

Contents

Foreword	xi
Symbols and Notation	xiii
Abbreviations	xv
1 Overview of Smart Cards	1
1.1 Card Classification	1
1.2 Card Formats	2
1.3 Card Elements	3
1.3.1 Printing and labelling	3
1.3.2 Embossing	4
1.3.3 Hologram	4
1.3.4 Signature panel	4
1.3.5 Tactile elements	4
1.3.6 Magnetic stripe	4
1.3.7 Chip module	5
1.3.8 Antenna	5
1.4 Smart Card Microcontrollers	5
1.4.1 Processor	8
1.4.2 Memory	8
1.4.3 Supplementary hardware	8
1.4.4 Electrical characteristics	9
2 Smart Card Operating Systems	11
2.1 File Management	11
2.1.1 File types	12
2.1.2 File names	12
2.1.3 File structures	13

2.1.4	File attributes	15
2.1.5	File selection	15
2.1.6	Access conditions	16
2.1.6.1	State-based access conditions	16
2.1.6.2	Rule-based access conditions	17
2.1.7	File life cycle	18
2.2	Commands	19
2.3	Data Transmission	22
2.3.1	Answer to Reset (ATR)	23
2.3.2	Protocol Parameter Selection (PPS)	24
2.3.3	Transmission protocols	24
2.3.3.1	T=0 transmission protocol for contact cards	25
2.3.3.2	T=1 transmission protocol for contact cards	25
2.3.3.3	USB transmission protocol for contact cards	25
2.3.3.4	Contactless transmission protocols	26
2.3.4	Secure Messaging	26
2.3.5	Logical channels	26
2.4	Special Operating System Functions	26
2.4.1	Cryptographic functions	27
2.4.2	Atomic processes	28
2.4.3	Interpreter	28
2.4.4	Application management	28
3	Application Areas	31
3.1	Smart Card Systems	31
3.2	Potential Uses	32
3.3	Application Types	33
3.3.1	Memory-based applications	33
3.3.2	File-based applications	33
3.3.3	Code-based applications	35
4	Basic Patterns	37
4.1	Data Protection	37
4.1.1	Definition of terms	38
4.1.2	General principles	39
4.1.3	Recommendations for smart card systems	40
4.1.4	Summary	43

4.2	Export Control	44
4.3	Cryptographic Regulation	46
4.4	Standards	47
4.4.1	Standards for card bodies	48
4.4.2	Standards for operating systems	48
4.4.3	Standards for data and data structuring	49
4.4.4	Standards for computer interfaces	49
4.4.5	Standards for applications	49
4.5	Documents for Smart Card Systems	50
4.5.1	Specification partitioning	52
4.5.1.1	System specification	52
4.5.1.2	Background system specification	52
4.5.1.3	Smart card specification	53
4.5.1.4	Terminal specification	54
4.5.2	Elements of a typical card specification	54
4.5.2.1	General information	54
4.5.2.2	Smart card	55
4.5.2.3	Smart card operating system	55
4.5.2.4	Application	56
4.5.3	Document distribution	58
4.5.4	Document version numbering	59
5	Architecture Patterns	61
5.1	Data	61
5.2	Data Coding	62
5.3	Files	63
5.3.1	Access conditions	64
5.3.2	File names	67
5.4	Log Files	67
5.4.1	Data storage	67
5.4.2	Assigning data to log files	68
5.4.3	Invoking logging	68
5.4.4	Access conditions for log files	68
5.4.5	Logged data	69
5.4.6	Consistency and authenticity of log data	70
5.4.7	Log file size	71
5.4.8	Logging process	72

5.5	Pairing	73
5.6	Protecting Transaction Data	74
5.7	Reset-proof Counters	77
5.8	Proactivity	77
5.9	Authentication Counter	79
5.10	Manual Authentication of a Terminal	81
5.11	PIN Management	83
5.12	One-time Passwords	84
5.13	Key Management	88
5.14	State Machines for Command Sequences	89
5.15	Speed Optimization	91
5.15.1	Computing power	93
5.15.2	Communication	93
5.15.3	Commands	94
5.15.4	Data and files	95
6	Implementation Patterns	97
6.1	Application Principles	97
6.1.1	Program code	97
6.1.2	Commands	99
6.1.3	Data	99
6.1.4	Security	100
6.1.5	Application architecture	102
6.1.6	System	106
6.2	Testing	108
6.3	User–Terminal Interface	114
6.4	Smart Card Commands	115
6.4.1	Command structure	116
6.4.2	Interruption of commands	117
6.4.3	Command coding	118
6.4.4	Parameterization	118
6.4.5	Test commands	119
6.4.6	Secret commands	119
6.5	Java Card	120
6.5.1	Data types	122
6.5.2	Arithmetic operations	128
6.5.3	Control structures	129

6.5.4	Methods	131
6.5.5	Applets	132
7	Operation Patterns	137
7.1	Initialization and Personalization	137
7.2	Migration	141
7.3	Monitoring	143
7.3.1	System integrity	143
7.3.2	Attack detection	144
8	Practical Aspects of Smart Cards	147
8.1	Acceptance	147
8.2	Tell-tale Signs of Difficult Smart Card Systems	150
8.2.1	Inappropriate use of smart cards	150
8.2.2	Unclear specifications	151
8.2.3	Abundant options	151
8.2.4	Piggyback applications	152
8.2.5	Economizing on testing	153
8.2.6	Downloading applications	154
8.2.7	Offline systems	155
8.2.8	Intolerant smart cards and terminals	155
8.2.9	Strict compatibility requirements	156
8.2.10	Excessively stringent security requirements	157
8.2.11	Exaggerated future-proofing	158
8.3	Prerequisites for Easy Smart Card Systems	159
8.3.1	Expert advice	159
8.3.2	Foresighted design	160
8.3.3	Prototyping	160
8.3.4	Single-application smart cards	161
8.3.5	Simple structures	161
8.3.6	Robust design	161
8.3.7	Centralized systems	163
8.3.8	Staged deployment	163
8.4	In-field Faults	164
8.4.1	Fault classification	164
8.4.2	Fault impact	165
8.4.3	Actions in response to a fault	167

8.4.4	Fault search procedure	168
8.4.5	Fault remedies	170
9	Illustrative Use Cases	173
9.1	Monastery Card	173
9.2	Access Card	176
9.3	Telemetry Module	184
9.4	Business Card	186
9.5	Theft Protection Card	190
9.6	Admission Pass	193
9.7	PKI Card	196
9.8	SIM Card	198
	Bibliography	203
	Index	209