WOLFGANG RANKL | WOLFGANG EFFING

Smart Card Handbook

FOURTH EDITION

WILEY

Contents

Preface to the Fourth Edition xxiii
Symbols and Notation xxv
Abbreviations xxix

1 Introduction 1
1.1 The history of smart cards 2
1.2 Card types and applications 7
1.2.1 Memory cards 8
1.2.2 Processor cards 8
1.2.3 Contactless cards 9
1.3 Standardization 10

2 Card Types 15
2.1 Embossed cards 15
2.2 Magnetic-stripe cards 16
2.3 Smart cards 18
2.3.1 Memory cards 20
2.3.2 Contactless memory cards 20
2.3.3 Processor cards 21
2.3.4 Contactless processor cards 23
2.3.5 Multi-megabyte cards 24
2.3.6 Security tokens 25
2.4 Optical memory cards 25

3 Physical Properties 29
3.1 Card formats 29
3.2 Contact field 36
3.3 Card body 38
3.4 Card materials 39
3.5 Card components and security features 42
3.5.1 Guilloche patterns 42
3.5.2 Signature panel 44
3.5.3 Microtext 44
3.5.4 Ultraviolet text 44
3.5.5 Barcode 44
3.5.6 Hologram 45
3.5.7 Kinegram 45
3.5.8 Multiple Laser Image (MLI) 46
3.5.9 Embossing 46
3.5.10 Laser engraving 47
3.5.11 Scratch field 47
3.5.12 Thermochrome display 48
3.5.13 Moduliertes Merkmal (modulated feature) method 48
3.5.14 Security features 49
3.6 Chip modules 50
3.6.1 Electrical connections between the chip and the module 51
3.6.2 TAB modules 53
3.6.3 Chip-on-flex modules 54
3.6.4 Lead-frame modules 57
3.6.5 Special modules 59

4 Electrical Properties 61
4.1 Electrical connections 62
4.2 Supply voltage 62
4.3 Supply current 65
4.4 Clock supply 69
4.5 Data transmission with T = 0 or T = 1 69
4.6 Activation and deactivation sequences 70

5 Smart Card Microcontrollers 73
5.1 Semiconductor technology 76
5.2 Processor types 79
5.3 Memory types 82
5.3.1 ROM (read-only memory) 84
5.3.2 EPROM (erasable read-only memory) 85
5.3.3 EEPROM (electrically erasable read-only memory) 85
5.3.4 Flash memory 90
5.3.5 RAM (random-access memory) 92
5.3.6 FRAM (ferroelectric random-access memory) 92
5.4 Supplementary hardware 93
5.4.1 Communication with T = 0 or T = 1 93

5.4.2 Communication with USB 94
5.4.3 Communication with MMC 95
5.4.4 Communication with SWP 95
5.4.5 Communication with I^2C 96
5.4.6 Timer 96
5.4.7 CRC (cyclic redundancy check) calculation unit 97
5.4.8 Random number generator (RNG) 97
5.4.9 Clock generation and clock multiplication 98
5.4.10 DMA (direct memory access) 99
5.4.11 Memory management unit (MMU) 100
5.4.12 Java accelerator 101
5.4.13 Coprocessor for symmetric cryptographic algorithms 102
5.4.14 Coprocessor for asymmetric cryptographic algorithms 103
5.4.15 Error detection and correction for nonvolatile memory 103
5.4.16 Mass memory interface 104
5.4.17 Multichip module 105
5.4.18 Vertical system integration (VSI) 106
5.5 Extended temperature range 107

6 Information Technology Foundations 109
6.1 Data structures 109
6.2 Encoding alphanumeric data 115
6.2.1 Seven-bit code (ASCII) 115
6.2.2 Eight-bit code (PC ASCII) 115
6.2.3 Sixteen-bit code (Unicode) 116
6.2.4 Thirty-two-bit code (UCS) 116
6.3 SDL notation 117
6.4 State machines 118
6.4.1 Basic theory of state machines 118
6.4.2 Practical applications 120
6.5 Error detection and correction codes 122
6.5.1 XOR checksums 124
6.5.2 CRC checksums 125
6.5.3 Reed–Solomon codes 127
6.5.4 Error correction codes 128
6.6 Data compression 129

