Inhaltsverzeichnis

Vorwort . . . . . **XXVII**

Symbole und Notationen . . . . . **XXIX**

Abkürzungen . . . . . **XXXIII**

1 Einleitung **1**
1.1 Geschichte der Chipkarten 2
1.2 Kartentypen und deren Anwendungen 8
1.2.1 Speicherkarten 8
1.2.2 Prozessorkarten 9
1.2.3 Kontaktlose Karten 10
1.3 Normung 11

2 Arten von Karten **17**
2.1 Hochgeprägte Karten 17
2.2 Magnetstreifenkarten 18
2.3 Chipkarten 21
2.3.1 Speicherkarten 22
2.3.2 Kontaktlose Speicherkarten 23
2.3.3 Prozessorkarten 23
2.3.4 Kontaktlose Prozessorkarten 26
2.3.5 Multi-Megabyte-Karten 27
2.3.6 Sicherheitstoken 28
2.4 Optische Speicherkarten 29

3 Physikalische Eigenschaften **31**
3.1 Kartenformate 32
3.2 Kontaktflächen 39

3.3 Kartenkörper 41
3.4 Kartenmaterialien 42
3.5 Kartenelemente und Sicherheitsmerkmale 45
3.5.1 Guillochen 46
3.5.2 Unterschriftsstreifen 46
3.5.3 Mikroschrift 47
3.5.4 UV-Schrift 47
3.5.5 Barkode 47
3.5.6 Hologramm 47
3.5.7 Kinegramm, Kippbild 48
3.5.8 Multiple Laser Image 48
3.5.9 Hochprägung 49
3.5.10 Lasergravur 50
3.5.11 Rubbelfeld 50
3.5.12 Thermochrome-Anzeige 51
3.5.13 Moduliertes Merkmal 52
3.5.14 Sicherheitsmerkmale 53
3.6 Chipmodule 54
3.6.1 Elektrische Kontaktierung zwischen Chip und Modul 55
3.6.2 TAB-Modul 57
3.6.3 Chip-on-Flex-Modul 58
3.6.4 Lead-Frame-Modul 61
3.6.5 Sondermodule 63

4 Elektrische Eigenschaften 65
4.1 Beschaltung 67
4.2 Versorgungsspannung 68
4.3 Versorgungsstrom 71
4.4 Taktversorgung 73
4.5 Datenübertragung mit T=0/1 74
4.6 An-/Abschaltsequenz 75

5 Mikrocontroller für Chipkarten 77
5.1 Halbleitertechnologie 80
5.2 Prozessortypen 83
5.3 Speicherarten 87
5.3.1 ROM 89

5.3.2 EPROM 90
5.3.3 EEPROM 90
5.3.4 Flash 96
5.3.5 RAM 97
5.3.6 FRAM 98
5.4 Zusatzhardware 99
5.4.1 Kommunikation mit T=0/1 99
5.4.2 Kommunikation mit USB 100
5.4.3 Kommunikation mit MMC 101
5.4.4 Kommunikation mit SWP 101
5.4.5 Kommunikation mit I^2C-Bus 102
5.4.6 Timer 102
5.4.7 CRC-Recheneinheit 103
5.4.8 Zufallszahlengenerator 103
5.4.9 Takterzeugung und Taktvervielfachung 104
5.4.10 DMA 106
5.4.11 Speicherverwaltung 106
5.4.12 Java-Beschleuniger 108
5.4.13 Koprozessor für symmetrische Kryptoalgorithmen 109
5.4.14 Koprozessor für asymmetrische Kryptoalgorithmen 109
5.4.15 Fehlererkennung und -korrektur bei nichtflüchtigem Speicher . . . 110
5.4.16 Schnittstelle zu einem Massenspeicher 110
5.4.17 Modul mit mehreren Chips 111
5.4.18 Gestapelte Chips 113
5.5 Erweiterter Temperaturbereich 114

6 Informationstechnische Grundlagen 115
6.1 Strukturierung von Daten 115
6.2 Kodierung alphanumerischer Daten 122
6.2.1 7-Bit-Kode 122
6.2.2 8-Bit-Kode 122
6.2.3 16-Bit-Kode 123
6.2.4 32-Bit-Kode 123
6.3 SDL-Symbolik 124
6.4 Zustandsautomaten 125
6.4.1 Grundlagen zur Automatentheorie 126
6.4.2 Praktische Anwendung 127

6.5 Fehlererkennungs- und Fehlerkorrekturkodes 130
6.5.1 XOR-Prüfsummen 132
6.5.2 CRC-Prüfsummen 133
6.5.3 Reed-Solomon-Kodes 135
6.5.4 Fehlerkorrekturkodes 136
6.6 Datenkompression 138

