DESIGNING INNOVATIVE APPLICATIONS USING NEAR FIELD COMMUNICATION (NFC) TECHNOLOGY

BÜŞRA ÖZDENİZCİ

B.A., Business Administration Işık University, 2009

B.S., Information Technology Işık University, 2010

Submitted to the Graduate School of Science and Engineering
in partial fulfillment of the requirements for the degree of
Master of Science
in
Information Technology

IŞIK UNIVERSITY

2012

IŞIK UNIVERSITY

GRADUATE SCHOOL OF SCIENCE AND ENGINEERING

DESIGNING INNOVATIVE APPLICATIONS USING NEAR FIELD COMMUNICATION (NFC) TECHNOLOGY

BÜŞRA ÖZDENİZCİ

APPROVED BY:

Assoc. Prof. Dr. VEDAT COŞKUN _____
(Thesis Supervisor)

Prof. Dr. İBRAHİM SOĞUKPINAR _____

Assoc. Prof. Dr. HACI ALİ MANTAR _____

APPROVAL DATE: 26.01.2012

DESIGNING INNOVATIVE APPLICATIONS USING NEAR FIELD COMMUNICATION (NFC) TECHNOLOGY

Abstract

Nowadays, there is a growing interest on rapid development and adoption of information technologies (IT) especially in contactless smart cards and mobile communication technologies. Near Field Communication (NFC) technology has become one of the promising technological developments in IT industry as well as one of the attractive research areas. NFC technology is a short range, high frequency, low bandwidth and wireless communication technology based on Radio Frequency Identification (RFID) technology, which simplifies and secures the interaction with ubiquitously around people. NFC ecosystem is designed from synergy of several technologies including mobile devices, smart cards, secure elements (SEs), Over-the-Air (OTA) technology, and mobile applications; hence it enables a variety of services with a dynamic environment. The aim of this study is to present NFC Loyal and NFC Internal applications with a comprehensive analysis of the NFC technology in aspects of technical, operational as well as business. NFC Loyal aims to promote loyalty and payment services on multi-application smart cards through a secure model. In case of NFC Internal, a reliable and low cost indoor navigation system is designed by taking advantages of NFC technology. This study gives valuable insights on the NFC technology's development and adoption.

YAKIN SAHA İLETİŞİMİ TEKNOLOJİSİ İLE YENİLİKÇİ SERVİSLERİN GELİŞTİRİLMESİ

Özet

Günümüzde bilgi teknolojilerinin, özellikle temassız akıllı kartlar ve mobil iletişim teknolojilerinin, hızlı gelişimine ve benimsenmesine yönelik artan bir ilgi söz konusudur. Yakın Saha İletişimi (NFC) teknolojiside IT sektöründe gelecek vaadeden teknolojik gelişmelerden ve aynı zamanda önemli araştırma alanlarından biri olmuştur. NFC teknolojisi kısa menzilli, yüksek frekanslı, düşük bant genişliğine sahip ve Radyo Frekanslı Tanımlama (RFID) teknolojisine dayanan kablosuz bir iletişim teknolojisidir. NFC teknolojisi insanların çevresiyle olan etkileşimini basitleştirmekle beraber güvence altına almayı hedefler. NFC ekosistemi birçok teknolojinin ve platformun bir arada çalışması üzerine tasarlanmıştır; bunlar başlıca mobil cihazlar, akıllı kartlar, güvenli elemanlar (SEs), Over-the-Air (OTA) teknolojisi ve mobil uygulamalardır. Bu yüzden NFC ekosistemi yüksek sayıda uygulamaya ve servise olanak sağlayan dinamik bir yapıdan oluşur. Bu çalışmanın amacı; iki yenilikçi NFC uygulamasının; NFC Loyal ve NFC Internal'ın kapsamlı bir NFC teknolojisi analizi ile sunulmasıdır. NFC Loyal sadakat ve ödeme servislerinin uygulamalı akıllı kartlarında güvenli bir model ile geliştirilmesini hedeflemektedir. NFC Internal ise, NFC teknolojisinin desteği ile düşük maliyetli ve güvenilir bir iç mekan navigasyon sistemi sağlamaktadır. Bu çalışma NFC teknolojisinin ilerleme ve gelişme süreci hakkında değerli bilgiler vermekte ve öngörülerde bulunmaktadır.

Acknowledgements

I am sincerely grateful to my major professor and supervisor Assoc. Prof. Dr. Vedat Coşkun for his immense knowledge, encouragement and support in my graduate education and thesis. Also, I would like to thank all of my faculty staff and Kerem Ok for their support in my graduate study. Finally, I would like to thank my dear parents and my brother for their patience and motivation.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AMI	Ambient Intelligence
APSD	Application Provider Security Domain
BIP	Bearer Independent Protocol
CAD	Computer-Aided Design
CASD	Controlling Authorities' Security Domain
CPU	Core Processor Unit
DR	Dead Reckoning
DTD	Document Type Definition
ECMA	European Computer Manufacturers Association
ETSI	European Telecommunications Standards Institute
GPS	Global Positioning System
GSM	Global System for Mobile
GSMA	GSM Association
HCI	Host Controller Interface
ICC	Integrated Circuit Card
IEC	International Electrotechnical Commission
ISD	Issuer Security Domain
ISO	International Organization for Standardization
IT	Information Technology
LLCP	Logical Link Control Protocol
MEMS	Micro Electro-Mechanical Sensors
MMS	Multimedia Message Service
MNO	Mobile Network Operator
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NFCIP-1	Near Field Communication Interface and Protocol-1
NFCIP-2	Near Field Communication Interface and Protocol-2

NFC-WI	NFC Wired Interface
OS	Operating System
JCP	Java Community Process
OMA	Open Mobile Alliance
OTA	Over-the-Air
RF	Radio Frequency
RFID	Radio Frequency Identification
RTD	Record Type Definition
SAR	Segmentation and Reassembly
SCD	Secure Common Domain
SCDM	Secure Common Domain Manager
SCDMS	Secure Common Domain Management System
SE	Secure Element
SMC	Secure Memory Card
SMS	Short Message Service
SWP	Single Wire Protocol
TMB	Trusted Mobile Base
UICC	Universal Integrated Circuit Card
UWB	Ultra Wide Band
XML	Extensible Markup Language

Chapter 1

Introduction

With the introduction of ubiquitous computing and Ambient Intelligence (AmI) visions, technology is started to become more *"invisible, embedded, and is enabled by simple interactions, attuned to all our senses and adaptive to users and contexts"* [1]. Today, increasingly objects in our everyday environment are associated with services. Increasing mobility of computing devices provided by mobile communications is becomes an important step in the development of ubiquitous computing.

Mobile phones already had several communication options with the external environments before the introduction of Near Field Communication (NFC) technology. When the mobile phones were initially introduced, their primary goal was to enable communication among mobile phones. Global System for Mobile (GSM) communication enabled functionality of mobile phones for several services, such as voice communication, Short Message Service (SMS), Multimedia Message Service (MMS) and Internet access. Then Bluetooth technology was introduced to create personal area wireless networks that connect peripherals with computing devices including mobile phones.

Currently a new way of interaction approach by NFC technology which is *touching paradigm* has been in question in our daily lives. This interaction can be identified as *"the deliberate bringing together of two devices, for the purpose of obtaining services"* [2]. NFC as one of the enablers for ubiquitous computing is a "*combination of contactless identification and interconnection technologies*" [3] which requires touching two NFC compatible devices to each other in few centimeters (up to 4 cm). User first interacts with a smart object which is either an NFC tag, NFC reader or another NFC enabled mobile phone, using her NFC mobile. After the touching

occurs, NFC mobile can make use of received data, or can use provided mobile services such as opening a web page, making a web service connection etc.

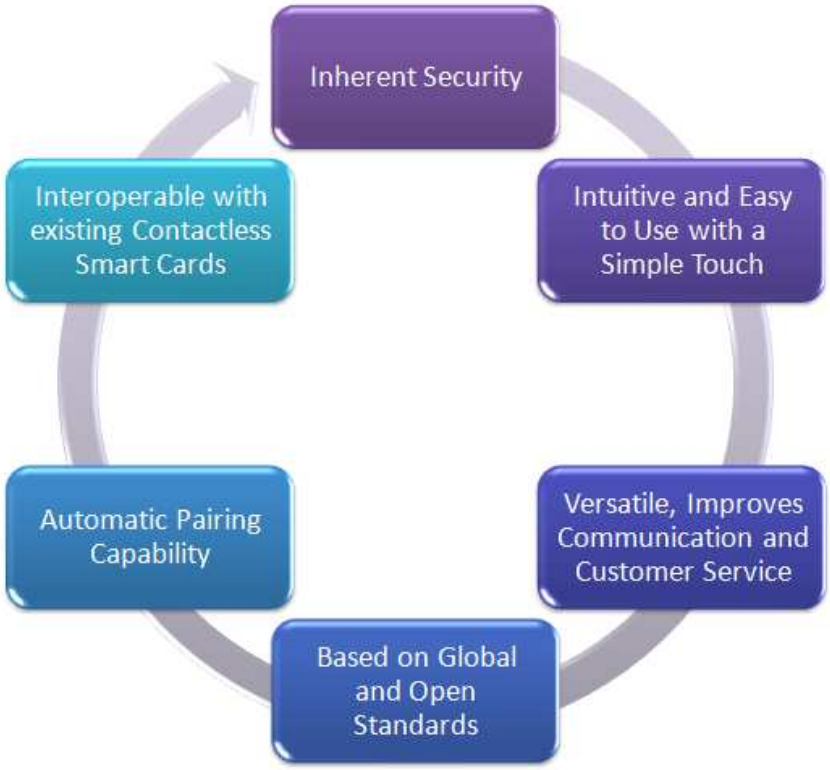

Figure 1.1. Key Benefits of NFC Technology

Up to now, many NFC trials have been conducted over the world, especially in payment application domain. All trials conclude the fact that with the development of NFC technology, mobile phone is subject to become safer, more convenient, speeder and more fashionable physical instrument.

NFC technology allows people to integrate their daily use cards such as loyalty, debit and credit cards into their mobile phones. Actually secure storage of the personal and private information such as credit card or debit card data within mobile phones is essential in which security and privacy issues become important concerns. However in NFC, interaction of two devices in close proximity makes the signal interception probability very low, which provides NFC technology an implicit security feature (Figure 1.1).

In addition to integrating those cards into mobile devices, NFC technology brings innovations to mobile communications. It enables two users to exchange data simply

by touching two mobile phones each other. Furthermore NFC technology gives NFC reader capability to mobile phones; hence they can read and get valuable information stored on passive tags.

Beside novel applications and services, NFC technology has a great potential in business opportunities; hence it has impressed many organizations with a great excitement from Mobile Network Operators (MNOs) to transport authorities and financial institutions. At this point, it is important to drive cooperation of all participating organizations within NFC ecosystem to enable sustainable business models which is essential for technology's acceptance and adoption on customer side.

In this study, we propose and design two innovative NFC applications called NFC Loyal and NFC Internal. We present their technical requirements, architectures and generic usage models. Also NFC technology is presented in a holistic approach. The motivation behind this study is to identify the gap between practice and theory, give some insights about the technology's development, and expose potential research areas.

The remainder of this study is organized as follows:

- Chapter 2 consists of information on communication essentials of NFC technology, operating modes, innovative applications, importance of secure elements (SEs), Over-the-Air (OTA) functionalities as well as brief information on NFC ecosystem and business models.
- Chapter 3 presents a promising service model called NFC Loyal for promoting NFC enabled loyalty and payment services on a single smart card.
- Chapter 4 presents an innovative, low cost indoor navigation system called NFC Internal with usage models.
- Chapter 5 provides conclusion of my thesis.

Chapter 2

Near Field Communication Technology

NFC technology was jointly developed by Philips and Sony in late 2002 for contactless communications, and Europe's ECMA International adopted the technology as a standard in December 2002. ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) adopted NFC technology in December 2003. In 2004, Nokia, Philips, and Sony founded the NFC Forum to promote the technology. Currently, NFC technology standards are acknowledged by ISO/IEC, ETSI (European Telecommunications Standards Institute), and ECMA (European Computer Manufacturers Association).

NFC is a short range, half duplex communication protocol based on Radio Frequency Identification (RFID) technology which provides easy and secure communication between NFC compatible devices. However NFC is distinct from far field radio frequency (RF) communication used in personal area and longer range wireless networks. NFC uses inductive coupling between transmitting and receiving devices, and the communication occurs within few centimeters with 13.56 operating frequency (Table 2.1).

In NFC, RF interface supports communication at data rates of 106, 212 as well as 424 kbps. The communication between two NFC devices is standardized in ISO/IEC 18092 standard as Near Field Communication Interface and Protocol-1 (NFCIP-1) and ISO/IEC 21481 standard as Near Field Communication Interface and Protocol-2 (NFCIP-2) [4, 5]. NFCIP-1 standard defines only device to device communication for both active and passive communication modes. However, RF layer of NFC is a super set of the standard protocols which is also compatible with the ISO/IEC 14443 standard (i.e. contactless proximity smart card standard) and JIS X 6319 standard as FeliCa (i.e. another contactless proximity smart card standard by Sony) as well as ISO/IEC 15693 standard (i.e. contactless vicinity smart card standard). These smart

card interfaces similarly operate at 13.56 MHz from card reader to card with distinct data rates and communication ranges [6].

NFC uses different modulation schemes (i.e., ASK with 100% or 10% modulation depth or load modulation) and coding techniques (i.e., NRZ-L, Manchester and Modified Miller coding) to transfer data. In each NFC transaction, the mode of NFC devices, the signaling type and standards used in RF interface (NFCIP-1, ISO/IEC 14443, JIS X 6319 Type F as FeliCa), and the data transfer rate is important in defining the modulation and coding scheme [6].

Table 2.1. Comparison of WPAN Technologies [7, 8]

Parameter	**Bluetooth**	**Zigbee**	**NFC**
Range	10-100 m	10-100 m	4-10 cm
Data Rate	0.8-2.1 Mbps	0.02-0.2 Mbps	0.02-0.4 Mbps
Cost	Low	Low	Low
Power Consumption	High	Medium	Low
Spectrum	2.4 GHz	2.4. GHz	13.56 GHz
Security	Low	Low	High
Network Topology	Piconets, Scatternets	Star, Tree, Mesh	One to one
Personalization	Medium	Low	High
Flexibility	High	High	High

2.1 Communication Essentials

NFC occurs between two NFC compatible devices, and these two NFC devices can operate in several modes. In device point of view, if a device generates its own RF field, it is called as an active device; if a device can not generate its own RF field, it is called as a passive device (Table 2.2). In terms of communication modes, they are distinguished based on whether each device has embedded power source. In the active mode of communication, both devices generate their own RF field to carry the

data. In the passive mode of communication, only active device generates the RF field while the passive device uses load modulation to transfer the data.

Table 2.2. Active vs. Passive Communication Mode [9]

Device A	**Device B**	**RF Field Generation**	**Communication Mode**
Active	Active	Both devices	Active Mode
Active	Passive	Device A only	Passive Mode
Passive	Active	Device B only	Passive Mode

In addition, there are two different roles that a device can play in NFC which can be illustrated as a *request and reply* concept as illustrated in Figure 2.1. Initiator is the device that initiates and controls the exchange of data. Target is the device that answers the requests from initiator.

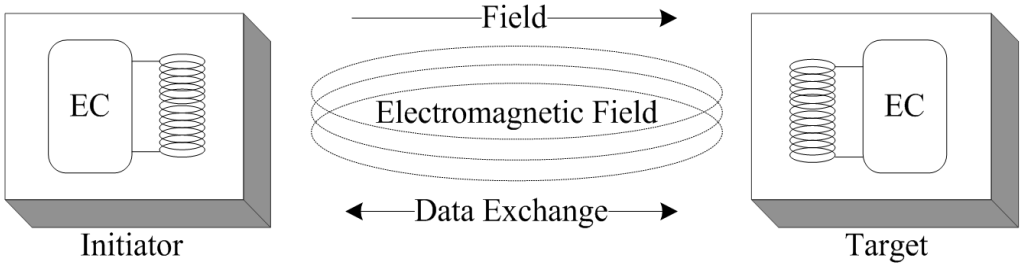

Figure 2.1. Communication between Initiator and Target

Table 2.3 shows the possible combinations of initiator/target roles with respect to active/passive roles for a device. An active device can become both an initiator and a target. However a passive device cannot be an initiator.

Table 2.3. Combinations of Active/Passive Device with Initiator/Target Device

Device Role	**Active Device**	**Passive Device**
Initiator	Possible	Not Possible
Target	Possible	Possible

2.1.1 NFC Devices

As mentioned, communication occurs between two smart NFC devices. These NFC devices are NFC enabled mobile phone, NFC tag, and NFC reader. Table 2.4 shows the possible interaction styles among the NFC devices.

Each interaction style enables different operating modes of NFC technology which can be reader/writer mode, peer-to-peer mode, and or card emulation mode. For instance, in reader/writer mode communication occurs between an NFC mobile on one side, and a passive RFID tag (NFC tag) on the other side; the NFC mobile reads the information stored on an NFC tag or writes information onto an NFC tag. Each operating mode uses distinct communication interfaces (i.e. ISO/IEC 14443, FeliCa, NFCIP-1 interfaces) on RF layer as well as has different technical and design requirements.

Table 2.4. Interaction Styles of NFC Devices and Operating Modes

Initiator Device	**Target Device**	**Operating Mode**
NFC Mobile	NFC Tag	Reader/Writer Mode
NFC Mobile	NFC Mobile	Peer-to-Peer Mode
NFC Reader	NFC Mobile	Card Emulation Mode

2.1.2 General Architecture of NFC Mobile

NFC enabled mobile phone is the most important element of an NFC based system. NFC mobile typically composed of various integrated circuits, secure elements (SEs) and NFC interface as illustrated in Figure 2.2. NFC interface within a mobile phone is composed of a contactless, analogue/digital front-end called NFC Contactless Front-end (NFC CLF), an integrated circuit called NFC controller to enable NFC transactions as well as an NFC antenna.

An NFC enabled mobile phone has at least one SE which is connected to the NFC controller for performing secure proximity transactions with external NFC devices. SE provides a dynamic and secure environment for programs and data. It enables storage of valuable and private data such as credit card information of user, and

secure storage and execution of NFC enabled services such as contactless payments. Also more than one SE can directly be connected to the NFC controller. The supported common interfaces between SEs and NFC controller are Single Wire Protocol (SWP) [10] and NFC Wired Interface (NFC-WI) [11].