7 Security Foundations 133
7.1 Cryptology 133
7.1.1 Symmetric cryptographic algorithms 138
7.1.1.1 DES algorithm 138
7.1.1.2 AES algorithm 140
7.1.1.3 IDEA algorithm 141
7.1.1.4 COMP128 algorithms 142
7.1.1.5 Milenage algorithm 142
7.1.1.6 Operating modes of block encryption algorithms 142
7.1.1.7 Multiple encryption 144

7.1.2 Asymmetric cryptographic algorithms 145
7.1.2.1 RSA algorithm 146
7.1.2.2 Generating RSA keys 148
7.1.2.3 DSS algorithm 151
7.1.2.4 Elliptic curves as asymmetric cryptographic algorithms 152
7.1.3 Padding 154
7.1.4 Message authentication code and cryptographic checksum 155
7.2 Hash functions 156
7.3 Random numbers 159
7.3.1 Generating random numbers 160
7.3.2 Testing random numbers 163
7.4 Authentication 166
7.4.1 Unilateral symmetric authentication 168
7.4.2 Mutual symmetric authentication 169
7.4.3 Static asymmetric authentication 170
7.4.4 Dynamic asymmetric authentication 172
7.5 Digital signatures 174
7.6 Certificates 178
7.7 Key management 180
7.7.1 Derived keys 181
7.7.2 Key diversification 182
7.7.3 Key versions 182
7.7.4 Dynamic keys 182
7.7.4.1 Generation with a symmetric cryptographic algorithm 182
7.7.4.2 Generation with an asymmetric cryptographic algorithm 183
7.7.5 Key data 183
7.7.6 Key management example 185
7.8 Identification of persons 187
7.8.1 Knowledge-based identification 188
7.8.2 Testing a secret number 188
7.8.3 The probability of guessing a PIN 190
7.8.4 Generating PIN codes 191
7.8.5 Verifying that a terminal is genuine 192
7.8.6 Biometric methods 194

8 Communication with Smart Cards 201
8.1 Answer to reset (ATR) 203
8.1.1 The initial character 206
8.1.2 The format character 207
8.1.3 The interface characters 207
8.1.3.1 Global interface character TA_1 208
8.1.3.2 Global interface character TA_i 209
8.1.3.3 Global interface character TC_1 209
8.1.3.4 Specific interface character TC_2 210
8.1.3.5 Specific interface character TA_i ($i > 2$) 210
8.1.3.6 Specific interface character TB_i ($i > 2$) 210

8.1.3.7 Specific interface character TC_i (i > 2) 211
8.1.3.8 Global interface character TA_2 211
8.1.4 The historical characters 211
8.1.5 The check character 214
8.1.6 Practical examples of ATRs 214
8.2 Protocol Parameter Selection (PPS) 217
8.3 Message structure: APDUS 221
8.3.1 Command APDU structure 221
8.3.2 Response APDU structure 224
8.4 Secure Data Transmission 225
8.4.1 Data objects for plaintext 227
8.4.2 Data objects for security mechanisms 227
8.4.3 Data objects for auxiliary functions 228
8.4.4 The authentic mode procedure 228
8.4.5 The combined mode procedure 230
8.4.6 Send sequence counter 231
8.5 Logical channels 233
8.6 Logical protocols 234
8.6.1 TCP/IP protocol 234
8.6.2 HTTP protocol 235
8.6.3 Bearer Independent Protocol (BIP) 236
8.7 Connecting terminals to higher-level systems 237
8.7.1 PC/SC 237
8.7.1.1 ICC-aware application 239
8.7.1.2 Service provider 239
8.7.1.3 ICC resource manager 240
8.7.1.4 IFD handler 240
8.7.1.5 IFD (interface device) 240
8.7.1.6 ICC (integrated chip card) 241
8.7.2 OCF 241
8.7.3 MKT 241
8.7.4 MUSCLE 242

9 Data Transmission with Contact Cards 243
9.1 Physical transmission layer 243
9.2 Memory card protocols 248
9.2.1 Telephone chip protocol 249
9.2.1.1 Resetting the address pointer 249
9.2.1.2 Incrementing the address pointer and reading data 250
9.2.1.3 Writing to an address 250
9.2.1.4 Erasing bytes 250
9.2.2 I^2C bus 251
9.2.2.1 Reading from an address 252
9.2.2.2 Writing to an address 253
9.3 ISO transmission protocols 254
9.3.1 The T = 0 transmission protocol 255
9.3.2 The T = 1 transmission protocol 260

