

Sebastian Bösing

Authentifizierung und Autorisierung im elektronischen Rechtsverkehr

Qualifizierte Signaturschlüssel- und Attributszertifikate
als gesetzliche Instrumente digitaler Identität



Nomos

Inhaltsverzeichnis

A	Einleitung	15
I.	Glaubwürdigkeit und Verbindlichkeit in der Informationsgesellschaft	15
II.	Identität im Cyberspace	17
III.	Technische Grundlagen der elektronischen Signatur	19
	1. Symmetrische Verschlüsselung	20
	2. Asymmetrische Verschlüsselung	20
	3. Kryptoanalyse	21
	4. Die elektronische Signatur	22
	a) Elektronisch signieren	22
	b) Überprüfen einer elektronischen Signatur	23
	c) Die Sicherheitsinfrastruktur	23
	aa) Unikatseigenschaft der Schlüsselpaare	24
	bb) Kryptographischen Sicherheit	24
	cc) Sicherheit der Anwendungsumgebung	25
	5. Zusammenfassung	26
IV.	Gesetzgebung in Deutschland	26
	1. Das deutsche SigG (1997)	26
	2. Die EG-Richtlinie 1999/93/EG	29
	3. Novellierung des SigG (2001)	30
	4. Anpassung der Formvorschriften des materiellen und formellen Rechts	31
	5. Die elektronische Signatur als Beweismittel	32
	6. Die qualifizierte elektronische Signatur als Beweismittel	33
	7. Zusammenfassung	34
V.	Gegenstand und Ziel der Untersuchung	34
B	Rechtliche Grundlagen einer gesetzlichen Infrastruktur für digitale Identität	38
I.	Das Verhältnis von Recht und Vertrauen	39
	1. Der Begriff des „rechtlichen Vertrauens“	39
	2. Vertrauensdefizite im Cyberspace ?	39
	a) Vertrauen in die Beweiskraft digitaler Daten	39
	b) Personales Vertrauen in digitale Identitäten	41
	c) Zusammenfassung	44
	3. Steuerungsstrategien für rechtliches Vertrauen im Netz	45
	a) Die Rezeption der Informationstechnologie durch das Recht in den 90er Jahren	45
	b) Vertrauen in Public-Key-Infrastrukturen durch Rechtssprechung	47
	c) Vertrauen in Public-Key-Infrastrukturen durch Privatautonomie	49
	d) Zusammenfassung	51
	4. Verfassungsrechtliche Verantwortung des Gesetzgebers gegenüber digitaler Identität	51
	a) Infrastrukturverantwortung des Gesetzgebers gegenüber dem elektronischen Rechtsverkehr	52

b)	Reichweite und Grenzen staatlicher Infrastrukturver- antwortung gegenüber digitaler Identität	53
c)	Zusammenfassung	55
5.	Gesetzliche Gestaltungsmöglichkeiten von Vertrauen in elektronische Kommunikation	55
a)	Vertrauen als Ausgleich zwischen materieller Gerechtigkeit und Rechtsfrieden	55
b)	Rechtliches Vertrauen durch technische Regulierung	58
c)	Konsequenzen für digitales Identitätsmanagement	59
aa)	Anforderungen an rechtliches Vertrauen in die Authentizität von Daten	59
bb)	Anforderungen an Vertrauen in die Validität von Daten	62
cc)	Zwischenergebnis	64
II.	Zertifizierung als Vertrauensschlüssel des elektronischen Rechtsverkehrs	64
1.	Rechtliche Grundlagen der gesetzlichen Zertifizierungsdienstleistung	65
a)	Der Zertifizierungsdiensteanbieter	65
b)	Gesetzlicher Tätigkeitsbereich des Zertifizierungsdiensteanbieters	66
c)	Das qualifizierte Zertifikat	69
aa)	Begriff	70
bb)	Darstellung der Inhalte	70
cc)	Interpretierbarkeit von Attributzertifikaten	71
2.	Virtuelle Zertifizierung	74
a)	Begriff	74
b)	Virtuelle Zertifizierung als Voraussetzung für Wettbewerb	75
c)	Systematische Grenzen virtueller Zertifizierungsinfrastrukturen	76
aa)	Anwendungsbasierende Verwendungsschranken bei geschlossenen Benutzergruppen	77
bb)	Rechtliche Verwendungsbeschränkungen von Zertifikaten	78
cc)	Verwendungsbeschränkungen als Problem praktischer Akzeptanz	79
dd)	Verwendungsbeschränkungen infolge technischer Standardisierungsdefizite	80
ee)	Zusammenfassung	80
d)	Rechtliche Grenzen virtueller Zertifizierung	81
aa)	Technikrechtliche Grenzen durch das SigG	81
(1)	Die Rolle des Sicherheitskonzepts gemäß §§ 4 Abs. 2 S. 5, 4 Abs. 5 SigG	82
(2)	Die Effektivität der weiteren Kontrollinfrastruktur des SigG	83
(3)	Konsequenzen für virtuelle Zertifizierungsinfrastrukturen	84
bb)	Selbstzertifizierung als rechtliche Grenze virtueller Zertifizierung ?	84
(1)	“Direct Trust” vs. “Trusted Third Party”	85
(a)	Direct Trust im Zertifikatsmanagement	86
(b)	Direct Trust innerhalb der gesetzlichen Sicherheitsinfrastruktur	87
(2)	Selbstzertifizierung als Problem der gewerberechtlchen Zuverlässigkeit	89

