

# Inhaltsverzeichnis

<b>1 Einführung und Überblick</b>	<b>1</b>
1.1 Ziel des Buches . . . . .	1
1.2 Wer soll dieses Buch lesen? . . . . .	1
1.3 Aufbau des Buches . . . . .	2
<b>2 Rechtliche Grundlagen der elektronischen Signatur</b>	<b>5</b>
2.1 Die Unterschrift als Teil gesetzlicher Formvorschriften . . . . .	5
2.2 Kategorien der Sicherheit mit elektronischen Signaturen . . . . .	7
2.2.1 Die einfache elektronische Signatur . . . . .	7
2.2.2 Die fortgeschrittene elektronische Signatur . . . . .	7
2.2.3 Die qualifizierte elektronische Signatur . . . . .	8
2.2.4 Akkreditierte Zertifizierungsdiensteanbieter . . . . .	10
2.2.5 Akkreditierung und Zertifizierung von Systemen . . . . .	10
2.2.6 Elektronische Zeitstempel . . . . .	11
2.3 Das deutsche Recht im internationalen Vergleich . . . . .	12
2.4 Die manuelle Unterschrift im Vergleich zu elektronischen Signaturen . . . . .	13
2.4.1 Funktionen einer Unterschrift . . . . .	13
2.4.2 Ersatz der manuellen Unterschrift durch die elektronische Signatur . . . . .	17
2.5 Beweisqualität elektronisch signierter Dokumente . . . . .	18
2.5.1 Beweiskraft einfacher und fortgeschrittener Signaturen . . . . .	18
2.5.2 Beweiskraft qualifizierter Signaturen . . . . .	19
2.5.3 Staatlich geprüfte Algorithmen . . . . .	20
2.5.4 Beweisqualität des biometrischen Merkmals „Unterschrift“ . . . . .	21
2.5.5 Schutz der biometrischen Daten . . . . .	22
2.6 Zusammenfassung der rechtlichen Situation für elektronische Signaturen . . . . .	23

<b>3 Technische Realisierung elektronischer Signaturen</b>	<b>27</b>
3.1 Informationstechnische Grundlagen . . . . .	27
3.1.1 Verfahren zur Verschlüsselung . . . . .	27
3.1.2 Hashverfahren . . . . .	29
3.1.3 Elektronisch signierte Zeitstempel . . . . .	32
3.2 Ablauf des elektronischen Signierens und Verifizierens . . . . .	33
3.2.1 Austausch mit fortgeschrittener Signatur . . . . .	33
3.2.2 Austausch mit fortgeschrittener Signatur und Zertifikaten	36
3.2.3 Austausch mit qualifizierter Signatur . . . . .	38
3.3 Schutz der Signaturschlüssel . . . . .	40
3.3.1 Passwörter – Schutz durch Wissen . . . . .	40
3.3.2 Sichere Verwahrung – Schutz durch Besitz . . . . .	41
3.3.3 Untrennbare Eigenschaften – Schutz durch Biometrie . . .	42
3.4 Biometrische Merkmale in elektronischen Signaturen . . . . .	44
3.4.1 Die Einbeziehung biometrischer Merkmale in elektroni-	
sche Signaturen . . . . .	44
3.4.2 Biometrische Merkmale in fortgeschrittenen elektroni-	
schen Signaturen . . . . .	47
3.4.3 Automatische Verifikation einer Unterschrift . . . . .	50
3.4.4 Verifikation einer Unterschrift durch einen Schrift-	
sachverständigen . . . . .	52
3.4.5 Biometrische Merkmale in einfachen und qualifizierten	
Signaturen . . . . .	52
<b>4 Die elektronische Signatur in Geschäftsprozessen</b>	<b>55</b>
4.1 Nutzenpotenziale elektronischer Signaturen in Geschäftsprozes-	
sen . . . . .	55
4.2 Einsatzszenarien in der Unternehmenskommunikation . . . . .	56
4.2.1 Unternehmensexterne Kommunikation . . . . .	56
4.2.2 Unternehmensinterne Kommunikation . . . . .	59
4.3 Ausgewählte Realisierungsaspekte . . . . .	60
4.3.1 Mehrfache Signatur . . . . .	61
4.3.2 Gemeinsame Signatur . . . . .	61
4.3.3 Zeitstempelsignatur . . . . .	63

