

# Table of Contents

<b>Preface</b> .....	<b>1</b>
About This Book I	
The Audience of This Book.....	2
No Need to Read the Whole Book.....	2
About the Authors .....	8
Acknowledgements .....	10
<b>Part I.</b>	
<b>Smart Card Introduction and Overview</b> .....	<b>11</b>
<b>1 What Makes the Smart Card “Smart”?</b> .....	<b>13</b>
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

<b>2 Introduction to Smart Card Software .....</b>	<b>23</b>
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
<b>3 Smart Cards and e-business .....</b>	<b>35</b>
3.1 Electronic Purses .....	37
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
<b>4 Cryptography.....</b>	<b>51</b>
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 .....	66
<b>5 Smart Card Readers and Terminals .....</b>	<b>69</b>
5.1 Smart Card Readers.....	69
5.2 Smart Card Terminals .....	71
5.3 Biometric Identification .....	72
<b>6 Smart Card Standards and Industry Initiatives.....</b>	<b>73</b>
6.1 ISO Standards.....	73
6.2 EMV ICC Specifications for Payment Systems.....	75
6.3 PC/SC.....	77
6.4 GlobalPlatform.....	80
<b>Part II.</b>	
<b>OpenCard Framework .....</b>	<b>83</b>
<b>7 Introduction to OpenCard.....</b>	<b>85</b>
7.1 The History of the OpenCard Framework.....	85
7.2 The OpenCard Consortium .....	86
7.3 The Objectives of the OpenCard Framework.....	87
7.4 The Advantages of Using OCF .....	88
7.5 The OCF Architecture .....	89
7.5.1 A Note on Notation.....	89
7.5.2 Architecture Overview.....	91
<b>8 The Utility Classes .....</b>	<b>97</b>
8.1 The OpenCard Core Definitions.....	97
8.2 The Core Utility Classes.....	98
8.2.1 Hex String Processing.....	98
8.2.2 The Configuration Provider .....	99
8.2.3 The Tracer.....	100
8.2.4 System Access .....	103

8.3	The Optional Utility Classes .....	105
8.3.1	The Loader Classes .....	106
8.3.2	The PassThruCardService.....	107
8.3.3	The Tag and TLV Classes.....	109
<b>9</b>	<b>The Terminal Layer .....</b>	<b>111</b>
9.1	Terminal Layer Core Components .....	112
9.1.1	Terminal Registry and Event Mechanism.....	113
9.1.2	Device Abstractions .....	114
9.1.3	The Terminal Layer Exceptions.....	117
9.1.4	PIN / Password Support.....	118
9.2	Terminal Layer Optional Components .....	121
9.2.1	The opencard.opt.terminal Package .....	122
9.2.2	The opencard.opt.terminal.protocol Package.....	124
9.3	Tracing in the Terminal Layer.....	126
9.4	Communicating with the Card Reader .....	126
9.4.1	The Java Communications API .....	127
9.5	The Implementation.....	128
9.5.1	Using the T=1 Protocol Support .....	129
9.5.2	Implementing the CardTerminal.....	131
9.5.3	Implementing the CardTerminalFactory.....	139
<b>10</b>	<b>The Service Layer.....</b>	<b>141</b>
10.1	The CardService Layer Core Components .....	143
10.1.1	The Application Access Classes .....	144
10.1.2	The Card Access Classes .....	148
10.1.3	The CardService Support Classes .....	152
10.1.4	The CHV Support Classes .....	157
10.1.5	The CardService Exceptions.....	161
10.2	The CardService Optional Components .....	162
10.3	Standard CardService Interfaces .....	164
10.3.1	The ISO File System CardService .....	165
10.3.2	The Signature CardService .....	168
10.3.3	The Application Management CardService.....	169

