

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	10
 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

3.1.1	GeldKarte	39
3.1.2	Mondex	40
3.1.3	Proton	41
3.1.4	Visa Cash	41
3.1.5	Common Electronic Purse Specification	43
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	49
4	Cryptography	51
4.1	Cryptographic Algorithms	51
4.1.1	Symmetric Cryptographic Algorithms	52
4.1.2	Public-Key Algorithms	56
4.1.3	Hybrid Algorithms	59
4.2	Smart Card Cryptographic Protocols	59
4.2.1	External Authentication	59
4.2.2	Internal Authentication	60
4.2.3	Secure Messaging	61
4.3	TLS and Smart Cards	67
5	Smart Card Readers and Terminals	69
5.1	Smart Card Readers	69
5.2	Smart Card Terminals	71
5.3	Biometric Identification	72
6	Smart Card Standards and Industry Initiatives	75
6.1	ISO Standards	75
6.2	EMV ICC Specifications for Payment Systems	77
6.3	PC/SC	79
6.4	GlobalPlatform	82

7	Introduction to OpenCard	87
7.1	The History of the OpenCard Framework	87
7.2	The OpenCard Consortium	88
7.3	The Objectives of the OpenCard Framework	89
7.4	The Advantages of Using OCF	89
7.5	The OCF Architecture	91
7.5.1	A Note on Notation	91
7.5.2	Architecture Overview	93
8	The Utility Classes	101
8.1	The OpenCard Core Definitions	101
8.2	The Core Utility Classes	102
8.2.1	Hex String Processing	102
8.2.2	The Configuration Provider	103
8.2.3	The Tracer	104
8.2.4	System Access	107
8.3	The Optional Utility Classes	109
8.3.1	The Loader Classes	110
8.3.2	The PassThruCardService	111
8.3.3	The Tag and TLV Classes	113
9	The Terminal Layer	115
9.1	Terminal Layer Core Components	116
9.1.1	Terminal Registry and Event Mechanism	117
9.1.2	Device Abstractions	118
9.1.3	The Terminal Layer Exceptions	121
9.1.4	PIN / Password Support	123
9.2	Terminal Layer Optional Components	125
9.2.1	The opencard.opt.terminal Package	126
9.2.2	The opencard.opt.terminal.protocol Package	128
9.3	Tracing in the Terminal Layer	130
9.4	Communicating with the Card Reader	130
9.4.1	The Java Communications API	131
9.5	The Implementation	132
9.5.1	Using the T=1 Protocol Support	133
9.5.2	Implementing the CardTerminal	135
9.5.3	Implementing the CardTerminalFactory	143

10	The Service Layer	145
10.1	The CardService Layer Core Components.....	147
10.1.1	The Application Access Classes	148
10.1.2	The Card Access Classes	152
10.1.3	The CardService Support Classes.....	156
10.1.4	The CHV Support Classes	161
10.1.5	The CardService Exceptions.....	164
10.2	The CardService Optional Components.....	166
10.3	Standard CardService Interfaces.....	168
10.3.1	The ISO File System CardService.....	169
10.3.2	The Signature CardService	172
10.3.3	The Application Management CardService.....	173
11	The OCF Security Concepts.....	175
11.1	OpenCard Security Overview	177
11.2	OpenCard Security Classes.....	179
11.2.1	Cryptographic Key Classes	180
11.2.2	The Smart Card Key Classes	181
11.2.3	CardService Interface Classes.....	183
11.2.4	Credentials	187
11.3	Running OCF in Browsers.....	188
11.3.1	Browser Security Models	189
11.3.2	Invocation of Privileged Methods.....	190
11.3.3	Security Implications.....	191
 Part III		
Smart Card Application Development Using OCF 193		
12	Using OCF	195
12.1	Preparing Your System	195
12.2	Configuring OCF on Your System.....	196
12.2.1	Setting the OCF Configuration Properties ..	196
12.3	The First Simple Application.....	198
12.3.1	Starting OCF and Shutting it Down Again	199
12.3.2	Obtaining a SmartCard Object via waitForCard(...)	200
12.3.3	Obtaining a CardService Object	201
12.3.4	Using this Sample Program with Other Cards	202

12.4	Smart Card Access of a Digital Signature	
	Application	202
12.4.1	Attributes.....	203
12.4.2	Constructor.....	204
12.4.3	cardInserted()	205
12.4.4	allocateServices(SmartCard, int)	206
12.4.5	cardRemoved()	207
12.4.6	signatureCardPresent()	208
12.4.7	getCardHolderData()	208
12.4.8	propagateAnEarlierException()	210
12.4.9	setCardHolderData(String).....	210
12.4.10	sign(int, byte[])	211
12.4.11	close()	212
12.4.12	Class SignatureCardException.....	212
12.4.13	The Complete Sample Source Code	213

13	OCF and e-business	215
13.1	Internet Stock Brokerage.....	215
13.1.1	Security Considerations.....	215
13.1.2	Secure Stock Brokerage Architecture.....	216
13.1.3	Protocols.....	217
13.2	Distributed Payment Systems	218
13.2.1	Card-to-Card Payment Schemes	219
13.2.2	Card-to-Card Payments via Internet	221
13.2.3	Architecture Overview	226
13.2.4	Implementation	228
14	Java Card and OCF	233
14.1	Developing a Card Applet.....	233
14.2	Inside the Java Card	234
14.2.1	The Java Card Framework	234
14.2.2	Lifetimes of On-card Programs and Objects.....	235
14.3	A Sample Java Card Applet.....	236
14.4	Using OCF to Work with Card Applets	242
14.4.1	Card Applet Proxies	243
14.4.2	Controlling Our Sample Card through OCF	245
15	Card and Application Management.....	255
15.1	Introduction.....	255
15.1.1	Card Management Systems.....	256
15.1.2	Application Management Systems	257
15.1.3	Key Management Systems.....	258

15.2 Using OCF for Card and Management.....	258
15.2.1 Example	259
15.2.2 Security	259
15.2.3 Architecture and Technology	261
15.2.4 Post-Issuance Application Download.....	262
15.2.5 Post-Issuance Application Personalization.....	264
16 OCF for Embedded Devices.....	267
16.1 Device Profiles	267
16.2 OCF for Embedded Devices	269
16.2.1 Differences between OCF and OCF for Embedded Devices	270
16.2.2 Footprint Statistics	272
Part IV	
Appendixes.....	273
A The Card	275
A.1 The IBM MultiFunction Card	275
A.2 The File Structure on the Card.....	276
A.3 Accessing the Card	283
B Useful Web Sites.....	285
C Bibliography	289
D Glossary.....	293
E Index	297