Near Field Communication

From Theory to Practice

Vedat Coskun | Kerem Ok | Busra Ozdenizci

WILEY

IPR2025-01151
Apple EX1021 Page 1

NEAR FIELD COMMUNICATION

FROM THEORY TO PRACTICE

Vedat Coskun, Kerem Ok and Busra Ozdenizci

NFC Lab – Istanbul, ISIK University, Turkey

WILEY

A John Wiley & Sons, Ltd., Publication

This edition first published 2012
© 2012 John Wiley & Sons Ltd

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Library of Congress Cataloging-in-Publication Data

Coskun, Vedat.
Near field communication : from theory to practice / Vedat Coskun, Kerem Ok, and Busra Ozdenizci.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-119-97109-2 (cloth)
1. Near field communication. I. Ok, Kerem. II. Ozdenizci, Busra. III. Title.
TK6570.N43C67 2012
621.384–dc23

2011033663

A catalogue record for this book is available from the British Library.

ISBN: 9781119971092

Typeset in 10/12pt Times by Aptara Inc., New Delhi, India

FSC www.fsc.org MIX Paper from responsible sources FSC® C013604

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

1

Executive Summary

Near Field Communication (NFC) is a new technology and ecosystem that has emerged in the last decade. NFC technology is a short range, high frequency, low bandwidth and wireless communication technology between two NFC enabled devices. Communication between NFC devices occurs at 13.56 MHz high frequency which was originally used by Radio Frequency Identification (RFID). Although RFID is capable of reception and transmission beyond a few meters, NFC is restricted to within very close proximity. Currently, integration of NFC technology into mobile phones is considered as the most practical solution because almost everyone carries one.

NFC technology enables communication between an NFC enabled mobile phone at one end, and another NFC enabled mobile phone, an NFC reader or an NFC tag at the other end. Potential NFC applications and services making use of NFC technology include e-payment, e-ticketing, loyalty services, identification, access control, content distribution, smart advertising, data/money transfer and social services. Due to its applicability to a wide range of areas and the promising value added opportunities, it has attracted many academicians, researchers, organizations, and commercial companies.

The changes or improvements on RFID to expose NFC technology can be described as:

- Short range communication, where RFID may use long range especially for active tags that contain embedded energy.
- Passive tag usage only (actually occurs only in reader/writer mode) whereas both active and passive tags are possible in RFID.
- Inherent secure data exchange because of short range communication.
- Implicit matching of pairs that express their willingness to perform NFC communication by bringing themselves close to each other.
- Interest from companies to integrate many services such as payment with debit and credit cards, loyalty, identification, access control and so on, because of the secure communication and implicit matching as described in the previous item.

Technology usage is now in the pilot phase in many countries. Usability issues and technology adoption are being explored by many academicians and industrial organizations. Many mobile

Near Field Communication: From Theory to Practice, First Edition. Vedat Coskun, Kerem Ok and Busra Ozdenizci.
© 2012 John Wiley & Sons, Ltd. Published 2012 by John Wiley & Sons, Ltd.

- *Public transportation:* Many cities use RFID enabled payment systems on public transportation to make payment easier.
- *Passports:* It has become an ordinary process to insert RFID tags into passports to prevent counterfeiting them. Information such as owner's photo, fingerprint, address, some private data and so on are embedded into the tag, so that modification and illegal usage is harder than using printed material alone.

1.2.3 Earlier Form of Smart Cards: Magnetic Stripe Cards

A magnetic stripe card is one that contains a digital storage space where the data are loaded during the manufacturing phase. The stripe is made up of tiny magnetic particles in a resin. It is traditionally a read-only item. It is read by physical contact by swiping the card past a device with a magnetic reading head. Currently, magnetic stripes are mostly used on bank debit and credit cards, loyalty cards, airline tickets and boarding passes.

1.2.4 Smart Card Technology

A smart card is an item that contains an embedded IC that has integrated memory, which mostly involves a secure microcontroller or an equivalently intelligent device. In terms of mechanism, smart cards can be considered in three groups; contact and contactless smart cards, and hybrid models.

Smart cards do not contain any power source; hence energy is supplied by the external device, or the reader that the card interacts with. Contact cards receive the required energy via physical contact whereas contactless cards receive power via an electromagnetic field.

A contact smart card communicates with a card reader by direct physical contact, whereas a contactless smart card uses an RF interface for the same purpose. Contact smart cards contain a micro module containing a single silicon IC card with memory and microprocessor. An external device provides a direct electrical connection to the conductive contact plate when the contact smart card is inserted into it. Transmission of commands, data, and card status information takes place over these physical contact points.

In the case of contactless smart cards, the communication is performed only when the devices are in close proximity. One reason for this is increasing security of the communication, and another is enabling higher energy transfer from the active (the device that has embedded power source) to the passive device. As a contactless smart card is brought within the electromagnetic field range of the smart card reader, the card reader spreads out an electromagnetic signal and the smart card is powered by the signal. Once the smart card is powered, it can respond to the request of the reader.

The three major contactless smart cards are ISO/IEC 10536 Close Coupling Smart Cards, ISO/IEC 14443 Proximity Coupling Smart Cards and ISO/IEC 15693 Vicinity Coupling Smart Cards. Close coupling smart cards operate at a distance of up to 1 cm, and proximity coupling smart cards operate at a distance of less than 10 cm (less than 4 in.) at 13.56 MHz. Vicinity coupling smart cards operate in a range of up to 1 m at 13.56 MHz, such as those used in access control systems.

2002. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) adopted NFC technology in December 2003. In 2004, Nokia, Philips, and Sony founded the NFC Forum to promote the technology. NFC technology standards are acknowledged by ISO/IEC (International Organization for Standardization/ International Electrotechnical Commission), ETSI (European Telecommunications Standards Institute), and ECMA (European Computer Manufacturers Association).

NFC is a joint adventure of various technologies. Smart cards, mobile phones, card readers, short range communication, secure communication, transaction and payment systems are the most significant leading technologies. As several technologies are involved, related organization bodies have provided the respective standards. The integrated form of those standards will hopefully define a common vision for secure and yet functional usage and transaction. An interoperable set of standards is essential for a successful NFC ecosystem. The most dominant standardization organizations are:

(i) *NFC Forum*

NFC Forum is an alliance for specifying the NFC standards built on ISO/IEC standards. NFC Forum was established with the aim of enabling NFC technology and making it spread throughout the world. NFC Forum is a non-profit industry association formed to improve the use of NFC short range wireless interaction in consumer electronics, mobile devices, and PCs. NFC Forum promotes implementation and standardization of NFC technology to ensure interoperability between devices and services. The mission of the NFC Forum is to promote the usage of NFC technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology.