The host controller is the heart of any mobile phone. Host Controller Interface (HCI) creates bridge between NFC controller and host controller [12]. An ISO/IEC 7816 interface supports the linkage of SEs to host controller. The host controller sets the operating modes of the NFC controller through HCI, processes data that is sent and received, and establishes a connection between NFC controller and SE.

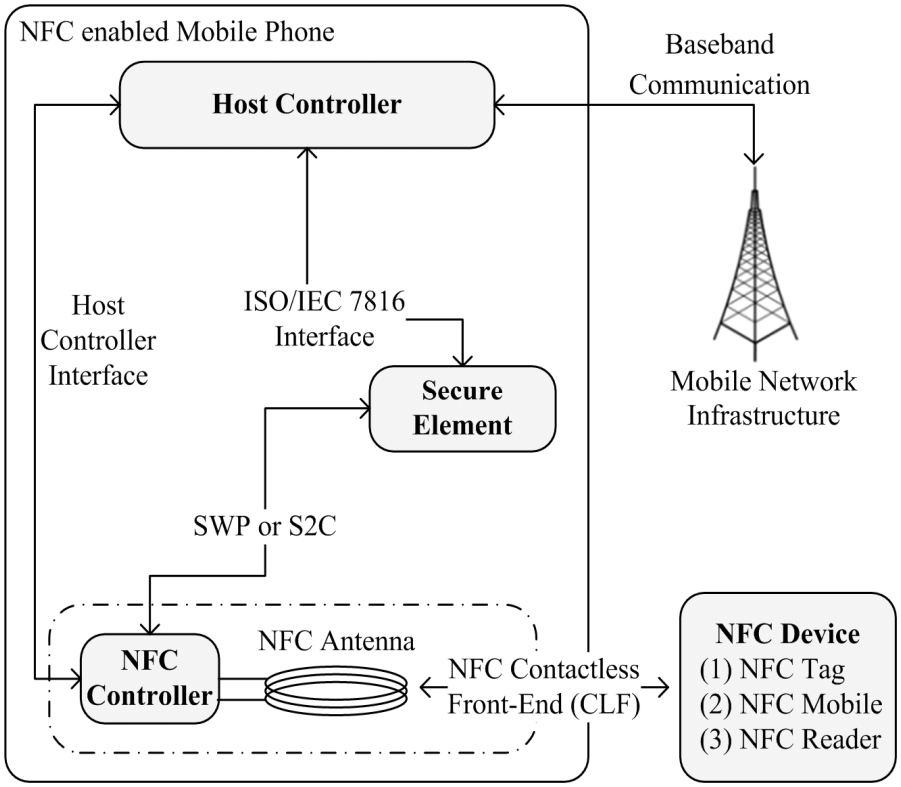

Figure 2.2. General Architecture of NFC enabled Mobile Phones

2.2 Standardization in NFC Ecosystem

As discussed, NFC technology benefits from various elements such as smart cards, mobile phones, card readers, payment systems etc. All these elements need to acquire accreditation from an assortment of governing bodies that have the responsibility for security and interoperability of various NFC devices. As mobile phones became best

solution for NFC technology especially for secure transactions, various standardization bodies defined how the NFC technology should be integrated to mobile phones and other related devices. Some other bodies defined supportive architectures and specifications for the security as well as the suppotive technologies for NFC mobiles such as smart cards for NFC transactions. The common vision of all standardization bodies is increasing the ease of access, interoperability and security for NFC technology.

Table 2.5. Some Standardization Bodies within NFC Ecosystem

Standardization Body	**Role**
NFC Forum	Promotes the usage of NFC technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology
GSM Association (GSMA)	Provides MNO vision for mobile NFC solutions by identifying technical options and providing recommendations
GlobalPlatform	Develops specifications that facilitate secure and interoperable deployment and management of multiple applications on secure smart cards
NXP Semiconductors	Co-inventor of NFC technology along with Sony, participates in and supports development of NFC
Mobey Forum	Non-profit, global, financial industry-driven forum who encourages the use of mobile technology in financial services
Smart Card Alliance	Non-profit association who works to stimulate the understanding, adoption and widespread application of smart card technology
StoLPan	Association who contributes to the establishment of an open, interoperable NFC service environment
Open Mobile Alliance (OMA)	Develops open standards for mobile phone industry and supports the development of mobile service enabler specifications and the creation of interoperable end-to-end mobile services
Java Community Process (JCP)	Holds the responsibility for the development of Java technology and guides the development of Java technical specifications

2.3 NFC Operating Modes and Applications

There are three operating modes reader/writer, peer-to-peer and card emulation modes as already mentioned. Reader/writer mode enables one NFC mobile to exchange data with one NFC tag. Peer-to-peer mode enables two NFC enabled mobiles to exchange data with each other. In card emulation mode, a mobile phone can be used as a smart card to interact with an NFC reader. Each operating mode has different technical infrastructure as well as benefits for the users.

NFC Forum standardized only two operating modes (reader/writer and peer-to-peer operating modes) from the application layer to the RF layer (Figure 2.3). For reader/writer mode, Record Type Definition (RTD) and NFC Data Exchange Format (NDEF) specifications are being used. Within peer-to-peer mode, Logical Link Control Protocol (LLCP) is used to connect peer-to-peer based application to RF layer, while card emulation mode provides smart card capability for mobile phones.

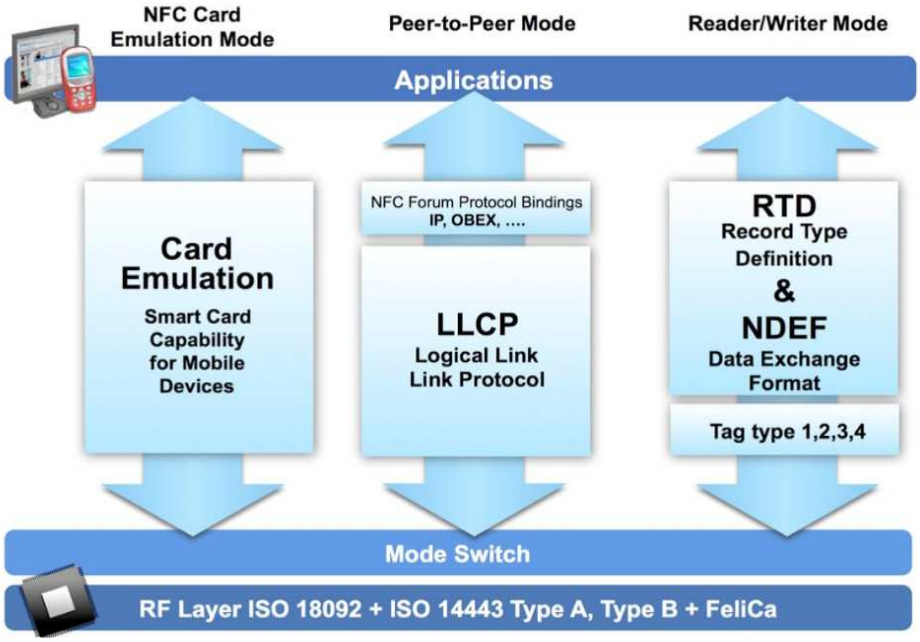

Figure 2.3. NFC Forum Technical Architecture

2.3.1 Reader/Writer Operating Mode

Reader/writer operating mode is the communication of an NFC mobile with an NFC tag for the purpose of either reading or writing data from or to those passive tags as

depicted in Figure 2.4. This mode internally consists of two modes; reader mode and writer mode. In reader mode, the initiator reads data from an NFC tag. NFC tag should have a pre-loaded program which performs returning the requested data to the initiator as well. In writer mode, the mobile phone writes data to an NFC tag. Reader/writer mode's RF interface is compliant to ISO/IEC 14443 Type A, Type B and FeliCa schemes. This mode usually does not need a secure area, in other words SE of an NFC enabled mobile phone.

NFC Forum standardized four types of NFC tags (i.e., Tag Type 1, Tag Type 2, Tag Type 3, and Tag Type 4) which can store valuable information [13]. In addition to NFC forum mandated tag types, NFC Forum has standardized data exchange format as NDEF between components. NDEF is a data format to exchange information between NFC devices [14]; between active NFC device and passive tag, or active NFC device and active NFC device. When an NFC device is in proximity of an NFC Forum mandated tag, NDEF message is received from NFC tag, as well as NDEF message transfer can be used over NFC Forum LLCP which is described in peer-to-peer mode communication essentials. The data format is same in both cases.

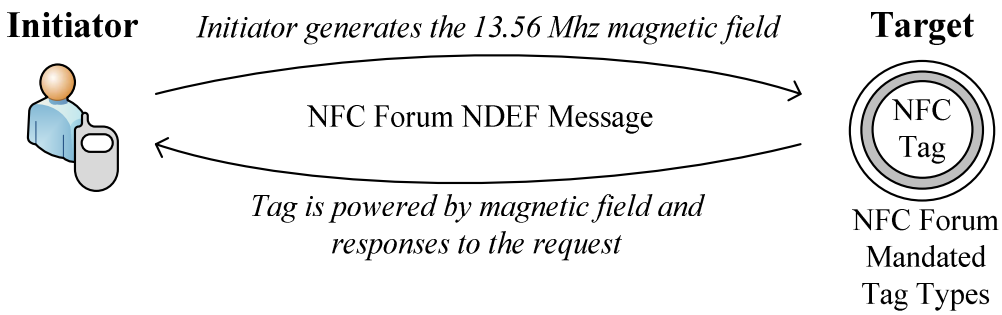

Figure 2.4. Reader/Writer Operating Mode

NDEF is a binary message format that encapsulates one or more a*pplication defined payloads* into a single message as illustrated in Figure 2.5. An NDEF message contains one or more NDEF records. Each record consists of a payload up to 2^{32}-1 octets in size. Records can be chained together to support larger payloads. Various record types for NDEF messaging format are defined by NFC Forum. The record type string field contains the name of the record type as record type name. Record type names are used by NDEF applications to identify the semantics and structure of the record content. Record type names may be MIME media types, absolute URIs,

NFC Forum external type names or well-known NFC type names [15]. Each RTD is identified by its record type name.

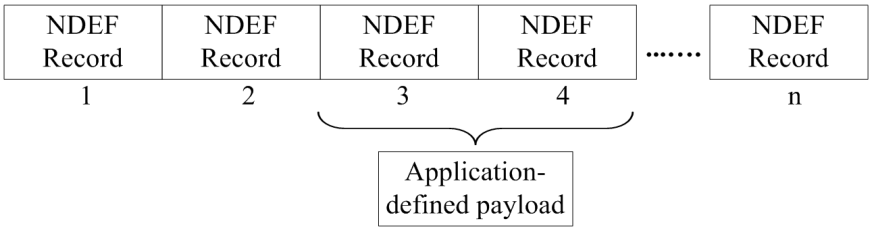

Figure 2.5. NDEF Message Structure

Reader/Writer Mode Applications: The most challenging application can be performed in this mode is the transfer of valuable information which can be a URL, phone number, news, product identification, advertisement or some other type of data. After the transfer operation, data can be used for many purposes by the mobile phone. Smart posters with NFC tags are the common way of providing those information services (Figure 2.6).

Up to now, high number of scenarios, proposals and demonstrations have been performed in this mode. This mode can be used in creating context aware and smart environments, controlling mechanisms remotely, supporting health services and education services and so on.

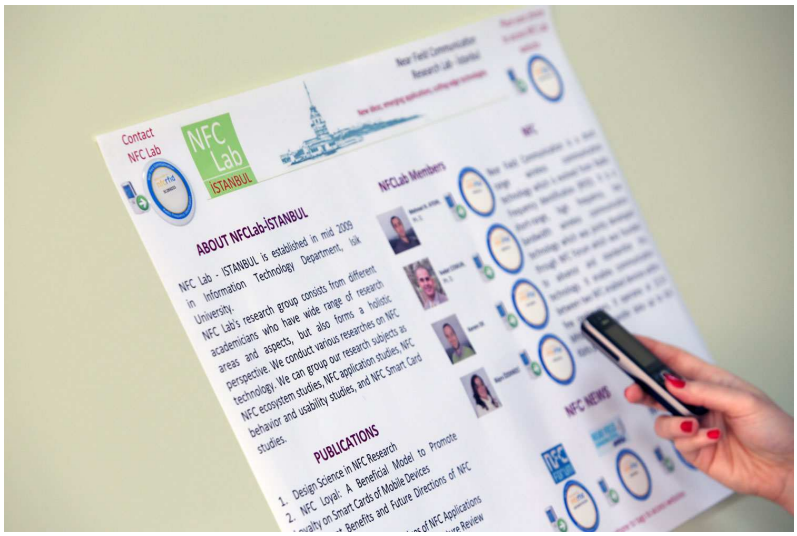

Figure 2.6. NFC Lab-Istanbul Smart Poster

Table 2.6 Examples for Reader/Writer Mode Applications

Application & Reference	**Description**
Remote Meal Ordering [17]	Enables users to easily benefit from NFC based catering service by making daily meal orders with a simple touch on NFC enhanced menu
Retail Support [18]	Allows customers to simply touch a product such as such as Audio CDs, DVDs or books that are tagged in the retail shop to receive a preview of the product's content on NFC mobile
Remote Grocery Shopping [19]	Provides a new way of grocery shopping process; touching based remote process. Whenever a customer wants to do her shopping, she can prepare a shopping list on her NFC mobile by simply touching tagged items she wants to buy.
Remote Controlling Services [20, 21, 22]	Enables remote control of services such as control of multimedia players through NFC tags placed in an environment. When a user touches an NFC tag which is a control icon, a control event is sent to the corresponding service. So, the service processes the event.
NFC Museum [23]	Facilitates interaction between visitors and works of art that are tagged. User can easily get information about the corresponding work of art by touching the tag on it.
News-on-the-Go [24]	Supports collection of news content by simply touching an information poster on the go. Such posters may be placed in public spaces like at train stations.
All-I-Touch [25]	Provides a mobile phone interface together with a cross-vendor online platform and a Facebook application. Users can touch pieces, places and people with their NFC mobile in order to inform friends what they touched, get product information at the point of sale, receive comments from their friends and share their own opinion.
MyState [26]	Provides a way for users to make the environment interactive by using Facebook application. By touching tagged physical objects with NFC mobile, a user can quickly publish information to the virtual world.
TaggyNet [27]	Brings two new features into social media networks: an advertising service and a location based service. Also a business model and a marketing appeal has presented in this study.

Especially creating smart environments is the most usage areas of this operating mode. Smart environments are usually performed by NFC tags that are distributed in different places. In accordance with [16], "*tags can provide support in user's everyday life activities by establishing a bridge between the physical and the digital worlds when they are ubiquitous in the everyday environments of users*" and "*the tags become an integral part of physical space, altering the way humans perceive and behave in it*".

City of Oulu project [16] in Finland is a good example which explores the use of NFC tags in a mixed of reality environment and user experiences. In this project, NFC tags distributed throughout the city which provide diverse services from bus timetable information to accessing information about play performances and cast of a theatre. It is possible to see other significant examples for smart environments such as Nice Future Campus, Smart Urban Spaces.

Table 2.6 presents some challenging applications from literature that are operating in reader/writer mode. Some of these applications are prototyped, demonstrated as well as evaluated in terms of usability as well.

2.3.2 Peer-to-Peer Operating Mode

This operating mode enables two NFC mobiles to exchange or share information such as contact records, virtual business cards, digital photos, text messages, or any other kind of data (Figure 2.7). Because of embedded power within mobile phones, both devices are in active mode during the communication in peer-to-peer mode. Two active devices establish a bidirectional half duplex channel to exchange information. This mode's RF interface is standardized by NFCIP-1 which enables *request and reply* model between devices.

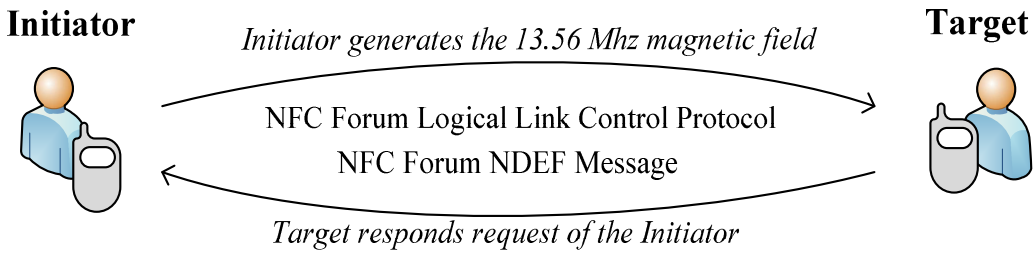

Figure 2.7. Peer-to-Peer Operating Mode

NFCIP-1 protocol provides a SAR (Segmentation and Reassembly) capability as well as data flow control depending on the Go & Wait principle usual for half duplex protocols. Furthermore, NFCIP-1 protocol allows error handling by using accept (i.e., ACK frame) and reject frame (i.e., NACK frame), and provides an ordered data flow. It provides a reliable and error free link layer [6].

In addition to NFCIP-1, a new data link layer protocol is standardized by NFC Forum to support peer-to-peer communication between two NFC enabled devices. LLCP is essential for any NFC application that involves in a bi-directional communication.

According to [28], it provides five important services; connectionless transport, connection oriented transport, link activation, supervision and deactivation, asynchronous balanced communication and protocol multiplexing. LLCP provides a solid ground for peer-to-peer applications and enhances the basic functionalities provided by NFCIP-1 protocol as well.

Peer-to-Peer Mode Applications: As mentioned, this mode is generally used for device pairing, networking, and file transfer operations (Figure 2.8). Peer-to-peer mode provides easy and secure data exchange between two NFC mobiles. Pairing Bluetooth devices, exchanging business cards, gaming are possible implementations of this mode.

Furthermore NFC technology is an enabler for social networking tools that can be integrated with the existing social network applications (e.g., Facebook, Twitter, LinkedIn) by making use of peer-to-peer operating mode. Hot-in-the-City [29], VisiExchange [30], Pass the Bomb and Exquisite Touch games [31] are some examples operating in this mode in literature.