(3) Selbstzertifizierung als Grund für „ernstliche Zweifel“ im Sinne des § 292a ZPO	92
(4) Analogiefähigkeit allgemeiner Rechtsgrundsätze	94
(a) Unbewusste Regelungslücke ?	94
(b) Analoge Anwendung der §§ 20, 21 VwVfG	96
(c) Selbstzertifizierung de lege ferenda	98
(aa) Regulierungsverzicht	98
(bb) Repressives Verbot der Selbstzertifizierung	99
(cc) Rechtsfolgenregulierender Ansatz	100
(dd) Verwendungsbeschränkungen im Zertifikat	101
cc) Zusammenfassung	102
3. Zertifizierung als privatwirtschaftliche Dienstleistung	103
a) Infrastrukturgewährleistung in der Post- und Telekommunikation als Leitmodell	103
b) Grenzen privatwirtschaftlicher Zertifizierungsdienstleistungen	105
aa) Technische und organisatorische Systemsicherheit	105
bb) Sicherheit der Teilnehmer-Identifizierung	107
cc) Die Attributskompetenz als Grenze privatwirtschaftlicher Zertifizierung	108
c) Zusammenfassung	109
C Attributzertifizierung als Bestandteil der gesetzlichen Zertifizierungsinfrastruktur	111
I. Attributzertifizierung im SigG	111
1. Definition	111
2. Zertifizierung von Attributen	112
3. Das Certification Practice Statement (CPS) als fakultative Erweiterung des Zertifikats	113
a) Begriff	113
b) Die Bedeutung von Certification Practice Statements innerhalb gesetzlicher Zertifizierungsinfrastrukturen	114
c) Rechtliche Gestaltungsmöglichkeiten des Risikos „Anwenderumgebung“ im Certification Practice Statement	115
d) Würdigung	117
II. Die personenbezogene Attributsgarantie des qualifizierten Attributzertifikats	118
1. Das qualifizierte Attributzertifikat	118
a) Definition	118
b) Die Haftung des Zertifizierungsdiensteanbieters für Attribute als Bestandteil qualifizierter Zertifikate	119
c) Persönliche Reichweite einer Haftung für qualifizierte Attributzertifikate gemäß § 11 SigG	120
d) Die Statusgarantie des qualifizierten Attributzertifikats	122
2. Die Attributskompetenz des Zertifizierungsdiensteanbieters	125
a) Die für das Attribut „zuständige Stelle“	125
b) Die „zuständige Stelle“ als Garant des Attributzertifikats ?	125