NFC Forum has standardized two operating modes (reader/writer and peer-to-peer operating modes) up to now. Record Type Definition (RTD) and NFC Data Exchange Format (NDEFF) specifications are provided by NFC Forum for reader/writer mode communication. Within peer-to-peer mode, Logical Link Control Protocol (LLCP) is used to connect peer-to-peer based application to the RF layer. Card emulation mode on the other hand, provides smart card capability for mobile phones.

Another important development introduced by NFC Forum is the "N-Mark" trademark which is a universal symbol for NFC, so that consumers can easily identify where their NFC enabled devices can be used.

(ii) *GlobalPlatform*

GlobalPlatform is a cross industry, non-profit association which identifies, develops and publishes specifications that facilitate secure and interoperable deployment and management of multiple embedded applications on secure smart cards. The goal of the GlobalPlatform specifications is to ensure interoperability on content management of smart cards, managing smart cards without any dependencies on hardware, manufacturers, or applications.

(iii) *GSM Association (GSMA)*

GSMA is an association of mobile operators and related companies devoted to supporting the standardization, deployment and promotion of GSM. GSMA represents the interests of the worldwide mobile communications industry. GSMA is focused on innovating, incubating and creating new opportunities for its members, all with the ultimate goal of driving the growth of the mobile communications industry.

decrease physical effort. Increasing processing power and wireless Internet access of mobile devices also helped with this issue and made this mode more attractive. For example; patients can upload their medical information using NFC technology from their homes and elderly people can order their meals from their homes. Clients can shop from home by touching their mobile devices to NFC tags placed on brochures.

Many more applications using reader/writer mode are developed than other modes. The most important reason for such development is that there are so many interesting and easy to implement use case scenarios that can be developed in reader/writer mode. Also developments and implementations of reader/writer mode applications are relatively easier to implement than others.

Peer-to-peer mode is rare when compared with other modes, which is studied mostly for device pairing, social networking, and file transfer operations. Peer-to-peer mode provides easy data exchange between two devices and enables some social networking cases (e.g., updating presence information on social networks).

In the study, it is found out that card emulation mode is mainly concerned with eliminating the need for a physical object. For example, the usage of a mobile phone eliminates the need to carry a credit card, a debit card, or even cash. Instead, a user makes payment with her mobile phone. NFC usage eliminates the need to carry a physical key and contactless smart key. As NFC can be used to enter rooms instead of electronic keys, it provides access control. Moreover, card emulation mode is used while cashing in ticket and mobile coupons. Actually these two processes also achieved the elimination of physical objects (paper-based tickets, coupons and so on) . The most important features of card emulation mode are the elimination of physical objects and providing access control. Also, the study stated that the commercially available applications are mostly developed using card emulation mode.

1.10.1 Future Scenarios on NFC

The main benefits of the reader/writer mode are identified as increasing mobility and decreasing physical effort. These benefits are in accordance with the mobility property of the mobile phone which in turn generally decreases physical effort. For example, calling someone provides mobility and eliminates the need to communicate face to face. Moreover with the mobile services usage, e-mail applications are developed for mobile phones and these e-mail applications enable users to read and write e-mails without any geographical restriction. It is seen in the study that the majority of real life scenarios can be adapted to this mode's applications. Application designs should include the data transfer from an NFC tag to a mobile phone and displaying it to the user. Moreover mobile phones can do additional processing with transferred data (e.g., can store the data in the mobile phone, and can transfer the data to any server on the Internet).

It has been seen that the peer-to-peer mode's major benefit is exchanging data easily. Data exchange between two NFC devices provides the possibility of secure transfer of critical data and social interaction. Since NFC devices can transfer data within 4 cm, exchanging critical data can be one of the key future applications of this mode.

It is stated in [5] that the card emulation mode's main aim is to make the mobile phone tightly coupled to its users. This can be considered as a challenge to the mobility property of mobile phones, however people carry mobile phones with them most of the time, and the

IPR2025-01151
Apple EX1021 Page 14

and trial projects are implemented in this application domain. Some of these projects have been completed or expanded into different application domains with growing participating entities or are still continuing. Some of the trials and projects are as follows:

- *Payez Mobile Project:* This is a joint initiative launched in November 2007. It is a mobile payment service pilot implemented with about 1000 testers and 500 retailers in Caen and Strasbourg. The global objective of the participants in this trial is to create a common vision, business solution for banks and MNOs in the contactless payment application domain.
- *C1000 NFC Pilot with Rabo Mobile in the Netherlands:* The Dutch based Rabobank has become the first bank in Europe to introduce mobile banking and low-cost calling services in a different way with Rabo Mobile (originally named Rabo Mobiel). It is a MVNO that is fully owned by Rabobank. Rabo Mobile initiated a new NFC pilot called 'Pay with your mobile phone at C1000' in the Netherlands. C1000 is one of the largest Dutch based supermarket chains. A number of NFC enabled applications in C1000 retail stores including mobile payment, and loyalty services were implemented over 6 months. Moreover, customers can bring their empty bottles and receive discount receipts to be used at the checkout from the bottle machines which are located within the supermarket or they can have a refund credited to their Rabobank accounts.
- *NFC Stadium experience in Manchester:* Manchester City Football Club and Orange UK provided an NFC enabled ticketing application. The fans are allowed to use their NFC enabled mobile phones to touch to the NFC readers at the stadium gates and enter through turnstiles to attend home games easily.
- *Bouygues Telecom trials in Paris:* France's major MNO Bouygues Telecom, RATP and SNCF who are the providers of Navigo contactless transit fare cards performed a 3-month NFC enabled transit ticketing trial in Paris. This trial's aim was to enable users to pay their fares at gates or at readers on buses which accept the Navigo ticketing application using their NFC enabled mobile phones.
- *O2 Wallet:* Telefonica O2, as one of the largest MNOs, announced O2 Wallet in November 2007 and performed a 6-month trial with various service providers. The O2 Wallet pilot paves the way for large usage of mobile phones as Oyster cards for travel around London, pay for purchases by Barclaycard, or access events. This application eliminates the need for users to carry Oyster smart cards in their wallets. Users can pay for their travel expenses through the Oyster application by simply touching their mobile phones to the Oyster NFC readers at London underground tube stations, on buses, and on trams.
- *London Fashion Week:* One of the largest MNOs in Europe, Telefonica O2, organized and performed a small trial at London Fashion Week which is the key event for designers in London to show their designs to fashion buyers throughout the world. The aim of this trial was to provide fashion buyers an opportunity to give instant feedback on the collection of designer Emilio de la Morena. This NFC enabled messaging trial was performed with a limited number of users.
- *Pass and Fly in Nice Airport:* Pass and Fly was a joint project of Nice Cote d'Azur Airport and Air France in partnership with Amadeus and IER. This pilot was launched in April 2009 and lasted for 6 months in Nice Cote d'Azur Airport. The aim of the pilot was to enable passengers to download digital boarding passes to their mobile phones using NFC technology.