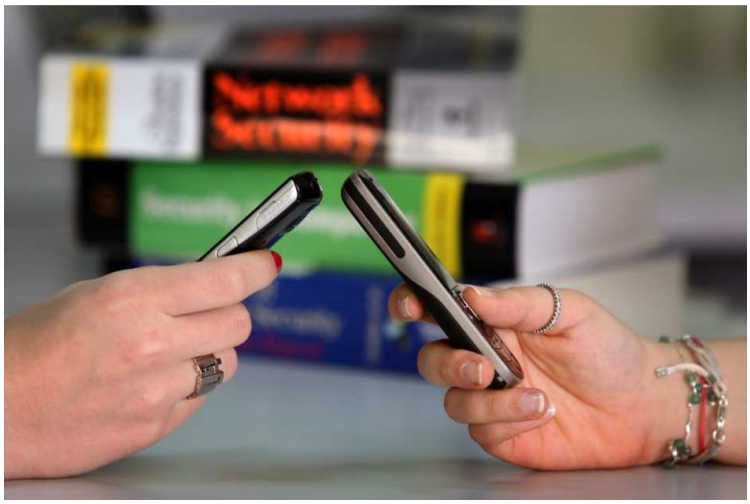

Figure 2.8. Secure Data Sharing

2.3.3 Card Emulation Operating Mode

This mode provides opportunity for an NFC mobile to function as a contactless smart card such as a credit card, debit card or a loyalty card. One NFC mobile may even store multiple contactless smart card applications concurrently on a single SE as smart card within NFC mobile. NFC devices use similar digital protocol and analogue techniques with smart cards, and they are completely compatible with the smart card standards that are based on ISO/IEC 14443 Type A, Type B and FeliCa smart card standards.

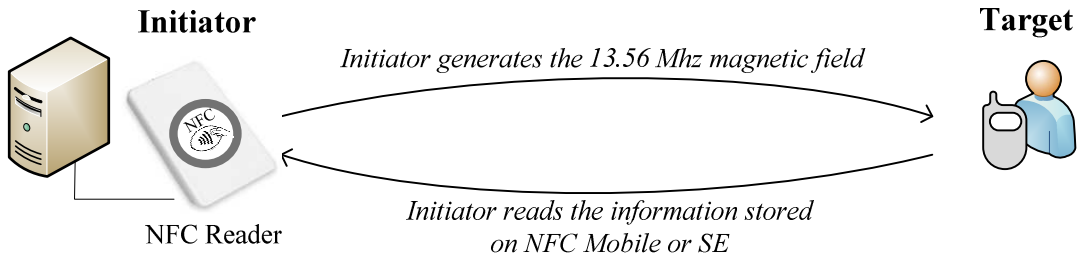

Figure 2.9. Card Emulation Operating Mode

As the user touches her NFC mobile to an NFC reader (Figure 2.9), NFC mobile behaves like a standard smart card, thus NFC reader interacts with the related application on the SE. Only card emulation mode uses SE efficiently and securely which performs functions that require high security.

Card Emulation Mode Applications: Card emulation mode is an important mode since it enables payment, ticketing, loyalty and similar applications that have high business value for all participating entities. Also this mode enable identification and access control mechanisms. The main motivation of this operating mode is to integrate all payment cards, keys, tickets, transport cards, access cards and so on into mobile phones.

Up to now, various pilots and projects on finance service domain have been performed with different technical infrastructures and business models over the world. Some of the challenging examples are Payez Mobile [32], Pay-Buy-Mobile [33]. Today, there is a big effort on commercial roll-out of NFC enabled payment systems in some countries; the aim is to perform a single, interoperable technical platform for all NFC services with a sustainable business model nationwide.

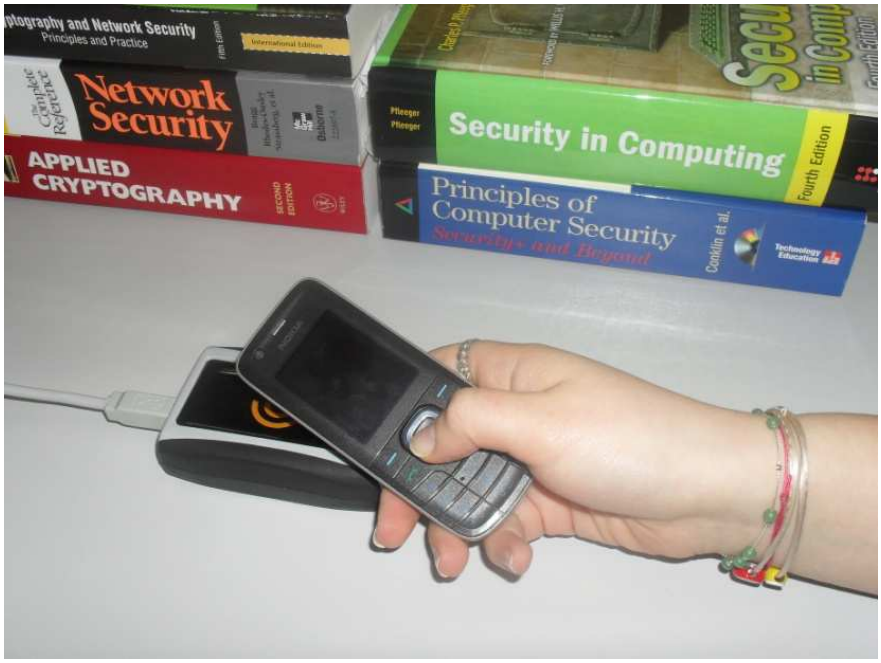

Figure 2.10. Interaction with NFC Reader

In terms of academic point of view, some studies have been performed as well as fruitful usability and user experience analyses in payment and payment related application domains. Some examples are:

- Automated reservation and ticketing service for tourists, and a system for car parking access and payment system for ticketing [34, 35],
- Virtual ticketing system and secure mCoupon system [36, 37, 38],
- Payment service by Smart Touch [39],
- NFC Ticketing system including usability testing [40],
- Offline Tapango system for electronic ticketing process including comparison with traditional paper ticketing process [41],
- Offline NFC payment service with electronic vouchers [42],
- Secure payment system built on a Service Oriented Architecture (SOA) including payment authorization process [43].

2.3.4 Benefits of NFC Applications

Each operating mode enables a variety of NFC services, and these modes provide different benefits for users. A comprehensive literature review on NFC applications and services is performed in study [44]. Characteristics and features of a number of NFC applications are identified, and benefits and impacts of those applications to human life are investigated by classifying them based on NFC operating modes.

The reason behind classification based on operating modes is that every operating mode has its own communication essentials, usage areas and benefits to users. Table 2.7 summarizes the explored benefits of operating modes depending on the reviewed applications, and presents the possible future scenarios for each mode.

2.4 Secure Element

Especially in contactless ticketing, payment and other similar application cases, storing and using valuable and private information (e.g. credit card information) in an unsecured memory of the NFC mobile is an unacceptable case. The data could be transmitted via a GSM interface to a malicious third party. Financial institutions increasingly seek to mitigate the risk of any fraud in order to protect their customers and hence their own company. To solve this issue, relevant NFC applications need to be executed and saved in a protected environment which is the memory of a SE within NFC mobile (Figure 2.11) [45].

Table 2.7 Benefits and Possible Future Scenarios of Operating Modes [44]

Operating Mode	Reader/Writer	Card Emulation	Peer-to-Peer
Benefits	-Increases mobility -Decreases physical effort - Ability to be adapted by many scenarios -Easy to implement	-Physical Object Elimination -Access Control	- Easy data exchange between devices - Device pairing
Future Scenarios	Many real-life scenarios can be adapted to NFC in this mode. In all of the scenarios, some data need to be read from an NFC tag, and additional jobs need to be done by NFC mobile	-Integration of id-cards, passports, finger-prints, driver-license -Storage area for critical information to provide user's privacy and authorizing people to access those information	-Secure exchange of critical data -Social interaction such as gossiping

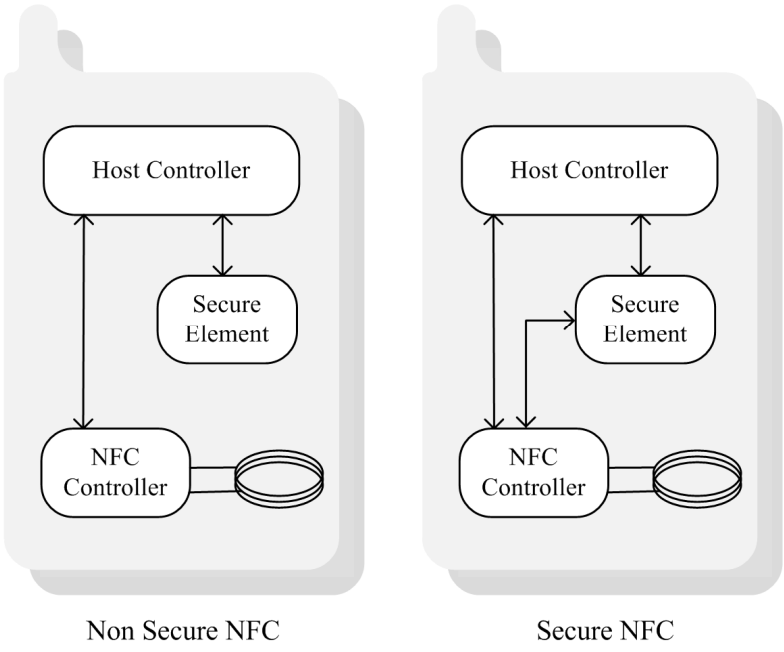

Figure 2.11. Non Secure NFC and Secure NFC

SE is combination of hardware, software, interfaces and protocols embedded in a mobile handset that enables secure storage. SE needs to have an operating system (OS) as usual [46]. OS (e.g. MULTOS, JavaCard OS, etc.) supports the secure execution of applications and the secure storage of application data, and also it may support the secure loading of applications.

2.4.1 Secure Element Alternatives

Up to now, various SE alternatives entered to the market that can enable financial institutions and other companies to offer secure NFC enabled services and empower the NFC ecosystem take off. In accordance with the studies [47, 48], mainly SE options can be grouped under removable ones, non-removable ones, software based SEs on dedicated hardware and other flexible SE solutions. Figure 2.12 shows the possible SE options currently within the NFC ecosystem for each category of SE. Actually understanding the characteristics of these SEs plays significant role for stakeholders and pricing models in the NFC value chain. The dominating SE will have a strong position to build trusted services on it.

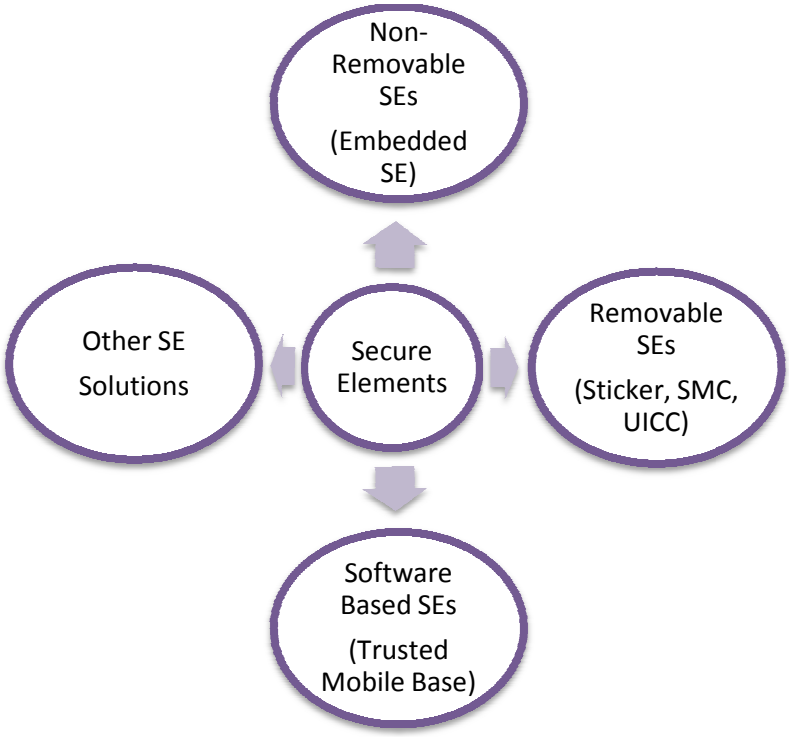

Figure 2.12. Secure Element Alternatives

Embedded SE: This SE alternative is a smart card like hardware integrated with the mobile phone, and it cannot be removed. Thus, the level of security provided by this SE is high [47]. This chip is embedded into the mobile phone during manufacturing stage, and it needs to be personalized after the device is delivered to the end user. Due to its embedded feature on NFC mobile, SE obviously cannot be used in other mobile phones. It should be replaced and personalized every time when the mobile phone is used by another user [47].

Stickers: NFC sticker's aim is to allow service providers to launch pilots quickly and start to deploy NFC services. Stickers are typically contactless cards with specifically designed NFC antenna which are attached on back of mobile phones. There are two types of stickers; active and passive. Active stickers are connected to the mobile phone's application execution environment (i.e., OS), which makes the sticker to become an integrated part of the mobile; whereas passive stickers do not allow dynamic application management since they do not have any connection with the mobile [48]. Active stickers enable all possible NFC services. Also OTA provisioning and life cycle management of those applications are possible because of stickers' connection with the mobile phones. Moreover, user can easily control her applications through user interface.

SMC: Secure memory card (SMC) is made up of a memory, an embedded smart card element and a smart card controller. Thereby, a SMC provides the same high level of security as a smart card, and it is compliant with most of the smart card interfaces and standards (e.g., GlobalPlatform, ISO/IEC 7816 and JavaCard). With the removable property and a large capacity memory, SMC can host several NFC applications [47]. SMC can be inserted in any device supporting NFC technology.

UICC: Universal Integrated Circuit Card (UICC) is a generic multi-application platform for smart card applications where SIM or USIM is implemented upon. It has been standardized by ETSI Project Smart Card Platform with the aim of defining a physical and logical platform for all smart card applications especially for financial services. UICC based SE is issued by one party who is generally MNO, and includes at least one application on the SE. Mainly, it hosts some required applications from UICC issuer such as SIM, USIM (UMTS/3G SIM) applications to authenticate the user in a 3G network and so on. In addition to SIM and USIM applications, UICC

can host non-telecom applications from various service providers such as loyalty, ticketing, healthcare, access control, identification service [47, 48].

Other SE Solutions: Several alternative architectures based on different connections of SEs and NFC interfaces is proposed so far, because of massive lack of NFC mobiles within the market. SE manufacturing companies are performing some hardware improvements on the existing SE solutions, and providing mobile phone independent solutions. Integration of NFC with SIM cards as SIM Application Toolkits, SIM cards or SD cards with only NFC antenna, SIM cards or SD cards with NFC functionality and antenna are some examples for alternative SE solutions. They enable to shorten the time to market of contactless payment and similar applications.

TMB: According to Mobey Forum [48], Trusted Mobile Base (TMB) is a promising upcoming technology and has the full potential of becoming SE in the future that is hosted at the root of the mobile phones. It is a secure isolated section on the Core Processor Units (CPUs) of mobile phones, and it enables OTA provisioning services to security domains. TMB related services can be provided via OTA similar with other SE alternatives. They have no additional hardware costs, since TMB is placed on the CPU.

2.4.2 OTA Technology

Today, MNOs have the ability to remotely configure a single mobile device; send software and OS updates; remotely lock a device to protect the application and the data when it is for example lost or stolen; troubleshoot the device remotely; and additional similar services. OTA technology contributes management of NFC enabled applications and SE life cycle remotely. OTA technology enables loading and installation of new NFC applications on SEs remotely, activation and deactivation SEs, remote service management (i.e. installation, personalization, update, termination) and life cycle management i.e. card block, unblock, re-issuance, PIN reset, change, parameters update) of NFC applications on the SEs and other online services [49].

UICC became the most popular way of promoting NFC services since it is personal, secure, and portable as well as managed easily via OTA technology. With OTA technology, new NFC applications can be delivered to an UICC. This ensures that an

NFC based system is dynamic and able to adapt to a changing environment. New entrants can have their application launched seamlessly, and existing participants can update their applications easily. Because the management is performed via OTA, the consumer does not need to go to a shop physically or connect their handset to a system to update available NFC applications.

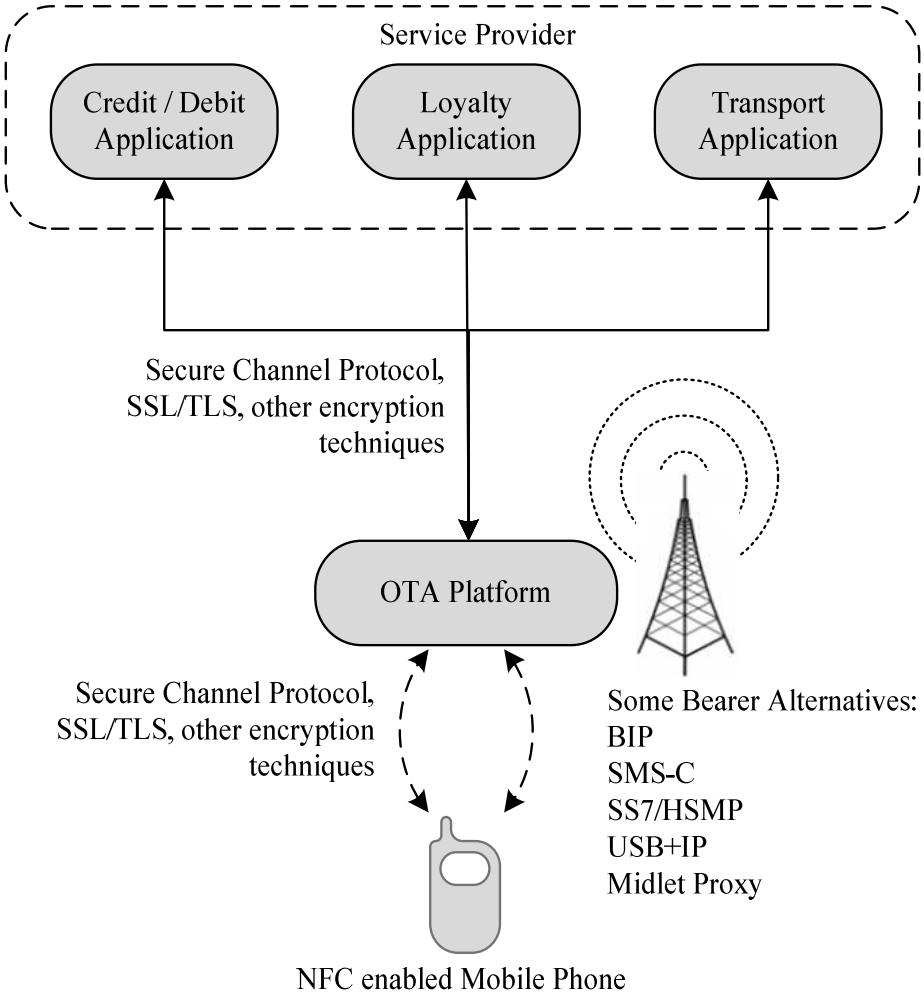

Figure 2.13. Remote SE Management via OTA

For instance, after UICC has been issued to the subscriber or user, it will be necessary to deploy a new NFC application once in a while. Using OTA, SE issuer (i.e., generally MNO) creates a secure space on UICC for the new NFC application, and assigns unique security keys to it. Thereafter application and required data are either downloaded OTA to this newly defined space or copied from a pre-loaded instance of the application on the UICC.

