Contents

Preface xv

Acknowledgments xxiii

List of Acronyms xxv

1 Executive Summary **1**

1.1 Towards NFC Era 2

1.1.1 Ubiquitous Computing 2

1.1.2 Mobile Phones 3

1.1.3 Technological Motivation of NFC 4

1.1.4 Wireless Communication, RFID, and NFC 4

1.2 Evolution of NFC 4

1.2.1 Earlier Form of RFID: Barcode Technology 4

1.2.2 RFID Technology 5

1.2.3 Earlier Form of Smart Cards: Magnetic Stripe Cards 6

1.2.4 Smart Card Technology 6

1.2.5 NFC as a New Technology 7

1.3 NFC Essentials 7

1.3.1 Smart NFC Devices 8

1.3.2 Standardization of NFC Enabled Mobile Phones 8

1.3.3 General Architecture of NFC Enabled Mobile Phones 10

1.3.4 Near Field Communication Interface and Protocol (NFCIP) 11

1.4 NFC Operating Modes and Essentials 11

1.4.1 NFC Operating Modes 11

1.4.2 Reader/Writer Mode Essentials 12

1.4.3 Peer-to-Peer Mode Essentials 13

1.4.4 Card Emulation Mode Essentials 13

1.4.5 Case Studies 13

1.5 SE and Its Management 14

1.5.1 Over-the-Air Technology 15

1.5.2 GlobalPlatform Card Specification 15

1.5.3 Trusted Service Manager 16

1.5.4 UICC Management Models 16

1.5.5 Multiple SE Environments 16

1.6 NFC Application Development 17
1.6.1 JSR 257 18
1.6.2 JSR 177 18
1.7 NFC Security and Privacy 19
1.7.1 Why is Security Important? 19
1.7.2 Primary Goals of Security Measures 20
1.7.3 Vulnerability, Threat, Attack, and Risk 21
1.7.4 Security Tools and Mechanisms 21
1.7.5 NFC Security 22
1.7.6 Privacy, Legal, and Ethical Aspects 24
1.8 NFC Business Ecosystem 25
1.8.1 Stakeholders in NFC Ecosystem 27
1.8.2 Understanding NFC Business Models 28
1.8.3 Business Model Approaches 30
1.9 Usability in NFC 30
1.10 Benefits of NFC Applications 31
1.10.1 Future Scenarios on NFC 32
1.11 NFC Throughout the World 33
1.11.1 NFC Cities 33
1.11.2 NFC Trials and Projects 34
1.12 Status of Academic Research on NFC Literature 36
1.13 Chapter Summary 39
References 39

2 Towards NFC Era 41
2.1 Ubiquitous Computing and NFC 41
2.1.1 Ubiquitous Computing 41
2.1.2 New Communication Interface Alternative for Mobile Phones: NFC Technology 42
2.2 Mobile Phones 43
2.2.1 Features of a Mobile Phone 44
2.2.2 Mobile Phone Network 45
2.2.3 Mobile Phone Architecture 46
2.3 Wireless Communication as a Communication Media for NFC Technology 47
2.3.1 Wireless, Mobile, and Nomadic Communication 48
2.3.2 Wireless and Mobile Communication Technologies 48
2.4 RFID Technology 50
2.4.1 Earlier Form of RFID: Barcode Technology 51
2.4.2 Barcodes vs. RFID Tags 53
2.4.3 Essentials of RFID Technology 53
2.4.4 RFID Tags as Transponders 54
2.4.5 RFID Readers 55
2.4.6 Frequency Ranges 55
2.4.7 Operating Principles of RFID Technology 55
2.4.8 Near Field vs. Far Field Transmission 57
2.4.9 Common RFID Applications Throughout the World 58

2.5 Smart Card Technology 58
2.5.1 Earlier Form of Smart Card: Magnetic Stripe Cards 59
2.5.2 Evolution of Smart Cards 60
2.5.3 Types of Smart Cards: Capability Based Classification 60
2.5.4 Smart Card Operating System (SCOS) 61
2.5.5 Types of Smart Cards: Mechanism Based Classification 63
2.5.6 Smart Card Applications 67
2.6 Comparison between RFID Tags and Contactless Smart Cards 67
2.7 More on NFC 68
2.7.1 Inherent Security and Pairing Capability of NFC 70
2.8 Chapter Summary 70
Chapter Questions 71
References 71

