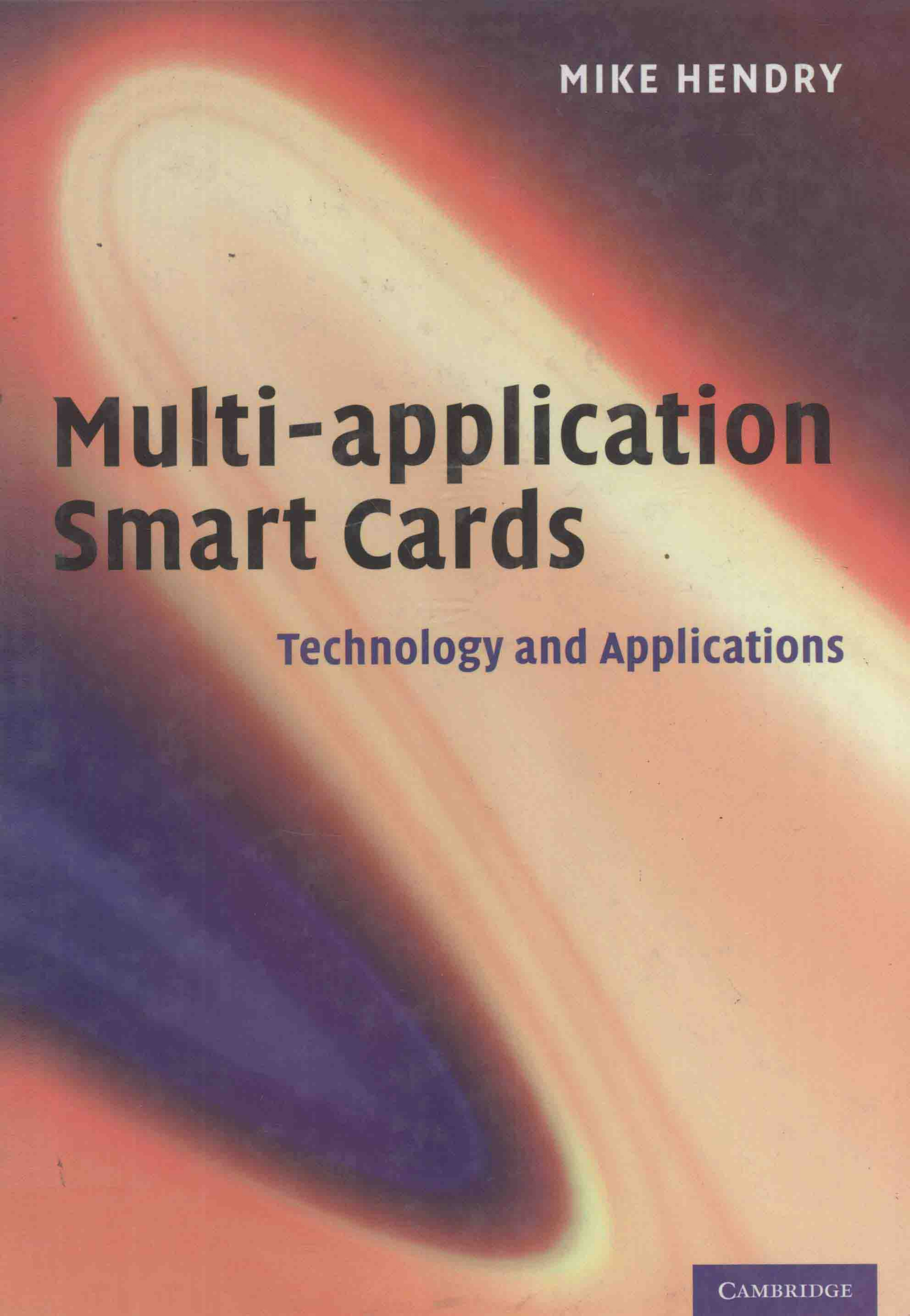
MIKE HENDRY

Multi-application Smart Cards

Technology and Applications



CAMBRIDGE

Multi-application Smart Cards

Technology and Applications

Mike Hendry

江苏工业学院图书馆
藏书章

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521873840

© Cambridge University Press 2007

This publication is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without
the written permission of Cambridge University Press.