7 Sicherheitstechnische Grundlagen 141
7.1 Kryptologie 141
7.1.1 Symmetrische Kryptoalgorithmen 147
7.1.1.1 DES-Algorithmus 147
7.1.1.2 AES-Algorithmus 149
7.1.1.3 IDEA-Algorithmus 150
7.1.1.4 COMP128-Algorithmen 151
7.1.1.5 Milenage-Algorithmus 151
7.1.1.6 Betriebsarten für Blockverschlüsselungsalgorithmen . 152
7.1.1.7 Mehrfachverschlüsselung 153
7.1.2 Asymmetrische Kryptoalgorithmen 155
7.1.2.1 RSA-Algorithmus 155
7.1.2.2 Schlüsselgenerierung für RSA 159
7.1.2.3 DSS-Algorithmus 161
7.1.2.4 Elliptische Kurven als asymmetrische Kryptoalgorithmen 162
7.1.3 Padding 164
7.1.4 Message Authentication Code und Cryptographic Checksum . . . 166
7.2 Hashfunktionen 167
7.3 Zufallszahlen 170
7.3.1 Erzeugung von Zufallszahlen 171
7.3.2 Prüfung von Zufallszahlen 174
7.4 Authentisierung 178
7.4.1 Einseitige symmetrische Authentisierung 180
7.4.2 Gegenseitige symmetrische Authentisierung 182
7.4.3 Statische asymmetrische Authentisierung 183
7.4.4 Dynamische asymmetrische Authentisierung 185
7.5 Digitale Signatur 187
7.6 Zertifikate 191
7.7 Schlüsselmanagement 193
7.7.1 Abgeleitete Schlüssel 195

7.7.2 Schlüsseldiversifizierung 195
7.7.3 Schlüsselversionen 195
7.7.4 Dynamische Schlüssel 196
7.7.4.1 Nutzung von symmetrischen Kryptoalgorithmen 196
7.7.4.2 Nutzung von asymmetrischen Kryptoalgorithmen . . . 197
7.7.5 Schlüsselinformationen 198
7.7.6 Beispiel für Schlüsselmanagement 199
7.8 Identifizierung von Personen 201
7.8.1 Identifizierung durch Wissen 202
7.8.2 Prüfung einer Geheimzahl 203
7.8.3 Wahrscheinlichkeit des Erratens einer PIN 205
7.8.4 Generierung einer PIN 206
7.8.5 Prüfung auf Echtheit des Terminals 208
7.8.6 Biometrische Verfahren 209

8 Kommunikation mit Chipkarten 217
8.1 Answer to Reset 219
8.1.1 Der Initial Character 222
8.1.2 Der Format Character 223
8.1.3 Die Interface Characters 223
8.1.3.1 Global Interface Character TA_1 224
8.1.3.2 Global Interface Character TA_i 225
8.1.3.3 Global Interface Character TC_1 226
8.1.3.4 Specific Interface Character TC_2 226
8.1.3.5 Specific Interface Character TA_i 227
8.1.3.6 Specific Interface Character TB_i 227
8.1.3.7 Specific Interface Character TC_i 227
8.1.3.8 Global Interface Character TA_2 228
8.1.4 Die Historical Characters 228
8.1.5 Der Check Character 231
8.1.6 Praxisbeispiele für ATRs 231
8.2 Protocol Parameter Selection 235
8.3 Struktur der Nachrichten 238
8.3.1 Struktur der Kommando-APDUs 239
8.3.2 Struktur der Antwort-APDUs 241
8.4 Sicherung der Datenübertragung 242
8.4.1 Datenobjekte für Klartext 245

8.4.2 Datenobjekte für Sicherheitsmechanismen 245
8.4.3 Datenobjekte für Hilfsfunktionen 246
8.4.4 Das Authentic-Verfahren 246
8.4.5 Das Combined-Verfahren 248
8.4.6 Sendefolgezähler 250
8.5 Logische Kanäle 251
8.6 Logische Protokolle 252
8.6.1 TCP/IP-Protokoll 253
8.6.2 HTTP-Protokoll 254
8.6.3 BIP-Protokoll 255
8.7 Anbindung von Terminals an übergeordnete Systeme 256
8.7.1 PC/SC 256
8.7.1.1 ICC-Aware Application 258
8.7.1.2 Service Provider 258
8.7.1.3 ICC Resource Manager 259
8.7.1.4 IFD Handler 259
8.7.1.5 IFD 260
8.7.1.6 ICC 260
8.7.2 OCF 260
8.7.3 MKT 260
8.7.4 MUSCLE 261

