteilung elektronischer Signaturen von einiger Bedeutung sein, weshalb in der Folge genauer auf die einschlägige Kasuistik zum Anscheinsbeweis einzugehen ist.

589 Für die entsprechende Vorgehensweise besteht weder in der Schweiz noch in Deutschland eine einheitliche Terminologie. Es wird von Indizienbeweis, Anscheinsbeweis, prima-facie-Beweis oder auch von tatsächlicher Vermutung gesprochen.[933] Eine anerkannte dogmatische Aufarbeitung fehlt sowohl in Lehre als auch Rechtsprechung.[934]

b) Kasuistik

aa) Schiffskollisions-Fall

590 Ist nachgewiesen, dass ein Schiff an geeigneter Stelle am Ufer eines Flusses verankert war (d.h. so, dass noch eine ausreichend breite Fahrrinne bestehen blieb), so geht die deutsche Praxis im Falle einer Kollision vom Verschulden des Führers eines kollidierenden Schiffes aus, weil erfahrungsgemäss bei einem typischen Geschehensablauf *jedes denkbare* Verhalten des Schiffsführers schuldhaft gewesen wäre.[935] Die Gerichte begnügen sich also damit, dass *irgendein schuldhaftes Verhalten* vorgelegen hat, und es wird auf den schwierigen Nachweis des tatsächlichen Geschehensablaufs verzichtet. Anhand dieses und ähnlicher Fälle wurde der Anscheinsbeweis im deutschen Schifffahrtsprozess aus alten Beweislastregeln entwickelt.[936]

---

932 Vgl. etwa das Urteil des Appellationsgerichts des Kantons Basel-Stadt vom 20. Dezember 1996, BJM 1998, 94 ff.; MEIER, 70 m.H.

933 In einem Urteil vom 22. Dezember 1992 spricht das Bundesgerichtes beispielsweise von einer «im Anscheinsbeweis enthaltenen Vermutung»; ZR 91/92 (1992/93), Nr. 87. In BGE 98 II 243 ist indessen von einem Indizienbeweis die Rede, der der Lebenserfahrung entspricht. In BGE 120 II 248 wiederum spricht das Bundesgericht von einer tatsächlichen Vermutung, die der Beweiserleichterung dient (ähnlich auch BGE 46 II 201 für den Beweis der Unabsichtlichkeit eines Unfalles in einem Versicherungsfalle). Oftmals werden die Begriffe tatsächliche Vermutung und Anscheins- bzw. prima-facie-Beweis auch synonym verwendet; so etwa bei MEIER, 65 ff.

934 BAUMBACH/LAUTERBACH/ALBERS/HARTMANN, Anh § 286 N 15; GREGER, Anscheinsbeweis, 1097 f.; GUGGENBÜHL, 17 f.; MÜLLER, 23.

935 Beispiel bei WASSERMEYER, 15 ff.

936 MÜLLER, 24 m.H.; WASSERMEYER, 15; GREGER, Beweis, 169.

bb) Auffahrunfall-Fall

591 Sehr ähnlich ist die Praxis deutscher Gerichte bei Auffahrunfällen im Strassenverkehr.[937] In der Regel fehlt auch hier die genaue Kenntnis vom Geschehensablauf, weshalb das Verschulden regelmässig nicht nachgewiesen werden könnte, und auch diesfalls stellt das Gericht Überlegungen an, ob nicht den Auffahrenden «nach dem ersten Anschein» ein Verschulden trifft. Dabei hilft der Erfahrungssatz, dass der Fahrer des auffahrenden Fahrzeugs bei Auffahrunfällen typischerweise die im Strassenverkehr erforderliche Sorgfalt unbeachtet liess, also unaufmerksam war, den erforderlichen Abstand nicht einhielt oder zu schnell fuhr. Auch hier wird also bei einer Kollision von *irgendeinem schuldhaften Verhalten* ausgegangen.

cc) Arzthaftpflicht-Fall

592 In BGE 120 II 248 hatte ein Arzt einer Patientin zur Behandlung von Schulterbeschwerden Cortison gespritzt. Durch die Injektion wurde eine schwere Entzündung mit Invaliditätsfolge ausgelöst, was trotz Fehlens konkreter Indizien auf mangelnde Sterilität der Spritze zurückgeführt wurde.

593 Wird durch eine ärztliche Behandlung eine (neue) gesundheitliche Beeinträchtigung verursacht und war die Möglichkeit negativer Auswirkungen der Behandlung erkennbar, so besteht nach BGE 120 II 248 eine *«tatsächliche Vermutung»* dafür, dass nicht alle gebotenen Vorkehren getroffen wurden und somit eine objektive Sorgfaltspflichtverletzung vorliegt. Diese Vermutung dient laut Bundesgericht *«der Beweiserleichterung.»*[938]

dd) Unfallversicherung

594 Der Unfallversicherte, der geltend macht, einen Unfall erlitten zu haben, muss zwar die Unfreiwilligkeit des Vorfalles gegenüber seinem Versicherer beweisen, die volle Überzeugung des Gerichts ist jedoch vielfach mangels Zeugen nicht erreichbar. In diesem Fall kann sich das Gericht mit dem Beweis der anderen Elemente des Unfalles zufrieden geben, also allein mit der *Möglichkeit*, dass der Schaden ohne den Willen des Verletzten entstanden ist. Umgekehrt reicht die alleinige Möglichkeit dann nicht mehr aus, wenn bestimmte Tatsachen nachgewiesen werden, welche an der Unfreiwilligkeit des Vorfalles Zweifel erwecken.[939]

ee) Einschreibebrief-Fall

595 Der Halter eines Lastwagens (Beklagter) war bei einer Versicherung (Klägerin) gegen Haftpflicht versichert, hatte jedoch eine Vierteljahresprämie nicht bezahlt. Nachdem durch den Lastwagen ein Unfall verursacht wurde, behauptete die Klägerin, den

---

937 OLG Hamm, VersR 1972, 1033; OLG Celle, VersR 1974, 496; OLG Düsseldorf VersR 1975, 956f.; vgl. etwa ROMMÉ, 5.

938 Vgl. auch BGE 117 II 256 E. 2b; ZR 88 (1989) Nr. 66.

939 BGE 90 II 233, 45 II 98, 107 II 273; MEIER, 72 ff.

Beklagten einmal mit Einschreibebrief in der gesetzlich vorgeschriebenen Form gemahnt und später ein zweites Mal an die Zahlung erinnert zu haben, worauf aber keine Zahlung eingegangen sei. Zum Zeitpunkt des Unfalles hätte daher kein Versicherungsschutz mehr bestanden. Der Beklagte bestritt den Eingang der Briefe.

596 Die Vorinstanz hatte den Eingang der Briefe *nach dem ersten Anschein* als erwiesen betrachtet, weil der Beklagte seinen Versand hatte beweisen können. Der BGHZ verlangte indessen für den Nachweis des Zugangs den vollen Beweis.[940] Dies zunächst mit dem Argument, nach den Erfahrungen des täglichen Lebens komme es auch unter normalen Verhältnissen immer wieder vor, dass abgeschickte Briefe, auch Einschreiben, den Empfänger nicht erreichten (auf eine Million Sendungen seien 266.3 gemeldete Verluste zu verzeichnen gewesen), weshalb die für die Annahme eines Anscheinsbeweises nötige *Typizität* nicht zu bejahen sei. Im Weiteren würde die Zulassung des Anscheinsbeweises bedeuten, dem Empfänger den in der Regel gar nicht zu führenden Beweis des fehlenden Zuganges aufzuerlegen, was darauf hinausliefe, den Zugang mit der Aufgabe der Sendung gleichzusetzen, was wiederum dem Wortlaut von § 130 BGB widerspräche, der den Zugang voraussetzt. Für ein solches Abweichen vom Gesetzeswortlaut bestünde zudem gar kein Bedürfnis, weil der Absender es in der Hand habe, förmlich zuzustellen oder einen Rückschein zu verlangen. *Der Absender habe demnach genügend Mittel zur Verfügung, den ihm obliegenden Beweis des Zugangs von vornherein sicherzustellen und es sei keineswegs unbillig, ihn das Beweisrisiko tragen zu lassen.*

ff) EFTPOS-Fall

597 Eine Rentnerin hatte ihre EC-Karte noch nie eingesetzt. Nachdem ihr mehrere Karten aus einer Handtasche gestohlen worden waren, wurden während mehrerer Tage Beträge abgehoben, bis die Klägerin – nach Bemerken des Diebstahls – die Karte sperren liess.

598 Das Landgericht Frankfurt a. M. ging von der hinreichenden Sicherheit des eingesetzten Systems aus. Es müsse daher davon ausgegangen werden, dass die Kundin in fahrlässiger Weise ihre PIN preisgegeben habe.[941] Die Bank steht in solchen Fall nach deutschem Recht[942] typischerweise vor der Schwierigkeit, keinen vollen Beweis dafür erbringen zu können, dass die PIN unsorgfältig aufbewahrt wurde. Dies darf indessen nicht dazu führen, dass sich ein Kunde regelmässig mit der einfachen Behauptung, die Karte sei ihm gestohlen worden, aus der Affäre ziehen kann. Deshalb wird der Bank regelmässig ein Anscheinsbeweis für eine unsorgfältige Aufbewahrung der PIN durch den Kunden zugestanden, *sofern der Systembetreiber alle zumutbaren Sicherheitsvorkehren getroffen hat*.[943]

---

940 BGHZ 24, 308 ff.

941 Urteil vom 12. 5. 1999, Aktenzeichen 2/1 S 336/98, abrufbar etwa unter http://www.bonnanwalt.de/entscheidungen/LG-FrankfurtaM2-1S336-98.html; vgl. auch KÖNIG, Anschein, 248.

942 Zur – abweichenden – schweizerischen Rechtslage hinten N 714 ff.

943 Vgl. auch RÜSSMANN, Haftungsfragen, 400.

c) *Dogmatische Einordnung des Anscheinsbeweises*

aa) Fragestellung

In der Folge soll die aufgezeigte Kasuistik zum Anscheinsbeweis auf ihre dogmatischen Grundlagen hin untersucht werden. 599

bb) Beweislasttheorie

Nach der so genannten *Beweislasttheorie* ging vor allem die ältere deutsche Literatur davon aus, dass durch einen zum Anscheinsbeweis tauglichen Erfahrungssatz die Beweislast umgekehrt würde.[944] 600

Beweislastregeln legen fest, wie das Gericht im Falle der Beweislosigkeit («non liquet») zu entscheiden hat.[945] Während eine Beweislastregel die Beweislast jedoch unabhängig vom Nachweis tatsächlicher Voraussetzungen festlegt, ist für das Greifen des Anscheinsbeweises der Nachweis einer «Basis» nötig: So muss etwa im EFT-POS-Fall[946] die Bank zunächst nachweisen, dass tatsächlich eine Transaktion mit der entsprechenden Karte und PIN ausgelöst wurde, und dass ihr System mit den ihr zumutbaren Sicherheitsmechanismen ausgestattet war. Gelingt der Anscheinsbeweis, so entscheidet das Gericht demnach entsprechend den einen Anschein begründenden Beweismitteln, d.h. es liegt kein «non liquet» vor. Gelingt der Entkräftungsbeweis, so liegt wieder ein «non liquet» vor, sodass die ursprünglichen Beweislastregeln greifen.[947] Damit kann es sich nicht um eine Beweislastregel handeln. Gegen eine solche Einordnung spricht ferner, dass der Anscheinsbeweis nach herrschender Rechtsprechung bloss erschüttert zu werden braucht, während eine echte Beweislastumkehr den Beweis des Gegenteils verlangt.[948] 601

Der Anscheinsbeweis hat indessen Einfluss auf die Beweisführungslast[949]: Gelingt er, so verlagert sich die Beweisführungslast in der konkreten Prozesssituation auf die Gegenpartei.[950] Die Einordnung des Anscheinsbeweises als Beweislastregel dürfte damit teilweise auch auf eine unsaubere begriffliche Trennung von Beweislast und Beweisführungslast zurückzuführen sein.[951] 602

---

944 Heute noch so WERNER, 338; zum Ganzen GREGER, Beweis, 171; DERSELBE, Anscheinsbeweis, 1099; PRÜTTING, 95. Ähnlich noch heute auch die schweizerische Rechtsprechung und Literatur zum Arzthaftpflichtrecht; vgl. ZR 88 (1989) Nr. 66 = SJZ 7/1989, 119 ff.; Heinz REY, Ausservertragliches Haftpflichtrecht, 2. A. Zürich 1998, N 655 ff. (der allerdings nicht von Anscheinsbeweis, sondern von *Kausalitätsvermutung* spricht).

945 Vorne N 557 ff.

946 Vorne N 597 f.

947 MÜLLER 29 f.

948 ENGELS, 61 f.; vorne N 585.

949 Zum Begriff N 558.

950 ENGELS, 61, 88.

951 ENGELS, 61; PRÜTTING, 95 f.

cc) «Rechtsbeweis»

603 Nach WASSERMEYER findet im *Schiffskollisions-Fall*[952] ein unmittelbarer Schluss von den Indizien auf das Verschulden statt. Der Beweis des konkreten Handelns des Schiffsführers, welcher aufgrund der Natur der Sache nicht zu erbringen sei, könne damit durch eine Änderung des Beweisgegenstandes umgangen werden.[953] WASSERMEYER spricht von einem *Rechtsbeweis*, der im Gegensatz zum Tatsachenbeweis stehe, weil nicht konkrete Tatsachen zu beweisen seien, sondern nur ein *schuldhaftes Handeln irgendeiner Art*, der Schluss auf das Verschulden also unmittelbar stattfinden könne.[954] Diese Konstruktion erscheint m. E. indessen abwegig, denn das Resultat einer Subsumtion direkt zu beweisen ist unmöglich; beweisbar sind lediglich deren tatsächliche Voraussetzungen.

604 Zuzustimmen ist WASSERMEYER immerhin bezüglich der Unbestimmtheit der unmittelbaren tatsächlichen Voraussetzungen des Verschuldens: *Worin* das schuldhafte Verhalten genau liegt, bleibt im Dunkeln; anerkannt ist nur, dass *irgendein* schuldhaftes Verhalten vorlag. Anders als WASSERMEYER impliziert, reicht es allerdings für einen Vollbeweis bereits aus, wenn das Gericht den Sachverhalt bei der Beweiswürdigung so weit erstellt, als er für die Subsumtion relevant ist. Genau dies geschieht, wenn das Gericht feststellt, dass nach der Würdigung der Beweise keine berechtigten Zweifel mehr daran bestehen, dass *irgendein* schuldhaftes Verhalten vorlag. Darin liegt nun aber nichts anderes als gewöhnliche richterliche Beweiswürdigung gestützt auf eine *tatsächliche Vermutung* [955].

dd) Beweiswürdigung oder Beweismass

605 Nach in der Schweiz und in Deutschland wohl herrschender Lehre und Rechtsprechung wird davon ausgegangen, der Anscheinsbeweis betreffe ausschliesslich die Art und Weise der richterlichen Beweiswürdigung, nicht jedoch das Beweismass.[956] Gerade in der Schweiz ist diese Frage von Bedeutung, denn sie beschlägt die *Überprüfbarkeit durch das Bundesgericht:* Während die Beweiswürdigung Sache der kantonalen Gerichte ist,[957] handelt es sich bei der Frage des Beweismasses um eine solche des Bundesrechts, die auch durch das Bundesgericht überprüfbar ist.[958]

606 Die Einordnung des Anscheinsbeweises als Fall der Beweiswürdigung mag m. E. zwar für den Fall der Schiffskollision Geltung haben – ist das Gericht voll vom Ver-

---

952 Vorne N 590.

953 WASSERMEYER, 5: «Anstelle des für ihn nicht beweisbaren subjektiven Tatbestandes wird dem Kläger gestattet, das Verschulden als solches zu beweisen.»

954 WASSERMEYER, 21.

955 Vorne N 572 ff.

956 BGE 120 II 250 (wo allerdings ungenau von einer tatsächlichen Vermutung gesprochen wird, welche «der Beweiserleichterung diene»; vgl. vorne N 592 f. und sogleich); BK-KUMMER, N 209 zu Art. 8 ZGB; MEIER, 72 ff.; OFTINGER/STARK, § 3 N 35; für *Deutschland* ENGELS, 67; GREGER, Beweis, 172 f.; DERSELBE, Anscheinsbeweis, 1098; MÜLLER, 31; PRÜTTING, 96; WASSERMEYER, 4; vgl. auch Begründung FormanpassungsG, 37.

957 BGE 120 II 250.

schulden des kollidierenden Führers überzeugt, so liegt wie erwähnt eine tatsächliche Vermutung vor.[959] Bereits im Auffahrunfall-Fall handelt es sich indessen offensichtlich um eine Scheinargumentation: Denn nebst den Möglichkeiten, dass der Fahrer unaufmerksam war, den erforderlichen Sicherheitsabstand nicht einhielt oder zu schnell fuhr, sind durchaus weiter Situationen denkbar, die zu einer Kollision führen können.[960] Und wenn im EFTPOS-Fall oder im Einschreibebrief-Fall sogar argumentiert wird, sofern der Beweisführer alle technisch sinnvollen und wirtschaftlich vertretbaren Möglichkeiten ausgeschöpft habe, stünde einem Anscheinsbeweis nichts mehr entgegen,[961] so hat dies endgültig nichts mehr mit der Überzeugung des Gerichts zu tun, denn diese hängt allein davon ab, ob die Massnahmen aus der Sicht des Gerichts tatsächlich zu Sicherheit führen, nicht aber von der Ergreifung der zumutbaren Massnahmen zur Beweissicherung. Gerade hiermit erfolgt offensichtlich eine Abkehr vom Erfordernis der vollen Überzeugung des Gerichts und damit eine *Reduktion des Beweismasses* auf das Darlegen einer *überwiegenden Wahrscheinlichkeit*. Diese auch in der Literatur immer mehr im Vordringen begriffene Auffassung wird gemeinhin als Beweismasstheorie bezeichnet.[962]

607 In ähnlicher Weise wird in der Schweiz regelmässig beim Beweis des natürlichen Kausalzusammenhangs im Haftpflichtrecht argumentiert (teilweise mit expliziter Bezeichnung als prima-facie- oder Anscheinsbeweis).[963] Nach herrschender Lehre muss es *«genügen, wenn Erfolge der fraglichen Art normalerweise von einer Ursache wie der festgestellten bewirkt zu werden pflegen oder wenn umgekehrt Ereignisse wie das zu beurteilende normalerweise Erfolge wie den fraglichen hervorrufen, sodass an andere Ursachen vernünftigerweise wohl nicht zu denken ist.»*[964]

608 Dasselbe gilt, wenn das Bundesgericht im Arzthaftpflicht-Fall von einer *«tatsächlichen Vermutung»* spricht, die *«der Beweiserleichterung»* diene:[965] Entweder wird das Gericht durch die dargelegten Indizien von einem Geschehensablauf überzeugt

---

958 MEIER, 77 mit Hinweis auf BGE 107 II 276. Im Weiteren ist diese Frage in internationalen Sachverhalten relevant: Die Beweiswürdigung erfolgt anhand der lex fori, während das Beweismass anhand der lex causae festgelegt wird; Ivo SCHWANDER, Einführung in das internationale Privatrecht, Erster Band: Allgemeiner Teil, 2. A. St.Gallen 1990, N 628; Max KELLER/Kurt SIEHR, Allgemeine Lehren des internationalen Privatrechts, Zürich 1986, 598 ff.; KOFMEL EHRENZELLER, 839 ff.

959 Die nicht mit einer Beweismassreduktion einhergeht; N 574 ff.

960 Etwa das Eindringen eines Insekts in den Wagen, plötzliches Unwohlsein u. dgl.; RÜSSMANN, Haftungsfragen, 399 geht beispielsweise von einer Fehlerquote von 10-30% aus.

961 Vgl. etwa auch RÜSSMANN, Haftungsfragen, 400.

962 ENGELS, 72 ff., 207 ff.; GREGER, Beweis, 173 f.; DERSELBE, Anscheinsbeweis, 1098 f.; MÜLLER, 30 f.; PRÜTTING, 96; ähnlich ROMMÉ, 135 f.; vgl. auch ROSSNAGEL, Sicherheitsvermutung, 3319.

963 BGE 107 II 273, 430, 113 Ib 424, 115 II 449, 121 III 363, 124 III 165; OFTINGER/STARK, § 3 N 35; VOGEL/SPÜHLER, 10 N 26a; anders MEIER, 73 f., der beim Nachweis der Kausalität keine Reduktion des Beweismasses akzeptieren will, es sei denn, die Beweisschwierigkeiten seien durch Pflichtverletzungen des Schädigers verursacht worden, wodurch erst eine rechtspolitische Lücke angenommen werden könne, die durch eine Beweismassreduktion zu füllen sei.

964 OFTINGER/STARK, § 3 N 35.

965 N 592.

und kann damit im Sinne einer tatsächlichen Vermutung von diesem ausgehen, oder er ist nicht überzeugt, gewährt dem Beweisführer aber eine Beweiserleichterung und reduziert damit das Beweismass, um trotzdem von dessen Sachverhaltsvariante ausgehen zu können.

ee) Materiellrechtliche Theorie

609 In der deutschen Literatur wird ferner zwischen der Beweismasstheorie und einer *materiellrechtlichen Theorie* unterschieden.[966] Die Vertreter der materiellrechtlichen Theorie argumentieren, nur dem materiellen Recht stünde es frei, eine Haftung auch an eine bloss glaubhaft zu machende Grundlage anzuknüpfen, während eine Modifikation der prozessrechtlichen Beweismassnorm nicht in Frage komme, weil Ziel des Zivilprozesses einzig eine richtige Entscheidung sei.[967] Ob diese weitere Differenzierung allerdings sinnvoll ist, ist m. E. fraglich – handelt es sich doch bei der Reduktion des Beweismasses auf blosse Wahrscheinlichkeit unabhängig von dessen systematischer Stellung in der Rechtsordnung um einen prozessualen Aspekt, der – ähnlich wie etwa die Frage der Beweislast[968] – letztlich auf materiellrechtlichen Erwägungen gründet.[969]

ff) Zusammenfassung

610 Der Begriff des Anscheinsbeweises vermischt zwei unterschiedliche Aspekte der Beweisführung. In einer Fallgruppe (Schiffskollisions-Fall und ähnliche) wird das Gericht durch Indizien *voll* davon überzeugt, dass *irgendein* schuldhaftes Verhalten vorliegt. Darin liegt indessen nichts anderes als eine gewöhnliche tatsächliche Vermutung, weshalb der Begriff des Anscheinsbeweises hier zu vermeiden ist. In einer zweiten Gruppe von Entscheidungen (Auffahrunfall-Fall, Diebstahlversicherungs-Fall, Arzthaftpflicht-Fall, Unfallversicherungs-Fall sowie EFTPOS-Fall) befindet sich der Beweisführer in Beweisnot, und das Beweismass wird gesenkt, um ihm den Beweis doch noch zu ermöglichen, weil Sinn und Zweck der anwendbaren Gesetze oder Verträge ohne eine Beweismassreduktion überhaupt nicht erreicht werden könnten. Nur hier ist von Anscheinsbeweis zu sprechen.

d) Voraussetzungen des Anscheinsbeweises

aa) Fragestellung

611 Im Folgenden soll versucht werden, die Voraussetzungen des Anscheinsbeweises abstrakt zu beschreiben.

---

966 GREGER, Beweis, 179 ff.; DERSELBE, Anscheinsbeweis, 1099; ENGELS, 63 ff.; MÜLLER, 32; PRÜTTING, 97.

967 So etwa GREGER, Beweis, 179; DERSELBE, Anscheinsbeweis, 1102 f.

968 Vorne N 557.

969 Darin liegt etwa auch der Grund, weshalb die Fragen des Beweismasses und der Beweislast in internationalen Sachverhalten anhand des in der Sache selbst anwendbaren Rechts (lex causae) und nicht anhand des im übrigen anwendbaren nationalen Zivilprozessrechts (lex fori) zu entscheiden sind; vgl. schon vorne N 605, insbesondere FN 958.

bb) Mangel an Beweismitteln bei beiden Parteien

Vom in Art. 8 ZGB statuierten Regelbeweismass darf das Gericht nur in Ausnahmefällen abweichen.[970] 612

Hat der *Beweisführer* die Mittel, einen Beweis zur vollen Überzeugung des Gerichts zu leisten, so verbietet das prozessrechtliche Ziel einer materiell richtigen Entscheidung eine Reduktion des Beweismasses. 613

Dies ist aber auch dann der Fall, wenn nur der *Beweisgegner* über die nötigen Beweismittel verfügt. Diesfalls ist auf dem Wege der prozessualen Mitwirkung bei der Beweisführung zu verfahren.[971] Wenngleich Anscheinsbeweis und Mitwirkungspflicht letztlich zu sehr änlichen Resultaten führen, liegt doch der Grund des Ersteren im Grundsatz von Treu und Glauben, während der Grund der Letzteren in der anwendbaren materiellrechtlichen Norm liegt.[972] 614

Der Anscheinsbeweis ist demnach nur dann zulässig, wenn *keine der beiden Parteien* über ausreichende Beweismittel verfügt. 615

cc) Vereitelung des Vertrags- bzw. Gesetzeszwecks

Es ist unbilliger, einen Schuldner für eine nicht bestehende Forderung haften, als den Gläubiger einer bestehenden Forderung mangels Beweisbarkeit leer ausgehen zu lassen.[973] 616

Der Anscheinsbeweis stellt eine Ausnahme von diesem Grundsatz dar, die einer Begründung bedarf, die sich aus dem jeweiligen Zweck des Vertrags bzw. des Gesetzes ergeben muss, dessen Voraussetzungen zu beweisen sind. Bei einem *Vertrag* ist zu fragen, ob die Vertragsparteien diesen so abgeschlossen hätten, wenn sie gewusst hätten, dass der Beweis dereinst kaum möglich sein würde. Wird diese Frage verneint, so ist von einer durch den Richter zu füllenden Vertragslücke auszugehen.[974] Setzt der *Gesetzgeber* eine Norm, bei der er davon ausgehen muss, dass regelmässig Beweisschwierigkeiten bestehen (wie etwa Art. 41 OR), so impliziert dies ebenfalls eine Reduktion des Beweismasses und damit eine Ausnahme von der genannten Regel.[975] Damit kann umgekehrt gesagt werden, dass der Anscheinsbeweis nur dann zulässig ist, wenn ein Beharren auf dem vollen Beweismass den Vertrags- oder Gesetzeszweck vereiteln würde. 617

Je nach Auffassung kann der Anscheinsbeweis damit als teleologische Reduktion der Regelbeweismassnorm mit anschliessender Füllung der entstehenden Lücke durch eine richterrechtliche Norm, welche nur ein reduziertes Beweismass fordert oder (bei 618

970 Vgl. etwa BK-KUMMER, N 211 zu Art. 8 ZGB.
971 Vgl. etwa § 50 ZPO ZH; FRANK/STRÄULI/MESSMER, N 1 ff., 3 zu § 50 ZPO ZH.
972 Vgl. sogleich N 616.
973 BK-KUMMER, N 28 zu Art. 8 ZGB.
974 Solche Verträge über das Beweismass sind m. E. zulässig; vorne N 566.
975 Vgl. etwa BK-KUMMER, N 211 zu Art. 8 ZGB.

Fehlen einer solchen Norm bzw. einer expliziten Regelung[976]) als Weiterentwicklung des Richterrechts bezeichnet werden.[977] In beiden Fällen ist indessen nach Art. 1 Abs. 2 ZGB *modo legislatoris* vorzugehen: Es geht nicht an, das zufällige Fehlen von Beweismitteln im Einzelfall durch eine Beweismassreduktion zu kompensieren (Billigkeitsentscheidung im Einzelfall), sondern eine Beweismassreduktion kommt nur dann in Frage, wenn die Beweisschwierigkeiten für die entsprechenden Normen (vertraglicher oder gesetzlicher Natur) *geradezu symptomatisch* sind.[978]

619 Die Figur des Anscheinsbeweises wurde anhand des Kausalitäts- und Verschuldensnachweises entwickelt. Gründe für eine Beschränkung der Anwendung auf dieses Gebiet sind indessen m. E. nicht ersichtlich. Vielmehr muss der Anscheinsbeweis generell zulässig sein, wenn Gesetzes- oder Vertragszweck dies verlangen.

dd) Zumutbare Massnahmen des Beweisführers

620 Der Anscheinsbeweis bleibt ein Eingriff in die Interessen des Beweisgegners, der nur dann gerechtfertigt ist, wenn der Beweisführer die ihm nach Treu und Glauben zumutbaren Massnahmen zur Beweissicherung ergriffen hat.[979] Die Frage nach der Zumutbarkeit der Massnahmen beantwortet sich durch eine Abwägung von Kosten und Nutzen, deren Ergebnis oftmals umstritten sein dürfte.

ee) Beweismass: Überwiegende Wahrscheinlichkeit

621 Sowohl die schweizerische als auch die deutsche Rechtsprechung lassen den Anscheinsbeweis dann zu, wenn ein *typischer Geschehensablauf* vorliegt, bei dem *nach der allgemeinen Lebenserfahrung* regelmässig von einem bestimmten Ereignis auf einen bestimmten Erfolg geschlossen werden kann.[980]

622 Voraussetzung kann jedoch m. E.unmöglich sein, dass eine Situation in dem Sinne *typischerweise* zu Beweisschwierigkeiten einer bestimmten Partei führt, als sie *im täglichen Leben absolut gesehen häufig vorkommt*, denn die absolute Häufigkeit eines Geschehens kann nicht Entscheidend für dessen juristische Beurteilung sein.[981] Der

---

976 Art. 8 ZGB regelt das Beweismass beispielsweise nicht explizit, und es ist umstritten ob er als Rechtsgrundlage des Regelbeweismasses herhalten kann; dazu etwa KOFMEL EHRENZELLER, 819.

977 MEIER, 73 f. spricht von einer rechtspolitischen Lücke (auch unechte Lücke; BK-MEIER-HAYOZ, N 275 ff. zu Art. 1 ZGB; oder Ausnahmelücke; KRAMER, 143 ff.) für den Fall, in denen die Beweisschwierigkeiten auf eine Pflichtverletzung des Schädigers zurückzuführen sind, setzt damit aber wie gezeigt wurde zu viel voraus.

978 Zur Lückenfüllung modo legislatoris BGE 110 III 106, 91 II 106 f., 90 II 442; ZK-BAUMANN/DÜRR/LIEBER/MARTY/SCHNYDER, N 44 der Vorbemerkungen zu Art. 1 und 4 ZGB.

979 So etwa das besprochene Einschreibebrief-Urteil BGHZ 24, 308 ff., 314; vorne N 595 f.; RÜSSMANN, Haftungsfragen, 400; MEIER, 73 f. setzt indessen für eine Beweismassreduktion eine *Pflichtverletzung des Beweisführers* voraus und verlangt etwa auch beim Anscheinsbeweis der Kausalität das volle Beweismass. Dies geht indessen zu weit – würde doch gerade der Kausalitätsnachweis ohne eine Beweismassreduktion zu oft misslingen; vorne N 607.

980 BGE 124 III 165, 121 III 363; für *Deutschland* etwa BGHZ 24, 308 ff., 312.

981 So aber etwa Fritz NICKLISCH, Haftpflichtprobleme der Bio- und Gentechnologie, in: Heinrich HONSELL/Heinz REY (Hrsg.), Symposium Stark, Neuere Entwicklungen im Haftpflichtrecht, Veranstaltet zum 70. Geburtstag von Emil W. Stark, Zürich 1991, 117 ff., 125.

mittels Anscheinsbeweis erschlossene Geschehensablauf soll nur (aber immerhin) insofern typisch sein, als er erfahrungsgemäss *relativ zu anderen möglichen Geschehensabläufen häufiger*, d.h. *überwiegend wahrscheinlich* ist.[982] Derartige Aussagen über Wahrscheinlichkeiten müssen sich indessen nicht zwingend aus der «allgemeinen Lebenserfahrung» (d.h. der Lebenserfahrung eines Durchschnittsmenschen) ergeben, sondern können wie alle anderen Erfahrungssätze[983] auch dem Erfahrungsschatz eines Experten entspringen.

623 Der Grad der Wahrscheinlichkeit des zu beweisenden Sachverhaltes ist zudem gerade nicht allein entscheidend für die Zulassung des Anscheinsbeweises: Eine sehr hohe Wahrscheinlichkeit, welche die Überzeugung des Gerichts um ein Haar zu begründen vermag, reicht zur Begründung eines Anscheinsbeweises etwa dann nicht aus, wenn die beweisbelastete Partei es in der Hand gehabt hätte, mit einfachen Mitteln für eine noch bessere Beweislage zu sorgen.[984] Umgekehrt vermag aber bereits eine Wahrscheinlichkeit von nur 70-90% einen Anscheinsbeweis zu begründen, wenn die Gegenpartei ansonsten den Beweis aufgrund der Natur der Sache gar nie führen könnte und dadurch der Gesetzes- oder Vertragszweck vereitelt würden.[985]

624 Weil dem Anscheinsbeweis damit regelmässig ein zumindest überwiegend wahrscheinlicher Geschehensablauf zu Grunde liegt, kann seine *Widerlegung* nur durch Darlegungen erfolgen, die *zumindest ernsthafte Zweifel* am dargelegten Geschehensablauf wecken.[986] Umgekehrt darf aber auch *nicht der volle Beweis* des Gegenteils verlangt werden; dies wäre nicht einmal dort zulässig, wo das Gericht bei einem indirekten Beweis von einem Geschehensablauf voll überzeugt ist (tatsächliche Vermutung).[987]

ff) Zusammenfassung

625 Gemäss der hier vertretenen Auffassung stellt der Anscheinsbeweis eine Beweismassreduktion dar *(Beweismasstheorie)*. Das Regelbeweismass der vollen Überzeugung des Gerichts ist demnach dann auf eine überwiegende Wahrscheinlichkeit zu reduzieren, wenn die Durchsetzung bestimmter Ansprüche *an einem für die anzuwendenden Normen (vertraglicher oder gesetzlicher Natur) geradezu symptomatischen Mangel an Beweismitteln beider Parteien zu scheitern droht* und dadurch *Gesetzes- bzw. Vertragszweck in Frage gestellt* würde und *der Beweisführer die ihm nach Treu und Glauben zumutbaren Massnahmen zur Beweissicherung getroffen hat*.

---

982 So auch Bernhard M. MAASSEN, Beweismassprobleme im Schadensersatzprozess, Köln/Berlin/Bonn/München 1975, 61.

983 Um nichts anderes handelt es sich; N 568 ff.

984 So im Einschreibebrief-Fall; vorne N 595 f., 620.

985 RÜSSMANN, Haftungsfragen, 395 f., 400.

986 BGH, VersR 1992, 117; 1978, 945; 1971, 642. Vgl. auch BGE 90 II 233: «(…) lorsque des faits sont établis qui permettent de douter du caractère involontaire de l'acte dommageable [es ging um einen Unfall, bei dem der Geschädigte zwei Finger verloren hatte], la simple possibilité d'un événement involontaire ne suffit plus»; vgl. etwa auch KÖNIG, Anschein, 250.

987 Vorne N 578; vgl. auch KÖNIG, Anschein, 250.

626 Die Widerlegung des Anscheinsbeweises muss bereits durch die Darlegung von Tatsachen möglich sein, die *ernsthafte Zweifel* am durch diesen gestützten Geschehensablauf zu wecken vermögen.[988]

E. Urkundenbeweis

1. Begriff der Urkunde

a) Urkundenbeweis im System der Beweismittel

627 Nach der traditionellen Dogmatik sind im Prozess *Augenschein*, *Urkunde*, *Zeugnis*, *Sachverständigengutachten*, *Parteibefragung* und allenfalls *Eid* als Beweismittel zulässig.[989]

628 Mittels eines Augenscheins nimmt das Gericht unmittelbar vom Sachverhalt oder von Indizien Kenntnis. Gegenstand eines Augenscheins kann alles sein, was der Sinneswahrnehmung zugänglich ist (also nicht nur visuell erfassbare Tatsachen, sondern beispielsweise auch akustische Phänomene).[990]

629 Die Urkunde ist ein *Augenscheinsobjekt besonderer Art.* Sie wird in den Prozessgesetzen regelmässig separat vom Augenschein behandelt.[991] Wo genau die Trennlinie zwischen Urkunde und Augenscheinsobjekt liegt, hängt vom anwendbaren Zivilprozessrecht ab und ist kantonal unterschiedlich.[992]

b) Weiter und enger Urkundenbegriff

630 Eine *Urkunde im weiten Sinn* ist ein Gegenstand, die der Aufzeichnung von Gedanken dient (Schriftstücke, Pläne u. dgl.) oder Dinge der Aussenwelt darstellt (Fotografien, Zeichnungen, Datenträger etc.).[993] Einen derart weiten Urkundenbegriff kennen etwa die Kantone Aargau und St. Gallen.[994] In Luzern ist der Urkundenbegriff auf Gegenstände beschränkt, die ohne Hilfsmittel lesbar sind; Fotografien u. dgl. sind damit zugelassen.[995]

---

988 Zur Übertragung dieser Ergebnisse auf den Beweis mit elektronischen Signaturen unten N 673 ff.

989 GULDENER, 328, 330 ff.; HABSCHEID, S. 400 ff.

990 HABSCHEID, N 667 ff.; VOGEL/SPÜHLER, 10 N 145 ff.

991 GULDENER, 332; differenzierter HÜRLIMANN, 41 f.; für *Deutschland* etwa BIZER/HAMMER, 622.

992 Etwa BÜHLER/EDELMANN/KILLER, N 3 zu § 233 ZPO AG; unwesentlich ist m. E., ob das Beweismittel ermöglicht, den zu beweisenden Sachverhalt als gegenwärtigen wahrzunehmen (diesfalls für Augenschein und bei zurückliegendem Sachverhalt für Urkunde Max KUMMER, Grundriss des Zivilprozessrechts, Nach den Prozessordnungen des Kantons Bern und des Bundes, 4. A. Bern 1984, 131 und darauf basierend BJ, Gutachten, 451 [FN 12]), denn Indizien können auf einen vergangenen Sachverhalt hinweisen, ohne dadurch zu Urkunden zu werden.

993 VOGEL/SPÜHLER, 10 N 107; FRANK/STRÄULI/MESSMER, N 2 vor § 183 ZPO ZH.

994 § 233 ZPO AG; BÜHLER/EDELMANN/KILLER, N 1 ff. zu § 233 ZPO AG; Christoph LEUENBERGER/Beatrice UFFER-TOBLER, Kommentar zur Zivilprozessordnung des Kantons St.Gallen, Zivilprozessgesetz vom 20. Dezember 1990, Bern 1999, N 1a f. zu Art. 103 ZPO SG; VOGEL/SPÜHLER, 10 N 107.

995 STUDER/RÜEGG/EIHOLZER, N 1 zu § 149 ZPO LU.

631 Oft beschränken die Kantone den Urkundenbegriff aber auch auf *Schriftstücke, die Gedanken festhalten (enger Urkundenbegriff)*.[996]

632 Eine *Unterschrift* ist in beiden Fällen regelmässig nicht erforderlich,[997] jedoch eine gewisse *Dauerhaftigkeit* der Aufzeichnung.[998]

c) Öffentliche und private Urkunden

633 Im Weiteren wird zwischen *öffentlichen* und *privaten Urkunden (Privaturkunden)* unterschieden. Erstere sind in gesetzlich vorgeschriebener Form durch einen Notar oder eine Behörde kraft ihres Amtes erstellt, letztere sind durch Private ausgestellte Schriftstücke.[999]

d) Zivil- und strafrechtlicher Urkundenbegriff

634 Der *zivilprozessuale Urkundenbegriff* ist schliesslich vom *strafrechtlichen* zu unterscheiden; so ist etwa die Authentifizierbarkeit des Ausstellers zwar Voraussetzung des strafrechtlichen, nicht aber des zivilprozessualen Urkundenbegriffs.[1000]

e) Elektronisch gespeicherte Dokumente insbesondere

635 Schriftlich ist nur ein Text, der in Schriftzeichen auf einem Träger festgehalten wird, wodurch er jederzeit lesbar ist. Eine grammatikalisch Betrachtungsweise spricht daher zunächst gegen eine Anerkennung elektronisch gespeicherter Dokumente als Urkunden, zumindest wenn der vorgängig geschilderte *enge Urkundenbegriff* zur Anwendung kommt, welcher ein *Schriftstück* voraussetzt.[1001]

636 Im Weiteren können elektronische Dokumente mit Leichtigkeit spurlos verändert werden,[1002] was einen Anscheinsbeweis bezüglich Echtheit und Erklärungsabgabe unzulässig macht.[1003] Dies spricht indessen nicht gegen eine Anerkennung als Urkunden, weil auch nicht unterzeichnete Papierdokumente, die aufgrund ihrer leichten Fälschbarkeit zum Anscheinsbeweis ebenfalls nicht zugelassen sind, regelmässig als Urkunden gelten.[1004]

---

996 HÜRLIMANN, 45 ff. In *Deutschland* wird der Begriff der Urkunde regelmässig in diesem Sinne verstanden; vgl. HEUN, 3 m.H.

997 FRANK/STRÄULI/MESSMER, N 1 zu § 185 ZPO ZH; ZR 57 (1958) Nr. 51; zum Sonderfall des provisorischen Rechtsöffnungstitels hinten N 663 ff.

998 SEIDEL, Dokumentenschutz I, 413.

999 GULDENER, 332 f.; HABSCHEID, N 931 f.; eingehend HÜRLIMANN, 55 ff.; zur öffentlichen Beurkundung auch hinten N 828 ff.

1000 Vgl. etwa BRITZ, 100; zum strafrechtlichen Urkundenbegriff etwa STRATENWERTH, § 35.

1001 Vorne N 630 f.; BIZER/HAMMER, 622 f.; GUT/WILDHABER, Abschnitt 2.3.

1002 N 22 ff.

1003 Ähnlich OBERHOLZER, Digitale Signatur, 444.

1004 N 654.

637 Ist die elektronische Einreichung von Dokumenten nicht zulässig,[1005] so sind die Dokumente zunächst auszudrucken. Wo die elektronische Einreichung zugelassen ist, gelten die Dokumente mehrheitlich als Augenscheinsobjekte.[1006]

638 Meines Erachtens spricht zumindest dann nichts für eine Anerkennung elektronischer Dokumente als Urkunden, wenn das Gericht über die für deren Anzeige und Ausdruck nötigen Mittel verfügt oder wenn sich die Möglichkeit bietet, dass die Parteien Hilfe leisten.

2. Beweiskraft unterschriebener Papierurkunden

a) Beweis der Abgabe einer Unterschrift

aa) Unterschriftenfälschung

639 Die Handunterschrift ist das am meisten automatisierte Schreibprodukt des Menschen. Sie widerspiegelt einen individuellen Entwicklungsprozess, der dazu führt, dass kaum zwei Menschen identische Unterschriften führen.[1007]

640 *Schriftvergleichende Gutachten*[1008] werden systematisch anhand eines Katalogs von zu überprüfenden Merkmalen erstellt, um die Nachvollziehbarkeit sicherzustellen. Die Untersuchungsmethoden bestehen nicht nur in einer visuellen Prüfung, sondern u.a. in einer detaillierten Analyse von Strichverlauf, -geschwindigkeit und Druckstärke mittels Stereo- und Rasterelektronenmikroskop.[1009]

641 Die erreichbare Präzision einer gutachterlichen Aussage hängt von einer Reihe von Umständen ab. Zunächst muss ausreichend Vergleichsmaterial aus der Entstehungszeit der fraglichen Unterschrift zur Verfügung stehen, weil sich Unterschriften im Laufe der Zeit verändern. Kurze Unterschriften, Unterschriften in Schul- oder Blockschrift oder gar Kürzel sind sehr viel einfacher zu fälschen als komplexe Gebilde.[1010] Die Erkennungsrate hängt zudem von der normalen Variationsbreite des Unterschreibers ab sowie von allfälligen besonderen Umständen, in denen eine Unterschrift ge-

---

1005 Etwa in den Kantonen Bern, Freiburg, Neuenburg, Solothurn, Wallis und Zug; RÜSSMANN, Herausforderung, 5.2; Botschaft ZertES, 5682.

1006 BRUNNER, 24 ff.; BRITZ, 68 ff.; RIHM, 498 f.; RÜSSMANN, Herausforderung; für Zürich (z.T. Zulassung als Urkunden) FRANK/STRÄULI/MESSMER, N 1 zu § 185 ZPO ZH; vgl. etwa auch Isaak MEIER, Beweisrecht – ein Model Law, AJP 10/1998, 1155 ff., 1160 f. In *Deutschland* sind unsignierte Dokumente nur als Augenscheinsobjekte zum Beweis zugelassen; BRITZ, 25 ff.; BIZER/HAMMER, 621; ERBER-FALLER, 120; HEUN, 3; Sven HÖHNE, Auswirkungen des SigG auf das Internet, 1997, http://www.iri.uni-hannover.de/Seminararbeiten/SigG/index.htm, Abschnitt E. IV. 1; MALZER, 106.

1007 Zum Ganzen MICHEL, 27 ff.; KILGUS, 27 ff.; zur Unterschrift als Legitimationsmittel STEINMANN, 13 f. Die folgenden Aussagen entstammen zum Teil einem Interview mit den Herren LANDERT und OEHNINGER, Schriftexperten am Unterschriftenlabor der Kriminalpolizei des Kantons Zürich.

1008 Zu unterscheiden von *graphologischen Gutachten*, d.h. Gutachten über Charaktereigenschaften eines Schreibers, deren Wert oftmals in Zweifel gezogen wird; MICHEL, 3 ff., 6.

