

CARL HANSER VERLAG

Wolfgang Rankl, Wolfgang Effing

**Handbuch der Chipkarten**  
Aufbau - Funktionsweise - Einsatz von Smart Cards

3-446-22036-4

[www.hanser.de](http://www.hanser.de)

# Inhaltsverzeichnis

<b>Vorwort zur vierten Auflage</b> . . . . .	V
<b>Inhalt im Überblick</b> . . . . .	VII
<b>Inhaltsverzeichnis</b> . . . . .	IX
<b>Symbole/Notationen</b> . . . . .	XVII
<b>Programmcode</b> . . . . .	XVIII
<b>Abkürzungen</b> . . . . .	XIX
<b>1 Einleitung</b> . . . . .	1
1.1 Geschichte der Chipkarten . . . . .	2
1.2 Anwendungsgebiete . . . . .	6
1.2.1 Speicherkarten . . . . .	7
1.2.2 Mikroprozessorkarten . . . . .	7
1.2.3 Kontaktlose Karten . . . . .	9
1.3 Normung . . . . .	10
<b>2 Arten von Karten</b> . . . . .	17
2.1 Hochgeprägte Karten . . . . .	17
2.2 Magnetstreifenkarten . . . . .	18
2.3 Chipkarten . . . . .	20
2.3.1 Speicherkarten . . . . .	21
2.3.2 Mikroprozessorkarten . . . . .	22
2.3.3 Kontaktlose Chipkarten . . . . .	23
2.4 Optische Speicherkarten . . . . .	26
<b>3 Physikalische und elektrische Eigenschaften</b> . . . . .	29
3.1 Physikalische Eigenschaften . . . . .	29
3.1.1 Formate . . . . .	30
3.1.2 Kartenelemente und Sicherheitsmerkmale . . . . .	34
3.2 Kartenkörper . . . . .	40
3.2.1 Kartenmaterialien . . . . .	42
3.2.2 Chipmodule . . . . .	44
3.2.2.1 Elektrische Kontaktierung zwischen Chip und Modul . . . . .	45
3.2.2.2 TAB-Modul . . . . .	47
3.2.2.3 Chip-on-Flex-Modul . . . . .	48
3.2.2.4 Lead-Frame-Modul . . . . .	50
3.2.2.5 Chip-On-Surface-Verfahren . . . . .	51
3.3 Elektrische Eigenschaften . . . . .	53
3.3.1 Beschaltung . . . . .	56
3.3.2 Versorgungsspannung . . . . .	57
3.3.3 Versorgungsstrom . . . . .	59
3.3.4 Taktversorgung . . . . .	61

3.3.5	Datenübertragung . . . . .	62
3.3.6	An-/Abschaltsequenz . . . . .	63
3.4	Mikrocontroller für Chipkarten. . . . .	64
3.4.1	Prozessortypen . . . . .	67
3.4.2	Speicherarten . . . . .	71
3.4.3	Zusatzhardware . . . . .	81
3.5	Kontaktbehaftete Karten . . . . .	91
3.6	Kontaktlose Karten . . . . .	93
3.6.1	ISO/IEC 10536 – Close Coupling Cards . . . . .	101
3.6.1.1	Induktive Datenübertragung . . . . .	103
3.6.1.2	Kapazitive Datenübertragung . . . . .	105
3.6.2	Remote-Coupling-Karten . . . . .	106
3.6.3	Proximity Integrated Circuit(s) Cards nach ISO/IEC 14 443 . .	107
3.6.3.1	Kommunikationsinterface Typ A . . . . .	109
3.6.3.2	Kommunikationsinterface Typ B . . . . .	111
3.6.3.3	Initialisierung und Antikollision (ISO/IEC 14 443-3). . . . .	112
3.6.3.4	Übertragungsprotokoll (ISO/IEC 14443-4). . . . .	139
3.6.4	Vicinity Integrated Circuits Cards nach ISO/IEC 15 693 . . . . .	151
3.6.5	Prüfmethoden für kontaktlose Chipkarten. . . . .	151
3.6.5.1	Part 4: Testverfahren für Close-coupling-Chipkarten . . . . .	152
3.6.5.2	Part 6: Testverfahren für Proximity-coupling-Chipkarten . . . . .	152
3.6.5.3	Part 7: Testverfahren für Vicinity-coupling-Chipkarten . . . . .	152
<b>4</b>	<b>Informationstechnische Grundlagen . . . . .</b>	<b>153</b>
4.1	Strukturierung von Daten . . . . .	154
4.2	Codierung alphanumerischer Daten. . . . .	160
4.2.1	7 Bit Code . . . . .	160
4.2.2	8 Bit Code . . . . .	160
4.2.3	16 Bit Code (Unicode) . . . . .	161
4.2.4	32 Bit Code (UCS) . . . . .	162
4.3	SDL-Symbolik . . . . .	163
4.4	Zustandsautomaten . . . . .	164
4.4.1	Grundlagen zur Automatentheorie . . . . .	164
4.4.2	Praktische Anwendung . . . . .	166
4.5	Fehlererkennungs- und Fehlerkorrekturcodes. . . . .	169
4.5.1	XOR-Prüfsummen . . . . .	170
4.5.2	CRC-Prüfsummen . . . . .	171
4.5.3	Reed-Solomon-Codes . . . . .	173
4.5.4	Fehlerkorrektur . . . . .	174
4.6	Datenkompression . . . . .	176
4.7	Kryptologie . . . . .	177
4.7.1	Symmetrische Kryptoalgorithmen . . . . .	183
4.7.2	Asymmetrische Kryptoalgorithmen . . . . .	191

