

Contents

Preface to the Third Edition	xiii
Symbols and Notation	xv
Program Code Conventions	xvii
Abbreviations	xix
1 Introduction	1
1.1 The History of Smart Cards	2
1.2 Application Areas	5
1.2.1 Memory cards	6
1.2.2 Microprocessor cards	6
1.2.3 Contactless cards	8
1.3 Standardization	9
2 Types of Cards	15
2.1 Embossed Cards	15
2.2 Magnetic-stripe Cards	16
2.3 Smart Cards	18
2.3.1 Memory cards	19
2.3.2 Microprocessor cards	20
2.3.3 Contactless smart cards	21
2.4 Optical Memory Cards	23
3 Physical and Electrical Properties	27
3.1 Physical Properties	27
3.1.1 Card formats	28
3.1.2 Card components and security features	31
3.2 The Card Body	38
3.2.1 Card materials	40
3.2.2 Chip modules	42
3.3 Electrical Properties	52
3.3.1 Electrical connections	53
3.3.2 Supply voltage	55

3.3.3	Supply current	58
3.3.4	External clock	60
3.3.5	Data transmission	60
3.3.6	Activation and deactivation sequences	61
3.4	Smart Card Microcontrollers	62
3.4.1	Processor types	66
3.4.2	Memory types	70
3.4.3	Supplementary hardware	80
3.5	Contact-type Cards	91
3.6	Contactless Cards	93
3.6.1	Close-coupling cards: ISO/IEC 10536	101
3.6.2	Remote-coupling cards	107
3.6.3	Proximity integrated circuit(s) cards: ISO/IEC 14 443	108
3.6.4	Vicinity integrated circuits cards (ISO/IEC 15 693)	153
3.6.5	Test methods for contactless smart cards	153
4	Informatic Foundations	155
4.1	Structuring Data	156
4.2	Coding Alphanumeric Data	161
4.2.1	7-bit code	161
4.2.2	8-bit code	161
4.2.3	16-bit code (Unicode)	163
4.2.4	32-bit code (UCS)	163
4.3	SDL Notation	164
4.4	State Machines	165
4.4.1	Basic theory of state machines	166
4.4.2	Practical applications	166
4.5	Error Detection and Correction Codes	169
4.5.1	XOR checksums	171
4.5.2	CRC checksums	172
4.5.3	Reed–Solomon codes	174
4.5.4	Error correction	174
4.6	Data Compression	176
4.7	Cryptology	177
4.7.1	Symmetric cryptographic algorithms	182
4.7.2	Asymmetric cryptographic algorithms	189
4.7.3	Padding	199
4.7.4	Message authentication code and cryptographic checksum	201
4.8	Key Management	202
4.8.1	Derived keys	202
4.8.2	Key diversification	203
4.8.3	Key versions	203
4.8.4	Dynamic keys	203
4.8.5	Key parameters	204
4.8.6	Key management example	206
4.9	Hash Functions	208

4.10 Random Numbers	210
4.10.1 Generating random numbers	211
4.10.2 Testing random numbers	213
4.11 Authentication	216
4.11.1 Symmetric unilateral authentication	218
4.11.2 Symmetric mutual authentication	219
4.11.3 Static asymmetric authentication	222
4.11.4 Dynamic asymmetric authentication	223
4.12 Digital Signatures	225
4.13 Certificates	229
5 Smart Card Operating Systems	233
5.1 Historical Evolution of Smart Card Operating Systems	234
5.2 Fundamentals	237
5.3 Design and Implementation Principles	242
5.4 Completion	245
5.5 Memory Organization	249
5.6 Smart Card Files	252
5.6.1 File types	254
5.6.2 File names	257
5.6.3 File selection	261
5.6.4 EF file structures	263
5.6.5 File access conditions	267
5.6.6 File attributes	270
5.7 File Management	271
5.8 Sequential Control	279
5.9 Access to Resources in Accordance with ISO/IEC 7816-9	280
5.10 Atomic Operations	288
5.11 Open Platform	290
5.12 Downloadable Program Code	293
5.13 Executable Native Code	296
5.14 Open Platforms	302
5.14.1 Java Card	303
5.14.2 Multos	322
5.14.3 Basic Card	323
5.14.4 Windows for Smart Cards	323
5.14.5 Linux	324
5.15 The Small-OS Smart Card Operating System	326
6 Smart Card Data Transmission	371
6.1 The Physical Transmission Layer	373
6.2 Answer to Reset (ATR)	377
6.2.1 ATR characters	379
6.2.2 Practical examples of ATRs	389

6.3 Protocol Parameter Selection (PPS)	392
6.4 Data Transmission Protocols	396
6.4.1 Synchronous data transmission	397
6.4.2 The T = 0 transmission protocol	403
6.4.3 The T = 1 transmission protocol	409
6.4.4 The T = 14 transmission protocol (Germany)	419
6.4.5 The USB transmission protocol	420
6.4.6 Comparison of asynchronous transmission protocols	421
6.5 Message Structure: APDUs	421
6.5.1 Structure of the command APDU	422
6.5.2 Structure of the response APDU	424
6.6 Securing Data Transmissions	425
6.6.1 The authentic mode procedure	429
6.6.2 The combined mode procedure	430
6.6.3 Send sequence counter	432
6.7 Logical Channels	434
7 Smart Card Commands	435
7.1 File Selection Commands	439
7.2 Read and Write Commands	442
7.3 Search Commands	450
7.4 File Manipulation Commands	452
7.5 Identification Commands	453
7.6 Authentication Commands	457
7.7 Commands for Cryptographic Algorithms	462
7.8 File Management Commands	468
7.9 Commands for Managing Applets	474
7.10 Commands for Completing the Operating System	474
7.11 Commands for Hardware Testing	477
7.12 Commands for Data Transmission Protocols	481
7.13 Database Commands: SCQL	482
7.14 Commands for Electronic Purses	486
7.15 Commands for Credit and Debit Cards	489
7.16 Application-Specific Commands	490
8 Security Techniques	491
8.1 User Identification	491
8.1.1 Testing a secret number	493
8.1.2 Biometric methods	498
8.2 Smart Card Security	510
8.2.1 A classification of attacks and attackers	511
8.2.2 Attacks and defensive measures during development	517
8.2.3 Attacks and defensive measures during production	520
8.2.4 Attacks and defense measures while the card is in use	521
9 Quality Assurance and Testing	565
9.1 Card Body Tests	566