1009 KILGUS, 32 ff.

1010 PORDESCH/NISSEN, 565 f.

leistet wurde (Unterschreiben mit Auflage auf den Knien, an der Wand, Alkoholeinfluss o.ä.), wobei der erfahrene Schriftsachverständige ein Entstehen unter besonderen Umständen von Fälschungsmerkmalen zu unterscheiden weiss. Nicht entscheidend ist, ob eine Unterschrift leserlich ist oder nicht, weil sich die Identifikation meist aus dem Kontext oder aus Vergleichsmaterial herleiten lässt. Entgegen der landläufigen Auffassung ist die Sicherheit schriftvergleichender Gutachten ziemlich hoch. Nur rund 20% der Gutachten können über die Echtheit einer Unterschrift gar keine Aussagen machen.[1011]

642 Anders ist die Sachlage freilich, wenn ein *Laie* in kurzer Zeit über die Echtheit einer Unterschrift entscheiden muss – etwa bei einer Unterschrift zur Identitätsprüfung am Bankschalter.[1012] Immerhin steht auch der Fälscher in solchen Situationen vor grösseren Schwierigkeiten, weil er in Anwesenheit einer anderen Person unterschreiben muss und u.U. die Möglichkeit fehlt, unmittelbar vor dem Leisten der Unterschrift zu üben.[1013] Zudem kommen Hilfsmittel wie Unterschriftenkarten u.dgl. zum Einsatz. Dennoch werden hierbei auch offensichtlich abweichende Unterschriften oftmals als gültig akzeptiert.[1014]

643 Bei der Beurteilung der Sicherheit von Handunterschriften ist demnach zwischen den Perspektiven des Unterschreibenden und des Adressaten einer Unterschrift zu unterscheiden. Während der Unterschreibende kaum damit rechnen muss, eine Fälschung gegen sich gelten lassen zu müssen,[1015] trägt der Adressat der Unterschrift durchaus ein Risiko, Leistungen an einen Unbekannten zu erbringen, ohne vom angeblichen Unterzeichner schadlos gehalten zu werden.[1016]

bb) Urkundenverfälschungen

644 Von der Fälschung der Handunterschrift ist die Verfälschung von Urkunden zu unterscheiden, die zwar eine echte Unterschrift tragen, jedoch durch Löschen von Text, Ausreissen bestimmter Partien, Übermalen u.dgl. verändert wurden. Derartige Verfälschungen können durch Experten normalerweise einfach festgestellt werden.[1017]

1011 Aussage von LANDERT und OEHNINGER (soeben FN 1007); Michael RIESS, Die Bedeutung des schriftvergleichenden Gutachtens in Strafverfahren, Ergebnisse einer empirischen Untersuchung, in: Wolfgang CONRAD/Brigitte STIER (Hrsg.), Grundlagen, Methoden und Ergebnisse der forensischen Schriftuntersuchung, Lübeck 1989, 47ff., 56, kommt auf einen Wert von knapp 30%; vgl. auch PORDESCH/NISSEN, 565.

1012 Dazu etwa STEINMANN, 18ff.; ähnlich auch GUT/WILDHABER, Abschnitt 2.6.1.

1013 MICHEL, 128f.; vgl. auch WEBER, E-Commerce, 322.

1014 MICHEL, 115; PORDESCH/NISSEN, 565.

1015 Die Zahl von 20% nichtliquider Fälle erscheint zwar auf den ersten Blick als hoch. Der Fälscher selbst trägt jedoch ein ausgesprochen hohes Risiko, denn wenn die Echtheit einer Unterschrift bestritten, so wird regelmässig ein Strafverfahren wegen Urkundenfälschung veranlasst, womit die Abschreckungswirkung des Urkundenfälschungstatbestandes ziemlich hoch sein dürfte.

1016 Eine Ausnahme hiervon bilden etwa Fälle, bei denen im Rahmen eines Auftragsverhältnisses eine Authentifikation mittels Unterschrift erfolgt, also etwa im Verhältnis zwischen Bank und Kunde bei Banküberweisungen; dazu eingehend hinten N 714ff.

1017 MICHEL, 157 ff.

645 Steht die Urheberschaft einer Urkunde fest, so wird daher bei unverdächtigen Urkunden üblicherweise davon ausgegangen, dass der ganze Text vom gleichen Urheber stammt. Teilweise statuieren die kantonalen Prozessgesetze sogar eine entsprechende gesetzliche Vermutung.[1018]

cc) Schriftverstellung

646 Gleich wie bei der elektronischen Kommunikation[1019] stellt sich auch bei einer Handunterschrift die Frage der Nichtabstreitbarkeit, d. h. ob der Urheber einer echten Unterschrift diese derart verstellen kann, dass sie für eine Fälschung gehalten wird, sodass er sich im Nachhinein wieder von einer Verpflichtung lösen kann.

647 Die Untersuchung eines Textes auf Schriftverstellung geschieht dadurch, dass man vom Verdächtigen ein Schriftstück mit erneut verstellter Schrift verlangt, das mit dem Originaldokument verglichen wird. Nach MICHEL gelingt Verdächtigen nur selten eine Verfremdung der Schreibleistung, die in einer derartigen Schriftprobe nicht wieder zum Vorschein käme.[1020]

dd) Urkundenbeweis als Anscheinsbeweis

648 Auch Urkunden unterstehen der freien richterlichen Beweiswürdigung.[1021] Bei *öffentlichen* Urkunden wird hierbei gemeinhin von einer tatsächlichen Vermutung der Echtheit ausgegangen. Aber auch die Echtheit unverdächtiger unterzeichneter *Privaturkunden* muss generell glaubhaft bestritten sein, damit es zu einer entsprechenden Beweisabnahme kommt – teilweise wird auch hier von einer tatsächlichen Vermutung gesprochen.[1022] In einigen Kantonen kann der angebliche Aussteller von Privaturkunden zur Niederschrift eines Diktates angehalten werden, worauf sich das Gericht eine Meinung bildet.[1023] In anderen Kantonen wird zur Prüfung der Echtheit von Urkunden ein gesondertes Prüfungsverfahren durchgeführt, zu dem nötigenfalls auch Schriftsachverständige erscheinen.[1024]

649 Richter sind allerdings kaum jemals Schriftexperten, und es finden vielfach auch keine der geschilderten Untersuchungsmethoden Anwendung.[1025] Anders als eine Expertise ist daher die oberflächliche Prüfung einer Privaturkunde durch ein Gericht eigentlich gar nicht geeignet, die für die Annahme einer tatsächliche Vermutung benötigte volle Überzeugung zu begründen. Der Grund, weshalb die Gerichte regelmässig von der Echtheit unverdächtiger Privaturkunden ausgehen, kann damit nicht in der

---

1018 GULDENER, 333.
1019 Vorne N 28 f.
1020 MICHEL, 204.
1021 Anders ist die Situation in *Deutschland*; vorne N 454 ff.
1022 BK-KUMMER, N 39 zu Art. 9 ZGB; BÜHLER, 79. Teilweise wird die Echtheit öffentlicher Urkunden durch die kantonalen Zivilprozessgesetze auch gesetzlich vermutet; GULDENER, 333; VOGEL/SPÜHLER, 10 N 113.
1023 Vgl. etwa § 187 ZPO ZH.
1024 Art. 273 ZPO GE; HABSCHEID, N 683.
1025 Vorne N 640.

hohen Beweiskraft der Urkunde liegen. Er liegt genau besehen vielmehr darin, dass ein regelmässiges Bestehen auf Schriftgutachten die Tauglichkeit von Privaturkunden als einfach handzuhabende Beweismittel massiv einschränken würde; dies gilt insbesondere für das Rechtsöffnungsverfahren, welches andernfalls durch das blosse Behaupten einer Fälschung regelmässig vereitelt werden könnte.[1026]

650 Geht man bei unverdächtigen Privaturkunden ohne ein Schriftgutachten von der Echtheit aus, so liegt darin also eine Reduktion des Beweismasses. Der Urkundenbeweis ist m.E. folglich nichts anderes ist als ein althergebrachter Fall des geschilderten Anscheinsbeweises mit der Besonderheit, dass die Begründung für die Reduktion des Beweismasses für einmal nicht im materiellen Recht, sondern im Prozessrecht zu suchen ist, wobei die Schlechterstellung der eigentlich nicht beweisbelasteten Partei zugunsten einer prozessökonomischen einfachen Beweisführung in Kauf genommen wird.

b) Beweis der Rekognition

651 Kann die Unterschrift auf einer Privaturkunde als echt gelten, so gehen Lehre und Praxis regelmässig von der Anerkennung (Rekognition) des darüber stehenden Textes aus. Abweichend zu beurteilen sind einzig Fälle, in denen ein Dokumentenaustausch bloss zu Informationszwecken stattfindet, also Wissens- und nicht Willenserklärungen abgegeben werden. Dies dürfte jedoch meist bereits aus den Umständen klar ersichtlich sein.[1027]

652 Bei der Beurteilung der Rekognition ist m.E. das Vertrauensprinzip[1028] von Bedeutung: Wer einen Text unterschreibt, signalisiert nach allgemeiner Verkehrssitte dessen Übereinstimmung mit seinem Willen. Umgekehrt kann und muss der Empfänger eines unterzeichneten Textes nach Treu und Glauben davon ausgehen, dass dieser dem Willen des Unterzeichners entspricht. Bestreitet der Unterzeichner die Rekognition, so hat er in erster Linie zu beweisen, dass der Empfänger bezüglich der Rekognitionsabsicht des Unterzeichners bösgläubig war; die Frage, ob eine tatsächliche Vermutung für die Rekognition spricht, verliert vor diesem Hintergrund an Bedeutung.

653 Wird eine Willenserklärung *zwischen Abwesenden* geäussert, so setzt die Rekognition noch die *Begebung* (d.h. das willentliche Inverkehrsetzen des Schriftstücks durch den Aussteller) voraus. Befindet sich eine Urkunde im Umlauf, so muss für die Begebung indessen auch der Anscheinsbeweis zulässig sein, will man nicht die Beweiseignung der Urkunde zunichte machen.[1029]

1026 Hinten N 663 ff.

1027 ZK-SCHÖNENBERGER/JÄGGI, N 37 zu Art. 13 OR; BK-KRAMER/SCHMIDLIN, N 12 der allgemeinen Erläuterungen zu Art. 12-15 OR; eingehend zur Rekognition hinten N 836 ff.

1028 Zum Vertrauensprinzip etwa GAUCH/SCHLUEP/SCHMID, N 206 ff.

1029 Vgl. schon vorne N 648 ff.

3. Beweiskraft nicht unterzeichneter Urkunden

a) *Nicht unterzeichnete Papierdokumente*

654 *Nicht unterzeichnete Urkunden* und damit auch *Computerausdrucke*[1030] sind zwar zum Urkundenbeweis zugelassen, von einem Anscheinsbeweis der Echtheit kann indessen mangels Unterschrift nicht ausgegangen werden.[1031]

b) *Kopien und Scans*

655 Die Praxis lässt auch *unbeglaubigte Kopien* regelmässig zum Urkundenbeweis zu.[1032] Weil indessen keine zuverlässige Möglichkeit besteht, eine kopierte Unterschrift zu überprüfen (die geschilderten Untersuchungsverfahren[1033] können nur auf das Original angewendet werden), ist die Beweiskraft von Kopien ähnlich niedrig wie diejenige nicht unterzeichneter Dokumente.[1034] In einigen Zivilprozessordnungen ist daher explizit vorgesehen, dass das Gericht die Vorlage des Originals verlangen kann.[1035] Gleich sind auch elektronische Kopien (Scans) zu behandeln; ob sie elektronisch eingereicht werden können oder auszudrucken sind, hängt vom kantonalen Recht ab.[1036]

656 Die *Beglaubigung* einer Kopie nimmt die Prüfung des Originals auf Unverdächtigkeit hin vorweg (die Urkundsperson hat, sofern sie die Beglaubigung überhaupt vornimmt, Verdachtsmomente in der Beglaubigungsurkunde aufzuführen[1037]), sodass beglaubigte Kopien hinsichtlich Beweiskraft die gleiche Wirkung wie das Original aufweisen.[1038]

c) *Telefax*

657 Telefaxausdrucke sind als Papierdokumente regelmässig zum Urkundenbeweis zugelassen.[1039] Bei der Beweiswürdigung ist jedoch gleich wie bei Kopien darauf

---

1030 Je nach Urkundenbegriff ist zudem nötig, dass Computerausdrucke menschliche Gedanken enthalten; BIZER/HAMMER, 623; vgl. auch vorne N 630 ff.

1031 In *Deutschland* gelten Computerausdrucke ebenfalls als Urkunden, die gesetzlichen Beweisregeln (vorne N 454 f.) kommen jedoch nicht zur Anwendung; BIZER/HAMMER, 623; SEIDEL, Dokumentenschutz I, 412.

1032 Etwa FRANK/STRÄULI/MESSMER, N 1 zu § 185 ZPO ZH.

1033 Vorne N 640.

1034 Vorne N 640; Gisela BEKEDORF/Manfred HECKER, Grundlagen und Probleme der Begutachtung von Nicht-Originalen, in: Wolfgang CONRAD/Brigitte STIER (Hrsg.), Grundlagen, Methoden und Ergebnisse der forensischen Schriftuntersuchung, Lübeck 1989, 247 ff., 268; FRANK/STRÄULI/MESSMER, N 1 zu § 185 ZPO ZH; problematisch ist demnach das Urteil des OGer LU, LGVE 1986 I 18, in dem glaubhaftes Bestreiten auch bei einer Fotokopie verlangt wurde (dies würde voraussetzen, dass auch die Photokopie eine gewisse Beweiskraft aufweist); unkritisch dazu STUDER/RÜEGG/EIHOLZER, N 1 zu § 151 ZPO LU.

1035 Etwa § 185 Abs. ZPO ZH.

1036 Hinten N 635 ff.

1037 BRÜCKNER, N 3393.

1038 SchKG-STAEHELIN, N 17 zu Art. 82 SchKG; anders HÜRLIMANN, 85.

1039 Anders für *Deutschland* HEUN, 5.

Rücksicht zu nehmen, dass ein solcher Ausdruck kaum Sicherheit liefern kann.[1040] Dies gilt erst recht für Computerfaxe, d.h. Faxübermittlungen, bei denen als Endgeräte nicht Faxgeräte sondern Computer mit Modems zum Einsatz kommen.[1041]

d) Elektronisch gespeicherte Dokumente

658 Die Beweiskraft elektronischer Dokumente ist aufgrund ihrer einfachen Manipulierbarkeit minim.[1042] Der Anscheinsbeweis für ihre Echtheit ist damit unzulässig.

e) Aufzeichnungen von Geschäftsbüchern

659 *Aufzeichnungen von Geschäftsbüchern u. dgl. auf Bild- und Datenträgern* haben nach Art. 962 Abs. 4 OR die gleiche Beweiskraft wie die ihnen zugrundeliegenden Originale. Hierbei handelt es sich um eine gesetzliche Beweisregel, die durch die besonderen Vorschriften über die Aufbewahrung derartiger Dokumente gerechtfertigt wird.[1043]

f) Zusammenfassung

660 Nicht unterzeichnete Dokumente sind mangels Zulässigkeit des Anscheinsbeweises für ihre Echtheit für sich allein nicht zum Beweis tauglich; sie erhalten ihre Beweiskraft vielmehr ausschliesslich im Zusammenspiel mit anderen Indizien. So kann etwa die Tatsache, dass die sich auf ein Dokument stützende Partei von einem prozessualen Vorgehen bis zur Beweiserhebung keine Kenntnis hatte, für die Integrität eines Dokumentes sprechen, weil es für sie bis dahin keinen Anlass gab, das Dokument zu verfälschen.[1044]

661 Demnach dürften oftmals vorsorgliche Beweissicherungsmassnahmen nötig sein – gerade elektronisch gespeicherte Dokumente der Gegenpartei sind aufgrund ihrer einfachen Manipulierbarkeit tendenziell als gefährdet zu betrachten.[1045] Schweizerische Gerichte üben allerdings grosse Zurückhaltung bei der Anordnung solcher Massnahmen.[1046] Zudem ist teilweise kein Zwangsvollzug vorgesehen; es kann also keine Beschlagnahme durch staatliche Organe erfolgen, sondern nur eine Aufforderung zur Herausgabe an die Gegenpartei, die danach möglicherweise noch Zeit für Manipulationen hat.[1047] Damit ist es oftmals schwierig, mittels unsignierter elektronisch gespeicherter Dokumente einen sicheren Beweis zu führen.

1040 HEUN, 4f.; HUNGER, 99f.; Klaus-J. MELLULIS, Zum Regelungsbedarf bei der elektronischen Willenserklärung, MDR 1/1994, 110f.; Siegfried STREITZ, Telefaxtechnik, CR 1/1995, 55ff.; STEINMANN, 22ff.

1041 Dazu etwa HEUN, 2ff.

1042 Vorne N 19ff.

1043 HABSCHEID, N 932; vgl. auch Art. 43 MWSTG und dazu die Literaturhinweise in FN 4.

1044 So etwa auch FREI, N 320.

1045 Eingehend RIHM, 503.

1046 Es gilt in erster Linie, die unbegründete Ausforschung der Gegenpartei zu verhindern; RIHM, 503.

1047 Für Zürich ZR 77 (1978) Nr. 50, S. 142f. Manipulationen können mit Hilfe von Informatikmitteln in sehr kurzer Zeit vorgenommen werden; vgl. etwa RIHM, 503.

4. Privilegierung der Urkunde als Beweismittel

a) *Allgemeines*

662 Aufgrund ihrer einfachen Handhabung und der ihr eigenen besonderen Ausdrucksmöglichkeiten ist die Urkunde ein effektives und sicheres Beweismittel. Im Verfahrensrecht erhält sie daher gegenüber den anderen Beweismitteln teilweise eine privilegierte Stellung.[1048] Insbesondere bei Entscheiden provisorischer Natur[1049] oder solchen mit geringem Streitwert (ausschliessliche Zuständigkeit des Friedensrichters)[1050] sind oft nur Urkunden als Beweismittel zulässig.

b) *Provisorische Rechtsöffnung insbesondere*

663 Nach Art. 82 SchKG wird *provisorische Rechtsöffnung* gewährt, wenn die Forderung auf einer durch öffentliche Urkunde festgestellten oder *durch Unterschrift bekräftigten Schuldanerkennung* beruht und der Schuldner nicht durch Urkunden deren Entkräftung glaubhaft macht. Nur der durch derartige Titel und das Fehlen von Belegen für deren Entkräftung geschaffene Anschein für das Bestehen der Schuld rechtfertigt die durch die Rechtsöffnung geschaffene Besserstellung des Gläubigers (bedingte Vollstreckbarkeit der Forderung).[1051] Der blosse Anschein reicht hingegen bereits aus, weil der Schuldner die Forderung weiterhin durch Aberkennungsklage gerichtlich überprüfen lassen kann, der Entscheid also provisorischer Natur ist.[1052] Dies dürfte auch der Grund dafür sein, dass Rechtsprechung und Lehre bei der provisorischen Rechtsöffnung regelmässig explizit von einer «tatsächlichen Vermutung»[1053] der Echtheit ausgehen, während dies beim normalen Urkundenbeweis teilweise unterbleibt.[1054]

664 Eine vergleichbare Lage besteht, wenn der Schuldner die *Kopie* einer Schuldanerkennung vor Gericht *anerkennt;* von einer solchen Anerkennung wird teilweise schon ausgegangen, wenn der Schuldner deren Echtheit nicht substanziiert bestreitet.[1055]

1048 BJ, Gutachten, 450 f.; BIZER/HAMMER, 620 f.

1049 Provisorische Rechtsöffnung nach Art. 82 SchKG (dazu sogleich N 663 ff.); gerichtliche Aufhebung oder Einstellung der Betreibung nach Art. 85 SchKG; für *Deutschland* § 592 ff. ZPO (Urkundenprozess) und dazu etwa ZÖLLER-GREGER, N 1 ff. vor § 592 ZPO.

1050 VOGEL/SPÜHLER, 12 N 17.

1051 Details bei AMONN/GASSER, § 19 N 5 ff., 64 ff.

1052 AMONN/GASSER, § 19 N 66 f.

1053 Wie beschrieben handelt es sich genau besehen um einen Anscheinsbeweis; vorne N 648.

1054 Vgl. insbesondere Urteil des Kantonsgerichtes FR vom 3. Februar 1947, SJZ 1949, 240 f.; vgl. auch Urteil des OGer BL vom 21. April 1988 i.S. Bank X. gegen P., BJM 1989, 256 ff., 257 f.; Urteil des OGer BL vom 27. Februar 1979 i.S. I. und L. gegen E.V., BlSchK 1985, 97 ff., 98; AMONN/GASSER, § 19 N 74; Ernst BLUMENSTEIN, Handbuch des schweizerischen Schuldbetreibungsrechtes, Bern 1911, 302 FN 20; Carl JAEGER/Hans Ulrich WALDER/Thomas M. KULL/Martin KOTTMANN, Bundesgesetz über Schuldbetreibung und Konkurs, Erläutert für den praktischen Gebrauch, 4. A. Zürich 1997, N 8 zu Art. 82 SchKG; André PANCHAUD/Marcel CAPREZ, Die Rechtsöffnung, La mainlevée d'opposition, Zürich 1980, § 4 N 1; SchKG-STAEHELIN, N 13 zu Art. 82.

1055 SchKG-STAEHELIN, N 17 zu Art. 82 SchKG m.H. Die Anerkennung der Schuldanerkennung ist von der Schuldanerkennung selbst zu unterscheiden – der Schuldner könnte die Schuldanerkennung anerkennen und hernach durch Urkunden deren Entkräftung nachweisen.

Weil zwischen Kopien unterzeichneter Dokumente und gar nicht unterzeichneten Dokumenten hinsichtlich der Beweiskraft genau besehen kein Unterschied besteht,[1056] müssten m.E. auch nicht unterzeichnete Dokumente als Rechtsöffnungstitel zulässig sein, sofern der Schuldner diese anerkennt.[1057] 665

Unsignierte *elektronisch gespeicherte* Dokumente sind als provisorische Rechtsöffnungstitel mangels Unterschrift grundsätzlich untauglich.[1058] Lässt aber das kantonale Recht elektronisch gespeicherte Dokumente zum Urkundenbeweis[1059] und unsignierte Papierdokumente als Rechtsöffnungstitel zu, sofern sie durch den Schuldner anerkannt werden, so muss m.E. auch die Zulassung (anerkannter) elektronisch eingereichter Dokumente möglich sein. 666

III. Beweisrecht und Haftungsfragen elektronisch signierter Dokumente

A. Echtheit

1. Allgemeines

a) Problemstellung

Wie beschrieben stellen sich beim Beweis mit elektronisch signierten Dokumenten zwei Hauptschwierigkeiten: Einerseits sind Teile der Indizienkette naturgemäss gar nicht zur vollen Überzeugung des Gerichts nachzuweisen, und andererseits ist dieser Beweis ausgesprochen komplex und kann durch ein Gericht ohne Hilfe Sachverständiger nicht durchgeführt werden.[1060] Zur Lösung des ersten Problems soll zunächst die geschilderte Praxis zum Anscheinsbeweis auf elektronische Signaturen zu übertragen versucht werden. Zur Lösung des zweiten Problems soll in der Folge untersucht werden, ob durch die im E-ZertES vorgesehene ex-ante-Prüfung für Zertifizierungsdiensteanbieter Abhilfe geschaffen werden kann. 667

Aus Gründen der kohärenteren Darstellung werden einige zwischen Signierschlüsselhalter und auf die Signatur vertrauendem Dritten bestehenden Haftungsfragen ebenfalls in diesem Paragraphen behandelt. 668

Auf die eher praktische Frage, ob eine Signatur durch das Gericht selbst oder mittels Gutachten zu überprüfen ist, sowie auf die Frage, ob elektronisch signierte Doku- 669

1056 Vorne N 655.
1057 A.M. SchKG-STAEHELIN, N 17 zu Art. 82 SchKG.
1058 SchKG-STAEHELIN, N 14 zu Art. 82 SchKG; GASSER, 92.
1059 Vorne N 637.
1060 N 217ff.

mente zum Urkundenbeweis zuzulassen sind (prozessuale Anerkennung), wird gesondert in § 11 eingegangen.

b) Fallgruppen

670 Das ZertES wird *vertragliche Regelungen* über den Einsatz elektronischer Signaturen nur am Rande berühren, weil die Parteiautonomie zur Auswahl des Signaturverfahrens gewahrt bleiben soll.[1061] Es soll daher eine Differenzierung zwischen der Situation in offenen Benutzergruppen (ohne Rahmenvertrag über die Wirkungen der Signatur) und geschlossenen Benutzergruppen (mit solchem Rahmenvertrag) vorgenommen werden. Im Weiteren ist zwischen Signaturen mit und ohne ex-ante-Prüfung zu unterscheiden. Demnach sind vier Fallgruppen zu untersuchen: Fallgruppe 1 mit Signaturen *ohne* ex-ante-Prüfung in *offenen* Benutzergruppen, Fallgruppe 2 mit Signaturen *ohne* ex-ante-Prüfung in *geschlossenen* Benutzergruppen, Fallgruppe 3 mit Signaturen *mit* ex-ante-Prüfung in *offenen* Benutzergruppen und Fallgruppe 4 mit Signaturen *mit* ex-ante-Prüfung in *geschlossenen* Benutzergruppen.

671 Zu beachten ist, dass die Fallgruppen ohne ex-ante-Prüfung sowohl qualifizierte elektronische Signaturen im Sinne des ZertES als auch andere Signaturen umfassen.[1062]

c) Darzulegende Indizienkette

672 Wie bereits beschrieben sind für den Beweis der Echtheit eines elektronisch signierten Dokumentes folgende Zusammenhänge nachzuweisen:[1063]

- Signierschlüssel – Prüfschlüssel (kryptographische Sicherheit);
- Prüfschlüssel – Name (sichere Zertifizierung);
- Name – Schlüsselhalter (Identifikation des Schlüsselhalters);
- Schlüsselhalter – Unterzeichner (alleinige Kontrolle des Signierschlüssels durch den Halter zum Signierzeitpunkt);
- Unterzeichner – Dokument (korrekte Präsentation des Dokuments);
- Dokument – Signatur (kryptographische Sicherheit).

2. Anscheinsbeweis für elektronische Signaturen

a) Voraussetzungen des Anscheinsbeweises

673 Der Anscheinsbeweis ist dann zulässig, wenn die Durchsetzung bestimmter Ansprüche *an einem für die anwendbaren Normen (vertraglicher oder gesetzlicher Natur) geradezu symptomatischen Mangel an Beweismitteln beider Parteien zu scheitern*

1061 Prinzip der freiwilligen Anerkennung der Zertifizierungsdiensteanbieter; vorne N 286, 512.

1062 Nach dem Prinzip der freiwilligen Anerkennung der Zertifizierungsdiensteanbieter sind auch nicht anerkannte Anbieter frei, qualifizierte Zertifikate auszustellen; vorne N 286, 512.

1063 Eingehend vorne N 199 ff.

droht und dadurch der Gesetzes- bzw. Vertragszweck in Frage gestellt würde und *der Beweisführer die ihm zumutbaren Massnahmen zur Beweissicherung getroffen hat*. Zudem muss die zu beweisende Tatsache zumindest überwiegend wahrscheinlich sein.[1064]

b) Symptomatischer Mangel an Beweismitteln

674 Der Beweis der alleinigen Kontrolle des Schlüsselhalters über seinen Schlüssel ist, wie bereits dargelegt, aus verschiedenen Gründen nicht zur vollen Überzeugung des Gerichts zu erbringen. Eine Schwierigkeit besteht darin, das zur Aktivierung des Signierschlüssels benötigte Passwort auszuspähen.[1065] Dies dürfte jedoch mit dem Aufkommen sicherer und ökonomisch sinnvoll einzusetzender biometrischer Authentifizierungsmechanismen in einigen Jahren zu bewältigen sein.[1066] Wohl noch für längere Zeit ökonomisch nicht sinnvoll lösbar bleibt hingegen das Präsentationsproblem; um dieses zu beheben, wäre ein «Klasse-3-Kartenleser» nötig, der mit komplexen Dokumentenformaten zu Rande kommen muss; solche Geräte sind auf absehbare Zeit noch nicht verfügbar.[1067] Schliesslich muss das Gericht auf die korrekte Arbeitsweise des Zertifizierungsdiensteanbieters vertrauen. Obwohl dieses Vertrauen teilweise durch organisatorische Massnahmen wie Protokollierung, Ausbildung, Kontrolle des Personals u.dgl. verbessert werden kann, dürfte die volle Überzeugung, dass auch in Einzelfällen keine Fehler passiert sind, unter Umständen nicht zu begründen sein. Dem auf die Signatur vertrauenden Dritten dürfte es daher kaum möglich sein, das Gericht von deren Echtheit voll zu überzeugen.

675 Umgekehrt wäre es aber auch für den angeblichen Unterzeichner beinahe unmöglich, das Gericht von einer Fälschung zu überzeugen, würde man die Beweisführunglast ihm übertragen.[1068] Es ist damit auch ausgeschlossen, die Beweissituation auf dem Wege einer prozessualen Mitwirkungspflicht des angeblichen Unterzeichners zu verbessern.[1069] Dieser Mangel an überzeugenden Beweismitteln ist in beiden Fällen symptomatisch für den Beweis mit elektronischen Signaturen.

676 Die Voraussetzung des symptomatischen Mangels an Beweismitteln ist demnach erfüllt.

c) Vereitelung des Gesetzes- bzw. Vertragszwecks

677 Zweck des ZertES soll unter anderem sein, die Verwendung qualifizierter elektronischer Signaturen zu begünstigen, dies wiederum mit dem Ziel, zuverlässige Grundlagen für sicheren elektronischen Geschäftsverkehr zu schaffen.[1070] Beharrte man

---

1064 Vorne N 611 ff.
1065 Vorne N 208 ff., 218.
1066 Vorne N 70 ff., 211.
1067 Vorne N 55 ff., 212.
1068 Eingehend hinten N 850 ff.
1069 Zur prozessualen Mitwirkungspflicht schon vorne N 614.

aber auf dem vollen Beweismass, so könnte, wie gezeigt, gerade dieser Zweck regelmässig nicht erfüllt werden. Gleiches gilt für vertragliche Regelungen.

678 Hinzu kommt, dass die Praxis auch beim Beweis mit Papierurkunden oftmals aus prozessualen Gründen ein reduziertes Beweismass genügen lässt, könnte doch das Prozessrecht bei einem Beharren auf dem vollen Beweismass seine Funktionen oftmals nicht wahrnehmen.[1071] Dies muss für elektronisch signierte Urkunden genauso gelten, will man diese gegenüber Papierurkunden beweisrechtlich nicht diskriminieren.

679 Die Voraussetzung für einen Anscheinsbeweis, dass der Gesetzeszweck durch für die anwendbaren Normen geradezu symptomatische Beweisschwierigkeiten vereitelt zu werden drohen, ist damit erfüllt.

d) Massnahmen zur Beweissicherung

680 Der Anscheinsbeweis rechtfertigt sich indessen nur dann, wenn der Beweisführer die ihm zumutbaren Massnahmen zur Beweissicherung tatsächlich ergriffen hat.[1072]

681 Anders als in früher geschilderten Fällen[1073] ist der Beweisführer bei elektronischen Signaturen nur zum Teil oder gar nicht am Erzeugen der Signatur beteiligt. Dennoch ist dort, wo Einflussmöglichkeiten bestehen (etwa wenn er die Auswahl des Signiersystems vorgenommen hat oder hinsichtlich des Nachweises des Signierzeitpunktes), darauf abzustellen, ob der Beweisführer diese in für ihn zumutbarer Weise genutzt hat. Im Rahmen der Besprechung der einzelnen Fallgruppen ist auf diese Einflussmöglichkeiten noch genauer einzugehen.

e) Zusammenfassung

682 Hat der Beweisführer die ihm zumutbaren Vorkehren zur Beweissicherung ergriffen,[1074] so ist der Anscheinsbeweis hinsichtlich der problematischen Indizien (Ausspähen der PIN, Präsentationsproblem, korrekte Arbeit des Zertifizierungsdiensteanbieters) m. E. zuzulassen.

3. Bedeutung der ex-ante-Prüfung für das Gericht

a) Regelungsmodelle

683 Liegt eine qualifizierte elektronische Signatur mit ex-ante-Prüfung nach Art. 3 ff. ZertES vor, so ist zu fragen, inwiefern das Gericht an die Ergebnisse dieser Prüfung

---

1070 Art. 1 Abs. 2 Bst. b E-ZertES; Vgl. etwa Kommentar ZertDV, 1; die Botschaft ZertES erwähnt dieses Ziel allerdings nicht mehr, sondern beschränkt sich darauf, auf die positiven Auswirkungen der materiellrechtlichen Anerkennung bei der Förderung des elektronischen Geschäftsverkehrs darzustellen; Botschaft ZertES, 5684 f.

1071 Vorne N 648 ff.

1072 Vorne N 620.

1073 Insbesondere im EFTPOS-Fall; vorne N 597 f.

1074 Auf diese ist im Rahmen der Besprechung der einzelnen Fallgruppen genauer einzugehen.

gebunden ist. Wie bereits erwähnt, sind vier Regelungsmodelle denkbar: Erstens eine gesetzliche Fiktion der Echtheit der Signatur, zweitens eine widerlegbare gesetzliche Vermutung, drittens ein gesetzlicher Anscheinsbeweis sowie viertens die Beibehaltung der freien richterlichen Beweiswürdigung.[1075]

b) Regelungvorschlag des Entwurfs

684 Anders als noch der VE-BGES, der in Art. 17 Abs. 1 eine gesetzliche Vermutung der Echtheit aufstellte,[1076] verzichtet der E-ZertES aufgrund kritischer Reaktionen in der Vernehmlassung nun vollständig auf eine Regelung der Beweiskraft und folgt damit der vierten Lösungsvariante.[1077] Die Botschaft geht jedoch nicht auf die Bedeutung der ex-ante-Prüfung für die Beweiswürdigung ein; es wird einzig darauf verwiesen, dass die Echtheitsvermutung aufgrund der Kritik in der Vernehmlassung fallen gelassen worden sei.[1078]

c) Interpretationsvorschlag

aa) Zweck der ex-ante-Prüfung

685 Zöge man nun aber aus dem Verzicht des Bundesrates auf eine Echtheitsvermutung den Schluss, die Echtheit der Signatur sei in jedem Fall durch aufwändige Sachverständigengutachten in allen Einzelheiten darzulegen, so würde m.E. das Wesen der ex-ante-Prüfung verkannt. Deren Ziel, Vertrauen in elektronische Signaturen zu schaffen,[1079] kann nur erreicht werden, indem man für elektronische Signaturen auch ein einfaches Beweisverfahren vorsieht, das nicht durch die Unwägbarkeiten der Würdigung komplexer technischer Sachverhalte durch überforderte Gerichte belastet ist. Eine Bedeutung der ex-ante-Prüfung ist demnach auch in der Entlastung der Gerichte von der Prüfung dieser Sachverhalte zu sehen.

bb) Tatsächliche Vermutung der Echtheit?

686 Anders als mit einem zum Zeitpunkt der Beurteilung einer Signatur verfassten Gutachten wird durch eine ex-ante-Prüfung aber nicht die Echtheit einer konkreten Unterschrift, sondern nur in abstrakter Weise die Zuverlässigkeit von Signaturverfahren sowie Organisation, technischen Mitteln u.dgl. des Zertifizierungsdiensteanbieters nach dem momentanen Stand der Erkenntnis überprüft. Schon deshalb kann die ex-ante-Prüfung keine tatsächliche Vermutung für die Echtheit einer konkreten Signatur begründen.

1075 Vorne N 290ff.

1076 Dazu Begleitbericht VE-BGES, 22; zustimmend mit Hinweis auf die Einfachheit der Lösung SCHLAURI/KOHLAS, 25f.; SWICO, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 128; vgl. auch SCHÖBI, Vertragsschluss, 106ff.; KOFMEL EHRENZELLER, 821f.

1077 Botschaft ZertES, 5691, 5708; RAGGENBASS, B47; SCHLAURI, Basistechnologie, 95.

1078 Botschaft ZertES, 5708.

1079 Vorne N 282.

cc) Beweismassreduktion

687 Will man die Entlastungswirkung der ex-ante-Prüfung aber gleichwohl nicht in Frage stellen, so kann die Ablehnung einer auf sie gestützten tatsächlichen Vermutung nicht bedeuten, dass der Echtheitsnachweis nun doch wieder gutachterlich zu führen wäre. Vielmehr soll die ex-ante-Prüfung *gerade trotz des Fehlens einer tatsächlichen Vermutung* im Sinne eines antizipierten Sachverständigengutachtens als Grundlage für den gerichtlichen Entscheid dienen.[1080]

688 Darin wiederum liegt erneut eine Reduktion des Beweismasses in der Art eines Anscheinsbeweises: Das Gericht muss prima facie vom Vorliegen der im Rahmen der ex-ante-Prüfung überprüften Aspekte ausgehen können.[1081] Voraussetzung bleibt aber auch hier, dass der Beweisführer die für ihn zumutbaren Massnahmen zur Beweissicherung ergriffen hat.[1082]

4. Signaturen ohne ex-ante-Prüfung und Rahmenvertrag

a) Anwendungsfälle

689 Zu Fallgruppe 1[1083] zählen Signaturen ohne ex-ante-Prüfung, die in offenen Benutzergruppen zur Anwendung gelangen. Anwendungsfälle sind etwa die Authentifizierung von Servern im WWW[1084], das Code Signing[1085] oder der E-Mail-Verkehr innerhalb eines Unternehmens bzw. die Authentifizierung von Personen etwa zur Zutrittskontrolle oder als Zugangsschutz für Computer. Zu nennen ist hier auch Pretty Good Privacy, das von einer stetig steigenden Zahl von Anwendern regelmässig zum Unterzeichnen von Nachrichten genutzt wird.[1086]

690 Zu Fallgruppe 1 gehören auch elektronische Signaturen, die zwar keine Anbieteranerkennung aufweisen, aber dennoch ein entsprechendes Sicherheitsniveau aufweisen (qualifizierte elektronische Signaturen im Sinne von Art. 2 Bst. c E-ZertES ohne Anbieteranerkennung).[1087]

b) Beweisführung

691 Weil bei Fallgruppe 1 keine ex-ante-Prüfung stattgefunden hat, sind sämtliche der geschilderten Zusammenhänge gutachterlich darzulegen.[1088]

1080 Vgl. etwa (allerdings in Bezug auf § 292a ZPO DE) LÜDEMANN/ADAMS, 12.

1081 Die einzelnen Glieder der Indizienkette werden in der folgenden Darstellung der einzelnen Fallgruppen dargelegt.

1082 Vorne N 620.

1083 Vorne N 670.

1084 Im Rahmen von SSL-Verbindungen kommen regelmässig digitale Signaturen zur Authentifizierung des Servers beim Client zur Anwendung; zu SSL vorne N 143 ff.

1085 Vorne N 137.

1086 Zu PGP vorne N 78; vgl. etwa C'T, PGP Key Certification Authority, http://www.heise.de/ct/pgpCA. PGP-Signaturen sind indessen nicht qualifizierte elektronische Signaturen, sondern nur fortgeschrittene; vorne N 382.

1087 Vorne N 280 ff., 514 ff.

692 Liegt das Ziel des Einsatzes in erster Linie darin, zu verhindern, dass sich ein unberechtigter Dritter in die Kommunikation einschaltet oder ein Computersystem bedient (Authentifizierung), und nur in zweiter Linie oder gar nicht, einem Kommunikationspartner zu einem späteren Zeitpunkt einen bestimmten Kontakt nachzuweisen (Nichtabstreitbarkeit) – erhält eine Signatur den Beweiszweck also erst nachträglich[1089] – so kann nicht die Rede davon sein, dass ein Beharren auf dem vollen Beweismass einen von den Parteien verfolgten Zweck vereiteln würde. Der Anscheinsbeweis ist demnach ausgeschlossen. Hinzu kommt, dass derartige Systeme meist kein für Beweiszwecke ausreichendes Sicherheitsniveau aufweisen.[1090]

693 Ein Anscheinsbeweis für die Echtheit einer Signatur ohne ex-ante-Prüfung und ohne Rahmenvertrag dürfte daher m. E. nur in Einzelfällen zulässig sein – etwa dann, wenn der Nachweis erbracht wurde, dass es sich um eine qualifizierte elektronische Signatur im Sinne von Art. 2 Bst. c E-ZertES handelt.[1091]

c) Haftung des Signierschlüsselhalters

aa) Fragestellung

694 Weil keine biometrische Koppelung zwischen Signierschlüssel und Schlüsselhalter besteht, kann der Halter seinen Schlüssel preisgeben und sich damit von Signaturen lossagen. Es stellt sich daher die Frage nach einer Pflicht des Halters zur Geheimhaltung seines Signierschlüssels und entsprechenden Haftungsfolgen.

bb) Vertragliche Haftung zugunsten Dritter

695 In der Regel statuieren die *AGB des Zertifizierungsdiensteanbieters* eine Verpflichtung des Signierschlüsselhalters, seinen Schlüssel geheim zu halten.[1092] Ob diese Verpflichtung auch als Vertrag zu Gunsten der auf die Signatur vertrauenden Dritten zu verstehen sind, ergibt sich aus diesen AGB. Meines Erachtens darf insbesondere nicht allein aus der Geheimhaltungspflicht zu Gunsten des Zertifizierungsdiensteanbieters auf eine Geheimhaltungspflicht (und entsprechende Haftung) zu Gunsten

---

1088 Vorne N 683 ff.

1089 Der Strafrechtler spräche von einer *Zufallsurkunde;* STRATENWERTH, § 35 N 17.

1090 Bei SSL beispielsweise kommen meist nur Softwaresigniereinheiten zur Anwendung. Der SSL-Signiermechanismus ist in gängiger WWW-Serversoftware integriert; dazu etwa http://www.freebsddiary.org/openssl-client-authentication.php. Auch wurden schon Code-Signing-Zertifikate (vorne N 137) für Microsoft Windows gefälscht, weil die unsichere Identitätsprüfung des US-Zertifizierungsdiensteanbieters VeriSign versagte; Patrick BRAUCH (pab.), Falsche Microsoft-Zertifikate, c't 8/2001, 54.

1091 In Anlehnung an die Lösung von § 292a ZPO DE, die für den Anscheinsbeweis ebenfalls nicht eine ex-ante-Prüfung, sondern nur den Nachweis (volles Beweismass!) einer qualifizierten elektronischen Signatur voraussetzt; dazu vorne N 456 ff., 460.

1092 Vgl. etwa Art. 4.1 f der AGB der deutschen Telesec, http://www.telekom.de/dtag/t-telesec/telesec_showdatei/1,2626,31,00.pdf; Abschnitt 3.2.1.1 des Identrus Certification Practice Statement, http://www.identrus.com/knowledge/pubs/Identity_Certificate_Policy.pdf; zur Haftung aus Rahmenvertrag mit dem Anbieter der Dienstleistung hinten N 732 ff.

allfällig auf die Signatur vertrauender Dritter geschlossen werden, weil Zertifikate etwa auch bloss zu Verschlüsselungszwecken ausgestellt werden können.[1093]

cc) Haftung aus Stellvertretungsrecht

696 Teilweise wird hinsichtlich der Wirkung digitaler Signaturen auf das *Stellvertretungsrecht* verwiesen. Es wird argumentiert, der Signierschlüsselhalter hafte bei einem Missbrauch seines Schlüssels gleich wie ein Vertretener in einem Fall der Vertretungswirkung ohne Genehmigung (d.h. für das positive Vertragsinteresse).[1094]

697 Eine solche Vertretungswirkung besteht jedoch nur dann, wenn der Vertretene Kenntnis vom Auftreten eines anderen in seinem Namen hat und dagegen nicht einschreitet (Duldungsvollmacht) oder dann, wenn der Vertretene zwar keine Kenntnis vom Handeln des Vertreters hatte, dieses jedoch bei pflichtgemässer Sorgfalt hätte erkennen müssen (Anscheinsvollmacht).[1095] Die Annahme einer Anscheinsvollmacht ist zudem nur dann gerechtfertigt, wenn ein Verhalten des Vertretenen selbst als Äusserung des Bevollmächtigungswillens verstanden werden kann, nicht jedoch dann, wenn durch Zufall oder das Verhalten Dritter der Anschein einer Vollmacht entsteht.[1096] Der Signierschlüsselhalter hat während eines Angriffs indessen meistens gerade *keine* Kenntnis vom Handeln des Angreifers, denn der Angreifer verschafft sich ohne Zutun des Schlüsselhalters Zugriff auf den Schlüssel. Weil derartige Angriffe gerade im Geheimen stattfinden, ist auch nicht davon auszugehen, dass der Schlüsselhalter davon hätte Kenntnis haben müssen.

698 Hinzu kommt, dass ein Angreifer eine Signatur nicht *in*, sondern *unter fremdem Namen* setzt, er tritt also nicht als Vertreter des Schlüsselhalters, sondern als der Schlüsselhalter selbst auf. Nach BGE 120 II 201 schliesst dies die stellvertretungsrechtlichen Gutglaubensvorschriften a priori aus.[1097]

699 Von einem Stellvertretungsverhältnis kann daher m.E. nicht ausgegangen werden.[1098]

dd) Vertrauenshaftung

700 Man könnte aber allenfalls auch unabhängig vom Stellvertretungsrecht argumentieren, wer ein Zertifikat auf sich ausstellen lasse, wecke beim Empfänger signierter Nachrichten Vertrauen in die Geheimhaltung des Signierschlüssel, weshalb er dem

---

1093 Vorne N 169 f.

1094 Begleitbericht VE-BGES, 23; ROSENTHAL, Missverständnisse, Rz 5; DERSELBE, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 48 f.

1095 GAUCH/SCHLUEP/SCHMID, N 1411 f.; BK-ZÄCH, N 48 und 52 zu Art. 33 OR; vgl. auch KPMG, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 112; kritisch zur Frage, ob bei PIN/TAN-Verfahren eine Anscheinsvollmacht angenommen werden kann SPINDLER, Bankrecht I, Rz 25 ff.

1096 BUCHER, OR AT, 613.

1097 Vgl. auch SIDLER, 67.

1098 Gl.M. KPMG, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 112; SCHÖBI, Vertragsschluss, 104 ff.

auf die Signatur vertrauenden Dritten im Falle der Preisgabe zumindest für das negative Interesse hafte.