---

4.7.3	Padding	201
4.7.4	Message Authentication Code/Cryptographic Checksum	202
4.8	Schlüsselmanagement	203
4.8.1	Abgeleitete Schlüssel	204
4.8.2	Schlüsseldiversifizierung	204
4.8.3	Schlüsselversionen	204
4.8.4	Dynamische Schlüssel	205
4.8.5	Schlüsselinformationen	207
4.8.6	Beispiel für Schlüsselmanagement	208
4.9	Hash-Funktionen	210
4.10	Zufallszahlen	212
4.10.1	Erzeugung von Zufallszahlen	213
4.10.2	Prüfung von Zufallszahlen	216
4.11	Authentisierung	219
4.11.1	Einseitige symmetrische Authentisierung	221
4.11.2	Gegenseitige symmetrische Authentisierung	223
4.11.3	Statische asymmetrische Authentisierung	225
4.11.4	Dynamische asymmetrische Authentisierung	227
4.12	Digitale Signatur	229
4.13	Zertifikate	232
<b>5</b>	<b>Chipkarten-Betriebssysteme</b>	<b>235</b>
5.1	Bisherige Entwicklung der Betriebssysteme	237
5.2	Grundlagen	240
5.3	Entwurfs- und Implementierungsprinzipien	245
5.4	Komplettierung	248
5.5	Speicherorganisation	253
5.6	Dateien in der Chipkarte	256
5.6.1	Dateitypen	258
5.6.2	Dateinamen	261
5.6.3	Selektion von Dateien	265
5.6.4	Dateistrukturen von EFs	267
5.6.5	Zugriffsbedingungen auf Dateien	271
5.6.6	Attribute von Dateien	274
5.7	Dateiverwaltung	276
5.8	Ablaufsteuerung	283
5.9	Ressourcenzugriffe nach ISO/IEC 7816-9	285
5.10	Atomare Abläufe	293
5.11	Open Platform	295
5.12	Nachladbarer Programmcode	299
5.13	Ausführbarer nativer Programmcode	302
5.14	Offene Plattformen	308
5.14.1	Java Card	308
5.14.2	Multos	328
5.14.3	Basic Card	329