9 Kontaktbehaftete Datenübertragung 263
9.1 Physikalische Übertragungsschicht 263
9.2 Protokolle für Speicherkarten 268
9.2.1 Protokoll für Telefonchips 270
9.2.1.1 Rücksetzen des Adresszeigers 270
9.2.1.2 Erhöhen des Adresszeigers und Lesen 271
9.2.1.3 Schreiben auf eine Adresse 272
9.2.1.4 Löschen von Bytes 272
9.2.2 I^2C-Bus 272
9.2.2.1 Lesen von einer Adresse 273
9.2.2.2 Schreiben auf eine Adresse 274
9.3 ISO-Übertragungsprotokolle 275
9.3.1 Übertragungsprotokoll T=0 276
9.3.2 Übertragungsprotokoll T=1 282
9.3.2.1 Blockaufbau 283

9.3.2.2 Sendefolge-/Empfangsfolgezähler 287
9.3.2.3 Wartezeiten 287
9.3.2.4 Mechanismen des Übertragungsprotokolls 290
9.3.2.5 Beispiel für die Datenübertragung mit T=1 293
9.3.3 Vergleich der Übertragungsprotokolle T=0 und T=1 294
9.3.4 Übertragungsprotokoll T=14 (Deutschland) 294
9.4 Übertragungsprotokoll USB 295
9.4.1 Elektrische Verbindung 297
9.4.2 Logische Verbindung 298
9.4.2.1 Übertragungsmodi 298
9.4.2.2 Datenpakete 299
9.4.3 Geräteklassen 300
9.4.4 Resümee und Ausblick 301
9.5 Übertragungsprotokoll MMC 301
9.6 Single-Wire-Protokoll 302

10 Kontaktlose Datenübertragung 307
10.1 Induktive Kopplung 308
10.2 Energieübertragung 310
10.3 Datenübertragung 311
10.4 Kapazitive Kopplung 312
10.5 Antikollision 312
10.6 Stand der Normung 314
10.7 Close-Coupling-Chipkarten (ISO/IEC 10536) 316
10.7.1 Energieübertragung 318
10.7.2 Induktive Datenübertragung 318
10.7.2.1 Übertragung von der Karte zum Terminal 319
10.7.2.2 Übertragung vom Terminal zur Karte 319
10.7.3 Kapazitive Datenübertragung 320
10.8 Remote-Coupling-Chipkarten 321
10.9 Proximity-Chipkarten (ISO/IEC 14443) 322
10.9.1 Physikalische Eigenschaften 323
10.9.2 Energieübertragung und Signalschnittstelle 324
10.9.3 Signal- und Kommunikationsschnittstelle 324
10.9.4 Kommunikationsinterface Typ A 326
10.9.5 Kommunikationsinterface Typ B 328
10.9.5.1 Datenübertragung vom Terminal zur Karte 328

10.9.5.2 Datenübertragung von der Karte zum Terminal 329
10.9.6 Initialisierung und Antikollision (ISO/IEC 14443-3) 330
10.9.6.1 Initialisierung und Antikollision Typ A 330
10.9.6.2 Initialisierung und Antikollision Typ B 343
10.9.7 Übertragungsprotokoll 360
10.9.7.1 Protokoll-Aktivierung bei Karten vom Typ A 360
10.9.7.2 Halbduplex-Blockprotokoll 367
10.9.7.3 Deaktivierung einer Karte 372
10.9.7.4 Fehlerbehandlung 372
10.10 Vicinity-Chipkarten (ISO/IEC 15693) 372
10.11 Near Field Communication (NFC) 376
10.11.1 Stand der Spezifikation 377
10.11.2 Das NFC-Protokoll 378
10.11.3 NFC-Anwendungen 379
10.11.3.1 Schnelle Information zu Dienstleistungen 379
10.11.3.2 Peer-to-Peer-Informationsaustausch 379
10.11.3.3 Mobiles Bezahlen 379
10.11.3.4 Secure NFC 380
10.12 FeliCa 381
10.13 Mifare 381

11 Kommandos von Chipkarten 383
11.1 Kommandos zur Auswahl von Dateien 387
11.2 Schreib- und Lesekommandos 389
11.3 Suchkommandos 398
11.4 Operationen auf Dateien 400
11.5 Kommandos zur Authentisierung von Personen 402
11.6 Kommandos zur Authentisierung von Geräten 405
11.7 Kommandos für Kryptoalgorithmen 410
11.8 Kommandos zur Verwaltung von Dateien 417
11.9 Kommandos zur Verwaltung von Anwendungen 422
11.10 Kommandos zur Komplettierung 424
11.11 Kommandos zum Test der Hardware 428
11.12 Kommandos für Datenübertragung 431
11.13 Datenbankkommandos – SCQL 433
11.14 Kommandos für elektronische Geldbörsen 436
11.15 Kommandos für Kredit- und Debitkarten 438