9.3.2.1 Block structure 261
9.3.2.2 Send/receive sequence counter 264
9.3.2.3 Waiting times 265
9.3.2.4 Transmission protocol mechanisms 267
9.3.2.5 Example of data transmission with the T = 1 protocol 270
9.3.3 Comparison of the T = 0 and T = 1 transmission protocols 270
9.3.4 The T = 14 transmission protocol (Germany) 271
9.4 USB transmission protocol 272
9.4.1 Electrical connection 273
9.4.2 Logical connection 274
9.4.2.1 Transfer modes 275
9.4.2.2 Data packets 275
9.4.3 Device classes 276
9.4.4 Summary and prospects 277
9.5 MMC transmission protocol 277
9.6 Single-wire protocol (SWP) 278

10 Contactless Data Transmission 283
10.1 Inductive coupling 284
10.2 Power transmission 285
10.3 Data transmission 286
10.4 Capacitive coupling 287
10.5 Collision avoidance 289
10.6 State of standardization 290
10.7 Close-coupling cards (ISO/IEC 10536) 291
10.7.1 Power transmission 292
10.7.2 Inductive data transmission 293
10.7.2.1 Transmission from the card to the terminal 293
10.7.2.2 Transmission from the terminal to the card 293
10.7.3 Capacitive data transmission 295
10.8 Remote coupling cards 296
10.9 Proximity cards (ISO/IEC 14443) 297
10.9.1 Physical properties 298
10.9.2 Power transmission and signal interface 299
10.9.3 Signal and communication interface 299
10.9.4 Type A communication interface 300
10.9.5 Type B communication interface 302
10.9.5.1 Data transmission from the terminal to the card 302
10.9.5.2 Data transmission from the card to the terminal 303
10.9.6 Initialization and anticollision (ISO/IEC 14443-3) 304
10.9.6.1 Type A initialization and anticollision 305
10.9.6.2 Type B initialization and anticollision 314
10.9.7 Transmission protocol (ISO/IEC 14433–4) 329
10.9.7.1 Protocol activation with Type A cards 330
10.9.7.2 Half-duplex block protocol (ISO/IEC 14433–4) 339
10.9.7.3 Deactivating a card 344
10.9.7.4 Error handling 344

10.10 Vicinity integrated circuit cards (ISO/IEC 15693) 344
10.11 Near field communication (NFC) 348
10.11.1 State of standardization 348
10.11.2 NFC protocol 349
10.11.3 NFC applications 350
10.11.3.1 Rapid access to information regarding services 350
10.11.3.2 Peer-to-peer information exchange 350
10.11.3.3 Mobile payment 350
10.11.3.4 Secure NFC 351
10.12 FeliCa 352
10.13 Mifare 352

11 Smart Card Commands 353
11.1 File selection commands 356
11.2 Read and write commands 358
11.3 Search commands 366
11.4 File operation commands 368
11.5 Commands for authenticating persons 370
11.6 Commands for authenticating devices 374
11.7 Commands for cryptographic algorithms 378
11.8 File management commands 384
11.9 Application management commands 389
11.10 Completion commands 391
11.11 Commands for hardware testing 395
11.12 Commands for data transmission 398
11.13 Database commands (SCQL) 399
11.14 Commands for electronic purses 402
11.15 Commands for credit and debit cards 405
11.16 Application-specific commands 406
11.17 Command processing times 407
11.17.1 Processing time estimation 407
11.17.1.1 Command processing 408
11.17.1.2 Proportionality factor for predefined functions 409
11.17.1.3 NVM operations 409
11.17.1.4 Data transfer 410
11.17.1.5 Calculated example: READ BINARY command 411
11.17.1.6 Calculated example: smart card initialization 413
11.17.2 Processing times of typical smart card commands 415
11.17.3 Typical command processing times 417

12 Smart Card File Management 421
12.1 File structure 421
12.2 The life cycle of files 422
12.3 File types 423
12.3.1 Master file (MF) 424
12.3.2 Dedicated file (DF) 424
12.3.3 Application dedicated file (ADF) 425