First published 2007

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

ISBN 978-0-521-87384-0 hardback

Cambridge University Press has no responsibility for the persistence or
accuracy of URLs for external or third-party internet websites referred to
in this publication, and does not guarantee that any content on such
websites is, or will remain, accurate or appropriate.

Multi-application Smart Cards

Technology and Applications

Multi-application smart cards have yet to realise their enormous potential, partly because few people understand the technology, market and behavioural issues involved. Here, Mike Hendry sets out to fill this gap with a comprehensive guide to the technology, business and implementation aspects of this pivotal technology.

Following a review of the state of the art in smart card technology, the book describes the business requirements of each smart-card-using sector, and the applications and support systems required to sustain multiple applications. Implementation aspects, including security, are treated in detail and numerous international case studies cover identity, telecoms, banking and transportation applications. Lessons are drawn from these projects to help deliver more successful applications in the future.

Invaluable for users and those responsible for specifying, evaluating and integrating multi-application systems, this book will also be useful to terminal, card and system designers, network, IT and security managers and software specialists.

Mike Hendry is a freelance consultant and industry expert on cards and payment systems. He has many years of international experience in industry, was the Technical and Operations Director of the UK Chip and PIN Programme, and is also the author of several books.

Foreword

Smart cards are a thriving industry!

How do we know this to be the case? Well, if we look at the landscape of a typical industry sector, we see in smart cards the same characteristics we would witness in any other established and mature market.

For instance, companies have been created and thrive financially, based solely on the technology itself. These companies compete fiercely for a market share and brand leadership. Aggressive actions, such as mergers and acquisitions, and rigorous oversight of intellectual property rights are commonplace in the quest to increase both the industry and shareholder value. Dedicated industry analysts have built careers by following market movements and advances in the technology, and by prognosticating its future potential.

Trade shows and events have been established in every region of the world, dedicated to the exhibition of the technology and the sharing of information and industry best practices. These highly specialised gatherings not only showcase the latest in smart-card technology, but carefully articulate its relevance to critical sectors such as government, financial, retail, transit, healthcare and mobile telecommunications.

Industry associations have emerged to develop standards for smart cards and the applications that depend on the technology. In addition to developing standards, these birds-of-a-feather organisations have become valuable forums for information exchange between technology providers and end-user communities.

Magazines, periodicals, newsletters and websites cater exclusively to the smart-card industry. At the time of writing, a Google search on 'smart cards' resulted in 92 500 000 possible sites to explore.

Clearly, there is much to communicate.

So, by all accounts, one would assume that, in the presence of this much information and activity, the smart-card industry is, indeed, established and mature. While this may be true of some market applications (GSM and EMV) and within some regions of the world (Europe and Asia), smart-card technology has not been woven into the fabric of every card-holder's daily life on a global basis – at least not yet.

Ultimately, however, the widespread and pervasive use of smart-card technology is not only predictable, but inevitable.

Driven by the need for security, smart-card technology *will* emerge as the platform of choice in key vertical markets. Driven by the need for card-holder acquisition and retention, smart-card technology *will* emerge as the platform of choice to deliver

试读结束，需要全本PDF请购买 www.ertongbook.com

enriched applications and services aligned with individual card-holders' lifestyles. And, driven by the need to remain competitive, smart-card technology *will* continue to drop in price as standards evolve and commoditisation of the technology continues.

With these drivers in mind, the smart-card industry is taking action to capitalise on market momentum and the unique value proposition of this singular technology. Without question, the smart-card industry is on a trend to move:

From several operating system models to a dominant few. This will drive economies of scale in the industry and drive down cost without hindering competition.

From single purpose, single application cards to multi-application cards. This will enhance the card-holder and issuer value proposition for smart cards and expand the business model, justifying the investment in the technology.

From contact technology to contactless and multiple interface (TCP/IP, NFC, etc.) technology. This will enhance the utility of a single card platform by allowing its integration into different use environments.

From a card form to alternative forms such as smart objects and tokens. This will allow differentiated marketing practices among issuers and broaden the commercial appeal of the technology in several consumer-based application areas.

From single issuer models to co-operative private-public sector partnerships. The flexible nature of the technology will encourage novel commercial arrangements to emerge.