Furthermore, it is possible to lock and/or delete NFC enabled services on UICC, or the entire content of the UICC via OTA, when it has been lost or stolen. This is vital functionality especially for credit card applications. MNO can lock and/or delete all services on the behalf of the NFC service providers.

High capacity bearers those are being used in OTA technology are very important in providing an NFC solution [49]. For example, embedded and SMC based SEs can only be accessed via OTA through MIDlet proxy. This connection requires that the communication is initiated on the mobile handset side, and secure http connection is established using GPRS or 3G communication [50]. Several kilobytes of data needs to be transferred to the UICC based SE when downloading activation data or an NFC application. Using GPRS/UMTS and BIP (Bearer Independent Protocol) protocol, applications are rapidly deployed OTA to the UICC card (Figure 2.13) [49].

2.4.3 Trusted Service Manager

In NFC based systems, TSM is generally required to create and manage a trusted environment among actors of the NFC ecosystem, mainly between service providers and MNOs. Integrating TSM into the ecosystem enables secure communication and interest protection of each entity, and also reduces the complexity of business models.

With respect to providing simplicity on the other hand, each player needs to be in touch with each other which creates complex communication environment when no TSM is used (Figure 2.14). As an alternative, TSM plays a central authority role in such a system and eliminates the complexities (Figure 2.15). TSM generally offers a single point of contact with MNOs for service providers (i.e., financial institutions, banks, transit authorities, retailers and others) who want to provide NFC enabled payment, ticketing, or loyalty services to customers [51].

TSM can provide its own OTA platform and business solutions. This allows sending and loading of NFC enabled applications via its own OTA link to the SE and managing SE platform at the same time. Especially in large NFC based systems, using TSM as a central and neutral trusted entity is a beneficial model.

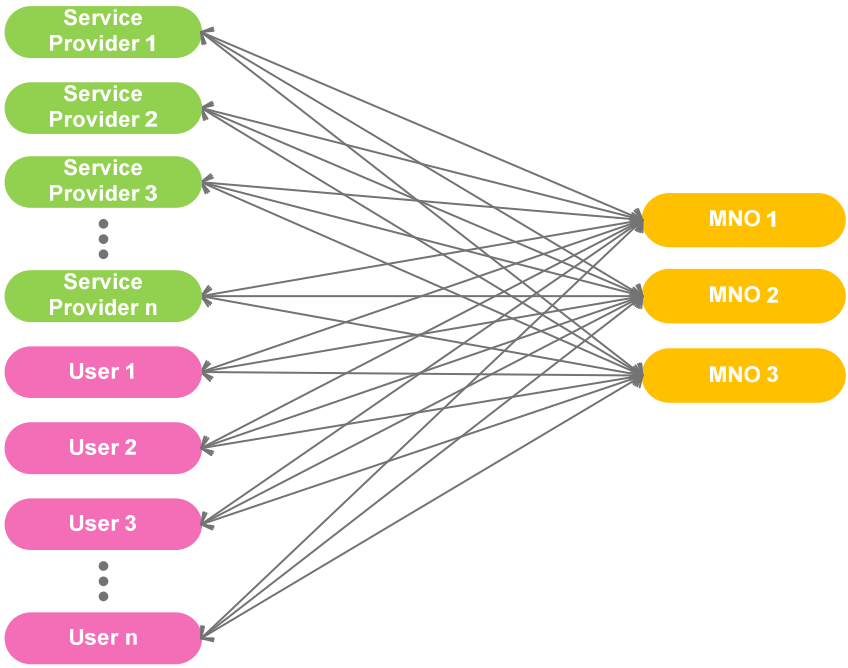

Figure 2.14. NFC Based System without TSM

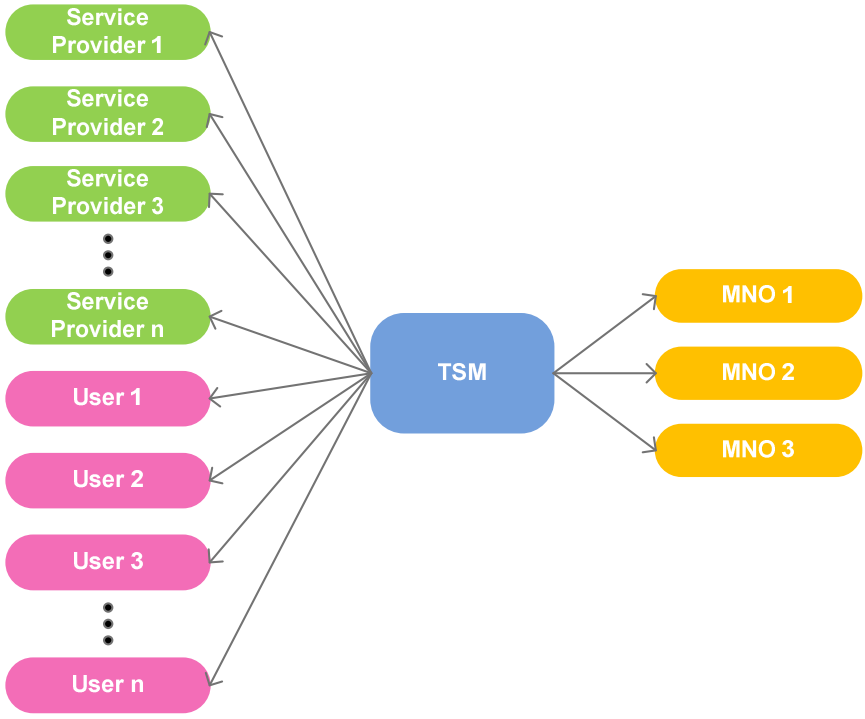

Figure 2.15. NFC Based System with TSM

Actually, the roles of TSM need to be defined and agreed between service providers and MNOs in order to provide efficient mobile NFC services to customers. TSM's role becomes important especially in mobile financial service cases. Major payment

brands as service providers, i.e. MasterCard and Visa, have strict requirements for the organizations those wish to act as TSMs. Many specifications and standards are already published about TSM's role in mobile financial services.

2.4.4 Life Cycle Management of Secure Elements

The life cycle management of SE within NFC mobile starts after issuance of SE to the user. The life cycle can be identified by two phases; installation and personalization process and remote management process. Hence, remote management process starts after installation and personalization of NFC application. Initially card holder downloads an NFC application, the related security domain together with its keys is created, and the application is installed to the SE. Remote personalization process can be performed and new application can be managed (i.e. updated, removed, renewed) remotely thereafter.

UICC based SEs provide great opportunity for extensive customer support via OTA as already mentioned before. Currently the most promising standard for management of multiple applications on the UICC smart cards is provided by GlobalPlatform. In accordance with those standards [52], UICC based SEs provides separate security domains with secret administrative keys for each application, administered by the applications. At the same time, smart card's OS implements a firewall that will prevent applications from accessing or sharing data between them. However, there are still some unsolved issues on UICC card management in NFC based services [53].

Figure 2.16 shows the typical structure of the security domains relating with the actors in NFC based system. Any GlobalPlatform compliant UICC based SE comes with one Issuer Security Domain (ISD) and the option for multiple SSDs (Supplementary Security Domain) [54]. These SSDs can be TSM security domains or application provider security domains (APSDs) for such as credit card, transport, ticket, loyalty applications. Application and data storage areas of TSMs and service providers are separated and isolated from each other. Also, each UICC based SE have only one controlling authority security domain. This architecture enables card issuers, service providers, and TSMs to perform key management and application verification during application loading and personalization processes.

On the ISD area of the UICC, card issuer (which is generally MNO) stores the keys for OTA provisioning, card content and security domain management. The ISD is created during manufacturing and the key for card content management is securely transferred from the manufacturer to MNO [54]. According to GlobalPlatform, ISD must authorize the creation of any SSDs and only ISD has the privileges to create an SSD. Also only ISD can assign authorized or delegated management privileges, which is presented in following section.

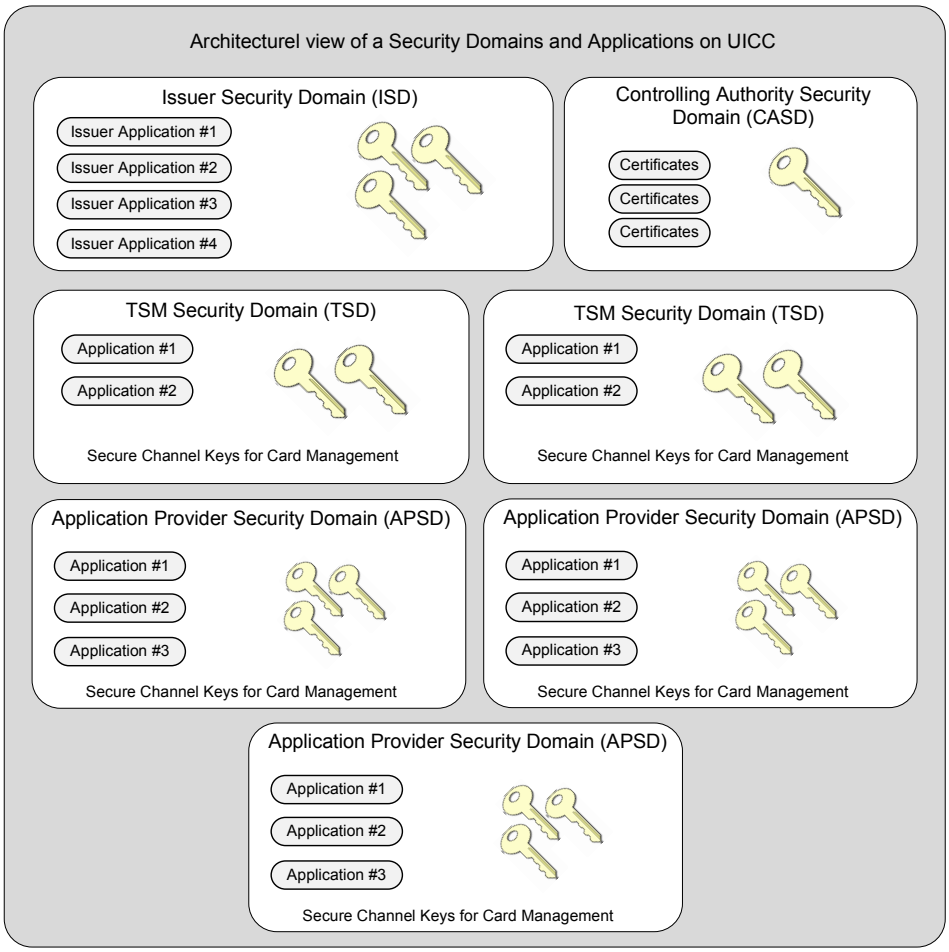

Figure 2.16. Architecture of Security Domains on UICC

2.4.5 UICC Management Models

As mentioned, most reliable proposal on management models of SEs has been provided by GlobalPlatform. According to GlobalPlatform [55], three card content management models (i.e. simple mode, delegated mode and authorized mode) on SE can be performed. These models cover application loading and personalization processes via OTA on UICC cards. Actually these models can be applied for the

other SE options with different infrastructures and requirements. Simple mode is completely card issuer centric model, whereas delegated mode and authorized mode are more TSM centric models.

- **Simple Mode:** In simple mode, the service provider delegate full management of its NFC enabled application to a TSM. TSM manages the security domain on behalf of the service provider. MNO is authorized to perform the card content management functions, i.e. loading, installing, activating and removing the application on the SE. TSM only manage the application lock, unlock and personalization processes using its own OTA server, but using network of MNO.
- **Delegated Mode:** Delegated management case can be described as TSM centric loading. In this case MNO is no more in charge of loading, installing, activating or removing the application. Card content management is performed by TSM with a pre-authorization from MNO. MNO needs to deliver a *management token* to the TSM for a pre-authorized card content management action. This *management token* can be also identified as *load token* which is a digital signature performed only by card issuer. Delegated management privilege allows delegated loading, installation, extradition, update and deletion. Service provider delegate full management of its application to a TSM, and TSM is responsible from the creation of its APSD and the management of its application loading and personalization process. TSM will use its own OTA platform. In some cases, SP may need to manage its own application personalization process to prevent any third party manipulation of application keys or application data which is valuable for their customers.
- **Authorized Mode:** The authorized management deployment is completely organized around the TSM centric loading. TSM has service provider applications and is able to perform card content management without authorization (or being forced to use a token) from MNO. The service provider delegates the card content management of its application to TSM and TSM uses its own OTA platform. As in delegated mode, service provider

may also want to manage its own application personalization instead of delegating it to TSM. In this mode, MNO has no linkage with the end user.

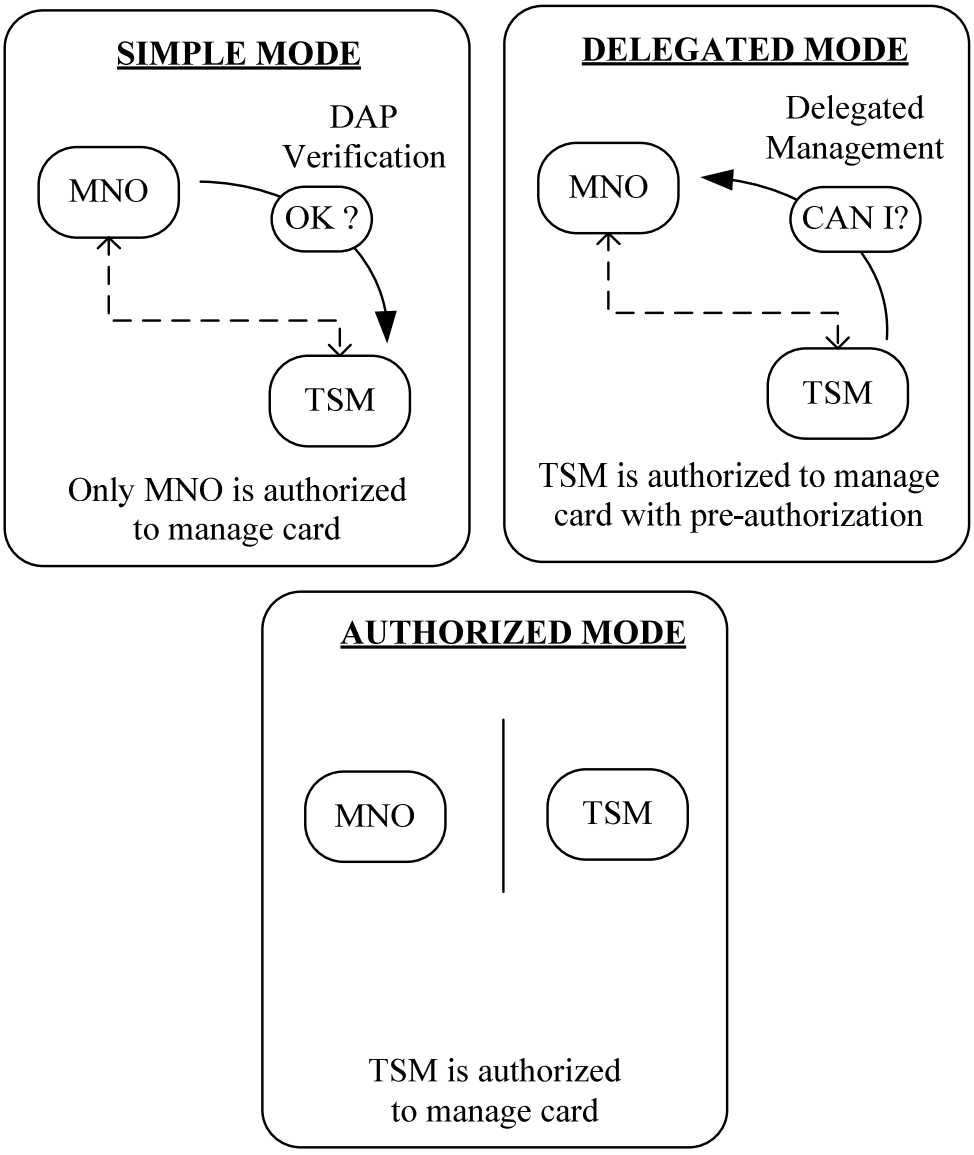

Figure 2.17. Application Management Models [32]

2.5 NFC Ecosystem

From ecosystem point of view, NFC industry has a new emerging business environment and large value chain including several industries and organizations i.e., MNOs, banking and payment services, transport operators, mobile handset manufacturers, NFC chip suppliers, software developers, other merchants including (Figure 2.18). The potential of NFC technology in business opportunities has

impressed many organizations with a great excitement especially organizations in mobile financial services industry.

Since NFC technology is made up of several components, it cuts across boundaries of many organizations from diverse business sectors. All parties have already experienced and agreed the fact that NFC technology cannot be provided by a single firm that could develop all the pieces of the technology. From technical point of view the standardization of NFC technology is already started and major technical decisions taken so far. NFC Forum, currently including more than one hundred members, is one of major organizations in the world who aims to coordinate all participating institutions in development of NFC based projects.