11.16 Anwendungsspezifische Kommandos 440
11.17 Ausführungszeiten von Kommandos 440
11.17.1 Formelsammlung zur Abschätzung von Ausführungszeiten 441
11.17.1.1 Kommandoabarbeitung 442
11.17.1.2 Proportionalitätsfaktor für vordefinierte Funktionen . . 443
11.17.1.3 NVM-Operationen 444
11.17.1.4 Datenübertragung 445
11.17.1.5 Rechenbeispiel: Kommando READ BINARY 446
11.17.1.6 Rechenbeispiel: Initialisierung einer Chipkarte 447
11.17.2 Zeitfunktionen typischer Chipkarten-Kommandos 449
11.17.3 Typische Ausführungszeiten von Kommandos 452

12 Dateiverwaltung in Chipkarten 455
12.1 Aufbau von Dateien 456
12.2 Lebenszyklus von Dateien 456
12.3 Dateitypen 458
12.3.1 Master File 458
12.3.2 Dedicated File 458
12.3.3 Application Dedicated File 459
12.3.4 Elementary File 459
12.3.5 Working EF 459
12.3.6 Internal EF 460
12.4 Dateien für eine Anwendung 460
12.5 Dateinamen 461
12.5.1 File Identifier 461
12.5.2 Short File Identifier 463
12.5.3 DF Name 463
12.5.4 Aufbau und Kodierung des Application Identifier 464
12.6 Selektion von Dateien 465
12.6.1 Selektion von Verzeichnissen 466
12.6.2 Explizite Selektion von EFs 466
12.6.3 Implizite Selektion von EFs 466
12.6.4 Selektion durch Pfadangabe 467
12.7 Dateistrukturen von EFs 467
12.7.1 Dateistruktur „transparent“ 468
12.7.2 Dateistruktur „linear fixed“ 469
12.7.3 Dateistruktur „linear variable“ 469

12.7.4 Dateistruktur „cyclic“ 470
12.7.5 Dateistruktur für Datenobjekte 471
12.7.6 Dateistruktur für Datenbanken 471
12.7.7 Dateistruktur „execute“ 471
12.7.8 Dateistruktur für Ablaufsteuerung 472
12.8 Zugriffsbedingungen auf Dateien 472
12.9 Attribute von Dateien 474
12.9.1 Attribut für WORM 474
12.9.2 Attribut für häufiges Schreiben 475
12.9.3 Attribut für EDC-Benutzung 475
12.9.4 Attribut für atomare Schreibzugriffe 475
12.9.5 Attribut für gleichzeitigen Zugriff 475
12.9.6 Attribut für Auswahl der Datenübertragung 476
12.9.7 Attribut für Dateiverschlüsselung 476

13 Chipkarten-Betriebssysteme 477
13.1 Bisherige Entwicklung der Betriebssysteme 479
13.2 Grundlagen und Aufgaben 482
13.3 Kommando-Abarbeitung 483
13.4 Entwurfs- und Implementierungsprinzipien 485
13.5 Komplettierung des Betriebssystems 489
13.5.1 Urlader für das Betriebssystem 493
13.5.2 Hardware-Erkennung 493
13.5.3 Soft- und Hardmaske 494
13.5.4 APIs von Betriebssystemen 494
13.6 Speicherorganisation und -verwaltung 495
13.6.1 Speichermanagement für RAM 496
13.6.2 Speichermanagement für EEPROM 496
13.6.3 Speichermanagement für Flash 499
13.7 Dateiverwaltung 502
13.7.1 Zeiger-orientierte Dateiverwaltung 503
13.7.2 FAT-orientierte Dateiverwaltung 504
13.7.3 Aufteilung des Speichers in Speicherseiten 506
13.7.4 Separierung von DFs 506
13.7.5 Mechanismen der Freispeicherverwaltung 507
13.7.6 Quota-Mechanismus 509
13.7.7 Datenintegrität 510