And from confusion to clarity on how to achieve interoperability. This will expand the size of the overall marketplace and provide a sustainable environment necessary for the rapid and widespread proliferation of the technology.

As these trends unfold over time, the utility of the smart card will multiply and play a significant rôle in enhancing daily lives, while safeguarding the applications and personal information of individual card-holders.

In this book, Mike Hendry takes care to address not only smart-card technology, but the transformation of the industry as described above. His work adds to the industry's rich body of knowledge and provides a fair and balanced view of smart cards as they exist today.

This industry, however, like many industries, is in a constant state of change and evolution. As such, any book on smart cards (or any non-fiction book for that matter) will become historical in context. So, I encourage you to study the information in this book as a 'first step' in your journey to understand the technology and the industry.

The next step – and on an on-going basis – will be to immerse yourself in the ebb and flow of the industry itself, through participation in industry associations, attendance at trade shows and events and by reading the periodicals and future new releases of books that cater to this subject.

Multi-application Smart Cards: Technology and Applications offers a foundation upon which to build your on-going involvement in the smart-card industry.

Welcome to our industry and to our unique technology!

Kevin Gillick
Executive Director, GlobalPlatform

Acknowledgements

Writing a book about multi-application smart cards is a microcosm of a multi-application smart-card project – although it demands of the author an understanding of the key issues, particularly those that affect structure and organisation, successful delivery requires input from a wide range of experts in different technology and application fields.

I have been fortunate to be able to draw on the experience of many such experts from different industries, viewpoints and countries. I greatly appreciated the early support, guidance and encouragement of Richard Poynder at the UK Smart Card Club, Greg Pote of the Asia-Pacific Smart Card Association and Ayse Korgav, Tono Aspinall and Kevin Gillick at GlobalPlatform; I am delighted that Kevin has provided a foreword.

Several extremely busy project managers and project owners have taken the time to contribute case studies or material for case studies, or to review case studies I have written; thanks are due to Erik Wellen and Dr Maan Kousa at King Fahd University for Petroleum and Minerals, Jusuk Lee of IBM Korea, Jason Lee at SK Telecom and Professor Ho Geun Lee of Yonsei School of Business, Dave Taylor at Barclaycard Business, James Lu in Taiwan, Wong Wan Ling at Welcome Real-Time, João Miguel Almeida of Link Consulting, Chua Siew Ling of QB, Chang Yun Chang at FEETC, Elvin Huang and Mike Cowen of MasterCard, Raymond Wong and T. K. Wong at the Hong Kong Immigration Department, Martin Arndt of the Royal Oman Police, Richard Pinnick at Fortress GB, Richard Poynder again, and Eddy Cheah and Wan Mohammad Ariffin in Malaysia.

For chapter reviews and advice in specific domains I have to thank Ian Duthie, Chris Shire, Julian Ashbourn, Bill Reding, Marc Kekicheff, Tim France-Massey, Ian Volans, Peter Jones and Peter Stoddart.

It has been a pleasure to work again with Julie Lancashire at Cambridge University Press, where the production team has also been very helpful in ensuring the quality of the final product. Meanwhile James Lu and Dr Lyndon Huang are working hard on the Chinese translation of the book, which will be published by the Taiwan Academy of Banking and Finance, where I also thank Emily Kuo and Erica Lin.

Lastly, but perhaps most of all, I would like to acknowledge the input of the hundreds of people all over the world with whom I have worked on smart-card projects and whose views and insights have helped to form my own.

My wife Valerie has tolerated the interruption to my work, sleeping patterns and mealtimes that any international book production involves; I never cease to be grateful for her understanding and support.

