

Contents

1	An Introduction to Smart Cards	1
	Keith Mayes	
1.1	Introduction	1
1.2	What is a Smart Card?	2
1.2.1	Magnetic Stripe Cards	2
1.2.2	Chip Cards	5
1.2.3	Microprocessor Chip Cards	6
1.2.4	Contact-less Smart Cards and RFIDs	6
1.2.5	Smart Tokens	7
1.3	Smart Card Chips	8
1.4	Tamper Resistance	11
1.5	Smart Card Characteristics	12
1.6	Issuer Control	13
1.7	Current Applications for Smart Cards	14
1.7.1	Mobile Telephony	15
1.7.2	Banking	17
1.7.3	Transport	17
1.7.4	Identity and Passports	18
1.7.5	Entitlement and Health	18
1.7.6	Physical and IT Access Control	19
1.7.7	Satellite TV	20
1.8	Smart Card Application Development	20
1.9	Development, Roll-Out and Lifecycle Management Issues	22
1.10	In Conclusion	23
	References	24
2	Smart Card Production Environment	27
	Claus Ebner	
2.1	Introduction	27
2.2	Smart Card Production Steps	29
2.2.1	Overview	29

2.2.2	Card Body Manufacturing	29
2.2.3	Personalization and related Services	35
2.2.4	Security and Quality	44
2.2.5	Current Trends	46
2.3	In Conclusion	48
	References	50
3	Multi Application Smart Card Platforms and Operating Systems	51
	Konstantinos Markantonakis	
3.1	Introduction	51
3.1.1	Smart card Platform Evolution	52
3.2	Java Card	55
3.2.1	<i>Java Card Forum</i>	55
3.2.2	Java Card Technology	56
3.3	GlobalPlatform	64
3.3.1	The GlobalPlatform Association	64
3.3.2	The GlobalPlatform Card Specification	65
3.4	Multos	72
3.4.1	<i>The MULTOS Consortium</i>	72
3.4.2	<i>MULTOS Specification</i>	73
3.4.3	The Multos Card Architecture	73
3.4.4	Multos Executable Language (MEL)	73
3.4.5	The Application Abstract Machine	75
3.4.6	Application Loading and Deletion	75
3.4.7	Communicating with a Multos Smart Card	76
3.4.8	Multos Files	76
3.4.9	Multos Security Features	76
3.5	Smartcard.NET Card	77
3.6	BasicCard	78
3.7	WfSC	78
3.8	Conclusions	79
	References	80
4	Smart Cards for Mobile Communications	85
	Keith Mayes and Tim Evans	
4.1	Introduction	85
4.2	SIM/USIM Standards	87
4.3	Subscriber Identity and Authentication	89
4.3.1	So how does SIM Authentication Work?	91
4.3.2	3G/USIM Authentication/Ciphering	92
4.3.3	SIM/USIM Authentication Algorithms	96
4.4	General Added Features	97
4.4.1	Phone Book	97
4.4.2	Roaming list	98
4.4.3	SMS Settings and Storage	98

4.4.4	Last Dialed numbers	99
4.4.5	Access Control Class	99
4.4.6	GPRS Authentication and encryption files	99
4.5	File Types	99
4.6	SIMs and USIMs Some Practical Comparisons	100
4.7	(U)SIM Value Added Services	103
4.8	The (U)SIM as a Handset Security Module	107
4.9	The Future Evolution of the (U)SIM	108
4.10	Conclusions	111
	References	112
5	Smart cards for Banking and Finance	115
	Konstantinos Markantonakis and Keith Mayes	
5.1	Introduction	115
5.2	Payment Card Technologies	116
5.2.1	Magnetic Stripe Cards	118
5.3	Smart Cards and EMV	120
5.3.1	Card Authentication	121
5.4	Cardholder Not Present Transactions	125
5.4.1	Purchase from a Genuine Merchant Using Someone Else's Payment Details	126
5.4.2	Genuine Purchaser Buying from a Rogue Merchant ..	126
5.4.3	Third Party Attacker	127
5.5	Dynamic Passcode Authentication	128
5.6	Could a Mobile Phone be a Token Reader?	131
5.7	Token Authentication Examples	132
5.8	E-Commerce Solutions	133
5.8.1	3D-Secure	133
5.8.2	Thoughts on 3D Secure	136
5.9	Just Wave Your Card to Pay	136
5.10	Concluding Remarks	137
	References	137
6	Security For Video Broadcasting	139
	Allan Tomlinson	
6.1	Introduction	139
6.2	Digital Video Basics	141
6.3	Scrambling	142
6.4	Synchronisation	143
6.5	Key Delivery	144
6.6	Access Requirements	145
6.7	Key Hierarchy	146
6.8	Implementation	147
6.9	In Conclusion	152
	References	153

