

# Inhalt

<b>1</b>	<b>Ausgangslage</b> .....	1
1.1	Zweck der digitalen Signatur.....	1
1.2	Technologien.....	2
1.2.1	Authentizität.....	2
1.2.2	Integrität.....	4
1.2.3	Geheimhaltung.....	5
1.2.4	Digitale Unterschrift.....	5
1.2.5	Datums- und Zeitstempel.....	6
1.2.6	Sende- und Empfangsbestätigung.....	6
1.2.7	Identifikation von Servern.....	6
1.3	Rechtliche Aspekte.....	7
1.3.1	Identifizierung des Vertragspartners.....	7
1.3.2	Sicherheit über den Inhalt von Dokumenten.....	8
1.3.3	Nachweisbarkeit übermittelter Daten.....	10
1.4	Resümee.....	11
<b>2</b>	<b>Konzept</b> .....	13
2.1	Zielsetzung.....	13
2.1.1	Analoge Kommunikation.....	13
2.1.2	Digitale Kommunikation.....	15
2.2	Das Prinzip der digitalen Signatur.....	15
2.2.1	Das Konzept der asymmetrischen Schlüssel.....	19
2.2.2	Erzeugen einer digitalen Signatur.....	21
2.2.3	Versenden des signierten Dokumentes.....	23
2.2.4	Prüfen der Signatur.....	24
2.3	Administrative Elemente.....	25
2.3.1	Der Nutzer bzw. Antragsteller.....	25
2.3.2	Zertifizierungsstelle oder Trust Center.....	27
2.3.2.1	Zeitstempeldienst.....	31
2.3.2.2	Zulassung sog. Pseudonyme.....	31
2.3.2.3	Pflege des Schlüsselverzeichnisses.....	32

2.3.2.4	24-Stunden-Sperrdienst .....	33
2.3.2.5	Schlüsselaufbewahrung .....	34
2.3.3	Prüfstellen .....	34
2.3.4	Regulierungsbehörde .....	35
2.4	Technische Komponenten .....	38
2.4.1	Die Chipkarte .....	39
2.4.2	Lesegeräte .....	43
2.5	Das Zertifikat.....	46
2.5.1	Der Inhalt des Zertifikates .....	46
2.5.2	Überprüfen von Zertifikaten .....	53
2.5.3	Verzeichnis der Zertifikate .....	53
2.5.4	Attribut-Zertifikate .....	54
<b>3</b>	<b>Anwendung</b> .....	<b>57</b>
3.1	Beantragen einer digitalen Signatur .....	58
3.1.1	Weitere Zertifizierungstellen .....	60
3.1.2	Freischalten der Chipkarte .....	62
3.2	Signieren.....	64
3.2.1	Einsatz der Signiersoftware .....	64
3.2.2	Versand.....	66
3.2.3	Verwendung von PGP .....	67
3.3	Prüfen einer Signatur .....	67
3.3.1	Prüfen des Siegels .....	68
3.3.2	Prüfen einer E-Mail mit PGP.....	70
3.4	Verifizieren der Zertifikate .....	70
3.4.1	Lokales Verzeichnis der Zertifikate .....	71
3.4.2	Online-Prüfung.....	74
3.5	Einbindung in Anwendungen .....	75
3.6	Zeitstempeldienst .....	77
3.7	Sicherheit .....	78
<b>4</b>	<b>Kryptoverfahren</b> .....	<b>81</b>
4.1	Entstehung .....	81
4.2	Grundlagen .....	82
4.3	Symmetrische Verfahren .....	84
4.3.1	Der Ablauf der Verschlüsselung .....	84
4.3.2	Schlüsselverwaltung.....	86
4.3.3	Algorithmen.....	87
4.4	Asymmetrische Verfahren .....	88
4.4.1	Die Charakteristik der Schlüssel.....	90
4.4.2	Verschlüsseln mit dem öffentlichen Schlüssel des Empfängers.....	91
4.4.3	Signieren mit dem privaten Schlüssel des Senders.....	95

4.4.4	Algorithmen.....	96
4.5	Hybride Verfahren .....	97
4.6	Kryptographische Hashverfahren.....	100
4.6.1	Bildung des Hashwertes.....	100
4.6.2	Verschlüsselung .....	101
4.7	Digitale Signatur .....	102
4.7.1	Erzeugen der Signatur.....	102
4.7.2	Prüfen der Signatur .....	104
4.7.3	Algorithmen.....	105
4.8	Sicherheit.....	105
4.8.1	Brute-Force-Attacke.....	106
4.8.2	Man in the middle .....	106
4.8.3	Craking Cyphers.....	106
4.8.4	Clear-Text-Attack.....	106
<b>5</b>	<b>Rechtliche Aspekte .....</b>	<b>107</b>
5.1	Internet – rechtsfreier Raum ? .....	107
5.2	Das Internet – neue Rechtsphänomene und -beziehungen .....	107
5.3	Vertragsschluß im Internet.....	108
5.3.1	Voraussetzungen des Vertragsschlusses .....	109
5.3.1.1	Das Angebot im Internet .....	110
5.3.1.2	Der Zugang von Willenserklärungen .....	110
5.3.1.3	Der Zugang elektronischer Willenserklärungen .....	111
5.3.2	Der EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr .....	112
5.3.3	Grundsatz der Formfreiheit von Verträgen .....	115
5.3.3.1	Vertragliche und gesetzliche Schriftform .....	115
5.3.3.2	Ausgangssituation im Internet.....	116
5.4	Integration Allgemeiner Geschäftsbedingungen (AGB) ..	122
5.5	Beweis und Beweisrecht.....	122
5.5.1	Grundzüge des Beweisrechts.....	123
5.5.2	Beweiswert elektronischer Dokumente.....	124
5.6	Das Recht der digitalen Signatur .....	125
5.6.1	Das Signaturgesetz .....	126
5.6.1.1	Der Begriff der digitalen Signatur.....	126
5.6.1.2	Rechtlicher Wert digitaler Signaturen.....	127
5.6.1.3	Haftungsrechtliche Aspekte .....	130
5.7	Europäische Entwicklung .....	131
5.8	Internationale Entwicklungen.....	133

<b>6</b>	<b>Einsatzfelder</b> .....	135
6.1	Business-Kommunikation.....	136
6.1.1	Business-to-Business-Kommunikation .....	136
6.1.2	Business-to-Customer-Kommunikation.....	137
6.1.3	Intranet (firmeninterne Kommunikation).....	138
6.2	Behördliche Kommunikation .....	139
6.2.1	Behörden untereinander .....	140
6.2.2	Behörden mit Bürgern.....	140
6.2.3	Intranet (behördenintern) .....	143
6.3	Private Kommunikation.....	143
<b>7</b>	<b>Ausblick</b> .....	145
7.1	Neue Anwendungsfelder .....	145
7.1.1	Firmentintern .....	146
7.1.2	Kommunen .....	147
7.1.3	Private Kommunikation.....	148
7.1.4	Anwendungssoftware.....	149
7.2	Rechtliche Harmonisierung .....	150
7.2.1	Anerkennung nur bei technischer Gleichwertigkeit .....	150
7.2.2	Europäische Entwicklungen .....	151
7.2.3	Bestrebungen der Vereinten Nationen .....	152
<b>8</b>	<b>Gesetzesgrundlage</b> .....	155
8.1	Signaturgesetz (SigG) .....	155
8.2	Signaturverordnung (SigV) .....	164
8.3	Der Maßnahmenkatalog.....	175
	<b>Glossar</b> .....	177
	<b>Literatur</b> .....	183
	<b>Index</b> .....	191