Shepperton, July 2006

Contents

Foreword by Kevin Gillick *page* xv
Acknowledgements xvii

Part I Introduction 1

1 Background 3
1.1 Smart cards in daily life 3
1.2 Card functions 4
1.2.1 From identification… 4
1.2.2 …to authentication 4
1.2.3 Data storage 5
1.3 Advanced applications 6
1.3.1 Cryptography 6
1.3.2 Database access and linking 6
1.3.3 Biometrics 6
1.3.4 Multiple applications 7
1.3.5 The universal helper 7
1.4 The smart-card business 7
1.5 Structure of this book 9

2 When is a card multi-application? 11
2.1 Single-function cards 11
2.2 Multi-function cards 11
2.2.1 Card-based functions (wired-logic cards) 12
2.2.2 Server-based functions 12
2.2.3 Multiple datasets 12
2.3 Multiple applications 13
2.3.1 Distinct and co-operative applications 13
2.3.2 Application selection 13
2.3.3 Application ownership 13
2.4 Operating systems 14
2.4.1 Application protection 14
2.4.2 Memory management 14

2.4.3 Application downloading and updating 14
2.4.4 Interpreter languages 15
2.4.5 'Open' features 15
2.5 Multiple organisations 15
2.6 Conclusion 16

3 **Smart-card basics** 17
3.1 What is a smart card? 17
3.1.1 Common features 17
3.1.2 Memory and wired-logic cards 17
3.1.3 Microprocessor cards 18
3.1.4 Memory types and sizes 19
3.2 Interfaces 19
3.2.1 Contact cards 20
3.2.2 Contactless cards 21
3.2.3 Dual interface 21
3.2.4 Dual-chip cards 22
3.3 Readers and terminals 22
3.3.1 Components 23
3.3.2 Contact sets and card transport 23
3.3.3 Terminals 24
3.4 Standards 24
3.4.1 Physical and magnetic stripe 24
3.4.2 Smart cards 25
3.4.3 Application standards 25
3.4.4 Testing standards 26
3.5 Smart-card manufacture and supply 26
3.6 References 28

Part II Technology 29

4 **Biometrics** 31
4.1 Identification requirements 31
4.1.1 Passwords, tokens and biometrics 31
4.1.2 Performance 32
4.1.3 Interoperability 33
4.1.4 Procedures 34
4.2 Biometric technologies 34
4.3 Biometrics in cards 36
4.3.1 On-card data capture 37
4.4 References 38

5 **Security and cryptography** 39
5.1 Cryptography 39

5.1.1 Algorithms 39
5.1.2 Key management 41
5.2 Security services 41
5.2.1 Confidentiality 41
5.2.2 Integrity 42
5.2.3 Authentication 43
5.2.4 Non-repudiation 43
5.2.5 Availability 44
5.3 Smart-card attacks 44
5.3.1 Trojan horses 44
5.3.2 Counterfeiting 45
5.3.3 Microprobing and electron microscopy 45
5.3.4 Environmental attacks 45
5.3.5 Differential power analysis 45
5.3.6 Yes-cards 46
5.3.7 Message interception 46
5.3.8 Preventing attacks 46
5.4 Security standards 46
5.4.1 Cards 47
5.4.2 Terminals and systems 48
5.4.3 Operations and management 48
5.5 Requirements definition 48
5.6 References 49

6 **Card technology** 50
6.1 Microcontrollers 50
6.1.1 Architecture 50
6.1.2 Feature size 50
6.1.3 Memory types and sizes 51
6.2 Cards 52
6.2.1 Materials 52
6.2.2 Construction 52
6.2.3 Form factors 54
6.3 Interfaces 56
6.3.1 USB 56
6.3.2 Contactless cards 56
6.3.3 Dual-interface cards 57
6.3.4 Legacy contactless card emulation 57
6.4 References 58

7 **Readers and terminals** 59
7.1 Reader type 59
7.1.1 Antennae for contactless readers 59
7.2 Terminals 61
7.2.1 Point of sale 61

试读结束，需要全本PDF请购买 www.ertongbook.com

7.2.2 Vending 62
7.2.3 Kiosks 63
7.2.4 PC-connected readers 63
7.2.5 Access control 64
7.2.6 Personal smart-card readers 64
7.3 Terminal management 65
7.4 Reference 68

8 Application selection: the ISO 7816 family 69
8.1 Scope and functions 69
8.2 Card initialisation 69
8.2.1 Power up and reset 69
8.2.2 Content of ATR 70
8.2.3 Protocol negotiation 71
8.2.4 Commands 72
8.2.5 File selection 72
8.2.6 Further application selection requirements 73
8.3 Native operating systems 74