701 Voraussetzung für eine derartige *Vertrauenshaftung* sind nach der Praxis des Bundesgerichts unter anderem eine rechtliche Sonderverbindung zwischen Schädiger und Geschädigtem, das Erwecken schutzwürdigen Vertrauens und dessen Enttäuschung unter Verletzung von Treu und Glauben.[1099] Vergleichbar ist auch der Fall der *Blankettfälschung*.[1100]

702 Während bei einer elektronischen Signatur die rechtliche Sonderverbindung möglicherweise noch zu begründen wäre, dürfte dies für die Vertrauensgrundlage indessen nicht mehr möglich sein. Denn Zertifikate können, wie beschrieben, auch zu anderen als zu Beweiszwecken eingesetzt werden, und wer ein Zertifikat anderweitig einsetzen will, wird sich auch nicht die Mühe machen, einen geheimen Schlüssel mit der für Beweiszwecke notwendigen Sorgfalt aufzubewahren. Umgekehrt ist daher ein einzig auf das Vorliegen eines Zertifikats gestütztes Vertrauen in die Geheimhaltung nicht gerechtfertigt.

703 Allein aus der Tatsache, dass eine Person ein Zertifikat auf sich ausstellen lässt, lässt sich damit m. E. keine Pflicht für die Geheimhaltung des Signierschlüssels und keine Haftung für dessen Missbrauch herleiten.

ee) Haftungserklärung des Schlüsselhalters

704 Eine Haftung des Signierschlüsselhalters ergäbe sich allenfalls aus einer Erklärung, wonach dieser sich gegenüber bestimmten Personen oder auch gegenüber der Allgemeinheit verpflichtet, für den Missbrauch seines Schlüssels zu haften. Dabei handelte es sich um eine einseitige, nicht empfangsbedürftige Willenserklärung, ähnlich einer nach aussen kundgegebenen Vollmacht. Ob der Signierschlüsselhalter für das positive oder negative Vertragsinteresse des auf die Signatur vertrauenden Dritten haftet, und unter welchen Bedingungen der Schlüsselhalter haften will, ergibt sich aus der Erklärung selbst. Die Wirksamkeit einer derartigen Erklärung hat ihre Grenzen in Art. 27 ZGB (Schutz der Persönlichkeit vor übermässiger Bindung): Eine Erklärung, bei einem unsicheren System gegenüber einer unbegrenzten Zahl von Adressaten ohne Beschränkung zu haften dürfte unwirksam sein, weil sich der Schlüsselhalter damit einem Fälscher schutzlos ausliefern würde. Handelt es sich allerdings um eine qualifizierte elektronische Signatur nach E-ZertES, so kann kaum mehr von einer unzulässigen Selbstbindung die Rede sein.

1099 Statt vieler GAUCH/SCHLUEP/SCHMID, N 982e ff. m. H.; grundsätzlich kritisch zur Konstruktion der Vertrauenshaftung etwa HONSELL, 4 N 22; SCHWENZER, N. 52.01.

1100 Dazu BGE 88 II 422; vgl. auch KPMG, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 107 ff.

705 KOHLAS/MAURER bezeichnen eine derartige Erklärung als *Commitment*.[1101] Sie gehen davon aus, dass der Zertifizierungsdiensteanbieter bei der Zertifizierung eine Erklärung über eine Haftungserklärung des Schlüsselhalters abgibt: "The main role of a certification authority is to make statements, through its own public key, about statements (claim of ownership or commitment) made by other entities."[1102]

706 Diese Betrachtungsweise muss vom geschilderten Vertrag zugunsten Dritter unterschieden werden. Der Zertifizierungsdiensteanbieter tritt hier vielmehr als Mittler auf, den der Schlüsselhalter einsetzt, um sein Commitment vertrauenswürdig zu verbreiten. Ob von einer Erklärung des Zertifizierungsdiensteanbieters über ein Commitment ausgegangen werden kann, ergibt sich aus dem Certification Practice Statement des Zertifizierungsdiensteanbieters, auf das im Zertifikat hingewiesen wird.

ff) Haftung aus Art. 59a E-OR?

707 Art. 59a E-OR setzt ein qualifiziertes Zertifikat eines *anerkannten* Zertifizierungsdiensteanbieters voraus. Bei einem Zertifikat ohne Anbieteranerkennung haftet der Schlüsselhalter daher aus Art. 59a E-OR e contrario *nicht*. Zu beachten ist, dass dies insbesondere auch für qualifizierte elektronische Signaturen gelten soll.[1103]

d) Zusammenfassung

708 Fallgruppe 1 umfasst zunächst Anwendungen elektronischer Signaturen, die nicht in erster Linie zum Zweck der Beweisführung eingesetzt werden. Kommt eine derartige Signatur dennoch einmal als Beweismittel zum Einsatz, so handelt es sich demnach um eine *Zufallsurkunde.* Dies schliesst die Zulassung des Anscheinsbeweises m.E. aus.

709 Hinzu kommt, dass der Empfänger eines signierten Dokumentes nicht ohne weiteres davon ausgehen darf, dass der Schlüsselhalter seinen Signierschlüssel zu Beweiszwecken einsetzen will. Vertrauen in dessen Geheimhaltung ist daher meist nicht gerechtfertigt, was eine Vertrauenshaftung des Schlüsselhalters in Missbrauchsfällen ausschliesst. Aufgrund der fehlenden ex-ante-Prüfung ist der Beweis zudem ausschliesslich durch Sachverständigengutachen zu führen.

710 Aus diesen Gründen sind Signaturen der Fallgruppe 1 – dazu gehören wie erwähnt auch qualifizierte elektronische Signaturen ohne Anbieteranerkennung gemäss Art. 2 Bst. c E-ZertES – als Beweismittel wenig geeignet; sie dürften eine Überzeugung des Gerichts vielfach nur im Zusammenspiel mit weiteren Indizien begründen können.

1101 Der Begriff «Commitment» ist etwa als *Haftungserklärung* übersetzbar. Zum Ganzen KOHLAS/MAURER, 552; zur ähnlichen Frage der Rekognition auch hinten N 838 ff.

1102 KOHLAS/MAURER, a.a.O.

1103 Dazu eingehend mit Kritik hinten N 755 ff.

5. Signaturen ohne ex-ante-Prüfung mit Rahmenvertrag

a) Anwendungsfälle

711 Der vorderhand wohl weitaus häufigste Anwendungsfall elektronischer Signaturen dürfte die Legitimation bei Online-Dienstleistungen mit hohen Sicherheitsbedürfnissen wie E-Banking sein.[1104] Hierzu wird vertraglich vereinbart, dass sich der Nutzer mittels der Signatur online anmeldet; die Signatur ersetzt damit die herkömmlichen Identifikationsmittel Passwort (bzw. PIN) und TAN. Dieser Einsatz elektronischer Signaturen zu Legitimationszwecken soll hier als *Fallgruppe 2a* bezeichnet werden.

712 Die Signatur kann indessen nicht nur zur Identifikation des Kunden beim Verbindungsaufbau verwendet, sondern auch zur Unterzeichnung *jeder einzelnen Transaktion*,[1105] was die Beweislage des Anbieters sowohl gegenüber den herkömmlichen Legitimationsmitteln PIN/TAN als auch gegenüber Fallgruppe 2a deutlich verbessert. Diese Einsatzvariante soll als *Fallgruppe 2b* bezeichnet werden. Entsprechende Anwendungen befinden sich heute in Entwicklung.[1106]

713 In beiden Fällen können sowohl fortgeschrittene als auch qualifizierte elektronische Signaturen zum Einsatz kommen.[1107]

b) Exkurs: Legitimationsmittel im Bankgeschäft

aa) Vorbemerkung

714 Als Anhaltspunkt zur rechtlichen Beurteilung der Fallgruppe 2a können Lehre und Rechtsprechung zu herkömmlichen elektronischen Legitimationsmitteln im Bankgeschäft dienen. Dazu zählen die Handunterschrift, Debitkarten sowie Passwort und TAN beim E-Banking. Debitkarten (wie die EC-Karte oder die Postcard) ermöglichen Bezüge an Geldautomaten sowie bargeldloses Bezahlen am Verkaufspunkt *(EFTPOS*[1108]*)*.[1109] E-Banking dient unter anderem dem Überweisungsverkehr. Frühere E-Banking-Systeme basierten auf Videotex[1110], heute wird fast ausschliesslich über das Internet kommuniziert.

bb) Girovertrag

715 Die genannten Legitimationsmittel dienen dem Zugriff auf ein *Girokonto*. Die Führung des Girokontos wird zwischen Kunde und Bank durch einen *Girovertrag* geregelt, einen «auf die Dauer gerichteten Geschäftsbesorgungsvertrag, in dem sich die

---

1104 Erste Pilotprojekte zur Legitimation mit digitalen Signaturen wurden in der Schweiz durch UBS und Postfinance durchgeführt; für einen Überblick etwa KNEUBÜHLER, 85; vgl. auch RASSMANN, insbesondere 39 ff.

1105 Etwa mittels Form Signing; vorne N 134 f.

1106 Ein Beispiel ist bei OBERHOLZER, EBPP, 127 ff. beschrieben.

1107 Zur Haftung des Anbieters für sorgfältige Auswahl des Signiersystems N 726.

1108 *Electronic Funds Transfer at the Point of Sale*; VON DER CRONE, 1 f.

1109 Eingehend STEINMANN, 25 ff.

1110 Zu Videotex etwa noch STEINMANN, 4.

Bank verpflichtet, für einen Kunden den Zahlungsverkehr zu übernehmen, insbesondere Zahlungen auszuführen und Überweisungen entgegenzunehmen.»[1111] Nach Art. 394 Abs. 2 OR kommt Auftragsrecht zur Anwendung.[1112] Der Einsatz einer Debitkarte oder von E-Banking beruht regelmässig auf weiteren, den Girovertrag ergänzenden AGB.[1113]

cc) Rechtliche Natur des Überweisungsauftrages

716 Eine einzelne Transaktion an einem EFTPOS-Terminal oder ein einzelner Zahlungsauftrag an die Bank ist zunächst als *Anweisung* nach Art. 466 ff. OR zu qualifizieren. Der Kunde (Anweisender) weist seine Bank (Angewiesene) an, dem Händler bzw. dem durch den Zahlungsauftrag Begünstigten (Anweisungsempfänger) einen bestimmten Betrag gutzuschreiben.[1114] Man spricht bei der Anweisung auch von einer *Ermächtigung* des Anweisenden gegenüber dem Angewiesenen zur Gutschreibung des angewiesenen Betrages auf das Konto des Anweisungsempfängers.[1115]

717 Nach einer *ersten Auffassung* ist eine Einzeltransaktion *zudem*[1116] als vom Girovertrag weitgehend unabhängiger, von der Bank von vornherein angenommener *Einzelauftrag* zu sehen.[1117] Eine *zweite Auffassung* (die in der Schweiz herrschende Lehre und Rechtsprechung) betrachtet die Einzeltransaktion hingegen als auftragsrechtliche Weisung im Rahmen des girovertraglichen Grundverhältnisses und gesteht ihr keine eigenständige Vertragsnatur zu.[1118]

718 Mit der Ausführung der Transaktion erhält der Beauftragte in beiden Fällen gegenüber dem Auftraggeber nach Art. 402 Abs. 1 OR Anspruch auf Aufwendungsersatz (durch Verrechnung mit dessen Bankguthaben in Form der Belastung des Girokontos).[1119]

dd) Dispositive Legitimationsordnung

719 Geht man entsprechend der erstgenannten Auffassung vom Wesen des Überweisungsauftrages als Einzelauftrag aus, so ist bei einem Missbrauch der Legi-

---

1111 BGE 100 II 370; BUIS, Banküberweisung, 38 ff.; GUGGENHEIM, 487 F.; KILGUS, 121 ff.; STEINMANN, 59 ff.; VON DER CRONE, 53 f. Daneben wird vielfach noch von einem *Kontokorrentvertrag* gesprochen; vgl. etwa STEINMANN, 58 f.; VON DER CRONE, 27 ff.

1112 GUGGENHEIM, 491; KILGUS, 122 m.H.; STEINMANN, 61.

1113 Dazu etwa STEINMANN, 57, 74 f.

1114 BUIS, Banküberweisung, 45; KILGUS, 133; die Schilderung der Verhältnisse bei Miteinbezug zweier oder mehrerer Banken würde den Rahmen dieser Arbeit sprengen; dazu etwa GUGGENHEIM, 500 ff.; VON DER CRONE, 44 ff.

1115 KILGUS, 133 f.; VON DER CRONE, 43 f.

1116 KILGUS, 134, spricht von einer *juristischen Doppelnatur* des Überweisungsauftrages.

1117 So etwa WEBER, Zahlungsaufträge, 88; ähnlich THOMANN, 164, unter Berufung auf die Sphärentheorie, und VON DER CRONE, 53 ff., 120 ff., der in erster Linie auf den Anweisungscharakter abstellt; vgl. auch KILGUS, 134; zur *deutschen* Praxis N 723, insbesondere FN 1127.

1118 BGE 121 III 131; 108 II 314; ZR 98 (1999) Nr. 42; GUGGENHEIM, 491 f.; KILGUS, 133 f.; Beat KLEINER, Die allgemeinen Geschäftbedingungen der Banken, Giro- und Kontokorrentvertrag, 2. A. Zürich 1963, 40; STEINMANN, 61; vgl. auch VON DER CRONE, 42 f.

1119 STEINMANN, 61; für *Deutschland* etwa REISER, 12; RÜSSMANN, Haftungsfragen, 395.

timationsmittel durch einen unberechtigten Dritten eine Belastung des Kontos für Aufwendungsersatz nicht möglich, weil keine Willenserklärung des Kontoinhabers vorliegt und allein aufgrund des Girovertrages auch nicht zu vermuten ist.[1120] Trägt der Kunde allerdings ein Verschulden an der missbräuchlichen Verwendung von Karte und PIN, kann die Bank gestützt auf Art. 402 Abs. 2 OR Schadenersatz fordern (positive Vertragsverletzung).[1121] Mitverschulden der Bank ist nach den Grundsätzen über das Selbstverschulden bei der Bemessung des Ersatzanspruches zu berücksichtigen.[1122]

720 Das Bundesgericht betrachtet den Zahlungsauftrag zusammen mit der wohl herrschenden Lehre als eine Weisung im Rahmen des girovertraglichen Grundverhältnisses.[1123] Es vertritt dabei die Meinung, eine Belastung des Kontos des Kunden bei Fälschungen sei in analoger Anwendung der checkrechtlichen Vorschrift von Art. 1132 OR[1124] zumindest nach dispositivem Recht nicht möglich.[1125]

721 Einige Autoren, die den Überweisungsauftrag ebenfalls als eine auftragsrechtliche Weisung betrachten, lehnen die Anwendbarkeit von Art. 1132 OR indessen ab. Nach deren Auffassung ist darauf abzustellen, ob die Bank die Legitimation des Anweisenden mit der gemäss Girovertrag bzw. diesen ergänzenden AGB erforderlichen *Sorgfalt* geprüft hat; ist dies der Fall, so hat sie den Girovertrag unabhängig von einer Fälschung *richtig erfüllt* und damit Anspruch auf Aufwendungsersatz nach Art. 402 Abs. 1 OR. STEINMANN etwa vertritt diese Meinung insbesondere für Fälle der Legitimation durch Code, weil es der Bank systembedingt nicht möglich sei, Fälschungen zu erkennen.[1126] Er übersieht dabei m. E. aber, dass die Haftung der Bank nach Art. 1132 OR keine Verschuldenshaftung ist und es folglich gerade nicht darauf ankommen kann, ob die Bank bei der einzelnen Legitimationsprüfung hinsichtlich der Sorgfalt überhaupt Spielraum hat.

1120 BUIS, Banküberweisung, 169; GUGGENHEIM, Verträge, 246 f.; KILGUS, 137 ff.; RÜSSMANN, Haftungsfragen, 396; THOMANN, 64 f.; VON DER CRONE, 61, 121; WEBER, Zahlungsaufträge, 88; für *Deutschland* N 723, insbesondere FN 1127.

1121 BGE 51 II 88; eingehend KILGUS, 142 ff.; GUGGENHEIM, Verträge, 247; WEBER, Zahlungsaufträge, 88; VON DER CRONE, 62, 122 f.; für *Deutschland* N 723, insbesondere FN 1127; für Österreich und zur Qualifikation des (verschuldeten) Einsatzes der Legitimationsmittel durch eine dritte Person als Handeln in fremdem Namen etwa JANISCH, 163 ff.; kritisch dazu jedoch SPINDLER, Bankrecht I, Rz 25 ff.

1122 VON DER CRONE, 62.

1123 Soeben N 717.

1124 Art. 1132 OR weist das Risiko für Checkfälschungen dem Bezogenen, also der Bank zu; eine Regelung der Legitimation fehlt im Auftragsrecht.

1125 Unveröffentlichter BGE vom 25. Oktober 1960 i. S. Okcuoglu gegen SBG, besprochen bei KILGUS, 93 ff., vgl. insbesondere 94 f.

1126 STEINMANN, 82, insbesondere FN 320.

ee) Parteiautonome Legitimationsordnung

722 Die dispositive Ordnung ist indessen praktisch nicht von grosser Bedeutung, weil die schweizerische Rechtsordnung Raum für privatautonome Risikoverteilungsordnungen lässt.

723 Betrachtet man den Zahlungsauftrag gemäss der ersten Auffassung als Einzelauftrag, oder lässt man mit dem Bundesgericht Art. 1132 OR analog zu Anwendung kommen, haftet der Kunde nach dispositivem Recht bei Fälschungen nicht, sofern ihn kein Verschulden trifft. Es bleibt den Parteien indessen nach herrschender Lehre und Rechtsprechung unbenommen, im Rahmen der gesetzlichen Schranken eine eigene Legitimationsordnung und damit die Risikoverteilung für Zufall zu Lasten des Kunden zu vereinbaren.[1127] Von dieser Möglichkeit machen die Banken regelmässig Gebrauch.[1128]

724 Die gesetzlichen Schranken einer solchen Legitimationsordnung liegen im Auftragsrecht (die Bank darf ihre eigenen Pflichten nicht auf ein absolutes Minimum beschränken), in Art. 20 OR (sittenwidrige Verfälschung der Geschäftsbeziehung), in der analogen Anwendung der Art. 100 und 101 OR sowie in Art. 8 UWG.[1129] Das Gericht hat demnach die in Frage stehenden AGB der Bank einer gewissen Inhaltskontrolle zu unterwerfen.[1130]

1127 BGE i.S. Okcuoglu (soeben FN 1125), 108 II 314, 109 II 116, 122 III 27; eingehend GUGGENHEIM, Contrats, 513 ff.; WEBER, Zahlungsaufträge, 89; kritisch BUCHER, Wer haftet, 101 ff. sowie DERSELBE, Belastung, 41 ff.; vgl. etwa auch David ROSENTHAL, Haften die Kunden für Hacker?, Die Weltwoche Nr. 23, 8. Juni 2000, 11. Aufgrund der weniger liberalen AGB-Gesetzgebung weitgehend anders ist die Lage im *europäischen Ausland*. Nach der in *Deutschland* herrschenden Auffassung muss die Bank entweder den Transaktionsbefehl nachweisen (für Aufwendungsersatz) oder ein Verschulden des Kunden (für Schadenersatz), wobei sie den Anscheinsbeweis für das Verschulden für sich hat, sofern ein ausreichend sicheres System zur Anwendung kam; vgl. vorne den EFT-POS-Fall, N 597 f.; Beschluss des BGH, Aktenzeichen XI ZR 42/00, DuD 2/2001, 106 ff., 107; OLG Hamm, Aktenzeichen 31 U 72/96, NJW 1997, 1711; LG Hannover, Aktenzeichen 20 S 97/97, WM 22/1997, 1123 ff.; LG Bonn, Urteil vom 11. Januar 1997, Aktenzeichen 5 S 163/94, WM 13/1995, 575 f.; Amtsgericht Frankfurt a.M., Aktenzeichen 30 C 2119/97-45, CR 12/1998, 723 ff.; dazu BUCHER, Belastung, 51 ff.; KILGUS, 109 ff.; KÖNIG, Anschein, 248 ff.; RÜSSMANN, Haftungsfragen, 395 ff.; eingehend SPINDLER, Bankrecht I, Rz 17 f., 19 ff., 22 ff., 32 ff., 78 ff., für qualifizierte elektronische Signaturen 97 ff.; Stefan WERNER, Anscheinsbeweis und Sicherheit des ec-PIN-Systems im Lichte der neueren Rechtsprechung, WM 32/1997, 1516 ff.

1128 Die standardisierten EC-Bedingungen sehen immerhin unter bestimmten Umständen die Schadensübernahme durch einen hierzu eigens geschaffenen Bancomat-Fonds vor; STEINMANN, 100 ff.

1129 Eingehend WEBER, AGB, 157 ff.; DERSELBE, Zahlungsaufträge, 89; vgl. auch BUCHER, Wer haftet, 101 ff.; KILGUS, 129 f., 137 f., 153, 157 ff.; STEINMANN, 175 ff.; THOMANN, 164; VON DER CRONE, 108, 124 f., BK-WEBER, N 43 ff. und insbesondere 75 zu Art. 100 OR. Banken sind als obrigkeitlich konzessionierte Gewerbe i.S. von Art. 100 Abs. 2 OR zu verstehen; BGE 112 II 454; 109 II 119 f.; THOMANN, 163 f.; WEBER, AGB, 154 f.; BK-WEBER, N 120 ff. zu Art. 100 OR. Zu Art. 8 UWG hinten N 737.

1130 Eingehend WEBER, AGB, 157 ff.; DERSELBE, Zahlungsaufträge, 89 f.; für eine weitergehende Inhaltskontrolle BUCHER, Wer haftet, 103; DERSELBE, Belastung, 44 ff.

ff) Aufklärungs- und Sorgfaltspflichten

725 Kommen elektronische Legitimationsmittel zur Anwendung, so ist der Kunde – anders als bei der Legitimation durch Handunterschrift – regelmässig nicht in der Lage, deren Sicherheit zu beurteilen. Er muss deshalb der fachkundigen Bank vertrauen.[1131]

726 Die Bank hat daher zum einen den Kunden vorvertraglich soweit nötig über die Sicherheitsrisiken des vorgeschlagenen Systems und die durch ihn zu ergreifenden Sicherheitsmassnahmen aufzuklären[1132] und haftet zum anderen für gebührende Sorgfalt bei Auswahl und Betrieb des Systems.[1133] Das aus einer unsorgfältigen Systemauswahl entstehende Risiko und das Risiko für Fehler, die der Kunde bei gehöriger Aufklärung durch die Bank hätte vermeiden können, sind nicht auf den Kunden abwälzbar. Der Sorgfaltsmassstab bei Systemauswahl und -betrieb bemisst sich einerseits am zur Verfügung stehenden Stand der Technik, andererseits müssen ökonomische Aspekte selbstverständlich ebenfalls in Betracht gezogen werden können. Es ist ein ausgewogenes Verhältnis zwischen finanziellem Aufwand und Sicherheit anzustreben.[1134]

c) Beweisführung mittels elektronischer Signatur

aa) Parteiautonome Legitimationsordnung

727 Zugleich mit der Einigung auf den Einsatz elektronischer Signaturen als Legitimationsmittel können die Parteien gleich wie bei den soeben beschriebenen herkömmlichen Legitimationsmitteln innerhalb der gesetzlichen Schranken eine parteiautonome Risikoordnung festlegen. Sie können bestimmen, dass der Anbieter an jedermann leisten darf, der sich durch eine gültige Signatur legitimiert und mithin das Fälschungsrisiko auf den Signierschlüsselhalter übertragen.[1135] Bestreitet der Kunde, eine Transaktion vorgenommen zu haben, hat der Anbieter diesfalls nur noch den korrekten Legitimationsvorgang und allenfalls den Eingang des Befehls für die einzelne umstrittene Transaktion zu beweisen. *Nicht* darzulegen ist, dass diese Vorgänge tatsächlich durch den Schlüsselhalter ausgelöst wurden und damit auch die entsprechende Indizienkette[1136].

1131 So etwa auch SPINDLER, Bankrecht I, Rz 45.

1132 Dazu SPINDLER, Bankrecht I, 43 ff.; STEINMANN, 147 ff. m.H.; THOMANN, 164; vgl. auch die Empfehlung der Kommission zu elektronischen Zahlungsinstrumenten und einführend dazu SPINDLER, Bankrecht I, Rz 20.

1133 Eingehend STEINMANN, 192 ff., 198 ff.; VON DER CRONE, 107; allgemein zu den auftragsrechtlichen Nebenpflichten etwa Wolfgang WIEGAND, Zur Haftung für Dienstleistungen, Urteilsanmerkung Zivilrecht, BGE 115 II 62 ff., recht 1990, 134 ff.

1134 STEINMANN, 42, 216 ff.; vgl. auch THOMANN, 164.

1135 N 723 f. Zu technischen Aspekten der digitalen Signatur als Legitimationsmittel vorne N 138 ff.; zur Prüfung der Signatur vorne N 117 ff. Gleich wie beim PIN/TAN-Verfahren kann in *Deutschland* auch für elektronische Signaturen keine parteiautonome Legitimationsordnung statuiert werden; N 723, insbesondere FN 1127; eingehend SPINDLER, Bankrecht I, Rz 85 ff.

1136 Vorne N 672.

bb) Elektronische Signatur zur Legitimation

728 Bei herkömmlichen Systemen (PIN/TAN) geschieht der Nachweis sowohl der Legitimation als auch der einzelnen Transaktionsbefehle anhand der Serverprotokolle des Anbieters (in Verbindung mit dem gutachterlich zu führenden Nachweis, dass diese nicht manipulierbar sind, was mangels positiver Nachweismöglichkeit meist eine Beweismassreduktion im Sinne des Anscheinsbeweises erfordert).[1137] Werden zur Legitimation digitale Signaturen eingesetzt (Fallgruppe 2a[1138]), kann diese später zusätzlich durch das unterzeichnete Token, nötigenfalls in Kombination mit einem Zeitstempel,[1139] nachvollzogen werden. Der Nachweis einzelner Transaktionsbefehle indessen kann weiterhin ausschliesslich mittels der Serverprotokolle geführt werden.

729 Voraussetzung des Anscheinsbeweises ist, dass der Beweisführer die für ihn zumutbaren Massnahmen zur Beweissicherung ergriffen hat.[1140] Geht man davon aus, dass es sich beim Nachweis der Manipulationssicherheit des Systems des Anbieters um einen Anscheinsbeweis handelt,[1141] und dass das Vorlegen des signierten Tokens eine für den Anbieter zumutbare Massnahme zur Verbesserung der Beweislage ist, hat der Systembetreiber das Token zum Beweis vorzulegen, um zum Anscheinsbeweis zugelassen zu werden.

cc) Signatur für einzelne Transaktionsbefehle

730 Nur in Fallgruppe 2b[1142] ist zusätzlich zum Nachweis der Legitimation beim Anmelden auch den Nachweis der einzelnen Transaktionsbefehle des Kunden anhand digitaler Signaturen vorgesehen. Dadurch kann die Beweissituation des Systembetreibers nochmals verbessert werden. Derzeit befinden sich derartige Systeme wie erwähnt in Entwicklung. Je nach Sicherheitsbedürfnissen einer konkreten Anwendung dürfte mit der Marktreife solcher Systeme die Zumutbarkeit ihres Einsatzes für den Anbieter ebenfalls bejaht werden, womit der Anscheinsbeweis wiederum nur mehr beim Einsatz eines solchen Systems zulässig sein wird.

dd) Reduzierte Sicherheitsanforderungen

731 Handelt es sich um eine qualifizierte elektronische Signatur, dürfte der Anscheinsbeweis in jedem Fall zulässig sein.[1143] Bei Anwendungen mit tieferen Sicherheitsanforderungen[1144] muss dies m. E. aber auch bei Signaturverfahren mit entsprechend tieferem Sicherheitsniveau der Fall sein (weniger hohe Sicherheitsanforderungen an das Serversystem, allenfalls Einsatz von Softwaresigniereinheiten u. dgl.), und zwar des-

---

1137 SPINDLER, Bankrecht I, Rz 77.
1138 N 711.
1139 Vorne N 172 ff.
1140 Vorne N 620.
1141 N 728.
1142 N 712.
1143 Vorne N 693.
1144 Beispielsweise dann, wenn auch durch mehrfache Transaktionen keine hohen Werte verschoben werden können, weil eine Beschränkung der Gesamttransaktionssumme besteht.

halb, weil bei der Bestimmung der dem Anbieter zumutbaren Beweissicherungsmassnahmen auch eine Abwägung zwischen Wirtschaftlichkeit und notwendiger Sicherheit zu erfolgen hat.[1145]

d) Haftungsfragen

aa) Haftung des Anbieters für Aufklärung

732 Die Anwender elektronischer Signaturen sind mit der neuen Technik noch nicht vertraut. Eine *Aufklärungspflicht* des Anbieters hinsichtlich der zu ergreifenden Sicherheitsmassnahmen (Auswahl einer geeigneten Signiereinheit, Geheimhaltung von PIN und Token, allenfalls Virenschutz, Sperrung des Zertifikats bei Kompromittierungsverdacht[1146]) ist damit zu bejahen.[1147]

bb) Haftung des Anbieters bei der Systemauswahl

733 Wie bei den herkömmlichen Legitimationssystemen trägt der Anbieter im Weiteren eine *Pflicht zur sorgfältigen Auswahl des Systems*. Dabei ist auf den Stand der Technik und die Wirtschaftlichkeit Rücksicht zu nehmen.[1148]

734 Zur Beurteilung der Frage, ob ein Verfahren dem Stand der Technik entspricht, dürften die Anforderungen des E-ZertES an anerkannte Zertifizierungsdiensteanbieter eine verhältnismässig wichtige Rolle spielen.[1149] Meines Erachtens sind zudem alle für einen bestimmten Zweck verfügbaren Techniken zu untersuchen und nicht etwa nur Signaturverfahren, zumindest sofern sie sowohl aus Sicht des Anbieters als auch aus Sicht des Kunden ähnliche Eigenschaften (Benutzerfreundlichkeit, Wirtschaftlichkeit u. dgl.) aufweisen. So ist etwa die bereits durch herkömmliche Verfahren (PIN/TAN) gebotene vergleichsweise hohe Sicherheit und Anwenderfreundlichkeit zu berücksichtigen, was bei Anwendungen mit hohen Sicherheitsbedürfnissen (wie E-Banking) den Einsatz von Klasse-2-Lesern nötig macht.[1150] Das geschilderte HBCI-Verfahren[1151] der deutschen Banken, welches auf Klasse-1-Geräten oder gar

---

1145 Vorne N 726; a. M. WERNER, 342, der indessen nicht weiter auf das Wesen des Anscheinsbeweises als Beweismassreduktion eingeht.

1146 Dazu etwa SPINDLER, Bankrecht I, 103 ff.

1147 Eingehend zum Inhalt der Aufklärungspflicht bei Code-Legitimation STEINMANN, 150 ff.; vgl. auch VON DER CRONE, 107.

1148 Vorne N 726.

1149 So auch WILDHABER, Signaturgesetze, 5.

1150 Softwaresigniereinheiten ermöglichen leichtes unbemerktes Ausspähen des Signierschlüssels durch bösartige Software (vorne N 64), was es ermöglicht, sogar unabhängig vom Computersystem des Kunden eine beliebige Zahl von Angriffen durchzuführen. Kommt ein Klasse-1-Kartenleser zum Einsatz, so muss der Angriff zwar durch auf das Kundensystem geladene Software durchgeführt werden, aber auch hier können, ist die PIN einmal ausgespäht, beliebig viele Angriffe ohne Interaktion des Kunden durchgeführt werden (vorne N 65, insbesondere FN 77). Erst ein Klasse-2-Kartenleser (mit separater Tastatur zur PIN-Eingabe) verlangt für jede Transaktion eine Interaktion des Kunden und entspricht damit bezüglich Sicherheit den PIN/TAN Systemen. Ungelöst bleibt indessen sowohl bei der PIN/TAN-Variante als auch beim Klasse-2-Leser das Präsentationsproblem (vorne N 55 ff.); SPINDLER, Bankrecht I, Rz 72.

1151 Homebanking Computer Interface; vorne N 147.

Softwaresigniereinheiten basiert, erfüllt daher m. E. diese Anforderungen an ein sorgfältig ausgewähltes System *nicht*.[1152]

735 Klasse-3-Kartenleser weisen nebst einer separaten Tastatur eine separate Anzeige auf, wodurch das Präsentationsproblem gelöst wird.[1153] Wird eine derartige Lösung eingesetzt, um Einzeltransaktionen zu unterzeichnen und nicht nur zur Anmeldung beim System (Fallgruppe 2b), kann gegenüber der PIN/TAN-Lösung um einiges höhere Sicherheit geschaffen werden. Sind Klasse-3-Systeme dereinst für den Massenmarkt tauglich und technisch sowie wirtschaftlich sinnvoll einsetzbar, dürfte zumindest für Hochsicherheitsanwendungen wie E-Banking der Einsatz derartiger Geräte auch anstelle des PIN/TAN-Verfahrens zu fordern sein.[1154] Kommen die Legitimationsmittel in der Öffentlichkeit zum Einsatz, sodass ein physisches Ausspähen der PIN durch unbeteiligte Dritte möglich wird (etwa am Geldautomat), so dürfte zudem – bei deren Verfügbarkeit – auch der Einsatz biometrischer Techniken nötig werden.[1155]

cc) Haftung des Signierschlüsselhalters

736 Die Haftungsordnung ergibt sich aus dem Rahmenvertrag, der dem Einsatz der Signatur zu Grunde liegt. Sieht dieser Vertrag vor, dass der Anbieter sich bei der Legitimationsprüfung auf gültige Signaturen verlassen darf, so haftet der Kunde grundsätzlich wie beschrieben auch für unverschuldete Fälschungen.

737 Eine durch den E-ZertES neu eingeführte gesetzliche Grenze bei der Übertragung der Haftung auf den Schlüsselhalter liegt in Art. 59a E-OR in Verbindung mit Art. 8 UWG.[1156] Nach Art. 8 UWG handelt unlauter, wer sich allgemeiner Geschäftsbedingungen bedient, die erheblich von der unmittelbar oder sinngemäss anwendbaren gesetzlichen Ordnung (im vorliegenden Fall von der Exkulpationsmöglichkeit nach Art. 59a E-OR) abweichen und geeignet sind, den Vertragspartner irrezuführen. Die bisher bereits gängigen Klauseln in E-Banking-Verträgen dürften jedoch kaum als irreführend zu bezeichnen sein, setzt ihre Anwendbarkeit doch schon nach geltendem Recht voraus, dass der Anbieter bei der Auswahl und Wartung des Systems sorgfältig vorgegangen ist.

1152 A.M. SPINDLER, Bankrecht I, Rz. 71, 93, der indessen übersieht, dass die Anweisung der Banken an die Nutzer, ihren Signierschlüssel nicht auf der Festplatte, sondern auf einem separaten Datenträger abzuspeichern und den Datenträger bzw. das Token nach der Benutzung aus dem Laufwerk bzw. Kartenleser zu entfernen, kaum zusätzliche Sicherheit schafft, weshalb HBCI um einiges unsicherer ist als das PIN/TAN-Verfahren; dazu schon vorne N 65, insbesondere FN 77. Zu ersten erfolgreichen Angriffen auf HBCI N 147, insbesondere FN 204.

1153 Etwa das Unterschieben von Dokumenten (bzw. einer gefälschten Maske zur Legitimation); vorne N 58 ff.

1154 Abwägend SPINDLER, Bankrecht I, Rz 72.

1155 Ähnlich Astrid ALBRECHT, zit. bei KREMPL, Finger, 62; BÜLLINGEN/HILLEBRAND, 342 f.

1156 Botschaft ZertES, 5709.

6. Signaturen mit ex-ante-Prüfung ohne Rahmenvertrag

a) Anwendungsfälle

Anwendungsfälle elektronischer Signaturen mit ex-ante-Prüfung, bei denen bereits der Erstkontakt auf digitalem Weg geknüpft wird, bei denen also kein Rahmenvertrag vorliegt, werden in Fallgruppe 3 zusammengefasst. Obwohl derartige Anwendungen vorderhand wohl nur selten vorkommen werden,[1157] waren sie es, die den Verfassern von E-ZertES und Signaturrichtlinie in erster Linie vorschwebten. 738

b) Beweisführung

aa) Basis des Anscheinsbeweises

Die ex-ante-Prüfung erlaubt in dieser Fallgruppe m.E. den Verzicht auf die Prüfung der gesamten Indizienkette und ihren Ersatz durch einen Anscheinsbeweis.[1158] Im Folgenden soll der Frage nachgegangen werden, welche Indizien oder Zusammenhänge durch diesen gedeckt sind, welche nicht, und welche als Basis für den Anscheinsbeweis neu nachzuweisen sind. 739

Signaturprüfung: Die Signatur muss auf einer anerkannten Signaturprüfeinheit ein positives Prüfresultat liefern. Das Prüfresultat kann selbstverständlich nicht Teil der ex-ante-Prüfung sein und ist daher zur vollen Überzeugung des Gerichts nachzuweisen. 740

Die *Anerkennung des Zertifizierungsdiensteanbieters* ist als Basis des Anscheinsbeweises voll nachzuweisen. Sie lässt sich anhand der von der Akkreditierungsstelle publizierten Liste der anerkannten Zertifizierungsdiensteanbieter[1159] und anhand des Wurzelzertifikats feststellen, das zur Überprüfung des Zertifikats des Unterzeichners verwendet wird. Das Wurzelzertifikat muss nachweislich vom Anbieter stammen, d.h. das Gericht oder der Sachverständige muss dieses aus sicherer Quelle beziehen oder zumindest die Übereinstimmung von dessen Hashwert mit dem durch den Zertifizierungsdiensteanbieter auf sicherem Weg publizierten Hashwert überprüfen.[1160] 741

Sicherheit der kryptographischen Mechanismen: Anerkannte Zertifizierungsdiensteanbieter sind verpflichtet, nur als sicher anerkannte Kryptographie (Signier- und Hashalgorithmus) einzusetzen. Ist der Anbieter anerkannt, kann das Gericht demnach prima facie von der Sicherheit der Kryptographie ausgehen. 742

Sichere Zertifizierung: Das Erzeugen der Zertifikate hat nach einem detailliert geregelten Vorgehen zu erfolgen. Auch dieses wird durch die Anerkennungsstelle im voraus überprüft und kann daher prima facie als gegeben betrachtet werden. 743

1157 Vorne N 221 ff.
1158 Vorne N 683 ff.
1159 Vorne N 522.
1160 Vorne N 120 ff.

744 *Identifikation des Schlüsselhalters:* Die Identität des Schlüsselhalters wird durch den Zertifizierungsdiensteanbieter anhand eines amtlichen Ausweises überprüft und die entsprechenden Belege werden archiviert.[1161] Die ex-ante-Prüfung umfasst auch die Kontrolle, dass der Zertifizierungsdiensteanbieter im Stande ist, dieses Prozedere sicher durchzuführen, und die Akten archiviert. Wünschenswert wäre im Übrigen eine Unterzeichnung des Zertifizierungsantrages durch Schlüsselhalter vor den Augen eines Mitarbeiters der Registrierungsstelle. Dies ermöglichte es, die Zertifizierung später eindeutig nachzuweisen.[1162]

745 Aus Gründen der Prozessökonomie, und weil auch der durch den Anscheinsbeweis Belastete angebliche Unterzeichner den Gegenbeweis aufgrund der Archivierung sehr leicht erbringen kann, rechtfertigt es sich aber m. E., prima facie von einer korrekten Überprüfung auszugehen.

746 *Kontrolle des Halters über den Signierschlüssel:* Der Zertifizierungsdiensteanbieter hat zu überprüfen, ob der Schlüsselhalter über eine sichere Signiereinheit verfügt.[1163] Das Gericht kann demnach prima facie vom Einsatz eines derartigen Gerätes ausgehen.[1164] Kommt dennoch ein unsicheres Gerät zum Einsatz, haftet der Schlüsselhalter jedenfalls nach Art. 59a E-OR.[1165]

747 Nicht gelöst wird durch derartige Geräte die Gefahr des physischen Ausspähens des Passwortes.[1166] Wie beschrieben muss jedoch gerade insoweit der Anscheinsbeweis zulässig sein.[1167]

748 *Gültigkeit des Zertifikats zum Signierzeitpunkt:* Ist das Zertifikat zum Zeitpunkt seiner Beurteilung durch das Gericht weder gesperrt noch abgelaufen (dies ergibt sich aus dem Ablaufdatum des Zertifikats bzw. der CRL und sollte durch die Signaturprüfeinheit angezeigt werden), war dieses auch zum Signierzeitpunkt gültig.[1168] Ist das Zertifikat indessen mittlerweile abgelaufen oder gesperrt, ist nachzuweisen, dass die Unterschrift noch zuvor gesetzt wurde.[1169] Dies kann durch Zeitstempel leicht geschehen; die Zeitstempelung eingehender Nachrichten ist zudem eine für den Empfänger *zumutbare Massnahme zur Beweissicherung*.[1170] Das Gegenteil hingegen,

---

1161 Vgl. etwa die Ausführungsbestimmungen zur ZertDV, 38.

1162 Die Unterzeichnung wird zwar durch ZertDV und Ausführungsbestimmungen nicht verlangt, aus Gründen der Beweissicherheit dürften die Zertifizierungsdiensteanbieter dennoch regelmässig auf ihr bestehen.

1163 Derzeit kommen hierzu vor allem Klasse-3-Kartenleser in Verbindung mit sicheren kryptographischen Tokens in Frage; vorne N 539.

1164 Dies rechtfertigt sich auch dann, wenn der Schlüsselhalter im Einzelfall ein anderes Gerät einsetzte. Die Verantwortung für den Einsatz eines sicheren Gerätes kann – nach gehöriger Information und Dokumentation durch den Zertifizierungsdiensteanbieter – dem Schlüsselhalter aufgebürdet werden.

1165 Hinten N 755 ff.

1166 Vorne N 70.

1167 Vorne N 673 ff., 682.

1168 Die Definition des Beginns einer Gültigkeitsdauer ist sinnlos; vorne N 107, insbesondere FN 144.

1169 Vorne N 187 ff.

1170 Allgemein zu Zeitstempeln vorne N 172 ff.

also ein nach der Sperrung oder der Revokation liegender Signierzeitpunkt, ist kaum nachweisbar, weil der Schlüsselhalter ja gerade bei einer Fälschung keine Möglichkeit hätte, einen Zeitstempel zu setzen. Der Anscheinsbeweis für die Gültigkeit des Zertifikats zum Signierzeitpunkt muss demnach *ausgeschlossen* sein.

749 Fraglich ist in diesem Zusammenhang, ob der Anscheinsbeweis für die Echtheit einer Signatur allenfalls auch bei einer auf einem zum Signierzeitpunkt abgelaufenen oder gesperrten Zertifikat beruhenden Signatur geführt werden kann; denn einerseits hat der Ablauf eines Zertifikats nicht zwingend die Kompromittierung des Signierschlüssels zur Folge, und andererseits kann eine Sperrung eines Zertifikats auch ohne den Anlass einer Schlüsselkompromittierung erfolgen.

750 Aus Gründen der Rechtssicherheit ist hier m. E. eine klare Grenze zu ziehen: Auch wenn der Schlüsselhalter die Grundlagen des Anscheinsbeweises nur zu erschüttern braucht, kann es nicht angehen, dass er – weil er vielleicht zufällig die für die Erschütterung des Anscheinsbeweises nötigen Tatsachen nicht darzutun vermag – trotz Sperrung oder Ablaufs seines Zertifikats plötzlich eine Fälschung gegen sich gelten lassen muss. Schliesslich bemerkt der auf die Signatur vertrauende Dritte den Ablauf des Zertifikats bei der Signaturprüfung sofort und kann die Signatur gleich zurückweisen, wie wenn sie mit einem ungültigen Signierschlüssel erstellt worden wäre. Die Zulassung einer Signatur zum Anscheinsbeweis muss daher strikte an den Nachweis gebunden sein, dass der Signierzeitpunkt vor dem Ablauf oder der Sperrung des entsprechenden Zertifikats lag.

751 *Korrekte Dokumentenpräsentation:* Signiereinheiten werden durch die Anerkennungsstelle vor der Zulassung geprüft. Insoweit besteht jedoch das Problem, dass derzeit noch keine Signiereinheiten auf dem Markt sind, die eine wirklich sichere Präsentation grösserer Dokumente ermöglichten.[1171] Wie beim Beweis der alleinigen Kontrolle des Signierschlüssels durch den Halter muss aber gerade auch hier der Anscheinsbeweis zulässig sein, will man elektronische Signaturen nicht grundsätzlich in Frage stellen.[1172]

bb) Zumutbare Massnahmen des Beweisführers

752 Um zum Anscheinsbeweis zugelassen zu werden, muss der Beweisführer die ihm zumutbaren Massnahmen zur Beweissicherung ergreifen. In Fallgruppe 3 hat der Beweisführer mit dem Betrieb der Signiereinheit gar nichts zu tun, weshalb er auch keine Verantwortung für deren Funktion trägt. Einzig die Zeitstempelung der eingehenden Nachricht zum Nachweis des Signierzeitpunktes ist Voraussetzung für den Anscheinsbeweis.[1173]

1171 Vorne N 61.
1172 N 673 ff.
1173 Soeben N 748.

cc) Zusammenfassung: Darzulegende Indizien

753 Ist demnach zur vollen Überzeugung des Gerichts erwiesen,

- dass eine Signatur bei der Prüfung mit einer gesetzeskonformen Prüfeinheit ein gültiges Resultat liefert,
- dass für den Prüfschlüssel ein qualifiziertes Zertifikat im Sinne von Art. 7 E-ZertES existiert,[1174]
- dass der Zertifizierungsdiensteanbieter zum Signierzeitpunkt anerkannt war, und
- dass das Zertifikat zum Signierzeitpunkt weder abgelaufen noch gesperrt war,

kann m.E. von der Echtheit der Signatur ausgegangen werden, d.h. die Beweisführungslast wechselt auf den angeblichen Unterzeichner des Dokumentes.

dd) Widerlegung des Anscheinsbeweises

754 Der Unterzeichner hat selbstverständlich die Möglichkeit, den Anscheinsbeweis zu erschüttern, indem er Tatsachen darlegt, die für den konkreten Fall einen vom typischen Gang der Dinge abweichenden Ablauf als ernsthaft möglich erscheinen lassen.[1175] Faktoren, die abstrakt geeignet sind, den Missbrauch zu ermöglichen, müssen hierzu ausreichen.[1176] Gelingt dieser Nachweis, wechselt die Beweisführungslast wieder auf die Seite des auf die Signatur vertrauenden Dritten. Dieser hat nun für den erschütterten Teil der Indizienkette (aber nur für diesen) den *vollen* Beweis zu erbringen.

c) Haftung des Signierschlüsselhalters[1177]

aa) Art. 59a E-OR

755 De lege lata liesse sich wohl auch für Signaturen mit Anbieteranerkennung nur mit Mühe eine Sorgfaltspflicht des Schlüsselhalters begründen.[1178] Der Bundesrat schlägt daher mit Art. 59a E-OR eine Norm als gesetzliche Grundlage einer solchen Haftung vor.