c)	Beständige Haftung gemäß § 5 Abs. 2 SigG als rechtsverbindliche Mitwirkungsakte der „zuständigen Stelle“ ?	127
aa)	Die Auskunftsverantwortlichkeit der „zuständigen Stelle“ gemäß SigG	128
	(1) Das öffentlich-rechtliche Attribut	128
	(2) Das privatrechtliche Attribut	130
bb)	Auskunftsvertrag zwischen „zuständiger Stelle“ und Zertifizierungsdiensteanbieter	132
cc)	Deliktische Haftung der „zuständigen Stelle“ im Rahmen von Attributsauskünften	134
dd)	Vertrauenshaftung der „zuständigen Stelle“	135
	(1) Rechtsscheinhaftung gegenüber Dritten	136
	(2) Rechtsscheinhaftung gegenüber dem Zertifizierungsdiensteanbieter	138
ee)	Zusammenfassung	138
d)	Unmittelbare Attributzertifizierung durch die „zuständige Stelle“	139
e)	Qualifizierte Attributzertifikate als exklusive Dienstleistung von Zertifizierungsdiensteanbietern	141
3.	Die Erforderlichkeit einer eigenständigen gesetzlichen Infrastruktur für gesonderte Attributzertifikate	143
a)	Die gesetzliche Privilegierung des qualifizierten Attributzertifikats	143
b)	Privilegierung durch die gesetzliche Förderung von Glaubwürdigkeit	144
c)	Die systematische Integrierbarkeit „isolierter“ Attributzertifikate in die gesetzliche Zertifizierungsinfrastruktur	146
d)	Exkurs: Die Anwendbarkeit der weiteren Kontrollinfrastruktur des SigG auf Anbieter „isolierter“ Attributzertifikate	149
e)	Die allgemeine Attributshaftung außerhalb des Geltungsbereichs des SigG	151
aa)	Haftung aus Attributzertifizierungsvertrag	151
	(1) Abgrenzung Rechtsgeschäft – Gefälligkeitsverhältnis	153
	(2) Drittschutz des Zertifizierungsvertrages	154
	(3) Unmittelbarer vertraglicher Anspruch zwischen Zertifizierungsdienst und Drittem als Adressat des Zertifikats	156
	(4) Schadensausgleich im Wege der Drittschadensliquidation	157
bb)	Deliktische Haftung des Zertifikatausstellers gegenüber Dritten	157
cc)	Vertrauenshaftung des Zertifikatausstellers gegenüber Dritten	158
f)	Zusammenfassung	162
D	Rechtliche Gestaltungsmöglichkeiten von Attributsinhalten	164
I.	Das Beschränkungsattribut gemäß §§ 7 Abs. 1 Nr. 7, 11 Abs. 3 SigG	164
1.	Das Beschränkungsattribut als Instrument individuellen Risikomanagements des Zertifikatinhabers	164
2.	Das Beschränkungsattribut des Zertifizierungsdiensteanbieters	166
3.	Anzeige des Beschränkungsinhalts gegenüber dem Rechtsverkehr	167
4.	Dogmatische Einordnung und Rechtsfolgen der Selbstbeschränkung gemäß § 7 Abs. 1 Nr. 7 SigG	168
5.	Zusammenfassung	171

II.	Das Attribut über die Vertretungsmacht	172
	1. Inhalt und Voraussetzungen der Zertifizierung	172
	2. Die rechtliche Verantwortlichkeit des Zertifizierungsdiensteanbieters für Vertretungsattribute	174
III.	Das Attribut über berufsbezogene Angaben	176
	1. Inhalt und Voraussetzungen der Zertifizierung	176
	2. Berufsständische Organisationsmodelle der Attributzertifizierung	177
	a) Kammer als Bestätigungsstelle im Sinne von § 5 Abs. 2 SigG	177
	b) Kammer als (virtueller) Zertifizierungsdiensteanbieter	178
	c) Kammer als Registrierungsstelle	179
	d) Kammer als Aussteller isolierter Attributzertifikate	179
	3. Kammerrechtliche Aspekte berufsbezogener Zertifizierung	180
	a) Rechtliche Grundlagen der berufsbezogenen Zertifizierung	180
	aa) Die Pflichtmitgliedschaft der Berufskammern	180
	bb) Aufgabenbereich der Kammern	181
	cc) Grenzen der Kammertätigkeit	182
	b) Die Verhältnismäßigkeit qualifizierter Zertifizierungsdienstleistungen aus Sicht der kammerrechtlichen Aufgabenwahrnehmung	182
	aa) Die Erforderlichkeit der Kammerzertifizierung als Infrastrukturmaßnahme	183
	bb) Die Erforderlichkeit der Kammerzertifizierung für die Berufsaufsicht	184
	cc) Zusammenfassung	185
	4. Landesrecht als Steuerungsinstrument berufsbezogener Zertifizierung	185
	a) Problemstellung	186
	b) Regelungskompetenz der Berufskammern	186
	c) Landesrechtliche Maßnahmen im Licht des Rechts der Wettbewerbsbeschränkungen	187
	aa) Die Anwendbarkeit von § 1 GWB auf landesrechtliche Zertifizierungsmonopole	187
	bb) Die Anwendbarkeit von Art. 81 EGV auf berufsbezogene Zertifizierungsmonopole	189
	cc) Zusammenfassung	191
E	Zusammenfassung und Ergebnisse	192
	Literaturverzeichnis	