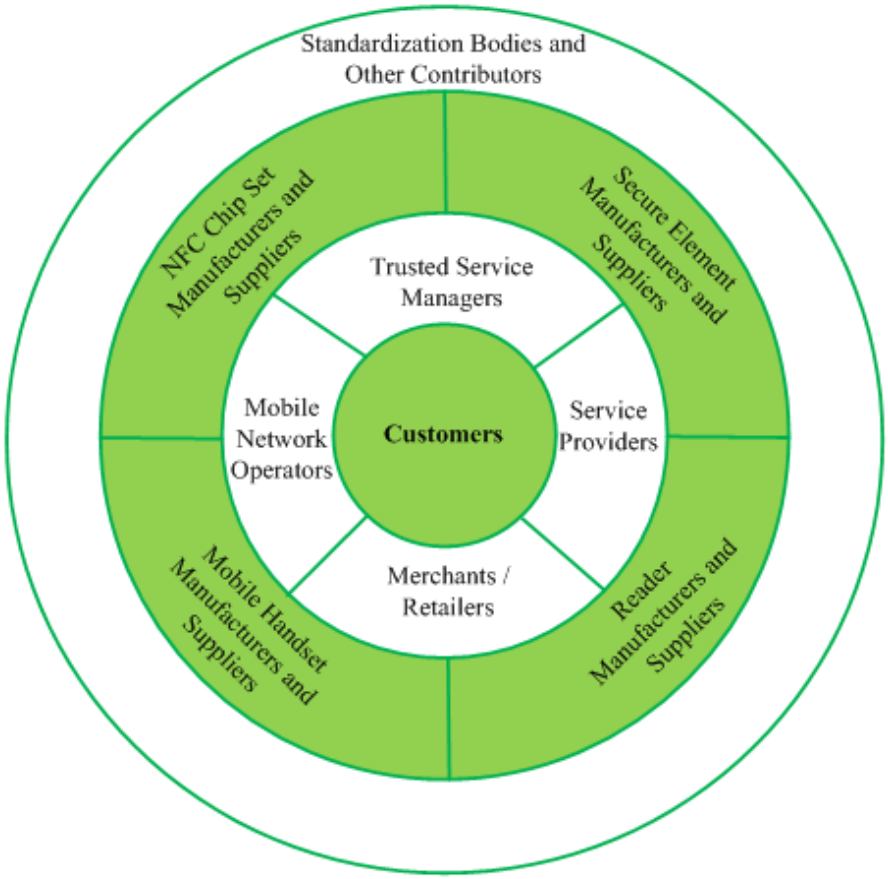

Figure 2.18. NFC Ecosystem

According to participants and observers of the technology, NFC take off has been slower than expected. It is also mentioned in [56] that the business cases and models of NFC technology is still unsure; use cases for the end customer are clear but the structure of the ecosystem as well as its value chain is not yet set. The main reason of this slow take off is mostly related with the formation of a common understanding and vision in NFC technology among participating organizations and industries. Thus a mutually beneficial business model could not have been sustained yet.

2.5.1 Business Model Approaches in NFC Ecosystem

Currently, mobile financial services include high number of business opportunities in NFC context, and also have the highest complexity in both technological and business aspects with respect to other NFC services such as smart poster and social networking services. Vast amount of proposals and approaches have been performed on NFC ecosystem up to now. Some challenging approaches and proposals of industry pioneers are presented here to give basic insights about NFC industry.

GSMA: GSMA is one of the important associations, represents mainly the MNO community. Pay-Buy-Mobile project (i.e., GSMA's one of the important projects in NFC enabled financial services) paved the way for financial service communities to work with MNOs in order to create a common vision within the NFC industry. Pay-Buy-Mobile project triggers adoption of UICC based SEs in NFC enabled mobile services. According to GSMA, UICC is main component of payment business solution as well as all mobile NFC services. They believe that it provides a secure, flexible channel for carrying out NFC enabled mobile payment transactions. In accordance with Pay-Buy-Mobile project, GSMA is also proposing use of trusted third party or TSM which needs to be controlled by a bank, an operator, or several actors jointly, or by an independent body. However, it is important to note that since MNOs are the issuers of UICCs now, they are at the core of the business environment; they will control the mobile phone and security domains within mobile phone [57, 58].

GSMA also indicates that "*One of the ways to establish the needed level of trust is to understand and incorporate the requirements of the banks and MNOs. The role of the TSM will be to implement the requirements of both parties, and is essential for*

the establishment of a stable and efficient Pay-Buy-Mobile ecosystem, providing value for all stakeholders" [57].

Mobey Forum: Mobey Forum is another important industry driven forum which has performed valuable studies on development of mobile financial services and encourages the use of mobile technology on behalf of financial institutions. They studied on various SE alternatives (i.e. stickers, embedded hardware, SMCs, UICCs, TMB), and proposed three operational business process frameworks (i.e. hotel concept, rental concept and ownership concept which is the best and ideal option) in order to manage especially UICC based SEs in NFC services. Each model addresses different business strategy options for stakeholders with distinct value chain as well as allows different levels of control over SE and platform management.

Mobey Forum states that "*For Financial Institutions and Other Service Entities the options that they can drive independently to the market (i.e. become the SE issuer) are Stickers and Secure SD cards. Some form of collaboration is possible with these options as well*" and "*In collaboration with other stakeholders the financial institutions can issue their applications through other SEs like eSEs (embedded hardware) and TMBs (trusted mobile base) and even become the SE issuer through appropriate agreements*" [48, 53]. TMBs are considered as a promising upcoming technology which is at the CPU of mobile phones. Hence Mobey Forum believes that handset vendors will leverage their position within the market by collaborating with financial institutions in the short run after the entrance of TMBs.

GlobalPlatform: GlobalPlatform as one of the key actors in standardization of smart cards, performed studies on management of NFC services on UICC based SEs which also supports Mobey Forum's business models. Three main UICC configuration scenarios are proposed. According to GlobalPlatform, MNO owns the UICC hosting; therefore each MNO may choose an appropriate business model and select the personalization features to be supported by the UICC and available to its partners (service providers and TSMs). GlobalPlatform also studies on the OTA provisioning and deployment of NFC services on other SE options [55].

Smart Card Alliance: In mobile payment studies of Smart Card Alliance, four different business models (i.e., operator centric, bank centric, peer-to-peer centric,

collaboration centric) have been offered for the NFC ecosystem which is different from Mobey Forum's approach. Collaboration model is the one which includes a trusted third party as TSM that manages the deployment of mobile applications. According to the survey results of Smart Card Alliance [59], in Operator Centric Model, MNOs will receive most of the revenue, whereas in the Bank-Centric Model, bank will receive most of the revenue. In case of Collaboration Model, "*…revenue choices were most similar to the Bank-Centric Model, with a tendency to follow today's payment network model with some revenue going to mobile operators for application download or secure element space rental*" [59]. Collaboration model enables mutually beneficial and acceptable business environment with lower risks for all stakeholders.

Today, to achieve a good business model, interoperability and standardization of the NFC technology model is essential. This will drive cooperation and collaboration of all participating entities (e.g. MNOs, merchants, service providers, TSMs, hardware manufacturers) in the NFC ecosystem, and also enable customer acceptance.

Chapter 3

NFC Loyal

In this chapter, paper of “NFC Loyal: A Beneficial Model to Promote Loyalty on Smart Cards of Mobile Devices” is presented, which is published in the proceedings of “IEEE International Conference for Internet Technology and Secured Transactions”. Followings are the information on the paper.

Paper Title: NFC Loyal: A Beneficial Model to Promote Loyalty on Smart Cards of Mobile Devices

Authors: Büşra Özdenizci, Vedat Coşkun, Mehmet N. Aydın, Kerem Ok

Conference: IEEE International Conference for Internet Technology and Secured Transactions

Conference Date: 8-11 November 2010

Conference Place: London

Conference Web Site: http://www.icitst.org/

3.1 NFC Loyal: A Beneficial Model to Promote Loyalty on Smart Cards of Mobile Devices

NFC is a short-range, high frequency, and low bandwidth wireless technology. NFC communication occurs between two devices that are within few centimeters, using 13.56 MHz, with a bandwidth not more than 424 kbps. NFC technology provides card emulation, reader/writer, and peer-to-peer operating modes where communication occurs between a mobile phone on one side, and an NFC reader, an RFID tag or a mobile phone on the other side.

A smart card is an Integrated Circuit Card (ICC), including embedded secure microcontroller consisting of internal memory which can process data. Today contactless smart card technology and integration with mobile phones increased its usage by the applications that need to deliver fast, secure transactions. It is true that development of smart card technology vastly affects usage of mobile devices. Smart cards enable secure storage of valuable information and provide secure area for the execution of applications on the smart card for this reason. In fact, smart cards' potential to increase its popularity depends on their ability to enable secure usage of multiple applications on a single card. Thus providing trusted, secure, interoperable, multi-application platform became a crucial issue for these applications.

It is currently a demanding area for researchers to enable fruitful secure concurrent execution of multiple applications on the same smart card. Lots of cards' data, including credit cards, debit cards, membership cards, and loyalty cards can be stored into one single device by installing the required applications on the smart card appropriately. By this way, advantages of loyalty / membership cards which act as an effective marketing tool can be enriched. With the help of the payment applications (i.e. credit and debit card applications), the availability, mobility, and simplicity of using such loyalty services can be increased to obtain more customer satisfaction and customer loyalty.

Customer loyalty is simply expressed as repetition of purchases [60]. Effectiveness of loyalty card schemes on customers is directly seen on the repeat purchase behavior of loyal customers through stimulating product or service usage, increasing switching costs. Specifically the significant changes on consumer behavior are; decreased

switching to other brands, increased usage frequency and repeat purchase rates for the program brand(s), greater propensity to be exclusively loyal to program brand(s), and greater tendency to switch between program brands (Figure 3.1).

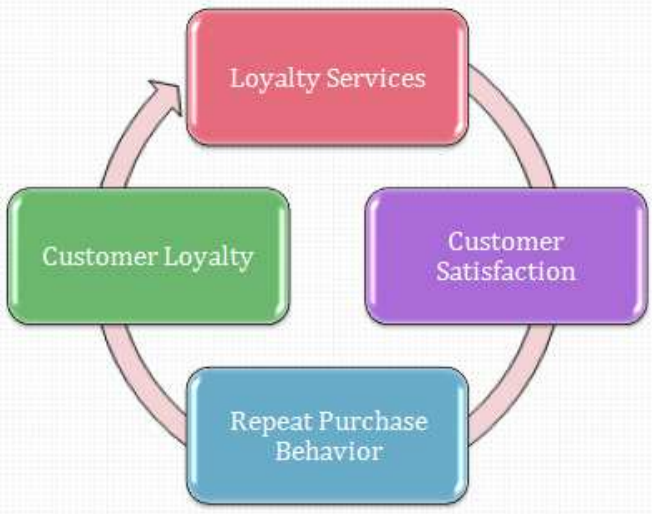

Figure 3.1. Loyalty Services as an Effective Marketing Tool

We believe that more attention on loyalty programs in terms of NFC technology is needed. Thus we propose NFC Loyal, which make use of improvements made by the new smart card technology. NFC Loyal extends the conventional understanding of loyalty card to a more efficient and secure usage by storing loyalty data on the smart card which is embedded to a mobile phone and by enabling secure data exchange between applications. According to our proposed model, loyalty and payment applications share and exchange valuable information to obtain mutual financial outcomes and to increase the repetition of purchase behavior of existing customers, and to start a purchase behavior if it already does not exist. Multi-applications share secret information as configured by the user. The payment applications send the data to a central common domain on a secure element, called as Secure Common Domain (SCD) to be stored and used afterwards. Partners such as membership, loyalty, and payment applications can use the data appropriately if they are authorized to do so, according to the prior configuration. Data sharing between applications will be limited and is configured by the user. Some subset on the purchase information those are transferred to the SCD by the payment applications, classified as sharable by the user, can be used by the loyalty applications. In this case the most important issue is no loyalty application is able to edit, or modify information on that database. Such a

model paves the way for other potential offers of loyalty applications and increases the intense competition between service providers.

We introduced the features of the NFC technology and Loyalty Card programs in the introduction section, together with early and brief definition of NFC Loyal. In Section 3.2, the technical background for NFC Loyal is provided. In Section 3.3, we explain NFC Loyal Card details, some scenarios, NFC Loyal architecture, SCD Management, and promising security architecture for SCD. Finally, a conclusion on the topic is provided in Section 3.4.

3.2 Technical Background

NFC technology has adopted smart cards as SE to provide a secure area for the execution of concurrent applications [47]. We highlight GlobalPlatform Card specification as a smart card specification for our model which is a cross-industry membership organization created specifically to maintain and promote multi-application smart card standards and more specifically the GlobalPlatform specifications [61].

GlobalPlatform Card specification is comprised of a number of logical and physical components that aim to provide application interoperability and security in an issuer controlled environment [61]. From a technical point of view, the operating systems running on secure elements must be able to install, personalize, and manage multiple applications preferably via OTA software installation mechanism. There are existing supporting architectures that enable secure coexistence of multi applications on the same smart card such as JavaCard [62]. Integration of GlobalPlatform Card Specification v2.2 with JavaCard technology v3.0 - latest versions - provides the necessary functionality for our proposed model in terms of secure storage of keys, key management system, and distinct security domains of GlobalPlatform Card Architecture.

The main entities of GlobalPlatform Specification that are involved in the communication session of the smart card architecture are Card Manager as central administrator of the card, Card Issuer, and Application/Service Providers which are the companies (banks, mobile network operators etc.) those have a business relationship with the Issuer. Card Manager can be viewed as a composition of three

entities which assume multiple responsibilities; The GlobalPlatform Environment (OPEN), The Issuer Security Domain, and Cardholder Verification Method Services [52].

Each entity has its own security domain. Security domains of GlobalPlatform act as on-card representatives of off-card authorities and have their own security architecture. They are responsible for cryptographic functions, key handling, generating keys, and implementing secure channel protocols. In accordance with GlobalPlatform Card Specification 2.2 [52], security domains will be the critical components in our SCD specification to store keys, and control access to the SCD database. Other required security domains in the GlobalPlatform Card are the Issuer Security Domain (ISD), Application Provider Security Domain (APSD) and Controlling Authorities' Security Domain (CASD).

3.3 NFC Loyal Card

3.3.1 NFC Loyal

NFC Loyal is a beneficial model to share the generated information via transactions among the payment applications and loyalty applications according to the filters as configured by the mobile user. Creation of NFC Loyal architecture includes several steps such as OTA transfer of the required applications to the smart card, configuration of the applications by the user, storage of transaction data by the payment applications, and retrieval and proper usage of the data by the loyalty applications as authorized by the smart card owner.

Usage of NFC Loyal provides different benefits to the actors. NFC Loyal actors are examined in two categories. User is the user of the NFC enabled mobile device, where service providers' side consists of the payment (credit and debit) card issuers, banks, and loyalty card issuers. The primary actor in this model is obviously the user. She is the one who should be initially be convinced to use NFC Loyal, more specifically to install SCD, and SCD manager (SCDM), and make use of it by the payment and loyalty applications installed on the smart card afterwards by the use as well. Mobile user will have benefits using NFC Loyal, such as earned coupons, discounts, free miles or free talks etc. from loyalty applications those are supposed to motivate the user. On the service providers' side, loyalty card issuers will face with

increase in purchase of the offered product or service (increase in repeat purchase behavior) and will acquire more loyal customers. Payment card issuers will experience increase in usage and banks can act as a loyalty firm by offering customers to use that bank's account. Absolutely, individual gains of each party (service providers and customers) will rise, if users and payment services agree to share more information with the loyalty services. The barrier on increasing the exchanged information is of course the pessimism about usage of the leaked data for bad reasons.

We highlight a new model that is expressed as Secure Common Domain Management System (SCDMS) which sustains the information sharing through a SCD, like a centralized database. Indeed, several challenging SCD management scenarios on a smart card can be mentioned. Applications on smart cards can either store information onto the SCD, or read the information those are written by the same or other applications as well. In this paper, we mainly focus on the scenarios or business cases which ensure the interaction between payment applications (i.e. credit and debit card applications) and loyalty applications installed on the secure element.

3.3.2 NFC Loyal Architecture

Payment and loyalty programs are to be OTA downloaded to the smart card, installed, and configured by the user, as already explained before. We use GlobalPlatform Card Specification that provides appropriate framework including all of the ingredients to enable NFC Loyal. According to that specification, the smart card architecture is comprised of a number of logical and physical components such as microprocessors, OPEN and GP Trusted Framework as the communication component, RTE as the run time environment, Security Domains to store information such as keys and files, and several application slots to install applications by the Card Issuer, Application Provider, and Global Services [52].

In our proposed model, we further extend this architecture to satisfy NFC Loyal needs, as shown in Figure 3.2 and described below:

- Payment and Loyalty applications are to be installed to the applications cluster, and they would create their security domains as expected on the Security Domain cluster.

- SCDM application is to be installed to the application cluster, and SCD would be created on the Security Domain cluster similarly.

3.3.3 Secure Common Domain (SCD)

SCD can be viewed as a centralized secure database storage cluster which aims to enable secure data storage and data sharing by the payment and loyalty applications. SCD is managed by the SCDM which acts as the interface between the SCD and the applications. SCDM is responsible to store the data that is sent by the payment applications, as well as respond to queries made by the loyalty applications as agreed by the user and configured accordingly. SCDM provides following services to the payment and loyalty applications:

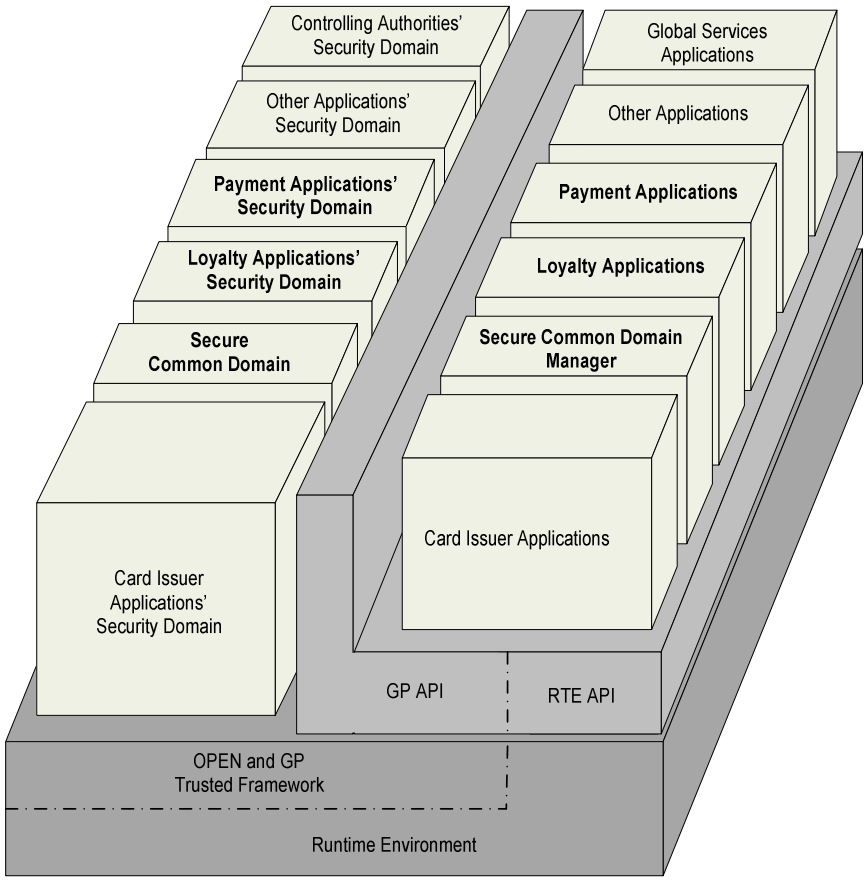

Figure 3.2. NFC Loyal Architecture

- Secure data insertion by the payment applications, so that only authorized actors can insert data
- Secure data storage, so that only authorized actors can access data

- Secure data retrieval by the loyalty applications, so that no eavesdropping or similar attack can succeed to reveal the content, and no active attack (replay attack etc.) is possible against other security concerns such as integrity
- Availability for all types of authorized requests
- Database design requirements such as Durability, Consistency, and Integrity are also to be satisfied
- Provides configuration option to user, so that only the intended data will be transferred to specified applications

3.3.4 NFC Loyal Model

The main actors of NFC Loyal are card issuer, card holder, loyalty service providers, payment service providers, certificate authority, and SCDM. The position of each actor is described below:

- **Card Issuer** being the controller on the smart card holds ultimate responsibility of the smart card and prepares the smart card in accordance with [29], so that it can further be used by the card holder as well as applications.
- **Card holder** is the actual user who currently owns and makes use of the smart card and maintains the contents of the smart card with the authorization of the card issuer.
- **Loyalty and Payment Service Providers** provide the services via the applications. Card holders sign an agreement with these companies before the related applications are installed.
- **Certificate Authority (CA)** handles all security and privacy issues of SCD Management, which is a trusted third party. CA issues digital certificates to be used by the service providers and SCDM, manages security credentials and public keys for message encryption, which is also part of PKI [63].
- **SCDM** provides management of SCD.