1174 Nur ein solches liefert Gewähr für die kryptographische Sicherheit. Die Beurteilung der Frage, ob ein qualifiziertes Zertifikat vorliegt, hängt allein von dessen Inhalt ab; Art. 2 Bst. f E-ZertES i.V.m. Art. 7 E-ZertES. Dieser kann mittels der Signaturprüfeinheit einfach untersucht werden.

1175 Vorne N 624.

1176 SPINDLER, Bankrecht I, Rz 73; denkbar wäre etwa der gutachterliche Nachweis, dass sich auf dem System des Kunden ein Virus befand, der unter Ausnutzung des Präsentationsproblems Signaturen fälscht (wobei sich aber immerhin die Frage stellt, ob der Kunde diesen schuldhaft nicht erkannt hat; sogleich N 758). Gerade hinsichtlich des Präsentationsproblems dürften die Anforderungen an einen solchen Nachweis nicht zu hoch gesteckt werden; ROSSNAGEL, Recht, 1826. Denkbar sind selbstverständlich auch von der Signatur unabhängige Umstände, insbesondere solche, die den Empfänger der Nachricht auch bei einer Handunterschrift zu einer Überprüfung hätten anhalten sollen, wie Transaktionen mit aussergewöhnlich hohem Wert u.dgl.

1177 Zur Haftung der Zertifizierungsdiensteanbieter vorne N 542 ff.

1178 Vgl. schon vorne N 694 ff.

Der Schlüsselhalter soll nach dieser Norm gegenüber einem auf seine Signatur vertrauenden Dritten haften, sofern dieser sich auf ein gültiges qualifiziertes Zertifikat eines anerkannten Zertifizierungsdiensteanbieters verlassen hat. Er wird bei einem Missbrauch nicht im Sinne einer Stellvertretung vertraglich gebunden (Haftung für das positive Interesse), sondern haftet für den Vertrauensschaden des auf die Signatur vertrauenden Dritten (negatives Interesse).[1179] Abs. 3 weitet die Haftung auf Fälle aus, in denen der Schlüssel wissentlich und willentlich Dritten anvertraut wurde; eine Exkulpation bei gehöriger Auswahl, Instruktion und Überwachung für eine Hilfsperson ist demnach ausgeschlossen.[1180] 756

Ein mangelhaftes Zertifikat, d.h. eines, das die von Art. 7 E-ZertES verlangten Eigenschaften nicht aufweist, kann keine Rechtswirkungen im Sinne von Art. 59a E-OR nach sich ziehen.[1181] 757

Die Haftung des Schlüsselhalters entfällt nach Art. 59a Abs. 2 Teilsatz 1 E-OR, wenn er beweist, dass er die nach den Umständen nötigen Vorkehren zur Geheimhaltung seines Schlüssels getroffen hat; was darunter zu verstehen ist, regelt der Bundesrat in den Ausführungsbestimmungen.[1182] 758

Nach Teilsatz 2 der genannten Bestimmung entfällt die Haftung, wenn der Schlüsselhalter beweist, dass er mangels Urteilsfähigkeit nicht zu Verantwortung gezogen werden kann.[1183] Die Beschränkung der Ausnahmen auf Urteilsunfähigkeit ist jedoch m.E. zu eng – der Haftungsausschluss nach dem ersten Teilsatz müsste etwa auch bei Willensmängeln greifen. Schliesslich stellt sich aber ohnehin die Frage, ob nicht das geltende Recht derartige Fälle bereits ausreichend abdeckt und damit auf Teilsatz 2 überhaupt verzichtet werden könnte.[1184] 759

Unklar ist im Weiteren, weshalb der Entwurf eine Beschränkung der Haftung auf Signaturen vornimmt, die auf qualifizierten Zertifikaten *anerkannter* Anbieter beruhen. Die Vorstellung, dass sich im Bereich offener Benutzergruppen nebst anerkannten Zertifizierungsdiensteanbietern auch solche ohne Anerkennung etablieren könnten, wie sie der kombinierten ex-post/ex-ante-Regelung der EU[1185] und dem schweizerischen Prinzip der freiwilligen Anerkennung[1186] eigentlich Pate stand, wird durch diese Regelung sabotiert, weil damit die entsprechenden Zertifikate in offenen Benutzergruppen ihre Vertrauenswürdigkeit verlieren. Im Weiteren kontrastiert die Regelung mit Art. 16 Abs. 1 E-ZertES, der festlegt, dass auch Anbieter qualifizierter Zertifikate *ohne Anerkennung* bei Verletzung der durch das Gesetz aufgestellten 760

1179 Art. 59a Abs. 1 E-OR; vgl. auch SCHLAURI, Basistechnologie, 100f. (die Artikelnummern in der Grafik beziehen sich versehentlich noch auf den VE-BGES).
1180 Botschaft ZertES, 5708f.; RAGGENBASS, B47.
1181 Botschaft ZertES, 5696; JACCARD, Projet, 81.
1182 Art. 59a Abs. 4 E-OR; vgl. auch JACCARD, Projet, 82.
1183 Vgl. Botschaft ZertES, 5708.
1184 So auch JACCARD, Projet, 82.
1185 Vorne N 293, 370 ff.
1186 Vorne N 286, 512.

Pflichten haften.[1187] Es ist daher zu hoffen, dass Art. 59a E-OR in der Endfassung noch auf qualifizierte Zertifikate nicht anerkannter Anbieter ausgedehnt wird.

bb) Überprüfung der Gültigkeit des Zertifikats

761 Mehrfach wurde gefordert, es sei eine Obliegenheit des auf ein Zertifikat vertrauenden Dritten in das Gesetz aufzunehmen, das Zertifikat beim Eingang der Nachricht auf Gültigkeit zu überprüfen.[1188] Der E-ZertES sieht denn auch tatsächlich als neue, zusätzliche Haftungsvoraussetzung vor, dass der Dritte sich auf ein *gültiges* Zertifikat verlassen hat.[1189] Aus Gründen der Rechtssicherheit ist diese Regelung zu begrüssen, denn der Signierschlüsselhalter darf nicht riskieren, trotz Sperrung seines Zertifikats gegenüber einem Dritten zu haften, weil dieser dessen Gültigkeit nicht überprüft hat. Sie entspricht zudem auch Art. 11 des UNCITRAL-Modellgesetzes über elektronische Signaturen.[1190]

cc) Überprüfung des Inhalts des Zertifikats

762 Die Botschaft geht davon aus, dass der Zertifikatsinhalt (besonders die haftungsbeschränkenden Klauseln[1191]) bzw. die entsprechenden Register (Certificate Repository und Certificate Revocation List) gegenüber beim Empfänger nicht als bekannt vorausgesetzt werden können, es sei denn, eine Obliegenheit zur Untersuchung ergäbe sich aus Treu und Glauben. Die Wirkung entsprechender Einträge entspräche ungefähr derjenigen des Eigentumsvorbehaltsregisters: Nur kommerziell tätige Adressaten trügen generell eine Obliegenheit zur Überprüfung.[1192] Diese Regelung scheint auf den ersten Blick sinnvoll, weil etwa beim Lesen von E-Mail das Zertifikat nur durch einige zusätzliche Mausklicks angezeigt werden kann, was oft unterbleiben dürfte.[1193]

763 Genau besehen wird auf diese Weise indessen die Wirksamkeit der im Zertifikat enthaltenen haftungsbeschränkenden Klauseln in Frage gestellt, denn gerade bei einer Fälschung haben Schlüsselhalter und Zertifizierungsdiensteanbieter keine Möglichkeit, den auf eine Signatur vertrauenden Dritten auf einem weiteren Weg (etwa durch einen «Disclaimer» am Ende der signierten Nachricht) auf die Haftungsbeschränkungen aufmerksam zu machen. Meines Erachtens ist daher eher von einer *generellen* Obliegenheit des auf eine Signatur vertrauenden Dritten zur Überprüfung des Zertifikatsinhaltes auszugehen. Nicht zuletzt entspräche dies auch Art. 11(b)(ii) des UNCITRAL-Modellgesetzes über elektronische Signaturen.[1194]

1187 Vorne N 543.
1188 So etwa Beat LEHMANN und Bruno WILDHABER, zit. bei SCHLAURI, Bundesgesetz, 363.
1189 Art. 16 Abs. 1 E-ZertES; Art. 59a E-OR; unklar JACCARD, Projet, 81.
1190 Vorne N 347.
1191 Vorne N 534 f.
1192 Botschaft ZertES, 5689.
1193 So auch noch SCHLAURI, Basistechnologie, 99.
1194 Zum MLES vorne N 347; gl. M. offenbar auch die Begründung deutschen SigG 01, 25.

7. Signaturen mit ex-ante-Prüfung und Rahmenvertrag

a) Anwendungsfälle

764 Die Anerkennung eines Zertifizierungsdiensteanbieters bürgt für hohe Sicherheit der Zertifikate und vereinfacht das Beweisverfahren. Zudem ermöglicht sie den Abschluss schriftformbedürftiger Rechtsgeschäfte. Es ist damit unter Umständen sinnvoll, trotz Bestehens eines Rahmenvertrages Signaturen mit Anbieteranerkennung einzusetzen (Fallgruppe 4).

b) Beweisführung

765 Wie bei den Fallgruppen 2a und 2b ist auch hier bei Vorliegen einer privatautonomen Legitimationsordnung nur zu beweisen, dass aus der Sicht des Systembetreibers eine gültige Legitimation erfolgte, nicht aber, dass diese tatsächlich auf eine Willensäusserung des Schlüsselhalters zurückzuführen ist.[1195]

c) Haftungsfragen

aa) Haftung des Systembetreibers

766 Anders als bei Signaturen ohne ex-ante-Prüfung kann der Systembetreiber in dieser Fallgruppe davon ausgehen, dass der Schlüsselhalter bereits durch den Zertifizierungsdiensteanbieter über die zur Geheimhaltung des Schlüssels notwendigen Massnahmen informiert wurde.[1196] Eine zusätzliche Aufklärungspflicht über diese Risiken[1197] dürfte sich daher erübrigen.

767 Hinzu kommt, dass Signaturverfahren mit ex-ante-Prüfung als dem Stand der Technik entsprechend gelten können. Dem Systembetreiber kann daher bei der Wahl eines anerkannten Verfahrens kaum eine unsorgfältige Systemauswahl vorgeworfen werden. Vorbehalten bleibt die Sicherheit des Serversystems des Anbieters (Nachweis der Nichtmanipulierbarkeit).[1198]

bb) Haftung des Schlüsselhalters

768 Der Wortlaut von Art. 59a E-OR differenziert nicht zwischen Fällen mit und ohne Rahmenvertrag, weshalb er auch in den ersteren Fällen von Bedeutung sein dürfte.[1199] Nichts spricht jedoch dagegen, diese gesetzliche Risikoverteilung im geschilderten Sinne durch eine parteiautonome Legitimationsordnung zu modifizieren.[1200]

1195 Vgl. vorne N 727 ff.
1196 Art. 9 Abs. 2 E-ZertES; vorne N 528.
1197 Vorne N 732.
1198 Wird – analog Fallgruppe 2b – jede einzelne Transaktion signiert, so sind die Anforderungen an das Serversystem indessen relativ tief; vorne N 712, 730.
1199 Zu Art. 59a E-OR vorne N 755 ff.
1200 Vgl. auch Botschaft ZertES, 5709.

B. Rekognition

769 Bezeichnet ein Erklärender einen Text als seinem eigenen Willen entsprechend, so spricht man von *Rekognition* oder *Anerkennung*. Die Rekognition ist nebst der Echtheit einer Urkunde ebenfalls Voraussetzung, um diese einer Person als Willenserklärung anrechnen zu können.[1201]

770 Ob ein Text als anerkannt gelten kann, ergibt sich allerdings nicht in erster Linie anhand der Sachlage zum Zeitpunkt des Setzens der Signatur, sondern daraus, ob der Empfänger eine Handlung als Rekognitionshandlung verstehen durfte und musste. Es handelt sich dabei um einen Anwendungsfall des Vertrauensprinzips[1202] und mithin um eine Rechts- und nicht um eine Tatfrage.[1203] Wie noch zu zeigen sein wird, darf der Empfänger indessen nur bei qualifizierten elektronischen Signaturen ohne weiteres von der Rekognition ausgehen.[1204]

771 Wird eine Willenserklärung unter Abwesenden abgegeben, so ist zu ihrer Rekognition nebst der Unterzeichnung auch ihre Begebung (Inverkehrsetzung) nötig. Für die Begebung von Papierurkunden muss, wie geschildert, der Anscheinsbeweis zulässig sein, sofern sich die Urkunden einmal im Umlauf befinden.[1205] Dies kann für digitale Dokumente nicht anders sein.

1201 Etwa ZK-SCHÖNENBERGER/JÄGGI, N 36 zu Art. 11 OR; eingehender zur Rekognitionsfunktion der Unterschrift hinten N 836 ff.
1202 Vgl. vorne N 652; hinten N 844.
1203 BGE 121 III 123; VOGEL/SPÜHLER, 13 N 166.
1204 Hinten N 844.
1205 Vorne N 653.

§ 11 Prozessuale Anerkennung

I. Fragestellung

Nach Art. 10 ZGB darf das kantonale Prozessrecht dort, wo das Bundesrecht für die Gültigkeit eines Rechtsgeschäfts keine besondere Form vorschreibt, auch für die Beweisbarkeit des Rechtsgeschäfts eine solche nicht vorschreiben. Die meisten Rechtsgeschäfte können formfrei und damit auch auf elektronischem Weg geschlossen werden.[1206] Elektronisch gespeicherte Dokumente, gleich ob signiert oder nicht, müssen daher zum Beweis zugelassen werden.[1207] 772

Elektronische Signaturen können de lege lata allerdings nach überwiegender Ansicht nur als *Augenscheinsobjekte* Eingang in das Beweisverfahren finden, nicht jedoch als Urkunden.[1208] Daraus ergeben sich im Vergleich zur Handunterschrift gewisse Nachteile; so sind elektronisch signierte Dokumente beispielsweise nicht als provisorische Rechtsöffnungstitel im Sinne von Art. 82 Abs. 1 SchKG zugelassen und können teilweise auch im Sühnverfahren oder in Verfahren mit ausschliesslicher Zuständigkeit des Friedensrichters nicht eingebracht werden.[1209] 773

Es fragt sich daher, ob und allenfalls auf welche Weise elektronisch signierte Dokumente wie herkömmlich unterschriebene Urkunden im Prozess anerkannt werden könnten. 774

II. Beweis mittels digitaler Signatur de lege lata

A. Fragestellung

Eine digitale Signatur ist – technisch gesehen – bloss Anhängsel eines normalen Dokuments[1210] und kann daher bei der Beweiswürdigung auch ganz ausser Acht gelassen werden, falls sich das Gericht etwa im Rahmen eines auf Urkunden beschränkten Verfahrens nicht in der Lage sieht, ihre Echtheit zu beurteilen. Sofern also unsignierte elektronisch gespeicherte Dokumente zum Urkundenbeweis zugelassen sind,[1211] so müssen dies signierte Dokumente genauso sein, wenn man die Signatur ausser Acht lässt. 775

1206 Eingehend hinten N 800 ff.
1207 Botschaft ZertES, 5682.
1208 Eingehend sogleich N 777 f.
1209 Vorne N 662 ff.
1210 Vorne N 43 ff.
1211 Vorne N 635 ff.

776 Soll jedoch die digitale Signatur selbst als Beweismittel eingesetzt werden, stellt sich die Frage, ob es sich bei ihr noch um einen Urkundenbestandteil handelt (das digital signierte Dokument also als normale unterzeichnete Urkunde betrachtet werden kann), oder ob sie ein vom Urkundentext gesondert zu betrachtendes Augenscheinsobjekt darstellt.

B. Elektronische Einreichung

777 Die Handhabung signierter elektronischer Dokumente ist bedeutend aufwändiger als die Handhabung unsignierter elektronischer Dokumente oder gar von Papierurkunden: Die Gerichte dürften vorläufig wohl weder die technischen Möglichkeiten noch das Know-how für die Überprüfung digitaler Signaturen haben.

778 Die einfache Handhabung ist aber gerade der Grund für die beschriebene Privilegierung der Urkunde gegenüber den anderen Beweismitteln.[1212] De lege lata dürfte damit eine Zulassung digital signierter Dokumente zum Urkundenbeweis ausgeschlossen sein. Die Signatur ist separat von der Urkunde als Augenscheinsobjekt zu beurteilen, was derzeit aufgrund der divergierenden Sicherheitsniveaus und der Komplexität der vorhandenen Systeme regelmässig Sachverständigengutachten notwendig macht.[1213]

C. Einreichung in ausgedruckter Form

779 GASSER[1214] plädiert für die Anerkennung ausgedruckter digital signierter Dokumente als provisorische Rechtsöffnungstitel (und damit selbstredend auch als Urkunden), thematisiert dabei jedoch die Sicherheit eines derartigen Ausdruckes nicht. Ein solcher Ausdruck besteht indessen nur aus dem signierten Text und einem durch das E-Mail-Programm beigefügten Symbol, welches das Vorliegen einer gültigen Signatur signalisiert.[1215] Die eigentliche Signatur[1216] wird indessen nicht gedruckt; weil die Signatur nur mit Computerhilfe überprüfbar ist, wäre dies jedoch auch nicht sinnvoll.[1217]

780 Es ist ein Leichtes, mit einer Bildbearbeitungssoftware den Ausdruck des Symbols für eine digitale Signatur nachzuahmen. Der Ausdruck eines digital signierten Dokumentes entspricht damit einem nicht unterzeichneten Papierdokument: Er ist zwar zum Urkundenbeweis zugelassen, der Anscheinsbeweis hinsichtlich der Echtheit des

---

1212 Dazu N 662 ff.

1213 Gl. M. BITZER/HAMMER, 623; BIZER/HERDA, 24; OBERHOLZER, Digitale Signatur, 444; ROSSNAGEL, Sicherheitsvermutung, 3314 f.; bezüglich der Rechtsöffnung BJ, Gutachten, 451; a.M. KILIAN, 609.

1214 GASSER, 93.

1215 Vergleichbar mit Darstellung 5 auf Seite 32.

1216 Vgl. Darstellung 6 auf Seite 35.

1217 HAMMER/BIZER, 690.

Dokumentes und der Erklärungsabgabe durch den Aussteller ist indessen nicht gegeben.[1218]

D. Einsatz als provisorischer Rechtsöffnungstitel

781 Digitale Signaturen sind de lege lata nur zum Augenscheinsbeweis zugelassen. Vorgelegt werden kann daher nur (aber immerhin) das elektronische Dokument ohne Signatur – sofern vom kantonalen Recht zugelassen, sogar in elektronischer Form und nicht nur ausgedruckt.[1219] Elektronisch signierte Dokumente sind demnach gleich zu behandeln wie unsignierte elektronische Dokumente[1220] und ohne Anerkennung durch den Schuldner de lege lata nicht als Rechtsöffnungstitel tauglich.[1221]

III. Beweis mittels digitaler Signatur de lege ferenda

A. Allgemeines

782 Gemäss Botschaft zum ZertES soll eine zivilrechtliche Gleichstellung der qualifizierten elektronischen Signatur auch eine Anerkennung in all denjenigen Fällen zur Folge haben, in denen sich Normen anderer Erlasse explizit oder implizit auf die Schriftlichkeitsvorschriften des OR beziehen, und zwar sowohl im kantonalen Recht als auch im Bundesrecht. Voraussetzung soll immerhin sein, dass die Gerichte mit der zur Überprüfung von Signaturen nötigen *Infrastruktur* ausgestattet sind. Elektronisch signierte Dokumente sollen diesfalls etwa auch im Rahmen eines Rechtsöffnungsverfahrens nach Art. 82 Abs. 1 SchKG zur Anwendung kommen können.[1222]

783 Sind bereits unsignierte elektronische Dokumente nach dem anwendbaren Zivilprozessrecht zum Urkundenbeweis zugelassen[1223] und verfügt ein Gericht über Infrastruktur und Know-how, welche ihm eine einfache Überprüfung auch der Signatur ermöglichen, so spricht m. E. in der Tat nichts gegen eine Anerkennung auch signierter Dokumente als Urkunden.[1224]

1218 Vorne N 658.
1219 Vorne N 775; zur Zulassung elektronischer Dokumente zum Urkundenbeweis N 635 ff.
1220 Dazu vorne N 663 ff.
1221 Vgl. auch Botschaft ZertES, 5688; BJ, Gutachten, 451, 464 f.; PESTALOZZI/VEIT, 602.
1222 Botschaft ZertES, 5688; LEGLER, E-Commerce, FN 30; abwartend noch BJ, Gutachten, 465.
1223 Vorne N 635 ff.
1224 Anders ist die Situation in *Deutschland*; dazu vorne N 461 oder etwa ROSSNAGEL, Sicherheitsvermutung, 3319 f.

B. Formatproblem

784 Der elektronische Verkehr mit Gerichten kann unterteilt werden in Dokumente, die erst zur Kommunikation mit dem Gericht verfasst werden (beispielsweise Klageschriften) und solche, die als Beweismittel dienen (etwa Vertragsurkunden, Quittungen u. dgl.). Während bei Ersteren die Möglichkeit besteht, Dokumentenformate gesetzlich festzulegen, was den Empfang und die Überprüfung der Dokumente stark vereinfacht,[1225] ist bei Letzteren mit einer Vielzahl von Dokumentenformaten zu rechnen, weil die Rechtsunterworfenen ihre Dokumentenformate (und damit die ganze Softwareausrüstung) kaum an der Infrastruktur der Gerichte ausrichten werden.

785 Zur Überprüfung von Signaturen muss nicht nur eine Signaturprüfeinheit vorhanden sein, sondern auch Software zur Darstellung der signierten Dokumente. Von den Gerichten zu verlangen, elektronisch signierte Dokumente beliebigen Formates entgegenzunehmen, hiesse daher, diese zur vorsorglichen Anschaffung einer Vielzahl von Softwareprodukten und entsprechender Infrastruktur zu zwingen.

C. Fehlende Auslastung der Prüfinfrastruktur

786 Erste überzogene Erwartungen an die Verbreitungsgeschwindigkeit elektronischer Signaturen mussten in letzter Zeit stark relativiert werden. Die Verbreitung elektronischer Signaturen im Rechtsverkehr dürfte vielmehr noch länger auf sich warten lassen.[1226] Es wäre m.E. aus dieser Perspektive verfrüht, die Gerichte sofort mit Prüfinfrastruktur auszurüsten und das Personal entsprechend zu schulen.

787 Eine Ausstattung der Gerichte mit Prüfinfrastruktur dürfte vielmehr nur dann sinnvoll sein, wenn gleichzeitig die Möglichkeit geschaffen wird, dass Rechtsschriften durch regelmässig mit dem Gericht verkehrende Personen wie beispielsweise Anwälte elektronisch signiert einreichen werden können (wie dies in der Revision der Bundesrechtspflege vorgesehen ist).[1227] Doch auch dann ist das geschilderte Formatproblem noch nicht gelöst: Während gängige Dokumentenformate akzeptiert werden könnten, müssten zur Überprüfung unüblicher Formate weiterhin Dritte hinzugezogen werden.

D. Konformitätsbestätigung als Lösungsvorschlag

1. Konzept

788 Eine Lösung für das Infrastruktur- und Formatproblem läge m.E. zumindest für ZertES-konforme Signaturen in einem *Zwischenschritt* bei der Einreichung elektro-

---

1225 Botschaft zur Totalrevision der Bundesrechtspflege, 4266.
1226 Eingehend § 5.
1227 Vorne N 506 ff.

nisch signierter Dokumente: Für den Fall, dass ein Gericht ein bestimmtes Dokumentenformat nicht akzeptieren kann oder gar nicht über die zur Überprüfung elektronischer Unterschriften notwendige Ausrüstung verfügt, könnte eine entsprechend ausgestattete vertrauenswürdige Fachstelle (vorzugsweise wohl ein Notar,[1228] allenfalls auch eine speziell hierfür geschaffene staatliche oder staatlich anerkannte Stelle) die Signatur überprüfen und dem Gericht einen entsprechenden Bericht erstatten. Dieser müsste in einer vom Gericht lesbaren Form (sei es auf Papier, sei es elektronisch signiert in einem dem Gericht bekannten Dokumentenformat) eingereicht werden und diejenigen Tatfragen abdecken, die das Gericht nicht selbst zu prüfen im Stande ist (Inhalt des signierten Dokumentes, positives Prüfresultat einer gesetzeskonformen Signaturprüfeinheit,[1229] Vorliegen eines qualifizierten Zertifikats eines zum Signierzeitpunkt anerkannten Zertifizierungsdiensteanbieters[1230] sowie allenfalls Gültigkeit von Zeitstempeln zum Nachweis der Gültigkeit des Zertifikats zum Signierzeitpunkt[1231]).[1232]

789 Eine derartige Lösung war im Vorentwurf zum BGES tatsächlich vorgesehen. Die Akkreditierungsstelle hätte nach Art. 21 VE-BGES die Gesetzeskonformität einer elektronischen Signatur in einer *Konformitätsbestätigung* bestätigen sollen. Die Motivation bestand laut Begleitbericht darin, die derzeit noch fehlende Infrastruktur der Gerichte zu ersetzen; das Formatproblem wurde nicht erwähnt.[1233] Die Bestimmung wurde im E-ZertES allerdings wieder gestrichen.[1234]

2. Konformitätsbestätigung als beglaubigte Kopie

790 Wird die Konformitätsbestätigung durch eine vom Staat mit der Aufgabe der Herausgabe derartiger Bestätigungen in der dafür geforderten Form und im vorgesehenen Verfahren beauftragten Stelle ausgegeben, handelt es sich um eine öffentliche Urkunde.[1235] Meines Erachtens kann man diese als *beglaubigte Kopie* des elektronisch signierten Dokumentes betrachten, weil sie – gleich wie die beglaubigte Kopie eines Papierdokumentes – dessen Inhalt wiedergibt und eine Aussage über die Prüfung von dessen Echtheit macht.[1236] Beglaubigte Kopien haben prozessrechtlich die gleichen Wirkungen wie die entsprechenden Originale. Ihr Inhalt (d.h. was durch die Urkundsperson überprüft wurde) wird nach Art. 9 ZGB gesetzlich als wahr vermu-

---

1228 So etwa auch LEGLER, Notariat, 141.

1229 Dazu vorne N 117 ff., 540.

1230 Erst die ex-ante-Prüfung nach E-ZertES erlaubt dem Gericht, auch ohne Sachverständigengutachten von der Echtheit der Signatur auszugehen; vorne N 685.

1231 Vorne N 172 ff., 187 ff.

1232 Vgl. vorne N 753.

1233 Begleitbericht VE-BGES, 25 f.

1234 Der Grund der Streichung bleibt im Dunkeln. Das Argument jedenfalls, aufgrund der neu eingeführten Pflicht der Zertifizierungsdiensteanbieter zur Ausstellung von Zeitstempeln erübrige sich eine Konformitätsbestätigung (Botschaft ZertES, 5699) verkennt den ursprünglichen Grund der Einführung, die fehlende Infrastruktur der Gerichte; vgl. aber N 792.

1235 Dazu N 828 ff.

1236 Vgl. etwa BRÜCKNER, N 3388; soeben N 788.

tet.[1237] Die Konformitätsbestätigung wäre damit als Surrogat des elektronischen Originals *zum Urkundenbeweis zugelassen* und wäre zum Anscheinsbeweis der Echtheit zugelassen.[1238]

791 Geht man davon aus, dass sich die Erfordernisse von Art. 82 SchKG an die Unterschrift eines provisorischen Rechtsöffnungstitels nach Art. 14 OR richten,[1239] kann eine Konformitätsbestätigung für eine elektronische Signatur, welche die Anforderungen von Art. 14 Abs. 2bis E-OR erfüllt, auch als provisorischer Rechtsöffnungstitel dienen.

3. Konformitätsbestätigung als Aufgabe der Kantone

792 Die Beglaubigung von Kopien ist eine Unterform der Sachbeurkundung.[1240] Es handelt sich um einen öffentlichen Beurkundungsakt, dessen verfahrensmässige Regelung und Durchführung in die verfassungsmässige Kompetenz der Kantone fällt.[1241] Die Regelung von Art. 21 VE-BGES, welche diese Kompetenz dem Bund übertrug wäre damit wohl verfassungswidrig gewesen.

E. Zusammenfassung

793 Die Vorstellung, dass Gerichte demnächst elektronisch signierte Dokumente ähnlich einfach wie Papierdokumente zum Urkundenbeweis entgegennehmen können, verkennt sowohl die durch unterschiedliche Dokumentenformate verursachten Schwierigkeiten als auch die vorderhand wohl nur langsame Verbreitung der Technik und die dementsprechend zu erwartende schlechte Auslastung entsprechender Infrastruktur.

794 Die m.E. einzig sinnvolle Möglichkeit, elektronische Signaturen auch aus prozessualer Sicht praxistauglich zu machen, bestünde daher in der Konzentration der Prüfinfrastruktur auf einige wenige staatliche oder staatlich anerkannte Konformitätsprüfstellen, deren Beglaubigungen elektronisch signierte Dokumente im Verfahren im Sinne von beglaubigten Kopien ersetzen könnten und damit zum Urkundenbeweis zuzulassen wären. In Anbetracht der m.E. grossen Bedeutung der prozessualen Anerkennung für die Akzeptanz elektronischer Signaturen wäre eine solche Lösung zu begrüssen.

1237 FRANK/STRÄULI/MESSMER, N 3 vor Art. 183 ff. ZPO ZH.

1238 Anders noch Simon SCHLAURI/Reto KOHLAS in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 187, wo eine explizite Anerkennung der Konformitätsbestätigung gefordert wurde.

1239 So Botschaft ZertES, 5688; SchKG-STAEHELIN, N 12 zu Art. 82 SchKG; OGer SO, SOG 1987 Nr. 8 = SJZ 1989, 363.

1240 RUF, N 478 ff., 1499 ff., 1522.

1241 BRÜCKNER, 4; RUF, N 130 ff.; Art. 55 Abs. 1 SchlT ZGB hält dies zusätzlich fest.

IV. Elektronische Signatur als hochtechnisches Beweismittel

795 Verglichen mit der Handunterschrift ist eine elektronische Signatur ein komplexes Beweismittel. Zumindest jenseits der beschriebenen prima-facie-Prüfung können die einzelnen Indizien von einem Laien kaum mehr beurteilt werden. Das Bundesgericht spricht in solchen Fällen von *hochtechnischen Sachverhalten.*[1242]

796 Fraglich ist deshalb, in welcher Art und Weise der Sachverhalt vorzutragen ist: Denn bedient sich die beweisführende Partei der Expertensprache, ist das Gericht evtl. nicht in der Lage, den Ausführungen zu folgen, und bedient sie sich einer vereinfachten Sprache, kann der Sachverhalt möglicherweise nur ungenau dargestellt werden.[1243]

797 Nach der Praxis des Bundesgerichts ist eine Übersetzung in die Laiensprache nicht erwünscht, denn in Fällen hochtechnischer Sachverhalte sehen die Verfahrensrechte regelmässig den Beizug von Experten vor. Die Parteien müssen dem Gericht mit ihren Aussagen ermöglichen, den Experten zu instruieren, d.h. der Gutachter muss durch die Parteivorbringen in die Lage versetzt werden, die Expertise auszuarbeiten. Dies setzt eine präzise Fachsprache voraus.[1244] Falls etwa ein Rechtsanwalt als Verfasser einer Rechtsschrift nicht in der Lage ist, die Beschwerdegründe dem Gericht verständlich darzulegen, so hat er die betreffenden Erklärungen durch eine Fachperson aufsetzen zu lassen.[1245]

798 Das Gericht muss bei der Beurteilung der Expertise den Sachverhalt nicht in sämtlichen wissenschaftlichen Aspekten nachvollziehen können. Seine Aufgabe beschränkt sich darauf, im Rahmen der Beweiswürdigung die Schlüssigkeit der Ausführungen des Gutachters zu beurteilen. Ein Abweichen von der Expertise ist nur aus triftigen Gründen zulässig.[1246]

1242 Etwa in BGE 121 I 37.
1243 SPÜHLER, 95.
1244 SPÜHLER, 95, mit Verweis auf einen unveröffentlichten BGE vom 18. Dezember 1998 in Sachen B. (4P 91/1998).
1245 SPÜHLER, 95, mit Verweis auf KassGer ZH, Kass.-Nr. 96/449 Z.
1246 SPÜHLER, 95; vgl. auch BGE 118 Ia 144 E. 1c und BIZER/HERDA, 25.

§ 12 Materiellrechtliche Anerkennung

I. Fragestellung und Vorgehen

799 In der Folge ist der bundesrätliche Lösungsvorschlag zu beurteilen, der eine ausnahmslose Gleichsetzung von Handunterschrift und qualifizierter elektronischer Signatur mit Anbieteranerkennung vorsieht. Hierzu wird zunächst das schweizerische System der materiellrechtlichen Formvorschriften dargelegt. Danach sind die gesetzgeberischen Zwecke der Vorschriften genauer zu betrachten und es ist zu untersuchen, ob diese Zwecke auch durch elektronische Signaturen erfüllt werden können. Abschliessend werden Alternativen beleuchtet, die dem Gesetzgeber zur Verfügung stehen, sofern die elektronische Signatur diese Zwecke nicht erfüllen kann. Dabei ist vor allem auf das im Vorentwurf für ein Bundesgesetz über den elektronischen Geschäftsverkehr vorgeschlagene Widerrufsrecht für Konsumentenfernabsatzverträge einzugehen.

II. Materiellrechtliche Formvorschriften

A. Grundlagen

1. Grundsatz der Formfreiheit

800 Im schweizerischen Privatrecht gilt der *Grundsatz der Formfreiheit*, wonach Willenserklärungen[1247] grundsätzlich ohne Rücksicht auf ihre Form Rechtswirkungen nach sich ziehen.[1248] Vorbehalten bleiben nur Willensäusserungen, für die das Gesetz eine besondere Form vorschreibt. Sämtliche Willenserklärungen, die formfrei gültig sind, können damit insbesondere auch auf elektronischem Weg abgegeben werden.[1249]

801 Ein erster Grund für das Prinzip der Formfreiheit liegt in der vertragsrechtlichen Vorstellung, dass allein die *Willenserklärung der Parteien* zu einer Rechtswirkung führt *(Konsensprinzip*[1250]*)*. Die Form, in der eine solche Erklärung abgegeben wird, ist für das Entstehen von Rechtswirkungen völlig gleichgültig.[1251] Ein weiterer Grund liegt im prozessualen *Grundsatz der freien Klagbarkeit von Forderungen.*[1252]

1247 Entgegen dem Wortlaut von Art. 11 OR sind nicht nur Verträge, sondern auch einseitige Rechtsgeschäfte gemeint; OR-SCHWENZER N 12 zu Art. 11 OR; ZK-SCHÖNENBERGER/JÄGGI N 9 zu Art. 11 OR.

1248 Art. 11 OR Abs. 1 OR; GAUCH/SCHLUEP/SCHMID, N 489 ff.; zur Entwicklung der Formfreiheit vgl. BK-KRAMER/SCHMIDLIN N. 1 ff. zu Art. 11 OR.

1249 WEBER/JÖHRI, 53; FRITZSCHE/MALZER, 17.

1250 GAUCH/SCHLUEP/SCHMID, N 491.

1251 ZK-SCHÖNENBERGER/JÄGGI, N 6 zu Art. 11 OR.

802 Der Grund für eine *Beschränkung* der Formfreiheit ergibt sich nie aus dem rechtlichen Tatbestand selber. Er muss in jenseits des rechtlichen Tatbestandes liegenden Zwecküberlegungen des Gesetzgebers zu finden sein. Diese können beispielsweise in einer Beschränkung des staatlichen Rechtsschutzes durch Formvorschriften liegen, beispielsweise zur Verfahrensbeschleunigung[1253], oder im Gedanken des Übereilungsschutzes oder der Rechtssicherheit durch Erzwingung einer besonders gearteten Ausformulierung von Willenserklärungen. Formvorschriften sind daher aus vertragsrechtlicher Sicht etwas Künstliches: Ein klarer, mängelfreier Wille der Parteien wird durch sie unter Umständen für unbeachtlich erklärt.[1254]

2. Gesetzliche Formvorschriften

a) Gültigkeitsform

803 Gesetzliche Vorschriften, die an die Form von Willenserklärungen Rechtsfolgen knüpfen, werden *Formvorschriften* genannt. Eine *Gültigkeitsvorschrift* hat bei Nichtbeachtung die Unbeachtlichkeit der Willenserklärung bzw. das Nichtzustandekommen des Rechtsgeschäfts zur Folge, sie ist *Gültigkeitsvoraussetzung* für das entsprechende Geschäft.[1255]

b) Beweisform

804 Die so genannte *Beweisform* unterwirft zwar den Abschluss eines Rechtsgeschäfts keiner bestimmten Form, setzt aber für dessen *Beweis* eine bestimmte Form voraus. Dies ist etwa im französischen *Code Civil* in Art. 1341[1256] für Geschäfte mit einer Vertragssumme von über 5000 Francs vorgesehen[1257] oder im US-amerikanischen *Statute of Fraud* für bestimmte Verträge über 500 Dollar.[1258] Folge derartiger Regelungen ist, dass eine grosse Zahl von Verträgen schriftlich zu schliessen sind.

805 Das schweizerische Recht kennt eine derartige Beweisform nicht. Das Schriftformerfordernis erstreckt sich damit nur auf einen relativ kleinen Teil aller geschlossenen Verträge.

c) Formungültigkeit

806 Nach Art. 13 Abs. 1 OR muss ein Vertrag, für den die schriftliche Form gesetzlich vorgeschrieben ist, die Unterschriften derjenigen Personen tragen, die durch ihn ver-

---

1252 ZK-SCHÖNENBERGER/JÄGGI, N 209 Vorbem. zu Art. 1-40 OR, N 7 zu Art. 11 OR.

1253 Im Erfordernis der schriftlichen Schuldanerkennung für die provisorische Rechtsöffnung nach Art. 82 SchKG kann eine solche Beschränkung gesehen werden.

1254 ZK-SCHÖNENBERGER/JÄGGI, N 8 zu Art. 11 OR.

1255 Eingehend sogleich N 806 ff.

1256 In Verbindung mit Art. 1 des Décret n. 80-533 vom 15. Juli 1980.

1257 ZK-SCHÖNENBERGER/JÄGGI, N 106 zu Art. 11 OR; vgl. etwa auch ZR 76 (1977) Nr. 64.

1258 Gemäss Statute of Fraud muss nicht der Vertrag selbst schriftlich vorliegen, sondern irgendein von der in Anspruch genommenen Partei unterzeichnetes Schriftstück, das den Abschluss des Vertrages beweist; Peter HAY, US-amerikanisches Recht, München 2000, N 263 ff.

pflichtet werden. Unterbleibt dies, ist die Rechtsfolge nach Art. 11 Abs. 2 OR *Formungültigkeit*, sofern nichts anderes bestimmt ist. Die Formungültigkeit gemäss bundesgerichtlicher Rechtsprechung stellt eine besondere Art der Nichtigkeit dar, die dadurch charakterisiert wird, dass ein materiell eigentlich einwandfreies Rechtsgeschäft nicht verbindlich ist.[1259] Die Formungültigkeit ist von Gesetzes wegen unwirksam und von Amtes wegen festzustellen. Jedermann kann sich auf sie berufen.[1260]

807 Dient die Form den Interessen einer (oder beider) Vertragsparteien *(Privatschutzfunktion)*, ist ein starres Festhalten an der Nichtigkeit oft unangemessen. Der Restbestand des formungültigen Geschäfts ist diesfalls mit einer Naturalobligation gleichzusetzen: *Vor* der Erfüllung besteht bei Formungültigkeit kein Erfüllungsanspruch.[1261] Auch die arglistige Herbeiführung eines formwidrigen Vertragsabschlusses begründet keinen Erfüllungsanspruch, weil der Rechtsmissbrauchstatbestand von Art. 2 Abs. 2 ZGB nach bundesgerichtlicher Rechtsprechung ausschliesslich negativ angerufen werden kann.[1262] Allenfalls ist eine Haftung aus *culpa in contrahendo* vorstellbar.[1263] *Nach* einer (freiwilligen) Erfüllung des formungültigen Geschäfts wird hingegen beispielsweise das Anrufen der Warnfunktion zum Zweck der Rückforderung des Geleisteten nicht mehr greifen, weil die Bedenkzeit zwischen Vertragsabschluss und -abwicklung im Resultat wie eine warnende Formvorschrift wirkt (Rechtsmissbrauchsverbot; Art. 2 Abs. 2 ZGB). Anders ist die Lage wiederum bei irrtümlicher oder arglistig herbeigeführter Erfüllung.[1264]

808 Falls eine Formvorschrift öffentliche Interessen oder die Interessen Dritter schützt *(Drittschutzfunktion)*, erweist sie sich hingegen als deutlich starrer: Die derart geschützten Interessen gehen denjenigen der Parteien grundsätzlich vor. Aber auch diesfalls wird regelmässig ein konkretes Rechtsschutzinteresse vorausgesetzt: Im Falle eines formungültigen Grundstückkaufes können sich Dritte auf den Mangel nur berufen, sofern sie durch diesen auch betroffen sind.[1265]

1259 BK-KRAMER/SCHMIDLIN, N 110 zu Art. 11 OR; vgl. auch BGE 116 II 702, 112 II 111, 104 II 104; GAUCH/SCHLUEP/SCHMID, N 548 ff. Anders die wohl herrschende Lehre; vgl. GAUCH/SCHLUEP/SCHMID, N 558 ff. m.H.

1260 BK-KRAMER/SCHMIDLIN, N 110 zu Art. 11 OR.

1261 BK-KRAMER/SCHMIDLIN, N 118 zu Art. 11 OR.

1262 BGE 116 II 702, 112 II 111, 104 II 104; BK-KRAMER/SCHMIDLIN, N 119 ff. zu Art. 11 OR; kritisch GAUCH/SCHLUEP/SCHMID N 557.

1263 BK-KRAMER/SCHMIDLIN, N 125 zu Art. 11 OR.

1264 Zum Ganzen BK-KRAMER/SCHMIDLIN, N 126 ff. zu Art. 11 OR; GAUCH/SCHLUEP/SCHMID, N 548 ff.

1265 BK-KRAMER/SCHMIDLIN, N 112 ff. zu Art. 11 OR.

3. Gewillkürte Formvorschriften

a) Allgemeines

809 Gesetzliche Formvorschriften dürfen durch die Vertragsparteien nicht abgeschwächt werden,[1266] die Parteien können jedoch sehr wohl durch Vereinbarung bestehende Formvorschriften verschärfen (die vom Gesetz vorgeschrieben einfache Schriftlichkeit kann beispielsweise durch qualifizierte Schriftlichkeit ersetzt werden[1267]) oder eigene Formvorschriften aufstellen, soweit das Gesetz keine solchen vorsieht. Man spricht diesfalls von *gewillkürter* oder *vertraglich vorbehaltener Form*.[1268] Die Freiheit, die Anwendung einer besonderen Form vorzubehalten, ist Ausfluss der Vertragsfreiheit.[1269]

b) Arten

810 Wie bei den gesetzlichen kann auch bei den gewillkürten Formvorschriften zwischen *Gültigkeitsform* und *Beweisform* unterschieden werden.[1270] Im Fall der gewillkürten Gültigkeitsform wollen die Parteien eine Verpflichtung erst mit Erfüllung der Form entstehen lassen. Bei der gewillkürten Beweisform sind – im Gegensatz zur gesetzlichen Beweisform – zwei Fälle zu unterscheiden: Der *erste Fall* der gewillkürten Beweisform ist eine *Beweisabrede*, gemäss der in einem allenfalls folgenden Prozess nur Urkunden (oder Akte in einer anderen vereinbarten Form), nicht aber weitere Beweismittel, zum Beweis zugelassen sein sollen (man spricht auch von einem *Beweisführungsvertrag*).[1271] Die Zulässigkeit derartiger Beweisabreden ist indessen umstritten.[1272] Der *zweite Fall* ist eine Abrede über eine spätere Verurkundung. Diesfalls hängt die Gültigkeit des Geschäfts nicht von der Einhaltung der Form ab – die Form hat bloss deklaratorischen Charakter.[1273]

c) Rechtsfolgen

811 Die Rechtsfolgen gewillkürter Formvorschriften bestimmen sich nach den allgemeinen Grundsätzen der Vertragsauslegung. Immerhin sind die gesetzlichen Auslegungsregeln von Art. 16 OR zu beachten: Ist für einen Vertrag, der von Gesetzes wegen an keine Form gebunden ist, die Anwendung einer solchen vorbehalten worden, wird vermutet, dass die Parteien vor Erfüllung der Form nicht verpflichtet sein wollen. Geht eine Abrede auf schriftliche Form ohne nähere Bezeichnung, gelten für deren Erfüllung die Erfordernisse der gesetzlich vorgeschriebenen Schriftlichkeit.[1274]

1266 Statt vieler ZK-SCHÖNENBERGER/JÄGGI, N 9 zu Art. 16 OR.
1267 ZK-SCHÖNENBERGER/JÄGGI, N 9 zu Art. 16 OR; differenzierend zur öffentlichen Beurkundung GAUCH/SCHLUEP/SCHMID, N 531.
1268 Art. 16 Abs. 1 OR; vgl. GAUCH/SCHLUEP/SCHMID, N 585 ff.; SCHMID, Unterschriftenwesen, 9.
1269 MERZ, N 395.
1270 SCHMID, Unterschriftenwesen, 10.
1271 FRANK/STRÄULI/MESSMER, N 11 vor § 133 ZPO ZH.
1272 FRANK/STRÄULI/MESSMER, a.a.O.; ZR 89 (1990) Nr. 118.
1273 GAUCH/SCHLUEP/SCHMID, N 588.
1274 MERZ, N 395; für *Deutschland* vorne N 452.

