
Java Card™ Technology for Smart Cards

Architecture and Programmer's Guide

Zhiqun Chen



ADDISON-WESLEY

Boston • San Francisco • New York • Toronto • Montreal
London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

Contents

Foreword	xvii
Preface	xix
Part 1 Introduction	1
1 From the Beginning.....	3
1.1 Smart Cards	3
1.1.1 Brief History.....	3
1.1.2 Benefits.....	4
1.1.3 Applications	5
1.2 Challenges in the Development of Smart Card Applications	7
1.3 Applying Java to Smart Cards	8
1.3.1 Benefits of Java Card Technology	8
1.3.2 Brief History of Java Card Technology	9
2 Smart Card Basics.....	11
2.1 Overview of Smart Cards	11
2.2 Basic Card Types	11
2.2.1 Memory Cards versus Microprocessor Cards	12
2.2.2 Contact Cards versus Contactless Cards	13
2.3 Smart Card Hardware	14
2.3.1 Smart Card Contact Points	14
2.3.2 Smart Card Central Processing Unit	15
2.3.3 Smart Card Coprocessors	15
2.3.4 Smart Card Memory System	16

2.4	Smart Card Communication	17
2.4.1	Card Acceptance Device and Host Applications	17
2.4.2	Smart Card Communication Model	17
2.4.3	APDU Protocol	18
2.4.4	TPDU Protocol	20
2.4.5	ATR	20
2.5	Smart Card Operating Systems	21
2.5.1	Smart Card File Systems	21
2.5.2	Master File	22
2.5.3	Dedicated File	22
2.5.4	Elementary File	22
2.6	Smart Card Systems	23
2.7	Smart Card Standards and Specifications	24
2.7.1	ISO 7816 Standards	24
2.7.2	GSM	25
2.7.3	EMV	25
2.7.4	Open Platform	25
2.7.5	OpenCard Framework	26
2.7.6	PC/SC	26

Part 2 Java Card Technology 27

3 Java Card Technology Overview..... 29

3.1	Architecture Overview	29
3.2	Java Card Language Subset	30
3.3	Java Card Virtual Machine	31
3.3.1	CAP File and Export File	32
3.3.2	Java Card Converter	33
3.3.3	Java Card Interpreter	34
3.4	Java Card Installer and Off-Card Installation Program	34
3.5	Java Card Runtime Environment	36
3.5.1	JCRE Lifetime	37
3.5.2	How Does the JCRE Operate during a CAD Session?	38
3.5.3	Java Card Runtime Features	39
3.6	Java Card APIs	40
3.6.1	java.lang Package	40
3.6.2	javacard.framework Package	41
3.6.3	javacard.security Package	41
3.6.4	javacardx.crypto Package	42

3.7	Java Card Applets	42
3.8	Package and Applet Naming Convention	43
3.9	Applet Development Process	44
3.10	Applet Installation	45
3.10.1	ROM Applets	46
3.10.2	Preissuance or Postissuance Applets	46
3.10.3	Postissuance Applet Installation	46
3.10.4	Error Recovery during Applet Installation	47
3.10.5	Installation Constraints	48
4	Java Card Objects	49
4.1	Java Card Memory Model	49
4.2	Persistent Objects	50
4.3	Transient Objects	51
4.3.1	Properties of Transient Objects	52
4.3.2	Transient Object Types	52
4.3.3	Creating Transient Objects	53
4.3.4	Querying Transient Objects	54
4.4	A Few Words about Object Creation and Deletion	54
5	Atomicity and Transactions	57
5.1	Atomicity	57
5.2	Block Data Updates in an Array	58
5.3	Transactions	59
5.3.1	Commit Transaction	59
5.3.2	Abort Transaction	59
5.3.3	Nested Transaction	60
5.3.4	Commit Capacity	60
5.3.5	TransactionException	61
5.3.6	Local Variables and Transient Objects during a Transaction	62
6	Java Card Exceptions and Exception Handling	65
6.1	Exceptions in the java.lang Package	65
6.2	Java Card Exceptions	66
6.2.1	Java Card Exception Reason Code	67
6.2.2	Throwing an Exception in the Java Card Platform	68
6.2.3	ISOException	69
6.2.4	UserException	69

7	Java Card Applets	71
7.1	Applet Overview.....	71
7.1.1	Applet Installation and Execution	71
7.1.2	Applet Communication	72
7.2	Class <code>javacard.framework.Applet</code>	73
7.3	<code>install</code> Method.....	74
7.3.1	Creating Objects in the Applet's Constructor.....	76
7.3.2	Registering the Applet Instance with the JCRE.....	76
7.3.3	Processing the Installation Parameters.....	77
7.3.4	Further Applet Initialization.....	79
7.4	<code>select</code> Method.....	80
7.4.1	SELECT APDU Format and Processing	80
7.4.2	Default Applet	81
7.5	<code>deselect</code> Method.....	82
7.6	<code>process</code> Method.....	82
7.7	Other Methods in the Class <code>javacard.framework.Applet</code>	83
8	Working with APDUs.....	85
8.1	APDU Class.....	85
8.1.1	APDU Object.....	86
8.1.2	APDU Buffer Size	86
8.2	Interface <code>ISO7816</code>	87
8.3	Working with APDUs in Applets	87
8.3.1	Retrieve the APDU Buffer	87
8.3.2	Examine the Command APDU Header	88
8.3.3	Receive APDU Command Data	89
8.3.3.1	Receiving Long Command Data	90
8.3.4	Process the APDU Command and Generate the Response Data	92
8.3.5	Return APDU Response Data	92
8.3.5.1	Sending Data from Other Locations.....	95
8.3.5.2	Sending a Long Response	95
8.3.6	Return the Status Word	97
8.4	Protocol-Specific APDU Processing	98
8.4.1	Method <code>getProtocol</code>	98
8.4.2	Method <code>getInBlockSize</code>	98
8.4.3	Method <code>getOutBlockSize</code>	99
8.4.4	Method <code>setOutgoingNoChaining</code>	101

