

Inhaltsverzeichnis

1 Einleitung	1
1.1 Einige Vorbemerkungen	1
1.2 Aufbau des Buches	4
2 Grundlagen	7
2.1 Einführung	7
2.2 Bedrohungen	8
2.3 Verschlüsselungsverfahren	12
2.4 Sicherheit von Verschlüsselungsverfahren	18
2.5 Unveränderbarkeit von Daten mittels Hashfunktionen	30
2.6 Authentifizierung	33
2.7 Elektronische Signaturen	46
2.8 Zeitstempel	52
2.9 Schlüsselverteilung	54
2.10 Das deutsche Signaturgesetz (SigG)	64
2.11 Spezielle Themen im ECommerce	70
2.12 Zusammenfassung	83
3 Klassifikation von eZahlungssystemen	85
3.1 Einführung	85
3.2 Marktplatzteilnehmer	88
3.3 Klassifikation	90
3.4 Vergleich	97
3.5 Sicherheitsaspekte	98
3.6 Zusammenfassung	102

4 Sicherheitskonzepte verschiedener Zahlungssysteme	103
4.1 Einleitung	103
4.2 Internetbanking	103
4.3 Kreditkarten-Systeme	111
4.4 Verrechnungssysteme	124
4.5 Scheckähnliche Systeme	138
4.6 Chipkarten-Systeme	143
4.7 Zusammenfassung	151
5 Methoden den eMarktplatz abzusichern	153
5.1 Einführung	153
5.2 Pretty Good Privacy (PGP)	154
5.3 PEM	158
5.4 MailTrust	161
5.5 PKCS	165
5.6 S/MIME	166
5.7 Das SSL-Protokoll	167
5.8 Das OTP-Protokoll	173
5.9 Zusammenfassung	177
6 Praktische Schutzmaßnahmen	179
6.1 Einführung	179
6.2 Ausgangssituation	179
6.3 Typische Angriffe und ihre Abwehr	181
6.4 Fazit	206
7 Ausblicke	209
7.1 Die Zukunft des eCommerce	209
A Glossar	213
Literaturverzeichnis	229
Stichwortverzeichnis	237