12.3.4 Elementary file (EF) 425
12.3.5 Working EF (WEF) 425
12.3.6 Internal EF (IEF) 425
12.4 Application files 425
12.5 File names 426
12.5.1 File identifier (FID) 426
12.5.2 Short file identifier (SFI) 428
12.5.3 DF name 429
12.5.4 Application identifier (AID) structure and coding 429
12.6 File selection 430
12.6.1 Selecting directories (MF and DF) 430
12.6.2 Explicit EF selection 431
12.6.3 Implicit EF selection 431
12.6.4 Selection using a path name 432
12.7 EF file structures 432
12.7.1 Transparent file structure 432
12.7.2 Linear fixed file structure 433
12.7.3 Linear variable file structure 434
12.7.4 Cyclic file structure 435
12.7.5 Data objects file structure 435
12.7.6 Database file structure 436
12.7.7 Execute structure 436
12.7.8 Sequence control file structure 436
12.8 File access conditions 436
12.9 File attributes 438
12.9.1 WORM attribute 439
12.9.2 High update activity attribute 439
12.9.3 EDC utilization attribute 439
12.9.4 Atomic write access attribute 439
12.9.5 Concurrent access attribute 440
12.9.6 Data transfer selection attribute 440
12.9.7 File encryption attribute 440

13 Smart Card Operating Systems 441
13.1 Evolution of smart card operating systems 442
13.2 Fundamental aspects and tasks 444
13.3 Command processing 447
13.4 Design and implementation principles 449
13.5 Operating system completion 452
13.5.1 Operating system boot loader 455
13.5.2 Hardware recognition 455
13.5.3 Soft and hard masks 456
13.5.4 Operating system APIs 457
13.6 Memory organization and memory management 457
13.6.1 RAM memory management 458
13.6.2 EEPROM memory management 459
13.6.3 Flash memory management 461

13.7 File management 463
13.7.1 Pointer-based file management 464
13.7.2 File management with a file allocation table (FAT) 466
13.7.3 Memory partitioning into pages 467
13.7.4 DF separation 467
13.7.5 Free memory management mechanisms 468
13.7.6 Quota mechanism 470
13.7.7 Data integrity 471
13.7.8 Cross-application access 472
13.8 Sequence control 472
13.9 ISO/IEC 7816-9 resource access 474
13.10 Atomic operations 480
13.11 Multitasking 483
13.12 Performance 484
13.13 Application management with global platform 485
13.13.1 Security domains 487
13.13.2 Issuer security domain 488
13.13.3 Global platform API 489
13.13.4 Global platform commands 489
13.14 Downloadable program code 491
13.15 Executable native code 493
13.16 Open platforms 499
13.16.1 ISO/IEC 7816 compatible platforms 499
13.16.2 Java card 499
13.16.2.1 The Java programming language 500
13.16.2.2 The properties of Java 501
13.16.2.3 Java virtual machine (JVM) 502
13.16.2.4 Java card virtual machine (JCVM) 504
13.16.2.5 Memory sizes in Java cards 505
13.16.2.6 Performance in Java cards 507
13.16.2.7 Java card runtime environment 508
13.16.2.8 Application partitioning (firewalls) 508
13.16.2.9 Command dispatching and application selection (dispatcher) 509
13.16.2.10 Transaction integrity (atomic operations) 510
13.16.2.11 Persistent and transient objects 510
13.16.2.12 Java Card application programming interface 511
13.16.2.13 Software development for Java in smart cards 514
13.16.2.14 Execution speed 517
13.16.2.15 File system 517
13.16.2.16 Cryptography and export restrictions 518
13.16.2.17 Future generations of Java cards 518
13.16.2.18 Summary and future prospects 519
13.16.3 Multos 519
13.16.4 BasicCard 520
13.16.5 Linux 521

13.17 The small-OS smart card operating system 521
13.17.1 Programming in pseudocode 523
13.17.2 Design aspects 524
13.17.3 File access 526
13.17.4 Access to internal secrets (PINs and keys) 526
13.17.5 Small-OS constants 529
13.17.6 Small-OS variables 529
13.17.6.1 Small-OS RAM variables 531
13.17.6.2 Small-OS EEPROM variables 532
13.17.7 Main loop and initialization 534
13.17.8 I/O manager 536
13.17.9 File manager 536
13.17.10 Return code manager 536
13.17.11 Operating system kernel 538
13.17.12 Command interpreter 539
13.17.13 Structure of program code for commands 540
13.17.14 Command set 541
13.17.14.1 SELECT command 541
13.17.14.2 READ BINARY command 545
13.17.14.3 UPDATE BINARY command 547
13.17.14.4 READ RECORD command 549
13.17.14.5 UPDATE RECORD command 552
13.17.14.6 VERIFY command 556
13.17.14.7 INTERNAL AUTHENTICATE command 560
13.17.15 A simple application example 563