9 JavaCard and GlobalPlatform 76
9.1 History 76
9.2 JavaCard 77
9.2.1 Scope and components 77
9.2.2 Applets 78
9.2.3 JavaCard Virtual Machine 78
9.2.4 JavaCard runtime environment 78
9.2.5 Security model 79
9.3 GlobalPlatform 80
9.3.1 GlobalPlatform architecture 80
9.3.2 Card Manager 81
9.3.3 GlobalPlatform API 83
9.3.4 Security domains 84
9.3.5 Card life-cycle management 84
9.3.6 GlobalPlatform device specification 85
9.3.7 GlobalPlatform system specification 87
9.4 JavaCard-based products 87
9.5 Status and implementations 88
9.6 References 89

10 Multos 90
10.1 History 90
10.2 Scope and functions 91
10.2.1 Multos executable language 91
10.2.2 Virtual machine 92

10.2.3 Application load and deletion 93
10.2.4 Multos step/one cards 94
10.3 Security 94
10.3.1 Common Criteria evaluation 94
10.3.2 Program and memory management 95
10.3.3 Runtime bytecode checking 95
10.3.4 Shell mode 96
10.3.5 Delegation 96
10.4 Status and implementations 96
10.5 Reference 97

11 **Other operating systems** 98
11.1 IBM MFC 98
11.2 Advantis 98
11.3 SECCOS 99
11.4 .NET 100
11.5 Special developments 101
11.6 Comparing operating systems with multi-application features 102
11.7 References 103

12 **Card management systems** 104
12.1 Legacy card management functions 104
12.2 Additional functions for smart-card management 104
12.2.1 Basic smart-card issuing 105
12.2.2 Links to real-time databases 105
12.2.3 Scripts and parameter updates 106
12.2.4 Customer-relationship management and the 'segment of one' 107
12.2.5 Multiple application issuers 107
12.2.6 Post-issuance application downloads 108
12.2.7 Life-cycle management 109
12.3 Deploying a smart-card management system 109
12.4 Functions of a smart-card management system 111
Case study A – King Fahd University of Petroleum and Minerals 112
Case study B – LG Card 115
12.5 References 116

Part III Business requirements 117

13 **Common business requirements** 119
13.1 Card issuing 119
13.1.1 Differentiation 120
13.1.2 Issuer control 120
13.1.3 Interoperability 121

13.2 Card and card-holder management 121
13.3 Application development 121
13.3.1 Speed and cost 121
13.3.2 Future-proofing 122
13.3.3 Platform independence 122
13.4 Application and memory management 122
13.5 Terminal management 123
13.6 Operations 124
13.6.1 Customer perspective 124
13.6.2 Retailer/acceptor perspective 125
13.6.3 Back-end systems 125
13.6.4 Exception handling 125
13.6.5 Cost and revenue management 126
13.7 Security 126
13.8 Trust and liability issues 126
13.9 Special needs 127
13.10 Reference 128

14 **Telecommunications** 129
14.1 Telephone cards 129
14.1.1 Other payment cards used in public telephones 130
14.2 Mobile telephony 130
14.2.1 Subscriber identity modules (SIMs) 130
14.2.2 SIM toolkit 132
14.2.3 3G 133
14.2.4 Application and parameter updating 133
14.2.5 Near Field Communication 134
14.2.6 Average revenue per user – the drive to add value 135
14.2.7 Network–manufacturer relationships 136
14.3 Mobile payment 136
Case study C – SK Telecom's Moneta service 137
14.4 Satellite and cable television 139
Case study D – SkyCard 140
14.5 Internet services 143
14.6 The future of multi-application cards in telecommunications 143
14.7 References 143

15 **Banking** 144
15.1 Types of card 144
15.1.1 Credit, debit and charge cards 144
15.1.2 ATM cards 145
15.1.3 Electronic purses and pre-authorised debit 146
15.1.4 Prepaid and gift cards 147
15.1.5 Customer cards 147
15.1.6 Commercial cards 148

15.2 Micropayments and cash displacement 148
15.3 Threats and attacks 148
15.4 Standards 149
15.4.1 EMV 149
Case study E – EMV deployment in Europe 150
15.4.2 Contactless cards 153
15.4.3 Electronic purses 154
15.4.4 Token authentication 154
15.4.5 Others 155
15.5 E-payment and m-payment 155
15.6 Loyalty 156
Case study F – Mashreqbank WOW! card 157
Case study G – United Bank Limited 160
15.7 Co-branding 161
15.8 The future of multi-application cards in banking 162
15.9 Reference 162

