

Inhaltsverzeichnis

Einführung	1
1 Digitale Signaturen	7
1.1 Technisches Konzept der Authentikationssysteme	7
1.1.1 Symmetrische Authentikationssysteme	8
1.1.2 Asymmetrische Authentikationssysteme	9
1.2 Kryptanalyse	10
1.2.1 Angriffsziele	12
1.2.2 Angriffsarten	13
1.3 Voraussetzungen für digitale Signaturen	14
1.3.1 Voraussetzungen zur Anerkennung digitaler Signaturen	14
1.3.2 Schutzfunktionen der digitalen Signatur	15
1.4 Verfahren der digitalen Signatur	18
1.4.1 Sichere Zuordnung von Schlüsseln	18
1.4.2 Interoperabilität digitaler Signaturen	19
1.4.3 Sichere Darstellung digital signierter Daten	20
1.5 Rechtliche Rahmenbedingungen	21
1.5.1 Utah Digital Signature Act	21
1.5.2 Signaturgesetz	21
1.5.2.1 Konzeption des Signaturgesetzes	22
1.5.2.2 Einordnung anderer Signaturverfahren	25
1.5.2.3 Rechtsfolgen digitaler Signaturen	27
1.5.3 Kritische Kommentierung	30
1.5.3.1 Akzeptanz digitaler Signaturen	32
1.5.3.2 Inkompatible Sicherheitsinfrastrukturen	33
1.5.3.3 Beschränkung auf natürliche Personen	34
1.5.3.4 Sichere digitale Signaturen	37
1.5.3.5 Haftung von Zertifizierungsstellen	38
1.5.3.6 Identifikationsfunktion digitaler Signaturen...	40
1.5.3.7 Wirtschaftliche Rahmenbedingungen	45
1.5.4 Weiterentwicklung des Signaturgesetzes	47
1.5.4.1 Evaluierungsbericht	48
1.5.4.2 Gesetzesentwurf für den modernen Geschäfts- verkehr	50



1.5.5	EU-Richtlinie zu elektronischen Signaturen	54
1.5.5.1	Konzeption der EU-Richtlinie	54
1.5.5.2	Stufenmodell elektronischer Signaturen	57
1.5.5.3	Gegenüberstellung von EU-Richtlinie und Si- gnaturgesetz	63
2	Rechtsgeschäfte	67
2.1	Rechtsgeschäftslehre	67
2.2	Willenserklärungen	69
2.2.1	Tatbestand der Willenserklärung	70
2.2.2	Wirksamwerden einer Willenserklärung	71
2.2.3	Abgabe einer Willenserklärung	73
2.2.4	Zugang einer Willenserklärung	73
2.2.4.1	Empfangstheorie	75
2.2.4.2	Vernehmungstheorie	77
2.2.4.3	Zugangshindernisse	79
3	Elektronische Kommunikationssysteme	83
3.1	Elektronische Geschäftssysteme	83
3.2	Request-Response Technik	86
3.2.1	Synchrone Bearbeitung	87
3.2.2	Trennung der Systeme	89
3.2.2.1	Betreiberkontrollierte Gesamtsysteme	90
3.2.2.2	Benutzerkontrollierte End-Systeme	92
3.3	Store-and-Forward Technik	94
3.3.1	Asynchrone Bearbeitung	95
3.3.2	Anwendung: Elektronische Post	96
3.3.3	Trennung der Systeme	98
3.3.4	Systemverantwortlichkeiten	99
3.3.4.1	Gesamtsysteme	100
3.3.4.2	Zentrale Transfersysteme	102
3.3.4.3	Lokale Transfersysteme	103
3.3.4.4	Verteilte Transfersysteme	106
4	Gültigkeit digitaler Signaturen	111
4.1	Gültigkeitskriterien digitaler Signaturen	112
4.2	Gültigkeit signierter Objekte	114
4.3	Klassifikationsschema der Gültigkeitskriterien	116
4.4	X.509 Gültigkeitsmodell	119
4.5	Gültigkeitsmodell nach dem Signaturgesetz	122
4.5.1	Definition der Gültigkeitskriterien	123
4.5.2	Definition der Gültigkeit signierter Objekte	125
4.5.3	Begründung der Gültigkeitskriterien	127
4.5.3.1	Technische Gültigkeitskriterien	128
4.5.3.2	Sicherheitsspezifische Gültigkeitskriterien	128