14 Smart Card Production 567
14.1 Tasks and roles in the production process 567
14.2 The smart card life cycle 569
14.3 Chip and module production 571
14.3.1 Chip design 572
14.3.2 Smart card operating system development 573
14.3.3 Chip fabrication in semiconductor plants 575
14.3.4 Chip testing on the wafer 578
14.3.5 Wafer sawing 579
14.3.6 Packaging chips in modules 581
14.3.7 Chip bonding 582
14.3.8 Encapsulating the chips in modules 583
14.3.9 Module testing 583
14.4 Card Body production 585
14.4.1 Monolayer card 585
14.4.2 Multilayer card 586
14.4.3 Injection-molded card bodies 586
14.4.4 Direct plug-in production (plug-in only) 588
14.4.5 Card bodies with integrated antennas 589
14.4.5.1 Etched antennas 590
14.4.5.2 Wound coils 591

14.4.5.3 Embedded antennas 591
14.4.5.4 Printed antennas 593
14.4.5.5 Connecting the antenna to the chip 593
14.4.6 Printing the card bodies 594
14.4.6.1 Sheet printing of card bodies 594
14.4.6.2 Printing single card bodies 595
14.4.6.3 Offset printing 596
14.4.6.4 Digital printing 597
14.4.6.5 Screen printing 598
14.4.6.6 Thermal transfer and thermal dye sublimation printing 598
14.4.6.7 Inkjet printing 599
14.4.7 Stamping the foils 599
14.4.8 Applying card components to the card body 599
14.5 Combining the card body and the chip 599
14.5.1 Milling the module cavity 600
14.5.2 Implanting the modules 601
14.5.3 Module printing 603
14.5.4 Plug-in stamping 604
14.6 Electrical testing of modules 605
14.7 Loading static data 609
14.7.1 Completing the operating system 609
14.7.2 Collaboration of the card producer and the card issuer 610
14.7.3 Initializing the application 612
14.7.4 Optimized mass data transfer to smart cards 613
14.7.5 Accelerating data transfer to the smart card 616
14.8 Loading individual data 618
14.8.1 Generating card-specific secret data 618
14.8.2 Personalization (individualization) 619
14.9 Envelope stuffing and dispatching 624
14.10 Special types of production 625
14.10.1 Production on demand (PoD) 625
14.10.2 Picture cards 626
14.10.3 Direct smart card issuing (instant issuing) 628
14.11 Termination of card usage 629
14.11.1 Deactivation 629
14.11.2 Recycling 630

15 Quality Assurance 633
15.1 Card body tests 634
15.1.1 Adhesion (or blocking) 635
15.1.2 Amplitude measurement 635
15.1.3 Bending stiffness 635
15.1.4 Card dimensional stability and warpage with temperature and humidity 636
15.1.5 Card dimensions 636
15.1.6 Card warpage 636
15.1.7 Delamination 636

15.1.8 Dynamic bending stress 636
15.1.9 Dynamic torsional stress 637
15.1.10 Electrical resistance and impedance of contacts 637
15.1.11 Electromagnetic fields 638
15.1.12 Embossing relief height of character 638
15.1.13 Flammability 638
15.1.14 Flux transition spacing variation 638
15.1.15 Height and surface profile of the magnetic stripe 638
15.1.16 Light transmittance 638
15.1.17 Location of contacts 639
15.1.18 Resistance to chemicals 639
15.1.19 Static electricity 639
15.1.20 Surface profile of contacts 639
15.1.21 Surface roughness of the magnetic stripe 640
15.1.22 Ultraviolet light 640
15.1.23 Vibration 640
15.1.24 *Wear test for magnetic stripe* 640
15.1.25 X-rays test 640
15.2 Microcontroller hardware tests 641
15.3 Test methods for contactless smart cards 642
15.3.1 Test methods for proximity smart cards 644
15.3.2 Test methods for vicinity coupling smart cards 645
15.4 Test methods for software 645
15.4.1 Fundamentals of smart card software testing 647
15.4.1.1 Analysis 648
15.4.1.2 Design 648
15.4.1.3 Implementation and test 648
15.4.1.4 System integration 648
15.4.1.5 Maintenance 648
15.4.2 Testing techniques and test strategies 649
15.4.2.1 Statistical program evaluation 649
15.4.2.2 Review 649
15.4.2.3 Blackbox test 649
15.4.2.4 Whitebox test 650
15.4.2.5 Greybox test 653
15.4.3 Dynamic testing of operating systems and applications 653
15.4.4 Test strategy 654
15.5 Evaluation of hardware and software 659
15.5.1 Common criteria (CC) 661
15.5.2 ZKA criteria 663
15.5.3 Additional evaluation methods 663
15.5.4 Summary 664