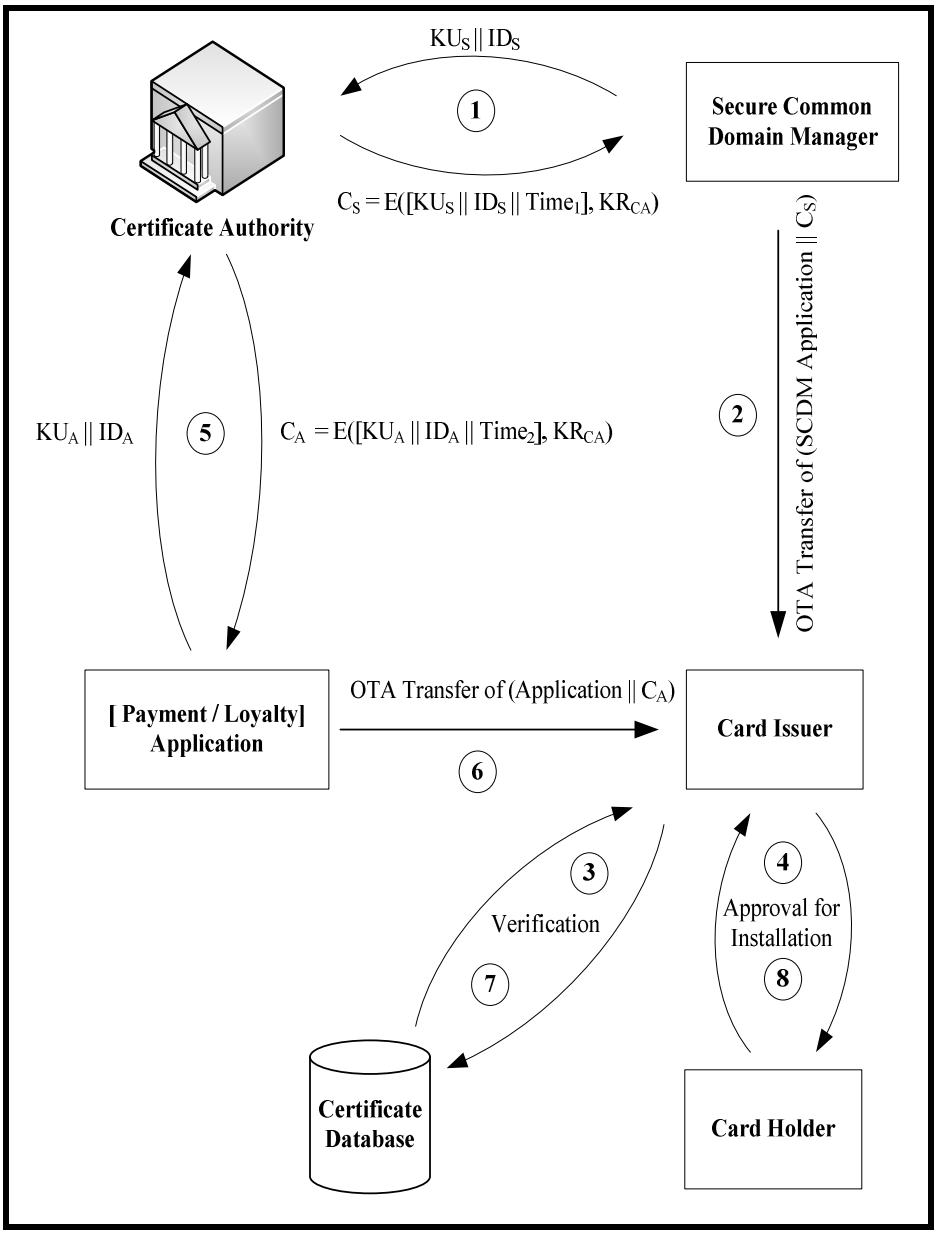

Figure 3.3. Loading SCDM and Other Applications

Remembering that Card Issuer is responsible from the security of the smartcard, all applications those need to run on the smartcard need to prove its identity against Card Issuer. We use certificates for authentication related purposes. SCDM as well as payment and loyalty applications need to receive a valid certificate from the Certificate Authority, and use it to prove its identity before the installation. We use a modified version of X.509, which is tailored considering the resource limitations of the smartcards. Figure 3.3 shows the interacting parties during SCD Management. It follows the steps hereunder:

Loading SCDM: (Step 1) SCDM application must obtain their own signed certificate from CA before installation and personalization of SCDM application, as shown in Figure 3.3. SCDM application forwards its own public key (KU_S) to the CA, trusted third party. CA prepares the certificate that contains subject's public key, id of the application and time information. CA signs the certificate by creating a hash value and then encrypting the hash value with its private key (KR_{CA}). (Step 2) As the card holder requests loading the SCDM, the SCDM application is OTA downloaded together with its certificate, and the Card Issuer accepts installation. (Step 3) Card Issuer checks and verifies the SCDM application's certificate through the certificate database. (Step 4) After verification of Card Issuer, Card Holder can approve the installation and personalization of SCDM application on the smart card.

Loading Loyalty and Payment Applications: After the SCDM application is loaded and installed, Card Holder may then load and install any payment and loyalty applications as she wishes in order to use NFC Loyal. (Step 5) Before the download of the applications (i.e. payment and loyalty applications), each application owner must obtain a signed certificate from CA by forwarding public key of the application (KUA) as SCDM owner did in step 1. CA again creates and signs the certificate by encrypting the related data similarly using its private key (KR_{CA}). So, each application receives its own certificate from CA. (Step 6) Applications and their own certificates can be loaded through OTA under the control of Card Issuer. (Step 7) The Card Issuer has to verify the application's certificate by checking the certificate database. (Step 8) After verification, approval of the smart card owner has to agree to the install and personalize payment and loyalty applications. With the approval of Card Holder, the smart card receives a CREATE SSD command and SSD is created by the ISD. Loading and personalization of all applications are performed by using GlobalPlatform content loading commands. After creation of security domains of applications and personalization [61], applications can be loaded and installed through "INSTALL [for load]" command and one or multiple "LOAD" commands. Installation is personalized through "INSTALL [for personalization]" command and consecutive "STORE DATA" commands.

SCDM Configuration as Required: After loading phases, Card Holder as the owner of the card, makes the necessary NFC configuration on the SCDM and the

applications those are already loaded onto the mobile device. In NFC Loyal, the payment applications can share all or partial information with loyalty applications, according to the presetting made by the user. To share partial information, a setting mechanism is required that provides marking the transaction tags those will be sent to SCD. Such a mechanism is beneficial for Card Holders who want more user privacy. The amount of the shared information can be low or high, depending on the user's sharing preferences. A card holder who prefers more privacy may configure the system accordingly, but will gain less than the card holder who prefers high profit and configures the system to exchange more data among the payment and loyalty applications. This configuration includes the setting mechanism that have mentioned in case scenarios.

Interaction with SCD: Through appropriate key management and security mechanism, applications and SCD can interact with each other. Payment applications can send information to the SCD and loyalty applications can receive information from that database securely. The interaction between entities and requirements are explained in the following part.

We propose using a high-level language, namely Extensible Markup Language (XML) [64], for the interaction between the SCDM and the payment as well as loyalty applications. XML documents must be both well formed and valid [64] in order to be used. In being a well formed document, the tags within the XML document must not violate XML guidelines. A well formed XML document conforms to the provided DTD document (i.e. Document Type Definition, a context-free grammar for describing XML tags and their nesting). After configuring an application, one separate DTD document must be prepared by the SCDM. After a DTD document is prepared, each exchanged XML document can be checked against its validity. DTD content can either be embedded into the related XML document, or can be prepared as a separate document. In our proposed model, DTD document is written and saved as a separate document for each transaction (Figure 3.4).

In NFC Loyal, payment applications on a single, dynamic SE stores partial information of occurred transaction to SCD, as defined by the users' filtering configuration. The transaction table has to be created in the database of SCDM. The transaction table typically consists of id, date, time, price, company and category

columns. ID refers to the transaction id, which is the primary key value and makes that transaction unique. Date and time refer to the occurred transaction's date and time information. Price information is related with the cost of the purchase or transaction. The company is where the customer or Card Holder makes the purchase and this information is the most critical option. Company and price information can be concealed by the user configuration. The last tag as category of the transaction is the categorization of the purchased item that can be described as market, gasoline, cosmetics, book, music etc. Please note that we describe the complete data structure in here, but each payment application will store only the appropriate parts of this definition, and each loyalty application will also be able to request data; both of which is defined by the previous configuration made by the user.

```
<! - -TRANSACTION.DTD document - - >
<!DOCTYPE Transaction [
<!ELEMENT Transaction (ID, date, time, price,
company, category)>
  <!ELEMENT ID (#PCDATA)>
  <!ELEMENT date (#PCDATA)>
  <!ELEMENT time (#PCDATA)>
  <!ELEMENT price (#PCDATA)>
  <!ELEMENT company (#PCDATA)>
  <!ELEMENT category (#PCDATA)>
]>
```

Figure 3.4. DTD Document

```
<! - - TRANSACTION.XML document - - >
<?XML VERSION= "ENCODING="ISO-8859- STANDALONE= "no"?>
<Transaction>
  <ID> 1</ID>
  <date> 15 April 2010 </date>
  <time> 14:00 </time>
  <price> 100 </price>
  <company> Gaseous </company>
  <category> Gasoline </category>
</Transaction>
```

Figure 3.5. Sample for Transaction XML Document

After each transaction, the related payment application creates an XML file containing the required information (Figure 3.5), encrypts XML file using SCDM's own public key and sends it to the SCDM through secure channel. SCDM decrypts the XML record using its own private key and store XML information in SCD. To achieve a secure channel protocol between applications and SCDM, one of the available public key encryption schemes such as RSA may be used. As stated in [63], the supporting functions of a PKI include key certification, authorization of participating entities, and the ability of a participating entity to have multiple keys. Secure channel allows a smart card and an off-card entity to authenticate each other and establish session keys in order to protect the integrity and confidentiality of subsequent communications [63]. For the establishment of secure channel, initiation of secure channel protocol through appropriate APDU commands is required by the off-card entity or by an on-card entity (e.g. secures domains, SCD). Secure Channel Protocol initiation phase is also involved the authentication of the off-card entity by the card.

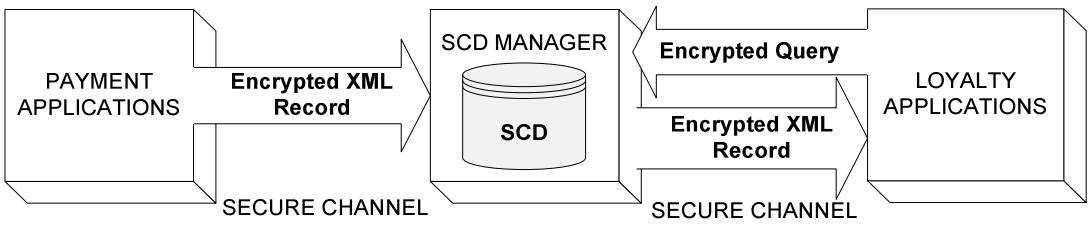

Figure 3.6. Interaction with SCD

After the secure channel protocol initiation, payment applications and loyalty applications can interact with the SCDM securely (Figure 3.6). Loyalty applications can request transaction information those have happened so far from SCDM, the query is encrypted by SCDM's public key and is sent to it. SCDM decrypts the incoming query using its own private key and processes the request. After the request is processed, SCDM sends the resultant data to the requesting application, encrypted with the public key of the requesting application. The requesting application further decrypts the incoming data using its private key similarly. A more advanced form of encryption, by creating session keys of secret key cryptography is also possible. Hence, secure data transfer between the SCDM and the applications are made possible by the NFC Loyal model.

3.4 Conclusion

In this paper, we introduce NFC Loyal, a beneficial model that enables sharing transaction data among payment and loyalty applications those are installed and configured on the smart card by the NFC enabled mobile device owner. In the scope of NFC Loyal, we propose an improvement based on the GlobalPlatform smart card specification. To facilitate our model, SCD segment needs to be created on the security domain cluster, and a corresponding manager, called as SCDM is to be installed on the Card Issuer Application cluster. SCDM provides secure storage and sharing of the transaction data afterwards. As a new purchase is realized, part of the transaction which is configured by the user previously, is transferred to SCDM by the payment application, using a secure channel. So, no eavesdropping or other attacks can be succeeded. After the data is accumulated on the SCD, authorized loyalty applications on the smart card may retrieve the data either case by case basis, such as after a request by the loyalty application, or after triggering an alarm as set prior on the SCDM.

Usage of NFC Loyal provides different benefits to the actors. Mobile user can for example gain coupons, discounts, free miles or free talks etc. from loyalty applications that motivates users to provide benefits to service providers. On the service providers' side, loyalty card issuers can gain from increase in purchases of the offered products or services (increase in repeat purchase behavior) and can acquire more loyal customers. Payment card issuers can experience increase in usage and banks can act as loyalty firms by offering customers to use that banks' account.

The complete architectural design of NFC Loyal is shown in the paper. Also the actors on the model, the business plan, and the required architectural plan are defined in detail. We further proposed a security model so that secrecy, integrity, and availability of the system are satisfied as well as the required access control mechanisms.

Chapter 4

NFC Internal

In this chapter, paper of “Development of an Indoor Navigation System Using NFC Technology” is presented, which is published in the proceedings of “Fourth International Conference on Information and Computing Science”. Followings are the information on the paper.

Paper Title: Development of an Indoor Navigation System Using NFC Technology

Authors: Büşra Özdenizci, Kerem Ok, Vedat Coşkun, Mehmet N. Aydın

Conference: The Fourth International Conference on Information and Computing Science

Conference Date: 25-27 April 2011

Conference Place: Phuket Island, Thailand

Conference Web Site: http://www.worldacademicunion.com/journal/1746-7659JIC/ICIC2011/Organizers.htm

4.1 Development of an Indoor Navigation System Using NFC Technology

Navigation is starting at an origin, travelling along a path to arrive a destination point. Navigation systems provide reading, controlling and updating the movement of one's position and orient while she is travelling on an intended route. If any diversion to outside of the route occurs, reorientation or correction to the destination is done [65]. Since all people use PDAs, mobile devices or personal navigation assistants, and navigation systems can run on those devices, demand and usage of outdoor navigation systems are increasing incredibly today. Outdoor navigation systems are generally based on Global Positioning System (GPS) which is a space based global navigation satellite system that provides reliable location information in almost all weather conditions and at all times on or near Earth [66]. GPS based outdoor navigation systems is a well explored and standardized research area whereas GPS receivers cannot perform well indoor environments because of absence of line of sight to the satellites.

Indoor navigation system has become a recent research area due to the unavailability of GPS indoor environment. Variety of technologies is tested and new designs are generated for indoor navigation in order to circumvent the lack of excellence. The existing solutions for indoor navigation systems are generally grouped as network based navigation systems which are based on networking technologies such as sensor networks [67], and independent navigation systems providing autonomous user positions. Network based navigation systems use technologies such as Bluetooth, Ultra Wide Band (UWB), Wi-Fi, or RFID. Position accuracy varies according to the technology used. Wi-Fi and UWB technologies provide higher position accuracy than Bluetooth and RFID technologies. Bluetooth is a simple, compatible short range communication technology which requires expensive receivers; and the position accuracy depends on the amount of cells used.

In case of RFID technology, position accuracy depends on the type of the tags, which is either active or passive, as well as the amount of these tags. Existing RFID based indoor navigation solutions are generally based on usage active RFID tags and require extensive usage of active RFID tags to get good position accuracy. Contrary to passive tags, active tags contain embedded batteries in order to increase the transmitting distance. The major drawback of using active RFID tag based solutions

is the high cost of the active tags. Studies in this area [150] also indicate that it does not provide an efficient tracking system.

Wi-Fi and UWB technologies have their own limitations as well. Wi-Fi requires expensive access points in any area where the person needs to be tracked [67]. In case of UWB an efficient indoor navigation system cannot be ensured due to some technical problems of the technology (e.g. antenna mismatch, low power emission, and possible external interference from other systems).

The other popular systems are independent navigation systems based on dead reckoning (DR) methods [68]. When marking position of a person on a map, two types of positioning are defined. Fix position determines the location by using the help of enough number of assisting devices, such as satellites. In the contrary, estimated current position is calculated based on the last fix position, the route, the speed of the item, and the elapsed time between current time and time of the calculation of the last fix position. Navigation systems based on DR methods use this methodology. DR methods use Micro Electro-Mechanical Sensors (MEMS) which are electronic accelerometers, magnetometers, and barometers. The major drawback of DR method based navigation system is that performance of the system is affected by the large errors. The errors of the estimation process are cumulative when calculation of new position is based on previous DR position.

Another independent, existing technology is assisted GPS (A-GPS) systems which enlarge the working area of the GPS technology [67]. With A-GPS systems, indoors GPS signals are processed efficiently through an assistance data server which is connected to a reference receiver. However, the signal strength sometimes is too low indoors.