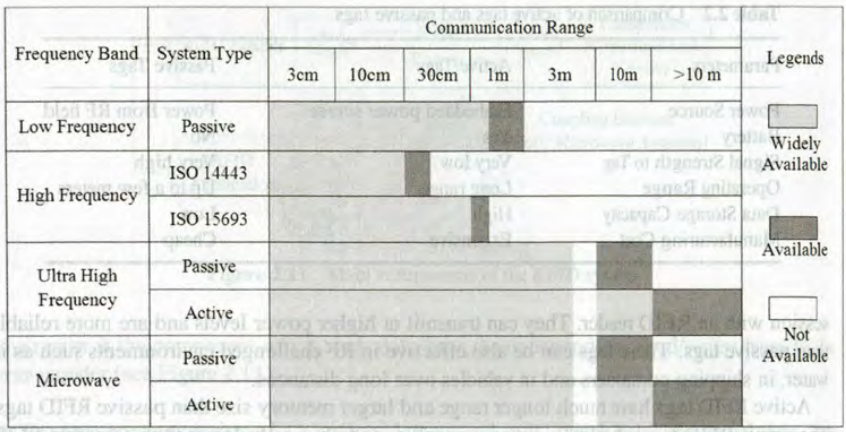

Figure 2.12 Communication range of the RFID system [3].

Inductively coupled transponders or tags are generally passive tags which have no internal power source. Thus they can be only used in near field cases. This means that all the energy for the embedded microchip within the tag has to be provided by the RFID reader in order for the microchip to operate.

For this purpose, the RFID reader's antenna generates a high frequency electromagnetic field. This field penetrates the cross section of the antenna's coil area and the area around the coil. The wavelength of the frequency range is several times greater than the distance between the RFID reader's antenna and the passive RFID tag. This electromagnetic field can be also identified as a simple magnetic alternating field.

When the RFID tag is placed in the electromagnetic field of the RFID reader, then the transponder gets energy from this magnetic field (see Figure 2.13). This power consumption can be described as a voltage drop at the internal resistance in the RFID reader's antenna through the supply current to the RFID reader's antenna. So, switching on and off a load resistance (or load modulator) at the transponder's antenna effects voltage changes at the RFID reader's antenna. If switching on and off the load modulator is controlled by data, then

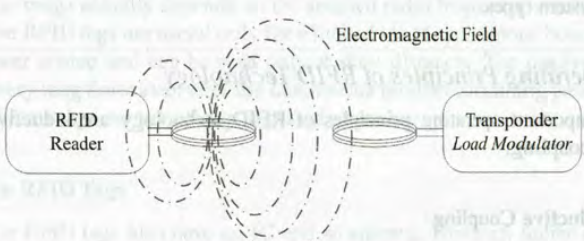

Figure 2.13 Inductive coupling.

microcontroller can store large amount of data and perform their own on-card functions such as security related operations and mutual authentication. These smart cards can interact intelligently with a smart card reader. These cards have their own operating system (see Section 2.5.4). Similarly, in terms of operating mechanism, smart cards are divided into three groups: contact, contactless, and hybrid smart cards. The details of the general features and interfaces are explained later in Section 2.5.5.

A smart card should obviously conform to the international standards. There are a number of standards and specifications that are relevant for smart card implementations and some of them are relevant for industry-specific applications. The complete smart card standardization bodies and specifications are ISO/IEC Standards, EMV 2000 Specifications, Federal Information Processing Standard 201 (FIPS 201), other Federal Information Processing standards, American National Standards Institute (ANSI) Standards, GlobalPlatform Specifications, Common Criteria (CC) Specifications, International Civil Aviation Organization (ICAO), International Airline and Transportation Association (IATA) Standards, G-8 Health Standards, The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191) Standards, Global System for Mobile Communication (GSM) Standards, Personal Computer/Smart Card (PC/SC) Workgroup Open Specifications, Open Card TM Framework, American Public Transportation Association's Contactless Fare Media System (CFMS) Standard, and Biometric Standards [4].

2.5.1 *Earlier Form of Smart Card: Magnetic Stripe Cards*

The process of attaching a magnetic stripe to a plastic card was invented by IBM in the 1960s. A magnetic stripe is the black or brown stripe placed on typically a credit card, or it can be placed on the back of an airline ticket or a transit card. The stripe is composed of tiny magnetic particles in a resin. The particles can be applied directly to the card or can be made into a stripe on a plastic backing which is applied to the card. Magnetic stripe cards are capable of storing data. These cards can be read by physical contact, by swiping the card on an external device which has magnetic reading head as depicted in Figure 2.15. Currently, magnetic stripes are mostly visible on financial debit or credit smart cards, airline tickets, and boarding passes.

Figure 2.15 Magnetic stripe card.

IPR2025-01151
Apple EX1021 Page 17

The material used to make the particles defines the coercivity of the stripe. Coercivity is the measure of difficulty to encode information on the magnetic stripe. The measure of coercivity is adjusted by the material used to make the particles. For instance, low coercivity stripes may use iron oxide and high coercivity stripes may use barium ferrite. The advantage of high coercivity is that it is harder to encode the information on the stripe. Hence, it is more difficult to erase the information on the card, so problems of accidental erasure are eliminated.

2.5.2 *Evolution of Smart Cards*

Smart cards were invented in the 1970s. The first mass use of the cards was for telephone payments in the 1980s. In the meantime, microprocessor smart cards were introduced. Microchips were integrated into debit cards in the 1990s. Smart card based electronic purse systems which store values on a card and do not need network connectivity, began to be used in Europe from the mid 1990s. One major improvement in smart card technology occurred in the 1990s; smart card based SIMs were introduced and started to be used in GSM based mobile phone environments in Europe. The use of smart cards increased with the ubiquity of mobile phones in Europe. In 1993, the international payment brands Europay, MasterCard, and Visa (EMV) collaborated to develop new specifications for smart cards in order to use them in payments both as a debit and a credit card. The first version of the EMV specifications, which stands for Europay, MasterCard, and Visa specifications, was released in 1994. EMVCo upgraded the specification in 2000. The specification was most recently upgraded in 2004. With the exception of some countries, there has been significant progress in the deployment of EMV-compliant Point of Sale (POS) equipment, as well as in the issuance of debit and credit cards using the EMV specifications. At that time, typically each country's national payment association was coordinated either by MasterCard International, Visa International, American Express, or JCB. They jointly planned and implemented EMV systems by considering various stakeholders. With the introduction of EMV specifications and systems throughout Europe, payment with contact smart card systems improved drastically. From a contactless smart card technology perspective, the major progress was the agreement of Visa and MasterCard in 2004–2006 to implement contactless payment and ticketing applications such as mass transit and highway tolls in the USA. With the introduction of contactless smart cards such as the MIFARE proximity smart card by Philips, contactless smart card applications started to have a considerable market share in Europe and the US.