16 **Transportation** 163
16.1 Existing public-transport card schemes 163
16.1.1 Revenue management 163
16.1.2 Speed and convenience 164
16.1.3 Operating costs 164
16.1.4 Interoperability 164
Case study H – Lisboa Viva and 7 Colinas 166
16.2 Non-transit usage 168
Case study I – Kaohsiung City Government 'TaiwanMoney' card 169
Case study J – EZ-Link/QB 171
16.3 Inter-modal use 172
16.3.1 Trains 173
16.3.2 Taxis 173
16.3.3 Road tolling 173
16.3.4 Parking 175
16.3.5 Air travel 176
16.4 Card and system requirements 177
16.4.1 Standards 177
16.4.2 Security 178
16.4.3 Dual-interface cards 178
16.4.4 Operational aspects 179
16.4.5 Upgrading systems 179
16.5 The future of multi-application cards in transportation 180
16.6 References 180

17 **Government and citizens' cards** 181
17.1 Databases and cards 181
17.2 Electronic passports 181

17.3 Identity cards 183
Case study K – The Sultanate of Oman – national ID programme 184
17.4 'Cartes ville' 185
17.5 Health cards 186
17.6 Student cards 189
17.7 Additional functions on government cards 190
17.7.1 Proof of age 190
17.7.2 Driving licences 190
17.7.3 Access to government services 190
Case study L – A UK local authority citizens' card scheme 191
17.7.4 E-commerce authentication 194
17.7.5 Payment 195
Case study M – Malaysian Government multipurpose smart card (MyKad) 195
17.7.6 Record of qualifications 198
17.8 Data protection and privacy issues 198
17.9 The future for multi-application government and citizens' cards 199
17.10 References 199

18 Campus cards and closed user groups 201
18.1 Identification 201
18.2 Physical access control 202
18.3 PC and systems access 202
Case study N – Shibboleth 203
18.4 Authorisation and signing 204
18.5 Cashless payment 205
Case study O – Gwernyfed High School 205
18.6 Operational requirements 207
18.6.1 Card issuance and card management 207
18.6.2 Biometric enrolment 207
18.6.3 Registration, certification and verification 207
18.6.4 Terminal management 208
18.6.5 Transaction processing 209
18.7 Card requirements 209
18.8 The future of multi-application campus cards 210

Part IV Implementation 211

19 Organisation and structure 213
19.1 Corporate culture 213
19.2 Identifying stakeholders 214
19.3 Trust hierarchies 214
19.4 Liability 215
19.5 Commercial requirements 216

19.5.1 Co-branding 216
19.5.2 Rôles of partners 216
19.5.3 Understanding each other's business 217
19.6 Card-holder 'domains of use' 217

20 Implementation 219
20.1 Defining the project scope and road-map 219
20.2 Business case and risk analysis 220
20.3 Choosing partners 220
20.4 Identifying and managing stakeholders 221
20.5 Project organisation 221
20.6 Timescales 221
20.7 Standards and specifications 222
20.8 Procurement 222
20.9 Operational process design 223
20.10 Managing risks, problem and learning 223
Case Study P – UK Chip and PIN programme 223
20.11 Testing 226
20.12 Going live 226
20.13 Communication 226

21 Prognosis 228
21.1 Technology 228
21.1.1 Microcontrollers 228
21.1.2 Cards 229
21.1.3 Terminals 229
21.1.4 Card and terminal management systems 230
21.1.5 Security 230
21.1.6 Standards 230
21.2 Applications 230
21.2.1 Key sectors 231
21.2.2 Inter-sector and intra-sector cards 232
21.3 Towards a more customer-focused view 233

Appendix A – Glossary 235
Appendix B – Further reading 239
B.1 Smart-card technology 239
B.2 Biometrics 239
B.3 Cryptography and card security 239
B.4 JavaCard 240
Appendix C – Standards 241
Index 245

试读结束，需要全本PDF请购买 www.ertongbook.com