A major limitation of indoor navigation systems is the high installation cost and the complexity of the system design. Additionally, most of the existing positioning systems are far from providing an accurate position in large buildings [67], [68]. Thus, an efficient and low cost indoor navigation system is strongly required inside large buildings consisting of many rooms, floors and large halls.

Navigation systems for indoor environments can be desirable at any time. For instance a person entering a building for the first time may want to go to an office

inside the building without spending much time. Such cases are very common at university campuses, airports, hospital complexes and shopping centers etc. A user-friendly indoor navigation system guiding people through huge buildings consisting of thousands of rooms can be helpful in such cases.

This paper presents an innovative, low cost indoor navigation system called NFC Internal which takes advantage of an emerging short range wireless communication technology; NFC. The main idea is to orient users by NFC enabled mobile phones which also have an embedded indoor navigation application. While application orients the user by gathering destination point from user; mobile device gathers the current position from NFC tags and shares the coordinate data with the application. Thus a user can determine her current position inside a building by touching her mobile device to the tags which are spread inside building.

The remainder of this paper is organized as follows. In Section 4.2, NFC based solution to indoor navigation is presented together with the system design and the implementation of the system. Section 4.3 concludes the paper and highlights future work.

4.2 NFC Internal

NFC is a bidirectional short range, wireless communication technology. The communication occurs between two near devices within few centimeters. 13.56 MHz signal with a bandwidth not more than 424 kbps [39] is used. NFC technology is based on Radio Frequency Identification (RFID) technology and can operate in card emulation, reader/writer, and peer-to-peer operating modes where communication occurs between a mobile phone on one side, and an NFC reader, a passive RFID tag (NFC tag), or a mobile phone on the other side respectively.

NFC Internal is very simple and easy to use. The user only needs to carry and use an NFC enabled mobile device. Indoor navigation application must be OTA (Over the Air) pre-loaded to the smart card. Than the user needs to simply touch to the URL Tag (NFC tag), that contains the URL of indoor map information just before entering the building or area. The map on the web site is OTA downloaded to user’s mobile device from the MapServer (i.e. a web server containing the map information). The indoor navigation application on the mobile phone automatically starts and uses this

map information afterwards. As the user selects destination point of her voyage inside the building, the indoor navigation application provides the optimal route to her destination. As the user navigates through the halls, she can touch to the Reference Tags (NFC tags) spread over the building to fix her current position on the map, and then get instructions to reorient her position to destination or to create a new optimal route to the destination as it is required. We believe that NFC technology is a seamless solution for indoor navigation systems when compared with all other existing solutions.

We can extend the use of NFC Internal to additional cases as well. The existing outdoor navigation systems and the NFC Internal can be coupled and such a solution provides higher functionality. For instance, assume that a new student currently staying in her home and needs to meet with her advisor to perform course registration process, but she neither knows the location of the university campus in the city, nor the office of her advisor within the campus. In such a case, user needs an NFC enabled mobile device which includes a GPS-based mobile navigation system for outdoors and also an indoor navigation application. The student starts the process by entering the name of the university campus and name of the advisor. GPS-based mobile navigation application orients the student until she reaches to the university campus. Map of surrounding area is shown on the mobile device screen, which the student's current position and a route to the campus are also indicated as well [69]. As student moves to the destination, the mapped area and the student's position are dynamically updated on the map. GPS based mobile navigation systems can also provide speech guidance to the student as well. When student reaches to the university campus, she needs to simply touch to the URL Tag on the entrance in order to get indoor map information and navigate inside. After the map is downloaded from MapServer, the outdoor application quickly shares the destination information with the indoor application on the mobile device which is a seamless solution. So, the student does not need to enter the destination address again. Now, user can start to navigate inside the campus by touching to the Reference Tags as described above.

4.2.1 System Design

Spatial Information Maps: Current Indoor map databases are generally based on 2D graphical representations which are developed by CAD (Computer-Aided Design) systems [70]. In accordance with [71], the CAD drawings of an indoor environment can be separated into floor maps of each floor in the building, and each CAD drawing of floor plan can further be converted into separate spatial information maps that annotate structural features such as walls, doorways, elevators, and staircases. In each separate spatial information map, the reference points are also expressed in vector spatial data structure which uses the 2D Cartesian coordinate system and each map is stored in the MapServer of the Indoor Environment with a unique floor identifier, and also a unique building identifier if the indoor is a complex or campus.

Reference Tags for NFC Internal: To navigate indoor environment, NFC Internal needs spatial information to calculate all accessible paths [71]. The indoor environment of buildings or complexes has large number of Reference Tags in our model. These Reference Tags are placed on each rooms', elevators', and stairs' entrances and also in corridors. The number of these tags depends on the size as well as structure and complexity of the building. A description for each Reference Tag is used to allow easy search for destination points, and each Reference Tag includes location information which is comprised from a building identifier data, a floor identifier data and vector spatial data. We use a vector spatial data structure instead of using raster data structure. Usage of vector spatial data allows efficient encoding topology and also network linkages can be efficiently employed [72]. Thus it is more useful for accurate positioning.

Algorithm for NFC Internal: With a quick and reliable graph derivation algorithm, the maps downloaded from the MapServer needs to be converted into link-node model with topological relationships, as seen in Figure 4.1 [70]. A link/node model is composed of corridor, way, road, path between buildings, room, hall, stair, lift, door of interest. The indoor navigation application finds shortest path between the current position and the destination by using these link-node relations. The computation of optimal route is based on Dijkstra's algorithm which solves source-sink shortest path problems efficiently [70], [73], when both the start and end nodes are given.

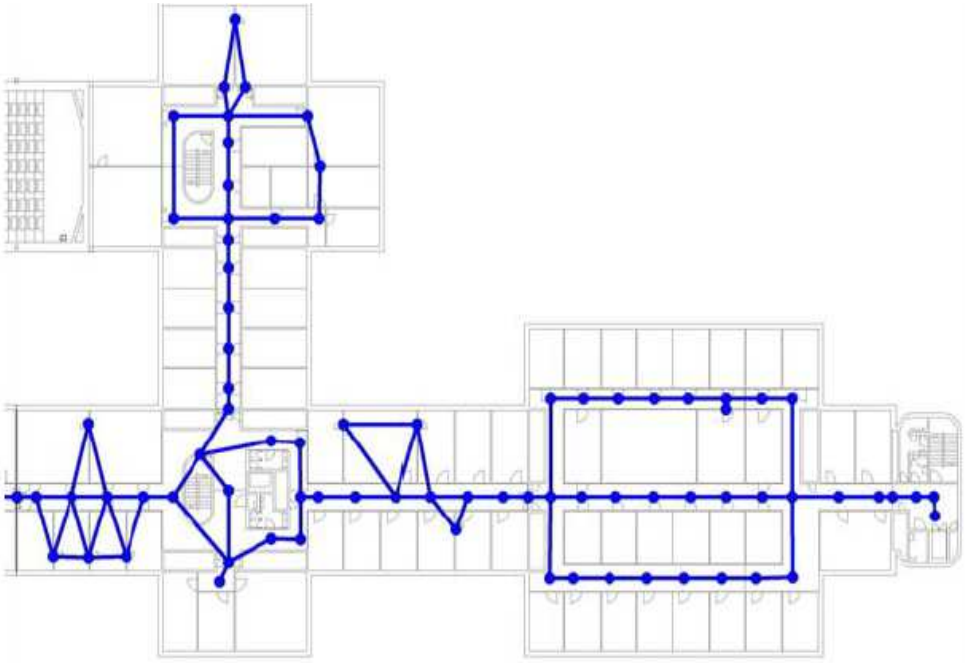

Figure 4.1. Link-Node Relations of an Indoor Environment [70]

4.2.2 How NFC Internal Works

This section shows how NFC Internal works in detail. The NFC Internal is comprised of two phases: initiating the indoor navigation system and navigating to destination. As described before, the main problem starts with the user who needs to reach to an intended point, but does not know the exact location of the place. In such situation, the user who has an NFC Internal system on her an NFC enabled mobile device is only required to follow the phases hereunder.

Initiating NFC Internal: As seen in Figure 4.2, the user touches to the URL Tag which contains the URL of the indoor's map information on the MapServer. This tag is placed on the entrance of the building.

1. The NFC enabled mobile device gets the address as it touches to the URL Tag.
2. Mobile device connects to the URL via OTA and requests the map information from the MapServer, and the map information is loaded to the mobile device afterwards.

3. After loading the map, indoor navigation application on the smart card automatically starts and converts the map data into link-node model as 2D network with topological relationships.
4. The application asks the user to enter the destination point. User specifies destination point just by choosing the person's name.
5. The application quickly computes the best route by using Dijkstra's shortest path algorithm.

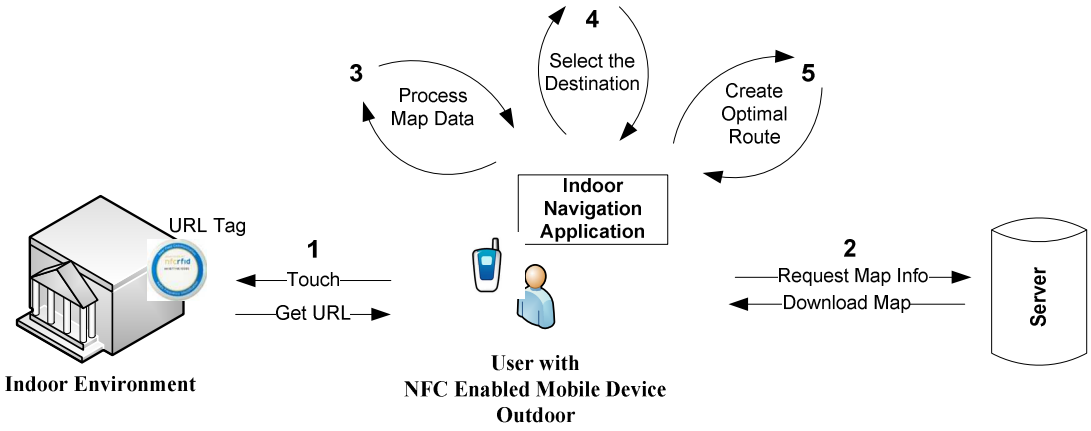

Figure 4.2. Initiating NFC Internal

Navigating to Destination: After the route is computed, application starts to orient the user towards the destination. As the user navigates along the path, she can touch to any Reference Tag to validate her navigation. User is only required to touch to a tag on her way to get this valuable help. The location data on the Reference Tag is transferred to indoor navigation application at this moment. It is obvious that information on the tag also shows the user's current location. The application uses this information to check whether the user is on the intended route or not. The application forms simple plain instructions as forward, left, right, backward etc. to orient the user which can be easily followed by the users. Also there are instructions to use stairs upward / downward or to use elevator up / down to a specific floor. These instructions are displayed on the screen of the mobile device.

Let's concentrate on the simple case shown in Figure 4.3. According to the scenario, user wants to be directed to Office A, and starts navigating inside the building for

this purpose. She touches to the first Reference Tag that she sees on her way, after which the location data on tag is transferred to the application on mobile device (Step 1'). So, the application figures out that she is on the intended route and gives user the first instruction as: “go straight ahead for 25 meters, turn right”. Similarly user touches to another Reference Tag on her route and application finds out that user is still on the correct route, so gives instructions to the user (Step 2').

There is a possibility that the user might get out of the route, towards Office A for example, and touches to a Reference Tag which is not on her route (Step 1"). With the transfer of location data, the application figures out that the user is out of route and calculates a new shortest path to Office A and gives user a new instruction as: “go straight ahead for 50 meters”. Similarly user touches to another Reference Tag on her new shortest route to Office A and application figures out that user is on the intended route indeed, and gives instructions to the user (Step 2"). As the user arrives the destination point, Office A (Step 3), the application tells user that she reached the destination, and ends the ongoing process.

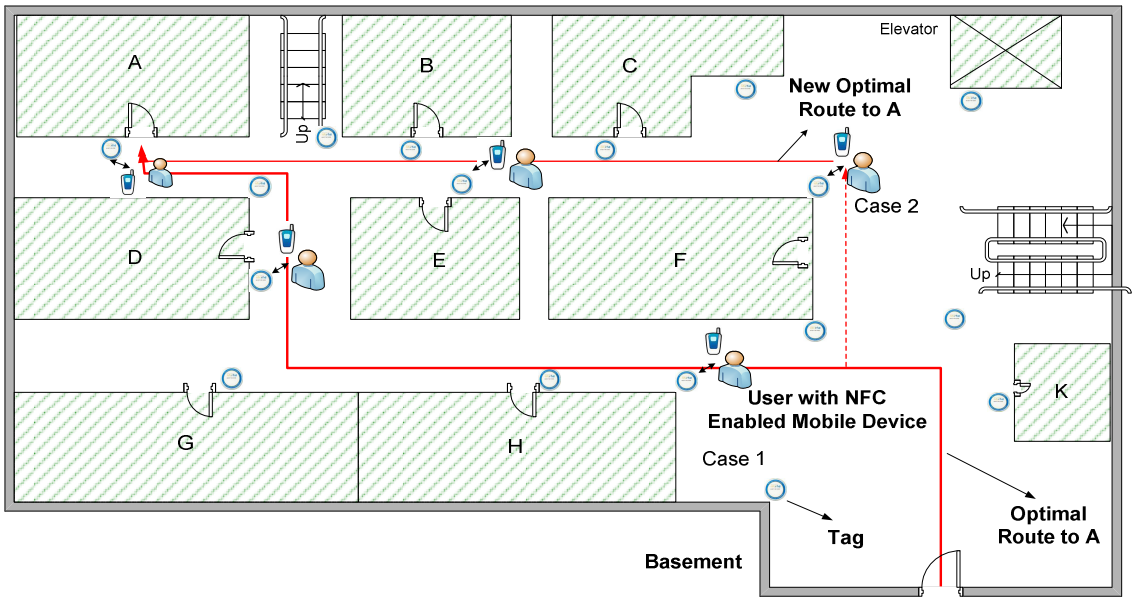

Figure 4.3. Navigating to Destination

4.3 Conclusion

This paper presents a new, reliable, and seamless indoor navigation solution that helps to create smart and context-aware environments. The use of NFC technology in

indoor navigation systems has a potential to increase the usability of these systems. Comparing to other existing indoor navigation solutions, NFC Internal has many advantages hereunder:

- Reduces the cost of indoor navigation systems by using cheap passive tags,
- Minimizes response time, because the time required to transfer data from NFC tag to mobile device and the time required to generate application's new path is little,
- Provides accurate position and orientation information, so the orientation of the user to the destination is facilitated,
- Eliminates the need for a server or a terminal to orient position, so location privacy of the user guaranteed,
- Provides exclusive control over her location data for the user.

On the other hand there is a limitation of the proposed system. In the system, on the go position information cannot be provided, since user can learn her position information as she touches an NFC tag.

Overall, we think that the proposed system is very simple to use and has several benefits to users. Furthermore, the use of NFC technology in indoor navigation systems has a potential to increase the usability of these systems.

In future extensions of this study, we will further try to conduct usability and performance tests and evaluation of technical issues, e.g. generation of valuable instructions for user.

Chapter 5

Discussion

In this chapter, a short discussion and evaluation of the presented NFC applications, NFC Loyal and NFC Internal, is given in different aspects.

5.1 NFC Loyal as a Secure Model

NFC Loyal model creates a win-win model on business side by using the benefits of NFC technology as well as facilitates the adoption and development of more card emulation mode NFC services on user side. NFC Loyal model is mainly build on the GlobalPlatform smart card architecture which is currently the most proper card specification that offers secure, and flexible multi-application card content management functionality during a card's life cycle.

The major component of GlobalPlatform is the notion of security domains. Each entity has its own security domain (i.e., Issuer Security Domain (ISD), Application Provider Security Domain (APSD) and Controlling Authorities' Security Domain (CASD)). Our NFC Loyal model is built on these security domain infrastructure to manage all cryptographic functions, key handling, key generation, secure channel protocol implementation, digital signature generation and verification for their providers' (i.e. card issuer or application provider or controlling authority) applications.

Another important issue in terms of security is that the SCDM installed on SE keeps all stored data securely, do not transfer the information to any other party (application) not installed on the smart card and configured properly, and not to any other remote server such as company database as well. This conforms to the current situation where database management system applications are trusted parties in this sense. The information that is stored on the SCD after each transaction is under the control and responsibility of the user, so that user can store partial or all information (i.e. date, time, price, category, location, company information etc.) of each payment

transaction that she performs. Briefly, this model enables secure storage of sensitive data on SEs of users mobile through a database management system. Hence, service providers can easily collect and perform analysis on these data by simple data mining methods.

There are some important limitations that should be highlighted within the scope of this study. Up to now, most of the performed trials in NFC context usually include limited number of services without the possibility of removal or insertion of any new or unused NFC service on SEs. Although NFC technology and GlobalPlatform specifications warrants the separation of various NFC applications on the same smart card with high security and minimal risk of corruption, some certain security specifications prohibits this coexistence of multiple applications on the same smart card. However, users would prefer a dynamic multi-application environment within NFC mobiles where they can download or remove NFC services easily. Problems with dynamic multi-application card content management and OTA service provisioning issues should be solved as soon as possible to remove restrictions in front of service providers and MNOs, and allow them to develop innovative NFC applications on a single SE.

5.2 NFC Internal

5.2.1 Efficiency of Dijkstra's Algorithm

Finding efficient algorithms for shortest path problems is one of the most common research topics today. The most important issue that needs to be also considered in developing NFC Internal application is the used shortest path algorithm's efficiency in terms of time complexity. Algorithm complexity analysis provides how much time an algorithm takes to solve a problem.

Actually there are a number of shortest path algorithms which are differing in terms of time efficiency. In our indoor navigation system, Dijkstra's algorithm is proposed that finds shortest paths to a graph's vertices in order of their distance from a given source and calculates single source shortest path problems with directed graphs and nonnegative weights.

According to the literature, today for graphs with only non-negative edge weights, the Dijkstra's algorithm is a better solution. Time efficiency of Dijkstra's algorithm

depends on the data structures used for implementing the priority queue and for representing an input graph itself. The time complexity of the algorithm is expressed as O ($|E| + |V|^2$) = O($|V|^2$) using Big-O notation, where V is number of vertices and E is the number of edges.

Dijkstra's algorithm can be implemented more efficiently by using a Fibonacci heap as a priority queue. Fibonacci heap improves Dijkstra's algorithm to O ($|E| + |V| \log |V|$). Dijkstra's algorithm is the fastest known single-source shortest-path algorithm for arbitrary directed graphs with unbounded nonnegative weights.