7	Introduction to the TPM	155
	Allan Tomlinson	
7.1	Introduction	155
7.2	Trusted Platforms	156
7.2.1	Fundamental Features of a Trusted Platform	157
7.2.2	Additional Features	159
7.3	TPM Features	160
7.3.1	TPM Components	160
7.3.2	I/O Block	160
7.3.3	Non-Volatile Storage	161
7.3.4	Attestation Identity Keys	162
7.3.5	Platform Configuration Registers	163
7.3.6	Programme Code	163
7.3.7	Execution Engine	163
7.3.8	Random Number Generator	164
7.3.9	SHA-1 Engine	164
7.3.10	RSA Key Generation	164
7.3.11	RSA Engine	165
7.3.12	Opt-In	165
7.3.13	Other Features	167
7.4	TPM Services	167
7.4.1	Roots of Trust	167
7.4.2	Boot Process	168
7.4.3	Secure Storage	168
7.4.4	Attestation	169
7.5	In Conclusion	171
	References	171
8	Common Criteria	173
	John Tierney	
8.1	Introduction	173
8.2	Evolution of National and International Standards	174
8.2.1	International Recognition	175
8.2.2	The need for security benchmarks	176
8.3	Evaluation Practicalities	177
8.3.1	Types of evaluation	178
8.3.2	Evaluation Assurance Levels	179
8.3.3	Augmentation of Assurance Levels	179
8.4	Evaluation Roles	180
8.4.1	Performing Evaluations	181
8.5	Developing Protection Profiles and Security Targets	182
8.5.1	Establish the security environment	182
8.5.2	Establish Security Objectives	183
8.5.3	Establish Security Requirements	183
8.5.4	Establish TOE Summary Specification	184

8.5.5	Establish Rationale	184
8.5.6	Claiming Compliance with Protection Profiles	185
8.6	An Example	185
8.6.1	Establish the Security Environment	186
8.6.2	Establish security objectives	186
8.6.3	Establish Security Requirements	187
8.6.4	Establish TOE summary specification	188
8.6.5	Establish Rationale	189
8.7	Deliverables	189
8.8	Evaluation Composition	190
8.9	In Conclusion	192
	References	193
9	Smart Card Security	195
	Michael Tunstall	
9.1	Introduction	195
9.2	Cryptographic Algorithms	197
9.2.1	Data Encryption Standard	197
9.2.2	RSA	199
9.3	Smart Card Security Features	202
9.3.1	Communication	202
9.3.2	Cryptographic Coprocessors	203
9.3.3	Random Number Generators	204
9.3.4	Anomaly Sensors	205
9.3.5	Chip Features	205
9.4	Side Channel Analysis	207
9.4.1	Timing Analysis	207
9.4.2	Power Analysis	208
9.4.3	Electromagnetic Analysis	213
9.4.4	Countermeasures	214
9.5	Fault Analysis	216
9.5.1	Fault Injection Mechanisms	217
9.5.2	Modelling the Effect of a Fault	218
9.5.3	Faults in Cryptographic Algorithms	218
9.5.4	Countermeasures	221
9.6	Embedded Software Design	222
9.6.1	PIN Verification	222
9.6.2	File Access	224
9.7	In Conclusion	225
	References	225