16 Smart Card Security 667
16.1 Classification of attacks and attackers 668
16.1.1 Classification of attacks 669

16.1.2 Consequences of attacks and classification of attackers 672
16.1.3 Classification of the attractiveness of attacks 674
16.2 A history of attacks 675
16.3 Attacks and defense measures during development 675
16.3.1 Smart card microcontroller development 679
16.3.2 Smart card operating system development 680
16.4 Attacks and defense measures during production 682
16.5 Attacks and defense measures during card usage 682
16.5.1 Attacks on the hardware 684
16.5.2 Attacks on the operating system 712
16.5.3 Attacks on applications 727
16.5.4 Attacks on the system 731

17 Smart Card Terminals 735
17.1 Mechanical properties 739
17.1.1 Contact unit with wiping contacts 739
17.1.2 Mechanically driven contact unit 740
17.1.3 Electrically driven contact unit 740
17.1.4 Card ejection 741
17.1.5 Ease of card withdrawal 742
17.2 Electrical properties 742
17.3 User interface 744
17.4 Application interface 744
17.5 Security 744

18 Smart Cards in Payment Systems 747
18.1 Payment transactions with cards 747
18.1.1 Electronic payment transactions with smart cards 748
18.1.1.1 Credit cards 748
18.1.1.2 Debit cards 749
18.1.1.3 Electronic purses 749
18.1.1.4 Open and closed system architectures 750
18.1.1.5 Centralized and decentralized system architecture 751
18.1.2 Electronic money 753
18.1.2.1 Processable 753
18.1.2.2 Transferable 753
18.1.2.3 Divisible 753
18.1.2.4 Decentralized 753
18.1.2.5 Monitorable 754
18.1.2.6 Secure 754
18.1.2.7 Anonymous 754
18.1.2.8 Legal framework and retention of value 755
18.1.3 Basic system architecture options 755
18.1.3.1 Background system 755
18.1.3.2 Network 755
18.1.3.3 Terminals 756
18.1.3.4 Smart cards 756

18.2 Prepaid memory cards 757
18.3 Electronic purses 759
18.3.1 Inter-sector electronic purses compliant with EN 1546 760
18.3.1.1 Data elements 763
18.3.1.2 Files 764
18.3.1.3 Commands 764
18.3.1.4 States 765
18.3.1.5 Cryptographic algorithms 766
18.3.1.6 General processes 767
18.3.1.7 Load process 768
18.3.1.8 Payment process 771
18.3.2 Common electronic parse specifications 774
18.3.3 Proton 775
18.4 EMV Application 776
18.4.1 Files and data elements 777
18.4.2 Commands 778
18.4.3 Cryptography 778
18.4.4 System architecture and transaction processes 779
18.4.5 Future developments 781
18.5 PayPass and payWave 782
18.6 The Eurocheque System in Germany 783
18.6.1 User functions 784
18.6.2 The overall system in brief 785
18.6.3 Girocard with chip 786
18.6.4 Supplementary applications 788
18.6.5 Summary 788

19 *Smart Cards in Telecommunication Systems* 789
19.1 Public card phones in Germany 789
19.2 Telecommunication 792
19.3 Overview of mobile telecommunication systems 795
19.3.1 Multiple access methods 795
19.3.1.1 Frequency division multiple access (FDMA) 796
19.3.1.2 Time division multiple access (TDMA) 796
19.3.1.3 Code division multiple access (CDMA) 798
19.3.1.4 Space division multiple access (SDMA) 798
19.3.2 Cellular technology 799
19.3.3 Cell types 800
19.3.4 Bearer services 802
19.4 The GSM system 802
19.4.1 Specifications 804
19.4.2 System architecture and components 806
19.4.3 Important data elements 808
19.4.3.1 Coding of alphanumeric characters 808
19.4.3.2 SIM service table (SST) 810
19.4.3.3 Fixed dialing numbers (FDN) 810
19.4.3.4 ICC identification (ICCID) 810

