

Table of Contents

Preface	1
About This Book	1
The Audience of This Book.....	2
No Need to Read the Whole Book.....	2
About the Authors	8
Acknowledgements	9
Part I.	
Smart Card Introduction and Overview	11
1 What Makes the Smart Card “Smart”?	13
1.1 What is a Smart Card?	13
1.1.1 The Benefits of Smart Cards.....	15
1.2 Smart Card Hardware	16
1.2.1 Memory Cards and Microprocessor Cards	16
1.2.2 Contactless Cards	17
1.2.3 The Computer on the Smart Card.....	17
1.2.4 Mechanical Contacts	19
1.2.5 The Size of a Smart Card	20
1.2.6 Hardware Security	21
1.2.7 The Manufacturing Process	21

2	Introduction to Smart Card Software	23
2.1	Smart Card Application Development Process.....	23
2.2	Communication with the Card.....	24
2.2.1	APDUs	24
2.2.2	T=0 and T=1	26
2.2.3	TLV Structures.....	27
2.3	Smart Card Operating Systems	28
2.3.1	File System Smart Cards	28
2.3.2	Java Card.....	31
2.3.3	Multos.....	32
2.3.4	Smart Card for Windows	33
3	Smart Cards and e-business	35
3.1	Electronic Purses.....	37
3.1.1	GeldKarte	39
3.1.2	Mondex.....	40
3.1.3	Proton	40
3.1.4	Visa Cash	41
3.1.5	Common Electronic Purse Specification.....	42
3.2	Authentication and Secure Access	43
3.2.1	Workstation Access	44
3.2.2	Network- and Server-Login	44
3.2.3	Secure Communication	45
3.3	Digital Signatures.....	46
3.4	Other Uses of Smart Cards in e-business	47
3.4.1	Electronic Ticketing	47
3.4.2	Loyalty Programs.....	48
3.4.3	Growth Expected.....	48
4	Cryptography	49
4.1	Cryptographic Algorithms	49
4.1.1	Symmetric Cryptographic Algorithms	50

4.1.2 Public-Key Algorithms.....	53
4.1.3 Hybrid Algorithms	56
4.2 Smart Card Cryptographic Protocols	57
4.2.1 External Authentication	57
4.2.2 Internal Authentication.....	58
4.2.3 Secure Messaging	59
4.3 TLS and Smart Cards	64
5 Smart Card Readers and Terminals	67
5.1 Smart Card Readers.....	67
5.2 Smart Card Terminals	69
5.3 Biometric Identification	70
6 Smart Card Standards and Industry Initiatives	71
6.1 ISO Standards.....	71
6.2 EMV ICC Specifications for Payment Systems	73
6.3 PC/SC	75
6.4 Visa Open Platform	78
Part II.	
OpenCard Framework	79
7 Introduction to OpenCard	81
7.1 The History of the OpenCard Framework	81
7.2 The OpenCard Consortium	82
7.3 The Objectives of the OpenCard Framework.....	83
7.4 The Advantages of Using OCF	84

7.5 The OCF Architecture	85
7.5.1 A Note on Notation.....	85
7.5.2 Architecture Overview.....	87
8 The Utility Classes	93
8.1 The OpenCard Core Definitions	93
8.2 The Core Utility Classes	94
8.2.1 Hex String Processing	94
8.2.2 The Configuration Provider	95
8.2.3 The Tracer	96
8.2.4 System Access	99
8.3 The Optional Utility Classes	101
8.3.1 The Loader Classes.....	101
8.3.2 The PassThruCardService.....	103
8.3.3 The Tag and TLV Classes	105
9 The Terminal Layer	107
9.1 Terminal Layer Core Components.....	108
9.1.1 Terminal Registry and Event Mechanism.....	109
9.1.2 Device Abstractions	110
9.1.3 The Terminal Layer Exceptions.....	113
9.1.4 PIN / Password Support.....	114
9.2 Terminal Layer Optional Components.....	117
9.2.1 The opencard.opt.terminal Package	118
9.2.2 The opencard.opt.terminal.protocol Package.....	118
9.3 Tracing in the Terminal Layer	121
9.4 Communicating with the Card Reader	121
9.4.1 The Java Communications API.....	122
9.5 The Implementation	123
9.5.1 Using the T=1 Protocol Support	124
9.5.2 Implementing the CardTerminal	126
9.5.3 Implementing the CardTerminalFactory	134