13.7.8 Anwendungsübergreifende Zugriffe . . . 511
13.8 Ablaufsteuerung . . . 512
13.9 Ressourcenzugriffe nach ISO/IEC 7816-9 . . . 513
13.10 Atomare Abläufe . . . 522
13.11 Multitasking . . . 524
13.12 Performance . . . 526
13.13 Verwaltung von Anwendungen mit Global Platform . . . 527
13.13.1 Security Domains . . . 529
13.13.2 Issuer Security Domain . . . 531
13.13.3 Die Global Platform API . . . 532
13.13.4 Die Global Platform-Kommandos . . . 533
13.14 Nachladbarer Programmkode . . . 534
13.15 Ausführbarer nativer Programmkode . . . 536
13.16 Offene Plattformen . . . 542
13.16.1 ISO/IEC 7816-kompatible Plattformen . . . 543
13.16.2 Java Card . . . 543
13.16.2.1 Die Programmiersprache Java . . . 544
13.16.2.2 Die Eigenschaften von Java . . . 546
13.16.2.3 Java Virtual Machine . . . 547
13.16.2.4 Java Card Virtual Machine . . . 548
13.16.2.5 Speichergrößen bei Javakarten . . . 550
13.16.2.6 Performance bei Javakarten . . . 551
13.16.2.7 Java Card Runtime Environment . . . 552
13.16.2.8 Anwendungstrennung . . . 552
13.16.2.9 Kommandoverteilung und Anwendungsselektion . . . 554
13.16.2.10 Transaktionsintegrität . . . 555
13.16.2.11 Persistente und Transistente Objekte . . . 555
13.16.2.12 Java Card Application Programmers Interface . . . 556
13.16.2.13 Softwareentwicklung für Java auf Chipkarten . . . 560
13.16.2.14 Ausführungsgeschwindigkeit . . . 562
13.16.2.15 Dateisystem . . . 563
13.16.2.16 Kryptografie und Export . . . 564
13.16.2.17 Kommende Generationen der Java-Karte . . . 564
13.16.2.18 Resümee und Zukunft . . . 565
13.16.3 Multos . . . 565
13.16.4 BasicCard . . . 566
13.16.5 Linux . . . 567

13.17 Chipkarten-Betriebssystem „Small-OS“ 568
13.17.1 Programmierung in Pseudokode 568
13.17.2 Designkriterien 570
13.17.3 Zugriff auf Dateien 573
13.17.4 Zugriffe auf interne Geheimnisse (PINs und Schlüssel) 573
13.17.5 Konstanten von Small-OS 576
13.17.6 Variablen von Small-OS 576
13.17.6.1 Variablen von Small-OS im RAM 577
13.17.6.2 Variablen von Small-OS im EEPROM 577
13.17.7 Hauptschleife und Initialisierung von Hardware und Betriebssystem 582
13.17.8 I/O-Manager 582
13.17.9 File Manager 583
13.17.10 Betriebssystemkern 583
13.17.11 Kommandointerpreter 584
13.17.12 Returncode Manager 584
13.17.13 Aufbau des Programmkodes eines Kommandos 588
13.17.14 Befehlssatz 589
13.17.14.1 Kommando SELECT 589
13.17.14.2 Kommando READ BINARY 593
13.17.14.3 Kommando UPDATE BINARY 594
13.17.14.4 Kommando READ RECORD 596
13.17.14.5 Kommando UPDATE RECORD 599
13.17.14.6 Kommando VERIFY 602
13.17.14.7 Kommando INTERNAL AUTHENTICATE 606
13.17.15 Beispiel für eine einfache Anwendung 609

14 Herstellung von Chipkarten 613
14.1 Aufgaben und Rollen bei der Herstellung 614
14.2 Der Chipkarten-Lebenszyklus 615
14.3 Herstellung von Chips und Modulen 618
14.3.1 Chipdesign 618
14.3.2 Entwicklung von Chipkarten-Betriebssystemen 620
14.3.3 Halbleitertechnische Fertigung der Chips 622
14.3.4 Test der Chips auf dem Wafer 624
14.3.5 Sägen der Wafer 626
14.3.6 Fixieren der Chips in Module 628
14.3.7 Bonden der Chips 629

14.3.8 Vergießen der Chips in den Modulen 630
14.3.9 Test der Module 631
14.4 Herstellung von Kartenkörpern 632
14.4.1 Einlagenkarte 633
14.4.2 Mehrlagenkarte 633
14.4.3 Spritzgegossene Kartenkörper 634
14.4.4 Direkte Plug-In-Produktion 636
14.4.5 Kartenkörper mit integrierter Antenne 637
14.4.5.1 Geätzte Antenne 639
14.4.5.2 Gewickelte Antenne 640
14.4.5.3 Verlegte Antenne 640
14.4.5.4 Gedruckte Antenne 641
14.4.5.5 Kontaktierung von Antenne und Chip 642
14.4.6 Druck von Kartenkörpern 643
14.4.6.1 Bogendruck für Kartenkörper 643
14.4.6.2 Einzelkartendruck für Kartenkörper 644
14.4.6.3 Offsetdruck 644
14.4.6.4 Digitaldruck 645
14.4.6.5 Siebdruck 645
14.4.6.6 Thermotransfer- und Thermosublimationsdruck 647
14.4.6.7 Tintenstrahldruck 648
14.4.7 Stanzen der Folien 648
14.4.8 Aufbringung von Kartenelementen auf den Kartenkörper 648
14.5 Zusammenführen von Kartenkörper und Chip 649
14.5.1 Fräsen der Modulaussparung 649
14.5.2 Implantierung der Module 651
14.5.3 Bedrucken von Modulen 655
14.5.4 Stanzen des Plug-Ins 655
14.6 Elektrischer Test der Module 656
14.7 Laden von statischen Daten 658
14.7.1 Komplettierung des Betriebssystems 659
14.7.2 Zusammenarbeit zwischen Kartenhersteller und -herausgeber . . . 660
14.7.3 Initialisierung der Anwendung 662
14.7.4 Optimierter Massendatentransfer in die Chipkarte 664
14.7.5 Beschleunigung des Datentransfers in die Chipkarte 666
14.8 Laden von individuellen Daten 669
14.8.1 Erzeugung von kartenindividuellen Geheimnissen 669