9.2 Microcontroller Hardware Tests	573
9.3 Evaluating and Testing Software	574
9.3.1 Evaluation	575
9.3.2 Test methods for software	581
9.3.3 Dynamic testing of operating systems and applications	589
10 The Smart Card Life Cycle	597
10.1 The Five Phases of the Smart Card Life Cycle	598
10.2 Phase 1 of the Life Cycle in Detail	600
10.2.1 Generating the operating system and producing the chip	600
10.2.2 Producing card bodies without integrated coils	612
10.2.3 Producing card bodies containing integrated coils	621
10.2.4 Combining the card body and the chip	628
10.3 Phase 2 of the Life Cycle in Detail	630
10.4 Phase 3 of the Life Cycle in Detail	638
10.5 Phase 4 of the Life Cycle in Detail	650
10.6 Phase 5 of the Life Cycle in Detail	652
11 Smart Card Terminals	655
11.1 Mechanical Properties	660
11.2 Electrical Properties	663
11.3 Security Technology	665
11.4 Connecting Terminals to Higher-Level Systems	667
11.4.1 PC/SC	667
11.4.2 OCF	671
11.4.3 MKT	672
11.4.4 MUSCLE	672
12 Smart Cards in Payment Systems	673
12.1 Payment Transactions using Cards	674
12.1.1 Electronic payments with smart cards	674
12.1.2 Electronic money	679
12.1.3 Basic system architecture options	681
12.2 Prepaid Memory Cards	684
12.3 Electronic Purses	685
12.3.1 The CEN EN 1546 standard	685
12.3.2 Common Electronic Purse Specifications (CEPS)	701
12.3.3 Proton	702
12.3.4 The Mondex system	703
12.4 The EMV Application	708
12.5 The Eurocheque System in Germany	714
13 Smart Cards in Telecommunications	723
13.1 Survey of Mobile Telecommunication Systems	727
13.1.1 Multiple-access methods	727
13.1.2 Cellular technology	730

13.1.3 Cell types	732
13.1.4 Bearer services	733
13.2 The GSM System	735
13.2.1 Specifications	737
13.2.2 System architecture and components	740
13.2.3 Important data elements	741
13.2.4 The subscriber identity module (SIM)	745
13.2.5 General Packet Radio System (GPRS)	786
13.2.6 Future developments	787
13.3 The UMTS System	789
13.4 Microbrowsers	794
13.5 The Wireless Identification Module (WIM)	802
13.6 Public Card Phones in Germany	804
14 Sample Applications	811
14.1 Contactless Memory Cards for Air Travel	811
14.2 Health Insurance Cards	814
14.3 Electronic Toll Systems	819
14.4 Digital Signatures	822
14.5 The PKCS #15 Signature Application	833
14.6 The FINEID Personal Identification Card	840
14.7 Tachosmart	840
15 Application Design	843
15.1 General Information and Characteristic Data	843
15.1.1 Microcontrollers	843
15.1.2 Applications	846
15.1.3 System considerations	848
15.1.4 Compliance with standards	850
15.2 Formulas for Estimating Processing Times	850
15.3 Timing Formulas for Typical Smart Card Commands	858
15.4 Typical Command Processing Times	860
15.5 Application Development Tools	864
15.6 Analyzing an Unknown Smart Card	868
15.7 Life-Cycle Models and Process Maturity	870
15.7.1 Life-cycle models	874
15.7.2 Process maturity	882
15.8 The Course of a Smart Card Project	885
15.9 Design Examples for Smart Card Applications	886
15.9.1 An electronic purse system for arcade games	888
15.9.2 Access control system	890
15.9.3 Testing the genuineness of a terminal	894
16 Appendix	897
16.1 Glossary	897
16.2 Related Reading	985

16.3 Literature	985
16.4 Annotated Directory of Standards and Specifications	994
16.5 Coding of Data Objects	1030
16.5.1 Data objects compliant with ISO/IEC 7816-4	1030
16.5.2 Data objects compliant with ISO/IEC 7816-6	1031
16.5.3 Data objects for chip manufacturers as specified by ISO/IEC 7816-6	1032
16.6 Registration Authorities for RIDs	1032
16.7 Selected RIDs	1032
16.8 Trade Fairs, Conferences and Conventions	1033
16.9 World Wide Web Addresses	1034
16.10 Characteristic Data and Tables	1044
16.10.1 ATR interval	1044
16.10.2 ATR parameter conversion tables	1044
16.10.3 Determining the data transmission rate	1046
16.10.4 Sampling times for serial data	1046
16.10.5 The most important smart card commands	1047
16.10.6 Summary of utilized instruction bytes	1051
16.10.7 Smart card command coding	1053
16.10.8 Smart card return codes	1056
16.10.9 Selected chips for memory cards	1058
16.10.10 Selected microcontrollers for smart cards	1060
Index	1067