B. Das schweizerische System der Formvorschriften

1. Überblick

812 Das schweizerische Recht kennt als Hauptformen von Formvorschriften die einfache Schriftlichkeit, die qualifizierte Schriftlichkeit, die öffentliche Beurkundung sowie die qualifizierte öffentliche Beurkundung.[1275] In jüngerer Zeit hat sich zudem als weitere Form die Textform entwickelt. Zu beschreiben sind sodann die Beglaubigung von Unterschrift und Handzeichen sowie weitere Sonderformen.

2. Einfache Schriftlichkeit

813 Die einfache Schriftlichkeit, vom Gesetz kurz als Schriftlichkeit bezeichnet, ist in Art. 13 f. OR definiert. Sie liegt dann vor, wenn eine Erklärung *verurkundet* und durch den Namenszug eigenhändig *unterschrieben* ist.[1276]

a) Verurkundung

814 Verurkundung ist das schriftliche Festhalten einer Erklärung auf einem dauerhaften Stoff.[1277] Die zur Verurkundung eingesetzte Schreibtechnik und die verwendete Schrift sind gleichgültig, solange die Schriftzeichen – als Ausfluss der Forderung nach andauernder Beweiskraft für die Unveränderheit des Inhaltes (Datenintegrität) – dauerhaft sind.[1278]

815 Inhaltlich muss die Verurkundung sämtliche objektiv und subjektiv wesentlichen Punkte der Willenserklärung umfassen, die der Formvorschrift unterstehen.[1279]

b) Unterschrift

aa) Formelles Element

816 Durch die Unterzeichnung fügt der Erklärende dem zu unterzeichnenden Text seinen Namen hinzu und gibt damit zu erkennen, dass er dessen Inhalt als seinem Willen entsprechend anerkennt.[1280] Der Begriff Unterschrift im formellen Sinn ist doppeldeutig: Einerseits bezeichnet er den *Vorgang des Unterschreibens*, andererseits die *Schriftzeichen*, die sich danach dauerhaft auf dem Dokument befinden.[1281] Diente die Unterschrift ausschliesslich dem Schutz des Erklärenden, wäre einzig das Unterschreiben Formerfordernis.[1282] In jedem Fall bezweckt die Unterschrift jedoch auch

---

1275 GAUCH/SCHLUEP/SCHMID, N 502 ff.
1276 BK-KRAMER/SCHMIDLIN, N 3 der allgemeinen Erläuterungen zu Art. 12-15 OR; SCHMID, Unterschriftenwesen, 11; ZK-SCHÖNENBERGER/JÄGGI, N 5 zu Art. 13 OR.
1277 BK-KRAMER/SCHMIDLIN, N 4 der allgemeinen Erläuterungen zu Art. 12-15 OR; ZK-SCHÖNENBERGER/JÄGGI, N 6 ff. zu Art. 13 OR; für *Deutschland* SEIDEL, Dokumentenschutz I, 410.
1278 ZK-SCHÖNENBERGER/JÄGGI, N 11 zu Art. 13 OR.
1279 ZK-SCHÖNENBERGER/JÄGGI, N 13 ff. zu Art. 13 OR.
1280 BK-KRAMER/SCHMIDLIN, N 9 der allgemeinen Erläuterungen zu Art. 12-15 OR.
1281 ZK-SCHÖNENBERGER/JÄGGI, N 18 zu Art. 13 OR.

den Beweis der Erfüllung der Formvorschrift selbst, weshalb die Unterschrift zumindest im Augenblick des Vertragsabschlusses auch in der Form dauerhafter Schriftzeichen vorhanden sein muss.

817 Nach Art. 14 Abs. 1 OR ist die Unterschrift eigenhändig, d.h. persönlich und von Hand, zu schreiben: Die Eigenart der Handschrift, die auch in der eigenhändigen Unterschrift zum Vorschein kommt, ist Ausdruck der Persönlichkeit des Ausstellers. Dies entspricht dem Zweck der Identifizierung des Unterzeichners.[1283]

818 Die *Faksimileunterschrift* (Stempel, Druck, Fotokopie) ist nicht in diesem Sinne eigenhändig und damit im Grunde zur Erfüllung der Schriftform untauglich. Art. 14 Abs. 2 OR statuiert eine Ausnahme für den Fall, dass die Faksimileunterschrift im Verkehr wie eine eigenhändige Unterschrift verwendet und anerkannt wird.[1284] Das Gesetz nennt als Beispiel die Ausgabe von Wertpapieren in grosser Zahl. Im Weiteren sind Faksimile-Unterschriften etwa bei Versicherungspolicen üblich, die zwar Einzelpapiere sind, aber dennoch in grosser Zahl ausgegeben werden.[1285]

bb) Materielles Element

819 Die Unterschrift muss zur Erfüllung der Formvorschriften nicht nur formell vorhanden sein, sie muss, wie erwähnt, auch gesetzt worden sein, um den Inhalt des Verurkundeten Schriftstücks als mit dem eigenen Willen übereinstimmend anzuerkennen; man spricht von der *Rekognition der Urkunde* durch den Unterzeichner. Fehlt dieser Zusammenhang – wie etwa bei einer Unterschrift im Scherz –, so steht dem Unterschreibenden die materielle Einwendung des fehlenden Rekognitions- bzw. Erklärungswillens offen.[1286]

820 Die Unterschrift hat normalerweise in der Schriftrichtung dem Text nachzufolgen, um die Rekognition auszudrücken. Sofern die Rekognitionsabsicht freilich anderweitig ersichtlich ist, kann auf dieses Erfordernis verzichtet werden.[1287] Bei Abänderungen des Urkundentextes (Streichungen, Hinzufügungen) gilt der ursprüngliche Text weiterhin, sofern nicht bewiesen wird, dass die Änderungen schon vor der Unterzeichnung vorhanden waren.[1288]

1282 ZK-SCHÖNENBERGER/JÄGGI, N 18 zu Art 13 OR.

1283 Zur Eigenhändigkeit vgl. ZK-SCHÖNENBERGER/JÄGGI, N 4 zu Art. 14 und 15 OR; SCHMID, Unterschriftenwesen, 23 ff.; für *Deutschland* SEIDEL, Dokumentenschutz I, 410.

1284 Vgl. ZK-SCHÖNENBERGER/JÄGGI, N 12 zu Art. 14 und 15 OR; SCHMID, Unterschriftenwesen, 48 ff.

1285 BK-KRAMER/SCHMIDLIN, N 12 zu Art. 15 OR; ZK-SCHÖNENBERGER/JÄGGI, N 13 zu Art 14 und 15 OR; bezüglich der in *Deutschland* ähnlichen Regelung etwa SEIDEL, Dokumentenschutz I, 411.

1286 Zum Ganzen ZK-SCHÖNENBERGER/JÄGGI, N 18 zu Art. 13 OR; eingehend zur Rekognition hinten N 836 ff.

1287 ZK-SCHÖNENBERGER/JÄGGI, N 37 ff. zu Art. 13 OR; im Ergebnis ähnlich SCHMID, Unterschriftenwesen, 26 ff.; für *Deutschland* SEIDEL, Dokumentenschutz I, 410; zur Integrität des Urkundentextes auch vorne N 644 f.

1288 ZK-SCHÖNENBERGER/JÄGGI, N 39 zu Art. 13 OR.

3. Textform

a) Allgemeines

821 In jüngerer Zeit hat sich mit der *Textform* eine Zwischenstufe zwischen Formfreiheit und Schriftlichkeit etabliert, die im Hinblick auf elektronisch übermittelte Willensäusserungen (E-Mail, Telefax, Übergabe elektronischer Datenträger) zusätzlich an Aktualität gewinnt.[1289] Der Schweizer Gesetzgeber spricht jeweils von einer Form, die den *Nachweis durch Text* ermöglicht.[1290] Im Gegensatz zur einfachen Schriftlichkeit fallen hierbei die Voraussetzungen der Verurkundung auf einem festen Urkundenstoff und der Handunterschrift weg, sodass auch Telefax, E-Mail, etc. diese Formvorschrift erfüllen können. Von der Mündlichkeit unterscheidet sich die Textform durch ihre visuelle Wahrnehmbarkeit bzw. physische Reproduzierbarkeit, womit «die nötige Sicherheit in bezug auf die Annahme einer Prorogation» erreicht werden soll.[1291]

822 Aufgrund der fehlenden Unterschrift schafft die Textform jedoch kaum erhöhte Beweiskraft und entwickelt gegenüber der Mündlichkeit auch eine nur unwesentlich erhöhte Warnfunktion.[1292] Ihr Einsatz ist daher in erster Linie dort sinnvoll, wo es ausschliesslich um die *Übermittlung von Information mit einer gewissen Dauerhaftigkeit* geht, also beispielsweise bei Informationen im Sinne der genannten Vorlage zu den Fernabsatzverträgen, die der Empfänger dauerhaft auf einem Datenträger abspeichern können muss, um die Möglichkeit einer erneuten Einsichtnahme zu wahren.[1293] Auch der deutsche Gesetzgeber sieht die Textform in erster Linie in Fällen mit überwiegendem Informationszweck vor.[1294]

823 Damit ist m.E. zweifelhaft, ob der Einsatz der Textform in ihrem angestammten Gebiet der Gerichtsstandsvereinbarungen überhaupt sehr sinnvoll ist.[1295]

1289 Eingehender zur Textform etwa Hans REISER, Gerichtsstandsvereinbarungen nach IPR-Gesetz und Lugano-Übereinkommen, Zürich 1995, 48 ff.

1290 Vgl. etwa Art. 5 Abs. 1 IPRG; Art. 9 Abs. 2 Bst. a GestG; § 11 Abs. 1 ZPO ZH.

1291 BGE 119 II 395; Frank VISCHER/Lucius HUBER/David OSER, Internationales Vertragsrecht, 2. A. Bern 2000, N 1277 f.

1292 Eine Beweisfunktion lässt sich allenfalls noch in Ansätzen aufgrund des auch für nicht unterzeichnete Urkunden geltenden strafrechtlichen Schutzes erkennen. Dieser darf aber aufgrund der Unmöglichkeit, Fälschungen anhand der Dokumente selbst nachzuweisen, nicht überbewertet werden. Dazu schon vorne N 22 ff., N 654 ff. Vgl. auch Karl SPÜHLER, Gerichtsstandsvereinbarungen überprüfen!? – Zum neuen Gerichtsstandsgesetz, SZW 5/2000, 238 ff., 239; MÜLLER/WIRTH-WIRTH, N 98 zu Art. 9 GestG (der dem Problem aber aufgrund der Fälschbarkeit von Handunterschriften keine grosse Bedeutung beimisst; dazu aber vorne N 639 ff.). Zur Warnfunktion hinten N 857 ff.

1293 Vorne N 487.

1294 Vgl. schon vorne N 448.

1295 Kritisch zur Textform etwa auch FREI, N 392 ff.; MALZER, 118; HUNGER, 111 ff.

b) *Textform im VE-BGEG insbesondere*

824 Zu bedauern ist m. E., dass im Rahmen des laufenden Gesetzgebungsverfahrens zum VE-BGEG auf eine *explizite* Einführung der Textform gerade im Bereich der Informationspflichten nach Art. 40d OR bzw. des VE-BGEG verzichtet wird.[1296] Die Botschaft zum ZertES geht davon aus, dass es besser sei, die Zulassung der Textform in diesen Bereichen der Rechtsprechung zu überlassen, um der technischen Entwicklung Raum zu lassen, d. h. etwa weil in Zukunft mit Systemen zu rechnen sei, die gesprochene Sprache maschinell in Text umzuwandeln und umgekehrt.[1297] Abgesehen davon, dass derartige Spezialfälle – sollten sie denn dereinst tatsächlich zu beurteilen sein – auch bei bestehender gesetzlicher Regelung durch eine teleologische Betrachtungsweise ziemlich einfach einzuordnen sein dürften,[1298] ist die durch eine derartige Nicht-Regelung mit blosser «en-passant-Erläuterung» in der Botschaft entstehende Rechtsunsicherheit gerade im Bereich der Formvorschriften nicht akzeptabel.[1299] Als Vorbild für eine explizite Regelung könnte etwa der beschriebene § 126b BGB dienen.[1300]

4. Qualifizierte Schriftlichkeit

825 Unter qualifizierter Schriftlichkeit sollen hier sämtliche Spielarten der Schriftlichkeit verstanden werden, bei denen zu den Voraussetzungen der einfachen Schriftlichkeit, d. h. Verurkundung und Unterschrift, weitere Kriterien hinzutreten, bei denen aber keine Behörde oder Urkundsperson involviert ist. Denkbar sind formelle Zusatzerfordernisse wie die vollständige Handschriftlichkeit *(Eigenschriftlichkeit)* des Dokuments (beispielsweise bei der eigenhändigen letztwilligen Verfügung nach Art. 505 ZGB), *Ausführlichkeitsvorschriften* (etwa bei Konsumentenverträgen[1301] oder der Kündigung der Miete von Wohn und Geschäftsräumen mittels eines Formulars mit vorgeschriebenem Inhalt; Art. 266 Abs. 2 OR) oder die Nennung bestimmter Begriffe (im Wechsel oder Checkrecht; Art. 991 Ziff. 1 und 1100 Ziff. 1 OR).

5. Beglaubigung von Unterschrift oder Handzeichen

826 Die Beglaubigung ist die einer Unterschrift oder einem Handzeichen beigefügte Erklärung einer zuständigen Behörde oder Urkundsperson über die Zugehörigkeit von Unterschrift oder Zeichen zu einer bestimmten Person.[1302] Sie wird im Bundesrecht vorausgesetzt, untersteht aber wie das Urkundswesen im Allgemeinen dem kantona-

---

1296 Dazu vorne N 487.

1297 Botschaft ZertES, 5684, 5688.

1298 Von Bedeutung dürfte in erster Linie sein, ob eine Information in der Form dauerhaft speicherbarer Schriftzeichen in den Einflussbereich des Empfängers gelangt – was etwa dann nicht der Fall ist, wenn er sie bloss per Telefon abrufen kann.

1299 So auch SUISA, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 168 f.; a. M. WIEGAND, 128.

1300 Vorne N 447 f.

1301 ZK-SCHÖNENBERGER/JÄGGI, N 29 zu Art. 11 OR.

1302 ZK-SCHÖNENBERGER/JÄGGI, N 87 ff. zu Art. 13 OR.

len Recht.[1303] Die Beglaubigung hat schriftlich und je nach kantonalem Recht durch einen Amtsstempel zu erfolgen, wobei die beglaubigte Unterschrift in Gegenwart des Beglaubigenden zu setzen oder zumindest durch den physisch anwesenden Unterzeichner zu bestätigen ist.[1304] Sie bestätigt ausschliesslich die Zusammengehörigkeit von Unterschrift und Unterzeichner (d.h. die Echtheit der Unterschrift) zu Beweiszwecken und insbesondere nicht die Rekognition des Urkundeninhaltes.[1305]

827 Art. 15 OR beispielsweise setzt die Beglaubigung des Handzeichens eines Schreibunfähigen voraus.[1306]

6. Öffentliche Beurkundung

828 Bei einer öffentlichen Beurkundung wird das formbedürftige Rechtsgeschäft in einem Schriftstück festgehalten, und zwar durch eine vom Staat mit dieser Aufgabe betraute Person, in der vom Staat geforderten Form und in dem dafür vorgesehenen Verfahren.[1307]

829 Ziel ist dabei zunächst die Schaffung erhöhter Rechtssicherheit durch Klarheit der Formulierungen und deutlicher Manifestation des Abschlusswillens der Parteien, insbesondere hinsichtlich nachfolgender Registereintragungen.[1308] Hinzu kommt die Aufbewahrung eines Doppels oder einer Kopie durch die ausstellende Behörde, was eine unbemerkte Fälschung zirkulierender Urkunden erschwert.[1309] Schliesslich wird gegenüber einfach schriftlichen Urkunden ein qualifizierter Übereilungsschutz geschaffen und durch die Mitwirkung einer sachkundigen und unparteiischen Urkundsperson das Bewusstsein der Parteien für Tragweite und Risiken des Geschäfts gefördert.[1310]

830 Die Modalitäten der öffentlichen Beurkundung, d.h. die zuständige Behörde oder Urkundsperson, das Mitwirken von Zeugen oder ein etwaiges Erfordernis der Unterschrift der (durch eine Erklärung belasteten) Partei bestimmt sich wie bei der Beglaubigung nach kantonalem Recht.[1311]

7. Qualifizierte Formen der öffentlichen Beurkundung

831 Ähnlich wie die einfache Schriftlichkeit kennt auch die öffentliche Beurkundung qualifizierte Formen. So bestehen auch hier teilweise Ausführlichkeitsvorschriften,

---

1303 ZK-SCHÖNENBERGER/JÄGGI, N 85 zu Art. 13 OR.
1304 ZK-SCHÖNENBERGER/JÄGGI, N 89 ff. zu Art. 13 OR.
1305 ZK-SCHÖNENBERGER/JÄGGI, N 88 und N 94f. zu Art. 13 OR.
1306 ZK-SCHÖNENBERGER/JÄGGI, N 25 ff. zu Art. 14 und 15 OR.
1307 GAUCH/SCHLUEP/SCHMID, N 524; vgl. auch vorne N 633.
1308 SCHMID, Öffentliche Beurkundung, N 42-44.
1309 BRÜCKNER, N 1458 ff.
1310 SCHMID, Öffentliche Beurkundung, N 35.
1311 Art. 55 SchlT ZGB; vgl. BK-GIOVANOLI/SCHAETZLE, N 35 zu Art. 493 OR.

es müssen Zeugen beigezogen werden, oder die Parteien haben zusätzlich zur Urkundsperson von Bundesrechts wegen persönlich zu unterschreiben.[1312]

8. Sonderformen

832 Andere Sonderformen werden bei der Eheschliessung[1313] und dem Nottestament[1314] verlangt. Auch die gerichtliche Genehmigung der Scheidungskonvention[1315] oder Beschlussvorschriften im Recht der juristischen Personen können im Prinzip als Sonderformen betrachtet werden.

C. Formzwecke und ihre Erfüllung durch elektronische Signaturen

1. Funktionale Äquivalenz

833 Auf früheren Stufen der Rechtsentwicklung war die Form *Geltungsgrund* der Rechtsfolgen, sie war *Wirkform*. Nach heutigem Recht ist die Form grundsätzlich *Zweckform*, d.h. sie dient nur noch äusserlichen Zwecken wie der Beweissicherung, der Rechtssicherheit oder dem Übereilungsschutz.[1316] Die Formvorschriften sind jedoch von der ihnen zugrundeliegenden rechtspolitischen Zielsetzung weitgehend abgelöst: Es ist irrelevant, ob die erfüllte Formvorschrift den hinter ihr stehenden Zweck im konkreten Fall wirklich erfüllt oder ob der Zweck auf andere Weise genauso erfüllt werden kann. Auch ist unbeachtlich, ob der vom Gesetzgeber verfolgte Zweck im konkreten Fall überhaupt von Bedeutung ist.[1317] Ausnahmen ergeben sich allenfalls aufgrund des Rechtsmissbrauchsverbots.[1318]

834 Die mit Formvorschriften verfolgten Zwecke sind durch Auslegung der gesetzlichen Bestimmungen zu finden.[1319] In vielen Fällen wird eine Formvorschrift jedoch nicht durch einen einzigen Zweck begründet, sondern durch mehrere Zwecke in unterschiedlicher Gewichtung.[1320]

835 Im Folgenden soll geklärt werden, ob elektronische Signaturen diese Zwecke ebenfalls erfüllen können, d.h. ob sie zur Handunterschrift *funktional äquivalent* sind.

1312 BK-KRAMER/SCHMIDLIN, N 84 ff. zu Art. 11 OR.
1313 Art. 113 ff. ZGB.
1314 Art. 506 ff. ZGB.
1315 Art. 111 ZGB.
1316 BK-MERZ, N 462 zu Art. 2 ZGB.
1317 BK-MERZ, a.a.O.
1318 Dazu vorne N 807.
1319 BK-KRAMER/SCHMIDLIN, N 10 zu Art. 11 OR; ZK-SCHÖNENBERGER/JÄGGI, N 43 zu Art. 11 OR; HELDRICH, 93.
1320 ZK-SCHÖNENBERGER/JÄGGI, N 44 zu Art. 11 OR.

2. Rekognition

a) Vorbemerkung: Willenserklärungen

836 Die *Willenserklärung* ist Voraussetzung für die Begründung eines jeden Rechtsgeschäfts. Sie besteht in der Mitteilung des Willens zur Begründung, Änderung oder Beendigung eines Rechts oder Rechtsverhältnisses und enthält damit das Element des Willens und dasjenige des Erklärungsvorgangs. Der Wille seinerseits kann in Geschäfts- und Erklärungswille geggliedert werden. Der Erstere ist der Wille des Erklärenden, ein Rechtsverhältnis in bestimmter Weise zu gestalten, der Letztere ist der Wille, den bestehenden Geschäftswillen dem Empfänger kundzutun, damit er Geltung erlange. Der Erklärungsvorgang umfasst die Abgabe der Erklärung sowie deren Empfang.[1321]

837 Ob ein Text als Willenserklärung aufgefasst werden kann, bestimmt sich im Streitfalle nach dem *Vertrauensprinzip*, d.h. danach, ob der Empfänger nach Treu und Glauben davon ausgehen darf und muss, dass es sich dabei um eine Willenserklärung handelt. Irrelevant ist damit insbesondere, ob der Erklärende überhaupt ein Erklärungsbewusstsein hatte.[1322]

b) Begriff der Rekognition

838 Bezeichnet ein Erklärender einen Text als seinem eigenen Willen entsprechend, spricht man von *Rekognition* oder *Anerkennung*.[1323] Die Rekognition kann eine stillschweigende oder eine ausdrückliche sein; so ist eine mündliche Willensäusserung nicht explizit als solche zu kennzeichnen, sondern ihr Charakter als Willenserklärung ergibt sich regelmässig bereits aus den Umständen. Ein nicht durch den Erklärenden selbst verfasster Text hingegen (etwa vorgedruckte Geschäftsbedingungen) wird übungsgemäss durch eine separate Rekognitionshandlung – meist eine Unterschrift – anerkannt.

c) Rekognition durch Handunterschrift

839 Die verkehrsüblichen Mittel zur Rekognition eines geschriebenen Textes sind die Handunterschrift sowie, bei Erklärungen unter Abwesenden, dessen *Begebung*.[1324] Ergibt sich aus den Umständen nichts anderes, darf und muss der Empfänger eines unterschriebenen Textes daher davon ausgehen können, dass es sich dabei gemäss Vertrauensprinzip um eine Willenserklärung des Unterzeichners handelt.

1321 Zum Ganzen statt vieler GAUCH/SCHLUEP/SCHMID, N 167 ff.

1322 GAUCH/SCHLUEP/SCHMID, N 206 ff.

1323 Etwa BK-KRAMER/SCHMIDLIN, N 10 vor Art. 12-15 OR; ZK-SCHÖNENBERGER/JÄGGI, N 36 zu Art. 11 OR.

1324 Vgl. ZK-SCHÖNENBERGER/JÄGGI, N 20 f. zu Art. 13 OR; BK-KRAMER/SCHMIDLIN, N 10 der Allgemeinen Erläuterungen zu Art. 12-15 OR; zur Rekognition mittels Handunterschrift vgl. bereits die Ausführungen bei N 819 f.

d) Rekognition durch elektronische Signatur

aa) (Einfache) elektronische Signatur

840 Eine elektronische Signatur kann automatisch und ohne Zutun des Anwenders gesetzt werden. Nach herrschender Lehre werden computergenerierte Erklärungen demjenigen zugerechnet, der das entsprechende Computersystem betreibt.[1325] Die automatische Erzeugung einer elektronischen Signatur ist damit kein Hindernis für deren Qualität als Rekognitionshandlung. Dies gilt a fortiori auch für Fälle, in denen zwar eine Benutzerinteraktion verlangt wird (etwa die Eingabe eines Passwortes zur Aktivierung des Signierschlüssels), die Software jedoch nicht auf den Zusammenhang mit dem Setzen einer Signatur hinweist.[1326]

841 Die Problematik liegt vielmehr darin, dass dem Erklärenden die mögliche Wirkung einer elektronischen Signatur als Rekognitionshandlung mangels Verkehrsübung nicht a priori bewusst sein muss. Die Erklärung, ein kryptographisches Schlüsselpaar zu halten (die etwa durch eine Zertifizierung des Prüfschlüssels oder Weitergabe eines solchen im Rahmen eines PGP Web of Trust[1327] zumindest implizit abgegeben wird), kann auch aus anderen Gründen erfolgen als demjenigen, damit Signaturen setzen zu wollen (etwa zum Zwecke der Verschlüsselung[1328]), ja es wäre unter Umständen sogar möglich, dass ein Anwender ein Zertifikat auf seinem Rechner installiert oder installiert erhält, ohne sich überhaupt im Klaren zu sein, dass er damit Signaturen setzen kann.[1329]

842 Der gute Glaube des Erklärungsempfängers bezüglich des Rekognitionswillens des Unterzeichners kann damit m. E. umgekehrt nicht ausschliesslich auf einer vorhandenen elektronischen Signatur gründen; es müssen vielmehr weitere Anhaltspunkte für die Rekognition bestehen, wie etwa der unter eine Nachricht gesetzte Name des Unterzeichners oder das Wissen des Empfängers, dass der Absender Signiersoftware einsetzt, die ihn auf die Rekognitionswirkung hinweist.[1330]

843 Es dürfte hingegen möglich sein, dass sich der Signierschlüsselhalter explizit gegenüber jedermann dazu bereit erklärt, elektronische Signaturen gegen sich als Rekognitionshandlung gelten zu lassen; durch eine solche Erklärung wird der gute Glaube eines Empfängers begründet. Auf die Haftung für Missbräuche des Signierschlüssels

---

1325 Statt vieler WEBER, E-Commerce, 312 f.

1326 Netscape Messenger 4.7 setzt beispielsweise bei entsprechender Einstellung automatisch eine digitale Signatur unter jede versandte Nachricht und öffnet dabei – falls in den Einstellungen überhaupt so festgelegt – einen Dialog mit der Nachricht «Bitte geben Sie das Kennwort bzw. die Kennnummer ein für Communicator Certificate DB». Ein Hinweis darauf, dass es sich um eine digitale Signatur handelt oder dass der Text der Nachricht damit anerkannt wird, fehlt.

1327 Vorne N 76 f.

1328 Dazu vorne N 169 f.

1329 Swisskey verteilte beispielsweise über Jahre hinweg an jeder grösseren Schweizer Informatikmesse Gratiszertifikate, die ein Anwender auch erhalten konnte, ohne sich über deren genauen Einsatzzweck aufklären zu lassen; vgl. soeben FN 1326.

1330 Zu undifferenziert KPMG, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 164 f.

(und eine entsprechende Pflicht, diesen geheim zu halten) hätte sie aber zunächst einmal keinen Einfluss, weil sie sich auch ausschliesslich auf Fälle beziehen kann, in denen die Echtheit einer Signatur anerkannt oder erwiesen ist.[1331]

bb) Qualifizierte elektronische Signatur

844 Anders liegen die Dinge hingegen bei qualifizierten elektronischen Signaturen gemäss E-ZertES.[1332] Nach Art. 9 Abs. 2 E-ZertES hat der Zertifizierungsdiensteanbieter den Antragsteller auf ein qualifiziertes Zertifikat auf die möglichen Folgen des Missbrauchs seines Signierschlüssels hinzuweisen. Dazu gehört auch, dass ein Signierschlüsselhalter in unglücklichen Fällen wie bei einer gefälschten Handunterschrift einem Dritten gegenüber für eine Willenserklärung einstehen muss, die er nicht abgegeben hat. Damit sollte dem Schlüsselhalter klar sein, dass eine elektronische Signatur die selben rechtlichen Wirkungen wie eine Handunterschrift aufweist und damit auch als Rekognitionshandlung verstanden werden darf.[1333]

845 Hinzu kommt, dass der Gesetzgeber in Art. 14 Abs. 2bis E-OR die qualifizierte elektronische Signatur mit Anbieteranerkennung der Handunterschrift explizit gleichstellt, was deren Tauglichkeit als Rekognitionsmittel impliziert.

e) Zusammenfassung

846 Zumindest qualifizierte elektronische Signaturen nach E-ZertES können die Rekognitionsfunktion der Handunterschrift erfüllen.

3. Beweis (Identität, Integrität)

a) Allgemeines

847 Ein bedeutendes Motiv sowohl für gewillkürte als auch für gesetzliche Formvorschriften liegt in der *Verbesserung der Beweislage* für die Abgabe des verurkundeten Inhalts durch den Unterzeichner.[1334] Die Handunterschrift gewährleistet dabei im Zusammenspiel mit der dauerhaften Fixierung der Erklärungen auf einem Urkundenstoff die Identifizierbarkeit des Unterzeichners sowie die Unveränderlichkeit des Urkundeninhaltes.[1335]

848 Teilweise wird auch gesondert von Identitäts-, Integritäts- und Echtheitsfunktion gesprochen.[1336] Diese einzelnen Funktionen sind aber m.E. für sich allein betrachtet nicht sinnvoll zu beurteilen.[1337]

1331 Zur Frage, ob auf dem Wege einer ähnlichen Erklärung auch eine Haftungsgrundlage geschaffen werden kann vorne N 704 ff.

1332 Vorne N 515 f.

1333 Zur Problematik der fehlenden Haftung für Signaturen ohne Anbieteranerkennung vorne N 755 ff.

1334 BK-KRAMER/SCHMIDLIN, N 11, 14 f. zu Art. 11 OR; ZK-SCHÖNENBERGER/JÄGGI, N 46 zu Art. 11 OR; GAUCH/SCHLUEP/SCHMID, N 499 f.; MK-EINSELE, N 7 zu § 125 BGB; PALANDT-HEINRICHS, N 1 zu § 125 BGB.

1335 Eingehend zur Fälschungssicherheit von Handunterschriften vorne N 639 ff.

Beim Einsatz von Formvorschriften zu Beweiszwecken können Interessen der vertragschliessenden Parteien im Zentrum stehen (Privatschutz), aber auch solche von Dritten oder der Allgemeinheit (Drittschutz; etwa bei der öffentlichen Beurkundung von Rechtsakten zur Schaffung verlässlicher Grundlagen zur Registerführung).[1338] Art. 260a Abs. 1 OR (Notwendigkeit einer Zustimmung des Vermieters zu Änderungen des Mieters an der Mietsache) dient beispielsweise in erster Linie der Beweissicherung zwischen den Parteien,[1339] während etwa die Bestimmungen zur Abtretung oder Verpfändung von Forderungen der Verkehrssicherheit dienen[1340] oder Art. 11 des Waffengesetzes (WG)[1341] zur Überwachung des Waffenhandels[1342] eingeführt wurde. 849

Entgegen der landläufigen Meinung sind auch Handunterschriften relativ fälschungssicher; in nur gerade gut 20% aller Fälle kann ein Gutachter keine Aussage darüber machen, ob eine Unterschrift gefälscht ist oder nicht.[1343] Das Risiko eines Fälschers, dass eine Unterschrift als gefälscht entlarvt wird, ist demnach hoch, auch wenn keinerlei weitere Indizien vorhanden sind. Damit sind an die elektronische Signatur durchaus hohe Anforderungen zu stellen, soll sie die Beweisfunktion erfüllen. 850

b) Einfache elektronische Signatur

Wie gezeigt fallen unter den Begriff der einfachen elektronischen Signatur des E-ZertES eine Vielzahl von Verfahren, die unter Umständen keine oder nur schwache Beweiskraft haben.[1344] Wurde eine Formvorschrift daher mit dem Ziel erlassen, eine bessere Beweislage zu schaffen, so kann die Handunterschrift durch derartige Verfahren nicht ersetzt werden.[1345] 851

c) Qualifizierte elektronische Signatur

Eine qualifizierte elektronische Signatur weist (zumindest auf dem Umweg über die Anzeige des Zertifikate durch die Signaturprüfeinheit) auf die Identität des Unterzeichners hin und deckt nachträgliche Veränderungen am signierten Text auf. Sie zielt damit in erster Linie auf die Erfüllung der Beweisfunktion ab. 852

1336 Etwa bei BK-KRAMER/SCHMIDLIN, N 13 vor Art. 12-15 OR; MENZEL, 150 ff.; OBERHOLZER, Digitale Signatur, 437f.; RASSMANN, 37; SEIDEL, Dokumentenschutz II, 485; WEBER, E-Commerce, 312.

1337 Vgl. schon vorne N 27.

1338 ZK-SCHÖNENBERGER/JÄGGI, N 47 zu Art. 11 OR.

1339 OR-WEBER/ZIHLMANN, N 4 zu Art. 260a OR.

1340 Art. 165 Abs. 1 OR; Art. 900 Abs. 1 ZGB; vgl. OR-GIRSBERGER, N 1 zu Art. 165 OR; BK-ZOBL, N 27 zu Art. 900 ZGB.

1341 SR 514.54.

1342 Dazu hinten N 870ff.

1343 Vorne N 641.

1344 Vorne N 515, 378.

1345 Unklar EBBING, 275, der einem unter einen elektronischen Text gesetzten Namenszug ohne Signatur bereits Beweiskraft zuspricht.

853 Die Fälschung einer qualifizierten elektronischen Signatur mag zwar im Einzelfall um einiges schwieriger sein als die Fälschung einer Handunterschrift.[1346] Umgekehrt ist das Schadenspotential bei der elektronischen Signatur aber auch sehr viel grösser, denn wenn der Signierschlüssel einem Angreifer einmal verfügbar ist, kann dieser beliebig viele Signaturen setzen, die vom Original nicht zu unterscheiden sind.[1347] Zudem dürfen die systembedingten Risiken der qualifizierten elektronischen Signatur, die Möglichkeit des physischen Ausspähens der PIN, das Präsentationsproblem sowie die relativ unsichere Identitätsprüfung durch den Zertifizierungsdiensteanbieter nicht aus den Augen verloren werden.[1348] Damit ist die oft gehörte Aussage, die qualifizierte elektronische Signatur sei bedeutend sicherer als die Handunterschrift, stark zu relativieren. Vielmehr haben beide Verfahren Schwächen, die jeweils dazu führen, dass sie für sich allein streng genommen die volle Überzeugung eines Gerichts von der Echtheit nicht zu erbringen vermögen.[1349]

854 Wie gezeigt, hat die zivilprozessuale Praxis aber mit dem Anscheinsbeweis für die Handunterschrift ein Mittel gefunden, um diese Schwächen zu umgehen, welches m. E.auch auf die qualifizierte elektronische Signatur übertragbar ist.[1350] Handunterschrift und qualifizierte elektronische Signatur sind daher bezüglich ihrer Beweiskraft durchaus *vergleichbar*.

855 Eine Schwierigkeit besteht darin, dass Gerichte noch nicht mit der zur Überprüfung elektronischer Signaturen nötigen Infrastruktur ausgestattet sind, weshalb für zur Beweisführung derzeit Sachverständigengutachten nötig sind.[1351] Man könnte argumentieren, Funktion der Schriftlichkeit sei auch, die *einfache* Beweisbarkeit zu gewährleisten, was durch die elektronische Signatur nicht erfüllt werde.[1352] In Anbetracht dessen, dass aber auch eine verlässliche Prüfung von Papierurkunden regelmässig nur durch Fachleute erfolgen kann,[1353] verliert dieses Argument jedoch an Gewicht.

d) Zusammenfassung

856 Gegen eine materiellrechtliche Anerkennung elektronischer Signaturen, deren Sicherheitsniveau dem Stand der Technik entspricht, ist m. E. aus der Perspektive der Beweisfunktion nichts einzuwenden. Dahin geht auch die herrschende Lehre.[1354]

1346 Eingehend vorne N 55 ff., N 62 ff.
1347 So etwa auch WEBER, E-Commerce, 322.
1348 Vorne N 218.
1349 Zur digitalen Signatur vorne N 199 ff., 217 f.; zur Handunterschrift N 639 ff.
1350 Vorne N 673 ff., 683 ff.
1351 Eingehend hinten N 782 ff.
1352 So etwa BIZER, 173 f., 175.
1353 Vorne N 648 f.
1354 FormanpassungsG, 16 f.; BIZER, 172 f.; ERBER-FALLER, 121; FRITZSCHE/MALZER, 19, 21; GUT/WILDHABER, Abschnitt 2.7.3.; OBERHOLZER, Digitale Signatur, 441; RIHACZEK, Beweis, 130; ROSSNAGEL, Rechtsverkehr, 98; SEIDEL, Dokumentenschutz II, 485 f.

4. Übereilungsschutz

a) *Allgemeines*

857 Oftmals sollen Formvorschriften eine Partei dazu anhalten, *die Folgen ihrer Erklärung genau zu überdenken*.[1355] Dies tun sie zum einen aufgrund der im Gegensatz zu einem formfreien Geschäft nötigen zusätzlichen Schritte (Verrichtungen zum Aufsetzen der Papierurkunde, Ausformulieren der Gedanken oder Lesen eines vorgefertigten Vertrages, Versand mit der Briefpost) und der dadurch gewonnenen Bedenkzeit[1356] und zum anderen dadurch, dass der Gebrauch der Schriftform gemäss allgemeiner Übung schon auf eine gewisse Bedeutung eines Geschäfts hinweist.[1357] Beispiele für Formvorschriften mit überwiegendem Übereilungsschutzzweck sind Art. 493 Abs. 1 OR (Bürgschaft)[1358], Art. 216 Abs. 1 OR (Kaufvertrag über ein Grundstück)[1359] sowie Art. 8 Abs. 1 KKG (Konsumkreditvertrag).

b) *Zeitliche Verzögerung*

858 Wenn auch durch die geschilderten Informationspflichten des Zertifizierungsdiensteanbieters in Kombination mit einer räumlich vom PC separierten Signiereinheit zumindest eine gewisse Bremswirkung geschaffen werden kann, so bleibt doch die Tatsache, dass die zeitliche Verzögerung zwischen Entschlussfassung und Erklärungsabgabe (Unterzeichnung, allenfalls zusätzlich Postversand) bei elektronischen Signaturen stark reduziert wird; soll doch der Einsatz elektronischer Kommunikationsmittel gerade hier für Effizienzgewinne sorgen. Hält man sich vor Augen, dass ein bisher schriftformbedürftiges Geschäft neu auch über eine WWW-Eingabemaske abgeschlossen werden können soll, die auch mit einer externen Signiereinheit innert kürzester Zeit ausgefüllt und abgeschickt werden kann, wird klar, dass die Warnfunktion auch mittels qualifizierter elektronischer Signaturen nicht gleich wie mit einer Handunterschrift erfüllt werden kann.[1360]

859 Der Vorschlag von RIHACZEK, elektronisch signierte Dokumente eine Zeit lang zur Korrektur zurückzuhalten,[1361] ist wohl kaum praktikabel und verursacht zudem wieder eine Zeitverzögerung, was durch den Einsatz elektronischer Kommunikationsmittel gerade verhindert werden soll.

1355 BK-KRAMER/SCHMIDLIN, N 11, 13 zu Art. 11 OR; ZK-SCHÖNENBERGER/JÄGGI, N 45 zu Art. 11 OR; GAUCH/SCHLUEP/SCHMID, N 498; MK-EINSELE, N 6 zu § 125 BGB; PALANDT-HEINRICHS, N 1 zu § 125 BGB; SCHÖBI, Vertragsschluss, 100 f.; WEBER, E-Commerce, 321.

1356 BK-KRAMER/SCHMIDLIN, N 13 zu Art. 11 OR; SCHÖBI, Vertragsschluss, 100.

1357 BK-KRAMER/SCHMIDLIN, N 13 zu Art. 11 OR; ZK-SCHÖNENBERGER/JÄGGI, N 45 zu Art. 11 OR.

1358 OR-PESTALOZZI, N 1 zu Art. 493 OR.

1359 BK-GIGER, N 9 ff. zu Art. 216 OR.

1360 So etwa auch SCHÖBI, Vertragsschluss, 100; MALZER, 107.

1361 RIHACZEK, Schriftform, 146.

c) *Verkehrsübung*

860 Wie schon bei der Rekognitionsfunktion[1362] führt die bei elektronischen Signaturen bisher fehlende Verkehrsübung auch beim Übereilungsschutz zunächst zu einem Defizit: Die Schriftform steht gemeinhin für Geschäfte von einer gewissen Bedeutung; eine entsprechende Verkehrsübung besteht bei elektronischen Unterschriften bisher nicht.[1363]

861 Ein erster Schritt zur besseren Gewährleistung des Übereilungsschutzes könnte auch hier darin bestehen, den Antragsteller bei der Ausstellung des Zertifikats auf die möglichen Rechtsfolgen der Verwendung einer Unterschrift aufmerksam zu machen, insbesondere auch darauf, dass er nun auch für ihn bedeutsamere Geschäfte elektronisch abschliessen kann.[1364] Nützlich im Zusammenspiel mit einer derartigen Information des Antragstellers ist zudem die räumlich vom PC separierte Ausgestaltung der Signiereinheit – das Unterschreiben hebt sich damit von der üblichen Arbeit mit dem PC ab und erfordert zusätzliche Konzentration des Unterzeichners.[1365]

862 Unnütz wäre m.E. hingegen das (zusätzliche) Einfügen einer eingescannten Unterschrift:[1366] Abgesehen davon, dass lange nicht alle Computerbenutzer die Kenntnisse haben, um eine Grafik in ein Dokument einzufügen, dürfte auch ein derartiger Vorgang – etwa durch Dokumentenvorlagen – regelmässig automatisiert werden, was jegliche Schutzwirkung eliminierte. Auch die Forderung nach einer Softwarefunktion, welche den Unterzeichner beim Setzen einer Signatur explizit auf die Bedeutung seines Tuns hinweist[1367] ist m.E. problematisch, weil häufig wiederholte Arbeitsabläufe am Computer erfahrungsgemäss schnell zu Routine werden und Hinweisdialoge schon nach kürzester Zeit nicht mehr gelesen, sondern einfach weggeklickt werden.[1368]

d) *Zusammenfassung*

863 Die bei elektronischen Signaturen fehlende zeitliche Verzögerung zwischen Entschlussfassung und Erklärungsabgabe sowie in gewissem Grade die fehlende Verkehrsübung schränken die Möglichkeiten zum Einsatz elektronischer Signaturen als Mittel zum Schutz vor Übereilung ein.[1369]

1362 Vorne N 836 ff.

1363 So etwa auch ERBER-FALLER, 121 f.; Alexander ROSSNAGEL, Schriftliche Stellungnahme zum Thema Datensicherheit, Kassel 1997, http://www.uni-kassel.de/fb10/oeff_recht/publikationen/dis-Datensicherheit.ghk, Abschnitt 3, «Anpassung von Formvorschriften».

1364 Vorne N 844; kritisch SCHÖBI, Vertragsschluss, 101.

1365 Begründung FormanpassungsG, 17; RIHACZEK, Schriftform, 145 f.; ROSSNAGEL, Rechtsverkehr, 98.

1366 Solches fordert EBBING, 275.

1367 So BIZER, 172; vgl. auch Botschaft Totalrevision Bundesrechtspflege, 4264.

1368 Im Ergebnis gleich MALZER, 107 f.

5. Dokumentenabschluss

Mit dem Namenszug am Ende der Urkunde *schliesst der Aussteller seine Erklärung ab*. Er zeigt damit an, dass er den bis dahin geschriebenen Text kennt und anerkennt.[1370] Text, der nach der Unterschrift steht, wird gemäss bundesgerichtlicher Praxis regelmässig nicht mehr als Teil der unterzeichneten Urkunde betrachtet.[1371] So gesehen hängt die Dokumentabschlussfunktion eng mit der beschriebenen Rekognitionsfunktion zusammen. 864

Signaturverfahren, die den Nachweis der Dokumentenintegrität ermöglichen, erwarten bei der Erzeugung der Signatur den zu signierenden Text als Input.[1372] Das Dokument wird durch eine solche Signatur insofern abgeschlossen, als nur die in die Erzeugung und Prüfung mit einbezogenen Bereiche als unterzeichnet gelten können. 865

Von grosser Bedeutung ist indessen, dass der Unterzeichner das Dokument auch wirklich vollständig zu Gesicht bekommt.[1373] Es muss deutlich angezeigt werden, wenn am Ende des Bildschirmrandes noch weitere Daten folgen. Meines Erachtens reicht hierzu eine einfache Bildlaufleiste (Scrollbar) nicht aus, weil wenig geübte Benutzer diese oft übersehen.[1374] 866

Die durch die Dokumentenabschlussfunktion gestellten Anforderungen können durch eine sinnvolle Gestaltung der Signiersoftware erfüllt werden. Die Dokumentenabschlussfunktion steht damit einer materiellrechtlichen Anerkennung zumindest dann nicht im Wege, wenn die Ausgestaltung der Signiersoftware geregelt ist.[1375] 867

6. Verhandlungsabschluss

Erst nach Abschluss der Vertragsverhandlungen setzen die Parteien ihre Unterschriften unter das fertige Vertragswerk bzw. lassen dieses öffentlich beurkunden. Diesfalls hat die Form auch die Funktion, *diesen Abschluss der Verhandlungen anzuzeigen;* das Papier ist vollendet und nicht mehr Entwurf.[1376] 868

1369 Gl. M. BJ, Gutachten, 462; zumindest implizit Botschaft ZertES, 5687; Begründung FormanpassungsG, 17; GASSER, 93; Marlis KOLLER-TUMLER, E-Banking und Konsumentenschutz, in: Wolfgang WIEGAND (Hrsg.), E-Banking, Rechtliche Grundlagen, Bern 2002, 143 ff., 158; MALZER, 107; OERTEL, 421; RIHACZEK, Beweis, 130; SCHAUER, 68; SCHÖBI, Vertragsschluss, 100. A.M. BIZER, 172; MENZEL, 154 ff.; RIHACZEK, Schriftform, 145 f.; VISCHER/ALBRECHT. Unklar SEIDEL, Dokumentenschutz II, 485.