10	Application Development Environments for Java and SIM Toolkit	229
	Gary Waite and Keith Mayes	
10.1	Introduction	229
10.2	Smart Cards Characteristics	230
10.2.1	Limitations	231
10.3	SIM Cards	232
10.4	Java Card	233
10.4.1	The Java Card Framework	235
10.5	Java SIM	238
10.5.1	sim.toolkit	239
10.5.2	sim.access	242
10.6	Application Development Tools	243
10.6.1	Compilers & Integrated Development Environments	243
10.6.2	Simulators	244
10.6.3	Protocol Analysis (Spy) Tools	245
10.6.4	Utilities	246
10.7	Mobile Phone Applications and the (U)SIM	247
10.7.1	SATSA	248
10.7.2	A Word on Testing	250
10.7.3	SIM Dongle Example	251
10.8	Looking To The Future	253
10.9	Concluding Remarks	253
	References	254
11	OTA and Secure SIM Lifecycle Management	257
	Joos Cadonau	
11.1	Introduction	258
11.2	The SIM Card As A Managed Platform	258
11.2.1	Common Stored and Managed Data	259
11.2.2	SIM Application Toolkit Interface SAT	260
11.2.3	Main Differences Between a SIM and a UICC/USIM Card	264
11.3	OTA - Over-The-Air Management	265
11.3.1	OTA Server Capabilities	267
11.4	Limitations and Improvements	268
11.4.1	Customer Managed Applications	270
11.5	SIM Lifecycle Management	271
11.6	In Conclusion	274
	References	275
12	Smart Card Reader APIS	277
	Damien Sauveron	
12.1	Terminology: Smart Card Reader, IFD, CAD and Terminal	277
12.2	OCF: OpenCard Framework	279
12.2.1	Overview	279

12.2.2	Example	281
12.3	PC/SC	282
12.3.1	Overview	282
12.3.2	Architecture	282
12.3.3	Various Implementations	285
12.3.4	Wrappers	288
12.3.5	Examples	289
12.4	STIP	291
12.5	In Conclusion	291
	References	292
13	RFID and Contactless Technology	295
	Gerhard P. Hancke	
13.1	Introduction	295
13.2	Contactless Technology	296
13.2.1	Applications	299
13.3	Radio Frequency Interface	301
13.3.1	Communication Theory	302
13.3.2	Inductive Coupling	305
13.4	Standards	311
13.4.1	ISO 14443	311
13.4.2	ISO 15693	317
13.4.3	ISO 18000	319
13.4.4	ISO 18092/NFC	320
13.5	Conclusion	321
	References	321
14	ID CARDS AND PASSPORTS	323
	Ingo Liersch	
14.1	Introduction	323
14.2	ID Cards	324
14.2.1	Requirements and Constituents of Modern National ID Cards	324
14.2.2	International Standards for ID Cards	331
14.2.3	Optical Personalisation of ID Cards	333
14.2.4	Countries and Their ID Cards	337
14.3	E-Passports	339
14.3.1	Introduction	339
14.3.2	Constituents of Passports	341
14.3.3	EU and ICAO Requirements	343
14.3.4	Security Protocols	344
14.4	Conclusion	345
	References	345

15 Smart Card Technology Trends	347
Chris Shire	
15.1 Trends In Smart Card Technology – Today And The Future ...	347
15.1.1 History	348
15.1.2 Technology Choices	351
15.1.3 Technology Drivers	355
15.1.4 Technology Trends	364
15.1.5 Emerging Applications	370
15.2 Conclusions	376
References	377
A Source Code for Chapter 12	381
A.1 C Language	381
A.2 Perl Language	385
Index	387

Smart Cards, Tokens, Security and Applications

Mayes, D.K.; Markantonakis, K. (Eds.)

2008, XXXVII, 392 p., Hardcover

ISBN: 978-0-387-72197-2