14.8.2 Personalisierung bzw. Individualisierung 670
14.9 Kuvertieren und Versenden 675
14.10 Sonderfertigungen 677
14.10.1 Production-on-Demand 677
14.10.2 Motivkarten 678
14.10.3 Direktausgabe von Chipkarten 680
14.11 Ende der Kartenbenutzung 681
14.11.1 Deaktivierung 681
14.11.2 Recycling 682

15 Qualitätssicherung 685
15.1 Test der Kartenkörper 686
15.1.1 Abnutzung des Magnetstreifens 687
15.1.2 Adhäsion 687
15.1.3 Biegesteifigkeit 687
15.1.4 Chemikalienbeständigkeit 688
15.1.5 Dynamischer Biegetest 688
15.1.6 Dynamischer Torsionstest 689
15.1.7 Elektrischer Widerstand der Kontakte 689
15.1.8 Elektromagnetische Felder 689
15.1.9 Entflammbarkeit 690
15.1.10 Feldwechsel im Magnetstreifen 690
15.1.11 Höhe der Prägung 690
15.1.12 Höhe und Oberflächenprofil des Magnetstreifens 690
15.1.13 Kartenformat und Kartendicke 690
15.1.14 Kartenformat und Kartenwölbung unter Einfluss von Temperatur und Luftfeuchtigkeit 691
15.1.15 Lage der Kontakte 691
15.1.16 Lichtdurchlässigkeit 691
15.1.17 Oberflächenprofil der Kontakte 691
15.1.18 Oberflächenrauheit des Magnetstreifens 692
15.1.19 Röntgenstrahlen 692
15.1.20 Schwingungen 692
15.1.21 Signalamplitude des Magnetstreifens 692
15.1.22 Statische Elektrizität 692
15.1.23 UV-Licht 693
15.1.24 Verbundfestigkeit von Mehrschichtkarten 693

15.1.25 Wölbung 693
15.2 Test der Hardware von Mikrocontrollern 693
15.3 Prüfmethoden für kontaktlose Chipkarten 695
15.3.1 Testverfahren für Proximity-Chipkarten 697
15.3.2 Testverfahren für Vicinity-Chipkarten 698
15.4 Testmethoden für Software 698
15.4.1 Grundlagen des Tests von Chipkarten-Software 700
15.4.1.1 Analyse 700
15.4.1.2 Design 700
15.4.1.3 Realisierung und Test 701
15.4.1.4 Systemintegration 701
15.4.1.5 Wartung 701
15.4.2 Testverfahren und Teststrategien 702
15.4.2.1 Statistische Programmauswertung 702
15.4.2.2 Review 702
15.4.2.3 Blackbox Test 703
15.4.2.4 Whitebox Test 704
15.4.2.5 Greybox Test 707
15.4.3 Dynamische Tests von Betriebssystemen und Anwendungen . . . 707
15.4.4 Vorgehensweise bei Tests 708
15.5 Evaluierung von Hardware und Software 713
15.5.1 Die Common Criteria 715
15.5.2 Die ZKA-Kriterien 717
15.5.3 Weitere Evaluierungsmethoden 719
15.5.4 Resümee 719

16 Sicherheit von Chipkarten 721
16.1 Systematik der Angriffe und Angreifer 723
16.1.1 Einstufung der Angriffe 723
16.1.2 Auswirkungen eines Angriffs und Einstufung der Angreifer 726
16.1.3 Einstufung der Angriffsattraktivität 729
16.2 Historie der Angriffe 730
16.3 Angriffe und Abwehrmaßnahmen während der Entwicklung 734
16.3.1 Entwicklung des Chipkarten-Mikrocontrollers 735
16.3.2 Entwicklung des Chipkarten-Betriebssystems 736
16.4 Angriffe und Abwehrmaßnahmen während der Produktion 738
16.5 Angriffe und Abwehrmaßnahmen während der Kartenbenutzung 739