4.3.4	Zeitspannensignatur . . . . .	66
4.3.5	Loginersatz . . . . .	69
4.3.6	Automatisierte Massensignaturen . . . . .	69
4.3.7	Bestimmter Verifizierer . . . . .	71
4.3.8	Signatur von Datenströmen . . . . .	73
4.4	Archivierung elektronisch signierter Dokumente . . . . .	75
4.4.1	Dokumentations- und Aufbewahrungsvorschriften . . . . .	76
4.4.2	Verlust der Sicherheitseignung von Algorithmen . . . . .	79
4.4.3	Gesetzliche Anforderungen an die Langzeitarchivierung elektronischer Signaturen . . . . .	80
4.4.4	ArchiSig - Konzept zur Langzeitarchivierung elektronisch signierter Dokumente . . . . .	82
4.4.5	Nutzdatenformate . . . . .	83
4.4.6	Archivierung erforderlicher Verifikationsdaten . . . . .	85
4.4.7	Signaturerneuerung . . . . .	87
4.4.8	Transformation elektronisch signierter Dokumente . . . . .	90
4.4.9	Erneuerung der Datenträger in einem Archivsystem . . . . .	91
<b>5</b>	<b>Fallstudie</b>	<b>95</b>
5.1	Rechtliche Grundlagen . . . . .	95
5.1.1	Gesetzliche Schriftformerfordernisse für Versicherungsverträge . . . . .	95
5.1.2	Pragmatische Anforderungen an die Form von Anträgen . . . . .	98
5.1.3	Eignung von biometrischen Merkmalen in elektronisch signierten Dokumenten . . . . .	99
5.2	Fachliche und technische Realisierung . . . . .	100
5.2.1	Ausgangszustand, Zielstellung und Voraussetzungen . . . . .	100
5.2.2	Anforderungen an den elektronischen Antragsprozess . . . . .	101
5.2.3	Modell des elektronischen Antragsprozesses mit elektronischen Unterschriften . . . . .	103
5.2.4	Hardware-Komponenten zur Erfassung der Unterschrift . . . . .	106
5.2.5	Übermittlung elektronisch signierter Dokumente an den Kunden . . . . .	108
5.3	Angriffsszenarien . . . . .	109

5.3.1	Technische Angriffsszenarien im Überblick . . . . .	109
5.3.2	Der Kunde als Angreifer im Versicherungsantragsprozess	114
5.3.3	Der Vermittler als Angreifer im Versicherungsantragsprozess . . . . .	116
5.3.4	Die Vertriebsorganisation als Angreifer im Versicherungsantragsprozess . . . . .	118
5.3.5	Das Versicherungsunternehmen als Angreifer des Versicherungsantragsprozesses . . . . .	119
5.3.6	Außenstehende als Angreifer des Versicherungsantragsprozesses . . . . .	121
5.4	Maßnahmen zum Schutz des Antrags . . . . .	121
5.4.1	Schutz durch Kryptographie . . . . .	121
5.4.2	Starke Kryptographie und staatlich geprüfte Algorithmen	122
5.4.3	Schutz durch das Signieren strukturierter Daten . . . . .	123
5.4.4	Zusätzlicher Schutz durch den Einsatz von Biometrie . . .	124
5.4.5	Vergleich symmetrischer und asymmetrischer Verfahren .	125
5.4.6	Schutz durch Gegenzeichnung des Vermittlers . . . . .	128
5.4.7	Schutz durch sichere Hardware . . . . .	129
5.4.8	Schutz durch einen Zeitstempel . . . . .	131
5.4.9	Einbindung der biometrischen Daten in eine Referenzdatenbank . . . . .	133
5.4.10	Das Zusammenwirken der Maßnahmen zum umfassenden Schutz des Prozesses . . . . .	133
<b>6 Zusammenfassung und Ausblick</b>		<b>141</b>
<b>Glossar</b>		<b>143</b>
<b>Abkürzungsverzeichnis</b>		<b>147</b>
<b>Abbildungs- und Tabellenverzeichnis</b>		<b>149</b>
<b>Literatur</b>		<b>151</b>
<b>Autorenverzeichnis</b>		<b>165</b>
<b>Index</b>		<b>167</b>