8.4.5	Method getNAD.....	101
8.4.6	Method waitExtension.....	101
8.5	Summary.....	102
9	Applet Firewall and Object Sharing	105
9.1	Applet Firewall.....	105
9.1.1	Contexts	106
9.1.2	Object Ownership.....	107
9.1.3	Object Access	107
9.1.4	Transient Array and Context	108
9.1.5	Static Fields and Methods	108
9.2	Object Sharing across Contexts	109
9.2.1	Context Switch	109
9.2.2	JCRE Privileges	110
9.2.3	JCRE Entry Point Objects	110
9.2.4	Global Arrays	111
9.2.5	Object Shareable Interface Mechanism	112
9.2.5.1	Shareable Interface	112
9.2.5.2	Shareable Interface Object	113
9.2.5.3	Thoughts behind the Shareable Interface Mechanism	113
9.2.5.4	An Example of Object Sharing between Applets	114
9.2.5.5	Create a Shareable Interface Object	115
9.2.5.6	Request a Shareable Interface Object	116
9.2.5.7	Use a Shareable Interface Object	118
9.2.5.8	Context Switches during Object Sharing	120
9.2.5.9	Parameter Types and Return Types in Shareable Interface Methods	121
9.2.5.10	Authenticate a Client Applet	122
9.2.5.11	getPreviousContextAID Method	126
9.2.5.12	Summary.....	127
10	Programming Cryptography	129
10.1	Quick Tour of Cryptography.....	129
10.1.1	Encryption and Decryption	130
10.1.2	Message Digest	133
10.1.3	Digital Signature	134
10.1.4	Random Data	135

10.2	Cryptographic Practice in Smart Card Applications	135
10.2.1	Ensuring Application Security	135
10.2.2	Functioning as a Secure Token.	136
10.2.3	Summary	137
10.3	Java Card Cryptography APIs	137
10.3.1	Design Principles	137
10.3.2	Architecture	138
10.3.3	Package Structure.	139
10.4	Code Examples	141
10.4.1	Compute a Message Digest	141
10.4.2	Build a Cryptographic Key	143
10.4.3	Sign and Verify a Signature	145
10.4.4	Encrypt and Decrypt Data	147
10.4.5	Generate Random Data	148
11	Java Card Platform Security.....	151
11.1	Java Card Platform Security Features.	151
11.1.1	Java Language Security	152
11.1.2	Additional Security Features of the Java Card Platform ...	152
11.2	Java Card Platform Security Mechanisms	153
11.2.1	Compile-Time Checking	154
11.2.2	Class File Verification and Subset Checking	154
11.2.3	CAP File and Export File Verification	156
11.2.4	Installation Checking	158
11.2.5	Cryptographically Enforced Chain Trust	160
11.2.6	Runtime Security Enforcement	160
11.2.7	Java Card Cryptographic Support	162
11.3	Applet Security	162
Part 3	Programming Guide and Tips.....	165
12	Step-by-Step Applet Development Guide.....	167
12.1	Design the Applet	167
12.1.1	Specify the Functions of the Applet.	167
12.1.2	Specify AIDs for the Applet.	168
12.1.3	Define the Class Structure and Method Functions of the Applet.	169
12.1.4	Define the Interface between the Applet and Its Host Application.	170
12.1.4.1	SELECT APDU	171
12.1.4.2	VERIFY APDU	171

12.1.4.3	CREDIT APDU	172
12.1.4.4	DEBIT APDU	172
12.1.4.5	GET BALANCE APDU	173
12.2	Construct the Applet Code	173
12.2.1	Wallet Applet Code	174
12.2.2	Implement Error Checking	180
12.3	What's the Next Step?	181
13	Applet Optimization	183
13.1	Optimizing an Applet's Overall Design	183
13.2	On-Card Execution Time	184
13.3	Method Invocations	184
13.4	Creating Objects in Applets	185
13.5	Reusing Objects	185
13.6	Eliminating Redundant Code	186
13.7	Accessing Arrays	187
13.8	The switch Statement versus the if-else Statement	189
13.9	Arithmetic Statements	191
13.10	Optimizing Variables in Applets	191
14	Working with int Data Type	195
14.1	32-Bit Arithmetic Operations	195
14.2	Array Size and Array Index	206
14.3	Storing and Computing int Values	207
14.4	Summary	213
Part 4	Appendices	215
A	Java Card Language Subset	217
B	Java Card 2.1 Application Programming Interface	224
	Glossary	357
	Bibliography	361
	Index	363