16.5.1 Angriffe auf die Hardware 740
16.5.2 Angriffe auf das Betriebssystem 771
16.5.3 Angriffe auf die Anwendung 787
16.5.4 Angriffe auf das System 791

17 Chipkarten-Terminals 795
17.1 Mechanische Eigenschaften 799
17.1.1 Kontaktiereinheit mit Schleifkontakten 800
17.1.2 Mechanisch angetriebene Kontaktiereinheit 800
17.1.3 Elektrisch angetriebene Kontaktiereinheit 801
17.1.4 Kartenauswurf 802
17.1.5 Ziehbarkeit 802
17.2 Elektrische Eigenschaften 803
17.3 Benutzerschnittstelle 805
17.4 Anwendungsschnittstelle 805
17.5 Sicherheitstechnik 805

18 Chipkarten im Zahlungsverkehr 809
18.1 Zahlungsverkehr mit Karten 810
18.1.1 Elektronischer Zahlungsverkehr mit Chipkarten 810
18.1.1.1 Kreditkarten 810
18.1.1.2 Debitkarten 811
18.1.1.3 Elektronische Geldbörsen 811
18.1.1.4 Offene und geschlossene Systemarchitekturen 812
18.1.1.5 Zentraler und dezentraler Systemaufbau 813
18.1.2 Elektronisches Geld 815
18.1.2.1 Verarbeitbarkeit 816
18.1.2.2 Übertragbarkeit 816
18.1.2.3 Teilbarkeit 816
18.1.2.4 Dezentral 816
18.1.2.5 Systemüberwachung 816
18.1.2.6 Sicherheit 817
18.1.2.7 Anonymität 817
18.1.2.8 Gesetzlicher Rahmen und Wertbeständigkeit 817
18.1.3 Grundsätzliche Möglichkeiten der Systemstruktur 818
18.1.3.1 Hintergrundsystem 818
18.1.3.2 Netzwerk 818

18.1.3.3 Terminals . . . 818
18.1.3.4 Chipkarten . . . 819
18.2 Vorbezahlte Speicherkarten . . . 820
18.3 Elektronische Geldbörsen . . . 822
18.3.1 Branchenübergreifende elektronische Geldbörse nach EN 1546 . . . 823
18.3.1.1 Datenelemente . . . 826
18.3.1.2 Dateien . . . 829
18.3.1.3 Kommandos . . . 829
18.3.1.4 Zustände . . . 830
18.3.1.5 Kryptografische Algorithmen . . . 831
18.3.1.6 Allgemeine Abläufe . . . 831
18.3.1.7 Ablauf beim Aufladen . . . 833
18.3.1.8 Ablauf beim Bezahlen . . . 834
18.3.2 CEPS . . . 839
18.3.3 Proton . . . 839
18.4 EMV-Anwendung . . . 841
18.4.1 Dateien und Datenelemente . . . 842
18.4.2 Kommandos . . . 842
18.4.3 Kryptografie . . . 843
18.4.4 System und Transaktionsabläufe . . . 844
18.4.5 Zukünftige Entwicklungen . . . 846
18.5 PayPass und payWave . . . 847
18.6 Das ec-System in Deutschland . . . 848
18.6.1 Funktionen für den Benutzer . . . 849
18.6.2 Gesamtsystem im Überblick . . . 850
18.6.3 Girocard mit Chip . . . 851
18.6.4 Zusatzanwendungen . . . 853
18.6.5 Resümee . . . 853

19 Chipkarten in der Telekommunikation . . . 855
19.1 Öffentliches Kartentelefon in Deutschland . . . 855
19.2 Telekommunikation . . . 858
19.3 Überblick zu Mobilfunksystemen . . . 861
19.3.1 Vielfachzugriffsverfahren . . . 862
19.3.1.1 Frequenzvielfachzugriff . . . 862
19.3.1.2 Zeitvielfachzugriff . . . 863
19.3.1.3 Kodevielfachzugriff . . . 864