5.2.2 Value Added Services

NFC Internal as a simple indoor navigation system can be also extended with more value added services. This system can take benefits of location based services. A good example can be shopping centers. When a user wants to reach a certain destination or a shop in a shopping center by using indoor navigation application of NFC Internal system, additional services can be offered to the user. For example, user may get latest ads or news about shops in the shopping centers (i.e., sales, price discounts and so on). The customers can access real-time information with their NFC mobiles. Such an information channel with the user can be created.

Chapter 6

Conclusion

Currently, a new way of interaction paradigm called *touching paradigm* by NFC technology is entered our daily lives. NFC requires only touching two NFC compatible devices to each other in few centimeters. It enables rich mobile commerce, marketing, and merchandising activities by integrating people's their daily use cards such as loyalty, debit and credit cards into their mobile phones. Also it allows people to gather valuable information immediately from context-aware or smart environments; exchange and share file, image, business cards and other data; pair Bluetooth devices; play games and so on.

Actually the technology is growing with the introduction of new services depending on the needs of people, and also with the introduction of new technical solutions for SEs, OTA platforms and capabilities and so on. At the same time, there is a great effort on establishment of more concrete standards to solve technical and business problems of NFC technology. This is really essential for the technology's maturity in terms of business and market dynamics.

In this study, first technical and business concepts of NFC technology is provided and assessed. Then we present two innovative NFC services; NFC Loyal and NFC Internal with their technical architectures, designs and generic usage models, which were also presented in international conferences.

The aim of NFC Loyal model is to promote the NFC enabled loyalty and payment applications on the same smart card within NFC mobile. NFC Loyal allows payment applications to share their transaction data through Secure Common Domain (SCD) with loyalty applications on a GlobalPlatform compliant SE. Such a beneficial model paves to way for more loyalty services, new business opportunities and models.

Another innovative application proposal is NFC Internal which is a low-cost and easy indoor navigation system. The aim is to orient users by NFC tags and NFC mobiles including an indoor navigation application. User with NFC mobile touches the NFC tags spread inside the building, and tags shares the coordinate data with the application within NFC mobile.

All these studies aim to understand NFC technology and its applications with different perspectives, and give valuable knowledge and insights on the development of technology. From academic perspective, NFC has still several open research areas for exploration and investigation, and also needs more rigorous research. In near future, I want to extend the paper of “NFC Loyal: A Beneficial Model to Promote Loyalty on Smart Cards of Mobile Devices” and explore the life cycle management of NFC Loyal model on smart cards with appropriate ecosystem model.

References

[1] J. Bravo *et al.*, "Towards Natural Interaction by Enabling Technologies: A Near Field Communication Approach", *European Conference on Ambient Intelligence (AmI'07)*, Darmstadt, Germany, 338-351, 2007.

[2] G. Chavira *et al.*, "Towards Touching Interaction: A Simple Explicit Input", *Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, Philadelphia, PA, 1-5, 2007.

[3] D. Ipiña *et al.*, "Touch Computing: Simplifying Human to Environment Interaction through NFC Technology", *1as Jornadas Científicas sobre RFID*, Ciudad Real, España, 2007.

[4] ECMA International, *ECMA 340: Near Field Communication Interface and Protocol (NFCIP-1)*, Available at: http://www.ecma-international.org/memento/TC47-M.htm, December 2004.

[5] ECMA International, *ECMA 352: Near Field Communication Interface and Protocol (NFCIP-2)*, Available at: http://www.ecma-international.org/memento/TC47-M.htm, June 2010.

[6] T. Tuikka and M. Isomursu, "Touch the Future with a Smart Touch", *VTT Tiedotteita – Research Notes 2492*, Espoo, Finland, Available at: www.vtt.fi/inf/pdf/tiedotteet/2009/T2492.pdf, 2009.

[7] Y. Chang *et al.*, "NCASH: NFC Phone-Enabled Personalized Context Awareness Smart-Home Environment", *Cybernetics and Systems*, 41 (2), 123 – 145, 2010.

[8] T. Kennedy and R. Hunt, "A Review of WPAN Security: Attacks and Prevention", *Proceedings of the International Conference on Mobile Technology, Applications, and Systems*, 56, 2008.

[9] E. Haselsteiner and K. Breitfuß, "Security in Near Field Communication (NFC)", *Philips Semiconductors*, Available at:

http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf, 2006.

[10] ETSI TS, ETSI TS 102 613, *Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics,* Technical Specification, September 2008.

[11] ECMA International, *ECMA 373: Near Field Communication Wired Interface (NFC-WI),* Available at: http://www.ecma-international.org/memento/TC47-M.htm, June 2006.

[12] ETSI TS, ETSI TS 102 622, *Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI),* Technical Specification, February 2008.

[13] NFC Forum, *NFC Forum Type Tags*, Available at: http://www.nfc-forum.org/resources/white_papers/NXP_BV_Type_Tags_White_Paper-Apr_09.pdf, 2009.

[14] NFC Forum, *NFC Data Exchange Format (NDEF),* Technical Specification, Version 1.0, July 2006.

[15] NFC Forum, *Record Type Definition (RTD),* Technical Specification, Version 1.0, July 2006.

[16] M. Isomursu, "Tags and the City", *PsychNology Journal*, 6 (2), 131-156, 2008.

[17] E. Siira and J. Haikio, "Experiences from Near-Field Communication (NFC) in a Meal Service System", *Proceedings of First Annual RFID Eurasia*, Istanbul, Turkey, 1-6, 2007.

[18] P. Nepper, N. Konrad, and U. Sandner, "Talking Media", *Proceedings of the 9th International Conference on Human Computer Interaction with Mobile Devices and Services*, 348-350, 2007.

[19] I. Cappiello, S. Puglia and A. Vitaletti, "Design and Initial Evaluation of a Ubiquitous Touch-Based Remote Grocery Shopping Process", *Proceedings of the First International Workshop on Near Field Communication*, Hagenberg, Austria, 9-14, 2009.

[20] I. Sánchez, M. Cortés and J. Riekki, "Controlling Multimedia Players using NFC Enabled Mobile Phones", *Proceedings of the 6th International Conference on Mobile and Ubiquitous Multimedia*, Oulu, Finland, 118- 124, 2007.

[21] I. Sánchez, J. Riekki and M. Pyykkönen, "Touch & Control: Interacting with Services by Touching RFID Tags", *Proceedings of the Second International Workshop on RFID Technology - Concepts, Applications, Challenges*, Barcelona, SPAIN, 53-62, 2008.

[22] Iván Sánchez *et al.*, "Touch & Compose: Physical User Interface for Application Composition in Smart Environments", *Proceedings of First International Workshop on Near Field Communication,* Hagenberg, Austria, 61-66, 2009.

[23] W. Rudametkin, L. Touseau, M. Perisanidi, A. Gómez and D. Donsez, "NFCMuseum: an Open-Source Middleware for Augmenting Museum Exhibits", *Proceedings of the International Conference on Pervasive Services,* Sorrento, Italy, 2008.

[24] U. Sandner, F. Resatsch, P. Nepper, J. M. Leimeister and H. Krcmar, "News-on-the-Go", *Proceedings of 9th International Conf. on Human Computer Interaction with Mobile Devices and Services*, Singapore, 361-363, 2007.

[25] F. Kneissl *et al.*, "All-I-Touch as Combination of NFC and Lifestyle", *Proceedings of First International Workshop on Near Field Communication,* Hagenberg, Austria, 51-55, 2009.

[26] R. Hardy, E. Rukzio, P. Holleis, G. Broll and M. Wagner, "MyState: Using NFC to Share Social and Contextual Information in a Quick and Personalized Way", *Proceedings of the 12th ACM International Conference Adjunct Papers on Ubiquitous Computing*, 2010.

[27] H. Aziza, "NFC Technology in Mobile Phone Next-Generation Services", *Proceedings of the Second International Workshop on Near Field Communication*, Monaco, 21-26, 2010.

[28] NFC Forum, *Logical Link Control Protocol,* Technical Specification, Version 1.0, December 2009.

[29] J. Haikio *et al.*, "Would You Be My Friend? - Creating a Mobile Friend Network with Hot in the City", *Proceedings of 43rd Hawaii International Conf. on System Sciences*, Hawaii, USA, IEEE, 1-10, 2010.

[30] P. Dobrigkeit *et al.*, "Exchange of Contact Data Between Mobile Phones Using NFCIP", *Fourth European Workshop on RFID Systems and Technologies (RFID SysTech)*, Freiburg, Germany, 1-9. 44, 2008.

[31] A. Nandwani *et al.*, "NFC Mobile Parlor Games Enabling Direct Player to Player Interaction", *Proceedings of Third International Workshop on Near Field Communication*, Hagenberg, Austria, 21-25, 2011.

[32] Payez Mobile, Available at: http://www.payezmobile.com.

[33] GSM World, *Pay-Buy-Mobile,* Available: http://www.gsm.org/our-work/mobile_lifestyle/mobile_money/pay_buy_mobile/index.htm.

[34] D. Baldo, G. Benelli and A. Pozzebon, "The SIESTA project: Near Field Communication Based Applications for Tourism", *International Symposium on Communication Systems Networks and Digital Signal Processing,* Newcastle upon Tyne, 721 – 725, 2010.

[35] G. Benelli and A. Pozzebon, "An Automated Payment System for Car Parks Based on Near Field Communication Technology", *International Conference for Internet Technology and Secured Transactions,* London, 1-6, 2010.

[36] M. Aigner, S. Dominikus and M. Feldhofer, "A System of Secure Virtual Coupons Using NFC Technology", *Proceedings of 5th IEEE International Conf. on Pervasive Computing and Communications*, New York, USA, 362-366, 2007.

[37] S. Dominikus and M. Aigner, "mCoupons: An Application for Near Field Communication (NFC)", *Proceedings of 21st International Conf. on Advanced Networking and Applications Workshops/Symposia,* Niagara Falls, CANADA, 421-428, 2007.

[38] H. C. Hsiang *et al.*, "A Secure mCoupon Scheme Using Near Field Communication", *International Journal of Innovative Computing, Information and Control,* 5 (11), 3901–3909, November 2009.

[39] M. Pasquet, J. Reynaud and C. Rosenberger, "Secure Payment with NFC Mobile Phones in The Smart Touch Project", *International Symposium on Collaborative Technologies and Systems,* Irvine, CA, 121 – 126, 2008.

[40] S. L. Ghiron *et al.*, "NFC Ticketing: a Prototype and Usability Test of an NFC-based Virtual Ticketing Application", *Proceedings of First International Workshop on Near Field Communication*, Hagenberg, Austria, 45-50, 2009.

[41] J. Neefs, F. Schrooyen and J. Doggen, "Paper ticketing vs. Electronic Ticketing Based on Off-line System 'Tapango'", *Proceedings of Second International Workshop on Near Field Communication*, Monaco, 3-8, 2010.

[42] G. Van Damme, K. Wouters, H. Karahan, and B. Preneel, "Offline NFC Payments with Electronic Vouchers", *Proceedings of the First ACM Workshop on Networking, Systems, and Applications for Mobile Handhelds*, 2009.

[43] Kiran S. Kadambi *et al.*, "Near-Field Communication-Based Secure Mobile Payment Service", *Proceedings of the 11th International Conference on Electronic Commerce*, 2009.

[44] K. Ok, M. N. Aydin, V. Coskun and B. Ozdenizci, "Current Benefits and Future Directions of NFC Services", *Proceedings of IEEE International Conference on Education and Management Technology*, Cairo, Egypt, 334-338, November 2010.

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

[46] EMVCo, *Contactless Mobile Payment Architecture Overview*, Available at: http://www.emvco.com/best_practices.aspx?id=162, 2010.

[47] M. Reveilhac and M. Pasquet, "Promising Secure Element Alternatives for NFC Technology", *Proceedings of the First International Workshop on Near Field Communication*, Hagenberg, Austria, 75-80, 2009.

[48] Mobey Forum, *Alternatives for Banks to offer Secure Mobile Payments*, Available at: http://www.mobeyforum.org/Press-Documents/Press-Releases/Alternatives-for-Banks-to-offer-Secure-Mobile-Payments, 2010.

[49] Smart Trust, *The role of SIM OTA and the Mobile Operator in the NFC Environment*, Available at: http://www.paymentscardsandmobile.com/research/reports/SIM-OTA-Mobile-Operator-role-NFC.pdf, 2009.

[50] StoLPaN, *Description of the Life-cycle management of NFC Applications*, Available at: http://www.nfc-forum.org/resources/white_papers/Stolpan_White_Paper_08.pdf, 2011.

[51] J. Langer and M. Roland, Anwendungen und Technik von Near Field Communication (NFC), ISBN: 978-3-642-05496-9, Springer, 2010.

[52] GlobalPlatform, *GlobalPlatform Card Specification*, Version 2.2, http://www.globalplatform.org/specificationscard.asp, March 2006.

[53] Mobey Forum Enrollment Task Force, *Best Practices for Mobile Financial Services,* MOBEY Forum, Available at: http://www.mobeyforum.org/content/download/460/2768/file/Best%20Practices%20for%20MFS%20Enrolment%20Business%20model%20analysis%20final.pdf, 2008.

[54] Smart Card Alliance, *Security of Proximity Mobile Payments,* A Smart Card Alliance Contactless and Mobile Payments Council White Paper, Available at: http://www.smartcardalliance.org/resources/pdf/Security_of_Proximity_Mobile_Payments.pdf, May 2009.

[55] GlobalPlatform, *GlobalPlatform's Proposition for NFC Mobile: Secure Element Management and Messaging,* White Paper, Available at: http://www.globalplatform.org/documents/GlobalPlatform_NFC_Mobile_White_Paper.pdf, April 2009.

[56] G. Madlmayr *et al.*, "Managing an NFC Ecosystem", *Proceedings of the 7th International Conference on Mobile Business,* Barcelona, Spain, 95-101, 2008.

[57] GSMA, *Pay-Buy Mobile Business Opportunity Analysis,* Version 1.0, White Paper, Available at: http://www.gsmworld.com/documents/gsma_nfc_tech_guide_vs1.pdf, November 2007.

[58] GSMA, *Mobile NFC Services,* Version 1.0, Available at: http://www.gsmworld.com/documents/nfc_services_0207.pdf, February 2007.

[59] Smart Card Alliance, *Proximity Mobile Payments Business Scenarios: Research Report on Stakeholder Perspectives,* White Paper, Available at: http://www.smartcardalliance.org/resources/lib/Mobile_Payment_Business_Model_Research_Report.pdf, July 2008.

[60] B. Sharp and A. Sharp, "Loyalty Programs and Their Impact on Repeat-Purchase Loyalty Patterns", *International Journal of Research in Marketing,* 14 (5), 473-486, December 1997.

[61] K. Markantonakis and K. Mayes, "An Overview of the GlobalPlatform Smart Card Specification", *Information Security Technical Report,* 8 (1), 17-29, March 2003.

[62] D. Sauveron, "Multi-application Smart Card: Towards an Open Smart Card?", *Information Security Technical Report,* 14 (2), 70-78, May 2009.

[63] K. Markantonakis and K. Mayes, “A Secure Channel Protocol for Multi-Application Smart Cards Based On Public Key Cryptography”, *Information Security Group Smart Card Centre,* 2010.

[64] W3C Recommendation, Extensible Markup Language (XML) 1.0, Available at: http://www.w3.org /TR/RECxml.

[65] P. Ruppel and F. Gschwandtner, “Spontaneous and Privacy-Friendly Mobile Indoor Routing and Navigation”, *Proceedings of Second Workshop on Services, Platforms, Innovations and Research for New Infrastructures in Telecommunications,* Lübeck, 2574-2583, 2009.

[66] Wikipedia, *Global Positioning System,* Available at: http://en.wikipedia.org/wiki/Global_Positioning_System.

[67] V. Renaudin, O. Yalak, P. Tomé, and B. Merminod, “Indoor Navigation of Emergency Agents”, *European Journal of Navigation*, 5, 36-45, 2007.

[68] R. Ivanov, “Indoor Navigation System for Visually Impaired”, *Proceedings of International Conference on Computer Systems and Technologies*, Sofia, 143-149, 2010.

[69] T. Ishikawa, H. Fujiwara, O. Imai, and A. Okabe, “Wayfinding with a GPS-Based Mobile Navigation System: A Comparison with Maps and Direct Experience”, *Journal of Environmental Psychology*, 28, 74-82, 2008.

[70] P. Y. Gilliéron and B. Merminod, “Personal Navigation System for Indoor Applications”, *Proceedings of 11th IAIN World Congress*, Berlin, 2003.

[71] A. K. L. Miu, *Design and Implementation of an Indoor Mobile Navigation System,* M.S. Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, USA, 2002.

[72] I. Heywood, S. Cornelius, and S. Carver, *An Introduction to Geographical Information Systems,* UK: Pearson Prentice Hall, Chapter 3, 2006.

[73] P.-Y. Gilliéron, D. Büchel, I. Spassov, and B. Merminod, “Indoor Navigation Performance Analysis”, *Procedings of 8th European Navigation Conference GNSS,* Rotterdam, 2004.

Curriculum Vitae

Büşra Özdenizci was born in 16 December 1987, in Trabzon. She received her BA degree in Business Administration in 2009 and her BS degree in Information Technology in 2010 from Işık University, Istanbul. She is currently working as a teaching and research assistant at the department of Information Technology of Işık University. Her research areas include Near Field Communication, Mobile Communication Technologies and Mobile Persuasion.

Other Conference Proceedings:

- B. Ozdenizci, M. N. Aydin, V. Coskun and K. Ok, NFC Research Framework: A Literature Review and Future Research Directions, Proc. of 14th International Business Information Management Association Conf. on Global Business Transformation through Innovation and Knowledge Management, Istanbul, TURKEY, 23-24 June 2010, 2672-2685.
- B. Ozdenizci, M. N. Aydin, V. Coskun and K. Ok, Design Science in NFC Research, *Proceedings of IEEE International Conference for Internet Technology and Secured Transactions,* London, 8-11 November 2010, 158-163.
- K. Ok, M. N. Aydin, V. Coskun and B. Ozdenizci, Current Benefits and Future Directions of NFC Services, *Proceedings of IEEE International Conference on Education and Management Technology,* Cairo, Egypt, 2-4 November 2010, 334-338.
- K. Ok, M. N. Aydin, V. Coskun and B. Ozdenizci, Exploring Underlying Values of NFC Applications, *Proceedings of International Conference on Management Technology and Applications,* Singapore, 10-12 September 2010, 283-287.