10 The Service Layer	137
10.1 The CardService Layer Core Components	139
10.1.1 The Application Access Classes	140
10.1.2 The Card Access Classes	144
10.1.3 The CardService Support Classes	148
10.1.4 The CHV Support Classes	153
10.1.5 The CardService Exceptions	155
10.2 The CardService Optional Components	156
10.3 Standard CardService Interfaces	158
10.3.1 The ISO File System CardService	159
10.3.2 The Signature CardService	162
10.3.3 The Application Management CardService	163
11 The OCF Security Concept	165
11.1 OpenCard Security Overview	166
11.2 OpenCard Security Classes	168
11.2.2 The Smart Card Key Classes	170
11.2.3 CardService Interface Classes	172
11.2.4 Credentials	175
11.3 Running OCF in Browsers	176
11.3.1 Browser Security Models	176
11.3.2 Invocation of Privileged Methods	177
11.3.3 Security Implications	179
Part III.	
Smart Card Application Development Using OCF	181
12 Using OCF	183
12.1 Preparing Your System	183
12.2 Configuring OCF on Your System	184
12.2.1 Setting the OCF Configuration Properties	184

12.3 The First Simple Application	185
12.3.1 Starting OCF and Shutting it Down Again.....	186
12.3.2 Obtaining a SmartCard Object via waitForCard(...)	187
12.3.3 Obtaining a CardService Object.....	188
12.3.4 Using this Sample Program with Other Cards	190
12.4 Smart Card Access of a Digital Signature Application	190
12.4.1 Attributes	191
12.4.2 Constructor	192
12.4.3 cardInserted()	192
12.4.4 allocateServices(SmartCard, Slot).....	194
12.4.5 cardRemoved()	195
12.4.6 signatureCardPresent()	196
12.4.7 getCardHolderData()	196
12.4.8 propagateAnEarlierException().....	198
12.4.9 setCardHolderData(String)	198
12.4.10 sign(int, byte[])	199
12.4.11 close()	200
12.4.12 Class SignatureCardException	200
12.4.13 The Complete Sample Source Code	201
13 OCF and e-business	203
13.1 Internet Stock Brokerage	203
13.1.1 Security Considerations	203
13.1.2 Secure Stock Brokerage Architecture	204
13.1.3 Protocols	205
13.2 Distributed Payment Systems.....	206
13.2.1 Card-to-Card Payment Schemes	207
13.2.2 Card-to-Card Payments via Internet.....	209
13.2.3 Architecture Overview	214
13.2.4 Implementation	216
14 Java Card and OCF	221
14.1 Developing a Card Applet.....	221
14.2 Inside the Java Card.....	222

14.2.1 The Java Card Framework	222
14.2.2 Lifetimes of On-card Programs and Objects	223
14.3 A Sample Java Card Applet	224
14.4 Using OCF to Work with Card Applets.....	230
14.4.1 Card Applet Proxies	231
14.4.2 Controlling Our Sample Card Applet through OCF	233
15 Card and Application Management	245
15.1 Introduction	245
15.1.1 Card Management Systems.....	246
15.1.2 Application Management Systems.....	247
15.1.3 Key Management Systems.....	247
15.2 Using OCF for Card and Application Management ...	248
15.2.1 Example	248
15.2.2 Security	249
15.2.3 Architecture and Technology	251
15.2.4 Post-Issuance Application Download	252
15.2.5 Post-Issuance Application Personalization	254
16 OCF for Embedded Devices	257
16.1 Device Profiles.....	257
16.2 OCF for Embedded Devices	259
16.2.1 Differences between OCF and OCF for Embedded Devices.....	260
16.2.2 Footprint Statistics	262

Part IV.	
Appendixes.....	263
A The Card	265
A.1 The IBM Multi Function Card.....	265
A.2 The File Structure on the Card.....	266
A.3 Accessing the Card	272
B Useful Web Sites	273
C Bibliography.....	277
D Glossary	281
E Index.....	285