3 NFC Essentials 73
3.1 Introduction to NFC 73
3.2 Standardization and Development Efforts of NFC Enabled Mobile Phones 76
3.2.1 NFC Forum 76
3.2.2 GlobalPlatform 79
3.2.3 GSM Association (GSMA) 80
3.2.4 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 80
3.2.5 ECMA International 81
3.2.6 ETSI and ETSI Smart Card Platform (ETSI SCP) 81
3.2.7 Java Community Process (JCP) 81
3.2.8 Open Mobile Alliance (OMA) 81
3.2.9 3rd Generation Partnership Project (3GPP) 82
3.2.10 EMVCo 82
3.3 General Architecture of NFC Enabled Mobile Phones 82
3.3.1 Secure Element 83
3.3.2 NFC Interface 86
3.3.3 Interface between SE and NFC Controller 86
3.3.4 Host Controller and HCI 89
3.4 Physical Layer of NFC 92
3.4.1 ISO/IEC 14443 – Proximity Contactless Smart Card Standard 92
3.4.2 Near Field Communication Interface and Protocol (NFCIP) 94
3.4.3 Data Transmission on RF Layer 96
3.5 Reader/Writer Operating Mode Essentials 99
3.5.1 Protocol Stack Architecture of Reader/Writer Mode 100
3.5.2 NFC Forum Mandated Tag Types 101
3.5.3 NDEF 102
3.6 Peer-to-Peer Operating Mode Essentials 108
3.6.1 Protocol Stack Architecture of Peer-to-Peer Mode 108
3.6.2 LLCP 109
3.7 Card Emulation Operating Mode Essentials 111
3.7.1 Protocol Stack Architecture of Card Emulation Mode 111

3.8 Chapter Summary 112

Chapter Questions 113

References 113

4 NFC Operating Modes 115

4.1 Mobile Interaction Techniques 115

4.1.1 NFC Technology Interaction Technique 117

4.2 Classification of NFC Devices 118

4.2.1 Active vs. Passive Devices 118

4.2.2 Initiator vs. Target Devices 119

4.3 Reader/Writer Mode 119

4.3.1 Smart Poster 120

4.3.2 Generic Usage Model 121

4.3.3 Leading Applications 123

4.3.4 Use Cases on Reader/Writer Mode 125

4.3.5 Underlying Application Benefits 127

4.4 Peer-to-Peer Mode 128

4.4.1 Generic Usage Model 129

4.4.2 Leading Applications 129

4.4.3 Use Cases on Peer-to-Peer Mode 130

4.4.4 Underlying Application Benefits 131

4.5 Card Emulation Mode 131

4.5.1 Generic Usage Model 132

4.5.2 Leading Applications 133

4.5.3 Use Cases on Card Emulation Mode 134

4.5.4 Underlying Application Benefits 135

4.6 Overview on Benefits of Operating Modes 135

4.7 Case Studies 136

4.7.1 Reader/Writer Mode Case Study: NFC Shopping 137

4.7.2 Peer-to-Peer Mode Case Study: NFC Gossiping 141

4.7.3 Card Emulation Mode Case Study: NFC Ticketing 142

4.8 Chapter Summary 148

Chapter Questions 148

References 148

5 Developing NFC Applications 151

5.1 Initial Steps in NFC Application Development 151

5.2 Why Java? 152

5.2.1 Why did we Choose Java? 152

5.2.2 Why is Java the Favorite? 153

5.3 Setting up the Environment for Java ME and NFC Programming 155

5.4 Introduction to Mobile Programing 158

5.4.1 Java ME Building Blocks 160

5.4.2 MIDlets 161

5.4.3 Package javax.microedition.lcdui 164

5.4.4 Creating a New MIDlet Project 165

5.4.5 *Inside a MIDlet Suite (MIDlet Packaging)* 168
5.4.6 *A More Detailed User Interface MIDlet* 171
5.4.7 *Push Registry* 177
5.5 NFC Application Development 179
5.6 Reader/Writer Mode Programing 179
5.6.1 *Package javax.microedition.contactless* 181
5.6.2 *Package javax.microedition.contactless.ndef* 183
5.6.3 *Package javax.microedition.contactless.rf* 185
5.6.4 *Package javax.microedition.contactless.sc* 185
5.6.5 *A Reader/Writer Mode Application* 185
5.6.6 *NFC Push Registry* 199
5.7 Peer-to-Peer Mode Programing 200
5.7.1 *Package com.nokia.nfc.p2p* 200
5.7.2 *Package com.nokia.nfc.llcp* 201
5.7.3 *A Peer-to-Peer Mode Application* 204
5.8 Card Emulation Mode Programing 211
5.8.1 *Accessing Secure Element Using JSR 257* 212
5.8.2 *Accessing Secure Element Using JSR 177* 212
5.9 Reader/Writer Mode Case Study: NFC Shopping 215
5.10 Peer-to-Peer Mode Case Study: NFC Gossiping 223
5.11 Chapter Summary 236
Chapter Questions 238
References 239