4.5.3.3	Anwendungsspezifische Gültigkeitskriterien...	129
4.5.3.4	Annahmen zu Gültigkeitskriterien	133
4.5.4	Gültigkeitsprüfung nach dem Signaturgesetz	136
4.5.5	Verwendung geprüfter Komponenten	140
4.6	Vergleich der Gültigkeitsmodelle	143
4.7	Zertifikate	146
4.7.1	Lebenszyklus der Zertifikate	146
4.7.2	Sperrung von Zertifikaten	149
4.7.3	Definition des fairen Sperrzeitpunktes	151
5	Zeitangaben	155
5.1	Notwendigkeit von Zeitangaben	155
5.2	Erstellung von Zeitangaben	158
5.2.1	Zeitangaben des Unterzeichners	159
5.2.2	Zeitstempeldienste	160
5.2.3	Zeitstempelbox	163
5.3	Bestätigung von Zeitpunkten	165
5.3.1	Zeitstempeln – Signieren	166
5.3.2	Signieren – Zeitstempeln	167
5.3.3	Zeitstempeln – Signieren – Zeitstempeln	169
5.3.4	Signieren – Zeitstempeln – Signieren	170
5.4	Bewertung der Zeitangaben	174
6	Stabilität digitaler Signaturen	177
6.1	Fiktion der Aktualität von Statusinformationen	177
6.2	Instabile digitale Signaturen	180
6.3	Sichere Überprüfung digitaler Signaturen	184
6.3.1	Signalisierung laufender Sperrprozesse	186
6.3.2	Signalisierung der Sperrung des Teilnehmer-Zertifikates	186
6.3.3	Verzögerter Beginn der Gültigkeitsprüfung	188
6.3.4	Bekanntgabe des Zeitpunktes der Antragstellung	190
6.4	Bewertung der Methoden	190
7	Nachhaltigkeit digitaler Signaturen	193
7.1	Zeitfaktoren digitaler Signaturen	193
7.2	Überprüfbarkeit von Zeitstempeln	196
7.3	Schutz der Nachhaltigkeit digitaler Signaturen	200
7.3.1	Re-Signierung	202
7.3.2	Verkettete Zeitstempel	205
7.3.3	Zeitstempeldienst mit Zeitstempelarchiv	207
7.3.4	Notariatsdienst mit Archiv	208
7.4	Bewertung der Verfahren	212



8	Fairness bei elektronischen Willenserklärungen	217
8.1	Formen elektronischer Willenserklärungen	217
8.1.1	Elektronisch übermittelte Willenserklärungen	218
8.1.2	Elektronisch archivierte Willenserklärungen	219
8.1.3	Automatisch erstellte Willenserklärungen	220
8.2	Wirksamwerden digital signierter Willenserklärungen	221
8.2.1	Kenntnisnahme digital signierter Willenserklärungen	222
8.2.2	Prüfung digital signierter Nachrichten	225
8.3	Faire Gestaltung der Gültigkeitsprüfung digitaler Signaturen	228
8.3.1	Faire Möglichkeit zur Kenntnisnahme digital signierter Nachrichten	229
8.3.2	Digitale Signaturen mit beigefügten Prüfinformationen	232
8.3.3	Vertrauenswürdig geprüfte digitale Signaturen	233
8.4	Bewertung der Konzepte	235
	Fazit und Ausblick	241
	Literaturverzeichnis	245
	Abkürzungsverzeichnis	255
	Sachverzeichnis	257



<http://www.springer.com/978-3-540-42351-5>

Digitale Signaturen

Bertsch, A.

2002, XIII, 264 S., Hardcover

ISBN: 978-3-540-42351-5