2.5.3 *Types of Smart Cards: Capability Based Classification*

Smart cards are plastic cards with an embedded microprocessor and memory. Some smart cards have only non-programmable memory, thus they have limited capabilities. The smart cards that have microprocessors have various functionalities. Smart cards, in terms of their capability, can be divided into two major groups: memory based and microprocessor based smart cards.

2.5.3.1 Memory Based Smart Cards

Memory based smart cards can store any kind of data including financial, personal and other special information. However, they do not have a processing capability. These cards need to

IPR2025-01151
Apple EX1021 Page 18

regarded as an important step towards ubiquitous computing. NFC uses the touching paradigm for interaction. The users need to touch their mobile phones to a reader or a tag in order to establish a connection. NFC is an extension of RFID technology and compatible with contactless smart card technology interfaces.

RFID technology is used for tagging and identifying objects over large ranges. An RFID system typically includes two major components: the transponder which is placed on the object to be identified; and the reader which has reading and/or writing capability. The transponders are usually RFID tags (either passive or active).

Contactless smart card technology uses contactless smart cards that need to protect private information and also perform fast and secure transactions. Some examples of smart cards are personal identity verification, transit fare payment cards, and electronic passports. The major standards for contactless smart cards are ISO/IEC 10536 for close coupling, ISO/IEC 14443 for proximity coupling, and ISO/IEC 15693 for vicinity coupling smart cards.

NFC technology is defined by the NFC Forum founded by Nokia, Philips, and Sony which allow communication based on RFID technology and ISO/IEC 14443 infrastructures. It operates in three modes (reader/writer, peer-to-peer, and card emulation) with RF of 13.56 MHz where communication occurs on one side between a mobile phone with NFC capability, and on the other side a passive RFID tag, an NFC device or an NFC reader, respectively.

The major properties of NFC technology are automatic pairing and implicit security due to its short range communication capability. When compared with other wireless technologies, it allows low data rate transfer within very close distances. It is more human centric, easy, fast and enables high security and privacy.

Chapter Questions

1. Explain ubiquitous computing, and its relationship with NFC.
2. What are the similarities and the differences between QR Code and RFID technology?
3. Explain the difference between active and passive RFID tags.
4. What are the differences between near field and far field transmission concerning energy transfer between an active and a passive device?
5. What are the differences between memory based and microprocessor based smart cards?
6. What are the differences between microprocessor based smart cards and PCs?
7. What are the challenges that a mobile OS faces, but a PC OS does not?
8. Draw the universal contactless smart card reader symbol.
9. What are the differences between proximity and vicinity coupling smart cards?
10. What are the differences between RFID tags and contactless smart cards?
11. What are the most important integral properties of NFC technology?

References

[1] Resarsch, F. (2010) *Ubiquitous Computing, Developing and Evaluating Near Field Communication Applications*, Gabler, ISBN: 978-3-8349-2167-3.

[2] Finkenzeller, K. (2010) *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, John Wiley & Sons, Ltd, ISBN: 978-0-470-69506-7.

[3] Dressen, D. (2004) Considerations for RFID technology selection. *Atmel Applications Journal*, **3**, 45–47.

IPR2025-01151
Apple EX1021 Page 19

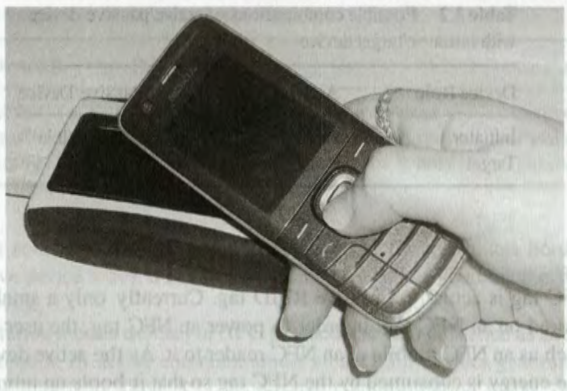

Figure 3.2 NFC mobile and NFC reader.

3.2 Standardization and Development Efforts of NFC Enabled Mobile Phones

NFC technology benefits from various elements such as smart cards, mobile phones, card readers, payment systems and so on. All these elements need to acquire accreditation from an assortment of governing bodies that have the responsibility for the security and interoperability of various NFC devices. As mobile phones became the best solution for NFC technology, especially for secure transactions, various standardization bodies defined how the NFC technology should be integrated into mobile phones and other related devices. Some other bodies defined the architectures and standards for the security as well as the ancillary technologies for NFC enabled mobile phones, such as smart cards for NFC transactions. The common vision of all standardization bodies is to increase the ease of access, interoperability and security for NFC technology. Figure 3.3 gives a summary of the standardization bodies that play a role in the development of NFC technology and Figure 3.4 gives the "big picture" for mobile phones and the bodies supporting them.

3.2.1 NFC Forum

NFC Forum is a non-profit industry association that was established with the aim of enabling NFC technology and making it spread around the world. NFC Forum is an alliance for specifying the NFC standards built on ISO/IEC standards. The introduction of this organization dates back to 2004 when a number of major companies including Nokia, Philips, and Sony formed an alliance for advanced usage of RFID technology in consumer applications. The NFC Forum later included companies such as Visa, MasterCard, Samsung, Microsoft, and Motorola.

NFC Forum focuses on improving the use of short range wireless interaction through NFC technology in consumer electronics, mobile devices, and PCs. The mission of NFC Forum is to promote the usage of NFC technology by developing specifications, ensuring interoperability

IPR2025-01151
Apple EX1021 Page 20

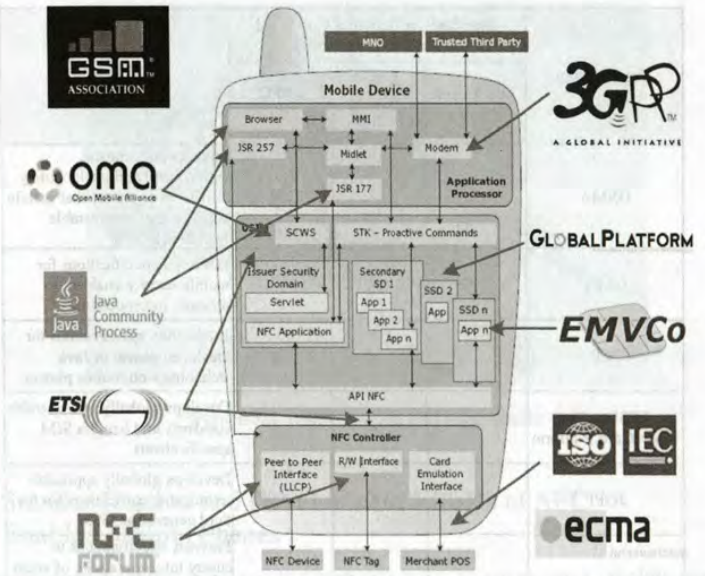

Figure 3.4 Standards and standardization bodies of NFC mobile. Reproduced by permission from GSMA. All rights reserved.