6 NFC Security and Privacy 241
6.1 Security in General 241
6.1.1 *Why is Security Important?* 242
6.1.2 *Primary Goals of Security Measures* 243
6.1.3 *Vulnerability, Threat, Attack, and Risk* 248
6.1.4 *Principles of Security* 253
6.2 Security Tools and Mechanisms 257
6.2.1 *Cryptography* 257
6.2.2 *Symmetric Cryptography* 258
6.2.3 *Asymmetric Cryptography* 259
6.2.4 *Hashing* 261
6.2.5 *Message Authentication Code (MAC) and HMAC* 261
6.2.6 *Digital Signature and Mobile Signature* 261
6.2.7 *Comparing Security Mechanisms* 262
6.2.8 *Digital Certificates and Certificate Authority* 263
6.2.9 *Do Not Keep Cryptographic Algorithms Secret* 263
6.2.10 *Key Types: Symmetric Key, Private Key, Public Key, Master Key, and Session Key* 264
6.2.11 *Key Management and its Importance* 264
6.2.12 *WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access)* 264
6.2.13 *Other Security Components* 264

6.3 NFC Security Framework 265

6.3.1 Security Issues on NFC Tag 266

6.3.2 Security Issues on NFC Reader 268

6.3.3 Security Issues on Smart Card 269

6.3.4 Security Issues on Communication 270

6.3.5 Middleware and Backend System Security 272

6.3.6 Standardized NFC Security Protocols 272

6.4 Privacy, Legal, and Ethical Aspects 277

6.4.1 It is a Different World 278

6.4.2 Some Examples on Privacy Issues 279

6.4.3 Summary on Privacy and Countermeasures 280

6.4.4 Some Proposals for Providing Privacy on Tags 280

6.4.5 What to do for Protecting Privacy 281

6.5 Chapter Summary 281

Chapter Questions 282

References 282

7 NFC Business Ecosystem 283

7.1 Business Ecosystem 283

7.1.1 Generic Features of a Business Ecosystem 285

7.1.2 Business Ecosystem of NFC 286

7.2 Stakeholders in NFC Ecosystem 286

7.2.1 Standardization Bodies and Other Contributors 287

7.2.2 NFC Chip Set Manufacturers and Suppliers 288

7.2.3 Secure Element Manufacturers and Suppliers 288

7.2.4 Mobile Handset Manufacturers and Suppliers 290

7.2.5 Reader Manufacturers and Suppliers 290

7.2.6 Mobile Network Operators 290

7.2.7 Trusted Service Managers 290

7.2.8 Service Providers 292

7.2.9 Merchants/Retailers 293

7.2.10 Customers 293

7.3 Business Models 293

7.3.1 Key Indicators in NFC Business Models 295

7.3.2 Business Model Alternatives 297

7.3.3 General Revenue/Expenditure Flow Model 300

7.4 Case Study: NFC Ticketing 301

7.5 Additional Reading: Pay-Buy-Mobile Project by GSMA 304

7.6 Chapter Summary 308

Chapter Questions 309

References 309

8 Secure Element Management 311

8.1 Introduction to OTA Technology 311

8.1.1 OTA Technology and Mobile Device Management 312

8.1.2 OTA Technology and UICC Based SEs 313

8.2 GlobalPlatform Specifications 314
8.2.1 GlobalPlatform Card Specification 314
8.2.2 GlobalPlatform Messaging Specification 316
8.3 Life Cycle Management of SEs 316
8.3.1 TSM in NFC Environment 317
8.3.2 Actors and Their Functional Roles in GlobalPlatform 318
8.3.3 UICC Based SE: Security Domains and Hierarchy 320
8.3.4 UICC Management Models 320
8.4 Multiple SE Environments 325
8.4.1 Architecture without Aggregation 325
8.4.2 Architecture with Aggregation 326
8.5 Alternative TSM Based OTA Management Model 326
8.6 Chapter Summary 328
Chapter Questions 329
References 329

9 NFC Cities and Trials 331
9.1 NFC Cities 331
9.1.1 City of Oulu 331
9.1.2 City of Nice 337
9.1.3 Smart Urban Spaces 339
9.2 NFC Trials and Projects 341
9.2.1 Contactless Payment Trials 341
9.2.2 Transport and Other Ticketing Trials 345
9.2.3 Other Trials 347
9.3 Chapter Summary 349
References 349

Index 351