1370 MALZER, 102; MENZEL, 153 f.; RASSMANN, 37; RIHACZEK, Beweis, 130; SEIDEL, Dokumentenschutz II, 485; zur Position der Unterschrift auf der Urkunde schon vorne N 819 f.

1371 Dazu schon vorne N 820.

1372 Vorne N 43 ff.

1373 So etwa auch HAMMER/BIZER, 691.

1374 So die eigene Erfahrung des Autors aus einer Reihe von EDV-Kursen für Juristen.

1375 Vgl. auch Begründung FormanpassungsG, 16; ERBER-FALLER, 121; RIHACZEK, Beweis, 130; ROSSNAGEL, Rechtsverkehr, 98; SEIDEL, Dokumentenschutz II, 485.

1376 BK-KRAMER/SCHMIDLIN, N 11 zu Art. 11 OR; BIZER, 171; HELDRICH, 91; KUNER/MIEDBRODT, Abschnitt II.

869 Beim Versand eines Entwurfs per Post wird regelmässig nicht das Papier selbst, sondern – wenn überhaupt – ein Begleitschreiben unterzeichnet. Dies dürfte bei elektronischen Signaturen ähnlich sein, sofern die Dokumente als Attachments versandt werden. Aber auch dann, wenn der Entwurfstext in eine E-Mail-Nachricht hineinkopiert wird, ist davon auszugehen, dass aufgrund von Begleitnotizen oder anderer Umstände auf den Entwurfsstatus des Dokumentes geschlossen werden kann. Zudem spielt die Verhandlungsabschlussfunktion in erster Linie bei gewillkürten Formvorschriften eine Rolle. Sie steht damit einer materiellrechtlichen Anerkennung der elektronischen Signatur nicht im Wege.[1377]

7. Kontrolle

870 In seltenen Fällen dienen Schriftformvorschriften der *staatlichen Kontrolle privaten Handelns*.[1378] So ist etwa nach Art. 11 des Waffengesetzes zur Übertragung einer Waffe ein schriftlicher Vertrag bestimmten Inhaltes aufzusetzen, der während zehn Jahren aufzubewahren ist. Im Zusammenspiel mit der Pflicht, Identität und Alter des Erwerbenden zu prüfen von Art. 9 Abs. 2 WG und der Waffenerwerbsscheinpflicht beim Ersterwerb von Art. 8 WG soll hier eine Überwachung des Waffenhandels erreicht werden.[1379]

871 Im deutschen Recht wird von Kontrollfunktion etwa im Hinblick auf die behördliche Überwachung kartellrechtlicher Verträge gesprochen. Nach § 15 GWB besteht etwa ein Schriftformerfordernis für Preisbindungen bei Verlagserzeugnissen.[1380] Ziel ist hier, den Wettbewerbsbehörden die Überprüfung dieser – erlaubten – Abreden zu ermöglichen und geheime Nebenabreden zu erschweren.[1381]

872 Die Effektivität derartiger Formvorschriften hängt in erster Linie von der Beweiskraft des eingesetzten Beurkundungsverfahrens und der Möglichkeit der dauernden Aufbewahrung ab (Perpetuierungsfunktion[1382]); im Lichte der Überlegungen zur Beweiskraft[1383] erscheint die Kontrollfunktion hinsichtlich der Anerkennung qualifizierter elektronischer Signaturen daher zunächst unproblematisch. Anders als im Zivilrecht ist im Strafrecht die Zulässigkeit des Anscheinsbeweises aber aufgrund der Unschuldsvermutung zumindest zweifelhaft.[1384] Anders als bei der Handunter-

---

1377 So auch BIZER, 172.

1378 PALANDT-HEINRICHS, N 1 zu § 125 BGB; MK-EINSELE, N 8 zu § 125 BGB; ERBER-FALLER, 119; Sigrun ERBER-FALLER, Gesetzgebungsvorschläge der Bundesnotarkammer zur Einführung elektronischer Unterschriften, CR 6/1996, 375 ff., 377.

1379 Philippe WEISSENBERGER, Die Strafbestimmungen des Waffengesetzes, Unter Berücksichtigung von Art. 260^{quater} StGB, AJP 2/2000, 153 ff., 159 f.

1380 RITTNER, § 9 N 23.

1381 RITTNER, § 8 N 6.

1382 Dazu sogleich N 873 ff.

1383 Vorne N 852 ff.

1384 Eingehend (zum Anscheinsbeweis, nicht aber zur Frage der Unterschriftenprüfung) Markus MÜLLER, Anscheinsbeweis im Strafprozess, am Beispiel der Feststellung von Kausalität und von Dispositionsprädikaten, Berlin 1998.

schrift, bei welcher der Anscheinsbeweis bloss bei einer gerichtlichen Überprüfung des Schriftbildes zum Einsatz kommt und durch Sachverständigengutachten verhältnismässig einfach gestützt werden kann, sollte deren Resultat in Zweifel gezogen werden, sind aussagekräftige Sachverständigengutachten über qualifizierte elektronische Signaturen nur in wenigen Fällen denkbar.[1385] Weil die Schriftform im geschilderten Art. 11 WG wohl in erster Linie der Strafverfolgung dienen soll, kann die elektronische Signatur die Funktion der Handunterschrift hier m. E. *nicht optimal* erfüllen.[1386]

8. Perpetuierung

873 Willenserklärungen werden durch die Schriftform dauerhaft verkehrsfähig gemacht.[1387] Man spricht von der *Perpetuierungsfunktion* der Schriftform.[1388]

874 Für eine Erfüllung der Perpetuierungsfunktion ist zunächst von Bedeutung, dass die zur Überprüfung benötigten Zertifikate ausreichend lange zur Verfügung stehen oder der Inhaber einer Urkunde die Beweiskraft der Signaturen von Zertifizierungsdiensteanbieter und Unterzeichner zumindest durch Zeitstempel verlängern kann. Dies bereitet kaum technische Schwierigkeiten.[1389]

875 Problematisch ist indessen, dass elektronisch gespeicherte Dokumente regelmässig umkopiert werden müssen, weil die Speichersysteme veralten und alte Medien damit bereits nach einigen Jahren nicht mehr lesbar sind,[1390] sowie dass Dateiformate schnell veralten, weil neuere Softwareversionen teilweise nicht mehr vollständig zu älteren Versionen kompatibel sind und alte Softwareversionen teilweise auf neuerer Hardware nicht mehr funktionieren. Bei der Einstellung der Weiterentwicklung eines Produkts tritt dieses Problem noch verschärft auf.

876 Meist befinden sich Dokumente jedoch bereits nach kurzer Zeit in den Händen desjenigen, der Ansprüche auf sie stützt (so etwa eine Zessionsurkunde in den Händen des Zessionars), sodass dieser selbst für das Umkopieren und die Verfügbarkeit der zur Sichtbarmachung nötigen Software sorgen kann. Grössere Schwierigkeiten verursacht der Zeitablauf nur in Fällen, bei denen Aufbewahrungsverantwortung und Aufbewahrungsinteresse auseinanderfallen. Beispiel hierfür ist die geschilderte Kontrollfunktion der Schriftform im Waffengesetz, bei der dem zur Aufbewahrung des schriftlichen Vertrages Verpflichteten bei Zulassung elektronischer Dokumente zusätzlich die Pflicht aufzuerlegen wäre, diese in lesbarem Zustand zu erhalten.[1391]

1385 Allein gestützt auf die Signatur kann keine Aussage über Echtheit oder Fälschung gemacht werden; vorne N 852 ff.

1386 Vgl. zudem sogleich N 875.

1387 BIZER/MIEDBRODT, 138.

1388 Begründung FormanpassungsG, 16; BIZER/MIEDBRODT, 138; FRITZSCHE/MALZER, 19; MALZER, 102; SEIDEL, Dokumentenschutz I, 410.

1389 Zur Verlängerung der kryptographischen Sicherheit durch Zeitstempel vorne N 191 ff.

1390 RIHACZEK, Schriftform, 145.

1391 Soeben N 870 ff.

877 Die Perpetuierungsfunktion ist damit zumindest dann gewährleistet, wenn derjenige, der ein Interesse am dauerhaften Bestand eines elektronischen Dokumentes hat, dieses auch aufbewahrt.[1392]

9. Inhaltsklarheit

878 Formvorschriften nötigen die Parteien, ihre Gedanken auszuformulieren, was Missverständnissen vorbeugen kann.[1393] Dies zum einen zwischen den Parteien selbst (etwa bei Informationspflichten bezüglich Widerrufsrechten u. dgl.), zum anderen aber auch gegenüber Dritten, die sich im Rechtsverkehr auf eine Urkunde verlassen (etwa bei der Forderungsabtretung nach Art. 165 Abs. 1 OR).[1394]

879 Die Funktion der Inhaltsklarheit ist unabhängig von einer Unterschrift und kann daher bereits durch die Textform gewahrt werden. Hinsichtlich der materiellrechtlichen Anerkennung elektronischer Signaturen stellt sie kein Problem dar.

10. Information

880 Formvorschriften werden vor allem in jüngerer Zeit auch zum Schutz der schwächeren Vertragsparteien erlassen. Sie sollen dabei vor allem auch dazu dienen, einer Vertragspartei Informationen über die ihr zustehenden Rechte zukommen zu lassen.[1395] Beispiele sind etwa die Informationspflicht über das Widerrufsrecht bei Fernabsatzverträgen nach VE-BGEG[1396] oder die Formularpflicht nach Art. 266l Abs. 2 OR für Kündigungen bei Wohn- und Geschäftsräumen.

881 Auch die Informationsfunktion stellt für die Anerkennung elektronischer Signaturen kein Problem dar.[1397]

11. Zusammenfassung

882 Die meisten Funktionen der Handunterschrift können zwar durch elektronische Signaturen genauso gut wahrgenommen werden. Es gibt jedoch Funktionen, die eine bestimmte Ausgestaltung der Signiersoftware und damit eine genaue gesetzliche Regelung voraussetzen, wie die Dokumentenabschlussfunktion, oder solche wie die Warnfunktion, die – mangels Verkehrsübung und Bewusstsein in der Bevölkerung einerseits und aufgrund der durch die Einführung des elektronischen Verkehrs gerade bezweckten Beschleunigung andererseits – durch elektronische Signaturen kaum je-

---

1392 Im Ergebnis gleich Begründung FormanpassungsG, 16.
1393 BK-KRAMER/SCHMIDLIN, N 14 zu Art. 11 OR; HELDRICH, 91.
1394 BK-KRAMER/SCHMIDLIN, a. a. O.; HELDRICH, a. a. O.
1395 Botschaft ZertES, 5683, 5688; Begleitbericht VE-BGEG, 14 f.; GAUCH/SCHLUEP/SCHMID, N 500a; SCHÖBI, Vertragsschluss, 102.
1396 Vorne N 501 ff.
1397 Dem Absender obliegt indessen durchwegs der Nachweis für die korrekte Information des Empfängers. Bei der Formularpflicht bei Kündigungen besteht zudem ein zusätzliches Interesse des Mieters an Rechtssicherheit (Beweisfunktion), weshalb die Textform allein nicht ausreicht.

mals ersetzt werden können. Nur schlecht zu erfüllen vermag die elektronische Signatur ferner die Überwachungsfunktion, sofern diese – wie im Waffengesetz – in erster Linie der Erleichterung der Strafverfolgung dienen soll.

883 Handunterschrift und elektronische Signatur können damit nicht als funktional äquivalent betrachtet werden. Die materiellrechtliche Anerkennung elektronischer Unterschriften bedarf einer differenzierten Betrachtungsweise.[1398]

III. Materiellrechtliche Anerkennung de lege lata

A. Fragestellung

884 Einige Stimmen in der Literatur befürworten eine Anerkennung der elektronischen Signatur auf dem Wege einer geltungszeitlich-teleologischen Auslegung der Formvorschriften *(richterrechtliches Modell)*.[1399] Nachdem im letzten Abschnitt gezeigt wurde, dass Handunterschrift und elektronische Signatur nur teilweise funktional äquivalent sind, soll untersucht werden, ob zumindest in denjenigen Bereichen, in denen funktionale Äquivalenz vorliegt, auf dem Wege der Auslegung des geltenden Rechts eine Anerkennung erfolgen kann.

B. Analoge Anwendung des Begriffs der Handunterschrift

885 Das Bundesgericht setzt bei der Beurteilung von Formvorschriften einen strengen Massstab an. Einzige Ausnahme von der Formstrenge ist die Anwendung des *Rechtsmissbrauchsverbotes* in denjenigen Fällen, in denen sich eine Partei bei Geschäften, die aus Gründen des Übereilungsschutzes formbedürftig wären erst nach der Erfüllung auf die Formvorschrift beruft und das Geleistete zurückfordert. Das Bundesgericht argumentiert, der Warnzweck der Formvorschrift sei durch die Wartezeit zwischen Vertragsabschluss und Erfüllung regelmässig bereits gewahrt, beschränkt sich indessen darauf, bei nicht gewahrten Formvorschriften die *Rückforderung* zu verweigern und gewährt keine Möglichkeit eine *Leistung* zu verlangen. Das formungültige Rechtsgeschäft entspricht demnach einer Naturalobligation.[1400]

886 Über diese Grenze hinauszugehen und bei fehlendem oder bereits erfülltem Zweck auch eine Leistungsklage zuzulassen hiesse, den Wortlaut von Art. 14 Abs. 1 OR zu

---

1398 So etwa auch LANGENBACH (FN 326): «Eine Gesetzesänderung, die auf eine pauschale Gleichsetzung der beiden 'Unterschriftsformen' [d.h. der elektronischen und der Handunterschrift] abzielt, ist nicht zu verantworten»; ERBER-FALLER, 122; OERTEL, 421; ROSSNAGEL, Rechtsverkehr, 99.

1399 Für eine richterrechtliche materiellrechtliche Anerkennung etwa EBBING, 273 ff., für eine richterrechtliche prozessuale Anerkennung KILIAN, 609; vgl. auch vorne N 264.

1400 Vgl schon vorne N 289 ff.

missachten, der eindeutig nach einer Handunterschrift auf festem Urkundenstoff verlangt.[1401] Auch wenn der Wortlaut keine absolute Grenze der Auslegung bildet,[1402] ist doch bei Formvorschriften das Vertrauen der Rechtsunterworfenen in einen klaren Gesetzeswortlaut besonders zu schützen: Als quasi «künstlicher» gesetzgeberischer Eingriff in das Konsensprinzip[1403] sind Formvorschriften weniger interpretationsfähig als Normen, die gesellschaftliche Wertungen festhalten und sich deshalb laufend fortentwickeln.

887 Gerade auch in Fällen des Drittschutzes[1404] spielt die Rechtssicherheit eine bedeutende Rolle – befände sich doch beispielsweise der debitor cessus bei der Präsentation einer elektronisch signierten Zessionsurkunde durch den Zessionar bis zu einem ersten Richterspruch im Zwiespalt, ob die Formvorschrift von Art. 165 Abs. 1 OR gewahrt und er damit zur Zahlung an den Zessionar verpflichtet sei. Die Befürwortung einer richterrechtliche Lösung würde bedeuten, das durch Art. 165 OR geschaffene Vertrauen des Gläubigers in die Gültigkeit einer Forderungsabtretung durch die entstehende rechtliche Unsicherheit wieder zunichte zu machen. Demnach wäre eine richterrechtliche Anerkennung der elektronischen Signatur nicht sinnvoll.

888 Ein Grund für die Integration elektronischer Signaturen in die Rechtsordnung liegt zudem darin, deren Verbreitung zu fördern.[1405] Können vertragsschliessende Parteien aber mangels einer klaren Regelung nicht sicher sein, ob ein bestimmtes Signaturverfahren der Voraussetzungen des Gesetzes entspricht, so werden sie dieses meiden. Will man also die Verbreitung elektronischer Signaturen fördern, so kommt man damit um eine gesetzliche Anerkennung nicht herum. Dies ist auch die in der Literatur in weit überwiegender Mehrheit vertretene Auffassung.[1406]

C. Elektronische Signatur als Faksimile-Unterschrift

889 Eine analoge Anwendung der Bestimmung zur Faksimile-Unterschrift[1407] auf elektronische Signaturen ist m.E. nicht sinnvoll, weil elektronische Signaturen nicht nur – wie die Faksimile-Unterschrift – in Massengeschäften zur Anwendung gelangen, sondern der Handunterschrift in allen Bereichen gleichgestellt werden sollen. Die Faksimile-Unterschrift ist zudem bei gesetzlichen Formvorschriften ohnehin fast bedeutungslos.

1401 Vorne N 813 ff.; BK-KRAMER/SCHMIDLIN, N 4 der allgemeinen Erläuterungen zu Art. 12-15 OR.

1402 Das Bundesgericht spricht von Methodenpluralismus, wobei je nach Situation einmal dieses und einmal jenes Auslegungselement den Vorrang erhält; BGE 127 III 323 m.H.; vgl. etwa auch HÖHN, 124 f.; KRAMER, 59 ff.; Roger ZÄCH, Tendenzen der juristischen Auslegungslehre, ZSR N.F. 96 (1997) I 313 ff., 332 f.

1403 Vorne N 801 f.

1404 Vorne N 808.

1405 Vgl. Art. 1 Abs. 2 Bst. b E-ZertES; Botschaft ZertES, 5682; vorne N 483 ff.

1406 Etwa Botschaft ZertES, 5684 f.; BJ, Gutachten, 453 f.; FRITZSCHE/MALZER, 20; MALZER, 107; OBERHOLZER, Digitale Signatur, 435 f.

1407 Art. 14 Abs. 2 OR; vorne N 818.

D. Elektronische Signatur als beglaubigtes Handzeichen

MALZER sieht die elektronische Signatur als Parallelfall zum *beglaubigten Handzeichen* nach § 126 Abs. 1 BGB[1408] (allerdings ohne gestützt auf diese Vorschrift explizit eine Anerkennung zu fordern).[1409] Meines Erachtens hinkt dieser Vergleich indessen, weil eine Beglaubigung die Leistung des Handzeichens selbst bezeugt und damit eine sehr hohe Sicherheit mit sich bringt, während eine Zertifizierung ausschliesslich die Zuordnung des Prüfschlüssels zu einer Person sicherstellt und nur mittelbar eine Aussage darüber macht, ob wirklich diese Person unterzeichnet hat. 890

E. Fazit

Eine materiellrechtliche Anerkennung der elektronischen Signatur auf dem Wege einer geltungszeitlichen Auslegung bzw. analogen Anwendung geltenden Rechts kann nicht befürwortet werden. 891

IV. Materiellrechtliche Anerkennung de lege ferenda

A. Fragestellung

Mit Art. 14 Abs. 2bis E-OR schlägt der Bundesrat eine pauschale Gleichsetzung von qualifizierter elektronischer Signatur mit Anbieteranerkennung nach E-ZertES und Handunterschrift vor.[1410] Ausnahmeregelungen sind nicht vorgesehen, der Bundesrat sieht die fehlende Übereilungsschutzwirkung vielmehr bereits durch das im Vorentwurf zum Bundesgesetz über den elektronischen Geschäftsverkehr vorgesehene Widerrufsrecht für Konsumenten-Fernabsatzverträge kompensiert.[1411] 892

Zunächst ist in der Folge der vorgeschlagene Wortlaut zu analysieren. Danach werden mögliche Alternativen zur Wahrung des Übereilungsschutzes beschrieben und schliesslich die bundesrätliche Lösung gewürdigt. 893

1408 Dieser entspricht Art. 15 OR.
1409 MALZER, 104.
1410 Zu den verschiedenen Regelungsmodellen vorne N 265.
1411 Botschaft ZertES, 5687; zum BGEG vorne N 487 ff.

B. Art. 14 Abs. 2bis E-OR

1. Allgemeines

894 Art. 14 Abs. 2bis OR soll wie folgt lauten:

> *«Der eigenhändigen Unterschrift gleichgestellt ist die qualifizierte elektronische Signatur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom (...) über Zertifizierungsdienste im Bereich der elektronischen Signatur beruht und auf den Namen einer natürlichen Person lautet.»*

895 Die Struktur dieser Norm ist – bezieht man auch die Definitionen der Tatbestandsmerkmale von Art. 2 E-ZertES mit ein – ausgesprochen komplex. Der Tatbestand umfasst vier Hauptmerkmale und rund ein Dutzend Untermerkmale, die sich aus den Definitionen der Hauptmerkmale ergeben.

2. Tatbestand

a) Anwendungsbereich

896 Art. 14 Abs. 2bis E-OR ist auf sämtliche gesetzlichen Schriftformvorschriften des Privatrechts anwendbar.[1412] Anders als noch der Vorentwurf beschränkt er sich nicht mehr auf mittels elektronischem Datenaustausch geschlossene Verträge,[1413] sondern lässt etwa auch einseitige Willenserklärungen zu. Zudem vermeidet er die durch die Formulierung des Vorentwurfs möglicherweise geweckten Zweifel hinsichtlich der Anwendbarkeit auf unter Anwesenden geschlossene Verträge.[1414]

897 Die Botschaft geht zudem davon aus, dass der Artikel auch Formvorschriften des eidgenössischen und kantonalen öffentlichen Rechts beeinflusst, sofern sich diese auf die Schriftform beziehen.[1415] Darunter sollen etwa Vorschriften wie Art. 82 Abs. 1 SchKG (Erfordernis der unterschriebenen Schuldanerkennung zur provisorischen Rechtsöffnung) fallen.[1416]

b) Signaturprüfung

898 Die Prüfung der Signatur mit einer gesetzeskonformen Signaturprüfeinheit (Art. 6 Abs. 3 E-ZertES) muss selbstverständlich ein positives Resultat zeitigen; für die Echtheit der Signatur ist der Anscheinsbeweis zulässig.[1417]

1412 Botschaft ZertES, 5707.

1413 Art. 15a VE-OR; dazu etwa Begleitbericht VE-BGES, 28; SCHLAURI, Basistechnologie, 85; kritisch etwa auch BRINER, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 161; CLUSIS, a.a.O., 162; ÉCONOMIESUISSE, a.a.O., 163; SWICO, a.a.O., 169.

1414 WIEGAND, 129.

1415 Botschaft ZertES, 5688.

1416 Eingehend zur prozessualen Anerkennung schon vorne N 772 ff.

1417 Vorne N 673 ff., 683 ff.

c) *Qualifizierte elektronische Signatur*

899 Es muss sich um eine qualifizierte elektronische Signatur im Sinne von Art. 2 Bst. c E-ZertES handeln, d.h. um eine *fortgeschrittene elektronische Signatur*, die auf einer *sicheren Signiereinheit* nach Art. 6 Abs. 1 und 2 E-ZertES und auf einem *qualifizierten* und *zum Zeitpunkt des Erzeugens gültigen Zertifikat* beruht.[1418]

aa) Qualifiziertes Zertifikat

900 Qualifiziert ist ein Zertifikat gemäss Art. 2 Bst. f E-ZertES dann, wenn es den von Art. 7 E-ZertES und den entsprechenden Ausführungsbestimmungen vorgeschriebenen Inhalt aufweist.[1419] Dieser kann mit Hilfe der Signaturprüfeinheit einfach angezeigt und mit Art. 7 E-ZertES verglichen werden. Bei der Beurteilung der Konformität mit den Ausführungsbestimmungen hingegen wäre das Gericht wohl überfordert, weshalb m.E. prima facie auf die Bezeichnung als qualifiziertes Zertifikat durch den anerkannten Zertifizierungsdiensteanbieter und eine oberflächliche Prüfung abgestellt werden darf (nur qualifizierte Zertifikate dürfen als solche bezeichnet werden).[1420]

901 Das qualifizierte Zertifikat ist bereits Voraussetzung für das Vorliegen einer qualifizierten elektronischen Signatur nach Art. 2 Bst. f E-ZertES, wird aber – wohl aus Gründen der besseren Formulierbarkeit – in Art. 14 Abs. 2bis E-OR wiederholt.

bb) Gültigkeit zum Signierzeitpunkt

902 Das Zertifikat muss nach Art. 2 Bst. c E-ZertES zum Zeitpunkt des Erzeugens der Signatur gültig gewesen sein.

903 Ist das Zertifikat auch zum Zeitpunkt seiner Beurteilung durch das Gericht noch gültig, kann auch von der Gültigkeit des Zertifikats zum Zeitpunkt des Erzeugens ausgegangen werden.[1421] Ist es hingegen mittlerweile abgelaufen oder gesperrt, so ist nachzuweisen, dass dies nicht vor dem Erzeugen der Signatur erfolgte.

904 Der Signierzeitpunkt kann nicht den in einem elektronischen Dokument enthaltenen Zeitangaben (etwa Absendezeit einer E-Mail-Nachricht) entnommen werden, weil diese Angaben durch einen allfälligen Fälscher rückdatiert werden könnten. Sein Nachweis erfolgt vielmehr separat (im Idealfall durch einen Zeitstempel oder allenfalls durch andere Beweismittel wie Zeugenaussagen u.dgl.).[1422] Der Anscheinsbeweis für den Signierzeitpunkt ist *ausgeschlossen*.[1423]

1418 Dazu vorne N 187ff., 516.
1419 Dazu schon vorne N 532ff.
1420 Vgl. auch vorne N 743.
1421 Der Beginn der Gültigkeitsdauer eines Zertifikats ist – anders als Art. 7 Abs.1 Bst. e E-ZertES vermuten liesse – belanglos; vgl. schon vorne N 107.
1422 Eingehend vorne N 172ff., 187ff.
1423 Dazu schon vorne N 681, 748f.; vgl. auch JACCARD, Projet, 90.

905 Ob ein Zertifikat zum Signierzeitpunkt abgelaufen war, ergibt sich aus dem in ihm selbst enthaltenen Ablaufdatum, das die Signaturprüfeinheit anzeigt.[1424] Ob es gesperrt war, kann anhand der durch den Zertifizierungsdiensteanbieter im Internet bereitgehaltenen Certificate Revocation List eruiert werden, die auch Informationen über den Zeitpunkt der Sperrung enthält.[1425] Diese wird durch die Signaturprüfeinheit automatisch aus dem Internet geladen und die Sperrung angezeigt.[1426]

cc) Fortgeschrittene elektronische Signatur

906 Als fortgeschrittene elektronische Signatur gilt eine Signatur dann, wenn sie *i)* die Voraussetzungen von Art. 2 Best. b E-ZertES erfüllt, d.h. ausschliesslich dem Halter zugeordnet ist, *ii)* dessen Identifizierung ermöglicht, *iii)* mit Mitteln erzeugt wird, die der Halter unter seiner alleinigen Kontrolle halten kann und *iv)* die Datenintegrität gewährleistet.[1427]

907 Wie bereits dargelegt, kann m.E. für eine qualifizierte elektronische Signatur gestützt auf das positive Prüfresultat, auf den Nachweis, dass das Zertifikat zum Zeitpunkt der Unterzeichnung gültig war sowie auf den Nachweis, dass der Zertifizierungsdiensteanbieter zum Signierzeitpunkt anerkannt war, der *Anscheinsbeweis der Echtheit* geführt werden.[1428] Wenn nun aber für die Echtheit der Anscheinsbeweis zulässig ist, so muss dieser m.E. auch bei der Beurteilung der materiellrechtlichen Anerkennung für das Untermerkmal der fortgeschrittenen elektronischen Signatur zulässig sein, denn es wäre inkonsequent, eine unverdächtige Signatur zwar prima facie als echt anzuerkennen, ihre Formgültigkeit hernach jedoch abzulehnen, weil nicht *voll bewiesen* sei, dass es sich um eine fortgeschrittene elektronische Signatur handelt.

dd) Sichere Signiereinheit

908 Weiteres Untermerkmal des Tatbestandsmerkmals der qualifizierten elektronischen Signatur ist, dass diese mit einer sicheren Signiereinheit erstellt wurde. Die Voraussetzungen an diese werden in Art. 6 E-ZertES sowie in den entsprechenden Ausführungsbestimmungen festgelegt.

909 Auch für dieses Tatbestandsmerkmal muss m.E. der Anscheinsbeweis zulässig sein.[1429]

d) Anbieteranerkennung

910 Das Zertifikat, auf dem die qualifizierte elektronische Signatur beruht, hat von einem nach Art. 3 ff. E-ZertES anerkannten Zertifizierungsdiensteanbieter zu stammen. Die Anerkennung des Anbieters muss indessen nur zum Zeitpunkt der Zertifizierung be-

---

1424 Vgl. etwa Abbildung 3 auf Seite 25; vgl. auch vorne N 107.
1425 Vorne N 88.
1426 Eingehend vorne N 86 ff.
1427 Dazu schon vorne N 515 sowie 375 ff.
1428 Vorne N 673 ff., 683 ff.
1429 Vorne N 746.

stehen. Wurde sie seither aufgehoben, so wird die Certificate Revocation List anderweitig verfügbar gehalten und damit die Überprüfbarkeit der Signaturen weiterhin gewährleistet – der Widerruf der Anerkennung wirkt sich daher nicht auf die Formgültigkeit aus.[1430]

e) Name einer natürlichen Person

911 Ein qualifiziertes Zertifikat kann nach Art. 2 Bst. f i.V.m. Art. 7 E-ZertES auf den Namen einer *natürlichen oder juristischen Person* lauten. Die materiellrechtliche Anerkennung einer Signatur ist indessen nach Art. 14 Abs. 2bis E-OR nur möglich, sofern das Zertifikat auf den Namen einer natürlichen Person lautet.[1431] Der Name ist Inhalt des Zertifikats, der wiederum mittels jeder Signaturprüfeinheit angezeigt werden kann. Diese Regelung ist der Handunterschrift nachempfunden; der Vertreter einer juristischen Person unterzeichnet auch mit eigenem Namen und nicht mit dem Namen der juristischen Person.

912 Ähnlich ist die Lage hinsichtlich des Einsatzes von *Pseudonymen*: Ein qualifiziertes Zertifikat kann zwar nach Art. 7 Abs. 1 Bst. c E-ZertES auch auf ein Pseudonym lauten. Nach der Botschaft ist eine materiellrechtliche Anerkennung jedoch nicht möglich, es sei denn, die Betroffenen wüssten, wer dahintersteht.[1432] Dieser Auffassung ist wohl zumindest bei Formvorschriften mit Drittschutzfunktion[1433] (etwa bei der Forderungsabtretung nach Art. 165 Abs. 1 OR) zuzustimmen. Hat eine Partei indessen mit Pseudonym unterzeichnet, so dürfte ihr auf das Vorliegen eines Pseudonyms gestützter Einwand der Formungültigkeit regelmässig treuwidrig sein.[1434]

f) Beweis insbesondere

913 Der Tatbestand von Art. 14 Abs. 2bis E-OR weist zwar genau besehen eine komplexe Struktur auf, der Beweis dieser Voraussetzungen gestaltet sich aber nicht ganz so schwierig, weil eine Reihe von Tatbestandsmerkmalen aus anderen erschlossen werden können (allenfalls mittels Anscheinsbeweis). In der Folge soll gezeigt werden, welche Elemente unmittelbar nachzuweisen sind und welche durch Schlüsse mittelbar erlangt werden können.

aa) Überprüfung durch das Gericht selbst

914 Verfügt das Gericht über die zur Überprüfung von elektronischen Signaturen und Zeitstempeln notwendige Infrastruktur (Signaturprüfeinheit),[1435] ist ihm das signierte Dokument elektronisch einzureichen.

1430 Art. 13 Abs. 2 E-ZertES; vorne N 522. Zum Nachweis der Anbieteranerkennung im Einzelnen bereits vorne N 741.
1431 Botschaft ZertES, 5707.
1432 Botschaft ZertES, 5707; anders BIZER/HERDA, 27.
1433 Vorne N 808.
1434 Zu undifferenziert noch SCHLAURI, Basistechnologie, 78. Vgl. auch vorne N 816 ff.
1435 Zur Frage, unter welchen Umständen dies allenfalls sinnvoll wäre vorne N 782 ff.

915 Das Gericht hat folgende Elemente zu überprüfen:

- Positives Resultat der Signaturprüfung mit einer gesetzeskonformen Prüfeinheit;
- die Bezeichnung des Zertifikats als qualifiziertes Zertifikat;[1436]
- die Ausstellung des Zertifikats auf den Namen einer natürlichen Person;[1437]
- dass der Zertifizierungsdiensteanbieter zum Signierzeitpunkt anerkannt war;[1438]
- dass das Zertifikat zum Signierzeitpunkt noch gültig war;[1439]
- falls zum Zeitpunkt der Beurteilung der Signatur der Zertifizierungsdiensteanbieter nicht mehr anerkannt oder das Zertifikat abgelaufen oder gesperrt ist, den Signierzeitpunkt.[1440]

916 Zwei Tatbestandsmerkmale von Art. 14 Abs. 2bis E-OR *(Ausstellung des Zertifikats auf den Namen einer natürliche Person* und *Anerkennung des Zertifizierungsdiensteanbieters zum Signierzeitpunkt)* können und müssen daher streng bewiesen werden.

917 Das Tatbestandsmerkmal des *qualifizierten Zertifikats* kann prima facie aus dessen Bezeichnung als solches geschlossen werden.[1441]

918 Das Tatbestandsmerkmal der *qualifizierten elektronischen Signatur* ergibt sich aus folgenden Überlegungen nach Art. 2 Bst. c E-ZertES:

- eine *fortgeschrittene elektronische Signatur* liegt vor, weil ein zum Signierzeitpunkt gültiges qualifiziertes Zertifikat eines zum Signierzeitpunkt anerkannten Zertifizierungsdiensteanbieters eingesetzt wurde (Anscheinsbeweis);[1442]
- eine *sichere Signiereinheit* wurde eingesetzt, weil der anerkannte Anbieter dem Schlüsselhalter eine solche empfohlen hat (Anscheinsbeweis);[1443]
- ein *qualifiziertes Zertifikat* vorliegt (Anscheinsbeweis);[1444]

1436 Die Bezeichnung ist für qualifizierte Zertifikate als Inhalt vorgeschrieben; vorne N 533. Der Inhalt kann mit der Signaturprüfeinheit angezeigt werden; vgl. etwa Abbildung 3 auf Seite 25.

1437 Der Name ist ebenfalls Inhalt des Zertifikats (vorne N 108, 533) und kann damit durch die Signaturprüfeinheit angezeigt werden.

1438 Eruierbar anhand der von der Akkreditierungsstelle publizierten Liste der anerkannten Anbieter; vorne N 522. Ist der Anbieter zum Zeitpunkt der Beurteilung der Signatur durch das Gericht noch anerkannt, so kann prima facie auf seine Anerkennung zum Signierzeitpunkt geschlossen werden. Ist er es nicht mehr, so ist zusätzlich der Signierzeitpunkt zu überprüfen; dazu sogleich.

1439 Ist das Zertifikat zum Zeitpunkt seiner der Beurteilung durch das Gericht noch gültig, so kann unmittelbar auf seine Gültigkeit zum Signierzeitpunkt geschlossen werden; vorne N 107, insbesondere FN 144. Ist es hingegen abgelaufen oder gesperrt, so muss zusätzlich nachgewiesen werden, dass der Signierzeitpunkt vor dem Ablauf- bzw. Sperrzeitpunkt lag. Ablauf- bzw. Sperrzeitpunkt werden beide durch die Signaturprüfeinheit angezeigt. Zum Nachweis des Signierzeitpunkts sogleich.

1440 Der Signierzeitpunkt ist etwa durch einen Zeitstempel oder Zeugenaussagen nachzuweisen; vorne N 681, 748 f. Genau genommen kann nicht der Signier*zeitpunkt* bewiesen werden, sondern die Tatsache, dass die Signatur vor dem Ablauf bzw. der Sperrung des Zertifikats respektive vor dem Ende der Anerkennung des Anbieters *existierte;* vorne N 172 ff., 189.

1441 Vorne N 900.

1442 Vorne N 906 ff.

1443 Vorne N 746, 908.

- das Zertifikat zum Signierzeitpunkt *gültig* war (voller Beweis nötig).[1445]

bb) Überprüfung mittels Gutachten

919 Verfügt das Gericht nicht über eine Signaturprüfeinheit, so muss ein Sachverständigengutachten (allenfalls eine Konformitätsbestätigung[1446]) zumindest folgende Sachfragen klären:

- Inhalt der signierten Nachricht;
- Positives Resultat der Signaturprüfung;
- Inhalt des Zertifikats;
- Qualifikation des Zertifikats als qualifiziertes Zertifikat i. S. v. Art. 7 E-ZertES in Verbindung mit den entsprechenden Ausführungsbestimmungen;
- falls das Zertifikat zum Zeitpunkt seiner Beurteilung gesperrt oder abgelaufen ist, wann die Sperrung oder der Ablauf erfolgte;
- falls das Zertifikat zum Zeitpunkt seiner Beurteilung gesperrt oder abgelaufen ist und ein Zeitstempel existiert, die Gültigkeit des Zeitstempels.

920 Die folgenden Merkmale kann das Gericht selbst überprüfen:

- Ausstellung des Zertifikats auf den Namen einer natürlichen Person;[1447]
- Anerkennung des Zertifizierungsdiensteanbieters zum Signierzeitpunkt.[1448]

3. Rechtsfolge

921 Rechtsfolge von Art. 14 Abs. 2bis E-OR ist die materiellrechtliche Anerkennung der qualifizierten elektronischen Signatur mit Anbieteranerkennung. Der Entwurf folgt – wie schon der Vorentwurf – dem Modell der ausnahmslosen materiellrechtlichen Anerkennung.[1449]

922 Zu beachten ist, dass die Anerkennung nur Normen betrifft, die ausschliesslich eine Handunterschrift fordern, d. h. solche mit einfacher Schriftlichkeit sowie qualifizierter Schriftlichkeit mit Ausführlichkeitsvorschriften.[1450] In Fällen der Eigenschriftlichkeit (etwa bei der eigenhändigen letztwilligen Verfügung nach Art. 505 ZGB oder der Bürgschaft natürlicher Personen mit einem Haftungsbetrag unter 2000 Franken nach Art. 493 Abs. 2 OR) ist dies nicht der Fall. Das Wertpapierrecht ist auf Forderungen zugeschnitten, die in einem Papier verkörpert sind; eine Gleichstellung ist

1444 Soeben N 917.
1445 Soeben N 915.
1446 Vorne N 782 ff.
1447 Anhand des dargelegten Zertifikatsinhaltes.
1448 Anhand der durch die Akkreditierungsstelle publizierten und damit m. E. als gerichtsnotorisch geltenden Liste der anerkannten Anbieter (vorne N 522) sowie des durch das Gutachten dargelegten Zeitstempels (fehlt ein solcher, so kann der Nachweis des Signierzeitpunktes natürlich auch anderweitig erbracht werden, etwa durch Zeugenaussagen).
1449 Vorne N 265.
1450 Zur qualifizierten Schriftlichkeit vorne N 825.

demnach auch insoweit nicht möglich.[1451] Gleiches gilt für die öffentliche Beurkundung.[1452] In Fällen des Formularzwangs, wie etwa bei der Ankündigung einer Mietzinserhöhung nach Art. 269d Abs. 1 OR, liegt es in der Kompetenz der Kantone, Formulare auch in elektronischer Form zur Verfügung zu stellen.[1453]

C. Alternativen zu Ausnahmebestimmungen

1. Widerrufsrecht

923 Der beschriebene Vorentwurf zu einem Bundesgesetz über den elektronischen Geschäftsverkehr (BGEG) schlägt ein Widerrufsrecht für Fernabsatzverträge vor. Unabhängig davon, ob das Ziel der goods-in-hand-Entscheidung mit der vorgeschlagenen Formulierung überhaupt zu erreichen ist,[1454] kompensiert ein Widerrufsrecht in jedem Fall zumindest den durch den Einsatz elektronischer Signaturen verloren gegangenen Übereilungsschutz. Dies wird denn auch vom Bundesrat als Begründung für den Verzicht auf Ausnahmebestimmungen von der Anerkennung vorgebracht.[1455]

2. Textform

924 In Bereichen, in denen ausschliesslich eine bestimmte Information zu vermitteln ist, in denen also weder Beweis- noch Warn- oder andere Funktionen der Unterschrift benötigt werden, kann der Gesetzgeber auf eine Unterschrift ganz verzichten. Man spricht diesfalls von Textform oder Darstellung durch Text.[1456]

3. Öffentliche Beurkundung

925 Das Gutachten des Bundesamtes für Justiz über «Digitale Signatur und Privatrecht» (Vertragsrecht) nennt für den Fall der ausnahmslosen Anerkennung die Möglichkeit, die Schriftform an Orten, wo eine Anerkennung aus Gründen des fehlenden Übereilungsschutzes nicht gewünscht ist, durch die öffentliche Beurkundung zu ersetzen.[1457] Eine derart drastische Verschärfung schiesst jedoch in den meisten Bereichen über das angestrebte Ziel hinaus. Der Weg der öffentlichen Beurkundung wurde denn auch offenbar nicht weiter verfolgt.

1451 Botschaft ZertES, 5687, 5707.
1452 Botschaft ZertES, 5687.
1453 Botschaft ZertES, 5687.
1454 Dazu vorne N 502.
1455 Botschaft ZertES, 5687; vgl. auch SCHÖBI, Vertragsschluss, 101.
1456 Eingehend vorne N 821 ff.
1457 BJ, Gutachten, 463; vgl. auch vorne N 828 ff.

D. Wertung des bundesrätlichen Vorschlags

1. Übereilungsschutz jenseits von Fernabsatzverträgen

926 Das im VE-BGEG vorgeschlagene Widerrufsrecht ist auf eine verhältnismässig kleine Zahl von Geschäftstypen beschränkt und deckt eine Reihe von Fällen nicht ab, in denen der Übereilungsschutz eine Rolle spielt. Beispiele für Formvorschriften, die durch die Anerkennung der elektronischen Signatur ihrer Warnfunktion verlustig gehen, sind etwa das Schenkungsversprechen und der Konsumkreditvertrag.[1458] Die bei Letzterem entstehende Lücke könnte beispielsweise dort genutzt werden, wo ein Finanzinstitut den Zugriff auf Online-Dienstleistungen mit qualifizierten elektronischen Signaturen anerkannter Zertifizierungsdiensteanbieter absichert. Die Regelung des E-ZertES würde es neu ermöglichen, über den gleichen Kanal auch Konsumkredite anzubieten. In Anbetracht der zielgenauen Werbemöglichkeiten (etwa Bannerwerbung für einen Kleinkredit bei niedrigem Kontostand) wird die durch die Vorlage geschaffene Gefahr offenbar, dass Kunden zu übereilten Kreditanträgen verlockt werden. Die Vorlage führt gerade im Bereich der Konsumkredite, in dem das Bedürfnis nach Übereilungsschutz eben erst durch das Konsumkreditgesetz von 1993 anerkannt wurde, wieder zu einem eklatanten Abbau des Schutzes. Der Bundesrat gibt zwar zu verstehen, die in der EU in Vorbereitung befindliche Richtlinie über Finanzdienstleistungen[1459], die ebenfalls ein Widerrufsrecht für Konsumentenverträge vorsieht, dereinst auch übernehmen zu wollen.[1460] Angesichts der politischen Verhältnisse hierzulande ist aber unklar, wie realistisch dieses Ansinnen ist.[1461]

927 Wollte man indessen im Geschäftsverkehr auf Übereilungsschutz überhaupt verzichten,[1462] hätte als Gebot der Verhältnismässigkeit an die Stelle der Anerkennung der elektronischen Signatur konsequenterweise ein völliger Verzicht auf Formvorschriften treten müssen. Es ist beispielsweise nicht einzusehen, weshalb bei einem elektronisch geschlossenen Vertrag über ein Grundstückvorkaufsrecht[1463] überhaupt auf der elektronischen Signatur beharrt wird, kann diese doch den mit der Norm verfolgten Übereilungsschutzzweck kaum erfüllen. Sinnvoll wäre hier entweder eine Ausnahme von der Anerkennung elektronischer Unterschriften für Vorkaufsverträge überhaupt oder aber eine zwischen Handelsrecht und bürgerlichem Recht insofern differenzierende Lösung, als Ersteres auf die Schriftform verzichten, während Letzteres indessen weiterhin eine *Hand*unterschrift verlangen sollte.

1458 Art. 243 Abs. 1 OR; Art. 8 Abs. 2 KKG; zur Ausnahme für Finanzdienstleistungen vorne N 494.

1459 Vorne N 359.

1460 Vgl. schon N 494, insbesondere FN 774.

1461 So spricht schon Rainer GONZENBACH, «Pacta sunt servanda» oder neues Licht auf einem alten Grundsatz – Notizen zu einem Konsumentenschutzproblem, ZSR NF 106 (1987) I 435 ff., 467 hinsichtlich der bestehenden Ausnahme (Art. 40a Abs. 2 OR) von einer «Lex Versicherungsgesellschaften»; weitere Hinweise auf Kritik bei HONSELL/PIETRUSZAK, FN 111.

1462 Solches impliziert Botschaft ZertES, 5687, wenn sie sagt, dass Übereilungsschutz als Mittel zum Schutze der schwächeren Vertragspartei zu verstehen sei.