<b>11 The OCF Security Concepts.....</b>	<b>171</b>
11.1 OpenCard Security Overview .....	173
11.2 OpenCard Security Classes .....	175
11.2.2 The Smart Card Key Classes .....	177
11.2.3 CardService Interface Classes .....	179
11.2.4 Credentials .....	182
11.3 Running OCF in Browsers .....	184
11.3.1 Browser Security Models .....	184
11.3.2 Invocation of Privileged Methods.....	185
11.3.3 Security Implications .....	187
 <b>Part III.</b>	
<b>Smart Card Application Development Using OCF .....</b>	<b>189</b>
 <b>12 Using OCF.....</b>	<b>191</b>
12.1 Preparing Your System .....	191
12.2 Configuring OCF on Your System.....	192
12.2.1 Setting the OCF Configuration Properties.....	192
12.3 The First Simple Application .....	194
12.3.1 Starting OCF and Shutting it Down Again.....	195
12.3.2 Obtaining a SmartCard Object via waitForCard(...) .....	196
12.3.3 Obtaining a CardService Object .....	197
12.3.4 Using this Sample Program with Other Cards.....	198
12.4 Smart Card Access of a Digital Signature Application .....	198
12.4.1 Attributes .....	199
12.4.2 Constructor .....	200
12.4.3 cardInserted().....	201
12.4.4 allocateServices(SmartCard, int) .....	202
12.4.5 cardRemoved() .....	203
12.4.6 signatureCardPresent() .....	204
12.4.7 getCardHolderData() .....	204
12.4.8 propagateAnEarlierException().....	206
12.4.9 setCardHolderData(String) .....	206
12.4.10 sign(int, byte[]) .....	207
12.4.11 close() .....	208
12.4.12 Class SignatureCardException .....	208

12.4.13	The Complete Sample Source Code .....	209
<b>13</b>	<b>OCF and e-business.....</b>	<b>211</b>
13.1	Internet Stock Brokerage .....	211
13.1.1	Security Considerations .....	211
13.1.2	Secure Stock Brokerage Architecture .....	212
13.1.3	Protocols .....	213
13.2	Distributed Payment Systems .....	214
13.2.1	Card-to-Card Payment Schemes .....	215
13.2.2	Card-to-Card Payments via Internet .....	217
13.2.3	Architecture Overview.....	222
13.2.4	Implementation .....	224
<b>14</b>	<b>Java Card and OCF .....</b>	<b>229</b>
14.1	Developing a Card Applet .....	229
14.2	Inside the Java Card.....	230
14.2.1	The Java Card Framework .....	230
14.2.2	Lifetimes of On-card Programs and Objects.....	231
14.3	A Sample Java Card Applet .....	232
14.4	Using OCF to Work with Card Applets .....	238
14.4.1	Card Applet Proxies.....	239
14.4.2	Controlling Our Sample Card Applet through OCF .....	241
<b>15</b>	<b>Card and Application Management .....</b>	<b>251</b>
15.1	Introduction .....	251
15.1.1	Card Management Systems.....	252
15.1.2	Application Management Systems .....	253
15.1.3	Key Management Systems.....	253
15.2	Using OCF for Card and Application Management .....	254
15.2.1	Example .....	254
15.2.2	Security .....	255
15.2.3	Architecture and Technology.....	257
15.2.4	Post-Issuance Application Download .....	259
15.2.5	Post-Issuance Application Personalization .....	260

<b>16 OCF for Embedded Devices .....</b>	<b>263</b>
16.1 Device Profiles .....	263
16.2 OCF for Embedded Devices.....	265
16.2.1 Differences between OCF and OCF for Embedded Devices .....	266
16.2.2 Footprint Statistics .....	268
 <b>Part IV.</b>	
<b>Appendixes.....</b>	<b>269</b>
 <b>A The Card .....</b>	<b>271</b>
A.1 The IBM MultiFunction Card .....	271
A.2 The File Structure on the Card .....	272
A.3 Accessing the Card.....	279
 <b>B Useful Web Sites .....</b>	<b>281</b>
 <b>C Bibliography.....</b>	<b>285</b>
 <b>D Glossary.....</b>	<b>289</b>
 <b>E Index .....</b>	<b>293</b>