- Encourage technology providers to develop and deploy NFC enabled products around a common set of specifications.
- Establish a certification program that ensures compliant products according to NFC Forum specifications.
- Promote global use of NFC technology by educating consumers and enterprise users on the applications and benefits of NFC technology.

NFC Forum standardized only two operating modes (reader/writer and peer-to-peer) from the application layer to the RF layer (see Figure 3.5). As mentioned in Table 3.4, for reader/writer mode, Record Type Definition (RTD) and NFC Data Exchange Format (NDEF) specifications are being used. In peer-to-peer mode, Logical Link Control Protocol (LLCP) is used to connect the peer-to-peer based application to the RF layer, while the card emulation mode provides smart card capability for mobile phones. Details from Figure 3.5 will be briefly touched upon for each operating mode throughout this chapter. For more details about these specifications, please visit the NFC Forum website (http://www.nfc-forum.org).

Another important development introduced by the NFC Forum is the "N-Mark" trademark which is a universal symbol for NFC (see Figure 3.6), so that consumers can easily identify where their NFC enabled devices can be used. The N-Mark has two meanings [1]:

- The existence of an N-Mark on an active device means that the device has passed NFC Forum certification testing. Once a product is certified, it can contain the N-Mark on it. The

on the smart card emulation side for the standards ISO/IEC 14443 Type B and ISO/IEC 15936, although read-out and editing is possible [5].

3.4.3 Data Transmission on RF Layer

The reader/writer mode allows data connection only at 106 kbps and relies on the RF interface that is compliant with the ISO/IEC 14443 (Type A, Type B) and FeliCa schemes. In peer-to-peer mode, the RF interface that allows all data connections such as 106, 212, and 424 kbps is based on the ISO/IEC 18092 (NFCIP-1) standard. In card emulation mode, the RF interface is based on the ISO/IEC 14443 (Type A, Type B) standard and FeliCa. The Type B is especially used for highly secure transactions such as contactless mobile payments and ticketing. In this section the modulation and coding techniques used by NFC are explained.

(i) *Modulation*

Like the RFID standards 14443 and FeliCa, NFC uses inductive coupling. The operating frequency is 13.56 MHz, and commonly a bit rate of 106 kbps (partly also 212 kbps and 424 kbps) is used. Modulation schemes used by NFC are ASK (Amplitude Shift Keying) with different modulation depth (100% or 10%) and load modulation:

- In the case of data transmission *from the initiator to the target* such as an NFC enabled mobile phone in card emulation mode, the target device uses 13.56 MHz carrier signal of the initiator device as energy source. The modulation scheme of the initiator device is ASK modulation. In peer-to-peer mode, both directions are modulated and coded like an initiator device. However, less power is required because both active NFC devices use their own power supply, generate their own RF field, and the carrier signal is switched off at the end of transmission.
- In the case of data transmission *from the target to the initiator,* due to the coupling of the coils of initiator and target devices, the passive target device also affects the active initiator device. A variation in the impedance of the target device causes amplitude or phase changes on the antenna voltage of the initiator device, which is detected by the initiator device. This technique is called load modulation. Load modulation is carried out in listening mode using an auxiliary carrier at 848 kHz which is modulated by the baseband and varies the impedance of the target device.

(ii) *Coding*

NFC employs three different coding techniques to transfer data: *NRZ-L, Manchester*, and *Modified Miller coding* (see Figure 3.19):

- In NRZ-L coding: a high state during one bit duration refers to logic 1 and a low state refers to logic 0.
- In Manchester coding: at logic 1, the first half of a bit is set to high state, and the second half of that bit is set to low state. At logic 0, the first half of a bit is set to low state and the second half is set to high state.
- In Modified Miller coding: at logic 1, a low pulse occurs after half of the bit duration. At logic 0, a low pulse occurs at the beginning of a bit. If logic 0 comes after logic 1, no pulse occurs at logic 0, hence the signal remains high.

In Manchester and Modified Miller coding schemes a single data bit is sent in a fixed time slot. This time slot is divided into two halves, called half bits. In Miller coding a 0 is encoded

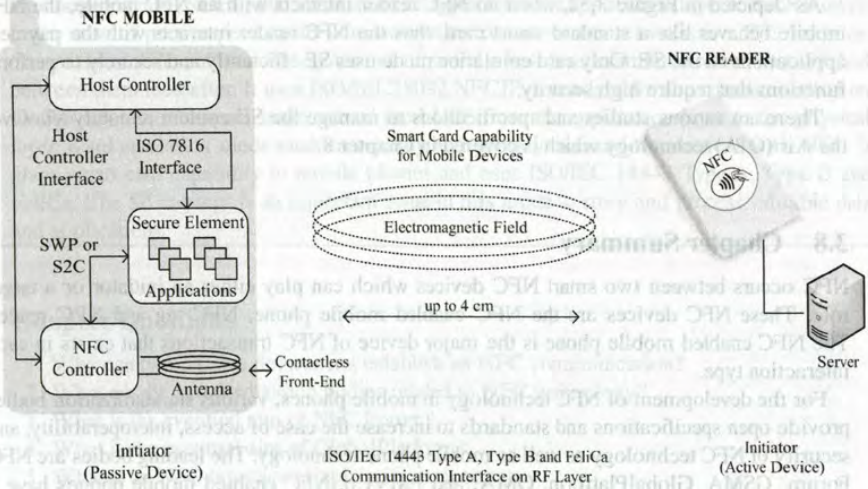

Figure 3.32 Communication architecture of card emulation operating mode.

3.7 Card Emulation Operating Mode Essentials

In card emulation mode, the NFC enabled mobile phone acts as a smart card. Either an NFC enabled mobile phone emulates an ISO 14443 smart card or a smart card chip integrated in a mobile phone is connected to the antenna of the NFC module. As the user touches her mobile phone to an NFC reader, the NFC reader initiates the communication. The communication architecture of this mode is illustrated in Figure 3.32.