1463 Art. 216 Abs. 3 OR.

2. Unsichere Inkraftsetzung des Bundesgesetzes über den elektronischen Geschäftsverkehr

928 Durch die (offenbar erst kurz vor der Verabschiedung beschlossene) Aufteilung der Vorlagen zu elektronischem Geschäftsverkehr[1464] und elektronischer Signatur[1465] riskiert der Gesetzgeber im Weiteren eine hinkende Regelung: Würde nämlich Art. 14 Abs. 2bis E-OR verabschiedet und das im VE-BGEG vorgesehene Widerrufsrecht später verworfen (dies scheint angesichts der teilweise geharnischten Reaktionen auf die Vorlage durchaus möglich – zudem wollte man durch die Aufteilung ja gerade eine Verzögerung der mehr oder minder unbestrittenen Signaturvorlage durch den heikleren VE-BGEG vermeiden), so blieben – nebst den genannten Formvorschriften jenseits der Fernabsatzverträge[1466] – auch die laut BGEG vom Widerrufsrecht erfassten Bereiche ohne Übereilungsschutz.

3. Ergebnis: Forderung nach Ausnahmebestimmungen

929 Der bundesrätliche Ansatz ist in seiner Absolutheit abzulehnen, weil er aufgrund der bereichsweise fehlenden funktionalen Äquivalenz von Handunterschrift und elektronischer Signatur Lücken in das System der Formvorschriften reisst. Eine Lösung mit Ausnahmevorschriften würde es erlauben, bedeutend differenzierter auf die einzelnen Formvorschriften einzugehen.

930 Nicht nur aufgrund der fehlenden Europa-Kompatibilität[1467] erscheint es daher unverständlich, weshalb der Bundesrat – ohne auf die in der Vernehmlassung erhobene Kritik[1468] einzugehen – an der ursprünglichen Lösung festhielt.

V. Einheit der Urkunde

931 Gleichzeitig mit Art. 14 Abs. 2bis E-OR schlägt der Bundesrat auch die Aufhebung von Art. 13 Abs. 2 OR vor, der bestimmt, dass auch Briefwechsel und Telegramm als schriftlich gelten.[1469] Dass eine einheitliche Urkunde nicht verlangt ist, ergibt sich bereits aus Art. 13 Abs. 1 OR. Notwendig ist einzig, dass die unterzeichneten Dokumente auf einen bestimmten Vertrag Bezug nehmen.[1470]

1464 VE-BGEG; vorne N 487 ff.
1465 VE-BGES bzw. E-ZertES; vorne N 479 ff.
1466 Soeben N 926.
1467 Art. 9 Abs. 2 der E-Commerce-Richtlinie erlaubt den Mitgliedstaaten Ausnahmen; vorne N 363 ff.
1468 Etwa KANTON BASEL STADT, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 159; Simon SCHLAURI/Reto KOHLAS, in: Zusammenstellung der Vernehmlassungen zum VE-BGES, 167 f.; vgl. auch SCHLAURI/KOHLAS, 254 ff.
1469 Botschaft ZertES, 5707.
1470 Botschaft ZertES, 5707; OR-SCHWENZER N 10 zu Art. 13 OR; BK-KRAMER/SCHMIDLIN, N 5 zu Art. 13 OR; anders ZK-SCHÖNENBERGER/JÄGGI, N 64 zu Art. 13 OR. Zur abweichenden Lösung in *Deutschland* vorne N 449 f.

Dies gilt selbstverständlich auch für elektronisch signierte Dokumente.[1471] 932

VI. Aspekte der gewillkürten Form

Nach der Auslegungsregel von Art. 16 Abs. 2 OR gelten für die Erfüllung der gewillkürten Form im Zweifel die Erfordernisse der gesetzlich vorgeschriebenen Schriftlichkeit, sofern die Abrede auf Schriftform ohne nähere Bezeichnung lautet.[1472] Mit der materiellrechtlichen Anerkennung der qualifizierten elektronischen Signatur mit Anbieteranerkennung bezieht sich Art. 16 Abs. 2 OR neu auch auf diese.[1473] 933

Zu beachten ist allerdings, dass Art. 16 Abs. 2 OR die Zustimmung der Parteien zum elektronischen Verkehr nicht vorwegnimmt. Diese ergibt sich auch nicht bereits daraus, dass eine Partei über ein qualifiziertes Zertifikat verfügt, sondern erst aus einer (allerdings auch konkludent möglichen) Einwilligung.[1474] 934

Vereinbaren die Parteien explizit die elektronische Form, so dürfte dies meist dazu dienen, technische Arbeitsabläufe zu vereinfachen. Weil die handschriftliche Form diese Vereinfachung gerade ausschliesst, wird ihre Anwendung bei vereinbarter elektronischer Form daher regelmässig nicht dem Willen der Parteien entsprechen. 935

1471 Botschaft ZertES, 5707.
1472 OR-SCHWENZER, N 7 zu Art. 16 OR.
1473 Botschaft ZertES, 5707.
1474 Eine elektronisch versandte Offerte etwa dürfte als konkludentes Einverständnis zum elektronischen Verkehr gesehen werden; Botschaft ZertES, 5687.

§ 13 Zusammenfassung der Ergebnisse

I. Sicherungsinfrastruktur

936 Hinsichtlich der gesetzlichen Regelung der Sicherungsinfrastruktur kann zwischen einem ex-ante- und einem ex-post-Ansatz unterschieden werden. Beim ex-ante-Ansatz werden die Zertifizierungsdiensteanbieter einer Vorabprüfung durch eine spezialisierte Stelle unterzogen («Anerkennung der Zertifizierungsdiensteanbieter»), an die hernach bestimmte Rechtswirkungen der Zertifikate geknüpft sind (insbesondere die materiellrechtliche Anerkennung entsprechender Signaturen, Haftungs- sowie allenfalls Beweisregeln). Beim ex-post-Ansatz werden die Voraussetzungen dieser Rechtswirkungen erst im Nachhinein durch die Gerichte geprüft. Die Vorteile des ex-ante-Ansatzes liegen in der zumindest teilweisen Entlastung der Gerichte von der komplexen Signaturprüfung und in der höheren Rechtssicherheit, ihre Nachteile bestehen im für die ex-ante-Prüfung zu betreibenden zusätzlichen Aufwand, der die Kosten der Zertifikate erhöht, und darin, dass ausländische Zertifizierungsdiensteanbieter zusätzlich zur Anerkennung in ihrem Heimatstaat eine Anerkennung in der Schweiz benötigen, was deren Markteintritt erschwert.[1475]

937 Der Bundesrat hat sich im E-ZertES für den ex-ante-Ansatz entschieden. Sollen digitale Zertifikate die vom Gesetz vorgesehenen Rechtswirkungen haben (materiellrechtliche Anerkennung entsprechender Signaturen, Haftung des Signierschlüsselhalters für von ihm verschuldete Missbräuche), muss der Zertifizierungsdiensteanbieter durch eine spezielle Stelle anerkannt worden sein. Werden diese Rechtswirkungen indessen nicht benötigt – etwa weil sie durch Vertrag ebenfalls herbeigeführt werden können – so kann die Anbieteranerkennung unterbleiben (Prinzip der freiwilligen Anerkennung der Zertifizierungsdiensteanbieter). Der Nachteil des ex-ante-Ansatzes, dass ausländische Anbieter einer zusätzlichen Anerkennung in der Schweiz bedürfen, wird unter anderem dadurch kompensiert, dass der Bundesrat in einem anderen Staat bereits anerkannte Anbieter in der Schweiz pauschal staatsvertraglich anerkennen kann.[1476]

II. Beweiswert elektronischer Signaturen

A. Problematik

938 Der Beweis der Abgabe einer Willenserklärung mittels einer elektronischen Signatur setzt den Nachweis der folgenden Kette von Zusammenhängen voraus:

1475 Vorne N 280 ff., 311 ff.
1476 Vorne N 512, 525 f.

- Signierschlüssel – Prüfschlüssel (kryptographische Sicherheit);
- Prüfschlüssel – Name (sichere Zertifizierung);
- Name – Schlüsselhalter (korrekte Identifikation des Schlüsselhalters durch die Registrierstelle);
- Schlüsselhalter – Unterzeichner (alleinige Kontrolle des Signierschlüssels durch den Halter zum Signierzeitpunkt);
- Unterzeichner – Dokument (korrekte Präsentation des Dokuments);
- Dokument – Signatur (kryptographische Sicherheit).

939 Dieser Nachweis ist im Prinzip nur durch aufwändige Sachverständigengutachten zu erbringen, was die Praxistauglichkeit digitaler Signaturen stark verschlechtert. Die Feststellungen, dass wirklich der Schlüsselhalter und nicht ein Dritter den Signierschlüssel eingesetzt hat, dass dem Schlüsselhalter dabei das signierte Dokument korrekt angezeigt wurde, und allenfalls auch der Nachweis, dass die Registrierstelle den Signierschlüsselhalter korrekt identifizierte, sind zudem naturgemäss auch durch Gutachten gar nicht zur vollen Überzeugung des Gerichts nachweisbar.

940 Dennoch sind elektronische Signaturen gerade in offenen Benutzergruppen das einzige Mittel, um die schlechte Beweislage bei der elektronischen Kommunikation wesentlich zu verbessern, weshalb sich die Frage stellt, ob nicht Mittel und Wege bestehen, diese Schwierigkeiten zu umschiffen. Nachdem der Bundesrat im Vorentwurf noch eine gesetzliche Vermutung für die Echtheit elektronischer Signaturen vorsah, verzichtet er im E-ZertES nun auf eine explizite Regelung, weshalb m.E. eine richterrechtliche Lösung als sachgerecht erscheint.[1477]

B. Anscheinsbeweis

941 Meines Erachtens kann eine solche Lösung anhand der Praxis zum so genannten *Anscheinsbeweis* gefunden werden. Beim Anscheinsbeweis handelt es sich um eine Beweismassreduktion, die dem Beweisführer dann gewährt wird, wenn beide Parteien in für die anwendbaren Normen (vertraglicher oder gesetzlicher Natur) geradezu symptomatischen Beweisschwierigkeiten stecken, die den Zweck der anwendbaren Normen zu vereiteln drohen, und wenn der Beweisführer die ihm zumutbaren Massnahmen zur Beweissicherung ergriffen hat. Das Gericht kann beim Anscheinsbeweis vom darzulegenden Sachverhalt ausgehen, auch wenn der Beweisführer ihn nur *glaubhaft* gemacht hat.[1478] In der schweizerischen Praxis kommt der Anscheinsbeweis etwa beim Kausalitätsnachweis im Rahmen von Art. 41 OR[1479] oder (wenn auch

---

1477 N 199 ff., 217 ff.

1478 Vorne N 599 ff., 610.

1479 Das Bundesgericht verlangt bloss eine überwiegende Wahrscheinlichkeit für den nachzuweisenden Kausalverlauf, weil diese Norm ansonsten aufgrund der regelmässig auftretenden Beweisschwierigkeiten kaum zur Anwendung gelangen könnte; vorne N 607.

nicht explizit als solcher bezeichnet) beim Beweis mit handschriftlich unterzeichneten Urkunden zur Anwendung.[1480]

C. Anwendung auf elektronische Signaturen

1. Offene Benutzergruppen

942 Die Voraussetzung der Vereitelung des Normzwecks durch geradezu symptomatisch auftretende Beweisschwierigkeiten ist bei elektronischen Signaturen gegeben. Weder Beweisführer noch Beweisgegner sind genau besehen in der Lage, die Echtheit (bzw. die Fälschung) einer elektronischen Signatur zur vollen Überzeugung des Gerichts nachzuweisen. Sowohl ZertES als auch die Rahmenverträge zum Einsatz elektronischer Signaturen als Legitimationsmittel (etwa bei E-Banking) wären indessen nutzlos, bestünde man dennoch auf dem vollen Beweismass.[1481]

943 Es bleibt die Voraussetzung der Ergreifung der zumutbaren Beweissicherungsmassnahmen durch den Beweisführer. In offenen Benutzergruppen ist die Zeitstempelung elektronischer Signaturen beim Empfang die einzige solche Massnahme; sie erlaubt den einfachen Nachweis, dass eine Signatur nicht nach Ablauf oder Sperrung des Zertifikats durch Rückdatierung gesetzt wurde.[1482]

2. Geschlossene Benutzergruppen

944 In geschlossenen Benutzergruppen ist zu differenzieren: Unterzeichnet der Schlüsselhalter jede Transaktion[1483] einzeln, so bleibt es allein bei der Zeitstempelung.[1484] Setzt er die Signatur nur zur Legitimationsprüfung bei der Anmeldung ein und gibt er danach die Transaktionsaufträge ab, ohne sie gesondert zu signieren, so kommt die Absicherung des Servers durch den Systembetreiber gegen Manipulationen hinzu.[1485]

3. Widerlegung des Anscheinsbeweises

945 Die Widerlegung des Anscheinsbeweises kann nur durch Darlegungen erfolgen, die *zumindest ernsthafte Zweifel* am durch Anscheinsbeweis erschlossenen Geschehensablauf wecken. Umgekehrt darf aber auch *nicht der volle Beweis* des Gegenteils ver-

---

1480 Genau besehen ist ein Gericht nicht in der Lage, durch einen visuellen Schriftenvergleich die Echtheit einer Unterschrift zu beurteilen, dennoch gehen die Gerichte bei unverdächtigen Urkunden vielfach von einer «tatsächlichen Vermutung» (sc. einem Anscheinsbeweis) der Echtheit aus; vorne N 648 ff.

1481 Vorne N 673 ff.

1482 Zur Kritik an der Formulierung von Art. 12 E-ZertES, der eine Pflicht der anerkannten Zertifizierungsdiensteanbieter zur Ausstellung von Zeitstempeln statuiert vorne N 198.

1483 Etwa Überweisungsaufträge beim E-Banking.

1484 Derartige Systeme sind derzeit erst in Entwicklung.

1485 Vorne N 727 ff.

langt werden; insbesondere müssen bereits Faktoren ausreichen, die abstrakt einen Missbrauch ermöglichen.

946 Gelingt die Widerlegung, so wechselt die Beweisführungslast wieder auf die Seite des auf die Signatur vertrauenden Dritten. Dieser hat nun für den erschütterten Teil der Indizienkette (aber nur für diesen) den *vollen* Beweis zu erbringen.[1486]

D. Bedeutung der ex-ante-Prüfung insbesondere

947 Die ex-ante-Prüfung ist m.E. als antizipiertes Sachverständigengutachten über die Zuverlässigkeit des Signierverfahrens und Zertifizierungsdiensteanbieters einer qualifizierten elektronischen Signatur zu betrachten. Ihr Sinn liegt unter anderem in der Entlastung der Gerichte von der komplexen Prüfung der Sicherheit einer Signatur und in der Steigerung der Rechtssicherheit, indem dieser Entscheid einer kompetenteren Behörde vorenthalten bleibt.

948 Der Bundesrat hat darauf verzichtet, im Gesetz eine Beweislastumkehr für die Echtheit qualifizierter elektronischer Signaturen mit Anbieteranerkennung vorzusehen. Soll indessen dieser Sinn der ex-ante-Prüfung gewahrt bleiben, so kann der Verzicht auf eine Beweislastumkehr nicht heissen, dass der Beweis mittels elektronischer Signatur zum Zeitpunkt ihrer Beurteilung einer erneuten Detailprüfung von Verfahren und Anbieter bedarf. Vielmehr muss das Gericht m.E. die bei der ex-ante-Prüfung vorweg geprüften Aspekte prima facie als gegeben hinnehmen.[1487]

E. Nachzuweisende Indizien

1. Signaturen ohne Rahmenvertrag

a) Signaturen ohne Anbieteranerkennung

aa) Einfache elektronische Signaturen

949 Sämtliche Glieder der genannten Indizienkette sind gutachterlich darzulegen und voll zu beweisen, was meist nicht zur vollen Überzeugung des Gerichts gelingen dürfte.[1488]

bb) Qualifizierte elektronische Signaturen

950 Die Tatsache, dass es sich um eine qualifizierte elektronische Signatur handelt, ist gutachterlich darzutun, was oftmals schwierig sein dürfte. Hernach greift indessen

---

1486 Vorne N 624, 754.
1487 Vorne N 683 ff.
1488 N 691.

ein Anscheinsbeweis für die Abgabe der unterzeichneten Erklärung durch den Signierschlüsselhalter.[1489]

b) Signaturen mit Anbieteranerkennung

951 Ist nachgewiesen,

- dass eine Signatur bei der Prüfung mit einer gesetzeskonformen Prüfeinheit ein gültiges Resultat liefert;
- dass für den Prüfschlüssel ein qualifiziertes Zertifikat im Sinne von Art. 7 E-ZertES existiert;[1490]
- dass der Zertifizierungsdiensteanbieter zum Signierzeitpunkt anerkannt war;
- und dass das Zertifikat zum Signierzeitpunkt weder abgelaufen noch gesperrt war,

kann m.E. prima facie von der Echtheit der Signatur ausgegangen werden.[1491]

952 Ist der Zertifizierungsdiensteanbieter zum Zeitpunkt der Beurteilung einer Signatur nicht mehr anerkannt, oder ist das Zertifikat zu diesem Zeitpunkt abgelaufen oder gesperrt, so ist für den Nachweis des dritten und vierten Punktes zusätzlich der Nachweis der Existenz der Signatur *vor* dem Widerruf der Anerkennung des Anbieters bzw. dem Ablauf oder der Sperrung des Zertifikats zu erbringen. Dies kann etwa durch Zeitstempel erfolgen.[1492]

2. Signaturen mit Rahmenvertrag

953 Bei Signaturen mit Rahmenvertrag (geschlossene Benutzergruppen) besteht nach schweizerischer Rechtsauffassung die Möglichkeit, durch eine parteiautonome Legitimationsordnung das Fälschungsrisiko weitestgehend auf den Kunden zu überwälzen, sodass der Systembetreiber nur noch das Vorliegen einer gültigen Signatur sowie die Nichtmanipulierbarkeit seines Serversystems nachweisen muss, aber nicht mehr die gesamte Indizienkette, welche auf die Willenserklärung des Unterzeichners schliessen liesse.[1493]

954 Zum Nachweis der Nichtmanipulierbarkeit des Systems ist der Anscheinsbeweis zulässig, sofern dargetan ist, dass das System dem Stand der Technik entspricht. Die Anforderungen können gesenkt werden, indem der Kunde die Signatur nicht mehr nur zur Anmeldung am System einsetzt, sondern jeden einzelnen Transaktionsauftrag signiert.

1489 Vorne N 693.

1490 Nur ein solches liefert Gewähr für die kryptographische Sicherheit. Die Beurteilung der Frage, ob ein qualifiziertes Zertifikat vorliegt, hängt allein von dessen Inhalt ab; Art. 2 Bst. f E-ZertES i.V.m. Art. 7 E-ZertES. Dieser kann mittels der Signaturprüfeinheit einfach untersucht werden.

1491 Vorne N 739 ff.

1492 Vorne N 753 f.

1493 Vorne N 727 ff.; nicht ausschliessbar ist die Haftung des Systembetreibers für Aufklärung und sorgfältige Systemauswahl; sogleich N 959 f.

III. Haftungsfragen

A. Offene Benutzergruppen

1. Situation de lege lata

De lege lata lässt sich m.E. keine Haftung des Signierschlüsselhalters für die Geheimhaltung seines Schlüssels begründen. Einzige Ausnahme ist eine explizite Erklärung des Schlüsselhalters, für seinen Schlüssel haften zu wollen (in der Beantragung eines Zertifikats allein kann aber gerade keine solche Erklärung gesehen werden). Bei unsicheren Systemen stösst eine solche Haftungserklärung zudem an die Grenzen von Art. 27 ZGB; sie dürfte nur bei qualifizierten elektronischen Signaturen schrankenlos gültig sein.[1494] 955

2. Situation de lege ferenda: Art. 59a E-OR

Nach Art. 59a E-ZertES soll der Schlüsselhalter gegenüber jedem Dritten haften, der sich sich auf sein *gültiges qualifiziertes Zertifikat* eines *anerkannten Zertifizierungsdiensteanbieters* verlassen hat. Zumindest für Zertifikate anerkannter Anbieter wird die geschilderte Haftungslücke damit geschlossen. 956

Meines Erachtens ist indessen nicht einzusehen, weshalb die Haftung auf Zertifikate *anerkannter* Anbieter beschränkt werden soll, denn das dem E-ZertES zu Grunde liegende Prinzip der freiwilligen Anerkennung der Zertifizierungsdiensteanbieter verlangt auch nach einer Haftung für Zertifikate ohne Anbieteranerkennung. 957

B. Geschlossene Benutzergruppen

Das Fälschungsrisiko kann wie erwähnt weitestgehend auf den Signierschlüsselhalter überwälzt werden.[1495] 958

Vertraglich nicht ausschliessen kann der Systembetreiber (insbesondere eine Bank) indessen seine auftragsrechtlichen Pflichten, den Kunden über die Risiken des eingesetzten Systems (und dabei allenfalls auch über die grundsätzliche Eignung des eingesetzten Signierverfahren für den entsprechenden Zweck) aufzuklären, und (insbesondere bei Signaturen, die nur zur Legitimationsprüfung, nicht aber zur Unterzeichnung der Einzeltransaktionen eingesetzt werden) sein eigenes Serversystem sorgfältig auszuwählen.[1496] 959

1494 Vorne N 694 ff.
1495 Soeben N 953.
1496 Vorne N 732 ff.

C. Haftung der Zertifizierungsdiensteanbieter

960 Systematisch unbefriedigend statuiert der E-ZertES zunächst in Art. 8 - 14 die Pflichten der *anerkannten* Zertifizierungsdiensteanbieter, um diese danach über die Haftungsnorm von Art. 16 (Abs. 1) auch auf die *nicht anerkannten* Anbieter qualifizierter Zertifikate auszudehnen. Der Entwurf bedarf diesbezüglich m.E. einer Korrektur. Im Weiteren ist zu fragen, ob nicht aus Gründen der Europa-Kompatibilität anstelle der milden Kausalhaftung eine Verschuldenshaftung vorzuziehen wäre.[1497]

961 Die einzige Möglichkeit, die Haftung der Zertifizierungsdiensteanbieter zu beschränken liegt darin, in die Zertifikate Haftungsausschlussklauseln nach Art. 7 Abs. 2 E-ZertES zu integrieren (Beschränkung des Transaktionswertes oder Einsatzbereiches eines Zertifikats). Sollen diese Klauseln indessen Wirkung zeigen, so muss ihre Bekanntheit beim auf eine Signatur vertrauenden Dritten – entgegen der Auffassung des Bundesrates – ohne weiteres vorausgesetzt werden können.[1498]

IV. Prozessuale Anerkennung

962 Der Bundesrat geht davon aus, dass mit der materiellrechtlichen Anerkennung elektronischer Signaturen auch die prozessuale Anerkennung einhergeht, d.h. die Zulassung elektronisch signierter Dokumente zum Urkundenbeweis und insbesondere zur provisorischen Rechtsöffnung. Dies zumindest dann, wenn das entscheidende Gericht mit der zur Überprüfung der Signaturen nötigen Infrastruktur ausgestattet ist. Meines Erachtens spräche unter diesen Umständen in der Tat nichts gegen eine prozessuale Anerkennung.[1499]

963 Die Problematik liegt indessen darin, dass die Gerichte nicht nur die Infrastruktur zur Überprüfung der Signaturen, sondern auch über Software zur Anzeige der verwendeten Dateiformate verfügen müssen, und darin, dass eine flächendeckende Ausstattung der Gerichte mit Signaturprüfeinheiten vorderhand mangels Auslastung nicht sinnvoll sein dürfte. Beide Probleme liessen sich m.E. durch eine Auslagerung der Signaturprüfung an qualifizierte Stellen (etwa einzelne entsprechend ausgerüstete Notariate oder besondere Signaturprüfstellen) lösen, wie es in Art. 21 VE-BGES noch in ähnlicher Weise vorgesehen war. Derartige Stellen hätten die zur Beurteilung der Echtheit nötigen und nicht durch das Gericht selbst überprüfbaren Aspekte in einer für das Gericht lesbaren Form (auf Papier oder in elektronischer Form) zu bestätigen. Derartige Bestätigungen können m.E. als öffentliche Urkunden betrachtet werden, welche als beglaubigte Kopien anstelle der elektronisch gespeicherten Originalurkunden zum Urkundenbeweis zuzulassen sind.[1500]

1497 Vorne N 528 ff., 530.
1498 Vorne N 762 f.
1499 Vorne N 782 f.

V. Materiellrechtliche Anerkennung

A. Allgemeines

964 Eine richterrechtliche materiellrechtliche Anerkennung, wie sie teilweise in der Literatur gefordert wurde, ist abzulehnen; die Anerkennung hat insbesondere aus Gründen der Rechtssicherheit durch den Gesetzgeber zu erfolgen.[1501] Der Bundesrat hat dies denn auch so vorgeschlagen: Handunterschrift und qualifizierte elektronische Signatur mit Anbieteranerkennung sollen durch einen neuen Art. 14 Abs. 2bis OR gleichgestellt werden.[1502]

B. Kritik am bundesrätlichen Regelungsvorschlag

965 Der Bundesrat anerkennt zwar, dass die elektronische Signatur insbesondere die Übereilungsschutzfunktion der Handunterschrift nur ungenügend erfüllen kann, schlägt aber trotzdem eine ausnahmslose materiellrechtliche Anerkennung vor. Dies mit der Begründung, das im Bundesgesetz über den elektronischen Geschäftsverkehr (BGEG) vorgeschlagene Widerrufsrecht für Konsumentenfernabsatzverträge würde zur Kompensation dieses Defizits ausreichen.[1503]

966 Meines Erachtens wäre indessen dem Regelungsmodell der Europäischen Union (Anerkennung mit Ausnahmebestimmungen) der Vorzug zu geben, denn erstens ist unsicher, ob das Widerrufsrecht nach VE-BGEG überhaupt jemals Gesetz wird – wurden doch die Gesetzesänderungen zu elektronischen Signatur und elektronischem Geschäftsverkehr gerade deshalb auf zwei Vorlagen aufgeteilt, weil bei Letzterem einige Opposition zu befürchten war – und zweitens weist auch diese Vorlage noch einige empfindliche Lücken auf – so ist etwa der Bereich der Finanzdienstleistungen vom Geltungsbereich ausgenommen und damit insbesondere auch Konsumkreditverträge, die vor noch nicht einmal zehn Jahren einer Formvorschrift mit Übereilungsschutzwirkung unterstellt wurden.[1504]

C. Voraussetzungen des Art. 14 Abs 2bis E-OR

967 Die vorgeschlagene Anerkennungsnorm Art. 14 Abs. 2bis E-OR ist sehr komplex. Bezieht man die Definitionen von Art. 2 E-ZertES mit ein, so enthält sie über ein Dutzend tatbestandsmässige Voraussetzungen.[1505] Genau besehen kann indessen ein

---

1500 Vorne N 784 ff.
1501 Vorne N 884 ff.
1502 Vorne N 892 ff.
1503 Vorne N 892.
1504 Vorne N 926 ff.
1505 Vorne N 894 ff.

grosser Teil dieser Merkmale – teilweise auf dem Wege des Anscheinsbeweises – aus anderen erschlossen werden.

968 Für eine Anwendung zu prüfen bleiben die folgenden Elemente:

- Positives Resultat der Signaturprüfung mit einer gesetzeskonformen Prüfeinheit;
- Bezeichnung des Zertifikats als qualifiziertes Zertifikat;
- Ausstellung des Zertifikats auf den Namen einer natürlichen Person;
- Anerkennung des Zertifizierungsdiensteanbieters zum Signierzeitpunkt;
- Gültigkeit des Zertifikats zum Signierzeitpunkt;
- falls zum Zeitpunkt der Beurteilung einer Signatur der Zertifizierungsdiensteanbieter nicht mehr anerkannt oder das Zertifikat abgelaufen oder gesperrt ist, der Signierzeitpunkt[1506].

969 Sofern das Gericht über eine Signaturprüfeinheit verfügt, kann es diese Prüfung selbst durchführen.[1507]

1506 Zum Nachweis des Signierzeitpunkts vorne N 952.
1507 Vorne N 914 ff.

Stichwortverzeichnis

A

Abschlussfunktion der Unterschrift, s. Dokumenten- und Verhandlungsabschlussfunktion
absolut notwendiger Zertifikatsinhalt nach E-ZertES 145
administrativen Hilfstätigkeit, Zertifizierungsdienste als 144
Akkreditierung der Anerkennungsstellen 141, 142
Akkreditierung der Zertifizierungsdiensteanbieter
– s. auch Anerkennung der Zertifizierungsdiensteanbieter
– als den EU-Mitgliedstaaten verbleibende Kompetenz 108
– als Voraussetzung der Anerkennung von Signaturen ausländischer Anbieter 108
– ausländische Anbieter nach SigG 01 114
– Begriff 80, 101
– beweisrechtliche Aspekte 117, 124
– mit Wurzelzertifikat 28
– nach SigG 01 113
Akkreditierungsstelle *141*, 142, 195, 207
Aktenverkehr mit Gerichten
– s. auch E-Government
– nach E-BGG 137
– nach FormanpassungsG 125
Anbieterakkreditierung, s. Akkreditierung bzw. Anerkennung der Zertifizierungsdiensteanbieter
Anbieteranerkennung, s. Akkreditierung bzw. Anerkennung der Zertifizierungsdiensteanbieter
Anbieterinnen von Zertifizierungsdiensten
– Begriff nach E-ZertES 141
– s. auch Zertifizierungsdiensteanbieter
Anerkennung de Zertifizierungsdiensteanbieter
– Bedeutung jenseits der materiellrechtlichen Anerkennung 133
Anerkennung der digitalen Signatur
– Begriff 73
– s. materiellrechtliche und prozessuale Anerkennung
Anerkennung der Zertifizierungsdiensteanbieter
– s. auch Akkreditierung der Zertifizierungsdiensteanbieter und ex-ante-Regelungsansatz
– als Gütezeichen 113, 114
– als privatrechtliches Rechtsgeschäft 143
– als Voraussetzung der Haftung des Schlüsselhalters nach Art. 59a E-OR 199
– als Voraussetzung von Art. 14 Abs. 2bis E-OR 236, 238
– Begriff 77
– beweisrechtliche Aspekte 107
– erleichterte für ausländische Anbieter 84
– ex lege 85
– internationale Aspekte 84
– internationale, nach E-ZertES 143
– nach E-ZertES 141 - 143
– nach Signaturrichtlinie 100
– Regelungsmodelle 78
– staatsvertragliche bei ausländischen Anbietern 84
– Überblick 142
Anerkennung eines Textes als Willenserklärung, s. Rekognition
Anerkennungsnorm
– Begriff 74
– Regelungsmodelle 79
– s. auch Art. 14 Abs. 2bis E-OR
Anerkennungsstelle
– als private Stelle 141
– Begriff 77
– Begriff nach E-ZertES 141
– Haftung nach E-ZertES 149
Anscheinsbeweis *157 - 168*
– als Aspekt der Beweiswürdigung 162
– als Beweismassreduktion 163, 164, 167
– als Rechtsbeweis 162
– als Regelungsmodell zur Steigerung der Beweiskraft digitaler Signaturen 76
– Begriff 164, 167
– bei abgelaufenem oder gesperrtem Zertifikat 197
– bei EC-Karten 123, 160, 190
  – s. auch EFTPOS-Fall
– bei Systemen mit Unterzeichnung der einzelnen Transaktionen 192
– beim Nachweis der materiellrechtlichen Anerkennung 234, 236, 237, 238
– Beweislasttheorie 161
– Beweismasstheorie 162
– dogmatische Einordnung 161 - 164
– Ergreifung der zumutbaren Beweissicherungsmassnahmen als Voraussetzung 160, 161, 163, 166, 182, 192, 193, 197, 245
– für Begebung eines Schriftstücks 173, 202
– für die Manipulationssicherheit des Serversystems 192
– für elektronische Signatur im Allgemeinen 178 - 180
– für elektronische Signaturen mit ex-ante-Prüfung ohne Rahmenvertrag 195

– für qualifizierte elektronische Signaturen ohne ex-ante-Prüfung 183
– gesetzlicher
  – als Regelungsmodell zur Steigerung der Beweiskraft digitaler Signaturen 76, 181
  – Begriff 76
  – nach § 292a ZPO DE 84, 117, 123, 124, 182, 183
– gestützt auf die ex-ante-Prüfung 182
– im Strafprozess 228
– materiellrechtliche Theorie 164
– nicht bei ausgedruckter elektronischer Signatur 204
– nicht bei unsignierten elektronischen Dokumenten 169
– nicht bei unsignierten Papierdokumenten 174
– nicht bei Zufallsurkunden ohne ex-ante-Prüfung 186
– nicht für die Gültigkeit des Zertifikates zum Signierzeitpunkt 197
– notwendiges Beweismass für Zulässigkeit 166-167
– nur in Einzelfällen bei Signaturen ohne ex-ante-Prüfung und Rahmenvertrag 183
– typischer Geschehensablauf 160, 166
– Urkundenbeweis als 172-173, 176
– Ursprung 158
– von der ex-ante-Prüfung auf die Anerkennung einer Signatur (Regelungsmodell) 80
– Voraussetzungen 164-168
– vorgezogener, nach SigG 97 110, 117
– vorgezogener, nicht mehr nach SigG 01 117
– Widerlegung 167
– Widerlegung bei elektronischer Signatur 198
Anscheinsvollmacht, als Grundlage der Haftung des Signierschlüsselhalters 184
Anwender, Anforderungen an den 22, 65
Anwendungen, als Notwendigkeit für die Verbreitung digitaler Signaturen 63
Application Service Provider 63
Art. 14 Abs. 2bis E-OR *234-240*
– als Beispiel des technikrechtlichen Regulierungsansatzes 139
– Anwendungsbereich 234
– Beweisfragen 237
– darzulegende Tatbestandselemente 237
– Einfluss auf die prozessuale Anerkennung 208
– materiellrechtliche Anerkennung als Ziel des E-ZertES 133
– Rechtsfolge 239
– und das BGG 138
– Voraussetzung der erfolgreichen Signaturprüfung 234
– Voraussetzung der fortgeschrittenen elektronischen Signatur 236
– Voraussetzung der qualifizierten elektronischen Signatur 235
– Voraussetzung der sicheren Signiereinheit 146, 236
– Voraussetzung des anerkannten Zertifizierungsdiensteanbieters 236
– Voraussetzung des qualifizierten Zertifikates 145, 235
– Voraussetzung des Zertifikates auf den Namen einer natürlichen Person 237
Art. 59a E-OR
– bei Signaturen mit ex-ante-Prüfung und Rahmenvertrag 201
– bei Signaturen ohne ex-ante-Prüfung 186
– Haftung für Signiereinheit 196
– i.V.m. Art. 8 UWG 194
– Überblick 198
– unklares Erfordernis der Anerkennung des Zertifizierungsdiensteanbieters 199
Art. 8 UWG 194
Arzthaftpflicht-Fall, als Fall des Anscheinsbeweises 159
ASP, s. Application Service Provider
asymmetrische Kryptographie 13
Attachment *14*, 28, 34, 35, 228
Attribute
– flexible bei Swisscert 42
– nach E-ZertES 146
– nach SigG 01 116
Attributzertifikat
– Begriff 31
– nach SigG 01 116
– nicht nach E-ZertES 146
Auffahrunfall-Fall, als Fall des Anscheinsbeweises 159
Aufklärung
– Hinsichtlich der Risiken elektronischer Legitimationsmittel 191
– Pflicht des Systembetreibers bei Signaturen mit ex-ante-Prüfung und Rahmenvertrag 201
– Pflicht des Systembetreibers bei Signaturen ohne ex-ante-Prüfung mit Rahmenvertrag 193
– Pflicht des Zertifizierungsdiensteanbieters als Kompensation des verlorengegangenen Übereilungsschutzes 225, 226
– Pflicht des Zertifizierungsdiensteanbieters nach SigG 01 116

– Pflicht des Zertifizierungsdiensteanbieters nach Signaturrichtlinie 101
– Pflichten des Zertifizierungsdiensteanbieters nach E-ZertES 144
Aufwendungsersatz, nach Art. 402 Abs. 1 OR 189
Aufzeichnungen von Geschäftsbüchern 175
Augenscheinsbeweis
– Begriff 168
– bei elektronisch gespeicherten Dokumenten 170
– mit elektronischer Signatur 124, 203, 204, 205
Ausdruck digital signierter Dokumente zur Beweisführung 204
Ausführungsbestimmungen
– zum ZertES 133, 147
– zur ZertDV 132
Auslastung der Prüfinfrastruktur der Gerichte, fehlende 206
Ausnahmen von der materiellrechtlichen Anerkennung 74, 242
Ausspähen
– des Signierschlüssels 19, 20, 193
– von PIN oder Passwort 19, *21*, 21, 56, 179, 180, 193, 194, 196, 224
Ausweisfälschung
– zur Erschleichung falscher Zertifikate 55
Authentifizierung
– als Begriffselement beim funktionalen Definitionsansatz 80
– als Begriffselement von Art. 2 Nr. 1 Signaturrichtlinie 103
– als Begriffselement von Art. 6 des UNCITRAL MLES 81
– durch Biometrie 83, 179
– durch digitale Signatur als digitaler Ausweis 37-40
– durch PIN/TAN, s. dort
– fortgeschrittene elektronische Signatur zur 104
– herkömmliche Methoden 64
Authentizität
– s. auch Authentifizierung
– Begriff 8
– der Gegenstelle im Internet 37-40
– keine separate Prüfung der Integrität 9
– Sicherung durch digitale Signatur 11
– verschiedene Methoden zur Absicherung 82
– Zusammenhang mit der Nichtabstreitbarkeit 9

B

bargeldloser Zahlungsverkehr, s. EFTPOS
bedingt notwendiger Zertifikatsinhalt nach E-ZertES 145
Begebung 173, 220
beglaubigte Kopie 174, 207
beglaubigtes Handzeichen, digitale Signatur als 233
Beglaubigung
– von Prüfschlüsseln, s. Zertifizierung
– von Unterschrift und Handzeichen 214, 217
Behördenverkehr, elektronischer, s. E-Government
Benutzergruppe
– Begriff 33
– geschlossene 246
  – Anwendbarkeit der Signaturrichtlinie 99
  – Anwendbarkeit des MLES 90
  – Anwendbarkeit des SigG 01 112
  – Anwendbarkeit des ZertES 193, 201
  – Begriff 33
  – Beweisführung und Haftung mit ex-ante-Prüfung 201
  – Beweisführung und Haftung ohne ex-ante-Prüfung 187-194
  – kein Interesse der Anbieter zur darüber hinaus gehenden Verwendung von Zertifikaten 61
  – KMU als Betreiber 63
  – Marktentwicklung 66
  – mit anerkanntem Zertifizierungsdiensteanbieter 114, 133
  – PKI ist nicht einzig sinnvolles Legitimationsmittel in 64
  – strategische Gründe für Beschränkung auf 61, 63
  – und Technologieneutralität 83
  – Verbreitung digitaler Signaturen in 61
  – wenig Regelungsbedarf 77
– offene
  – Bedeutung der Anerkennung des Zertifizierungsdiensteanbieters 133
  – Begriff 33
  – Beweisführung und Haftung mit ex-ante-Prüfung 195-200
  – Beweisführung und Haftung ohne ex-ante-Prüfung 182-186
  – digitale Signatur als einziges Mittel zur Absicherung elektronischer Kommunikation 150
  – Etablierung nicht anerkannter Anbieter 78
  – höhere Investitionen 64
  – im öffentlichen Bereich 67
  – kleiner Anreiz zur Anschaffung von Signierinfrastruktur 62
  – Notwendigkeit von Rechtsgrundlagen zur Etablierung digitaler Signaturen 64
  – und Technologieneutralität 82
  – Verbreitung digitaler Signaturen in 60
  – Vorteile 66
– semi-geschlossene 34, 42

Besitz, als Voraussetzung zum Erzeugen einer Signatur 20
Beteiligung des Bundes an Zertifizierungsdiensten 144
Beurkundung, öffentliche, s. öffentliche Beurkundung
Beweis 151
– mittelbarer und unmittelbarer 153
Beweis des Gegenteils 157, 167
Beweisabrede 213
Beweiseignung der digitalen Signatur, s. digitale Signatur, Beweiseignung
Beweiserleichterung, s. Anscheinsbeweis
Beweisform 211
Beweisführung
– mit Signaturen mit ex-ante-Prüfung ohne Rahmenvertrag 195
– mit Signaturen mit ex-ante-Prüfung und Rahmenvertrag 201
– mit Signaturen ohne ex-ante-Prüfung mit Rahmenvertrag 191
– mit Signaturen ohne ex-ante-Prüfung und Rahmenvertrag 182
Beweisführungslast *151*, 153, 155, 161, 198, 247
Beweisführungsvertrag 213
Beweisfunktion, der Handunterschrift 89, 222-224
Beweislast 117, 148, *151*, 152, 153, 156, 158, 161
Beweislasttheorie, für den Anscheinsbeweis 161
Beweislastumkehr
– als gesetzliche Vermutung ohne Vermutungsbasis 156
– für Haftung der Zertifizierungsdiensteanbieter nach E-ZertES 148
– für Pflichtverletzungen der Zertifizierungsdiensteanbieter nach SigG 01 117
– für Pflichtverletzungen der Zertifizierungsdiensteanbieter nach Signaturrichtlinie 107
Beweislastvertrag *152*, 153
Beweismass 76, 151, *152*, 153, 155, 157, 162, 163, 164, 167, 173, 180, 182, 183, 192
– Abweichung nur in Ausnahmefällen 165
– -norm, Anscheinsbeweis als teleologische Reduktion der 165
– Reduktion, Anscheinsbeweis als 163
Beweismasstheorie, für den Anscheinsbeweis 162
Beweismittel
– digitale Signatur als hochtechnisches 209
– Einordnung der elektronischen Signatur im Bundeszivilprozess 138
– elektronische Dokumente als 10
– mögliche für den Signierzeitpunkt 235
– Privilegierung der Urkunde als 75, 176, 204
– signiertes Legitimations-Token als 38
– symptomatischer Mangel an 165, *166*, 167, 179
– Urkunde im System der 168
– vertragliche Beschränkung auf Urkunden 213
– Zulassung elektronischer Signaturen als 103, 107
Beweisregel 76, 84, 110, 122, 174, 175, 244
Beweissicherungsmassnahmen
– zumutbare, als Voraussetzung des Anscheinsbeweises 160, 161, 163, 166, 182, 192, 193, 196, 197, 245
Beweiswürdigung
– Anscheinsbeweis als Aspekt der 162
– Prinzip der freien richterlichen 114, 181
– tatsächliche Vermutung als Aspekt der 155
Bewilligungspflicht, für Zertifizierungsdiensteanbieter 100, 110, 113
BGEG *134-137*, 217, 240, 241
BGES *132*, 134
– s. auch ZertES
Biometrie *21*, 56, 83, 90, 179, 183, 194
BioTrusT 22
Blankettfälschung, Praxis zur, als Grundlage der Haftung des Signierschlüsselhalters 185
bösartige Software *17*, 17, 19, 20, 37, 41, 56, 193
Botschaft zum ZertES 132
brute force attack 16, 20
Bund, Beteiligung an Zertifizierungsdiensten 144
Bundesgericht, elektronischer Aktenverkehr mit dem 138
Bundesgesetz über den elektronischen Geschäftsverkehr, s. BGEG
Bundesgesetz über die technischen Handelshemmnisse, s. THG
Bundesgesetz über elektronische Signaturen, s. BGES
Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur, s. ZertES
Bundesrechtspflege, Totalrevision 137
Bürgschaft 98, 119, 225, 239

C

CA
– Begriff 24
– s. Zertifizierungsdiensteanbieter
CD-R 9
Certificate Repository *25*, 43, 144, 200
Certificate Revocation List 19, *26*, 29, 32, 50, 113, 144, 196, 200, 236, 237
Certification Authority
– Begriff 24
– s. Zertifizierungsdiensteanbieter
Certification Body, s. Anerkennungsstelle

Certification Practice Statement *24*, 29, 30, 93, 183, 186
Certification Service Provider
– Begriff 23
– s. Zertifizierungsdiensteanbieter
Chipdrive Monitor Kit 18
Chipkarte, s. Token
Client 7
Client-Authentifizierung *39*, 39, 68
Code Civil, französischer 211
Code Signing *37*, 38, 182
Commitment, s. Verpflichtungserklärung
Computerausdruck, Beweiskraft 174
CPS, s. Certification Practice Statement
CRL, s. Certificate Revocation List
Cross-Zertifizierung, s. Kreuzzertifizierung
CSP, s. Certification Service Provider

D

Darstellung durch Text, s. Textform
Data Encryption Standard 44
Datenintegrität *8*, 9, 10, 11, 43, 44, 64, 80, 81, 82, 83, 147, 175, 214, 215, 222, 236
Datennachricht, nach MLEC 88
Datenschutz 22, 67, 108, 144
Datenspuren 10
Datenträger, einmal beschreibbarer 9
Datenverkehr, paketorientierter 7
Debitkarte, s. EFTPOS
Denial of Service Attack 10
DES, s. Data Encryption Standard
deterministischer Erfahrungssatz, s. Erfahrungssatz, deterministischer
Dienste der Informationsgesellschaft, Begriff nach der E-Commerce-Richtlinie 97
Dienste des Internet 7
digital envelope 45
digital ID
– Begriff 24
– s. digitaler Ausweis
digitale Identität
– Begriff 24
– s. auch Zertifikat
digitale Signatur
– Abbildung aus Nutzersicht 32
– als digitaler Ausweis 37
– als hochtechnisches Beweismittel 209
– Anerkennung, s. materiellrechtliche und prozessuale Anerkennung
– Anwendungsbeispiele 33-44
– Aufbau einer, nach S/MIME 35
– Begriff 11-12
– Beweiseignung 54-59, 84
– Erzeugen 13-18
– Gültigkeit 32
– Kombination mit Verschlüsselung 14
– kryptographische Sicherheit 15
– langsame Verbreitung 60-66
– mit Rückgewinnung der Nachricht, s. opake Signaturverfahren
– prüfen 31-33
– Unterschied zur Handunterschrift 19, 58
– Verwendung zur Authentifikation 37
– Wesen 13
– Zeitstempel zur Absicherung 50
digitaler Ausweis
– s. auch Zertifikat
– Verwendung der digitalen Signatur als 37
digitaler Fingerabdruck, s. Hashwert
digitalisierte Unterschrift 12, 83, 90
Dilemma der Computersicherheit 65
Direct Trust 23
Diskette, Speicherung des Signierschlüssels auf 19
diskreter Logarithmus 15
Dokumentenabschlussfunktion, der Handunterschrift 227
DoS, s. Denial of Service Attack
Dritter, auf die Signatur vertrauender
– Ansprüche aus ZertES 147
– Interesse an der Zeitstempelung 53
– Obliegenheit zur Überprüfung der Gültigkeit des Zertifikates 200
– Obliegenheit zur Überprüfung des Zertifikatsinhaltes 200
– Pflichten nach Signaturrichtlinie 107
– Pflichten nach UNCITRAL MLES 93
Dritter, der Signierschlüssel erzeugt 13
Dritter, vertrauenswürdiger
– s. auch Zertifizierungsdiensteanbieter
– als Voraussetzung jedes Signaturverfahrens in offenen Benutzergruppen 82
– zur Zeitstempelung 46
Drittschutzfunktion, von Formvorschriften *212*, 223, 232, 237
Duldungsvollmacht, als Grundlage der Haftung des Signierschlüsselhalters 184