19.3.1.4 Raumvielfachzugriff 865
19.3.2 Zellulartechnik 866
19.3.3 Zelltypen 868
19.3.4 Trägerdienste 869
19.4 Das GSM-System 869
19.4.1 Die Spezifikationen 871
19.4.2 Systemarchitektur und Komponenten 873
19.4.3 Wichtige Datenelemente 877
19.4.3.1 Kodierung alphanumerischer Zeichen 877
19.4.3.2 Diensteerkennungen 877
19.4.3.3 Festrufnummern 878
19.4.3.4 ICCID 878
19.4.3.5 IMEI 878
19.4.3.6 IMSI 878
19.4.3.7 Ki und Kc 878
19.4.3.8 Kurznachrichten 878
19.4.3.9 Kurzrufnummern 879
19.4.3.10 LAI 879
19.4.3.11 MSISDN 879
19.4.3.12 TMSI 879
19.4.4 Die SIM 879
19.4.4.1 Kommandos einer SIM 882
19.4.4.2 Dateien einer SIM 884
19.4.4.3 Beispiel für eine typische Kommandosequenz 896
19.4.4.4 Authentisierung der SIM 897
19.4.4.5 Abläufe beim Ein- und Ausschalten des Mobiltelefons 900
19.4.4.6 SIM Application Toolkit 904
19.4.4.7 Over The Air (OTA)-Kommunikation 910
19.4.4.8 Remote File Management 912
19.4.4.9 Remote Applet Management 914
19.4.4.10 Dual-IMSI 914
19.4.4.11 Realisierung einer Homezone 916
19.4.4.12 Funktionsweise des SIM-Lock 917
19.4.4.13 Funktionsweise von Prepaid-Lösungen 917
19.4.5 Zukünftige Entwicklungen 920
19.5 Das UMTS-System 920
19.5.1 Zukünftige Entwicklungen 926

19.6 Die WIM 927
19.7 Mikrobrowser 930

20 Chipkarten im Gesundheitswesen 935
20.1 Krankenversichertenkarte in Deutschland 935
20.2 Elektronische Gesundheitskarte in Deutschland 939
20.2.1 Die Kartenarten 940
20.2.2 Die Anwendungen auf der eGK 941
20.2.3 Das elektronische Rezept 942
20.2.4 Resümee und Ausblick 943

21 Chipkarten im Transportwesen 945
21.1 Elektronische Fahrkarte 945
21.1.1 Systemarchitektur 946
21.1.2 Octopus-Karte 948
21.1.3 Erfassung der Fahrt 949
21.1.4 Typische Transaktionen 951
21.1.4.1 Identifikation und Authentisierung 951
21.1.4.2 Check-in-Vorgang 952
21.1.4.3 Check-out-Vorgang 953
21.1.5 Zusatzanwendungen 953
21.1.6 Evolution der elektronischen Fahrkarten 954
21.2 Skipass 954
21.2.1 Systemarchitektur 956
21.2.2 Skikarte 957
21.2.3 Typische Abläufe 960
21.2.3.1 Identifikation und Authentisierung 960
21.2.3.2 Lesen von Daten 961
21.2.3.3 Schreiben von Daten 963
21.2.4 Zukünftige Entwicklungen 964
21.3 Tachosmart 965
21.4 Elektronische Mautsysteme 966

22 Chipkarten für Identifikation und Pässe 971
22.1 Personalausweis FINEID 971
22.2 Reisepass nach ICAO 972

23 Chipkarten für IT-Sicherheit 977

23.1 Digitale Signatur 977
23.1.1 Die normativen Rahmenbedingungen 978
23.1.2 Die gesetzlichen Rahmenbedingungen in Deutschland 978
23.1.3 Der Systemaufbau 981
23.1.4 Kartenausgabe 981
23.1.5 Signieren und Verifizieren von Dokumenten 982
23.1.6 Das Trustcenter 984
23.1.7 Die Signaturkarte 984
23.1.8 Resümee und Ausblick 988
23.2 Signaturanwendung nach PKCS #15 988
23.3 Smart Card Web Server 992

24 Gestaltung von Anwendungen 995
24.1 Allgemeine Hinweise und Kennzahlen 995
24.1.1 Mikrocontroller 995
24.1.1.1 Produktion 995
24.1.1.2 Lebensdauer 996
24.1.1.3 Datenübertragung 998
24.1.1.4 Ausführungsgeschwindigkeiten von Algorithmen . . . 998
24.1.2 Anwendungen 998
24.1.2.1 Schlüsselmanagement 998
24.1.2.2 Daten 999
24.1.2.3 Datenaustausch 1000
24.1.3 System 1001
24.1.3.1 Sicherheit 1001
24.1.3.2 Benutzerschnittstelle 1001
24.1.3.3 Konzeption 1001
24.1.4 Normenkonformität 1002
24.2 Hilfsmittel zur Anwendungserstellung 1003
24.3 Analyse einer unbekannten Chipkarte 1005

25 Anhang 1007
25.1 Glossar 1007
25.2 Weiterführende Literatur 1072
25.3 Literaturverzeichnis 1073
25.4 Normen- und Spezifikationsverzeichnis 1079
25.5 Web-Adressen 1097

Stichwortverzeichnis **1101**