5.14.4	Windows for Smart Cards . . . . .	330
5.14.5	Linux. . . . .	332
5.15	Chipkarten-Betriebssystem „Small-OS“ . . . . .	332
<b>6</b>	<b>Datenübertragung zur Chipkarte. . . . .</b>	<b>377</b>
6.1	Physikalische Übertragungsschicht . . . . .	379
6.2	Answer to Reset – ATR . . . . .	384
6.3	Protocol Parameter Selection – PPS . . . . .	399
6.4	Übertragungsprotokolle . . . . .	403
6.4.1	Synchrone Datenübertragung. . . . .	404
6.4.1.1	Protokoll für Telefonchips. . . . .	405
6.4.1.2	I <sup>2</sup> C-Bus . . . . .	407
6.4.2	Übertragungsprotokoll T = 0 . . . . .	410
6.4.3	Übertragungsprotokoll T = 1 . . . . .	416
6.4.3.1	Blockaufbau. . . . .	417
6.4.3.2	Sendefolge-/Empfangsfolgezähler ( <i>send sequence counter/receive sequence counter</i> ) . .	420
6.4.3.3	Wartezeiten . . . . .	420
6.4.3.4	Mechanismen des Übertragungsprotokolls . . . . .	423
6.4.3.4	Beispiel für die Datenübertragung mit T = 1 . . . . .	426
6.4.3.5	Unterschiede zwischen T = 1 nach ISO/IEC und T = 1 nach EMV . . . . .	427
6.4.4	Übertragungsprotokoll T = 14 (Deutschland) . . . . .	427
6.4.5	Übertragungsprotokoll USB . . . . .	428
6.4.6	Vergleich der asynchronen Übertragungsprotokolle . . . . .	428
6.5	Struktur der Nachrichten-APDUs . . . . .	429
6.5.1	Struktur der Kommando-APDUs . . . . .	430
6.5.2	Struktur der Antwort-APDUs . . . . .	432
6.6	Sicherung der Datenübertragung. . . . .	433
6.6.1	Das Authentic-Verfahren . . . . .	436
6.6.2	Das Combined-Verfahren . . . . .	438
6.6.3	Sendefolgezähler ( <i>send sequence counter</i> ) . . . . .	440
6.7	Logische Kanäle ( <i>logical channels</i> ) . . . . .	441
<b>7</b>	<b>Kommandos von Chipkarten . . . . .</b>	<b>443</b>
7.1	Kommandos zur Auswahl von Dateien . . . . .	447
7.2	Schreib- und Lesekommandos . . . . .	450
7.3	Suchkommandos . . . . .	457
7.4	Operationen auf Dateien . . . . .	459
7.5	Identifizierungskommandos . . . . .	461
7.6	Authentisierungskommandos . . . . .	465
7.7	Kommandos für kryptografische Algorithmen . . . . .	469
7.8	Kommandos zur Verwaltung von Dateien . . . . .	475
7.9	Kommandos zur Verwaltung von Applets . . . . .	482
7.10	Kommandos zur Komplettierung des Betriebssystems . . . . .	482