E

E-Banking 33, 38, 39, 43, 63, 68, 96, 187, *187-191*, 193, 194
EBPP 40
ECash 40
Echtheit
– s. auch Indizienkette der digitalen Signatur

– Begriff 9
– Beurteilung bei Handunterschrift durch Laien 171
– Beweis bei elektronisch signierten Dokumenten 177-201
– Beweis bei nicht unterzeichneten Dokumenten 174
– Beweis bei Papierurkunden 172
– Beweis bei unterzeichneten Papierurkunden 76, 172, 176
– Regelungsmodelle für den Beweis 76
– Schriftgutachten 171
– Vermutung nach deutschem Recht 122
– Vermutung nach MLES 91
– Vermutung nach VE-BGES 150, 245
Echtheitsfunktion, der Handunterschrift, s. Beweisfunktion
EC-Karte, s. EFTPOS
E-Commerce-Richtlinie 97-99
EDI 36
E-Filing, s. E-Government
EFTPOS 63, 123, 160, *187*, 188
E-Government 5, 36, 67, 68, 69, 73, 86, 98, 137, 144
Eigenschriftlichkeit *217*, 239
einfache elektronische Signatur
– Beweisfunktion 223
– nach E-ZertES 140
– nach SigG 01 112
– nach Signaturrichtlinie 103
– Rekognition 221
einfache Schriftlichkeit 214
Einheit der Urkunde 121, 242
Einschreibebrief-Fall, als Fall des Anscheinsbeweises 159
Einwilligung in die Teilnahme an der elektronischen Kommunikation 121, 243
Electronic Bill Presentment and Payment, s. EBPP
Electronic Data Interchange, s. EDI
elektronisch gespeichertes Dokument
– als Augenscheinsobjekt 170
– als Rechtsöffnungstitel 177
– Beweiskraft 175
– Zulassung zum Urkundenbeweis 170
elektronische Einreichung digital signierter Dokumente bei Gericht
– de lege ferenda 205-208
– de lege lata 204
elektronische Form, nach FormanpassungsG 118, 119
elektronische Kopie, s. Scan
elektronische Signatur
– s. auch einfache elektronische Signatur und digitale Signatur
– Begriff 11
– Begriff nach UNCITRAL MLES 90
– fortgeschrittene, s. fortgeschrittene elektronische Signatur
– funktionaler Begriff 81
– qualifizierte, s. qualifizierte elektronische Signatur
– technikrechtlicher Begriff 81
elektronischer Vertragsschluss, nach der E-Commerce-Richtlinie 98
ElGamal 45
E-Mail 7
enabling principle *98*, 119
enger Urkundenbegriff *169*, 169
Entlastungsbeweis
– für Signierschlüsselhalter 199
– für Zertifizierungsdiensteanbieter 117
Entschlüsselungsschlüssel 45
Erbrecht, als Ausnahme vom enabling principle nach der E-Commerce-Richtlinie 98
Erfahrungssatz
– als Beweisgegenstand 151
– Begriff 154
– deterministischer 154
– statistischer 154
– und tatsächliche Vermutung 155
Erklärung des Signierschlüsselhalters
– zur Haftung, s. Verpflichtungserklärung
– zur Rekognition 221
Erschüttern
– der einer tatsächlichen Vermutung zu Grunde liegenden Hypothese 156
– des Anscheinsbeweises, s. Anscheinsbeweis, Widerlegung
Europa-Kompatibilität 148, 242, 250
ex-ante- und ex-post-Regulierungsansatz
– Begriffe 77
– bei Beweisregeln 84
– Bei der Anerkennung der Signatur 77
– im UNCITRAL MLES 91
– Kombination 80
– nur ex-ante im E-ZertES 139
– Vor- und Nachteile 78
ex-ante-Prüfung
– s. auch Anerkennung und Akkreditierung der Zertifizierungsdiensteanbieter
– als Gütezeichen 113
– Bedeutung für das Gericht 79, 124, 180-182
– der Verfahren und Komponenten 79
– nach MLES 92, 93

– Regelungsmodelle 78
– Zuständigkeit 79
excess inertia, s. Pinguin-Effekt
excess momentum 60
ex-post-Regulierungsansatz
– s. auch ex-ante- und ex-post-Regulierungsansatz
– als Alternative zur Anerkennung ausländischer Zertifizierungsdiensteanbieter 85
Extensions, eines Zertifikats nach X.509 *30*, 146
E-ZertES
– Arten elektronischer Signaturen 140
– Definitionen nach 140, 141
– Entwicklung 132-133
– fehlende Technologieneutralität 140
– Haftung der Zertifizierungsdiensteanbieter 147
– Haftung des Signierschlüsselhalters, s. Art. 59a E-OR
– keine Sanktionen 149
– materiellrechtliche Anerkennung, s. dort
– Regelungsmodell 139
– Signaturprüfeinheit 147
– Signiereinheit 146
– technikrechtlicher Ansatz 139
– Ziele und Mittel 133

F

Faksimile-Unterschrift
– Begriff 215
– digitale Signatur als 232
Fallgruppen, zum Beweis mit elektronisch signierten Dokumenten 178
Fälschung
– Ausspähen von Signierschlüssel, PIN oder Passwort, s. dort
– digitale Signatur vs. Handunterschrift 58, 224
– durch Rückdatierung 49
– einer digitalen Signatur 58
– einer Handunterschrift 170
– Präsentationsproblem, s. dort
Fälschungsrisiko, als Grund für langsame Verbreitung digitaler Signaturen 63
Familienrecht, als Ausnahme vom enabling principle nach der E-Commerce-Richtlinie 98
Fernabsatzrichtlinie 94
– Ausnahmen vom Anwendungsbereich 96
– Regelungsbereich 95
Fernabsatzverträge, nach BGEG 135, 136, 233, 241
Fiktion
– der Echtheit der digitalen Signatur 181
– der Sicherheit eines Verfahrens nach UNCITRAL MLES 92
Finanzdienstleistungen
– als Ausnahme vom VE-BGEG 135, 241, 251
– als Ausnahme von der Fernabsatzrichtlinie 96
Fingerabdruckprüfung, s. Biometrie
Forderungsabtretung, s. Zession
Form Signing *36*, 64
Form, gewillkürte 74, 75, 91, 118, 121, *213*, 213, 222, 228, 243
FormanpassungsG 53, 75, 80, 111, 117, *118-125*
– Beweiserleichterung 123
– Einheit der Vertragsurkunde 121
– elektronische Form 118, 119
– gewillkürte elektronische Form 121
– gewillkürte Schriftform 121
– keine prozessuale Anerkennung 124
– prozessuale Aspekte 122
– Regelungsmodell 118
– Textform 118, 120
– Ziele 118
Formatproblem, beim elektronischen Aktenverkehr mit Gerichten 206
Formularzwang und materiellrechtliche Anerkennung 240
Formungültigkeit 212
fortgeschrittene elektronische Signatur
– nach E-ZertES 140
– nach SigG 01 112
– nach Signaturrichtlinie 104
fortgeschrittene elektronische Signatur besonderer Qualität, s. qualifizierte elektronische Signatur
freie richterliche Beweiswürdigung, s. Beweiswürdigung, freie richterliche
freiwillige Akkreditierung der Zertifizierungsdiensteanbieter, s. Akkreditierung der Zertifizierungsdiensteanbieter
freiwillige Anerkennung der Zertifizierungsdiensteanbieter, Prinzip der, s. dort
FTP 7
funktionale Äquivalenz 89
– Begriff im UNCITRAL MLES 88
– von digitaler Signatur und Handunterschrift 88, 219, 231, 242
funktionaler und technikrechtlicher Regulierungsansatz *80*, 81, 82, 83, 90, 91, 100, 103, 104, 106, 109, 139, 140

G

geheimer Schlüssel, s. Schlüssel, geheimer
Genehmigungspflicht für Zertifizierungsdiensteanbieter, s. Bewilligungspflicht
Gerichte
– Aktenverkehr nach dem Entwurf für eine Totalrevision der Bundesrechtspflege 137

– Aktenverkehr nach FormanpassungsG 125
gerouteter Datenverkehr 7
Geschäftsbücher, Aufzeichnungen von 175
geschlossene Benutzergruppe, s. Benutzergruppe, geschlossene
Gesetz über Rahmenbedingungen für elektronische Signaturen, s. SigG 01
Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, s. FormanpassungsG
Gesetz zur Regelung der Rahmenbedingungen für Information- und Kommunikationsdienste, s. IuKDG
Gesetzeszweck, Vereitelung als Voraussetzung des Anscheinsbeweises 165, 179
gesetzliche Vermutung
– Begriff 156
– der Echtheit digitaler Signaturen 76, 80, 110, 125, 181, 245
– mit glaubhaft zu machender Vermutungsbasis 157
– mit voll zu beweisender Vermutungsbasis 157
– ohne Vermutungsbasis, als Beweislastumkehr 156
– unwiderlegbare
  – Begriff 156
  – s. auch Fiktion
– widerlegbare 156
– Widerlegung 157
– Wirkung 156, 157
gewillkürte elektronische Form, nach FormanpassungsG 121
gewillkürte Form, s. Form, gewillkürte
Girovertrag 187
Glaubhaftmachen
– Begriff
– s. auch Beweismass und Anscheinsbeweis
Gleichsetzung von elektronischer Signatur und Handunterschrift, s. materielle und formelle Anerkennung
Global ID, von Identrus 42
goods-in-hand-Entscheidung 95, 240
GovLink 138
graphologisches Gutachten 170
Groupe de Réflexion 130
Grundsatz der Formfreiheit 210
Guide to Enactment, zum UNCITRAL MLES 89
Gültigkeitsform 211
Gutachten *59*, 124, 150, 168, 170, 173, 177, 181, 204, 207, 224, 229, 239
Gütesiegel, Anbieteranerkennung als staatlich anerkanntes 77, 113, 133

H

Haftung der Anerkennungsstellen, nach E-ZertES 149
Haftung der Zertifizierungsdiensteanbieter 85
– Beschränkung nach E-ZertES 148
– Kreis der Haftpflichtigen nach E-ZertES 148
– nach E-ZertES 147-148
– nach MLES 93
– nach SigG 01 117
– nach Signaturrichtlinie 107
– Verjährung nach E-ZertES 149
– Verschuldenshaftung 148
Haftung des Signierschlüsselhalters
– aus Art. 59a E-OR 186
– aus Stellvertretungsrecht 184
– bei Signaturen mit ex-ante-Prüfung ohne Rahmenvertrag 198
– bei Signaturen mit ex-ante-Prüfung und Rahmenvertrag 201
– bei Signaturen ohne ex-ante-Prüfung mit Rahmenvertrag 194
– bei Signaturen ohne ex-ante-Prüfung und Rahmenvertrag 183-186
– Beschränkung 148
– für Überprüfung der Gültigkeit des Zertifikates 200
– nach MLES
– Obliegenheit zur Überprüfung des Zertifikatsinhaltes 200
– Vertrauenshaftung 184
Haftung des Systembetreibers 191, 193, 201
Haftungsbeschränkungen, nach E-ZertES 148
halbgeschlossene Benutzergruppe 34
Handelsrecht, vs. bürgerliches Recht, bei der materiellrechtlichen Anerkennung 241
Handunterschrift
– als biometrisches Merkmal 21
– als Legitimationsmittel 187, 191
– als Voraussetzung der einfachen Schriftlichkeit 214
– analoge Anwendung auf digitale Signatur 231
– Anscheinsbeweis der Echtheit 176
– Beweis der Abgabe 170-173
– digitalisierte 12, 103, 104, 226
– Fälschungssicherheit 170
– Gleichsetzung mit elektronischer Signatur, s. materiellrechtliche und prozessuale Anerkennung
– kopierte 174, 177
– Nachbildung, s. Faksimile-Unterschrift

– Rechtsöffnungstitel 176, 208
– tatsächliche Vermutung der Echtheit 176
– Unterschiede zur digitalen Signatur 58, 209, 223, 230
– zur späteren Identifikation des Signierschlüsselhalters 55
Hardwaresigniereinheit 18, *20*, 20, 21, 22, 39, 56, 62
– s. auch Kartenleser
Hash-Algorithmus
– Feld im Zertifikat 30
– Sicherheit 54, 57, 195
Hash-Baum 47, 48
Hashwert
– Abbildung 15
– als Input des Signieralgorithmus 15
– Angriff auf 16
– Begriff 15
– durch Hardware erzeugt 18
– Publikation als Zeitstempel 27, 47
– Publikation des, zur sicheren Verbreitung des Wurzelzertifikates 32, 195
– Vergleich zum Prüfen einer Signatur 32
Haustürverträge 135
HBCI 21, *39*, 83, 124, 194
Hierarchical Trust 23
Hierarchie von Zertifikaten 27
hochtechnisches Beweismittel, elektronische Signatur als 209
Homebanking Computer Interface, s. HBCI
hybride Verschlüsselungsverfahren 45
Hypothese über einen Geschehensablauf 155, 156, 157

I

Identifikation, des Absenders, s. Authentizität
Identitätsfunktion, s. Beweisfunktion
Identrus *41-42*, 68, 183
IETF, s. Internet Engineering Task Force
IG-Top 68
Immobilien, Verträge über, als Ausnahme vom enabling principle 98
Indizienbeweis 158
– Begriff 153
– s. auch mittelbarer Beweis und Anscheinsbeweis
Indizienkette der digitalen Signatur *54-57*, 58, 123, 129, 150, 177, 178, 191, 195, 198, 247, 248
Induktionsschluss 154
Information, als Funktion von Formvorschriften 230
Informationspflicht, s. Aufklärung
Informationsübermittlung, als Zweck der Textform 216
Infrastruktur-Inseln, als Grund für die langsame Verbreitung digitaler Signaturen 61
Inhaltsklarheit, als Funktion von Formvorschriften 230
Integrität, s. Datenintegrität
Integritätsfunktion, s. Beweisfunktion
interdepartementale Arbeitsgruppe «DigSig» 131
intermediate Hash 47
internationale Anerkennung
– nach E-ZertES 143
– nach MLES 93
– nach SigG 01 114
– Regelungsmodelle 84
Internationale Fernmeldeunion 29
Internet Engineering Task Force 7, 34
Interoperabilität, fehlende, als Grund für langsame Verbreitung digitaler Signaturen 61
Interoperabilitätsspezifikationen 31, 61, 109
Introducer (bei PGP) 23
irgendein schuldhaftes Verhalten (Anscheinsbeweis) 158, 162, 164
Iris, s. Biometrie
ITU, s. Internationale Fernmeldeunion
ITU-T Empfehlung X.509 29
IuKDG 109
IuKDG-Bericht 111

J

JavaScript
– Code Signing 37
– Form Signing 36

K

kartellrechtliche Verträge, Kontrollfunktion der Schriftform 228
Kartenleser
– Installation 39, 62, 64
– Klasse 1 *21*, 39, 193
– Klasse 2 21, *21*, 56, 193
– Klasse 3 18, *21*, 56, 146, 147, 179, 194, 196
– Klasse 4 21
– Klassen von 21
– Marktreife 18, 56
– schwierige Installation als Grund für langsame Verbreitung digitaler Signaturen 62
Kausalhaftung, milde der Zertifizierungsdienstanbieter nach E-ZertES 148
KKG 225, 241
kleine und mittlere Unternehmen 63, 66, 68

Kompromittierung des Signierschlüssels 20, *26*, 30, 52, 56, 92, 193, 196, 197, 224
– des Zeitstempeldiensteanbieters 47
– des Zertifizierungsdiensteanbieters 33
Konformitätsbestätigung 205-208
– als Aufgabe der Kantone 208
– als beglaubigte Kopie 207
– Begriff 207
– notwendiger Inhalt 239
Konsumenten, Einsatz digitaler Signaturen durch 62
Konsumentenfernabsatzverträge, s. Fernabsatzverträge
Konsumkreditvertrag
– als Beispiel einer Formvorschrift mit überwiegender Übereilungsschutzfunktion 225
– Notwendigkeit einer Ausnahme von der materiellrechtlichen Anerkennung 241, 251
Kontrollfunktion, der Handunterschrift 228
Konzessionssystem, zur Ausgabe von Zertifikaten 78
Koordinationsgruppe Informationsgesellschaft (KIG) 131
Kopie
– als Rechtsöffnungstitel 177
– Aufbewahrung bei der öffentlichen Beurkundung 218
– beglaubigte 207
– Beweiskraft 174
Kosten-Nutzen-Analyse des Anwenders 62
KPMG, als erste akkreditierte Anerkennungsstelle der Schweiz 142
Kreuzzertifizierung 27, *28*, 108
Kryptographie 11
kryptographische Sicherheit
– des Zertifikates 55
– digitaler Signaturen *15*, 54, 178
– nach E-ZertES 146
– Nachweis 195
– Verlängerung durch Zeitstempel 51-52, 229
– Verlust durch Zeitablauf 16, 58
– von Zeitstempeln 47
kryptographischer Schlüssel, s. Schlüssel, kryptographischer

L

langsame Verbreitung der digitalen Signatur, Gründe für die 60-66
LDAP 25, 26
Legitimationsmittel im Bankgeschäft 187-191
Legitimationsmittel, digitale Signatur als *37-40*, 191
Legitimationsordnung
– dispositive beim Girovertrag 188
– parteiautonome 191, 201
– parteiautonome beim Girovertrag 190
Leistungsfähigkeit von Computern, Einfluss auf die kryptographische Sicherheit 16
Lightweight Directory Access Protocol 25
Liste der anerkannten Zertifizierungsdiensteanbieter 142, 195, 238, 239
lokales Authentifizierungsmittel, digitale Signatur als 38

M

Mangel an Beweismitteln bei beiden Parteien, als Voraussetzung des Anscheinsbeweises, s. Beweismittel, symptomatischer Mangel an
Marktprozess, rekursiver, s. Pinguin-Effekt
Marktwirtschaftlicher und technikrechtlicher Regulierungsansatz 82
Massnahmenkatalog nach SigG 97 109
materiellrechtliche Anerkennung
– s. auch Art. 14 Abs. 2bis E-OR
– s. auch enabling principle
– als Grundlage der prozessualen 75
– Ausnahmen von *74*, 98, 100, 118, 119, 130, 135, 210, 233, 239, 240, 241, 242
– Bedeutung 130
– Begriff 74
– bei der gewillkürten Form 75
– de lege ferenda 233-242
– de lege lata 231-233
– Differenzierung zwischen Handelsrecht und bürgerlichem Recht 241
– Gutachten zur Feststellung der 239
– höhere Rechtssicherheit durch Anbieteranerkennung *78*, 81, 91, 107, 113, 133, 139, 244, 247, 251
– im FormanpassungsG 111
– internationale, nach MLES 93
– nach der Signaturrichtlinie 102, 106, 107
  – gemeinschaftsweit 108
  – international 108
– nach E-ZertES 133
– nach MLES 91
– nach SigG 01 119
– Regelungsmodelle 74, 231
– Überprüfung nach dem Entzug der Anbieteranerkennung 142
– und gewillkürte Form 75
– Voraussetzung der erfolgreichen Signaturprüfung 234

– Voraussetzung der fortgeschrittenen elektronischen Signatur 236
– Voraussetzung der Gültigkeit des Zertifikats zum Signierzeitpunkt 235
– Voraussetzung der qualifizierten elektronischen Signatur 235
– Voraussetzung der sicheren Signiereinheit 146, 236
– Voraussetzung des anerkannten Zertifizierungsdiensteanbieters 236
– Voraussetzung des qualifizierten Zertifikates 235
– Voraussetzung des Zertifikates auf den Namen einer natürlichen Person 237
materiellrechtliche Theorie, für den Anscheinsbeweis 164
M-Commerce 41
Mehrwertsteuer 5
Microsoft Windows, Zertifikatsverwaltung unter 38
milde Kausalhaftung, der Zertifizierungsdiensteanbieter nach E-ZertES 148
MIME-Standard 34
MLEC 88-89
MLES 80, 81, *89-94*, 102, 103, 108, 200
Mobile Commerce, s. M-Commerce
Mobiltelefon 17, 20, 41, 62
Model Law on Electronic Commerce, s. MLEC
Model Law on Electronic Signatures, s. MLES
Model Law, Begriff 88
Motion Spoerry 130

N

Name einer natürlichen Person, Ausstellung des Zertifikats auf den, als Voraussetzung der materiellrechtlichen Anerkennung 237
Naturalobligation, als Folge der Formungültigkeit 212, 231
negatives Vertragsinteresse 185, 199
Netzwerkexternalitäten 60
Nichtabstreitbarkeit *9*, 11, 43, 64, 183
– bei digitaler Signatur als reines Authentifikationsmittel 38
– bei Handunterschrift 172
– Gefährdung durch bösartige Software 21
– Gefährdung durch Präsentationsproblem 17
– Gefährdung durch Weitergabe des Tokens 21
Non-Repudiation, s. Nichtabstreitbarkeit
Notar, als Prüfstelle für digitale Signaturen 207
Notariatsdienste, s. Zeitstempel

O

Object Signing 37
OCSP-Protokoll 26
offene Benutzergruppe, s. Benutzergruppe, offene
öffentliche Beurkundung 169, 207, 208, 213, 214, *218*, 223, 227, 240
öffentliche Urkunde, vs. Privaturkunde 169
öffentlicher Bereich, als Ausnahme von der materiellrechtlichen Anerkennung nach der Signaturrichtlinie 106, 114
öffentlicher Schlüssel, s. Schlüssel, öffentlicher
öffentliches Recht, s. E-Government
opake Signaturverfahren 14
OpenPGP 34

P

parteiautonome Legitimationsordnung 190
Parteiautonomie, s. Benutzergruppe, geschlossene, Anwendbarkeit von MLES, Signaturrichtlinie, SigG und ZertES
Passwort 20
– als Alternative zur digitalen Signatur 64, 90
– als Legitimationsmittel, digitale Signatur als Ersatz 38, 187
– Aufklärung über Geheimhaltungspflicht, s. dort
– Ausspähen, s. dort
– Eingabe als Rekognitionshandlung 221
– Eingabe über Telefontastatur 41
– fahrlässige Preisgabe bei EFTPOS 160, 161
– mit TAN im E-Banking, s. Transaktionsnummer
– schuldhafte Preisgabe als positive Vertragsverletzung 189
– Schutz des Signierschlüssels durch 13, *20*
– Weitergabe 21
– Zusenden zur Identifikation 24, 43
PDA, s. Personal Digital Assistant
PDF, s. Portable Document Format
Perpetuierungsfunktion der Handunterschrift 228, 229
Personal Digital Assistant 17, 41
Personalisierung des Schlüsselpaares, s. Signierschlüsselhalter, Identifikation durch den Zertifizierungsdiensteanbieter
persönliche Identifikationsnummer
– Begriff 20
– s. auch Passwort
PGP Web of Trust, s. Web of Trust
PGP, s. Pretty Good Privacy
PIN, s. Passwort
Pinguin-Effekt 60, 62
PKCS, s. Public Key Cryptography Standards
PKI, s. Public-Key-Infrastruktur und Sicherungsinfrastruktur
PKIV, s. ZertDV
Portable Document Format 9

positives Vertragsinteresse 184, 185, 199
Postcard, s. EFTPOS
Präsentationsproblem *17*, 18, 147, 179, 180, 193, 194, 198, 224
presumption
– der Sicherheit im MLES 92
– of signing im MLES 92
Pretty Good Privacy *23*, 34, 35, 61, 104, 182, 221
prima-facie-Beweis, s. Anscheinsbeweis
Primfaktorzerlegung 15
Prinzip der freiwilligen Anerkennung der Zertifizierungsdiensteanbieter *78*, 139, 199
private key, s. Schlüssel, geheimer
private Urkunde 169
privater Schlüssel, s. Schlüssel, geheimer
Privatschutzfunktion, von Formvorschriften 212
Privaturkunde 169
Profile, zum X.509-Standard 31
provisorische Rechtsöffnung 75, 129, *176*, 177, 203, 204, 208, 234
prozessuale Anerkennung 203-208
– als Regelungsbereich des ZertES 133
– auf dem Wege der materiellrechtlichen 133, 234
– Begriff 75
– de lege ferenda 205
– de lege lata 203
– durch Konformitätsbestätigung, s. dort
– in Deutschland 111, *124*
– nach dem Vorschlag zur Signaturrichtlinie 106
– nicht geregelt bei der Totalrevision der Bundesrechtspflege 138
– Regelungsmodelle 75
– richterrechtliche 75, 231
Prüf- und Bestätigungsstellen, nach SigG 01 115
Prüfeinheit, s. Signaturprüfeinheit
prüfen, s. digitale Signatur, prüfen
Prüfschlüssel
– abweichender Begriff im E-ZertES 140
– als Zertifikatsinhalt 24, 30, 145
– Begriff 12, 141
– des Zertifizierungsdiensteanbieters 27
– Einmaligkeit nach Art. 6 Abs. 2 E-ZertES 146
– Einsatz zum Prüfen einer Signatur 31
– kryptographische Sicherheit, s. dort
– Zertifikat ohne 31
– Zertifizierung, s. dort
Pseudonym 65, 108, 115, 145, 147, 237
Public Key Cryptography Standards (PKCS) 19
public key, s. Prüfschlüssel
Public-Key-Infrastruktur
– s. auch Sicherungsinfrastruktur
– Alternativen zur, in geschlossenen Benutzergruppen 64
– Identrus, als Beispiel einer privaten, s. dort
– Literaturhinweise 139
– offene, s. Benutzergruppe, offene
– Verordnung über eine in der Schweiz, s. ZertDV
Public-Key-Kryptographie 11, *13*, 15, 38, 45, 82, 83, 90, 140

Q

qualifizierte elektronische Signatur
– Anscheinsbeweis mit 123, 183, 192, 236
– Begriff 102
– Beweis des Tatbestandsmerkmals der 238
– Beweis mit und Haftung des Schlüsselhalters 178, 182-186
– Beweisfunktion 223
– internationale Anerkennung nach SigG 01 114
– Kontrollfunktion 228
– materiellrechtliche Anerkennung 119, 235
– mit Anbieterakkreditierung bzw. -anerkennung, s. dort
– nach E-ZertES 140
– nach SigG 01 112
– nach Signaturrichtlinie 105
– Rekognitionsfunktion 202, 222
– Übereilungsschutzfunktion 225
– Vergleich zur solchen mit Anbieterakkreditierung nach SigG 01 113
– Voraussetzungen nach Art. 2 Bst. c E-ZertES 235-236, 238
qualifizierte elektronische Signatur mit Anbieterakkreditierung
– s. auch qualifizierte elektronische Signatur mit Anbieteranerkennung
– Begriff 102
– nach SigG 01 112
– nach Signaturrichtlinie 107
– öffentlicher Bereich 114
qualifizierte elektronische Signatur mit Anbieteranerkennung
– s. auch qualifizierte elektronische Signatur mit Anbieterakkreditierung
– Einsatz mit Rahmenvertrag 201
– Haftung des Signierschlüsselhalters 198
– materiellrechtliche Anerkennung von 233
qualifizierte öffentliche Beurkundung 214, *218*
qualifizierte Schriftlichkeit 214, *217*
qualifiziertes Zertifikat
– als Voraussetzung von Art. 14 Abs. 2^{bis}s E-OR 238

– Ausgabe als Voraussetzung für die Haftung des Zertifizierungsdiensteanbieters 148
– Begriff nach E-ZertES 145
– Begriff nach SigG 01 112, 115
– internationale Anerkennung nach SigG 01 114
– nach Signaturrichtlinie 101, 105
– Pflichten der Anbieter von, nach E-ZertES 144
Quantencomputer 16

R

Rahmenvertrag, s. Benutzergruppe, geschlossene
rechtliche Wirkungen der Signatur, Aufklärung über, s. dort
rechtlichen 116
Rechtsbeweis, Anscheinsbeweis als 162
Rechtsöffnung, s. provisorische Rechtsöffnung
rechtspolitische Zielsetzungen, Ablösung der Formvorschriften von 219
Rechtssicherheit
– Bedeutung bei Formvorschriften 232
– fehlende als Grund für die langsame Verbreitung digitaler Signaturen 64
– höhere, des ex-ante-Regulierungsansatzes 78
– höhere, des technikrechtlichen Regulierungsansatzes 81
Regelbeweismass *152*, 155, 167
Registrierstelle *24*, 55, 112
Rekognition
– als materielles Element der Unterschrift 215
– Begriff 220
– Beweis bei elektronischer Signatur 202
– Beweis bei Papierurkunden 173
– durch Handunterschrift 220
– Erklärung des Signierschlüsselhalters zur 221
– und Dokumentenabschlussfunktion 227
– Vermutung im UNCITRAL MLES 92
Rekognitionsfunktion der Handunterschrift 89, *220-222*
Rentabilität von Zertifizierungsdiensteanbietern 63
Replay Attack, bei der Authentifizierung 37
Reputation, positive durch Einsatz digitaler Signaturen 62
Revokation von Zertifikaten, s. Zertifikat, Sperrung
richterrechtliches Modell
– bei der Beweiswürdigung digitaler Signaturen 79
– bei der materiellrechtlichen Anerkennung 74, 231
– bei der prozessualen Anerkennung 75
Richtlinie
– Begriff im EU-Recht 94
– über den elektronischen Geschäftsverkehr, s. E-Commerce-Richtlinie
– über den Fernabsatz von Finanzdienstleistungen, s. Finanzdienstleistungsrichtlinie
– über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, s. Signaturrichtlinie
Rijndael-Algorithmus 44
Root Certification Authority 27
Root-Zertifikat, s. Wurzelzertifikat
Router 7
Routing 8, 9
RSA 13, 15, 16, 45
Rückdatierungsproblem 47, *49*, 235

S

S/MIME
– Begriff 34
– Interoperabilität 61
– Versand der Zertifikate 28
Sachverständigengutachten, s. Gutachten
Sanktionen, keine nach E-ZertES 149
Scans 138, 174
Schiffskollisions-Fall, als Fall des Anscheinsbeweises 158
Schlüssel
– geheimer
  – Begriff 12
  – s. auch Signierschlüssel
– kryptographischer 12
– öffentlicher
  – Begriff 13
  – s. auch Prüfschlüssel
– privater, s. Signierschlüssel
Schlüsselhalter, s. Signierschlüsselhalter
Schlüsselpaar 12
Schlüsselraum 16
Schlüsselzertifizierung, s. Zertifizierung
schriftvergleichendes Gutachten 170
Schriftverstellung 172
Schuldanerkennung, durch Unterschrift bekräftigte 176
Schweizerische Akkreditierungsstelle SAS 142
Secure Electronic Transaction, s. SET
Secure Socket Layer, s. SSL
semi-geschlossene Benutzergruppe 34
Sensibilisierung für Sicherheitsprobleme, fehlende als Grund für langsame Verbreitung digitaler Signaturen 65
Server 7
Server-Authentifizierung 38
Serverzertifikat 39
Session (auf einmal beschreibbarem Datenträger) 9
Session Key 45
SET 40

Sicherheit elektronischer Signaturen
– Anwendungssicherheit 77
– finanzielle 77
– kryptographische, s. kryptographische Sicherheit 77
– organisatorische 77
– technische 77
Sicherungsinfrastruktur
– Begriff 25
– nach E-ZertES 132, 139-149
– nach SigG 01 112-115
– nach SigG 97 109
– Regelung als notwendige rechtliche Rahmenbedingung für den E-Commerce 131
– Regelungsbedarf 77
– Regelungsmodell in der Schweiz 139
– Regelungsmodelle 77-85
– staatliche, als Kondensationspunkt für private Anwendungen 69
– Vorteile einer offenen 66
– Zeitstempel als wichtiger Teil der 49
SigG 01 111-118
SigG 97 109-111
Signaturerstellungseinheit
– Begriff nach E-ZertES 146
– s. auch Signiereinheit
Signaturprüfeinheit *32*, 33, 58, 147, 237
Signaturprüfschlüssel
– Begriff nach E-ZertES 140
– s. auch Prüfschlüssel
Signaturprüfung, positives Resultat als Voraussetzung von Art. 14 Abs. 2bis E-OR 238
Signaturrichtlinie 79, 80, 81, 82, 85, 87, 90, 98, *99-108*, 112, 114, 115, 116, 119, 120, 139, 140, 143, 145, 146, 148, 195
Signaturschlüssel
– Begriff nach E-ZertES 140
– s. auch Signierschlüssel
Signiereinheit *14*, 18, 22, 62, 146, 236, 238
– s. auch Hard- und Softwaresigniereinheit
Signierschlüssel
– Begriff 12, 141
– Beweis der Kontrolle über 196
– brute force attack 16
– des Zertifizierungsdiensteanbieters 33
– Erzeugen der Signatur 13
– Erzeugung 13
– Erzeugung durch Dritten 13
– Kompromittierung 26
– Pflicht zur Geheimhaltung, s. Haftung des Signierschlüsselhalters
– Sicherheit, s. kryptographische Sicherheit
– Zugriffsschutz 19-22
Signierschlüsselhalter
– Begriff 23
– Haftung, s. Haftung des Signierschlüsselhalters
– Identifikation durch den Zertifizierungsdiensteanbieter 24, 43, 55, 101, 144, 147
Signierzeitpunkt 47, 50, 56, 84, 140, 178, 180, 196, 197, 207, 235, 238, 239
SigV 01 111
SigV 97 109
SIM-Karte 20, *41*
Single Sign-on 38
Smartcard, s. Token
Softwaresigniereinheit *19*, 21, 22, 39, 183, 193, 194
Sonderformen der Beurkundung 219
Sperrung von Zertifikaten, s. Zertifikat, Sperrung
Spoofing 8
SSL *38*, 60, 182, 183
SSO, s. Single Sign-on
Staat
– als Betreiber von Zertifizierungsdiensten 144
– Beteiligung am Betrieb von Zertifizierungsdiensten 68
– Monopol zur Ausgabe von Zertifikaten 78
staatsvertragliche Anerkennung der Zertifizierungsdiensteanbieter 84
Standards *33-44*
Statute of Fraud, amerikanisches 211
Stellvertretungsrecht, Haftung des Signierschlüsselhalters aus 184
Strategiepapier «für eine Informationsgesellschaft in der Schweiz» *131*
strategische Gründe für geschlossene Benutzergruppe 61, 63
Streichliste, s. Transaktionsnummer
substantive rule, hinsichtlich der Sicherheit eines Verfahrens im MLES 92
Surety, Inc. (Zeitstempeldiensteanbieter) 49
Swisscert *42-44*, 68
Swisskey 24, 60, *63*, 144
Symbol für eine gültige Signatur 31

T

TAN, s. Transaktionsnummer
Tastatureingaben, Protokollieren von, s. Ausspähen, von PIN oder Passwort
tatsächliche Vermutung
– als Aspekt der Beweiswürdigung 155
– als Bezeichnung für den Anscheinsbeweis 158, 159, 163
– Anscheinsbeweis als 162, 163, 164
– Begriff 155

– der Echtheit einer Urkunde 76, 172
– für Echtheit digitaler Signaturen 80, 181
– und Beweisführungslast 155
– und Beweismass 155
– und Erfahrungssatz 155
– vs. Indizienbeweis 154
– Widerlegung 156
Täuschen des Empfängers einer Signatur 33
TCP/IP-Protokoll 7, 8
technikrecht 80
technikrechtlicher Regulierungsansatz
– s. auch funktionaler und technikrechtlicher Regulierungsansatz
– vs. funktionaler Ansatz 80
– vs. marktwirtschaftlicher Ansatz 82
Technologieneutralität
– Begriff 82
– im E-ZertES 140
– im MLES 90
– in der Signaturrichtlinie 103, 106
– in geschlossenen Benutzergruppen 83
– in offenen Benutzergruppen 82
– keine Notwendigkeit in offenen Benutzergruppen 82
– Streit um, in der EU 102
– Zeitstempel 117
Telefax 174
Telesec 49, 60, 183
Textform 216-217
– als Alternative zu Ausnahmen von der pauschalen materiellrechtlichen Anerkennung 240
– nach FormanpassungsG 118, 120
– nach VE-BGEG 217
– Rechtsunsicherheit aufgrund fehlender Regelung 217
THG 141, 142, 143
timestamp, s. Zeitstempel
Token
– als Werbeträger 63
– Begriff 20
– bei digitalem Geld 40
– Datenpaket bei der Client-Authentifizierung 37
– mit biometrischer Erkennung 42
– Schutz durch PIN oder Passwort 20
– Swisscert 42
– unnötig bei der Signaturprüfung 32
– Zeitstempel 48
Towitoko 18
Transaktionsaufträge, Signieren der einzelnen 38, 187
Transaktionsnummer *40*, 40, 43, 64, 67, 184, 187, 191, 192, 193, 194
Travelling-Salesman-Problem 15
Triple-DES 44
Trojanisches Pferd, s. bösartige Software
Typizität, als Voraussetzung des Anscheinsbeweises 160

U

Übereilungsschutzfunktion, der Handunterschrift 98, 100, 120, 136, 219, *225-226*, 231, 240, 241, 242
Übereilungsschutzfunktion, der öffentlichen Beurkundung 218
Überregulierung, als Grund für die langsame Verbreitung digitaler Signaturen 64
Überwachung, Angst vor, als Grund für die langsame Verbreitung digitaler Signaturen 65
Überwachungssystem
– nach SigG 01 113
– nach Signaturrichtlinie 101
Überweisungsauftrag
– rechtliche Natur 188
– s. auch Transaktionsaufträge, Signieren der Einzelnen
Überzeugung des Gerichts 123, 151, 152, 155, 157, 159, 163, 165, 167, 172, 179, 186, 195, 198, 224
UBS Internet Card 39
Umsetzung der Signaturrichtlinie 99, 101, 104, 111, 120
UMTS 40
UN/EDIFACT 36
UNCITRAL 87
UNCITRAL Model Law on Electronic Commerce, s. MLEC
UNCITRAL Model Law on Electronic Signatures, s. MLES
UNCITRAL Working Group on Electronic Commerce 88
UNECE 36
Unfallversicherungs-Fall, als Fall des Anscheinsbeweises 159
Unterrichtungspflichten des Zertifizierungsdiensteanbieters, s. Aufklärung
Unterschieben von Dokumenten, s. Präsentationsproblem
Unterschrift, s. Handunterschrift
Urkunde
– als Augenscheinsobjekt besonderer Art 168
– Begriff 168
– Beweiskraft einer nicht unterzeichneten 174, 175
– im System der Beweismittel 168
– Privilegierung als Beweismittel 75, 176
– Verfälschung 171

Urkundenbeweis 124, 168-177
– als Anscheinsbeweis 172-173, 176, 180
– Besonderheiten nach deutschem Recht 122
– Zulassung elektronisch gespeicherter Dokumente zum 170
Urteilsunfähigkeit, als Haftungsausschlussgrund nach Art. 59a E-OR 199
USB-Token 20
UWG 149, 190, 194

V

VE-BGEG, s. BGEG
VE-BGES 132
Verbraucher-, s. Konsumenten-
Verfügbarkeit von Informatiksystemen 10
Verhandlungsabschlussfunktion, der Handunterschrift 227
Verjährung, der Haftung der Zertifizierungsdiensteanbieter nach E-ZertES 149
Verkehrsfähigkeit, von Zertifikaten 80, 81
Verkehrsübung, fehlende
– Rekognitionsfunktion 221
– Übereilungsschutzfunktion 226
Verschlüsselung 14
– asymmetrische 45
– Begriff 44
– hybride Verfahren 45
– symmetrische 44
Verschuldenshaftung
– der Zertifizierungsdiensteanbieter nach SigG 01 117
– der Zertifizierungsdiensteanbieter nach Signaturrichtlinie 107
– keine, der Zertifizierungsdiensteanbieter nach E-ZertES 148
Vertrag zugunsten Dritter
– als Grundlage der Haftung des Signierschlüsselhalters 183
vertraglich vorbehaltene Form, s. Form, gewillkürte
Vertragszweck
– Vereitelung als Voraussetzung des Anscheinsbeweises 165, 179
Vertrauen 13, 22, 23, 28, 46, 55, 59, 68, 77, 78, 82, 107, 179, 181
Vertrauenshaftung, des Signierschlüsselhalters 184, 186
Vertrauensprinzip 173, 202, 220
Vertrauensschaden, s. negatives Vertragsinteresse
Vertraulichkeit 8, 14
Vertretungsrecht, in Zertifikat 31, 105, 116, 145, 146, 237
Verurkundung, als Voraussetzung der einfachen Schriftlichkeit 214
Verwechslungsgefahr hinsichtlich eines Namens, unterscheidendes Element bei 30, 55, 145
Virtual Private Network 38
Virus, s. bösartige Software
Vorgezogener Anscheinsbeweis, s. Anscheinsbeweis, vorgezogener
VPN, s. Virtual Private Network

W

Wahrscheinlichkeitssatz, s. Erfahrungssatz, statistischer
WAP, s. Wireless Application Protocol
Warnfunktion, s. Übereilungsschutzfunktion
Web of Trust 23
weiter Urkundenbegriff 168
Wertpapierrecht, nicht erfasst von der materiellrechtlichen Anerkennung 239
What you see is what you sign, s. Präsentationsproblem
Widerrufsrecht 241
– als Alternative zu Ausnahmen von der pauschalen materiellrechtlichen Anerkennung 233, 240, 241, 242
– nach BGEG 134, 135, 136-137
– nach dem Entwurf für eine Finanzdienstleistungsrichtlinie 96
– nach Fernabsatzrichtlinie 96
Willenserklärung 220
Wireless Application Protocol 40
Wireless Identification Module 41
Wirkform 219
Wissen, als Voraussetzung des Erzeugens einer Signatur 20, 56
World Wide Web *7*, 8, 19, 36, 37, 39, 40, 182, 183, 225
Wurzel-Hash 47
Wurzelzertifikat 27-28
– Angriff auf 27, 33, 58
– einer staatlich anerkannten Root CA 28, 124
– Sperrung 33
WWW, s. World Wide Web

X

X.509 16, 26, *29-31*, 34, 61, 146

Y

YellowNet 39

Z

ZDA, s. Zertifizierungsdiensteanbieter

Zeitablauf, Verlust der kryptographischen Sicherheit durch 58
zeitliche Verzögerung, fehlende und Übereilungsschutzfunktion 225
Zeitpunkt des Setzens der Signatur, s. Signierzeitpunkt
Zeitstempel *46-53*, 58, 112, 116, 144, 192, 196, 197, 207, 229, 235, 237, 239
Zentraler Kredit-Ausschuss 21, 39
ZertDV, s. Zertifizierungsdiensteverordnung
ZertES
– s. E-ZertES
– Botschaft zum 132
– voraussichtliches Inkrafttreten 133
Zertifikat
– Abbildung 25
– Abfrage der Gültigkeit 26
– Ablauf *26*, 58
– absolut notwendiger Inhalt nach E-ZertES 145
– Attribute nach E-ZertES 145
– Attributzertifikat 31
– auf den Namen einer natürlichen Person, als Voraussetzung von Art. 14 Abs. 2bis E-OR 238
– bedingt notwendiger Inhalt nach E-ZertES 145
– Begriff 24
– Beschränkung von Transaktionswert oder Geltungsbereich 117, 145
– Gültigkeit zum Signierzeitpunkt, als Voraussetzung von Art. 14 Abs. 2bis E-OR 238
– Inhalt 24, 29
– Inhalt, Obliegenheit zur Überprüfung des 200
– Kosten 24, 62, 63
– Modifikation nach der Ausstellung 31, 44
– Prüfung 32
– qualifiziertes, s. qualifiziertes Zertifikat
– self signed 27
– Sperrung *26*, 32, 49, 58, 107, 115
– staatliche Ausgabe 78
– Standards 19, 34
– Validierung 26
– Veröffentlichung 25
– Widerruf, s. Sperrung
Zertifikatshierarchie 27, 28
Zertifikatsrücknahmeliste, s. Certificate Revocation List
Zertifizierung 23, *23*, 55, 133, 141, 142, 186, 195, 221
Zertifizierungsdiensteanbieter
– Akkreditierung, s. dort
– Anerkennung, s. dort
– Aufsicht nach E-ZertES 143
– Begriff 23
– Begriff nach E-ZertES 141
– Begriff nach SigG 01 112
– Bewilligungspflicht 110, 113
– Bewilligungspflicht, s. dort
– fehlende Anerkennung als Grund für langsame Verbreitung digitaler Signaturen 61
– freiwillige Anerkennung, Prinzip der, s. dort
– Haftung, s. dort
– Pflichten nach E-ZertES 144
– Pflichten nach UNCITRAL MLES 93
– Rentabilität 63
Zertifizierungsdiensteverordnung 79, *131*, 132, 138, 141, 142, 196
Zession 73, 230, 232, 237
Ziel des Beweises 151
ZKA, s. Zentraler Kredit-Ausschuss
Zugangsnachweis 10, 52
Zustellungsreformgesetz, deutsches 125
Zwecke von Formvorschriften 219-231
Zweckform 219
Zweifel, ernsthafte, zur Widerlegung des Anscheinsbeweises, s. Anscheinsbeweis, Widerlegung