19.4.3.5 International mobile equipment identity (IMEI) 810
19.4.3.6 International mobile subscriber identity (IMSI) 810
19.4.3.7 Ki (Key individual) and Kc (Key cipher) 810
19.4.3.8 Short messages service (SMS) 811
19.4.3.9 Abbreviated dialing numbers (ADN) 811
19.4.3.10 Location area information (LAI) 811
19.4.3.11 Mobile station ISDN number (MSISDN) 811
19.4.3.12 Temporary mobile subscriber identity (TMSI) 811
19.4.4 The subscriber identity module (SIM) 811
19.4.4.1 SIM commands 814
19.4.4.2 SIM files 816
19.4.4.3 Example of a typical command sequence 826
19.4.4.4 Authentication of the SIM 826
19.4.4.5 Mobile telephone switch-on and switch-off processes 830
19.4.4.6 SIM application toolkit (SAT) 833
19.4.4.7 Over-the-air (OTA) communication 838
19.4.4.8 Remote file management (RFM) 840
19.4.4.9 Remote applet management (RAM) 841
19.4.4.10 Dual IMSI 842
19.4.4.11 Implementing a home zone 844
19.4.4.12 Operating principle of SIM lock 845
19.4.4.13 Operating principle of prepaid systems 845
19.4.5 Future developments 848
19.5 The UMTS system 848
19.5.1 Future developments 852
19.6 The wireless identification module (WIM) 854
19.7 Microbrowsers 857

20 Smart Cards in Health Care Systems 861
20.1 Health insurance cards in Germany 861
20.2 Electronic health care cards in Germany 864
20.2.1 Card types 865
20.2.2 Applications in electronic health care cards 866
20.2.3 Electronic prescriptions 868
20.2.4 Summary and prospects 868

21 Smart Cards in Transportation Systems 869
21.1 Electronic tickets 869
21.1.1 System architecture 870
21.1.2 Octopus card 871
21.1.3 Trip registration 873
21.1.4 Typical transactions 874
21.1.4.1 Identification and authentication 875
21.1.4.2 Check-in transaction 876
21.1.4.3 Check-out transaction 876
21.1.5 Value-added services 876
21.1.6 Evolution of electronic tickets 877

21.2 Ski Passes 878
21.2.1 System architecture 878
21.2.2 Ski cards 880
21.2.3 Typical transactions 882
21.2.3.1 Identification and authentication 882
21.2.3.2 Reading data 883
21.2.3.3 Writing data 884
21.2.4 Future developments 885
21.3 Tachosmart 887
21.4 Electronic toll systems 887

22 Smart Cards for Identification and Passports 893
22.1 FINEID personal ID card 893
22.2 ICAO-compliant passports 894

23 Smart Cards for IT Security 899
23.1 Digital signatures 899
23.1.1 Applicable standards 900
23.1.2 The legal framework in Germany 900
23.1.3 System architecture 903
23.1.4 Card issuing 903
23.1.5 Signing and verifying documents 904
23.1.6 Trust center (TC) 905
23.1.7 Signature cards 906
23.1.8 Summary and prospects 909
23.2 Signature applications compliant with PKCS #15 909
23.3 Smart Card Web Server (SCWS) 912

24 Application Design 917
24.1 General information and characteristic data 917
24.1.1 Microcontrollers 917
24.1.1.1 Production 917
24.1.1.2 Service life 918
24.1.1.3 Data transmission 919
24.1.1.4 Algorithm execution times 920
24.1.2 Applications 920
24.1.2.1 Key management 920
24.1.2.2 Data 921
24.1.2.3 Data exchange 921
24.1.3 System aspects 922
24.1.3.1 Security 922
24.1.3.2 User interface 922
24.1.3.3 High-level design 923
24.1.4 Compliance with standards 923
24.2 Application generation tools 924
24.3 Analyzing an unknown smart card 926

25 Appendix 929
25.1 Glossary 929
25.2 Related reading 991
25.3 Bibliography 991
25.4 Directory of standards and specifications 999
25.5 Web addresses 1018

Index 1021