---

7.11	Kommandos zum Test der Hardware . . . . .	486
7.12	Kommandos für Datenübertragung . . . . .	489
7.13	Datenbankkommandos – SCQL. . . . .	491
7.14	Kommandos für elektronische Geldbörsen . . . . .	494
7.15	Kommandos für Kredit- und Debitkarten . . . . .	497
7.16	Anwendungsspezifische Kommandos . . . . .	498
<b>8</b>	<b>Sicherheitstechnik. . . . .</b>	<b>501</b>
8.1	Benutzeridentifizierung. . . . .	501
8.1.1	Prüfung einer Geheimzahl . . . . .	503
8.1.2	Biometrische Verfahren . . . . .	509
8.1.2.1	Grundlagen . . . . .	509
8.1.2.2	Physiologische Merkmale. . . . .	515
8.1.2.3	Verhaltensbasierte Merkmale . . . . .	517
8.2	Sicherheit einer Chipkarte . . . . .	521
8.2.1	Systematik der Angriffe und Angreifer . . . . .	522
8.2.2	Angriffe und Abwehrmaßnahmen während der Entwicklung . . . . .	529
8.2.2.1	Entwicklung des Chipkarten-Mikrocontrollers. . . . .	529
8.2.2.2	Entwicklung des Chipkarten-Betriebssystems . . . . .	530
8.2.3	Angriffe und Abwehrmaßnahmen während der Produktion . . . . .	532
8.2.4	Angriffe und Abwehrmaßnahmen während der Karten- benutzung . . . . .	533
8.2.4.1	Angriffe auf der physikalischen Ebene . . . . .	535
8.2.4.2	Angriffe auf der logischen Ebene . . . . .	554
<b>9</b>	<b>Qualitätssicherung und Test . . . . .</b>	<b>577</b>
9.1	Test der Kartenkörper . . . . .	578
9.2	Test der Hardware von Mikrocontrollern . . . . .	584
9.3	Evaluierung und Test von Software . . . . .	585
9.3.1	Evaluierung. . . . .	586
9.3.2	Testmethoden für Software. . . . .	593
9.3.2.1	Grundlagen des Tests von Chipkarten-Software. . . . .	594
9.3.2.2	Testverfahren und Teststrategien. . . . .	596
9.3.3	Dynamische Tests von Betriebssystemen und Anwendungen . . . . .	601
<b>10</b>	<b>Lebenszyklus einer Chipkarte. . . . .</b>	<b>607</b>
10.1	Die 5 Phasen des Chipkarten-Lebenszyklus . . . . .	608
10.2	Phase 1 des Lebenszyklus im Detail. . . . .	610
10.2.1	Erstellung des Betriebssystems und Herstellung der Chips . . . . .	610
10.2.2	Herstellung der Kartenkörper ohne integrierte Spule . . . . .	622
10.2.3	Herstellung von Kartenkörpern mit integrierter Spule. . . . .	630
10.2.4	Zusammenführen von Kartenkörper und Chip . . . . .	635
10.3	Phase 2 des Lebenszyklus im Detail. . . . .	638
10.4	Phase 3 des Lebenszyklus im Detail. . . . .	644
10.5	Phase 4 des Lebenszyklus im Detail. . . . .	656
10.6	Phase 5 des Lebenszyklus im Detail. . . . .	658

<b>11 Chipkarten-Terminals</b> .....	661
11.1 Mechanische Eigenschaften .....	666
11.2 Elektrische Eigenschaften .....	670
11.3 Sicherheitstechnik .....	671
11.4 Anbindung von Terminals an übergeordnete Systeme. ....	674
11.4.1 PC/SC .....	674
11.4.2 OCF .....	678
11.4.3 MKT .....	678
11.4.4 MUSCLE .....	679
<b>12 Chipkarten im Zahlungsverkehr</b> .....	681
12.1 Zahlungsverkehr mit Karten .....	682
12.1.1 Elektronischer Zahlungsverkehr mit Chipkarten .....	682
12.1.2 Elektronisches Geld .....	687
12.1.3 Grundsätzliche Möglichkeiten der Systemstruktur .....	689
12.2 Vorbezahlte Speicherkarten .....	692
12.3 Elektronische Geldbörsen .....	693
12.3.1 CEN-Norm EN 1546 .....	694
12.3.2 CEPS ( <i>common electronic purse specifications</i> ) .....	709
12.3.3 Proton .....	710
12.3.4 Das Mondex-System .....	711
12.4 EMV-Anwendung .....	716
12.5 Das ec-System in Deutschland .....	722
<b>13 Chipkarten in der Telekommunikation</b> .....	731
13.1 Überblick zu Mobilfunksystemen .....	735
13.1.1 Vielfachzugriffsverfahren ( <i>multiple access</i> ) .....	735
13.1.2 Zellulartechnik .....	739
13.1.3 Zelltypen .....	741
13.1.4 Trägerdienste ( <i>bearer services</i> ) .....	741
13.2 Das GSM-System .....	743
13.2.1 Die Spezifikationen .....	746
13.2.2 Systemarchitektur und Komponenten .....	748
13.2.3 Wichtige Datenelemente .....	751
13.2.4 Die SIM ( <i>Subscriber Identity Module</i> ) .....	754
13.2.5 GPRS ( <i>General Packet Radio Service</i> ) .....	794
13.2.6 Zukünftige Entwicklung .....	795
13.3 Das UMTS-System .....	796
13.4 Mikrobrowser .....	805
13.5 Die WIM ( <i>Wireless Identification Module</i> ) .....	808
13.6 Öffentliches Kartentelefon in Deutschland .....	814
<b>14 Beispielhafte Anwendungen</b> .....	819
14.1 Kontaktlose Speicherkarte für Flugverkehr .....	819
14.2 Krankenversichertenkarte .....	822