3.7.1 Protocol Stack Architecture of Card Emulation Mode

NFC devices that are operating in card emulation mode use similar digital protocol and analog techniques as smart cards and they are completely compatible with the smart card standards (see Figure 3.33). Card emulation mode includes proprietary contactless card applications such as payment, ticketing and access control. These applications are based on ISO/IEC 14443 Type A, Type B and FeliCa communication interfaces.

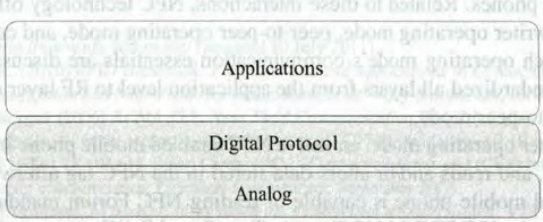

Figure 3.33 Protocol stack of card emulation operating mode.

the development stage. One type is a GUI (Graphical User Interface) application which must be present for all operating mode applications and provides both a GUI for the user and the capability to read NFC components. The second type is a Secure Element (SE) application which is needed in order to provide a secure and trusted environment for applications requiring security such as payment, ticketing and authentication in SEs.

Reader/writer mode and peer-to-peer mode applications generally consist of only the GUI application since those operating modes do not require any secure operations. In Java language, MIDlets are the Java applications running on the mobile phone and provide the stated properties.

On the other hand, SE applications are used for card emulation mode applications. Card emulation mode applications consist of both GUI and SE components. These applications interact with NFC readers and MIDlets installed on a mobile phone. In Java language, Applets are JavaCard applications running on SEs or smart cards.

There are various development tools on the market and the user may choose the appropriate development tool for the targeted mobile phone, since applications are mobile phone dependent. For an Android mobile case for example, the application should be developed using Android SDK which can be downloaded from http://developer.android.com/. For a Symbian 3 mobile, the application should be developed with Qt SDK. This SDK can be downloaded from http://qt.nokia.com/.

SDKs also provide mobile phone simulators. Inside a simulator, tags can be created and edited. After the application development phase, the application should be transferred to actual mobile devices and should be tested in a real time environment. Applications can be installed on a mobile phone by connecting it to a computer using wired connection or Bluetooth or alternatively it can be installed online via an Internet resource.

Two JSRs (Java Specification Requests) are developed under the Java platform to enable NFC based applications. JSR 257 (Contactless Communication API) is for mainly reader/writer mode programming and JSR 177 (Security and Trust Services API) is for card emulation mode programming. JSR 257 is mainly concerned with discovering contactless targets in the proximity, notifying applications upon discovery, and performing tag operations. JSR 177 supports communication with smart card applications and also provides application level digital signature signing, user credential management, and cryptographic operations.

5.2 Why Java?

5.2.1 Why did we Choose Java?

To develop NFC applications easily in any platform, an NFC programming language should provide the fundementals of NFC programming and should serve as a basis role for readers. There are different NFC application development platforms currently available. New ones may also arise in the future.

We have chosen Java as the programming language; since it is widely used and is a well-known programming language. It also provided one of the first APIs in NFC technology. Nokia 6212 and Nokia 6131 NFC SDKs are development platforms that are able to work with JSR 257 and 177 which provide NFC programming in Java. Although those phones are outdated, the main function of this chapter is to give a basic knowledge of NFC programming. Learned NFC programming skills from Java technology will help users easily develop NFC

IPR2025-01151
Apple EX1021 Page 24

(vi) *Bouquet of services*

The aim of this service is to provide multiple services to users within a single platform. For this purpose, the Oulu city card is used in different service entities to provide multiple services such as payment, event ticketing and transportation ticketing.

(vii) *Learning*

In order to support learning, several projects are being conducted. The aims of these projects cover:

- Improving learning through growth in motivation at school;
- Adding a sense of community through sharing and commenting on learned information;
- Improving communication between school and parents.

There are also other projects being conducted including smart sports, mobile math, multipurpose tagged cities, interoperable student cards, social networking and NFC solutions for mobile workers in the public sector. The projects also implement the following solutions to technical problems:

- Subscription to services;
- Unsubscribing to services;
- Application provisioning;
- Credit card payment;
- Multiple payment cards;
- E-purse payment;
- Access control and ticketing;
- Exchange tickets;
- Locking and unlocking an application;
- Deleting an application;
- Losing phone;
- Profile creation and edition.

9.2 NFC Trials and Projects

As already mentioned, there have been various NFC trials and projects throughout the world. Payment and ticketing applications are possibly the most well-known and promising everyday applications of NFC technology, and are the most complex from the ecosystem aspect as well. Thus most of the tests and trial projects are implemented in this application domain. In addition to the NFC cities, this section tries to present and illustrate different NFC projects in different countries. Some of these projects have been completed, or expanded into different application domains with growing participating entities, or still continue.

9.2.1 Contactless Payment Trials

(i) *Visa payWave payment pilot in Malaysia*

A short, but successful case comes from Malaysia that was launched at April 2006. The MNO Maxis Communications, Maybank which is the largest bank and financial group in Malaysia, and Visa collaborated to implement an NFC enabled payment in Malaysia. This is the world's first mobile Visa payWave payment pilot. It was implemented in the capital of Malaysia, Kuala Lumpur, involving about 2000 merchants and

200 participants. Participants were selected from Maybank Visa cardholders and Maxis mobile network subscribers. Other vendors that took part in this pilot were Vivotech for NFC enabled contactless terminals or readers, and NXP Semiconductors for NFC chip set and embedded hardware based secure elements (SEs) for mobile handsets. This payment trial had a big part to play in the commercial roll out of NFC services in Malaysia in April 2009 [7,14].

(ii) *HSBC trials in USA*

Another case comes from a global banking and financial services company. HSBC launched an NFC enabled mobile payment pilot in partnership with MasterCard in January 2007 in the USA. This pilot lasted for 6 months, and tested the use of NFC enabled mobile handsets in payment. The payment service was used where payment by contactless credit card and MasterCard PayPass was accepted. About 36 000 merchants accepted the MasterCard PayPass payment option at that time. More than 200 bank employees in New York, Chicago and several other large US cities used the OTA installation and personalization process to download HSBC credit card information on their NFC enabled mobile phones. The application itself and TSM platform was provided by Vivotech. Nokia 3220 NFC enabled mobile handsets were used with embedded hardware based SEs. These SEs and NFC chip sets were supplied by NXP Semiconductors [7,14].

(iii) *Payez Mobile project*

The Payez Mobile project is a joint initiative launched in November 2007 [12, 13]. It is a wide mobile payment service pilot implemented with about 1000 testers and 500 retailers in Caen and Strasbourg. It involves four MNOs (i.e., Bouygues Telecom, NRJ Mobile, Orange, and SFR), eight leading French banks (i.e., BNP Paribas, Crédit Agricole, LCL, Crédit Mutuel, CIC, Groupe Caisse d'Epargne, La Banque Postale, and Société Générale), Visa and MasterCard. This project combines the capabilities of the named organizations and also makes use of technologies developed in the ITEA SmartTouch project.

The contactless payment service provided by Payez Mobile is fully compatible with the existing Visa and MasterCard international specifications. Moreover, MasterCard and Visa applications can be hosted simultaneously in the same SE. The global objective of the participants in the Payez Mobile trial is to create a common vision, namely, a business solution for banks and MNOs in the contactless payment application domain.

Technically, the Payez Mobile experiment relies on the combination of four issues. The first issue is that payment applications provided by banks are installed on multi-application enabled UICC based SE of the mobile phone. The second issue is that NFC technology is used only in handling the payment service from the NFC enabled mobile device to the merchant terminal. The third issue is that Single Wire Protocol (SWP) is used for managing communication to UICC based SE from the NFC interface. Finally, advanced OTA mechanisms are required to deploy multiple applications remotely. The providers of UICC based SEs and secure OTA platforms are Gemalto and Obertur Card Systems. In addition, the NFC enabled mobile phones used in the project are the Motorola L7, Sagem My700, and LG L600V.

This contactless mobile payment service uses the existing bank card infrastructure. The payment methods are defined by Payez Mobile. The first method is for amounts less than 20 euros, so that if customers wish, they can pay without using a PIN. The second

IPR2025-01151
Apple EX1021 Page 26

(v) *EZ-Link and StarHub trials in Singapore*

A subsidiary of the land transport authority, EZ-Link, processes more than 4 million financial transactions daily in Singapore and issues millions of cards. EZ-Link launched an NFC enabled ticketing trial with the MNO StarHub in October 2007 which lasted for 6 months. Throughout the trial, about 20 000 terminals were used which accept Singapore's transit purse, EZ-Link. These terminals were generally on trains and buses, however they can also be found in some retail stores, restaurants, and vending machines [7].

The StarHub and EZ-Link Singapore trial was the world's first NFC FeliCa trial providing ticketing as well as smart poster services. Users can touch tags located on smart posters to download URLs, coupons or other promotional content. Users can also check their purse balance, transaction history and other details from a mobile device.

The other partners of this transit ticketing trial were Vivotech as the NFC reader supplier and NXP Semiconductors as the provider of NFC chip set for mobile phones. The trial was implemented with more than 800 users who had used specially designed NFC enabled mobile phones provided by Sony with embedded FeliCa SEs.

According to the trial's results, if the technology is offered, 23% of post-trial survey respondents said they would be "very likely" to adopt the technology. Another 45% of the respondents said that they would be "likely" to adopt the technology. Another important result is that about 83% of users used their phones during the trial to pay for transit fares, and about 70% of users checked their transaction histories [7].

(vi) *Pay-Buy-Mobile trial in Australia*

A Pay-Buy-Mobile (see Chapter 7) pilot was performed in Australia with participation of Australia's largest MNO Telstra, National Australia Bank and Visa (payWave). The pilot was launched in August 2008 and lasted for 3 months. About 500 users and 12 merchants participated in this small pilot. The users were generally from the Telstra and National Australia Bank staff.

Telstra provided and issued SIM based SEs for users. Payment application of the National Australia Bank and Visa was installed on SIMs of Sagem my700X NFC enabled mobile phones. The other vendors were Inside Contactless for NFC chip set in mobile phones, Vivotech for NFC readers in the merchant stores and Cassis International for TSM business solutions. With this pilot, users could touch to the NFC readers for purchases of $35 or less. According to the results of Telstra, about 95% of trial participants said that they would be "likely" or "extremely likely" to use the NFC technology in the future [7].

(vii) *ING Bank trial in Romania*

The Dutch bank ING and MasterCard (PayPass) tested the viability of NFC technology in mobile payment systems for low value purchases in Romania. The trial was launched in November 2008 and lasted for 7 months. The trial involved many MNOs in Romania and only one TSM platform provided by Venyon.

This trial was one of the first which enabled users to top up and check their contactless MasterCard PayPass account balances via OTA with a special code. This trial was also the first for ING Bank and MasterCard in Romania. They worked with the payments technology vendor Collis, OTA service platform provider for NFC payments Venyon and Taiwan based NFC outfit Toro on the project [7].

NFC enabled payment terminals were established at about 11 stores including fast food restaurants, cinemas, and newsagents. About 360 bank customers participated in the trial with Nokia 6212 NFC enabled mobile phones which have embedded SEs where the payment application was installed.

(viii) *Cep-T Cuzdan Launch in Turkey.*

Another good NFC launch case comes from Turkey. Garanti Bank, Yapı Kredi Bank and the MNO Turkcell collaborated in the NFC enabled mobile-wallet service. The service is launched commercially in 2011 [7].

Turkcell brought the NFC enabled Android phone (U8650NFC Sonic) to the market as Turkcell T20. Turkcell preloads the mobile wallet software to the mobile phone which also supports more than one bank-issued application. The phone supports the single wire protocol standard, enabling secure applications to be stored on SIM cards. Turkcell also supports its mobile wallet flexible antennas for the mobile phones those do not have NFC capability.

Turkcell is also serving as TSM to download and manage secure applications in its wallet. The TSM platform is built in-house. Two payment applications from two of Turkey's largest privately owned banks are available currently.

9.2.2 *Transport or Other Ticketing Trials*

(i) *NFC public transport ticketing with RMV in Hanau*

RMV (Rhein-Main-Verkehrsverbund) is one of the largest regional public transport authorities in Europe that provides transportation service for five million inhabitants in the state of Hess, Germany. Nokia, and Vodafone as one of the largest MNOs together with a public transport authority for Frankfurt's greater area, RMV, performed a joint project in the NFC enabled transport ticketing service domain. The trial started in early 2005 with about 200 users [7].

In this trial, RMV customers used Nokia 3220 NFC enabled mobile phones which have a smart NFC shell where tickets are stored to access a local bus network in Hanau, a city near Frankfurt. The RMV electronic ticketing application is securely stored on an integrated smart card controller in the mobile phone.

According to the first survey results, NFC enabled mobile phones are seen as more attractive and innovative than smart cards. Many pilots have been done with other operators and third parties. The service expanded into broader applications, including information, loyalty, and payment application domains with growing number of users. Currently, NFC ticketing with RMV is commercially available with loyalty programs. For example, Nokia NFC enabled mobile phones can also be used as a bonus card called the "RMV ErlebnisCard".