---

14.3	Elektronische Mautsysteme . . . . .	827
14.4	Digitale Signatur . . . . .	831
14.5	Signaturanwendung nach PKCS #15 . . . . .	841
14.6	Personalausweis FINEID . . . . .	848
14.7	Tachosmart . . . . .	848
<b>15</b>	<b>Design von Anwendungen . . . . .</b>	<b>851</b>
15.1	Allgemeine Hinweise und Kennzahlen . . . . .	852
15.1.1	Mikrocontroller . . . . .	852
15.1.2	Anwendungen . . . . .	854
15.1.3	System . . . . .	857
15.1.4	Normenkonformität . . . . .	858
15.2	Formelsammlung zur Abschätzung von Ausführungszeiten . . . . .	859
15.3	Zeitfunktionen typischer Chipkarten-Kommandos . . . . .	867
15.4	Typische Ausführungszeiten von Kommandos . . . . .	870
15.5	Hilfsmittel zur Anwendungsgenerierung . . . . .	872
15.6	Analyse einer unbekanntes Chipkarte . . . . .	876
15.7	Vorgehensmodelle und Prozessreifegrad . . . . .	879
15.7.1	Vorgehensmodelle ( <i>life cycle models</i> ) . . . . .	883
15.7.1.1	Wasserfall-Modell . . . . .	884
15.7.1.2	V-Modell . . . . .	885
15.7.1.3	Prototypen-Modell . . . . .	886
15.7.1.4	Evolutionäres-/Inkrementelles Modell . . . . .	888
15.7.1.5	Spiralmodell . . . . .	889
15.7.2	Prozessreifegrad ( <i>process maturity</i> ) . . . . .	890
15.8	Ablauf eines Chipkarten-Projekts . . . . .	893
15.9	Beispiele für die Konzeption von Chipkarten-Anwendungen . . . . .	894
15.9.1	Börse für Spielautomat . . . . .	896
15.9.2	Zugangskontrolle . . . . .	899
15.9.3	Prüfung auf Echtheit eines Terminals . . . . .	902
<b>16</b>	<b>Anhang . . . . .</b>	<b>905</b>
16.1	Glossar . . . . .	905
16.2	Übersetzung von Fachwörtern . . . . .	955
16.2.1	Übersetzungsliste Deutsch – Englisch . . . . .	956
16.2.2	Übersetzungsliste Englisch – Deutsch . . . . .	963
16.3	Weiterführende Literatur . . . . .	970
16.4	Literatur . . . . .	970
16.5	Kommentiertes Normen- und Spezifikationsverzeichnis . . . . .	977
16.6	Kodierung von Datenobjekten . . . . .	1002
16.6.1	Datenobjekte nach ISO/IEC 7816-4 . . . . .	1002
16.6.2	Datenobjekte nach ISO/IEC 7816-6 . . . . .	1003
16.6.3	Datenobjekt für Chiphersteller nach ISO/IEC 7816-6 . . . . .	1004
16.7	Registrierungsstellen für RID . . . . .	1004
16.8	Ausgewählte RIDs . . . . .	1005



---

16.9	Veranstaltungen . . . . .	1005
16.10	World-Wide-Web-Adressen . . . . .	1006
16.11	Kennwerte und Tabellen . . . . .	1019
16.11.1	Zeitbereich für den ATR . . . . .	1019
16.11.2	Umrechnungstabelle für Datenelemente des ATR . . . . .	1019
16.11.3	Tabelle zur Ermittlung der Übertragungsgeschwindigkeit . . . . .	1020
16.11.4	Tabelle mit Abtastzeitpunkten . . . . .	1021
16.11.5	Tabelle der wichtigsten Chipkarten-Kommandos . . . . .	1022
16.11.6	Übersicht über die verwendeten Instruction-Bytes . . . . .	1027
16.11.7	Codierung von Chipkarten-Kommandos . . . . .	1028
16.11.8	Chipkarten-Returncodes . . . . .	1031
16.11.9	Ausgewählte Chips für Speicherkarten . . . . .	1033
16.11.10	Ausgewählte Mikrocontroller für Chipkarten . . . . .	1035
	Sachverzeichnis . . . . .	1041