(ii) *NFC stadium experience in Manchester*

The MNO Orange UK performed a trial of contactless ticketing services with Manchester City Football Club. This small trial was launched in August 2006 with about 20 users who held valid season tickets. Nokia 3220 NFC enabled mobile phones with embedded hardware based SEs were used. Manchester City Football Club and Orange UK provided a ticketing application for these devices. The participating fans were allowed to use their NFC enabled mobile phones to touch to the NFC readers at the gates of the Manchester City football ground and enter the turnstiles easily [7].

(iii) *Bouygues Telecom trials in Paris*

France's major MNO Bouygues Telecom performed a 3-month NFC enabled transit ticketing trial in Paris. This trial was launched in November 2006. About 50 users participated in this trial. The main service providers were RATP (Régie Autonome des Transports Parisiens) and SNCF (Société Nationale des Chemins de fer Français) who are the providers of Navigo contactless transit fare cards. They provided an NFC enabled ticketing application which was loaded and installed on the user's SIM based SE. This trial's aim is to enable users to pay for fares at gates or at readers on buses which accept the Navigo ticketing application using their NFC enabled mobile phones.

Users also could recharge their cards over the mobile internet service. Bouygues Telecom provided an NFC enabled mobile phone from a Japanese mobile handset manufacturer, NEC, which was specially designed for the trial. Other vendors involved were Axalto/Gemalto as the SIM based SE provider and Inside Contactless as the NFC chip set provider. This first trial by Bouygues Telecom led to subsequent transit ticketing and payment pilots in France [7].

(iv) *O2 Wallet*

Telefonica O2, as one of the largest MNOs, announced O2 Wallet in November 2007 and performed a 6-month trial in conjunction with various service providers, namely, TfL (Transport for London), TranSys who operates the Oyster smart card for TfL, Venyon for TSM business solutions, Barclaycard, Visa Europe (payWave), Nokia, Giesecke & Devrient for data management, Innovision for smart poster tags, NXP Semiconductors, Inside Contactless, Consult Hyperion for consulting, and AEG Europe. O2 Wallet included many services from transport ticketing to smart poster applications, and was the UK's first large scale NFC pilot [7,15].

O2 Wallet pilot paved the way for the large usage of mobile phones as Oyster cards for travel around London, paying for purchases by Barclaycard and accessing events. About 500 O2 mobile network subscribers participated in the pilot and they were equipped with Nokia 6131 NFC enabled mobile phones. Embedded hardware based SEs were used in the pilot. The user only needs to store an NFC enabled Oyster application on her mobile phone and preload her application. This application eliminates the need for users to carry Oyster smart cards in their wallets. Users can pay for their travel expenses through the Oyster application by simply touching their mobile phones to the Oyster NFC readers at London underground tube stations, and on buses and trams (see Figure 9.8). If the user's phone rings while making a transaction, she can still answer the call. A call or text message does not interfere with the NFC service.

In addition to the preloaded ticketing application in O2 Wallet, payment, smart poster and access control applications are enabled by the service providers. The payment service is provided by Barclaycard who introduced the first credit card in the UK and Visa payWave for O2 Wallet. Users were able to make payments with their Barclaycard payment application installed on their mobile phones. This payment application can be used at about 5000 merchants including Books Etc., Chop'd, Coffee Republic, EAT, and Krispy Kreme.

Users could also touch to smart posters to gather information on restaurants and other locations. The tags on smart posters serve as shortcuts for services enabled through the mobile phone. For example, when a user touches a tag on a smart poster, she can automatically dial a number, send a text message or view a website containing information

IPR2025-01151
Apple EX1021 Page 29

Figure 9.8 O2 Wallet [1]. Photographed by Juha Sarkkinen, The City of Oulu, Smart Touch Project.

about an event, and so on. Another important service of O2 Wallet is access control. Users can access and enter the VIP area of O2 entertainment venues using their NFC enabled mobile phone.

According to the results from conducted surveys after the O2 Wallet pilot, more than half of the participants said that if contactless services were available, they would use them on their mobile phones. About 90% of the participants were satisfied with NFC technology, and again a large majority said that touching mobile phones is more convenient than using Oyster smart cards. Currently, there is a lot of work being done to expand the services of O2 Wallet. The pilots and trials are leading O2 Wallet to a commercial launch.

(v) *Orange trials in Spain*

Another transit ticketing trial was launched in April 2008 in Malagna. This was a small trial that tested fare collection on buses with about 50 users. The partners in this pilot were the EMT as the transit fare collection provider, and France Telecom-Orange Spain as the MNO. The NFC enabled mobile phones supplied by Sony were the Sony Ericsson Z750i. The application was stored on SIM based SEs and was provided by Oberthur Technologies. This was Orange Spain's first NFC pilot in the NFC based ticketing application domain [7].

9.2.3 Other Trials

(i) *London Fashion Week trials*

An attractive and innovative case was implemented by one of the largest MNOs, Telefonica O2, in the UK. O2 organized and performed a small trial in February 2008 at London Fashion Week which is the key event for designers in London to show their designs to fashion buyers from around the world. The aim of this trial was to provide fashion buyers the opportunity to give instant feedback to the collection of Emilio de la Morena. This NFC enabled messaging trial was performed with a limited number of buyers or users.

IPR2025-01151
Apple EX1021 Page 30

Near Field Communication

From Theory to Practice

Vedat Coskun, Kerem Ok and Busra Ozdenizci
NFC Lab – Istanbul, ISIK University, Turkey

This book provides the technical essentials, state-of-the-art knowledge, and standards of Near Field Communication (NFC). The NFC-Lab Istanbul research centre conducts intense research on NFC technology.

In this book, the authors present contemporary research on all aspects of NFC, addressing related security issues as well as various business models. In addition, the book provides information and guidance for designers wanting to design a NFC project, programmers looking to implement applications, and analyzers wishing to analyze requirements of a new NFC based system. Furthermore, the authors introduce the technical and administrative issues related to NFC technology, standards, and global stakeholders. It also offers use case studies for each NFC operating mode offering an insight into their usage. Examples of NFC application development are provided using JAVA technology, and security considerations are discussed in detail.

This book will be an invaluable guide for business and ecosystem analysts, project managers, mobile commerce consultants, system and application developers, mobile developers and practitioners. It will also be of interest to researchers, software engineers, computer scientists, information technology specialists including students and graduates.

Companion Website

www.wiley.com/go/coskun

Key Features:

- Offers a complete understanding of the NFC technology, including standards, technical essentials, operating modes, application development with Java, security and privacy, business ecosystem analysis
- Provides analysis, design as well as development guidance for professionals from administrative and technical perspectives
- Discusses methods, techniques and modeling support including UML, demonstrating them with real cases
- Contains case studies such as payment, ticketing, social networking and remote shopping

Also available as an e-book

Enjoyed this book?
Why not tell others about it and write a review on your favourite online bookseller.

ISBN 978-1-119-97109-2

9 781119 971092

WILEY
wiley.com